UNIVERSIDADE FEDERAL DE PELOTAS
Centro de Desenvolvimento Tecnológico
Programa de Pós-Graduação em Computação

Dissertação

Investigação do Impacto de Fenômenos de Variabilidade e do Efeito BTI na Robustez de Contramedidas a Ataques DPA/DEMA

Plínio Finkenauer Junior

Pelotas, 2020

Plínio Finkenauer Junior

Investigação do Impacto de Fenômenos de Variabilidade e do Efeito BTI na Robustez de Contramedidas a Ataques DPA/DEMA

Dissertação apresentada ao Programa de Pós-Graduação em Computação do Centro de Desenvolvimento Tecnológico da Universidade Federal de Pelotas, como requisito parcial à obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Rafael Iankowski Soares
Coorientador: Prof. Dr. Vinícius Valduga de Almeida Camargo

Pelotas, 2020

Universidade Federal de Pelotas / Sistema de Bibliotecas
Catalogação na Publicação

F511i Finkenauer Junior, Plínio

Investigação do impacto de fenômenos de variabilidade e do efeito BTI na robustez de contramedidas a ataques DPA/DEMA / Plínio Finkenauer Junior ; Rafael Soares Iankowski, orientador ; Vinícius Valduga de Almeida Camargo, coorientador. — Pelotas, 2020.

107 f. : il.

Dissertação (Mestrado) — Programa de Pós-Graduação em Computação, Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas, 2020.

1. Criptografia. 2. Ataques de canal lateral. 3. Lógica com pré-carga em trilha dupla. 4. Variabilidade de processo. 5. BTI. I. Iankowski, Rafael Soares, orient. II. Camargo, Vinícius Valduga de Almeida, coorient. III. Título.

CDD : 005

Elaborada por Maria Inez Figueiredo Figas Machado CRB: 10/1612

Plínio Finkenauer Junior

Investigação do Impacto de Fenômenos de Variabilidade e do Efeito BTI na Robustez de Contramedidas a Ataques DPA/DEMA

Dissertação aprovada, como requisito parcial, para obtenção do grau de Mestre em Ciência da Computação, Programa de Pós-Graduação em Computação, Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas.

Data da Defesa: 05 de junho de 2020

Banca Examinadora:

Prof. Dr. Rafael Iankowski Soares (orientador)
Doutor em Ciências da Computação pela Pontifícia Universidade Católica do Rio Grande do Sul.

Prof. Dr. Vinícius Valduga de Almeida Camargo (coorientador)
Doutor em Microeletrônica pela Universidade Federal do Rio Grande do Sul.

Prof. Dr. Alan Carlos Junior Rossetto
Doutor em Microeletrônica pela Universidade Federal do Rio Grande do Sul.

Prof. Dr. Leomar Soares da Rosa Junior
Doutor em Microeletrônica pela Universidade Federal do Rio Grande do Sul.

Everything passes, but nothing entirely goes away.
— JENNY DISKI

RESUMO

FINKENAUER JUNIOR, Plínio. **Investigação do Impacto de Fenômenos de Variabilidade e do Efeito BTI na Robustez de Contramedidas a Ataques DPA/DEMA**. Orientador: Rafael Iankowski Soares. 2020. 107 f. Dissertação (Mestrado em Ciência da Computação) – Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas, Pelotas, 2020.

Ataques a canais laterais constituem uma classe de técnicas que exploram vulnerabilidades oriundas da implementação física de um sistema criptográfico para extrair dados confidenciais. A despeito da pressuposta segurança proporcionada por protocolos criptográficos, os ataques a canais laterais beneficiam-se da inerente correlação existente entre dados processados por um sistema e propriedades físicas propagadas por este. Visando neutralizar a ação desses ataques, contramedidas são propostas com o intuito de suprimir a correlação identificável. Apesar de proporcionarem uma significativa redução da dependência dos dados, a mesma não pode ser completamente removida. Complementarmente, a ininterrupta diminuição de escala na tecnologia CMOS acarreta no aumento e relevância de fatores de variabilidade e envelhecimento em parâmetros que interferem no comportamento de circuitos integrados. Assim, intensifica-se a necessidade pelo projeto de circuitos capazes de garantir o sigilo de informações e que apresentem uma maior confiabilidade ao nível de sistema. Sob esse panorama, este trabalho se propôs a investigar o impacto de fenômenos de variabilidade e do efeito BTI no contexto da segurança apresentada por circuitos projetados para prevenção aos ataques por canais laterais. Os resultados obtidos demonstraram que a variabilidade de processo afeta severamente a proteção fornecida pelas contramedidas, reduzindo substancialmente sua eficácia e, portanto, não devendo ser negligenciada por projetistas de dispositivos criptográficos. A avaliação de fenômenos de variabilidade que ocorrem em diferentes escalas espaciais permitiu concluir que os efeitos locais são mais prejudiciais à segurança das contramedidas, devido ao maior desbalanceamento interno provocado. Adicionalmente, verificou-se que contramedidas implementadas em tecnologias com dimensões mais diminutas apresentam maior dano à proteção, considerando a maior influência dos efeitos locais. Ademais, a análise de *corners*, realizada a partir de simulações determinísticas, mostrou-se insuficiente em abranger os fatores de variabilidade, corroborando a necessidade por simulações estatísticas. Por outro lado, a influência da degradação decorrente do efeito BTI não se manifestou de maneira significativa na segurança das contramedidas, comportando-se de maneira heterogênea, apesar do impacto negativo causado no atraso de propagação dos circuitos.

Palavras-chave: Criptografia. Ataques de Canal Lateral. Ataques por Análise de Potência. Lógica com Pré-Carga em Trilha Dupla. Variabilidade de Processo. BTI.

ABSTRACT

FINKENAUER JUNIOR, Plínio. **Investigation of the Impact of Process Variability and BTI Aging on the Robustness of Countermeasures to DPA/DEMA Attacks**. Advisor: Rafael Iankowski Soares. 2020. 107 f. Dissertation (Masters in Computer Science) – Technology Development Center, Federal University of Pelotas, Pelotas, 2020.

Side-channel attacks consist of a class of techniques that exploit vulnerabilities emerging from the physical implementation of a cryptographic system to extract confidential data. Despite the supposed security provided by cryptographic protocols, side-channel attacks benefit from the inherent correlation between data processed by a system and the physical properties propagated by it. Aiming to neutralize the action of these attacks, countermeasures are designed intending to thwart the correlation. Although they provide a significant reduction in data dependency, this correlation cannot be completely removed. Additionally, the downscaling of CMOS technology results in the increase and relevance of factors of variability and aging on parameters that interfere with integrated circuits. Thus, it intensifies the need for circuits capable of ensuring the confidentiality of the information and offering higher reliability at the system level. Under this scenario, this work proposes to investigate the impact of variability phenomena and the BTI effect in the security provided by circuits designed to prevent side-channel attacks. The obtained results demonstrated that process variability severely affects the protection provided by countermeasures, substantially reducing their effectiveness, and should not be neglected by designers of cryptographic devices. By evaluating the variability phenomena that occur at different spatial scales, we conclude that local effects are more damaging to the safety of countermeasures, due to the higher internal unbalancing it causes. Additionally, we verified that countermeasures implemented in smaller technologies present more damage to their protection, given the higher impact of local effects. Furthermore, the corner analysis, performed through deterministic simulations, showed to be insufficient to incorporate the variability factors, corroborating the need for statistical simulations. On the other hand, the influence of degradation due to the BTI effect did not manifest itself significantly in the safety of the countermeasures, showing a heterogeneous behavior, despite the negative impact observed on the delay of the circuits.

Keywords: Cryptography. Side Channel Attacks. Power Analysis Attacks. Dual-rail Pre-charge Logic. Process Variability. BTI.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryption Standard*
ASIC	*Application Specific Integrated Circuit*
BSIM	*Berkeley Short-channel IGFET Model*
BTI	*Bias Temperature Instability*
CI	Circuito Integrado
CMOS	*Complementary Metal-Oxide Semiconductor*
CPL	*Complementary Pass-Transistor Logic*
DEMA	*Differential Electromagnetic Analysis*
DES	*Data Encryption Standard*
DF	*Duty Factor*
DPA	*Differential Power Analysis*
DPDN	*Differential Pull-Down Network*
DPL	*Dual-rail Pre-charge Logic*
DPPL	*Differential Pass-transistor Pre-charge Logic*
DR	*Dual-Rail*
DUT	*Device Under Test*
FF	*Fast-Fast*
HCI	*Hot-Carrier Injection*
IoT	*Internet of Things*
iDDPL	*Improved Delay-based Differential Pre-charge Logic*
KDE	*Kernel Density Estimation*
LER	*Line Edge Roughness*
LV	*Letter-Value*
LWR	*Line Width Roughness*
MC	Monte Carlo
MGG	*Metal Gate Granularity*

NBTI *Negative Bias Temperature Instability*
NED *Normalized Energy Deviation*
NMOS *N-channel Metal Oxide Semiconductor*
NSD *Normalized Standard Deviation*
PAA *Power Analysis Attack*
PBTI *Positive Bias Temperature Instability*
PCSL *Pre-Charge Static Logic*
PGG *Poly Gate Granularity*
PMOS *P-channel Metal Oxide Semiconductor*
PL *Pre-charge Logic*
PTM *Predictive Technology Model*
QQ Quantil-Quantil
R-D *Reaction-Diffusion*
RDF *Random Dopant Fluctuations*
RET *Resolution Enhancement Techniques*
RTN *Random Telegraph Noise*
SABL *Sense Amplifier Based Logic*
SCA *Side Channel Attack*
SEMA *Simple Electromagnetic Analysis*
SET *Single Event Transient*
SPA *Simple Power Analysis*
SPICE *Simulation Program with Integrated Circuit Emphasis*
SS *Slow-Slow*
T-D *Trapping-Detrapping*
TDPL *Three-phase Dual-rail Pre-charge Logic*
WDDL *Wave Dynamic Differential Logic*
WFV *Work Function Variation*

SUMÁRIO

1 INTRODUÇÃO

O crescente desenvolvimento de aplicações e sistemas no domínio da Internet das Coisas (*Internet of Things* - IoT), acompanhado pela proliferação de sistemas eletrônicos embarcados, apontam para um aumento na demanda pela segurança dos dados. Relatórios recentes presumem que o número de dispositivos conectados à internet será mais de três vezes o tamanho da população global em 2023, representando 29,3 bilhões de dispositivos (CISCO, 2020). Cerca de metade dessas conexões, 14,7 bilhões, suportará uma ampla variedade de aplicações IoT. No Brasil, estima-se que a disseminação de sistemas IoT possa gerar, no aspecto econômico, receitas entre 50 e 200 bilhões de dólares em 2025 (BNDES, 2017).

Concomitantemente ao progresso tecnológico apontado, emergem preocupações acerca da proteção de dados pessoais e da segurança de informação. Assim, tais sistemas precisam adotar protocolos de criptografia para manter a confidencialidade e a integridade dos dados. Ademais, os protocolos de criptografia já são amplamente empregados para garantir a autenticação em transições que utilizam *smart cards* e a comunicação segura entre usuários na internet (FUJINO; KUBOTA; SHIOZAKI, 2017).

A criptografia consiste em um conjunto de procedimentos que permite a proteção de informações e o compartilhamento de mensagens de maneira sigilosa. Para isso, algoritmos criptográficos são concebidos através de funções matemáticas que aplicam uma chave secreta ao dado a ser transmitido, ocultando informações confidenciais do usuário. Como os algoritmos de criptografia são públicos, atribui-se à esta chave criptográfica o segredo da encriptação da mensagem. Assim, o objetivo de um agente malicioso é revelar a chave secreta e, consequentemente, obter acesso às informações sigilosas. Para os algoritmos criptográficos atuais, tais como o AES (*Advanced Encryption Standard*), não há uma maneira efetiva para recuperar a chave, além de uma busca exaustiva por todas as possibilidades de chave correta. Entretanto, o tamanho de chave criptográfica adotada pelo AES, por exemplo, varia de 128 a 256 bits, tornando necessário um tempo imensamente longo para examinar todas as alternativas de chave secreta. Portanto, assume-se que um sistema criptográfico com o tamanho de chave suficientemente grande é computacionalmente seguro.

Apesar de sua pressuposta proteção no nível do *software*, a implementação em *hardware* de um sistema ainda é vulnerável a um ataque por canal lateral (em inglês, *Side Channel Attack* - SCA) (KOCHER, 1996). Os SCAs visam revelar chaves criptográficas com base nas informações vazadas a partir de canais físicos de um circuito durante sua execução, como por exemplo o consumo de energia (KOCHER; JAFFE; JUN, 1999), o tempo de processamento (KOCHER, 1996) e as emissões eletromagnéticas (QUISQUATER; SAMYDE, 2001). Essa categoria de ataques representa uma severa ameaça aos módulos que integram os sistemas criptográficos, visto que tais técnicas provaram-se bem sucedidas em revelar a chave secreta de algoritmos implementados em uma variedade de plataformas, desde *smart cards* (KASPER; OSWALD; PAAR, 2012) até circuitos integrados de aplicação específica (em inglês, *Application Specific Integrated Circuit* - ASIC) (ÖRS et al., 2004). Nesse cenário, é necessário considerar a segurança dos algoritmos de criptografia conjuntamente com os dispositivos que os implementam.

A abordagem de ataque que investiga a correlação entre os dados processados por um sistema criptográfico e seu consumo de energia é denominada Análise Diferencial de Potência (em inglês, *Differential Power Analysis* - DPA). A Análise Diferencial Eletromagnética (em inglês, *Differential Electromagnetic Analysis* - DEMA) aplica um procedimento semelhante ao proposto em DPA, considerando a radiação eletromagnética emitida pelo sistema criptográfico. Em ambos os ataques, busca-se identificar a chave secreta baseando-se no fato de que as operações realizadas durante a execução do algoritmo criptográfico possuem características de potência ou radiação eletromagnética dependentes dos dados processados (TIRI; VERBAUWHEDE, 2003).

Visando minimizar a eficácia desses ataques, diferentes contramedidas vêm sendo propostas na literatura. A principal abordagem destas ações consiste em remover as dependências entre os valores processados e a grandeza física analisada, reduzindo assim a fuga de informações (MANGARD; OSWALD; POPP, 2007). As contramedidas podem ser projetadas em variados níveis de abstração, porém tendem a ser mais efetivas aos SCAs em níveis mais baixos de implementação (SAKIYAMA; SASAKI; LI, 2015). No contexto de DPA e DEMA, essas técnicas visam a implementação de células lógicas que apresentem o consumo de energia independente dos dados, ou seja, o mesmo consumo para todos os dados computados. Para isso, as ações propostas buscam a definição de células lógicas obtidas a partir de um arranjo de transistores capaz de produzir caminhos balanceados, a fim de obter, durante a computação dos dados, características elétricas similares em termos de capacitâncias internas, corrente e tensão elétrica.

Não obstante, o processo de fabricação de circuitos integrados (CIs) ocasiona a introdução de desvios aleatórios nas características físicas dos transistores, causando o desequilíbrio dos CIs, o qual acarreta em vulnerabilidades que enfraquecem os proto-

colos de segurança (BURLESON; MUTLU; TIWARI, 2016). A contínua miniaturização dos transistores na tecnologia CMOS (*Complementary Metal-Oxide Semiconductor*), motivada pela busca por uma maior densidade de integração e redução do atraso de um circuito, provoca um aumento na variabilidade de parâmetros elétricos deste, impactando todos os aspectos do desempenho de um sistema (REIS; WIRTH; CAO, 2015). Estes fenômenos de variabilidade podem ser categorizados em espaciais e temporais. Os efeitos espaciais podem ser detectados imediatamente após a fabricação e são fixos no tempo. Em contrapartida, efeitos temporais são variáveis em relação ao tempo e provocam alterações no funcionamento do circuito devido a condições de operação (MARICAU; GIELEN, 2013). Ademais, efeitos temporais não são detectados durante a etapa de teste, pois esta é realizada na fábrica antes de ocorrer a degradação no circuito.

Os fenômenos espaciais são decorrentes do processo de fabricação e podem ser divididos em globais e locais, conforme a escala em que ocorrem. Tais fenômenos também podem ser classificados de acordo com o impacto causado no CI, sendo modelados como fatores aleatórios ou sistemáticos (AGARWAL; NASSIF, 2007). Efeitos estocásticos, como a flutuação aleatória de dopantes (em inglês, *Random Dopant Fluctuations* - RDF) (MAHMOODI; MUKHOPADHYAY; ROY, 2005), apresentam grande potencial de influência na segurança de contramedidas, visto que acarretam na variação de parâmetros elétricos do dispositivo (KUHN et al., 2008).

Os efeitos temporais, por sua vez, se classificam em mecanismos transientes e de envelhecimento. Fenômenos transientes são oriundos de sinais que interferem no funcionamento típico do circuito, tais como efeitos de ruído ou perturbações eletromagnéticas originadas por partículas ionizantes. Esses efeitos transientes distorcem apenas temporariamente o desempenho do circuito (MARICAU; GIELEN, 2013). Em contraste, efeitos de envelhecimento causam uma degradação gradual de características do CI, podendo acarretar em falhas permanentes no sistema. Os fenômenos de envelhecimento, tal como o *Bias Temperature Instability* (BTI), são dependentes do histórico de uso dos transistores (SCHRODER; BABCOCK, 2003). Assim, um uso desbalanceado destes tende a ocasionar um desequilíbrio no circuito criptográfico.

No entanto, o impacto dos fenômenos de variabilidade na proteção de contramedidas ao nível de transistor não foi suficientemente investigado na literatura. Estudos realizados por LIN; BURLESON (2009) e RENAULD et al. (2011) demonstraram que a maneira convencional de avaliar a segurança contra ataques por análise de potência não é suficiente na presença de variações provocadas pelo processo de fabricação. Contudo, estes trabalhos concentram-se majoritariamente nos efeitos provenientes de fenômenos globais. As consequências oriundas de efeitos de envelhecimento na segurança de contramedidas, especificamente resultantes do fenômeno BTI, foram investigadas por GUO et al. (2015). De acordo com os autores, os ataques tradicionais

por análise de potência não são significativamente afetados por fenômenos de envelhecimento. De forma semelhante, KARIMI; MOOS; MORADI (2019) argumentam que a quantidade de informação explorável por ataques de análise de potência é reduzida quando o dispositivo opera após um período de tempo. Entretanto, os experimentos realizados neste trabalho basearam-se em implementações desprotegidas, ou seja, sem a aplicação de técnicas de contramedidas.

Com base no panorama apresentado, este trabalho tem como objetivo principal investigar e compreender o impacto de modelos de variabilidade e degradação no grau de proteção de contramedidas de ocultação voltadas para ataques a canais laterais. A despeito da concepção de variadas técnicas de proteção, estas não contemplam a ação da variabilidade em suas soluções. Dessa forma, considerando as lacunas existentes relativas à avaliação dos efeitos de variabilidade e degradação em circuitos de contramedidas, justifica-se a necessidade de abranger a influência dos mecanismos de variabilidade supracitados, possibilitando uma análise mais precisa do nível de proteção destas soluções propostas na literatura.

O trabalho está estruturado da seguinte forma: no Capítulo 2 é realizada a fundamentação teórica referente aos ataques a canais laterais, onde abordam-se os principais conceitos relacionados à análise de potência e às contramedidas estudadas. No Capítulo 3, apresenta-se o tópico de confiabilidade de circuitos digitais, descrevendo os efeitos de variabilidade e degradação tratados. No Capítulo 4, é exposta a metodologia proposta para a análise dos efeitos de confiabilidade, enquanto o Capítulo 5 apresenta os resultados obtidos. Por fim, o Capítulo 6 expõe as considerações finais e o direcionamento futuro do trabalho.

2 ATAQUES A CANAIS LATERAIS

A criptoanálise é uma ciência cujo objetivo envolve descobrir dados cifrados, beneficiando-se de vulnerabilidades dos sistemas criptográficos. Tais sistemas aplicam uma chave criptográfica para modificar um dado de entrada, denominado texto simples, para um dado codificado, denominado texto cifrado. Tradicionalmente, um agente malicioso busca investigar a estrutura interna do algoritmo criptográfico, explorando expressões matemáticas para predizer a chave secreta ou recuperar a informação não cifrada (PAAR; PELZL, 2009). Porém, desde a publicação de KOCHER (1996), uma nova classe de ataques contra sistemas criptográficos tem se expandido. Nestes ataques, a estratégia adotada para explorar as vulnerabilidades fundamenta-se nas características de operação do sistema em que o algoritmo foi implementado (RÖMER; SEIFERT, 2001). Essas características, tais como o tempo de processamento, consumo de energia ou emissão de radiação eletromagnética, são inerentes ao funcionamento do sistema e são intituladas *canais laterais*. A Figura 1 ilustra a fuga de informações por meio de canais laterais.

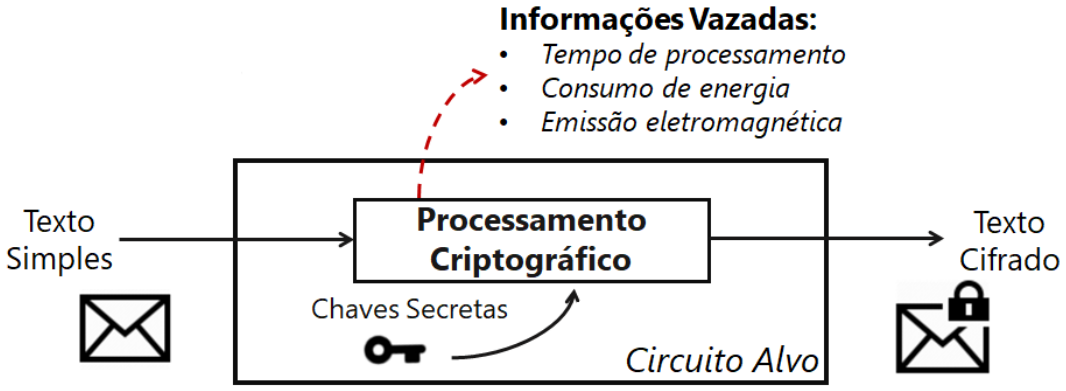


Figura 1 – Representação da fuga de informações por canais laterais.

Os ataques a canais laterais (SCA) visam extrair a informação processada por um sistema, monitorando o vazamento intrínseco das grandezas físicas (TILBORG, 2005). Considerando que as informações vazadas por meio dos canais laterais dependem dos dados computados durante a execução do algoritmo criptográfico, es-

tando diretamente correlacionadas com a chave secreta, um agente mal intencionado pode realizar um ataque para obter a chave e, assim, ser capaz de revelar os dados confidenciais (BARENGHI et al., 2012).

Os ataques a sistemas criptográficos podem ser categorizados por dois critérios (SPREITZER et al., 2018). O primeiro os divide em ataques passivos, no qual o sistema criptográfico opera normalmente e as propriedades físicas deste são observadas; e ativos, no qual o sistema criptográfico é deliberadamente manipulado para ter o seu comportamento alterado. O segundo critério classifica os ataques em invasivos e não-invasivos. Nos ataques invasivos, o sistema criptográfico pode ser operado e examinado conforme for conveniente. Por outro lado, ataques não-invasivos exploram apenas as interfaces diretamente acessíveis do sistema, não deixando evidências do ataque. Particularmente, ataques passivos que monitoram a potência dissipada ou a radiação eletromagnética emitida por um sistema tornaram-se um tópico de notória atenção na comunidade científica, pois suas informações de canal lateral podem ser facilmente adquiridas utilizando instrumentos de medição não-invasivos.

O restante do capítulo está dividido da seguinte maneira: a Seção 2.1 apresenta os métodos de ataque pela análise de potência, abordando o consumo de energia em circuitos integrados. A Seção 2.2 expõe as contramedidas aos ataques, relatando as diferentes topologias investigadas; e, por fim, a Seção 2.3 apresenta as métricas empregadas para avaliar a robustez das contramedidas.

2.1 Ataques por Análise de Potência

A exequibilidade de um ataque por análise de potência (em inglês, *Power Analysis Attack* - PAA) fundamenta-se na forte dependência existente entre a potência dissipada por um sistema digital com seus dados processados internamente e operações executadas (BELLIZIA et al., 2017). PAAs exploram essa correlação para inferir informações confidenciais. Tipicamente, a potência dissipada pelo circuito é monitorada através da corrente que flui pela fonte de alimentação do sistema criptográfico. As variações no consumo de energia são então medidas e armazenadas utilizando um osciloscópio digital. Essas variações capturam a atividade de chaveamento dos transistores e são dependentes dos dados computados pelo algoritmo criptográfico. A Figura 2 apresenta uma configuração genérica para obtenção dos traços e realização de um ataque por análise de potência.

O conjunto de amostras de potência medidas durante a execução do sistema atacado em resposta a uma dada entrada é chamado de traço de consumo. PAAs tem êxito em extrair informação de um sistema, porque os perfis dos traços de consumo se manifestam de maneira diferente para diferentes dados e diferentes operações (MANGARD; OSWALD; POPP, 2007). Uma vez que os traços tenham sido adquiridos,

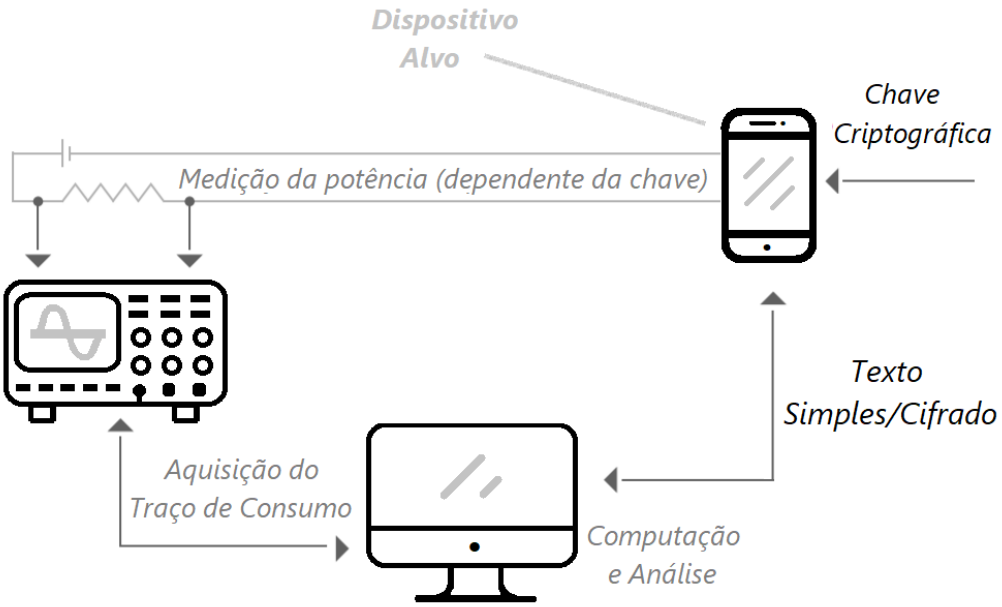


Figura 2 – Configuração típica para realização de um ataque por análise de potência.

realizam-se as análises para obter os dados secretos. A Análise Simples de Potência (em inglês, *Simple Power Analysis* - SPA) (KOCHER; JAFFE; JUN, 1999) é um método de ataque que inspeciona características que são visíveis diretamente em único traço de potência. A Figura 3 exibe um exemplo de traço de consumo, no qual é possível observar as diferentes operações executadas por um sistema. SPAs requerem conhecimento detalhado a respeito da implementação do algoritmo no *hardware* atacado. Em contrapartida, a Análise Diferencial de Potência (DPA) é um método mais efetivo, que emprega uma avaliação estatística e modelos de consumo de potência aplicados a uma quantidade elevada de traços para revelar a chave criptográfica do sistema. Esta análise será abordada com mais detalhes na subseção 2.1.2.

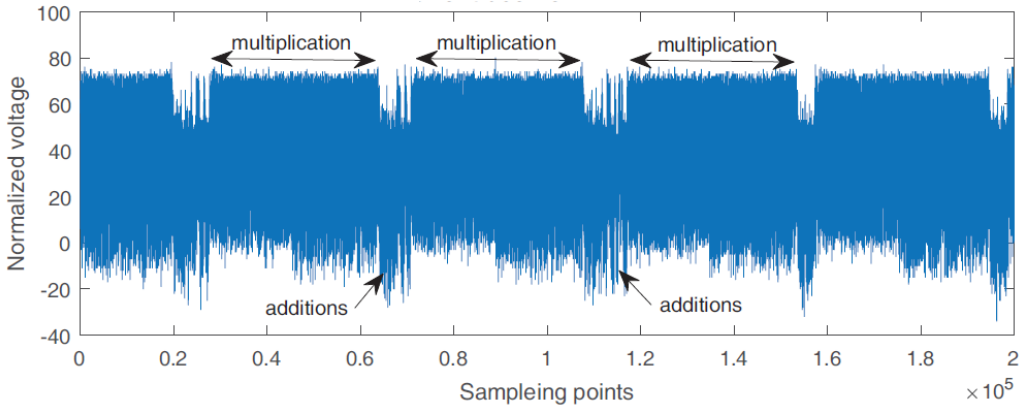


Figura 3 – Traço de potência obtido de um sistema executando diferentes operações.
Fonte: LUO; FEI; KAELI (2018).

2.1.1 Dissipação de Potência em Circuitos Integrados

A potência dissipada em circuitos digitais baseados em lógica CMOS estática é essencialmente caracterizada por dois fatores: potência estática e potência dinâmica. A potência é dita estática quando o circuito não apresenta mudanças de estados entre os transistores, ou seja, não há atividade de chaveamento no CI (WESTE; ESHRAGHIAN, 1985). A potência estática é causada por uma corrente de baixa magnitude, conhecida como corrente de fuga, que gera caminhos condutivos estáticos quando o transistor está operando na região de corte.

A potência dinâmica, em contraste, está relacionada com o chaveamento dos transistores, ocorrendo durante as transições de estado do circuito e é dependente dos dados que estão sendo processados (RABAEY; CHANDRAKASAN; NIKOLIC, 2008). A potência dinâmica é caracterizada pela soma da potência de curto circuito e potência de chaveamento. A potência de curto circuito é originada pela corrente temporária que ocorre durante uma transição na saída do circuito, em que, por um breve momento, ambas as redes complementares CMOS estão simultaneamente ativas. A potência de chaveamento (P_{ch}) é expressa pela Equação 1, em que V_{DD} corresponde à tensão da fonte de alimentação, C_L modela a capacitância de saída, f representa a frequência de chaveamento e α o fator de atividade (MANGARD; OSWALD; POPP, 2007). O fator de atividade é definido pelo número médio de transições 0 $\rightarrow$ 1 que ocorrem no circuito.

$$P_{ch} = V_{DD}^2 \cdot C_L \cdot f \cdot \alpha \tag{1}$$

A Figura 4 ilustra as possíveis transições de estado na saída de um inversor CMOS: 0 $\rightarrow$ 1 e 1 $\rightarrow$ 0. Em condições normais de operação, corrente é absorvida pela capacitância de saída, C_L, durante a transição 0 $\rightarrow$ 1; enquanto, na transição 1 $\rightarrow$ 0, a energia previamente armazenada na capacitância é descarregada. Essa assimetria viabiliza as informações exploradas por ataques DPA. A saída de uma porta lógica CMOS pode ainda passar pelos estados 0 $\rightarrow$ 0 e 1 $\rightarrow$ 1, os quais dissipam apenas potência estática.

A potência total dissipada por um circuito é dada pela soma das potências estática e dinâmica. Conforme supracitado, usualmente, PAAs exploram a potência dinâmica dissipada por um sistema, pois a mesma está diretamente associada ao comportamento funcional do circuito. Entretanto, com a redução das dimensões dos transistores e aumento da relevância da corrente em fuga em novas tecnologias, a potência estática também pode ser explorada como uma fonte de canal lateral para extrair chaves criptográficas (ALIOTO et al., 2014).

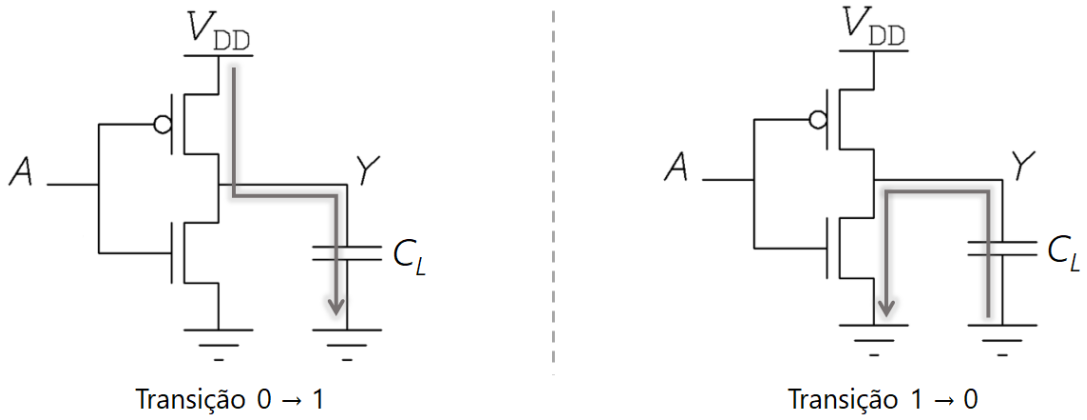


Figura 4 – Origem do consumo de energia dinâmico em um inversor CMOS.

2.1.2 Análise Diferencial de Potência

O propósito da Análise Diferencial de Potência (DPA) é obter a chave secreta de um sistema criptográfico. Para isso, o método se baseia na avaliação de uma elevada quantidade de traços de consumo, os quais foram capturados enquanto o sistema realizava operações criptográficas com diferentes blocos de dados. DPA se caracteriza por ser um modelo de ataque bastante eficiente mesmo sob a presença de ruído nos sinais coletados, além de não necessitar conhecimento detalhado acerca da arquitetura do sistema atacado.

Conforme apresentado anteriormente, a implementação do ataque DPA envolve essencialmente duas fases: obtenção dos traços de consumo e análise destes dados adquiridos. No estágio de captura, os traços são coletados à medida que diferentes dados de entrada são computados pelo sistema. A fase de análise dos dados, por sua vez, emprega uma estratégia de divisão e conquista (CORMEN et al., 2009), buscando revelar sub-chaves individualmente, até determinar a chave completa.

De maneira generalizada, a técnica define um resultado intermediário do algoritmo criptográfico como alvo do ataque, considerando que este resultado deve ser obtido a partir de uma fração do dado simples e da chave criptográfica de entrada. Em seguida, aplica-se uma função de seleção avaliada para cada hipótese de chave, com o intuito de particionar o conjunto de traços coletados em dois subconjuntos. Posteriormente, computa-se a média dos traços de cada subconjunto e, por fim, a diferença das médias destes subconjuntos, gerando uma curva de hipótese para cada hipótese de chave. A Figura 5 apresenta uma síntese do fluxograma empregado pelo método DPA, como proposto originalmente por KOCHER; JAFFE; JUN (1999), destacando as seguintes etapas:

i. *Escolha de um resultado intermediário alvo*: O valor selecionado deve ser proveniente de alguma função do algoritmo criptográfico que compute concomitantemente a chave secreta e o texto simples ou o texto cifrado. O alvo do ataque

propriamente dito consiste na escolha de um bit da saída desta função selecionada. De acordo com a literatura, tipicamente utiliza-se a função de substituição (em inglês, *Substitution Box* - S-Box) do algoritmo. A operação realizada pelas S-Boxes é responsável por introduzir não-linearidade na execução dos algoritmos criptográficos simétricos, tais como o DES (*Data Encryption Algorithm*) e AES.

ii. *Aquisição dos traços*: Nesta etapa, armazena-se um traço de consumo para cada elemento de um conjunto de diferentes textos simples submetidos à função selecionada anteriormente, formando pares de traço e texto correspondentes. Após a aquisição dos traços, opcionalmente emprega-se um estágio de pré-processamento, aplicando filtros para remoção de ruído nas medições.

iii. *Cálculo de resultados hipotéticos*: Realiza-se o cálculo de valores hipotéticos para a função alvo, utilizando os textos de entrada e todas as possibilidades de valores de chave secreta. Deve-se ressaltar que, como o consumo de energia explorado está correlacionado a uma fração do valor intermediário, o método permite concentrar-se em uma parcela da chave ao invés do todo. Assim, considerando o algoritmo criptográfico AES-128[1], por exemplo, o número de variações da chave secreta investigada pelo DPA é 2^8 e não 2^{128}.

iv. *Particionamento dos dados*: Cada traço coletado é classificado de acordo com os resultados obtidos no passo (iii), considerando o texto de entrada equivalente. Assumindo que o alvo do ataque seja o bit menos significativo da saída da S-Box, os traços podem ser separados em dois subconjuntos: S_0 e S_1, de acordo com o valor gerado no bit alvo. Após a divisão, calcula-se a média de cada um destes subconjuntos.

v. *Teste de hipóteses*: Por fim, computa-se a diferença entre a média dos dois subconjuntos, subtraindo os pontos do primeiro subconjunto com os pontos do segundo. Se a hipótese de chave utilizada estiver correta, o gráfico da diferença das médias resultará em picos facilmente discerníveis, indicando que o valor hipotético se correlaciona com o dado efetivamente processado. Caso contrário, os subconjuntos se cancelam e a diferença será próxima a zero, descartando a hipótese adotada. Este procedimento se repete para as demais S-Boxes, até que toda a chave criptográfica seja revelada.

Uma variante mais sofisticada do DPA emprega um modelo de potência para a investigação da correlação dos valores hipotéticos com o dado efetivo (MANGARD; OSWALD; POPP, 2007). O procedimento adota os mesmos passos iniciais exibidos

[1] O AES-128 utiliza subchaves de 16 bytes, tornando necessárias 4096 ($2^8 \cdot 16$) execuções do DPA. Ainda assim, este valor é factível e significativamente menor que 2^{128}.

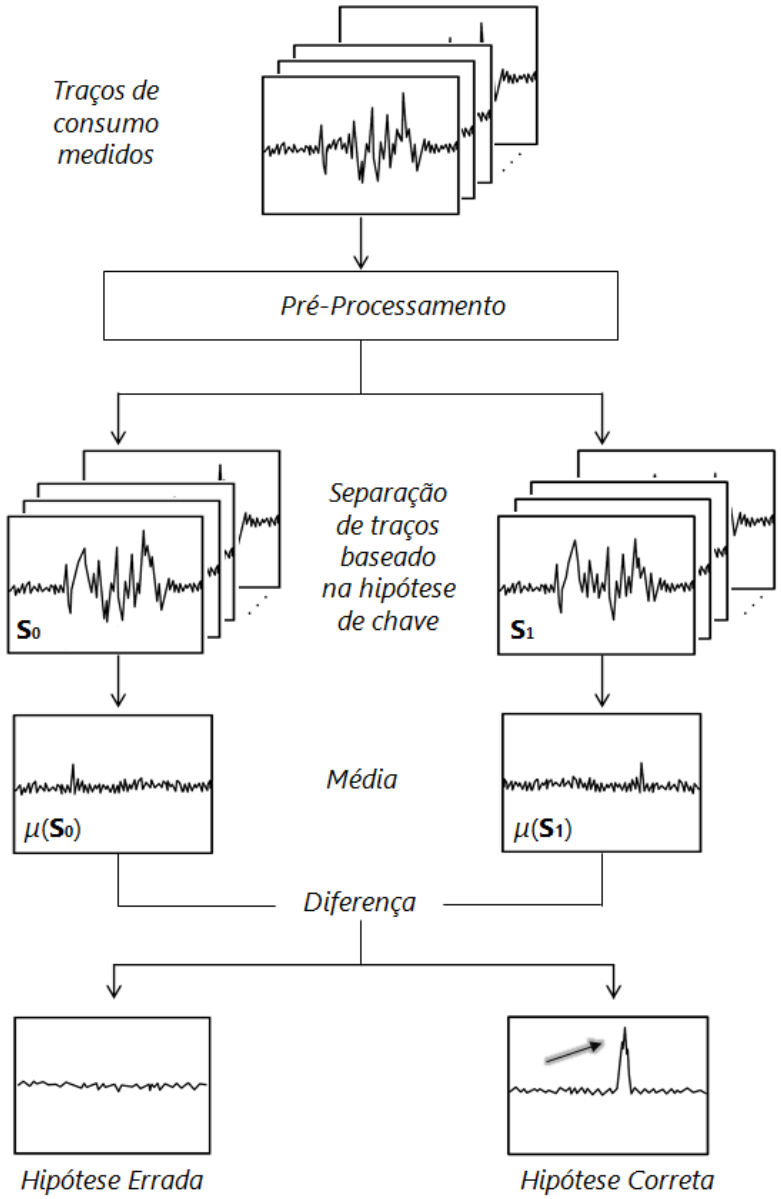


Figura 5 – Fluxo de ataque adotado pelo método DPA.

acima, diferenciando-se na classificação dos traços e análise utilizada para avaliação das hipóteses de subchaves. Nesta abordagem, os resultados hipotéticos calculados na etapa (iii) são mapeados em valores de potência, de acordo com o modelo adotado. Tal modelo teoriza como o consumo de energia depende dos valores internos. Tipicamente, a distância ou o peso Hamming do bit menos/mais significativo são os modelos de potência adotados. Para a identificação da hipótese de subchave correta, calcula-se o coeficiente de correlação entre os valores mapeados e os traços capturados. Novamente, se o gráfico apresentar um valor de pico destacado, verifica-se que a hipótese selecionada era a correta.

2.1.2.1 Análise Diferencial Eletromagnética

A Análise Diferencial Eletromagnética (DEMA) utiliza as radiações eletromagnéticas emitidas por um circuito como fonte de informação de canal lateral para inferir a chave criptográfica (QUISQUATER; SAMYDE, 2001). DEMA aplica um fluxo similar ao adotado pelo ataque DPA, tendo em vista que a potência dissipada por um dispositivo e suas emissões eletromagnéticas estão fortemente relacionadas (DINU; KIZHVATOV, 2018). As ondas eletromagnéticas são decorrentes das variações das correntes que fluem em um sistema criptográfico durante as atividades de chaveamento dos transistores, e podem ser medidas utilizando sensores como o *near-field probe*. De forma análoga ao SPA, se apenas um traço individual de emissão eletromagnética for empregado na investigação, o método é denominado *Simple Electromagnetic Analysis* (SEMA).

Ataques baseados em radiação eletromagnética são mais suscetíveis ao ruído e a aquisição de dados pode ser dificultada em caso de blindagem eletromagnética, no entanto a etapa de medição das ondas eletromagnéticas apresenta o benefício de poder ser realizada a uma certa distância do dispositivo alvo de ataque (MULDER et al., 2005). Em contrapartida, ataques baseados na análise de potência podem ser combatidos com o isolamento da alimentação do sistema criptográfico através de reguladores de tensão (YU; KöSE, 2018).

2.2 Contramedidas

Contramedidas são técnicas de projeto implementadas para tornar os circuitos menos suscetíveis à ação dos ataques SCAs. Tais técnicas podem ser desenvolvidas em diferentes níveis de abstração e mostram-se mais relevantes em reduzir a dependência dos dados com as informações de canais laterais quando projetadas ao nível de transistor (MANGARD; OSWALD; POPP, 2007). No contexto de ataques DPA e DEMA, as contramedidas podem ser categorizadas em métodos de mascaramento ou ocultação, de acordo com a abordagem adotada.

As técnicas de mascaramento buscam inserir aleatoriedade na informação processada por um circuito criptográfico, tornando uma parcela do consumo de energia do sistema randômica. O método de mascaramento pode ser implementado inserindo operações logicamente redundantes com um valor previamente definido, denominado máscara (MULDER et al., 2009). Uma outra abordagem de mascaramento envolve a introdução de ruído nas medições dos traços de consumo, por meio da adição de atrasos aleatórios durante a execução do algoritmo criptográfico (CLAVIER; CORON; DABBOUS, 2000).

Métodos de ocultação, por sua vez, propõem-se a projetar as portas lógicas de um circuito de forma que o consumo de energia seja uniforme, tornando-o independente

dos dados que estão sendo processados (MURESAN; GREGORI, 2008). Tipicamente, busca-se atingir a uniformidade de consumo aplicando a combinação de duas técnicas: lógica de trilha dupla (em inglês, *dual-rail* - DR) e lógica de pré-carga (em inglês, *pre-charge logic* - PL) (MANGARD; OSWALD; POPP, 2007). Como tais técnicas são aplicadas pelas contramedidas abordadas neste trabalho, a seguir, descreve-se o funcionamento das mesmas.

- **Trilha Dupla**

  Circuitos projetados com trilha dupla (DR), ou lógica complementar, utilizam dois bits de informação para representar um único sinal. Dessa forma, todos os sinais do circuito são codificados com valores logicamente complementares. Conforme ilustrado na Figura 6, um dado de entrada A é representado utilizando dois sinais: A_1 e A_0. O dado A_1 indica o valor lógico verdadeiro, ou 1 binário, enquanto o dado A_0 indica o valor lógico falso, ou 0 binário. Assim, em trilha dupla, um dado é válido somente quando seus bits duais apresentam valores opostos, ou seja, (0, 1) ou (1, 0). A notação utilizada na imagem será adotada no restante do texto, com A e B representando os sinais de entrada, S a saída do circuito, e os valores subscritos 1 e 0 denotando os dados reais e complementares, respectivamente. Conforme supracitado, o objetivo da codificação DR, no contexto das contramedidas, é atingir o equilíbrio do consumo dinâmico que ocorre durantes as transições do circuito. O procedimento adotado pela lógica complementar auxilia neste propósito ao garantir que sempre que haja uma transição 0 $\rightarrow$ 1, também ocorra uma transição 1 $\rightarrow$ 0, independente da entrada do circuito.

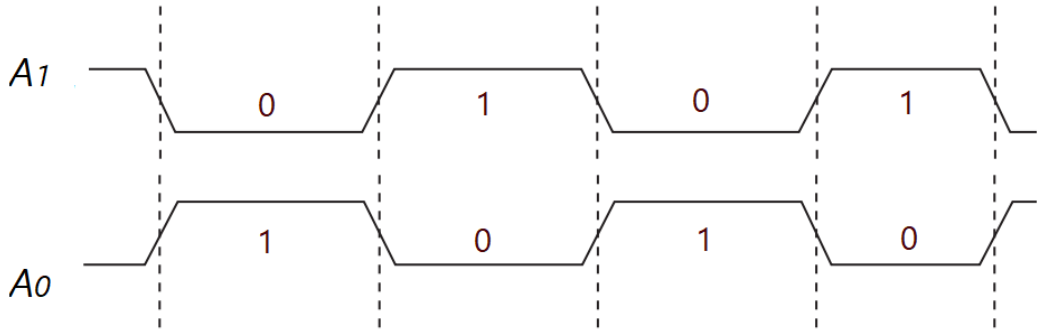


Figura 6 – Representação de um dado codificado em trilha dupla, na qual A_0 representa o valor complementar de A_1.

- **Lógica de Pré-Carga**

  A lógica de pré-carga (PL), ou lógica dinâmica, consiste em um protocolo de duas fases: pré-carga e avaliação. Na fase de pré-carga, todos os sinais são definidos com o mesmo valor inicial, de forma que as entradas e saídas possuam o mesmo valor. Durante a fase de avaliação, os valores são ajustados de acordo

com os dados processados e o circuito se comportará de acordo com a função lógica implementada. A Figura 7 apresenta a forma de onda equivalente de um dado de um circuito dinâmico alternando entre os dois estados lógicos, sendo o valor de pré-carga estabelecido como ‘0’. O comportamento de circuitos com PL garante a ocorrência de apenas um evento de transição por ciclo nas saídas de uma porta lógica. Tipicamente, os transistores responsáveis pela funcionalidade do circuito são todos incorporados num único plano e um sinal de controle é responsável por definir a fase em que o sistema se encontra (SEDRA; SMITH, 2007).

Figura 7 – Forma de onda de um dado implementado em lógica dinâmica.

2.2.1 Topologias Adotadas por Contramedidas de Ocultação

A associação das duas técnicas descritas acima resulta na lógica de pré-carga com trilha dupla (em inglês, *Dual-rail Pre-charge Logic* - DPL). A Figura 8 ilustra o comportamento observado por um dado implementado utilizando a lógica DPL. Conforme pode ser visualizado no diagrama de ondas, durante a fase de pré-carga, ambos os sinais são estabelecidos com o mesmo valor lógico; enquanto que na etapa de avaliação, os sinais assumem valores complementares de acordo com a função lógica implementada. Dessa forma, circuitos DPL realizam apenas uma transição durante qualquer ciclo de processamento, independente do dado processado. Como a potência dissipada por um circuito digital baseado em lógica CMOS estática é fortemente associada ao número de transições que ele realiza, o comportamento de uma célula DPL concebe a base para obter o consumo de energia independente dos dados. Assim, beneficiando-se da lógica DPL, diferentes estilos lógicos são propostos com a tentativa de atingir um consumo uniforme. Nas próximas subseções, serão abordadas as topologias de contramedidas revisadas neste trabalho, descrevendo seu comportamento e justificando a escolha de cada uma. Ressalta-se que não é o objetivo deste trabalho realizar uma comparação entre as topologias, e sim, destacar a necessidade de considerar os fenômenos de variabilidade ao avaliá-las.

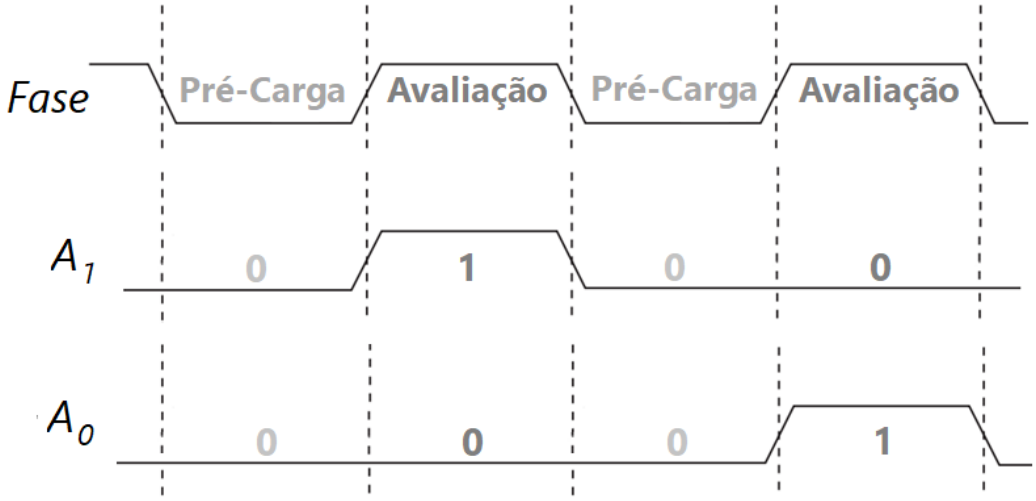


Figura 8 – Forma de onda de um dado implementado em lógica de pré-carga com trilha dupla.

2.2.1.1 Sense Amplifier Based Logic

Sense Amplifier Based Logic (SABL) (TIRI; AKMAL; VERBAUWHEDE, 2002) foi a estratégia pioneira em empregar a lógica de pré-carga em trilha dupla como medida de resistência aos ataques DPA. Circuitos SABL são projetados para apresentar um consumo interno de energia constante e independente dos dados. Durante a fase de pré-carga, que ocorre quando o sinal de controle está no nível lógico baixo, os sinais do circuito são definidos com o valor '0'. Nessa etapa, todos os nodos e capacitâncias internas são carregados. Na subsequente fase de avaliação, quando o sinal de controle alterna para o nível lógico alto, o circuito opera de acordo com a função estabelecida e os nodos internos são descarregados.

Portas lógicas SABL apresentam alta resistência aos ataques DPA, pois alternam para a fase de avaliação em momentos fixos de tempo e sua estrutura de transistores suprime a influência das capacitâncias internas. Em contrapartida, tais circuitos requerem no mínimo o dobro de área quando comparados aos equivalentes em CMOS, e apresentam um aumento significativo no consumo de energia (MANGARD; OSWALD; POPP, 2007).

A Figura 9 apresenta o arranjo de transistores da porta lógica NAND/AND implementada na topologia SABL. A rede *pull-down* diferencial (*differential pull-down network* - DPDN) é responsável por realizar a função lógica, enquanto o sinal clk controla as operações do circuito. Destaca-se que uma porta lógica NOR/OR pode ser derivada a partir da Figura 9, pela simples inversão dos sinais de entrada e saída dos transistores da DPDN. O esquemático de transistores da porta lógica XOR/XNOR para a topologia SABL, assim como para os demais estilos lógicos descritos na sequência, podem ser conferidos no Apêndice A dessa dissertação.

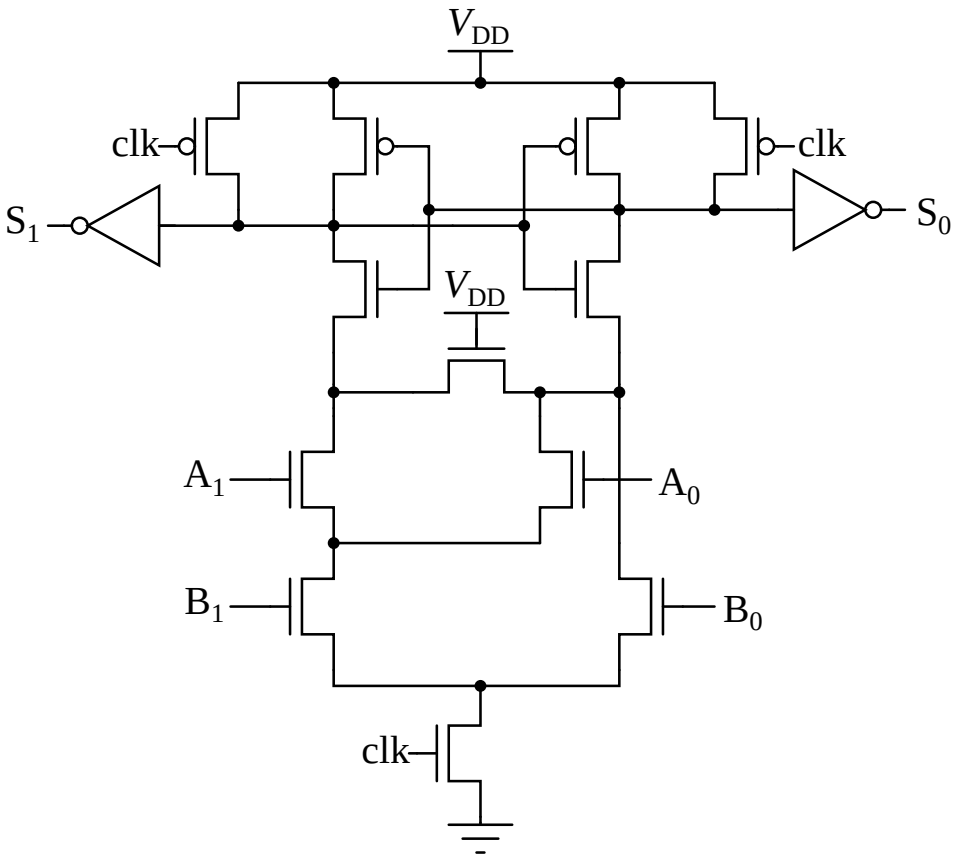


Figura 9 – Esquemático da porta lógica NAND/AND para a topologia SABL.

2.2.1.2 Wave Dynamic Differential Logic

Com o intuito de reduzir os custos de integração e esforço de projeto, TIRI; VERBAUWHEDE (2004) propuseram a *Wave Dynamic Differential Logic* (WDDL). Essa topologia se caracteriza por beneficiar-se de circuitos CMOS disponíveis em uma biblioteca de células padrão (*standard cell*). A estrutura genérica de uma porta combinacional WDDL consiste em dois circuitos que implementam funções booleanas monotônicas positivas. Uma função booleana é dita monotônica positiva quando as saídas sempre alternam na mesma direção que as entradas (ZHANG; VEGA; TAYLOR, 2016). Além disso, na topologia WDDL não há um sinal de controle para todo o circuito, de forma que apenas as entradas recebem o valor de pré-carga, propagando esse sinal através da lógica combinacional do circuito.

Apesar da vantagem de usufruir do fluxo de uma biblioteca regular de CIs, WDDL apresenta o problema de *early evaluation*. De acordo com os valores de entrada, os componentes complementares de uma porta lógica podem alternar para a fase de avaliação em momentos diferentes de tempo, causando a dependência dos dados. A Figura 10 apresenta o esquemático da porta lógica NAND/AND implementada na topologia WDDL. O circuito utiliza uma porta AND para os sinais logicamente verdadeiros e uma porta OR para os sinais logicamente falsos.

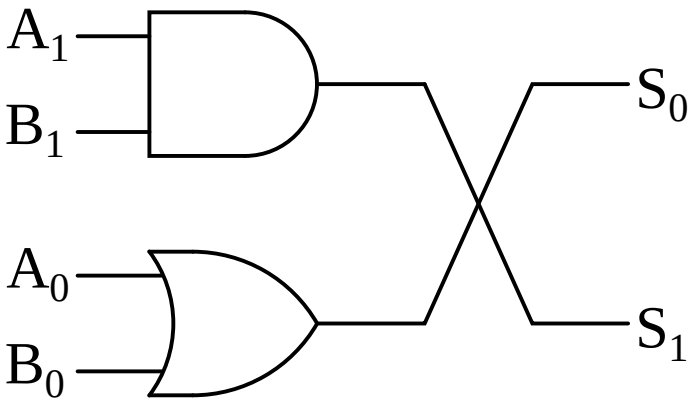


Figura 10 – Esquemático da porta lógica NAND/AND para a topologia WDDL.

2.2.1.3 Pre-Charge Static Logic

Pre-Charge Static Logic (PCSL) (CHONG et al., 2015) é um estilo lógico que busca o balanceamento dos caminhos internos de carga e descarga como estratégia para mitigar a dependência dos dados. A ideia principal da topologia baseia-se na adição de transistores logicamente redundantes para equilibrar as capacitâncias internas e os caminhos de corrente, tornando o consumo de energia das operações menos evidente. O arranjo de transistores da porta lógica NAND/AND implementada na topologia PCSL está ilustrado na Figura 11, na qual req representa o sinal de controle e os asteriscos indicam os transistores redundantes (*dummies*), cuja função é fazer o balanço das capacitâncias internas.

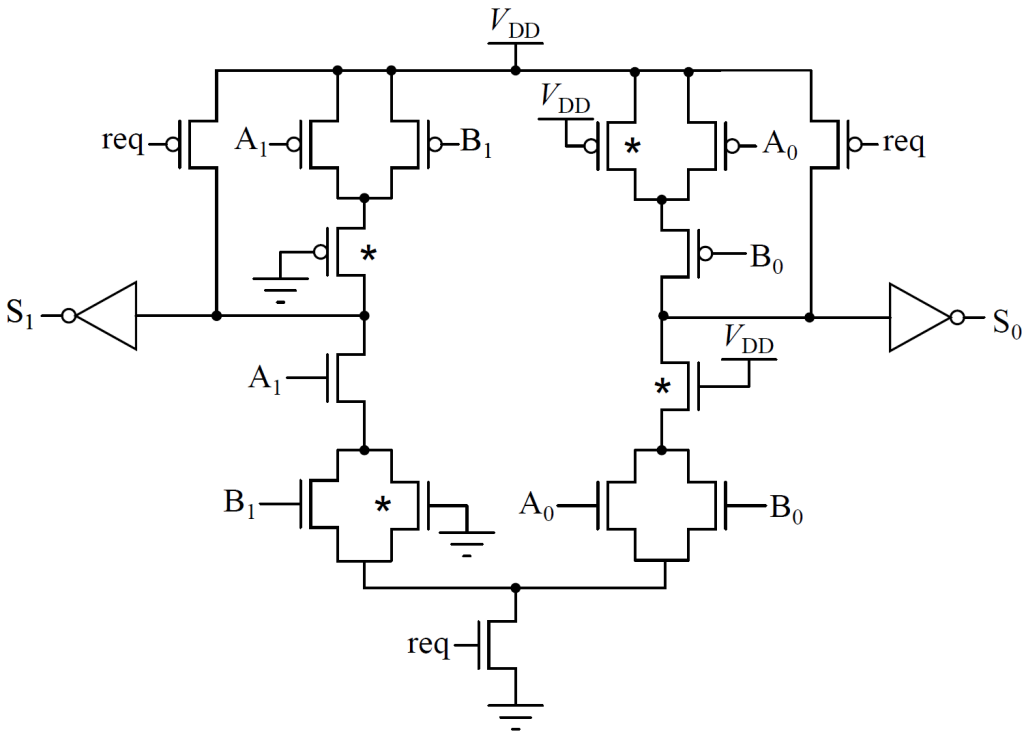


Figura 11 – Esquemático da porta lógica NAND/AND para a topologia PCSL.

2.2.1.4 *Differential Pass-transistor Pre-charge Logic*

Differential Pass-transistor Pre-charge Logic (DPPL) (PANG et al., 2015) é uma topologia baseada na lógica de transistor de passagem complementar (em inglês, *Complementary Pass-Transistor Logic* - CPL). Essa forma de lógica utiliza transistores conectados em série, da entrada para a saída do circuito, com o intuito de bloquear ou transmitir a passagem de um dado sinal (SEDRA; SMITH, 2007). Para implementar a lógica complementar, o circuito é composto por duas redes idênticas de transistores de passagem, cujo controle é operado pelos mesmos sinais.

Os circuitos DPPL buscam a homogeneização do consumo de energia concentrando a etapa de pré-carga nos transistores PMOS. Nessa fase, todos os sinais de entrada recebem o valor '0', de forma que apenas os transistores PMOS estejam ativos. Na etapa de avaliação, o circuito realiza a função lógica através dos transistores NMOS. A Figura 12 exibe o arranjo de transistores das portas lógicas NAND e AND, nas versões de trilha simples, implementadas na topologia DPPL. Ressalta-se que para a concepção da porta NAND/AND na lógica de trilha dupla, ambos os circuitos devem ser empregados.

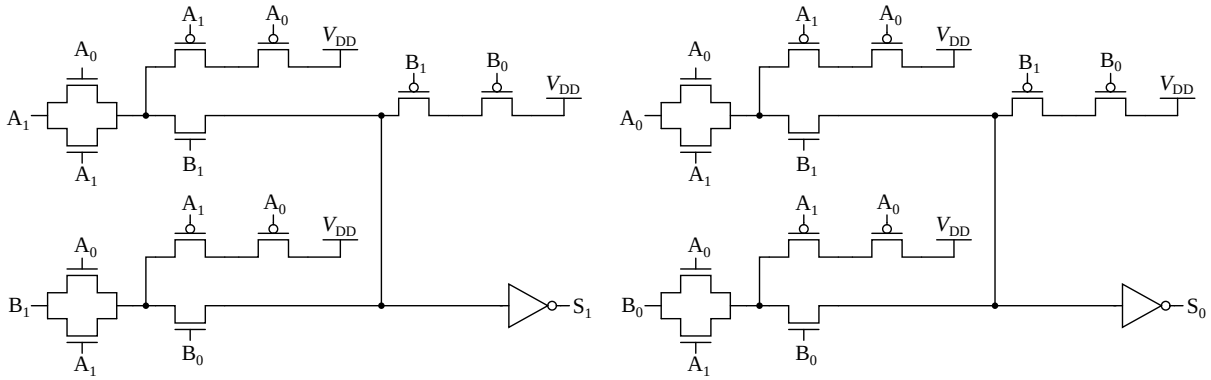


Figura 12 – Esquemático da porta lógica NAND/AND para a topologia DPPL.

2.2.1.5 *Improved Delay-based Differential Pre-charge Logic*

Em abordagens de contramedidas de ocultação mais recentes, propõe-se a aplicação de trilha dupla associada a um protocolo de lógica dinâmica de três fases (em inglês, *Three-phase Dual-rail Pre-charge Logic* - TDPL) (BUCCI et al., 2006). Adicionalmente às duas etapas tradicionais da lógica dinâmica, pré-carga e avaliação, TDPL possui uma fase extra de operação, denominada pós-avaliação. Semelhante à etapa de pré-carga, a fase de pós-avaliação é responsável por conduzir o circuito para um mesmo estado, estabelecendo todas as entradas e saídas com o valor lógico oposto ao definido no período de pré-carga. A Figura 13 ilustra o comportamento de um dado de um circuito TDPL alternando entre os dois estados lógicos, em que os valores determinados para as etapas de pré-carga e pós-avaliação são '0' e '1', respectivamente.

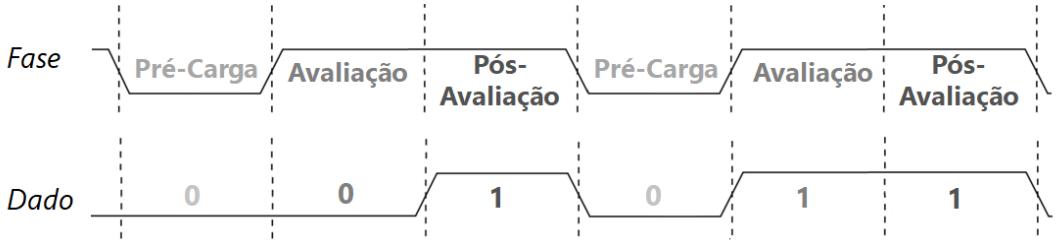


Figura 13 – Forma de onda de um dado implementado em lógica dinâmica de três fases.

No contexto dos ataques DPA, *Improved Delay-based Differential Pre-charge Logic* (iDDPL) (BELLIZIA; SCOTTI; TRIFILETTI, 2018) é um exemplo de topologia de ocultação baseada na lógica TDPL. Nos circuitos iDDPL, após a etapa de avaliação, na qual é computada a função lógica, as trilhas duplas são conectadas à tensão de alimentação, estabelecendo todos os sinais de entrada com o valor lógico '1'. A presença dessa fase extra de pós-avaliação é responsável por evitar o vazamento de informação devido ao efeito de memória. Tal efeito caracteriza o desequilíbrio nas capacitâncias internas de um circuito, causado pela dependência dos nodos internos de uma célula lógica com os valores processados pelo mesmo (BONGIOVANNI et al., 2015). A Figura 14 apresenta o esquemático de transistores da porta lógica NAND/AND implementada na topologia iDDPL, com a entrada clk representando o sinal de controle.

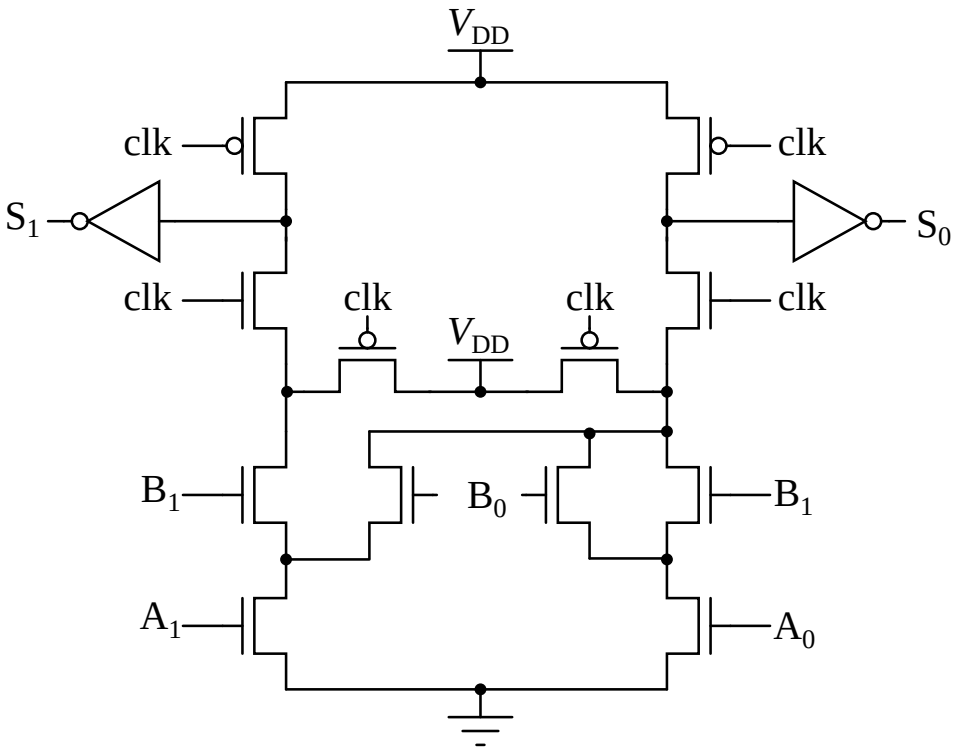


Figura 14 – Esquemático da porta lógica NAND/AND para a topologia iDDPL.

2.3 Métricas de Segurança

Com o intuito de quantificar o desequilíbrio de potência em células lógicas, parâmetro explorado em ataques por análise de potência, duas métricas amplamente utilizadas na literatura foram consideradas. O Desvio Padrão Normalizado (em inglês, *Normalized Standard Deviation* - NSD) (BUCCI et al., 2006) e o Desvio Normalizado de Energia (em inglês, *Normalized Energy Deviation* - NED) (TIRI; AKMAL; VERBAUWHEDE, 2002) estimam a proteção de um circuito de acordo com a variação de energia em diferentes ciclos. Essas métricas de segurança são estimadas para um conjunto de medições de energia (E) contendo todos os arcos de transição possíveis para o circuito. A energia de um arco de transição é dada pela Equação 2, na qual V_{DD} é a tensão da fonte de alimentação, $i(t)$ é a corrente absorvida pelo circuito e T é o período de medição.

$$E = \int_0^T V_{DD} \cdot i(t) dt \tag{2}$$

As métricas NSD e NED são definidas pelas Equações 3 e 4, respectivamente. Nas equações, $\sigma(E)$ e $\overline{E}$ representam o desvio padrão e a média do conjunto de energias, enquanto $max(E)$ e $min(E)$ denotam a energia máxima e mínima entre os possíveis arcos de transição.

$$NSD = \frac{\sigma(E)}{\overline{E}} \tag{3}$$

$$NED = \frac{max(E) - min(E)}{max(E)} \tag{4}$$

Ambas as métricas sempre são atribuídas com valores positivos, pois os parâmetros aplicados por suas equações sempre assumem valores maiores que zero também. Idealmente, um circuito sem vazamento de informações possuirá todas as medições de energia iguais. Assim, os valores máximos e mínimos do conjunto serão iguais e o desvio padrão será zero, levando a valores de NSD e NED também iguais a zero. Dessa forma, valores mais baixos de NSD e NED indicam uma célula menos vulnerável, reduzindo a possibilidade de vazamento de informações de energia para um ataque DPA.

3 VARIABILIDADE EM CIRCUITOS INTEGRADOS

O ritmo acelerado de progresso apresentado pela indústria de semicondutores foi conduzido pelo aumento da densidade de transistores por unidade de área do *chip*, conforme previsto pela Lei de Moore (MOORE, 1965). Essa maior integração dos dispositivos foi viabilizada pela contínua miniaturização das dimensões dos transistores e permitiu a redução de potência e atraso em circuitos digitais, além da diminuição do custo de fabricação por transistor. Em contrapartida, associado às dimensões diminutas impostas pelos nodos tecnológicos modernos, surgiram efeitos indesejáveis ao funcionamento dos CIs (LEWYN et al., 2009). Tais efeitos, até então negligenciáveis em tecnologias mais antigas, estão diretamente relacionados à perda de confiabilidade e robustez dos dispositivos, provocando variações nas propriedades elétricas dos transistores. Sob esse panorama, este capítulo introduz os principais efeitos de variabilidade que influenciam no comportamento do dispositivos.

A variabilidade descreve uma propriedade estatística que auxilia a compreender o quanto os dados de um experimento diferem-se entre si. A variabilidade também está presente em diversas situações do cotidiano. Consideremos o desempenho de um *smartphone* em relação à autonomia de bateria, por exemplo. Naturalmente, não obtemos a mesma durabilidade de bateria após cada recarga do aparelho. Essa variação verificada na capacidade da bateria depende de diferentes fatores, tais como a ativação de conexões sem fio, o uso de aplicativos e dados móveis, ou mesmo a iluminação da tela. Esses diversos fatores representam fontes potenciais de variabilidade no comportamento do sistema.

No contexto dos circuitos integrados, a variabilidade descreve a dispersão observada nas características elétricas dos transistores, podendo ser categorizada de diferentes maneiras. A divisão entre efeitos constantes ou variáveis ao decorrer do tempo representa a principal distinção entre os fenômenos de variabilidade (SAXENA et al., 2008), conforme ilustrado na Figura 15. Efeitos de variabilidade de tempo zero (*time-zero*) se manifestam de forma fixa ao longo do tempo, exibindo o mesmo impacto nos transistores desde a fabricação. Por outro lado, fenômenos de variabilidade temporal se caracterizam por serem variáveis em relação ao tempo e dependentes das condi-

ções de operação dos circuitos.

Cada categoria mencionada acima pode ainda ser divida internamente. Essas subdivisões auxiliam a identificar as causas responsáveis pelas variações. Efeitos de variabilidade *time-zero* são oriundos do processo de fabricação e se classificam em globais (extrínsecos) e locais (intrínsecos). Efeitos temporais, por sua vez, se diferenciam em fenômenos de envelhecimento, ou degradação, e fenômenos transientes. No restante do capítulo, os fatores de variabilidade supracitados são abordados com mais detalhes. A Seção 3.1 apresenta diferentes efeitos de variabilidade *time-zero*, descrevendo seus impactos na confiabilidade dos transistores. Os efeitos dependentes do tempo são expostos na Seção 3.2, destacando o fenômeno de *Bias Temperature Instability* (BTI).

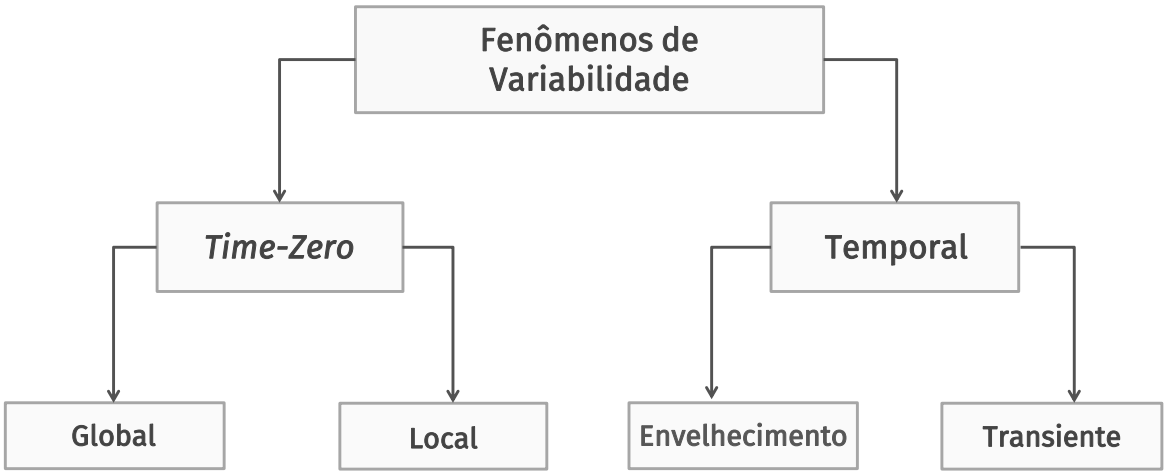


Figura 15 – Categorização dos efeitos de variabilidade em circuitos CMOS.

3.1 Variabilidade de Processo

A variabilidade de processo (*time-zero*) origina-se da crescente complexidade necessária para a produção dos dispositivos CMOS (MARICAU; GIELEN, 2013). Em tecnologias de escala micrométrica, as propriedades elétricas dos dispositivos concebidos apresentavam pouca influência de efeitos de variabilidade (BANSAL; RAO, 2011). Entretanto, com a redução das dimensões dos transistores para o regime nanométrico, particularmente em tecnologias abaixo dos 100 nm, tornou-se inexequível o controle e uniformidade do processo de fabricação. A Figura 16 exibe a porcentagem de variação para alguns parâmetros de transistores de diferentes tecnologias, de acordo com seus valores nominais. A variabilidade relativa dos parâmetros foi mensurada a partir de três desvios padrões sobre a média. Pelo gráfico, é possível observar

um aumento da variação no comprimento do canal (L_{eff}), espessura do óxido de porta (T_{ox}) e tensão de limiar (V_{th}), conforme o nodo tecnológico diminui. Ademais, as dimensões atomísticas dos transistores e a natureza discreta da matéria, associadas às limitações da etapa de fabricação, provocam os dispositivos a se comportarem de maneira distinta das características projetadas, gerando incerteza a respeito do correto funcionamento de um CI.

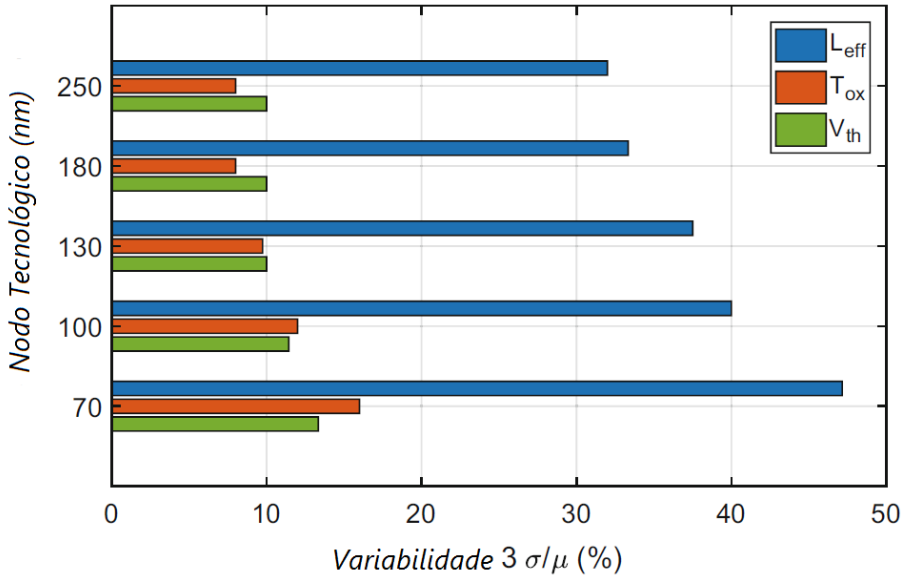


Figura 16 – Variabilidade de parâmetros de acordo com o nodo tecnológico. Fonte: CHAMPAC; GARCIA GERVACIO (2018)

Os fatores de variabilidade de processo podem ser diferenciados segundo a escala espacial em que se manifestam, sendo divididos em efeitos globais e locais, conforme apresentado na Figura 15. Variações globais (*inter-die*) referem-se aos desvios que ocorrem de forma idêntica entre os parâmetros dos transistores fabricados para um dado circuito, mas de maneira divergente quando comparados a transistores de outros CIs. Essas variações podem se manifestar em diferentes níveis do processo de fabricação, como entre os CIs do mesmo *wafer* (*die-to-die*), entre *wafers* de um dado lote (*wafer-to-wafer*) e, ainda, entre lotes distintos (*lot-to-lot*). Por outro lado, variações locais (*intra-die)* resultam em desvios aleatórios e diferentes para cada transistor do mesmo circuito integrado. A Figura 17 ilustra a distinção entre efeitos globais e locais. Ademais, a variabilidade de processo também pode ser categorizada de acordo com a origem de seus efeitos, classificando-os em extrínsecos e intrínsecos. Efeitos extrínsecos são oriundos da não idealidade do processo de fabricação dos dispositivos semicondutores. Efeitos intrínsecos, por sua vez, se originam das variações de parâmetros relacionados à escala atomística das dimensões do transistor. Usualmente, variações extrínsecas e intrínsecas podem ser associadas aos efeitos globais e locais, respectivamente (KANNO et al., 2007; BÖHM; HOFER, 2013).

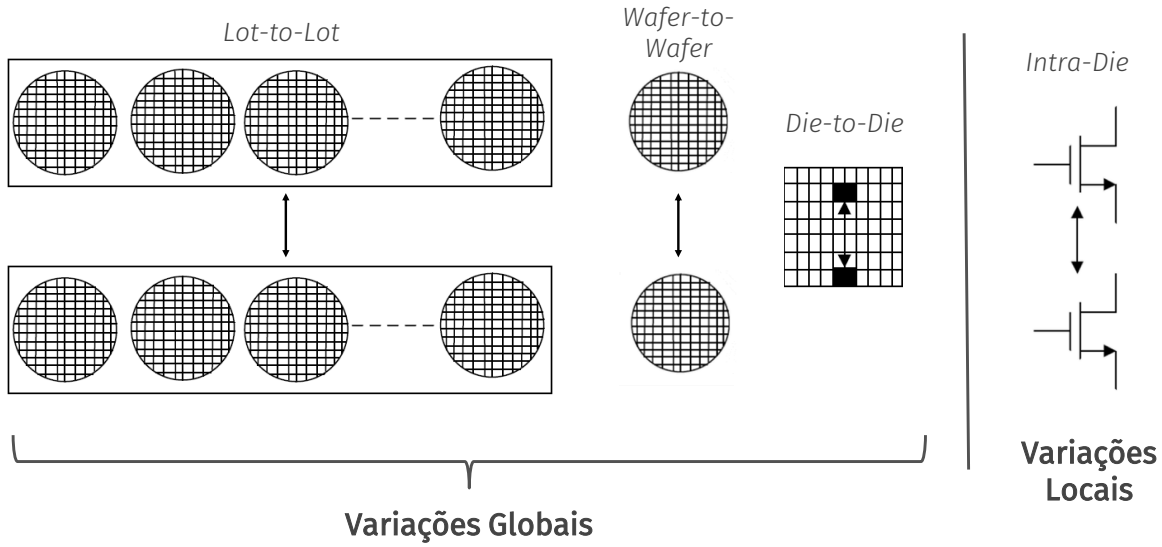


Figura 17 – Representação da variabilidade de processo, demonstrando efeitos globais e locais. Fonte: PANDIT; MANDAL; PATRA (2014)

3.1.1 Efeitos Globais

Conforme mencionado anteriormente, as variações globais (extrínsecas) resultam da falta de controle sobre o processo de fabricação dos dispositivos semicondutores. Com a miniaturização dos transistores, a diferença nas características de desempenho de um dado circuito, fabricado em elevadas unidades, tornou-se mais relevante. Essas variações afetam os transistores de um circuito de maneira homogênea, provocando os mesmos desvios nos parâmetros de todos dispositivos em um dado CI.

Durante o processo de fabricação dos dispositivos, diferentes etapas podem causar variações extrínsecas; entretanto, o procedimento litográfico representa o principal agente responsável pelos desvios paramétricos observados (CHIANG; KAWA, 2007). A fotolitografia é a técnica que permite reproduzir no *wafer* o padrão de leiaute projetado. Nessa etapa, um material fotossensível (fotorresiste) é exposto à luz, com o intuito de projetar o padrão geométrico presente no molde (fotomáscara) do CI no substrato do dispositivo. Porém, existem limites físicos nos quais a projeção pode ser realizada e, desde a miniaturização para o nodo tecnológico de 130 nm, o comprimento de onda da luz utilizada no processo se manteve o mesmo (193 nm) (JACOB et al., 2017). Dessa forma, devido à difração da luz, os padrões da fotomáscara são transferidos com algum grau de distorção para o *wafer*, originando os efeitos de proximidade óptica (CHAMPAC; GARCIA GERVACIO, 2018). Estes efeitos provocam variações nas dimensões do comprimento do canal do transistor e, consequentemente, afetam a tensão de limiar do mesmo (WIRNSHOFER, 2013).

Ao longo do *wafer*, gradientes térmicos produzidos durante a etapa de recozimento (*annealing*), responsável por difundir os íons implantados, podem introduzir variações

no comprimento do canal e no perfil de dopagem do dispositivo (BHUSHAN; KETCHEN, 2015). Além disso, estas oscilações de temperatura sucedidas durante diferentes etapas da fabricação, podem ocasionar variações espacias na tensão de limiar, produzindo gradientes dos valores de V_{th} em direção a uma determinada orientação do *wafer* (BÖHM; HOFER, 2013).

Os efeitos de variabilidade global supracitados podem ser minimizados empregando estratégias de leiaute e técnicas de aprimoramento de resolução (em inglês, *Resolution Enhancement Techniques* - RET). Leiaute de centroide comum, por exemplo, reduz a influência de gradientes no transistor, dividindo o dispositivo em associações simétricas menores, de forma que seus centroides coincidam. Ademais, como os dispositivos possuem diferentes condições de contorno, elementos *dummy* são frequentemente inseridos para diminuir o descasamento (*mismatching*) entre um grupo de transistores. Por outro lado, correção óptica de proximidade (em inglês, *Optical Proximity Correction*) e máscaras de mudança de fase (em inglês, *Phase-Shift Masks*) são exemplos de RETs que visam diminuir os efeitos de distorção causados pela etapa de litografia (LIEBMANN et al., 2001). Assim, embora existam diferentes fatores contribuintes para as variações extrínsecas, esses podem ser previstos e não representam uma barreira insuperável.

3.1.2 Efeitos Locais

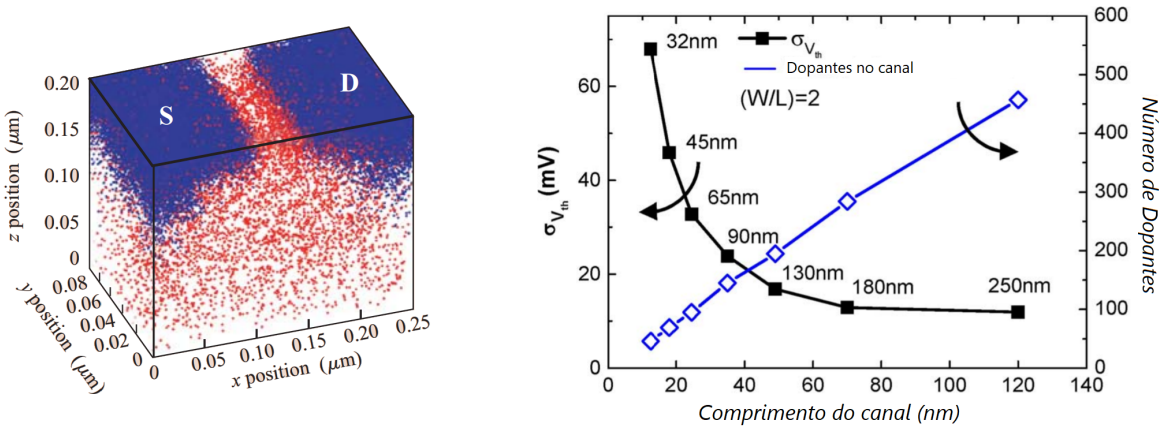
Fenômenos locais (intrínsecos) não resultam diretamente das imprecisões do processo de fabricação, mas da variabilidade inerente ao processo, decorrente da característica atomística intrínseca à matéria (BÖHM; HOFER, 2013). À medida que a área do canal do transistor é continuamente reduzida, a variabilidade observada no desempenho de um CI tende a ser dominada pelos efeitos locais. Tais efeitos se caracterizam por influenciarem cada dispositivo do CI de maneira diferente, sendo independentes de leiaute. Dessa forma, em contraste aos fenômenos globais, a variabilidade local se manifesta de maneira aleatória e, portanto, não pode ser prevista ou completamente controlada (WIRNSHOFER, 2013).

O desempenho de um transistor CMOS tradicional é influenciado por três principais fatores de variabilidade local: a flutuação aleatórias dos dopantes (em inglês, *Random Dopant Fluctuations* - RDF) na região do canal (MAHMOODI; MUKHOPADHYAY; ROY, 2005), a rugosidade da borda na porta do terminal (em inglês, *Line Edge Roughness* - LER) (ASENOV; KAYA; BROWN, 2003) e a granularidade do elemento integrante da porta (*Poly Gate Granularity* - PGG ou *Metal Gate Granularity* - MGG) (WANG et al., 2011). Nas próximas subseções, tais efeitos serão abordados com mais detalhes.

3.1.2.1 Random Dopant Fluctuations

O efeito RDF representa a principal fonte de variabilidade local e origina-se da natureza discreta dos átomos dopantes na região do canal de um transistor CMOS (K.SAHA, 2010). O número de dopantes em um transistor está associado ao perfil de dopagem e ao comprimento e largura do seu canal. Assim, dada uma mesma concentração de dopantes e conforme as dimensões do dispositivo são reduzidas, o número total de átomos dopantes também diminui. Dessa forma, para um mesmo circuito integrado, dois transistores terão características diferentes devido à aleatoriedade da localização e quantidade dos dopantes presentes. A Figura 18 (a) ilustra o posicionamento aleatório dos dopantes no canal de um transistor.

A região do canal do transistor é dopada com impurezas durante a etapa de implantação iônica no processo de fabricação, na qual átomos de um material diferente do substrato são inseridos. Esta etapa de dopagem é responsável por alterar as propriedades elétricas do semicondutor, auxiliando no ajuste da tensão de limiar, na formação dos terminais de fonte e dreno e em tecnologias recentes na inclusão de implantes Halo. Assim, o principal efeito do RDF nas características de um dispositivo são variações causadas na tensão de limiar (CHAMPAC; GARCIA GERVACIO, 2018). A Figura 18 (b) apresenta o aumento no desvio padrão da tensão de limiar ($\sigma_{V_{th}}$), à medida que o número de dopantes localizados no canal diminui, devido à miniaturização dos transistores. Este aumento no desvio padrão indica que a discrepância na tensão de limiar de transistores supostamente idênticos é ampliada.



(a) (b)

Figura 18 – (a) Ilustração da distribuição aleatória dos dopantes na região do canal de um transistor. Fonte: BERNSTEIN et al. (2006) (b) Comportamento do desvio padrão da tensão de limiar ($\sigma_{V_{th}}$) de acordo com a redução do nodo tecnológico. Fonte: YE et al. (2011)

3.1.2.2 *Line Edge Roughness*

O fenômeno LER descreve a distorção no formato das bordas da porta ao longo da direção da largura do canal (YE et al., 2011). Conforme abordado na subseção 3.1.1, o procedimento litográfico utiliza fontes de luz com comprimento de onda maior que as dimensões mínimas do transistores. Assim, variações na intensidade da exposição à luz, associadas à aleatoriedade dos polímeros agregados ao fotorresiste, causam a formação do LER (PANDIT; MANDAL; PATRA, 2014). De forma análoga ao RDF, o principal impacto do efeito LER no comportamento de um dispositivo se manifesta através de desvios nos valores da tensão de limiar.

Semelhantemente, *Line Width Roughness* (LWR) define a flutuação espacial que ocorre entre duas bordas projetadas, ou seja, o efeito LER entre bordas adjacentes. Estes fatores de variabilidade, LER e LWR, estão matematicamente relacionados (MARICAU; GIELEN, 2013). A Figura 19 (a) exemplifica o fenômeno de LER nas bordas da porta de um transistor, enquanto a Figura 19 (b) ilustra a relação entre os efeitos LER e LWR.

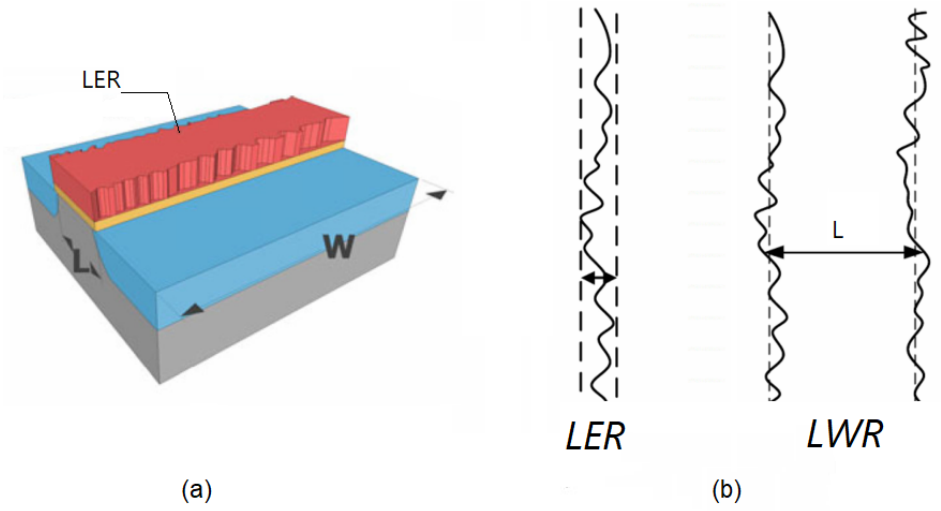


Figura 19 – (a) Representação do efeito LER sobre o polissilício de um transistor. Fonte: CHAMPAC; GARCIA GERVACIO (2018). (b) Ilustração da relação entre os fenômenos LER e LWR.

3.1.2.3 *Gate Granularity*

Transistores CMOS planares convencionais utilizam uma camada de silício policristalino (polissilício) como material para desenvolvimento dos terminais de porta. Entretanto, a não uniformidade do processo de dopagem acarreta na orientação aleatória da estrutura granular do polissilício. Essa distribuição estocástica resulta em desvios na tensão de limiar, dependentes da localização das bordas dos grãos de polissilício ao longo da porta do dispositivo (BROWN; ROY; ASENOV, 2007).

Em nodos tecnológicos mais recentes, com o intuito de diminuir a corrente de fuga, adotou-se a utilização de materiais isolantes com alta constante dielétrica (*high-k*), o que veio a reduzir o impacto de RDF (MARKOV et al., 2014). Para isso, os terminais de silício policristalino precisaram ser substituídos por uma camada de metal, devido à baixa compatibilidade de integração entre os componentes *high-k* e polissilício. Não obstante, as flutuações no tamanho e orientação dos grãos de metal empregado resultam em variações locais na função trabalho (em inglês, *Work Function Variation* - WFV), as quais se refletem em desvios na tensão de limiar de cada dispositivo no CI (DADGOUR et al., 2010). A Figura 20 ilustra o comportamento aleatório do efeito WFV em um dado metal utilizado como porta.

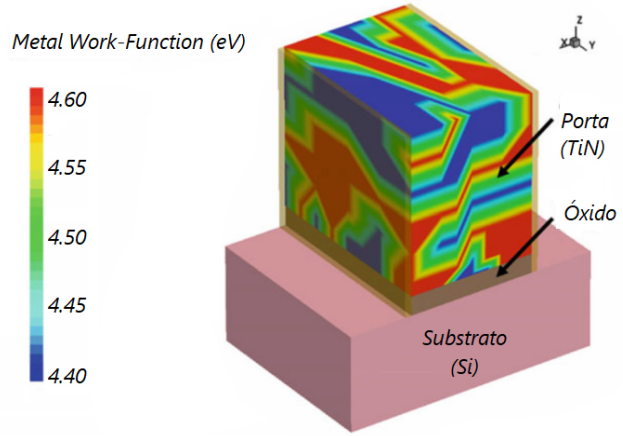


Figura 20 – Vista isométrica de um transistor, demonstrando o fenômeno WFV no metal. Fonte: WIRNSHOFER (2013).

3.2 Variabilidade Temporal

A variabilidade temporal denota efeitos que alteram as características do transistor ao decorrer do tempo, se manifestando após o CI ter sido fabricado e utilizado por um determinado período (MARICAU; GIELEN, 2013). O impacto dos efeitos temporais no desempenho de um dispositivo é dependente das condições de operação do circuito, tais como a temperatura, tensão de operação e atividade de chaveamento. Os fatores de variabilidade temporal se distinguem em fenômenos transientes ou de envelhecimento, de acordo com a influência do efeito causado. Fenômenos transientes distorcem apenas temporariamente os parâmetros elétricos do circuito, enquanto os efeitos de envelhecimento causam uma degradação gradual no desempenho, provocando danos permanentes.

- **Efeitos Transientes**

  Fenômenos transientes caracterizam-se por alterar as condições normais de operação de um circuito integrado por um período limitado de tempo. Entre os

efeitos transientes, destacam-se o *Random Telegraph Noise* (RTN) e os *Single Event Transients* (SET):

- *Random Telegraph Noise* manifesta-se na forma de saltos discretos e aleatórios na corrente de dreno do dispositivo. Este comportamento representa a causa dominante do ruído de baixa frequência, além de estar associado a flutuações na tensão de limiar (WIRTH et al., 2014). Segundo GRASSER et al. (2014), os mecanismos que originam o RTN são os mesmos responsáveis pelo fenômeno *Bias Temperature Instability*, e serão abordados na subseção 3.2.1.

- *Single Event Transients* são observados como distúrbios elétricos decorrentes da passagem de uma única partícula ionizante em um nodo sensível do CI. De acordo com carga gerada pela incidência da partícula, um pulso transiente pode ser formado e propagado pelo circuito, acarretando em falhas no funcionamento do mesmo (GADLAGE et al., 2004). De forma análoga, *Single Event Upsets* são perturbações que ocorrem em elementos de memória. Tais efeitos são particularmente danosos a sistemas aeroespaciais e não serão tratados neste trabalho.

- **Efeitos de Envelhecimento**

  Os fenômenos de envelhecimento, também denominados fenômenos de degradação, resultam em alterações dos parâmetros elétricos do dispositivo durante a operação e ao longo do tempo. Os principais efeitos de envelhecimento a afetar a confiabilidade dos circuitos em tecnologias nanométricas são: *Hot-Carrier Injection* (HCI), *Time-Depedent Dieletric Breakdown* (TDDB), Eletromigração e *Bias Temperature Instability* (BTI):

  - *Hot-Carrier Injection* ocorre quando portadores de alta energia (*hot carriers*) são injetados na camada dielétrica do transistor durante a atividade de chaveamento. Tais *hot carriers* são oriundos da presença de um elevado campo elétrico na região de dreno do dispositivo e referem-se aos elétrons que obtém energia suficiente para superar a interface entre o substrato e óxido, permanecendo como cargas fixas no óxido de porta (CHEN et al., 1985). HCI é proeminente em transistores NMOS, manifestando-se como um aumento na tensão de limiar e redução da mobilidade dos portadores do dispositivo.

  - *Time-Depedent Dieletric Breakdown* se caracteriza como a falha da camada isolante dielétrica em resistir ao campo elétrico aplicado sobre ela, originando um caminho condutivo entre o substrato e o óxido de porta. Cada

material dielétrico possui um valor limite de campo elétrico que pode suportar. Caso se aplique um campo elétrico consideravelmente maior que este valor, ocorre um *hard breakdown*, resultando no rompimento abrupto do dielétrico. Porém, mesmo sob campos elétricos menores que o máximo sustentado, o valor limite pode ser eventualmente excedido devido ao desgaste gradual do material isolante durante a operação do dispositivo, caracterizando a ruptura do dielétrico dependente do tempo (MARICAU; GIELEN, 2013).

– O efeito de eletromigração ocorre nos contatos e interconexões internas de um CI e refere-se à transferência de material causada pelo movimento dos íons em um condutor (TU, 2003). A aplicação de uma elevada corrente elétrica na superfície de um metal condutor resulta na colisão de elétrons com outros átomos condutores. Essas constantes colisões gradualmente removem átomos de metal dos fios, aumentando a resistência do condutor e, assim, reduzindo a confiabilidade do circuito.

Acerca dos diferentes fatores de variabilidade temporal citados, este trabalho focará no impacto causado pelo fenômeno BTI, o qual será exposto na sequência. Embora um dispositivo deva ser projetado para lidar com os variados efeitos de degradação, o fenômeno BTI tornou-se o fator de preocupação dominante para a variabilidade temporal desde o nodo tecnológico de 90 nm (MAHAPATRA; GOEL; MUKHOPADHYAY, 2016).

3.2.1 *Bias Temperature Instability*

O efeito de envelhecimento *Bias Temperature Instability* (BTI) decorre da aplicação de uma tensão de polarização no terminal de porta do transistor e resulta em alterações graduais nas características deste, tais como a tensão de limiar, a transcondutância e a mobilidade do canal, degradando o desempenho dos dispositivos e, consequentemente, dos circuitos CMOS. Como consequência, a vida útil dos dispositivos é reduzida e, caso não seja tratado, o efeito pode provocar a falha prematura de CIs (MAHAPATRA; GOEL; MUKHOPADHYAY, 2016). Conforme o nome sugere, a deterioração dos parâmetros elétricos é influenciada e acelerada pelo aumento da polarização e da temperatura em que o dispositivo está submetido (KERBER; CARTIER, 2014).

O fenômeno BTI frequentemente é categorizado de acordo com a condição de polarização, causadora da degradação, no terminal de porta do transistor: *Negative Bias Temperature Instability* (NBTI) e *Positive Bias Temperature Instability* (PBTI). NBTI ocorre nos dispositivos PMOS, à medida que o terminal de porta é polarizado negativamente em relação aos demais, acarretando em desvios negativos na tensão

de limiar. Em contrapartida, PBTI afeta os transistores NMOS quando o terminal de porta é polarizado positivamente em relação aos outros terminais, provocando desvios positivos na tensão de limiar (PUSCHKARSKY et al., 2018). Para dispositivos convencionais, os efeitos de PBTI podem ser negligenciados, tendo em vista que o impacto de NBTI é significativamente mais relevante (MAHAPATRA; GOEL; MUKHOPADHYAY, 2016). Entretanto, para dispositivos fabricados com materiais de alta constante dielétrica (*high-k*), as implicações de BTI nas características do transistor são similares para ambas as variantes do fenômeno (MARICAU; GIELEN, 2013).

A origem do fenômeno BTI para dispositivos NMOS é associada ao aprisionamento de elétrons na porção dielétrica do óxido de porta. Para dispositivos PMOS, o fenômeno é uma consequência da geração de determinados estados no dielétrico de porta ou na interface entre o dielétrico e semicondutor (KERBER; NIGAM, 2018). Esses estados, denominados de armadilhas, são responsáveis pela captura e emissão de cargas. O aprisionamento de cargas, por sua vez, diminui a corrente do dispositivo, devido ao menor número de portadores no canal, resultando nos desvios observados na tensão de limiar. Ademais, a mobilidade de portadores no canal também é afetada, considerando que uma carga aprisionada interfere eletrostaticamente com estes portadores.

Diferentemente de outros efeitos de degradação, como o HCI e o TDDB, transistores afetados pelo BTI podem se recuperar parcialmente da degradação quando não polarizados diretamente. Em circuitos digitais, em que transistores operam em dois níveis de tensão, podemos avaliar o efeito de BTI nestes dois casos. A Figura 21 ilustra o comportamento tipicamente observado na tensão de limiar de um transistor PMOS, devido ao efeito BTI (KACZER et al., 2011). Ao aplicar uma tensão de polarização no terminal de porta do dispositivo, o mesmo encontra-se sob o período de estresse (*stress*), em que verifica-se um aumento gradual da tensão de limiar, decorrente do paulatino aprisionamento de portadores. Entretanto, ao remover essa tensão de estresse, nota-se a diminuição de uma fração significativa da tensão de limiar. Essa etapa de recuperação é denominada relaxação (*relaxation*).

A caracterização dos mecanismos responsáveis pelo efeito BTI foi inicialmente descrita através do modelo *Reaction-Diffusion* (R-D) (JEPPSON; SVENSSON, 1977). De acordo com o modelo, a tensão de estresse aplicada no dispositivo provoca a quebra de ligações covalentes entre átomos de hidrogênio e silício. Essa etapa de dissociação, denominada reação (*reaction*), ocorre na interface entre o semicondutor e o dielétrico de porta do transistor. No subsequente estágio de difusão (*diffusion*), os átomos de hidrogênio liberados combinam-se entre si, difundido em direção ao terminal de porta. Esse processo, conforme a teoria R-D, é responsável pela geração de estados de interface, os quais atuam como armadilhas, acarretando no aumento da tensão de limiar (ALAM; MAHAPATRA, 2005). Embora tenha sido amplamente ado-

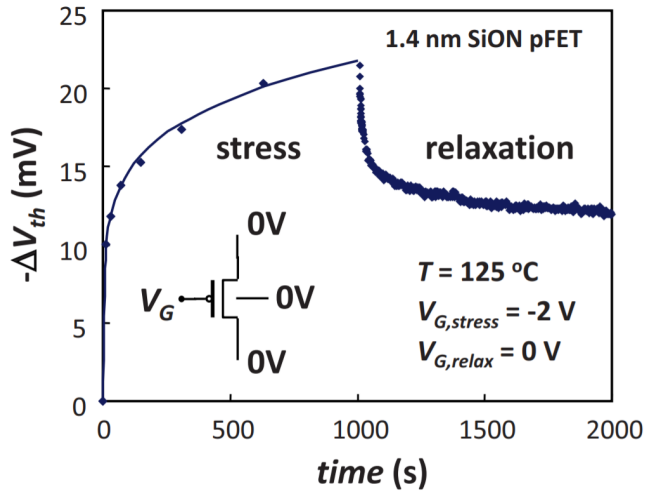


Figura 21 – Variação observada na tensão de limiar, decorrente do efeito NBTI, ilustrando os períodos de estresse e recuperação. Fonte: KACZER et al. (2011).

tado, medições mais recentes apresentaram inconsistências na caraterização, pelo modelo R-D, de determinados comportamentos, especialmente para a etapa de relaxação (GRASSER et al., 2011). Assim, o modelo de armadilhas (*Trapping-Detrapping* – T-D) foi proposto como uma alternativa para explicar o fenômeno BTI, e será descrito com mais detalhes na sequência.

3.2.1.1 Modelo de armadilhas

O modelo de armadilhas (T-D) descreve o fenômeno BTI baseando-se nas atividades de captura e emissão de portadores de carga por armadilhas localizadas no dielétrico do dispositivo. De acordo com a teoria T-D, após a aplicação de uma tensão de estresse, o canal do transistor é formado e passa a ser povoado por portadores de carga; alguns destes portadores podem ser capturados pelas armadilhas, ficando, então, aprisionados no dielétrico. Uma carga fixa (aprisionada) no dielétrico com o mesmo sinal dos portadores acaba, por efeito Coulombiano, repelindo outros portadores do canal do transistor e, consequentemente, diminuindo a corrente e aumentando a tensão de limiar do dispositivo (VELAMALA et al., 2013). Ademais, a caracterização do efeito assume as seguintes premissas acerca das armadilhas (WIRTH; SILVA; KACZER, 2011):

i. A captura e a emissão de portadores de carga são eventos aleatórios, governados por constantes de tempo características, as quais são uniformemente distribuídas em escala logarítmica;
ii. O número de armadilhas apresenta uma distribuição de Poisson;
iii. A distribuição de energia das armadilhas possui uma curva em forma de U (*U-shaped*);

iv. A amplitude dos desvios na tensão de limiar induzida pelas armadilhas segue uma distribuição exponencial.

A Figura 22 ilustra o processo de aprisionamento de cargas em armadilhas presentes no dielétrico de um transistor. Conforme supracitado, a probabilidade de captura e emissão de cargas por uma armadilha é uma função das constantes de tempo de captura (τ_c) e emissão (τ_e), respectivamente. O valor assumido pelas constantes de tempo depende das condições em que o dispositivo está inserido, tais como a tensão de polarização e a temperatura do ambiente (WIRTH; SILVA, 2015). Adicionalmente, conforme o transistor passa por atividades de chaveamento, a probabilidade de ocupação de uma armadilha se altera à medida que a tensão de polarização também varia passando pelas fases de estresse e recuperação. Assim, quanto maior for o ciclo de trabalho (em inglês, *duty factor* - DF), maior será a probabilidade de ocupação de uma armadilha (TOLEDANO-LUQUE et al., 2011).

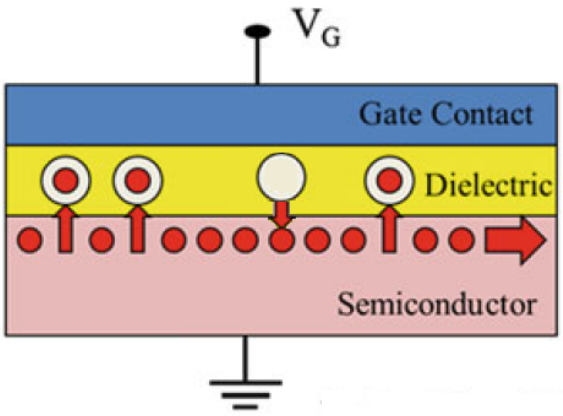


Figura 22 – Captura e emissão de cargas (em vermelho) por armadilhas (em cinza) presentes no dielétrico de um transistor. Fonte: WIRTH; SILVA (2015).

3.2.1.2 Relação entre os efeitos BTI e RTN

Conforme mencionando anteriormente, o mecanismo de armadilhas descreve tanto o fenômeno RTN quanto o efeito BTI. Entretanto, tais fenômenos se distinguem em relação às características de suas constantes de tempo. As armadilhas que contribuem para o ruído RTN mantém-se alterando o seu estado entre ocupada e vacante. Dessa forma, as contantes de captura e emissão apresentam, aproximadamente, os mesmos valores. Em contrapartida, as armadilhas responsáveis pelo efeito BTI possuem uma alta probabilidade de se manterem ocupadas após a ocorrência de um evento de captura, tornando o tempo de captura consideravelmente menor que o tempo de emissão (WIRTH; SILVA, 2015).

4 METODOLOGIA

Neste capítulo, descreve-se a abordagem empregada para a investigação dos efeitos de variabilidade na segurança proporcionada por técnicas de contramedidas. Conforme exposto no Capítulo 2, as técnicas revisadas apresentam topologias que buscam ocultar o vazamento de informações por meio da homogeneização do consumo de energia. Destaca-se que o propósito deste trabalho não é realizar uma análise comparativa entre as diferentes técnicas de contramedidas selecionadas como estudos de caso, e, sim, avaliar o impacto dos fatores de variabilidade na proteção fornecida por tais técnicas. Para tanto, as topologias foram escolhidas com o critério de abranger e amostrar estilos lógicos com aplicações distintas, sendo a WDDL por ser baseada em células padrão; SABL pela sua alta segurança e ser referência na literatura; iDDPL por ser considerada o estado-da-arte e pela lógica baseada em três etapas (pré-carga, avaliação e pós-avaliação); DPPL por ser baseada em transistores de passagem; e PCSL pela adição de transistores do tipo *dummy* para gerar um equilíbrio de capacitâncias internas.

Para cada estilo lógico citado, implementaram-se as portas lógicas básicas AND, OR e XOR. Tais circuitos lógicos representam o objeto de análise para as métricas de segurança apresentadas anteriormente. Devido ao arranjo de transistores, e tendo em vista o emprego da lógica complementar, uma porta lógica OR/NOR pode ser derivada a partir da porta AND/NAND, apenas invertendo suas entradas e saídas. Dessa forma, como os resultados atingidos para ambos os circuitos são análogos, as análises para a porta OR/NOR serão omitidas. Inicialmente, a Seção 4.1 expõe a metodologia aplicada para a investigação dos fatores de variabilidade de processo. A Seção 4.2, por sua vez, apresenta o procedimento adotado para a análise do efeito de *Bias Temperatura Instability*. Em ambas as análises, a influência da variabilidade na robustez das contramedidas é mensurada por meio de simulações SPICE (*Simulation Program with Integrated Circuit Emphasis*).

4.1 Análise do Impacto da Variabilidade de Processo

A investigação efetuada acerca dos efeitos de variabilidade de processo pode ser dividida em três etapas: implementação dos circuitos nos estilos lógicos de contramedidas, simulações elétricas do tipo Monte Carlo (MC) considerando os modelos de variabilidade e, por fim, análise dos resultados por meio das métricas NSD e NED. Na sequência, as duas primeiras etapas serão descritas com mais detalhes, enquanto a discussão dos resultados será elaborada no próximo capítulo.

4.1.1 Descrição *Netlist* dos Circuitos

A implementação das topologias mencionadas foi realizada através de *netlists* SPICE, considerando o modelo de transistores da tecnologia TSMC *bulk* CMOS, para os nodos de 40 nm e 65 nm. Um arquivo *netlist* refere-se à descrição textual do circuito a ser simulado, especificando seus elementos e interconexões. Ademais, como estes circuitos se beneficiam da lógica *dual-rail*, o esquemático de uma porta lógica abrange ambos os valores verdadeiros e falsos na saída. Assim, a implementação de uma porta AND corresponde a de uma porta NAND.

À exceção dos circuitos projetados para a topologia WDDL, para a qual utilizou-se a biblioteca de células padrão da tecnologia TSMC, o dimensionamento dos transistores para as demais contramedidas foi determinado pela aplicação do método *Logical Effort* (SUTHERLAND; SPROULL; HARRIS, 1999). Essa técnica busca otimizar e equilibrar o tempo de atraso associado às redes de *pull-up* e *pull-down* dos circuitos CMOS, utilizando um inversor como referência. Para isso, torna-se necessário identificar, para cada transistor, o caminho mais longo que este faça parte e conecte a alimentação à saída do circuito. Uma vez definida a quantidade de transistores presentes neste caminho, este valor é multiplicado pelo tamanho mínimo (W_{min}) determinado pela tecnologia utilizada. Por fim, devido à diferença de condutância entre os dois planos, deve-se estipular um parâmetro de simetria entre os transistores PMOS e NMOS. Esse parâmetro (λ) é calculado para o inversor de referência e define a proporção real da largura da rede *pull-up* para a rede *pull-down*. Assim, todos os transistores PMOS dos circuitos possuem um fator λ associado ao seu W_{min}. Neste trabalho, o parâmetro λ foi definido a partir de sucessivas iterações com diferentes estimativas, com o intuito de obter o valor que uniformize os tempos de atraso das transições $0 \rightarrow 1$ e $1 \rightarrow 0$.

4.1.2 Simulações Elétricas

A validação dos circuitos implementados deu-se a partir de seu comportamento lógico, obtido por meio das formas de onda e medições obtidas pela ferramenta de simulação elétrica. Com o intuito de reproduzir um cenário mais realista e obter sinais de entrada mais adequados, cada porta lógica a ser simulada possui dois inversores

em série para cada entrada do circuito. Além disso, as saídas do circuito são conectadas a quatro inversores associados em paralelo (*fan-out of* 4), visando representar o comportamento capacitivo das células lógicas. A Figura 23 ilustra o ambiente de simulação adotado para os circuitos a serem analisados.

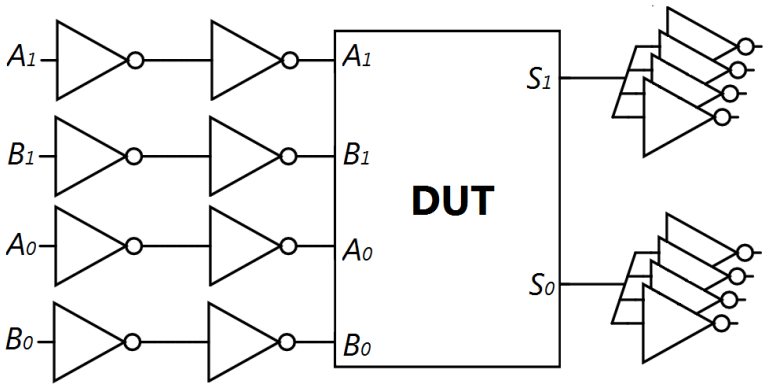


Figura 23 – Ambiente de simulação para os circuitos avaliados (*Device Under Test* - DUT).

A simulação para validação de cada porta lógica abrange todos os possíveis arcos de transição para esse dado circuito. A ferramenta de simulação é responsável por processar os sinais de entrada especificados e gerar as saídas de acordo com a lógica implementada no DUT e seu ambiente de simulação. Para cada circuito a ser investigado, realizaram-se simulações desconsiderando qualquer efeito de variabilidade, a fim de extrair as medidas de atraso de propagação e consumo de energia nominais para cada arco. Tais valores nominais descrevem o comportamento do circuito sob condições típicas, a partir da simulação determinística, e atuam como base para comparação da influência da variabilidade nas métricas de segurança analisadas. Em uma simulação determinística, todas as variáveis de entrada são especificadas com valores pré-definidos. Assim, para uma determinada condição de entrada, sucessivas simulações determinísticas produzirão exatamente os mesmos resultados na saída.

A caracterização do impacto da variabilidade de processo foi realizada decompondo os efeitos em locais e globais, conforme abordado no Capítulo 3. Os efeitos de variabilidade foram integrados aos parâmetros dos transistores adotando o conjunto de modelos estatísticos fornecido pelo processo tecnológico da TSMC, para os respectivos nodos de 40 nm e 65 nm. Nestes modelos, propriedades críticas dos transistores são definidas por meio da aplicação de um conjunto de equações e variáveis aleatórias, de acordo com as especificações do processo. Tais propriedades incluem tanto parâmetros elétricos dos transistores, como a tensão de limiar e a mobilidade de superfície, quanto parâmetros de fabricação e dependentes de leiaute, como a espessura do óxido do terminal de porta e as dimensões efetivas de largura e comprimento do canal. Além disso, a abordagem adotada nos modelos abrange a utilização de bi-

bliotecas estatísticas e simulações Monte Carlo, permitindo avaliar a correlação entre os desvios dos parâmetros dos dispositivos. Destaca-se que o conjunto de modelos de variabilidade utilizado foi calibrado experimentalmente pelo fabricante. Entretanto, devido ao termo de confidencialidade assinado, restringe-se o esclarecimento de detalhes acerca dos modelos.

Simulações Monte Carlo consistem em um método estatístico que envolve amostragem aleatória e sucessivas iterações, selecionando valores diferentes a cada rodada. Em cada iteração, o valor estabelecido para as variáveis aleatórias é determinado por suas respectivas distribuições de probabilidade. Conforme supracitado, no contexto das simulações elétricas, as variáveis aleatórias são utilizadas como parâmetros em equações que definem o comportamento do dispositivo. Ademais, dada à natureza estocástica dos fenômenos investigados, um número elevado de dispositivos deve ser avaliado para que se obtenham resultados de simulação MC significativos.

Neste cenário, um conjunto de 1000 simulações SPICE Monte Carlo foi realizado para cada porta lógica implementada em cada topologia, tanto para os fenômenos locais quanto os globais. Cada rodada de simulação MC varia aleatoriamente parâmetros críticos do dispositivo, de acordo com o modelo de variabilidade indicado. Além disso, para cada simulação, extraem-se os dados de atraso e potência envolvendo as possíveis transições do circuito. Com o intuito de garantir a reprodutibilidade da sequência de variáveis aleatórias gerada, utilizou-se a mesma semente[1] como entrada para as diferentes topologias.

4.1.2.1 Análise de Corners

A análise de *corners* é uma metodologia tradicional para a avaliação dos efeitos de variabilidade e consiste em selecionar combinações de flutuações extremas (*corners*) nos parâmetros que definem o comportamento do dispositivo. Essa análise baseia-se na premissa de que se o circuito opera corretamente nas condições mais pessimistas, irá funcionar de modo correto para todas as demais condições de processo.

Tipicamente, *Fast-Fast* (FF) and *Slow-Slow* (SS) são os *corners* de maior preocupação aos projetistas de CIs. FF refere-se à condição em que os desvios nos parâmetros de todos os dispositivos são estabelecidos para maximizar a capacidade de condução de corrente do circuito. Em contrapartida, SS visa minimizar essa mesma capacidade. Sob esse contexto, as topologias de segurança também foram submetidas a simulações determinísticas, ponderando as condições FF e SS, de acordo com as bibliotecas de *corners* da TSMC.

[1] A semente caracteriza um número utilizado para iniciar um algoritmo pseudo-aleatório. Se um gerador de números pseudo-aleatórios for reinicializado com a mesma semente, produzirá a mesma sequência de números.

4.2 Análise do Impacto de BTI

Semelhantemente à análise da variabilidade de processo, o estudo realizado em relação aos efeitos do fenômeno BTI também pode ser decomposto em três etapas: (i) implementação dos circuitos nos estilos lógicos de contramedidas; (ii) simulações elétricas considerando o mecanismo de BTI; e (iii) análise dos resultados por meio das métricas NSD e NED. De forma análoga à seção anterior, as duas primeiras etapas serão abordadas com mais detalhes na sequência, enquanto os resultados serão discutidos no próximo capítulo.

Neste trabalho, o impacto do efeito BTI foi investigado adotando o ambiente de simulação proposto por BOTH; FURTADO; WIRTH (2018). O modelo apresentado pelos autores caracteriza o fenômeno de acordo com a teoria de armadilhas. O impacto na tensão de limiar é estimado a partir das características e propriedades das armadilhas, as quais são incluídas nas equações do modelo de transistores BSIM de tecnologias preditivas. Dessa forma, inviabilizou-se a utilização do modelo de transistores da tecnologia TSMC e empregou-se o modelo da tecnologia preditiva de 45 nm CMOS HP PTM[2].

Com exceção da topologia WDDL, que beneficiava-se da utilização da biblioteca de células padrão da tecnologia TSMC, todas as implementações descritas anteriormente foram reutilizadas nesta etapa. Porém, considerando o novo modelo empregado, o dimensionamento dos transistores foi recalculado, aplicando novamente o método *logical effort*. Ademais, as portas lógicas desenvolvidas no estilo lógico WDDL foram reescritas utilizando o design *full custom*.

O ambiente de simulação utilizado demanda a integração de determinados parâmetros de entrada ao *netlist* dos circuitos. De acordo com o modelo, a probabilidade de ocupação das armadilhas é definida como uma função das constantes de captura e emissão, e do tempo de operação do dispositivo. Para a definição das constantes de tempo, é necessário estipular o ciclo de trabalho (DF) de cada transistor. DF é estabelecido como a fração do tempo de operação em que o transistor esteve ativo (sob estresse), possuindo um valor entre *0* e *1*. Caso o transistor esteja sempre desligado (fase de relaxação), o valor de DF é definido como *0*. Por outro lado, caso o transistor esteja sempre ativo (fase de estresse), determina-se o valor de DF como *1*.

O valor de DF associado a um dispositivo está fortemente relacionado com a estrutura do circuito lógico em que o mesmo está inserido. Para esclarecer essa relação, a Figura 24 apresenta o arranjo de transistores para a porta lógica AND, com o valor de DF associado a cada transistor da célula. Considerando as quatro transições possíveis para a saída da porta lógica, as entradas A e B assumem o valor lógico '0' em metade das ocasiões e o valor '1' na outra metade. Assim, para cada transistor

[2]Disponível em: `http://ptm.asu.edu/`

que esteja vinculado a uma das entradas e apresente um caminho direto entre ele e à tensão de alimentação (positiva ou negativa, de acordo com o tipo do transistor), defini-se o valor de DF como *0,5*. A Figura 24 exibe esse cenário para os transistores P_1, P_2 e N_1.

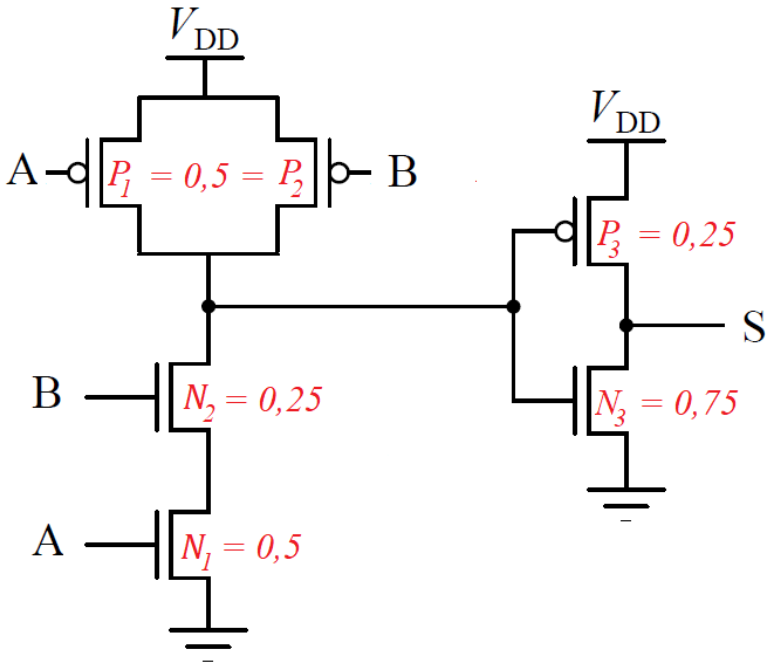


Figura 24 – Arranjo de transistores da porta lógica AND, em conjunto com seus valores de DF.

Para os demais transistores do circuito, calculam-se os valores de DF considerando o ciclo de trabalho de cada transistor um evento independente e aplicando as propriedades da probabilidade definidas nas Equações 5 e 6:

$$P(A \cap B) = P(A) \cdot P(B) \tag{5}$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{6}$$

Considerando os transistores da rede *pull-down*, os quais estão associados em série na Figura 24, para que o transistor N_2 esteja ativo, é necessário que o transistor N_1 também esteja. Dessa forma, admitindo a hipótese de que o valor do ciclo de trabalho de cada sinal de entrada é *0,5*, o DF do transistor N_2 é determinado pela aplicação da Equação 5, conforme exposto abaixo:

$$P(N_2) = P(B \cap N_1) = P(B) \cdot P(N_1) = 0,5 \cdot 0,5 = 0,25 \tag{7}$$

Para os transistores do inversor conectado à saída da porta lógica NAND, é necessário identificar o ciclo de trabalho dos transistores que estão associados à sua entrada. Para a rede *pull-up*, o DF do transistor P_3 é estabelecido de acordo com a

saída da rede *pull-down* do circuito anterior. No contexto da Figura 24, o transistor P_3 só estará ativo quando N_2 também estiver e, portanto, seus valores de DF são iguais. De forma recíproca, a entrada do transistor N_3 é definida pela saída da rede *pull-up* do circuito predecessor. Nessas circunstâncias, para o transistor N_3 estar ativo é suficiente que apenas um dos transistores, P_1 ou P_2, também esteja. Assim, o DF de N_3 é calculado de acordo com a Equação 6, conforme demonstrado abaixo:

$$P(N_3) = P(P_1 \cup P_2) = P(P_1) + P(P_2) - P(P_1 \cap P_2) = 0,5 + 0,5 - (0,5 \cdot 0,5) = 0,75 \quad (8)$$

A partir da metodologia relatada acima, calcularam-se os valores de DF para cada porta lógica implementada. Como as topologias estudadas utilizam a lógica dinâmica, o procedimento deve ser estendido para abranger as duas fases de processamento: avaliação e pré-carga. Para ambos os estágios adota-se a mesma abordagem, salientando as seguintes ponderações para a probabilidade dos sinais de entrada durante cada fase:

- *Avaliação*: Como nesta etapa o circuito opera conforme projetado, os sinais de entrada de cada porta lógica (A_0, A_1, B_0, B_1) são definidos com o valor de DF igual a *0,5*. Ademais, para as topologias que utilizam um sinal de controle, este deve estar sempre com o valor lógico '1' para que o circuito esteja em operação. Assim, os transistores NMOS que possuam o sinal de controle como entrada, estão sempre ativos durante a etapa de avaliação (DF = *1*), enquanto os transistores PMOS estão sempre desligados (DF = *0*).
- *Pré-carga*: Durante esta etapa, todos os sinais (entradas e controle) são estabelecidos com o valor lógico '0'. Desta forma, para a fase de pré-carga, os transistores NMOS estão sempre desligados (DF = *0*) e os transistores PMOS estão sempre ativos (DF = *1*).

Após o cálculo dos valores de DF para cada estágio de processamento, o resultado final do ciclo de trabalho de cada transistor é determinado pela média simples dos DFs de cada fase. Para a topologia iDDPL, deve-se considerar também a etapa adicional de processamento: pós-avaliação. Nessa etapa, em contraste com a fase de pré-carga, todos os sinais de entrada recebem o valor lógico '1'. Assim, durante o estágio de pós-avaliação, os transistores NMOS estão sempre ativos (DF = *1*) e os transistores PMOS estão sempre desligados (DF = *0*). Os valores de DF para cada circuito e topologia implementada estão expostos no Apêndice B deste trabalho.

O ambiente empregado para as simulações elétricas das topologias é o mesmo apresentado anteriormente para a avaliação da variabilidade de processo, estando ilustrado na Figura 23. Conforme supracitado, o mecanismo de BTI utilizado para as simulações foi proporcionado por BOTH; FURTADO; WIRTH (2018). Neste modelo,

as estatísticas caracterizantes das armadilhas que descrevem o efeito BTI foram integradas ao simulador de circuitos Ngspice, a partir da modificação dos modelos de transistores BSIM. Considerando o comportamento aleatório das armadilhas, o simulador requer a realização de simulações Monte Carlo para que se obtenham resultados consistentes e com significância estatística. Sob esse contexto, um conjunto de 1000 simulações Monte Carlo foi efetuado para cada porta lógica implementada em cada topologia. As simulações abrangem todos os possíveis arcos de transição para o circuito sob análise e, em cada rodada de simulação MC, os dados de atraso e potência relacionados a estes arcos foram extraídos.

5 RESULTADOS E DISCUSSÕES

Neste capítulo, são apresentados os resultados obtidos pelas simulações SPICE para as portas lógicas projetadas nas cinco topologias selecionadas. Por uma questão de organização, o capítulo está estruturado da seguinte maneira: A Seção 5.1 relata os resultados acerca dos efeitos de variabilidade *time-zero*, apresentando uma discussão a respeito do impacto causado por fenômenos de variabilidade local e global nas métricas de segurança. Para estas simulações, empregou-se o modelo de transistores da tecnologia TSMC *bulk* CMOS. Na sequência, a Seção 5.2 descreve os resultados obtidos para a análise do efeito de BTI, demonstrando sua influência nas métricas de segurança para as diferentes células lógicas. Para o simulador utilizado na análise do impacto de BTI, adotou-se o modelo de transistores da tecnologia preditiva de 45 nm CMOS HP PTM.

5.1 Variabilidade de Processo

Os resultados obtidos para as 1000 simulações Monte Carlo de cada topologia, ponderando fatores de variabilidade local e global, são discutidos nesta seção. Inicialmente, os efeitos são relatados considerando o nodo tecnológico de 40 nm. Conforme mencionado no Capítulo 2, valores mais baixos para as métricas de segurança denotam um circuito mais robusto aos ataques por análise de potência.

As Figuras 25 e 26 apresentam a relação das métricas de segurança entre as duas fases de processamento dos circuitos, pré-carga e avaliação, nas quais um ataque DPA pode ser realizado[1]. Cada ponto no gráfico representa a métrica calculada para uma única simulação MC. As Figuras 25 (a) e (b) ilustram os resultados de NSD para a porta AND/NAND, ponderando os efeitos de variabilidade local e global, respectivamente. Independentemente da topologia analisada, nota-se o impacto maior da variabilidade local, a qual produz dados substancialmente mais esparsos do que os resultados globais. Os gráficos de dispersão da métrica NED para a AND/NAND são

[1] A topologia iDDPL, apesar de possuir três estágios, também apresenta apenas duas etapas plausíveis para o ataque: avaliação e pós-avaliação, a qual equivalerá à fase de pré-carga nos resultados exibidos.

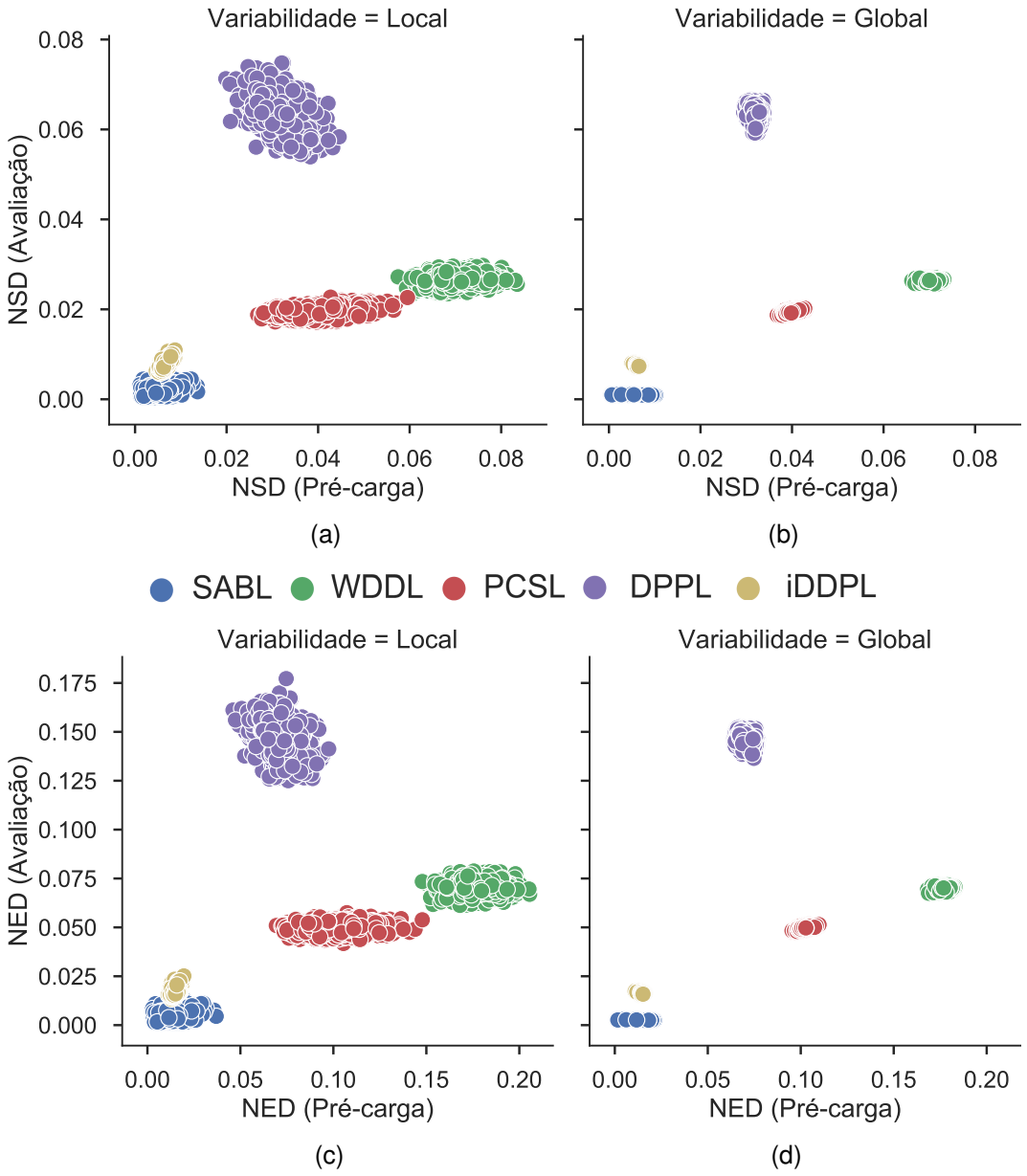


Figura 25 – Gráfico de dispersão da métrica NSD para as 1000 simulações MC nas fases de pré-carga e avaliação para a porta AND/NAND, considerando variabilidade (a) local e (b) global, e para a métrica NED, ponderando variabilidade (c) local e (d) global.

exibidos nas Figuras 25 (c) e (d), nos quais observa-se o mesmo padrão de comportamento, com a variabilidade local gerando valores consideravelmente mais espaçados.

A associação de NSD entre pré-carga e avaliação para a porta XOR/XNOR, ponderando os efeitos locais e globais, é demonstrada nas Figuras 26 (a) e (b), respectivamente. De forma semelhante à porta AND/NAND, a variabilidade local mostrou-se responsável por produzir os valores com maior grau de dispersão, exceto para a topologia PCSL, na qual os efeitos globais também representam um papel significativo, principalmente durante a fase de pré-carga. Como a porta XOR/XNOR apresenta uma estrutura intrinsecamente mais balanceada, os valores de NSD são inferiores aos ob-

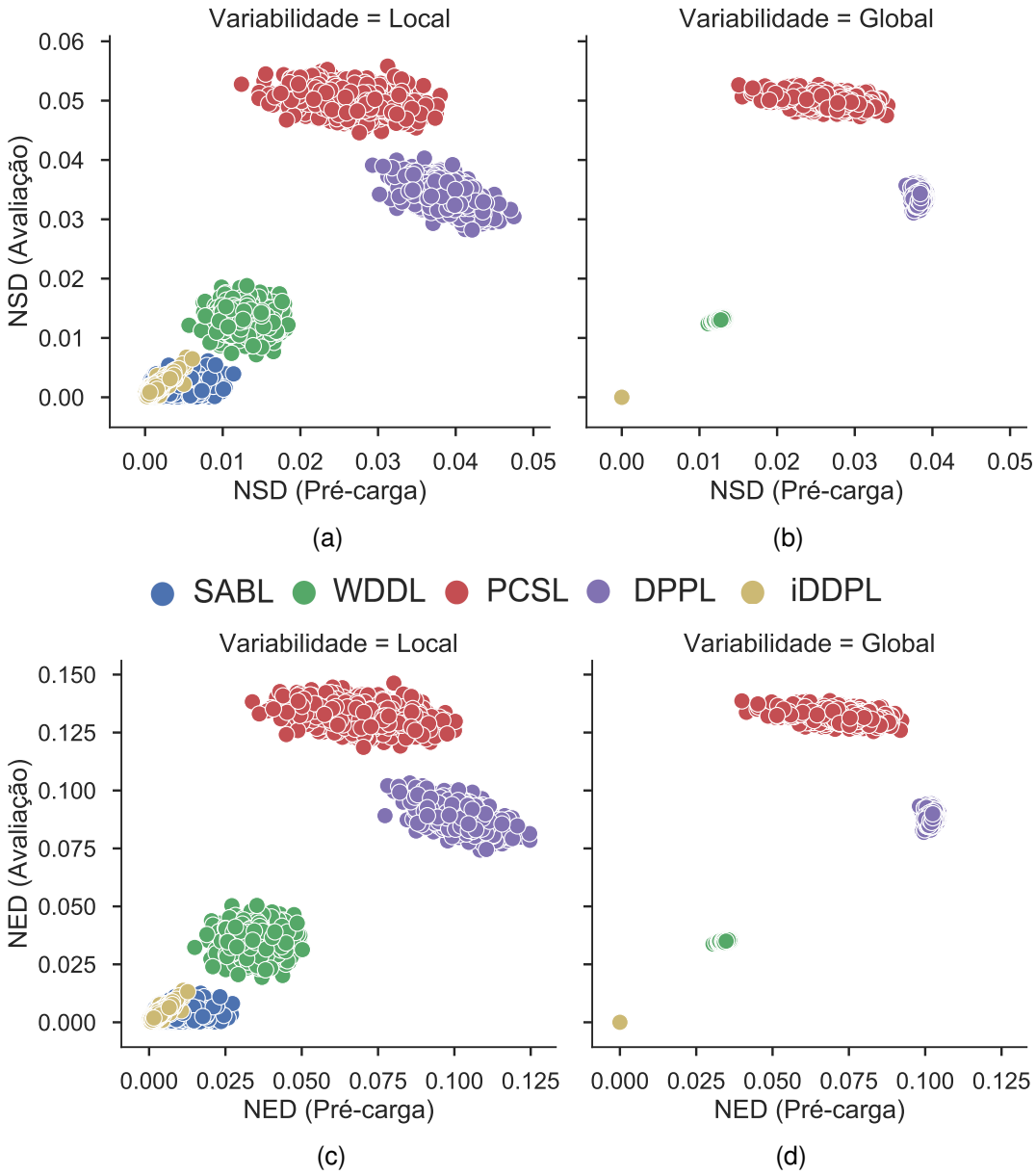
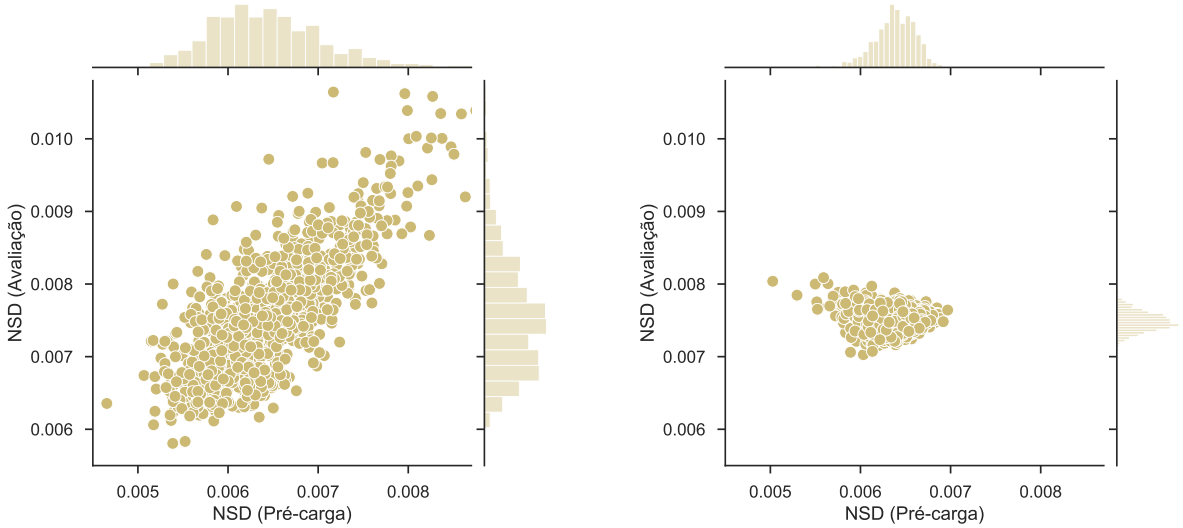


Figura 26 – Gráfico de dispersão da métrica NSD para as 1000 simulações MC nas fases de pré-carga e avaliação para a porta XOR/XNOR, considerando variabilidade (a) local e (b) global, e para a métrica NED, ponderando variabilidade (c) local e (d) global.

tidos para AND/NAND. Esse comportamento se reflete nos pontos de sobreposição exibidos para um número maior de topologias na variabilidade global. As Figuras 26 (c) e (d) apresentam os resultados de NED para a porta XOR/XNOR. Novamente, observa-se a mesma tendência de dispersão dos dados, na qual os fenômenos locais se manifestam como a principal fonte de variações nos valores das métricas. É importante salientar que para os gráficos de variabilidade global, os dados para topologia SABL estão representados, porém foram ocultados pelas observações da topologia iDDPL, tendo em vista que ambos os estilos lógicos apresentaram um comportamento semelhante.

Conforme ressaltado acima, as métricas de segurança demonstraram um comportamento semelhante para todas as topologias examinadas. Portanto, as análises subsequentes concentram-se nos resultados obtidos para a métrica NSD, haja visto que os valores de NED estão de acordo. Além disso, para qualquer topologia e circuito avaliado, a influência da variabilidade decorrente de efeitos locais mostrou-se significativamente maior que a originada por fatores globais. Para ratificar essa tendência, as Figuras 27 e 28 ilustram, à parte, a distribuição de frequência dos resultados de NSD para a porta AND/NAND nas topologias iDDPL e DPPL, as quais manifestaram o menor e maior grau de variação, respectivamente. Em conjunto com os diagramas de dispersão, histogramas são dispostos nas margens, demonstrando a disposição dos valores para cada fase de processamento. Para ambas as topologias, os gráficos evidenciam que a variabilidade local produz notavelmente mais dados que diferem-se entre si, independente da fase de processamento. Ademais, os histogramas para a variabilidade local exibem um grau de achatamento mais elevado que os expostos para os efeitos globais, os quais, por sua vez, apresentam maior concentração de valores no centro na distribuição.

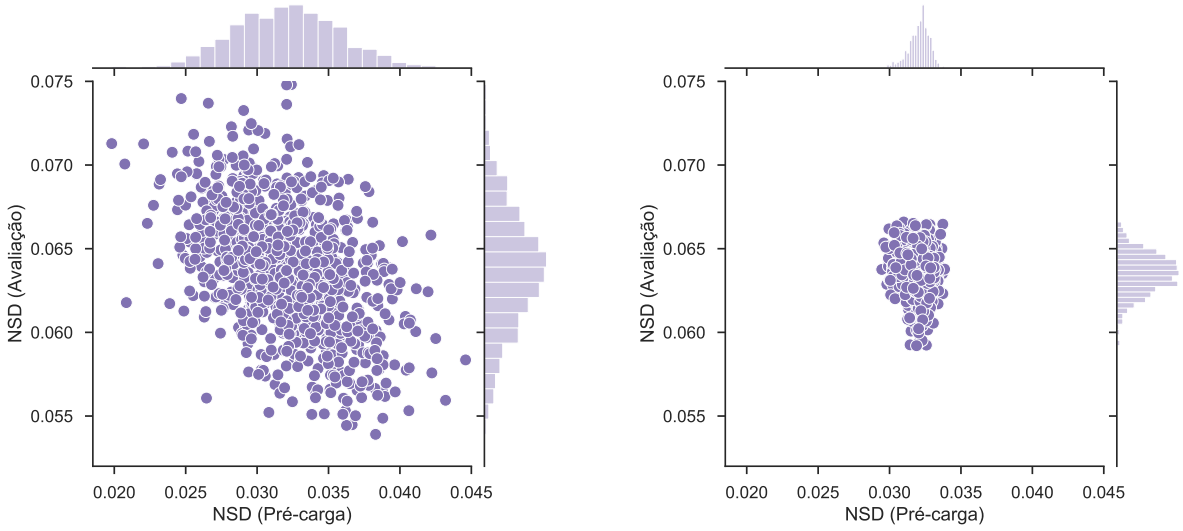


(a) Variabilidade Local

(b) Variabilidade Global

Figura 27 – Distribuição dos resultados de NSD para a porta AND/NAND implementada na topologia iDDPL, avaliando efeitos (a) locais e (b) globais.

Conforme pode ser visualizado no Apêndice C desta dissertação, os resultados para a porta lógica XOR/XNOR mostraram-se análogos aos expostos acima para a porta NAND/AND, destacando com mais ênfase a proeminência dos efeitos locais na dispersão dos resultados. Estes resultados podem ser explicados pelo caráter distinto dos desvios provocados pelos efeitos. A variabilidade global afeta todos os transistores de um determinado circuito de maneira semelhante. Assim, os desvios são observados de forma sistemática, apresentando pouca influência na homogeneidade do



(a) Variabilidade Local

(b) Variabilidade Global

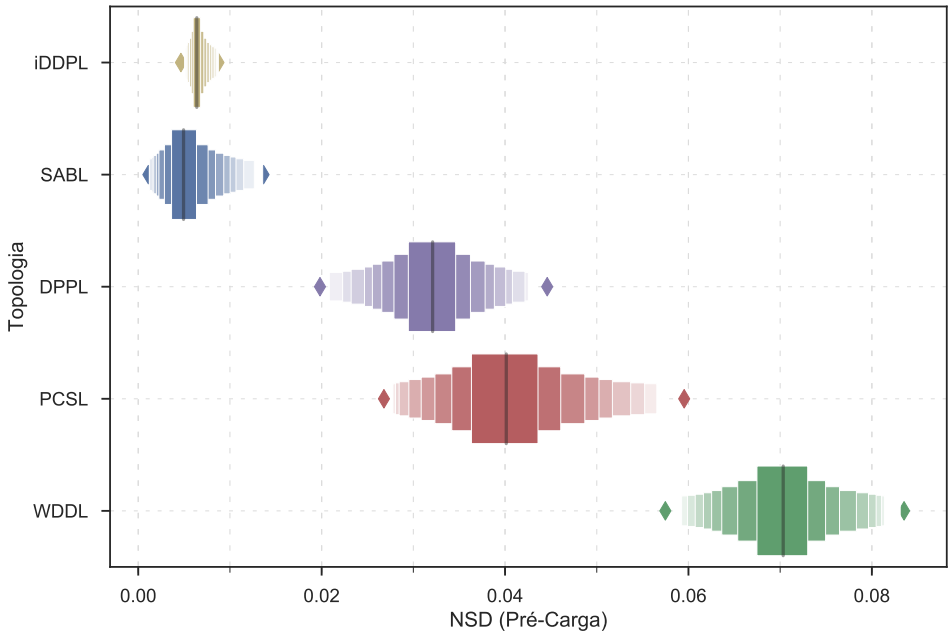
Figura 28 – Distribuição dos resultados de NSD para a porta AND/NAND implementada na topologia DPPL, avaliando efeitos (a) locais e (b) globais.

consumo de energia viabilizada pelas topologias. Em contrapartida, os fatores locais impactam os transistores presentes num mesmo circuito de forma desigual. Como consequência, as variações no comportamento do circuito se manifestam de maneira aleatória, contribuindo para um notável desequilíbrio no consumo de energia e, por conseguinte, provocando a maior dispersão verificada nos dados. Portanto, como os fenômenos de variabilidade local dominam os desvios observados para as métricas de segurança, as próximas subseções focam nessa fonte de variabilidade. Ademais, enfatizando o comportamento equivalente exibido pelas métricas, o restante da seção concentra-se nos resultados obtidos para a métrica NSD.

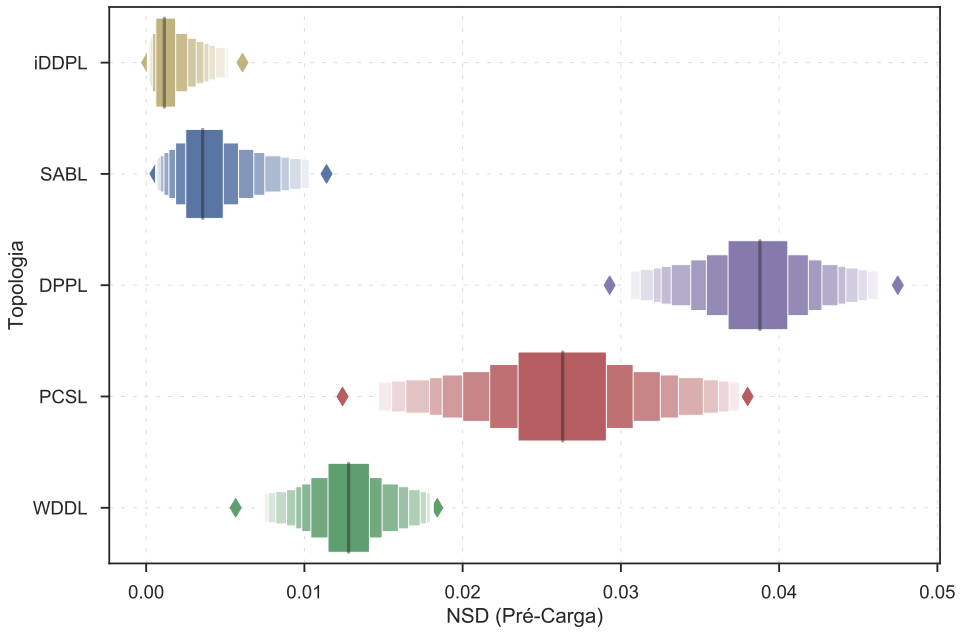
5.1.1 Efeitos Locais

As Figuras 29 e 30 apresentam as distribuições da métrica NSD para as cinco topologias, avaliando os efeitos locais paras as portas AND/NAND e XOR/XNOR, durante os estágios de pré-carga e avaliação, respectivamente. As distribuições são visualizadas como gráficos *letter-value* (LV), os quais podem ser compreendidos como uma extensão dos gráficos de caixa (*boxplots*). O gráfico LV fornece uma descrição mais aprimorada da distribuição dos dados, pois expressa múltiplos quantis (HOFMANN; WICKHAM; KAFADAR, 2017). Um quantil corresponde a uma proporção acumulada dos pontos, fracionados em intervalos com mesma probabilidade. No gráfico LV, a caixa maior representa o intervalo interquartil, abrangendo 50% dos valores. As caixas mais largas subsequentes (exibidas diretamente à esquerda e direita do intervalo interquartil) denotam os oito quantis, contendo 25% dos dados. Assim, o intervalo compreendido entre os oito quantis representa 75% dos valores. Dando continuidade,

cada caixa diminui de tamanho sucessivamente e o número de valores cobertos pela caixa é reduzido pela metade. Adicionalmente, as caixas mais centrais são coloridas com maior intensidade para expressar a maior frequência de dados. A linha vertical mais grossa caracteriza a mediana, cujo valor define o centro da distribuição, separando a metade maior e menor do conjunto de valores, enquanto os diamantes nas extremidades descrevem os valores mínimo e máximo.

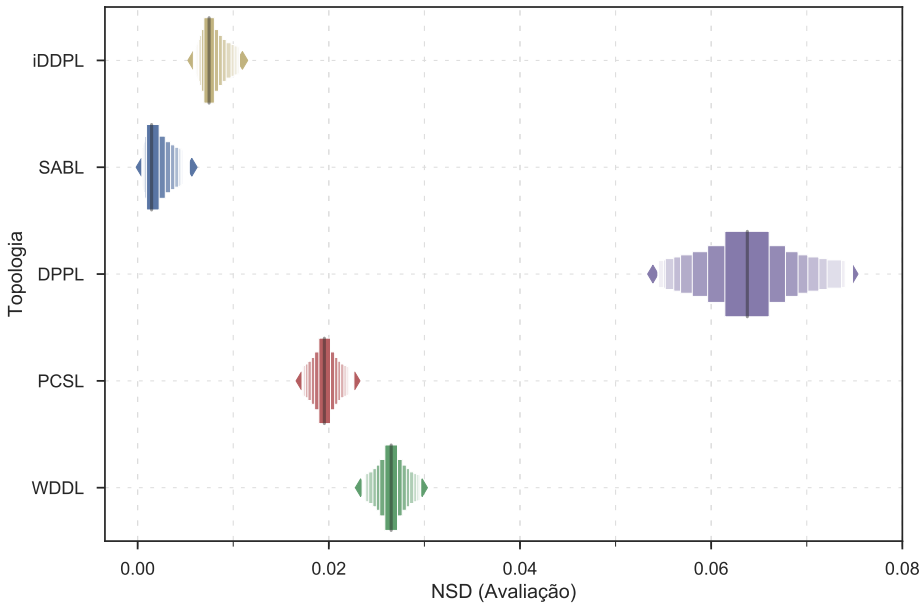


(a) AND/NAND

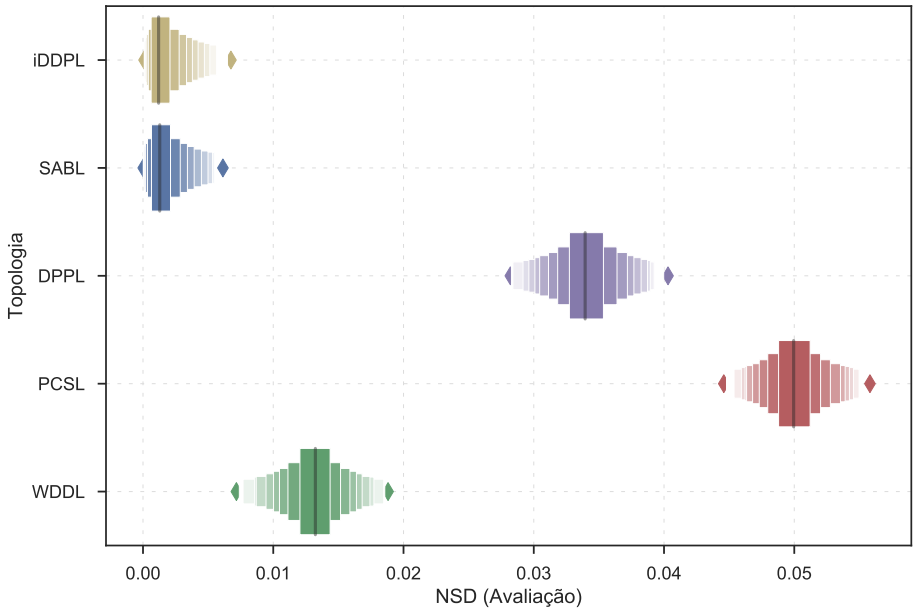


(b) XOR/XNOR

Figura 29 – Gráfico *letter-value* demonstrando as distribuições da métrica NSD, durante a fase de pré-carga, para as portas (a) AND/NAND e (b) XOR/XNOR, considerando efeitos de variabilidade local.



(a) AND/NAND



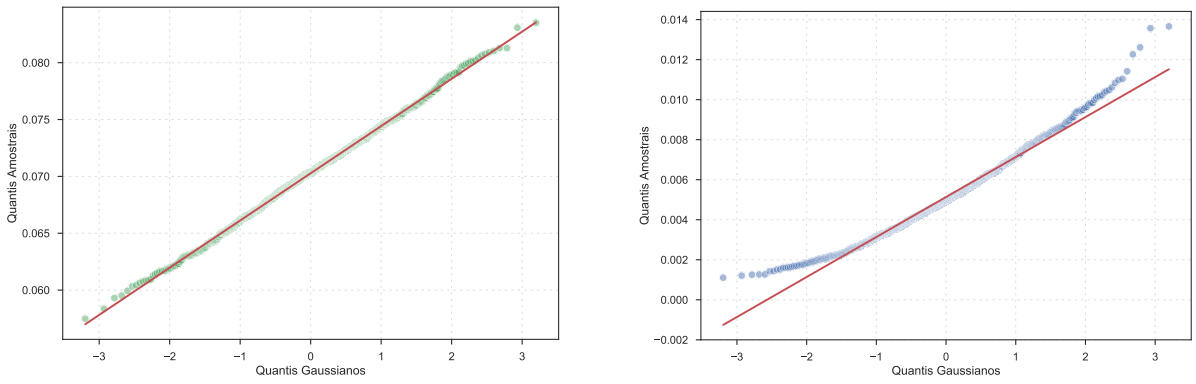
(b) XOR/XNOR

Figura 30 – Gráfico *letter-value* demonstrando as distribuições da métrica NSD, durante a fase de avaliação, para as portas (a) AND/NAND e (b) XOR/XNOR, considerando efeitos de variabilidade local.

De acordo com os gráficos LV expostos, os estilos lógicos resistentes ao DPA podem ser categorizados em dois grupos: (i) contramedidas cujas distribuições são razoavelmente simétricas e (ii) contramedidas que apresentam uma cauda mais pesada à direita da distribuição. O primeiro grupo consiste das topologias menos seguras, ou seja, os estilos lógicos cujos os resultados de NSD mostraram-se mais críticos. Embora WDDL, PCSL e DPPL demonstrem diferentes níveis de dispersão e se alternem acerca da ordem referente aos valores de NSD, todas essas topologias exibem uma

distribuição satisfatoriamente simétrica, centrada em torno do valor mediano. Em contrapartida, o segundo grupo compreende as topologias mais robustas: SABL e iDDPL. Como mencionado anteriormente, as distribuições de tais contramedidas apresentam uma assimetria positiva, o que significa que há uma grande concentração de observações tendendo à cauda do lado direito (valores mais elevados da métrica). Ainda a respeito dessas contramedidas mais robustas, observa-se na Figura 29 que apesar da topologia SABL possuir os valores mais baixos para NSD, a mesma apresenta um desvio nos resultados tão elevado, que seus piores casos são mais críticos que aqueles produzidos para a iDDPL, indicando um circuito potencialmente menos seguro.

Visando corroborar a distinção estabelecida entre topologias com distribuições simétricas e assimétricas, as figuras a seguir apresentam gráficos QQ (quantil-quantil) para os dados exibidos acima, ponderando a fase de pré-carga. O gráfico QQ propicia um método visual para avaliar a semelhança entre distribuições, permitindo inferir se um conjunto de dados provém de alguma distribuição teórica. Neste modelo de representação, cada ponto corresponde a um dos quantis calculados na amostra (eixo das ordenadas) projetado contra o mesmo quantil teórico (eixo das abscissas). Caso a distribuição suposta descreva adequadamente os dados analisados, os pontos plotados situam-se ao longo de uma linha reta. À vista disso, selecionou-se a distribuição normal (gaussiana) para verificar a suposição acerca do comportamento das topologias. A distribuição normal é caracterizada por uma função de probabilidade na qual a maioria das observações assume valores próximos ao centro, exibindo uma curva simétrica em torno da média.

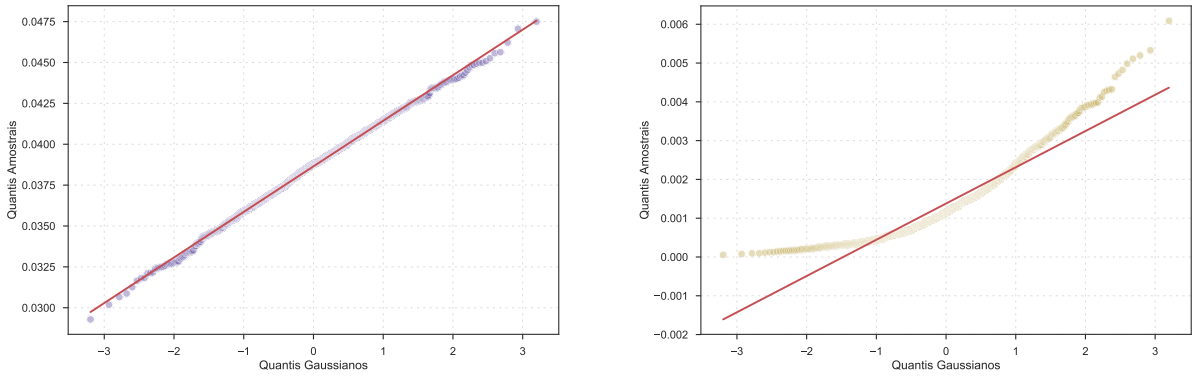


(a) (b)

Figura 31 – Gráfico QQ avaliando a normalidade da distribuição da métrica NSD para a porta AND/NAND, durante a fase de pré-carga, nas topologias (a) WDDL e (b) SABL.

A Figura 31 expõe os gráficos para a porta AND/NAND implementada nos estilos lógicos WDDL e SABL, os quais obtiveram o menor e maior valor de NSD, respectivamente. De forma análoga, a Figura 32 ilustra os gráficos para a porta XOR/XNOR, considerando as topologias DPPL e iDDPL. Observando as topologias menos seguras

(WDDL e DPPL), a linearidade dos pontos sustenta a hipótese de que os dados sejam normalmente distribuídos. Por outro lado, as contramedidas mais robustas (SABL e iDDPL) apresentam seus quantis mais afastados da reta, especialmente nas caudas, indicando que os dados não seguem uma distribuição gaussiana. Ademais, os pontos nas extremidades, curvando-se acima e à esquerda da linha, atestam a assimetria positiva da distribuição.



(a) (b)

Figura 32 – Gráfico QQ avaliando a normalidade da distribuição da métrica NSD para a porta XOR/XNOR, durante a fase de pré-carga, nas topologias (a) DPPL e (b) iDDPL.

As diferenças exibidas entre as distribuições dos dois grupos de topologias podem ser compreendidas pela variação de energia ocasionada nos arcos de transição das portas lógicas. Os arcos de transição expressam as possíveis mudanças de estado na saída do circuito e foram denotados da seguinte forma:

- Transição T_1: $A_0 : 0 \rightarrow 1, A_1 : 0 \rightarrow 0, B_0 : 0 \rightarrow 1, B_1 : 0 \rightarrow 0$
- Transição T_2: $A_0 : 0 \rightarrow 1, A_1 : 0 \rightarrow 0, B_0 : 0 \rightarrow 0, B_1 : 0 \rightarrow 1$
- Transição T_3: $A_0 : 0 \rightarrow 0, A_1 : 0 \rightarrow 1, B_0 : 0 \rightarrow 1, B_1 : 0 \rightarrow 0$
- Transição T_4: $A_0 : 0 \rightarrow 0, A_1 : 0 \rightarrow 1, B_0 : 0 \rightarrow 0, B_1 : 0 \rightarrow 1$

A Figura 33 ilustra as distribuições do consumo de energia observado para as transições das respectivas topologias apresentadas nas Figuras 31 (a) e (b). Os pontos denotados pelo marcador ‘X’ expressam o valor nominal de energia para cada arco, ou seja, os resultados obtidos para uma simulação típica. Analisando as distribuições dos arcos para a topologia WDDL, nota-se que estas demonstram o mesmo comportamento verificado para a métrica NSD, apresentando um formato simétrico em torno do valor mediano. Em contraste, os arcos obtidos para a topologia SABL refletem as distribuições visualizadas para as topologias mais seguras, exibindo uma cauda mais prolongada em direção aos maiores valores. Ademais, comparando ambas as contramedidas, é possível observar que as distribuições das transições da topologia SABL

apresentam maior variação e se sobrepõem entre si, enquanto os arcos da topologia WDDL se distribuem de maneira afastada. Dessa forma, observa-se um maior desvio padrão para as contramedidas mais seguras e, por conseguinte, uma tendência maior a manifestar valores mais extremos para a métrica NSD.

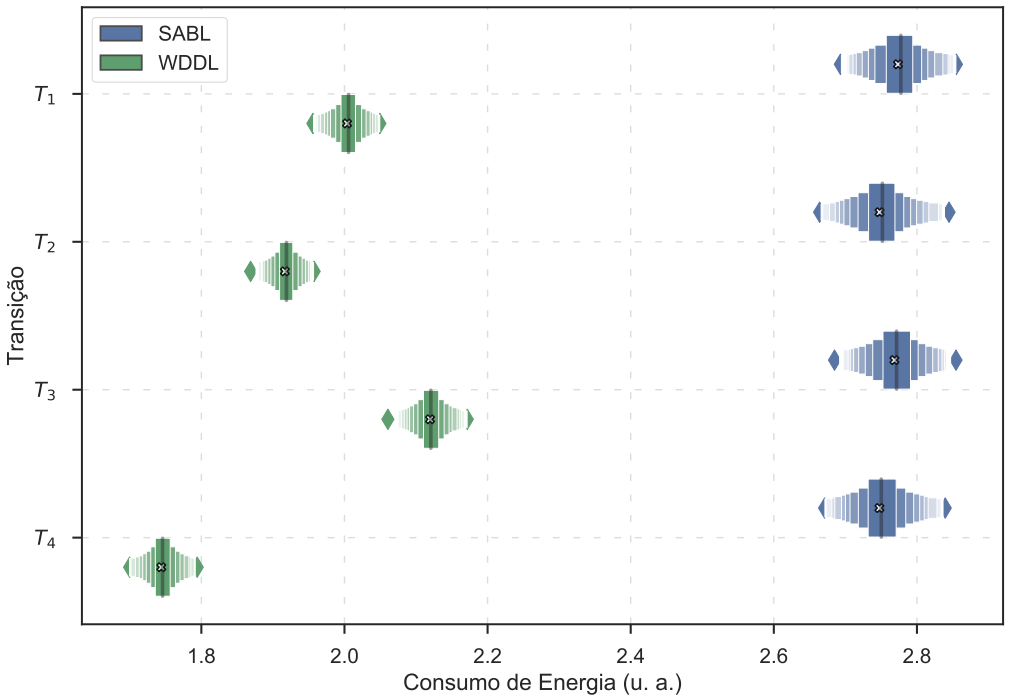


Figura 33 – Gráfico LV demonstrando as distribuições de energia para as transições da porta lógica AND/NAND implementada nas topologias WDDL e SABL.

Com o intuito de melhor elucidar as distribuições das topologias analisadas, as próximas figuras exibem histogramas para a métrica NSD, juntamente com o gráfico LV, considerando o estágio de avaliação dos circuitos. Nos histogramas abaixo, a linha contínua representa o valor nominal de NSD. Como mencionando previamente, este valor nominal descreve a métrica medida a partir de uma simulação sob condições típicas, desconsiderando qualquer fator de variabilidade. As linhas tracejadas, por sua vez, caracterizam os valores obtidos pela análise de *corners*, conforme descrito na legenda. A Figura 34 apresenta a distribuição de frequência para a porta AND/NAND implementada na topologia WDDL, selecionada para expressar o primeiro grupo. Além do histograma demonstrar um formato simétrico, correspondente com o modelo gaussiano, o gráfico LV permite observar como a mediana coincide com o valor nominal. À vista disso, conclui-se que os estilos lógicos desse grupo produzem proporcionalmente desvios acima e abaixo do valor nominal.

Com relação ao segundo grupo, a Figura 35 ilustra a distribuição para a porta AND/NAND referente à topologia SABL. Em conformidade com o exposto anteriormente, o gráfico exibe uma distribuição assimétrica positiva, possuindo uma longa cauda tendendo para o lado direito das observações. Esse comportamento suscita a

maioria das medições de NSD a estar acima do valor nominal, implicando que a topologia não seja tão segura quanto sugere sua simulação regular. Por conseguinte, esse enviesamento à direita surge como um problema, tendo em vista que muitas portas lógicas no circuito criptográfico apresentarão um vazamento de informações maior do que o esperado.

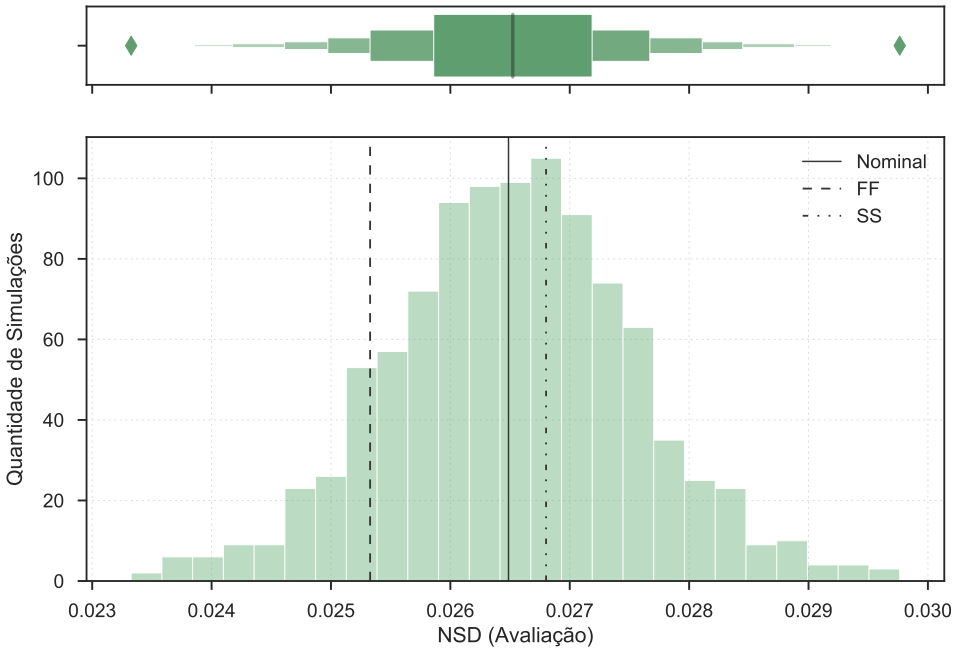


Figura 34 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica AND/NAND implementada na topologia WDDL.

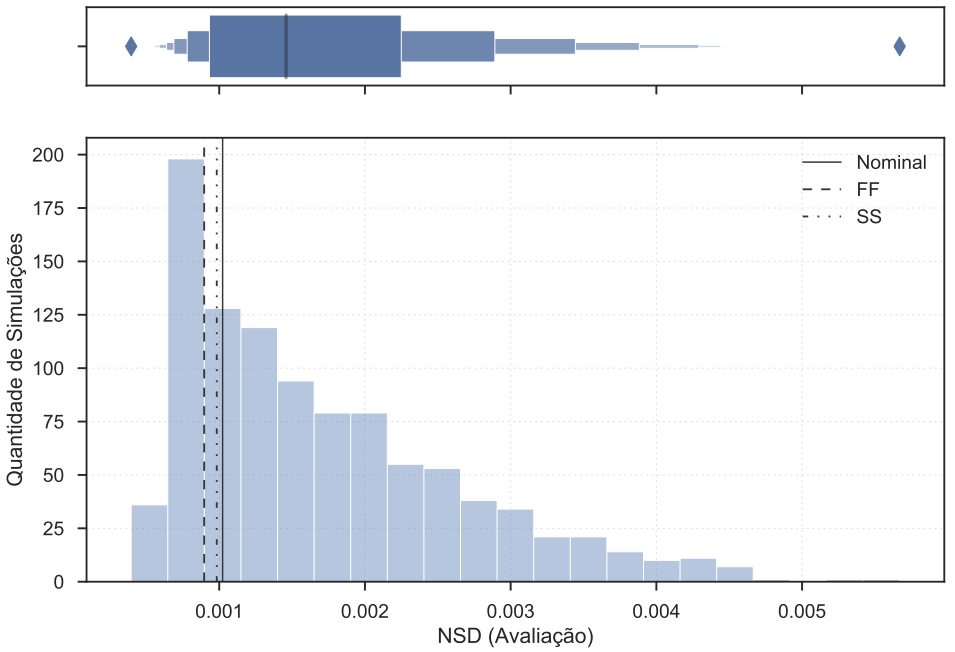


Figura 35 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica AND/NAND implementada na topologia SABL.

Adicionalmente, considerando a proximidade dos resultados de *corner* com o valor nominal, os histogramas acima demonstram como a análise de *corners* não é suficiente para capturar o comportamento da variabilidade *time-zero*. Isso ocorre porque nesse método de análise todos os transistores do circuito são modelados sob a mesma condição, rápida (FF) ou lenta (SS), acarretando na ausência do desequilíbrio de consumo. Em relação às topologias mais seguras, esse problema é agravado pelo formato da distribuição. Em tais circunstâncias, é aconselhável que o projetista de CI se concentre na redução da dispersão dos dados, ao invés de buscar melhorar gradualmente o valor nominal das métricas.

De maneira similar, os gráficos abaixo apresentam a distribuição de frequência para a porta XOR/XNOR. A Figura 36 ilustra o histograma para o estilo lógico PCSL, enquanto a Figura 37 exibe o gráfico para iDDPL, caracterizando o grupo das topologias menos e mais resistentes, respectivamente. Analisando os histogramas, observa-se o mesmo padrão de comportamento verificado para a porta AND/ NAND, no qual a topologia menos segura demonstra uma distribuição gaussiana, com a mediana coincidindo com o valor nominal. Em contraste, tendo em vista o maior balanceamento inerente à porta XOR/XNOR, a topologia mais robusta apresentou todas as observações de NSD acima do valor nominal, confirmando o maior impacto da variabilidade nas contramedidas desse grupo. Ademais, a análise de *corners* mostrou-se novamente ineficiente em compreender a influência dos fenômenos de variabilidade local nas métricas de segurança, especialmente para os estilos lógicos mais seguros. Dessa forma, salienta-se a imprescindibilidade de realizar simulações Monte Carlo, apesar do alto custo computacional requerido.

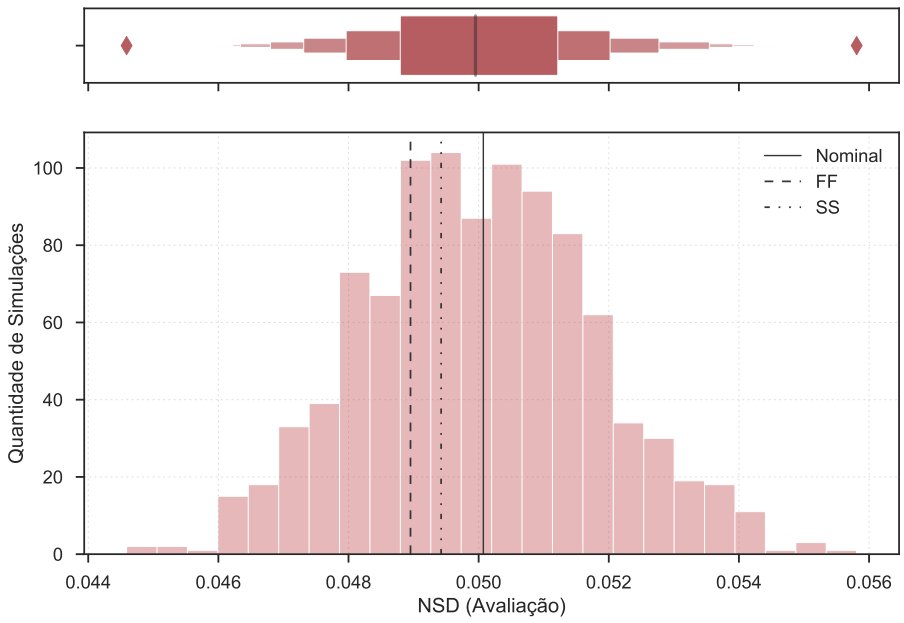


Figura 36 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica XOR/XNOR implementada na topologia PCSL.

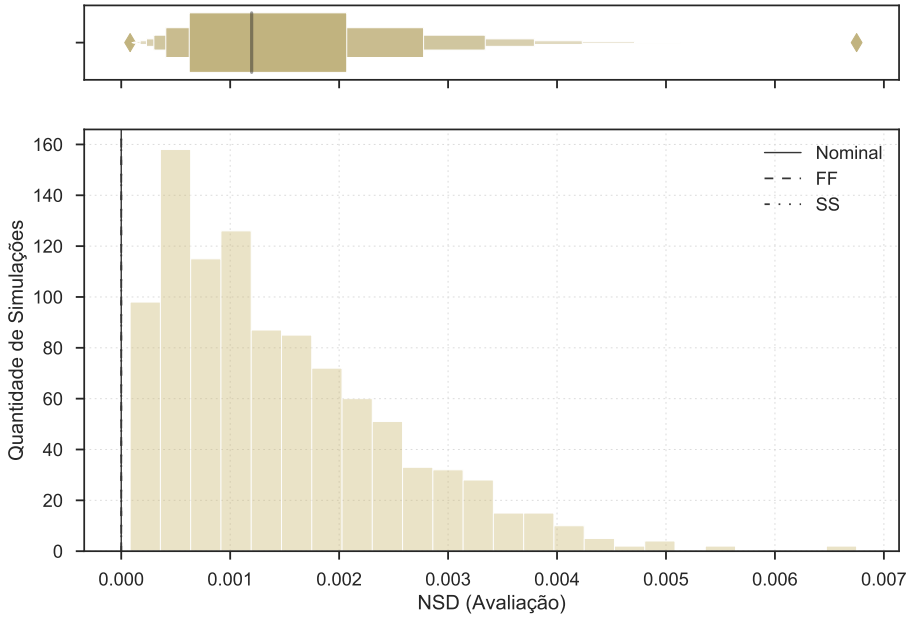


Figura 37 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica XOR/XNOR implementada na topologia iDDPL.

A Tabela 1 apresenta um compêndio do comportamento da métrica NSD sob influência dos fenômenos de variabilidade local, considerando todas as topologias discutidas. A tabela descreve os resultados de ambas as portas lógicas, avaliando medidas de dispersão (média, desvio padrão e coeficiente de variação) e formato (assimetria e curtose) das distribuições. O coeficiente de variação é definido pela divisão do desvio padrão pela média e mede a variação relativa dos dados, permitindo uma comparação mais justa entre as variabilidades de diferentes conjuntos. A assimetria, por sua vez, representa o grau e o sentido do afastamento da simetria, indicando em qual extremo da distribuição as observações estão mais concentradas. Valores próximos de zero denotam uma distribuição simétrica, enquanto valores abaixo ou acima de zero caracterizam uma distribuição com uma cauda mais longa à esquerda ou direita, respectivamente. Por fim, a curtose determina o grau de achatamento da distribuição. Tal distinção é realizada comparando o coeficiente de curtose com o valor de referência, 3, o qual define a distribuição como mesocúrtica, sugerindo que a concentração dos dados ocorre de forma semelhante à da distribuição normal. Valores abaixo ou acima de 3 classificam a distribuição como platicúrtica ou leptocúrtica, respectivamente, indicando uma curva mais achatada ou alongada.

Analisando a tabela, verifica-se que, independente da porta lógica ou estágio de processamento investigado, a classe das topologias mais seguras (SABL e iDDPL) mostrou-se mais suscetível ao impacto causado pelos efeitos de variabilidade, demonstrando um grau de dispersão em relação à média substancialmente mais elevado. Ademais, os coeficientes de assimetria e curtose corroboram o formato das distribuições, no qual as contramedidas do grupo menos resistente (WDDL, PCSL e

Tabela 1 – Medidas descritivas da distribuição da métrica NSD para todas as topologias analisadas, ponderando os efeitos de variabilidade local.

Porta Lógica	Fase de Processamento	Medida (u. a.)	SABL	iDDPL	WDDL	PCSL	DPPL
AND/ NAND	*Avaliação*	*Nominal*	0,10	0,74	2,65	1,94	6,37
		μ	0,17	0,75	2,65	1,95	6,37
		σ	0,09	0,08	0,10	0,09	0,35
		$CV(\%)$	54,93	10,66	3,90	4,68	5,54
		As	1,06	0,83	0	0,06	0,01
		K	3,70	4,00	3,21	2,95	2,98
	Pré-Carga	*Nominal*	0,43	0,64	7,04	3,99	3,22
		μ	0,51	0,65	7,03	4,01	3,21
		σ	0,20	0,06	0,41	0,52	0,36
		$CV(\%)$	39,27	9,66	5,89	13,08	11,39
		As	0,60	0,61	0	0,21	0,04
		K	3,43	3,56	2,97	2,97	3,02
XOR/ XNOR	*Avaliação*	*Nominal*	0	0	1,31	5,01	3,39
		μ	0,15	0,14	1,32	5,00	3,40
		σ	0,11	0,11	0,18	0,18	0,19
		$CV(\%)$	72,62	71,36	13,28	3,55	5,73
		As	0,98	1,13	-0,06	0,10	0,08
		K	3,79	4,42	3,10	2,86	2,88
	Pré-Carga	*Nominal*	0	0	1,27	2,59	3,85
		μ	0,38	0,14	1,28	2,63	3,86
		σ	0,18	0,09	0,19	0,41	0,28
		$CV(\%)$	46,72	71,12	15,28	15,40	7,19
		As	0,74	1,17	0,06	-0,03	-0,11
		K	3,62	4,33	3,00	2,93	2,94

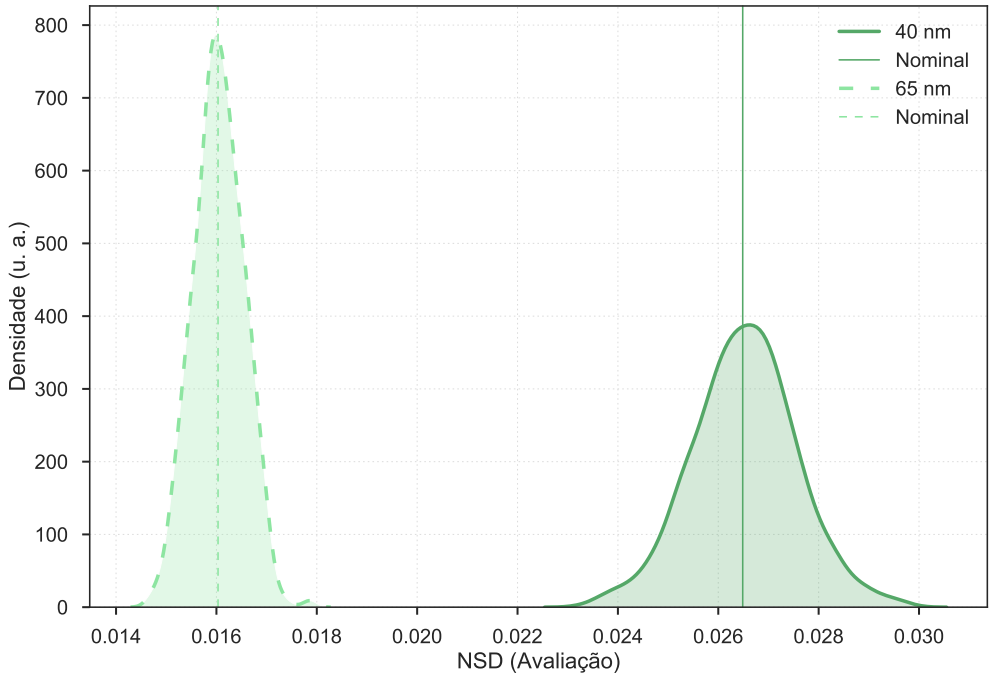
Nota: Para melhor visualização dos dados, as medidas de dispersão foram multiplicados por um fator de 100.
μ = média; σ = desvio padrão; CV = coeficiente de variação; As = coeficiente de assimetria e K = coeficiente de curtose.

DPPL) apresentam um comportamento gaussiano, enquanto as demais foram definidas como leptocúrticas e assimétricas positivas, indicando uma cauda mais alongada, com alta concentração de valores tendendo ao extremo direito da distribuição.

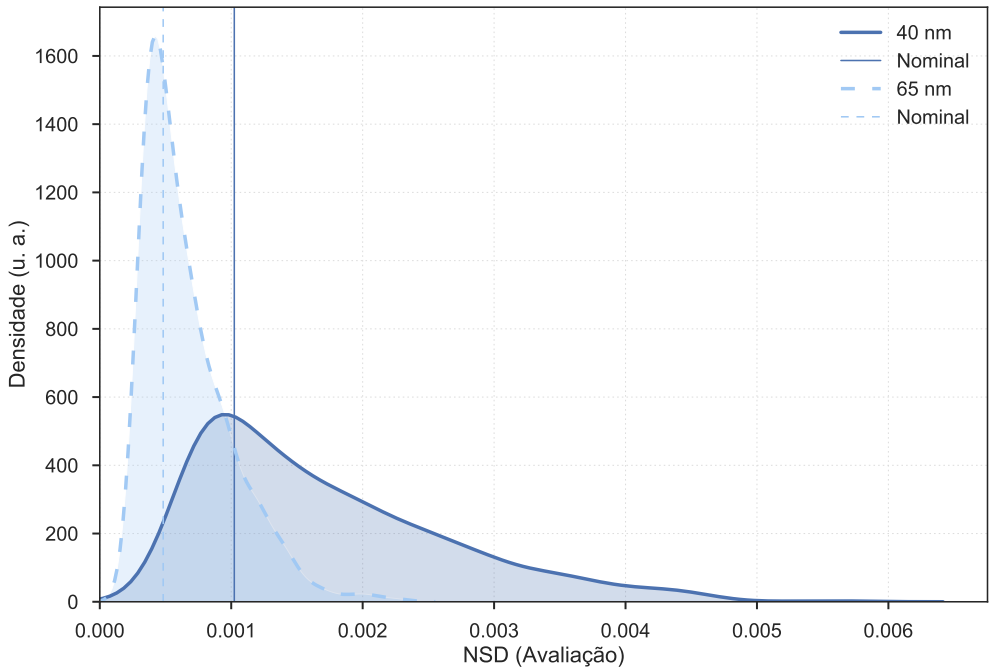
5.1.2 Comparação entre Nodos Tecnológicos

Com o intuito de demonstrar o aumento do impacto da variabilidade associado à miniaturização das dimensões dos transistores, as simulações também foram realizadas adotando o nodo tecnológico de 65 nm. As próximas figuras apresentam comparações das distribuições da métrica NSD para ambos os processos utilizados neste trabalho: 40 nm e 65 nm. As distribuições são visualizadas baseando-se na estimativa de densidade por *kernel* (em inglês, *Kernel Density Estimation* - KDE). KDE é uma técnica para estimar a função densidade de probabilidade de uma variável aleatória

e consiste em gerar uma distribuição empírica e suave a partir da posição singular de todos os pontos da amostra (WEGLARCZYK, 2018). Para isso, cada observação individual é substituída por uma função gaussiana centralizada no valor do dado e, então, somada com as demais para obter o valor da densidade, convergindo na curva de distribuição dos dados.



(a)



(b)

Figura 38 – Distribuição da densidade de probabilidade da métrica NSD para a porta AND/NAND, na fase de avaliação, considerando as topologias (a) WDDL e (b) SABL.

Reiterando o critério especificado anteriormente, duas topologias foram designadas para caracterizar o grupo dos estilos lógicos menos e mais seguros, respectivamente. A Figura 38 apresenta as KDEs para a porta AND/NAND, durante o estágio de avaliação, analisando os fenômenos locais. As curvas traçadas com uma linha contínua denotam o nodo de 40 nm, enquanto os contornos delineados pela linha tracejada representam o nodo de 65 nm. As linhas verticais, por sua vez, caracterizam o valor nominal da métrica para cada caso. A Figura 38 (a) ilustra as distribuições da topologia WDDL, considerando o grupo das contramedidas menos robustas. À parte de produzir um valor nominal consideravelmente mais elevado, a distribuição de NSD para o nodo de 40 nm apresenta um grau de dispersão superior, tendo em vista a curva mais achatada, a qual denota maior influência dos efeitos de variabilidade. Por outro lado, as KDEs geradas para a topologia SABL são ilustrados na Figura 38 (b). Independentemente da relativa proximidade entre os valores nominais, a distribuição de NSD associada ao nodo de 40 nm apresenta uma cauda notavelmente mais inclinada para o lado direito, em direção aos valores mais críticos da métrica. Consequentemente, o padrão exposto pelas distribuições demonstra como o aumento da variabilidade relacionado à diminuição da tecnologia CMOS se propaga para as métricas de segurança, culminando na limitação da eficiência das contramedidas aos ataques DPA.

A distribuição de NSD para a porta XOR/XNOR implementada nas topologias (a) PCSL e (b) iDDPL está exposta na Figura 39. Observando as curvas de distribuição, nota-se o mesmo comportamento constatado acima, com a topologia menos segura (PCSL) demonstrando maior impacto decorrente da variabilidade do nodo tecnológico menor, tendo em vista os dados mais espaçados. Para o estilo lógico mais resistente (iDDPL), a cauda mais longa em direção à extremidade direita, exibida para o processo de 40 nm, reforça a premissa de que a miniaturização das dimensões está associada a uma maior influência dos fatores de variabilidade.

5.1.3 Impacto no Desempenho dos Circuitos

O foco deste trabalho fundamenta-se na investigação do impacto dos fatores de variabilidade no nível de proteção fornecido por topologias de contramedidas de ocultação. Entrementes, também realizou-se a análise da influência desses efeitos no desempenho das portas lógicas. A Figura 40 apresenta a relação entre o atraso de propagação máximo e o consumo de energia médio para todas as topologias investigadas, avaliando os dados obtidos para cada uma das 1000 simulações MC. As Figuras 40 (a) e (b) exibem os resultados para a porta AND/NAND, considerando os efeitos de variabilidade local e global, respectivamente, enquanto as Figuras 40 (c) e (d) ilustram o comportamento da porta XOR/XNOR. Para cada ponto no gráfico, a posição nos eixos horizontal e vertical caracteriza a associação do tempo de atraso com o valor de potência medido. Assim, pontos mais próximos do início dos eixos

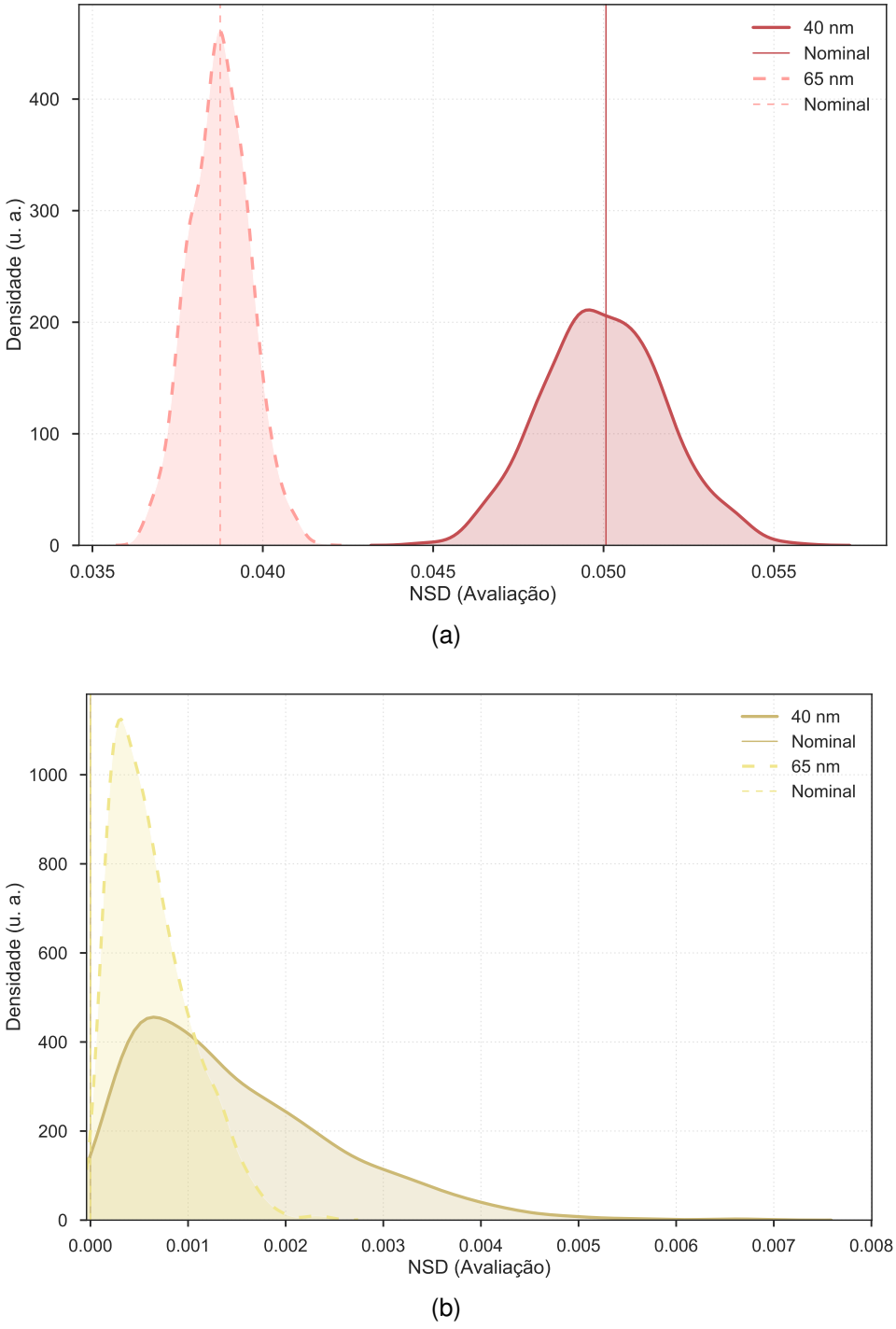


Figura 39 – Distribuição da densidade de probabilidade da métrica NSD para a porta XOR/XNOR, na fase de avaliação, considerando as topologias (a) WDDL e (b) iDDPL.

denotam um circuito com desempenho mais desejável. Salienta-se que a origem das coordenadas não é representada nos diagramas, com o intuito de apresentar uma melhor visualização dos resultados. De acordo com os gráficos, observa-se que o efeito causado pelos distintos fatores espaciais de variabilidade é relativamente semelhante, com os fenômenos globais demonstrando um grau levemente maior de dispersão no desempenho dos circuitos, especialmente para a porta XOR/XNOR. Considerando as

topologias mais seguras, nota-se que, em contrapartida à robustez observada nas métricas de segurança, está implicado o custo de elevado impacto na performance, tendo em vista o alto consumo de energia da topologia iDDPL e a ampla variação nos valores de SABL.

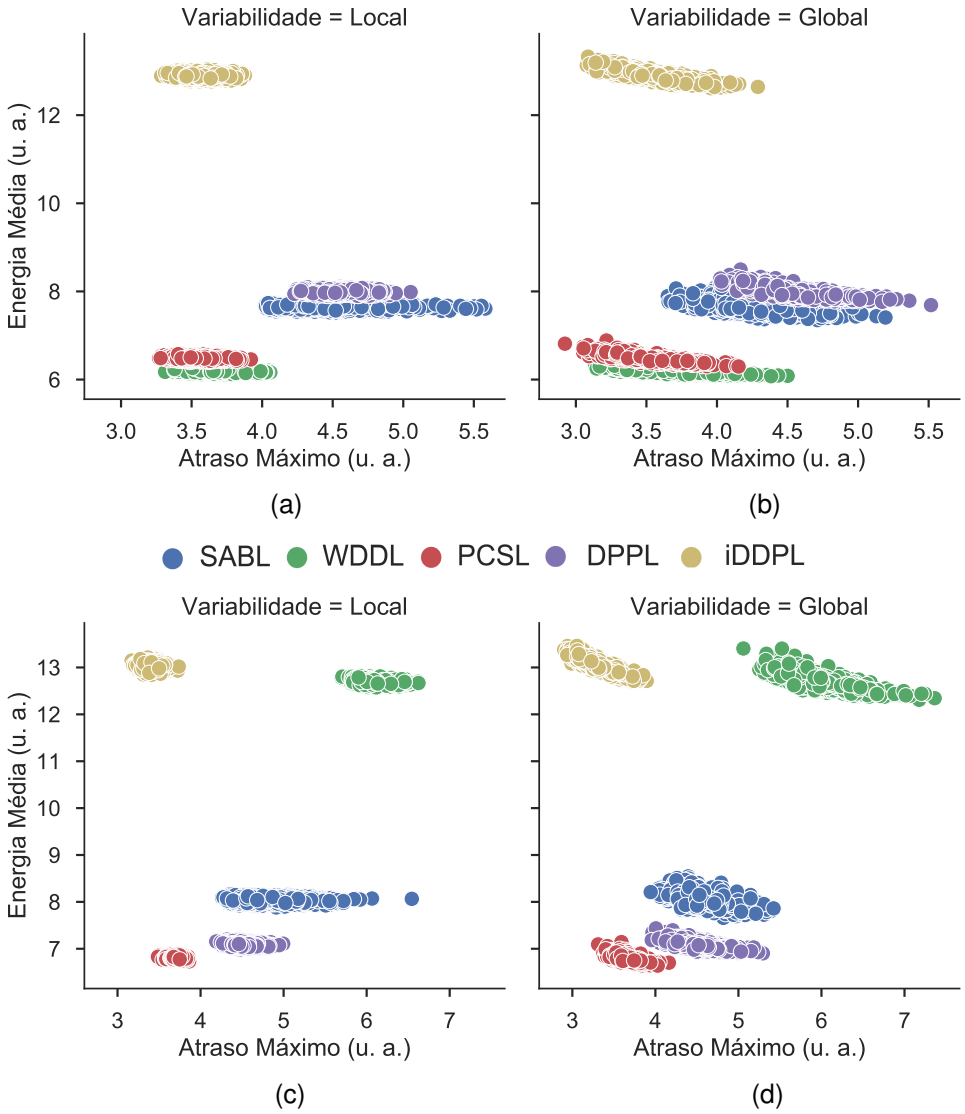


Figura 40 – Diagrama de dispersão da relação potência-atraso para a porta AND/NAND, considerando todas as topologias e efeitos de variabilidade (a) local e (b) global, e para a porta XOR/XNOR, ponderando fatores (c) locais e (d) globais.

Devido ao grande volume de dados, e visando uma apresentação mais coesa e inteligível dos resultados, optou-se por condensá-los conforme visualizado ao longo desta seção, priorizando as topologias mais representativas. Não obstante, uma parcela maior dos resultados específicos de cada porta e topologia está exposta no Apêndice C deste trabalho.

5.2 *Bias Temperature Instability*

Nesta seção, são apresentados os resultados obtidos para as 1000 simulações Monte Carlo de cada topologia, considerando o impacto do fenômeno de envelhecimento BTI nas métricas de segurança. Inicialmente, os resultados são relatados considerando a porta lógica AND/NAND. Apesar das simulações terem sido validadas por meio da inspeção do comportamento lógico dos circuitos analisados, os dados obtidos para a célula AND/NAND implementada na topologia DPPL mostraram-se inconsistentes e, portanto, acabaram por serem descartados da análise e discussão neste momento.

A Figura 41 apresenta o gráfico de dispersão das métricas NSD e NED para a porta lógica AND/NAND, exibindo a relação dos resultados entre os dois estágios de processamento do circuito. Os pontos representados pelo marcador 'X' expressam o valor nominal das métricas extraídas para cada topologia. Este valor nominal descreve o resultado obtido para a métrica a partir de uma simulação determinística e sob condições típicas de operação, ou seja, desconsiderando os efeitos de BTI. Avaliando a distribuição dos dados, é possível observar que o impacto do fenômeno BTI na dispersão dos resultados é relativamente diminuto, tendo em vista a coesão demonstrada pelos pontos. Não obstante, nota-se que a variação é ampliada para os estilos lógicos com valores mais elevados de métricas, em particular para a etapa de avaliação.

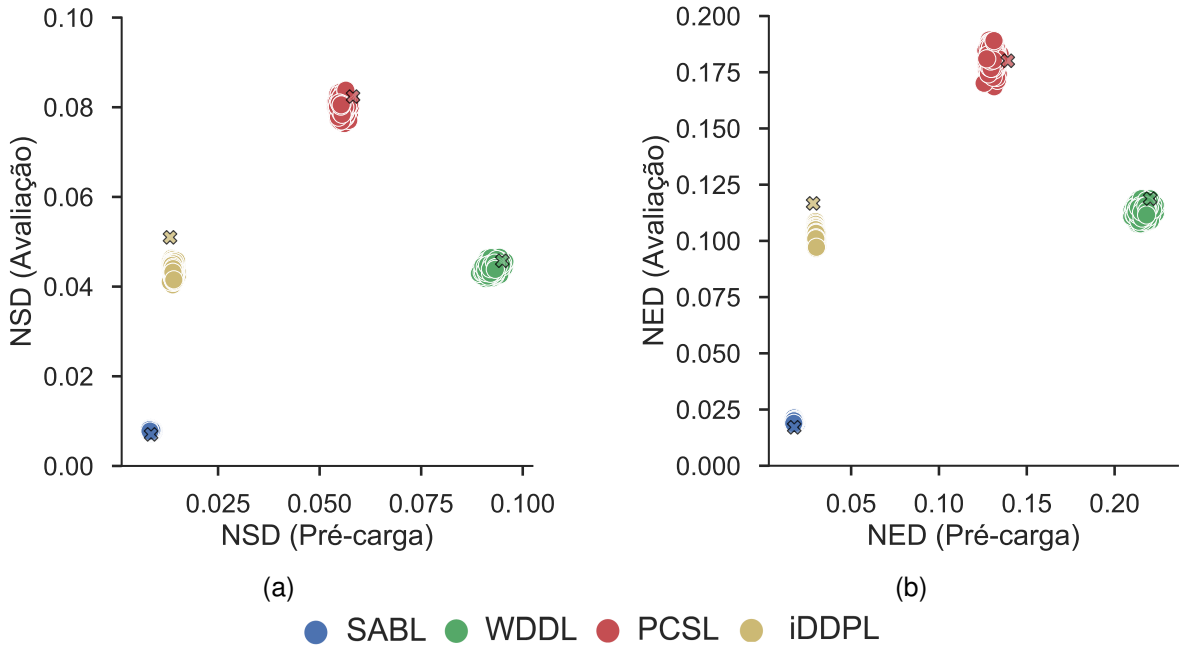


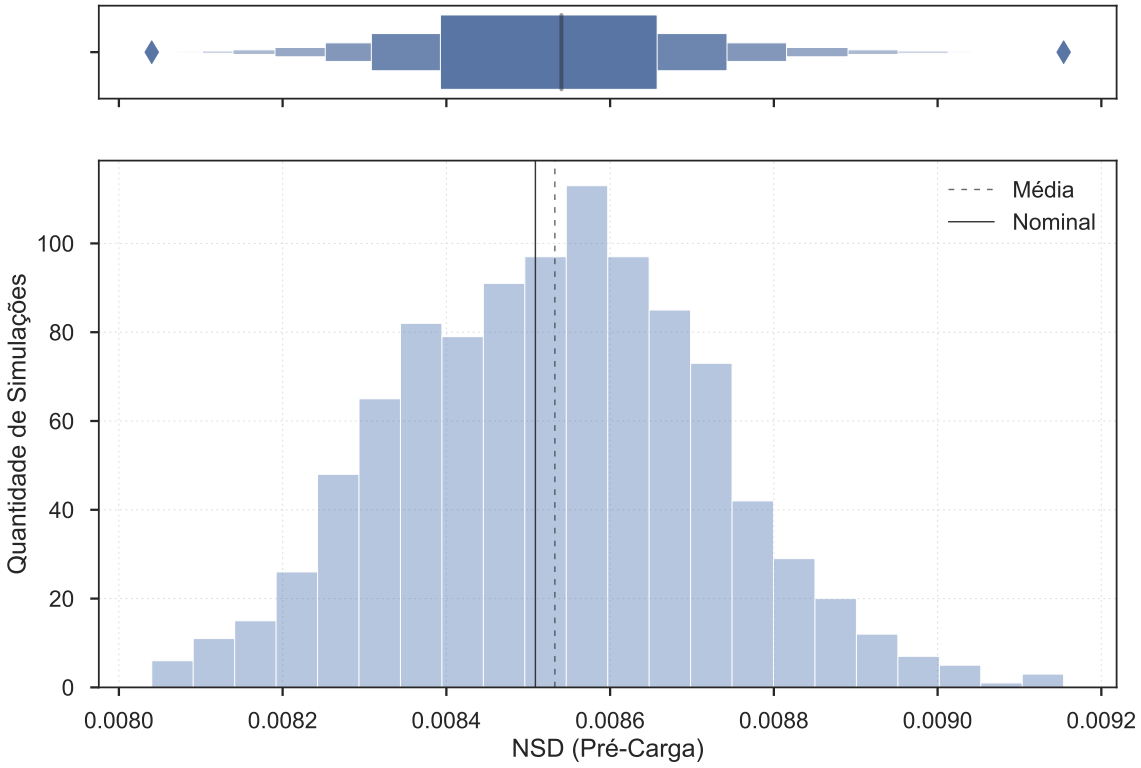
Figura 41 – Gráfico de dispersão para as 1000 simulações MC, avaliando as métricas NSD (a) e NED (b) para a porta AND/NAND, durante as fases de pré-carga e avaliação.

Ainda na Figura 41, considerando o comportamento das topologias em relação aos valores nominais das métricas, verifica-se que a degradação decorrente do efeito BTI

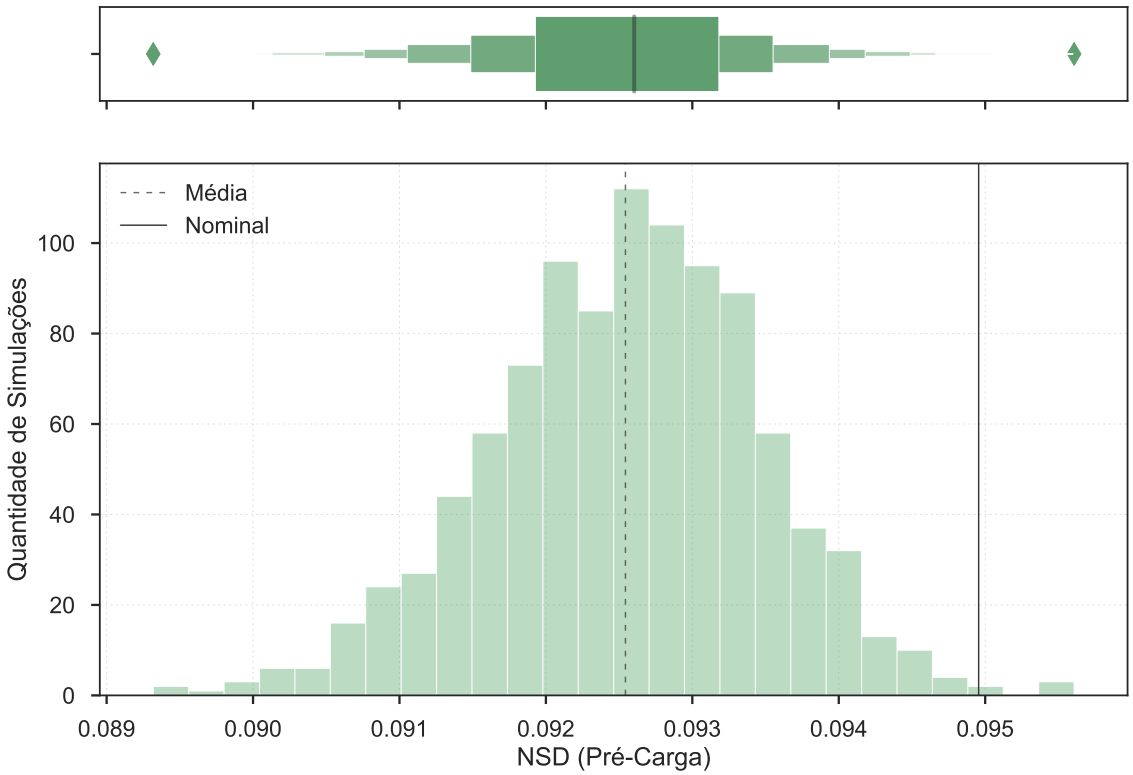
se propaga de maneira desigual na segurança dos circuitos. De acordo com os gráficos, observa-se que as distribuições se encontram bastante próximas aos resultados nominais, sugerindo que as métricas de segurança associadas as contramedidas não são significativamente afetadas pelo fenômeno. Além disso, é possível identificar topologias que apresentam a ampla maioria dos dados abaixo dos valores nominais, indicando que nestes cenários o efeito BTI pode ser vantajoso em termos de segurança. Embora essa atuação benéfica aparente ser contra-intuitiva, ponderando o desgaste que o fenômeno ocasiona nos transistores, a investigação da distribuição da energia dos arcos das topologias auxilia a compreender como o efeito atua nas métricas avaliadas. Ademais, como os dados das topologias expressam a mesma tendência de dispersão entre ambas as métricas, as análises a seguir focam nos valores obtidos para a métrica NSD, salientando que os resultados de NED são proporcionais.

Para melhor elucidar o comportamento divergente das contramedidas sob o efeito de BTI, as figuras a seguir exibem a distribuição de frequência das topologias SABL e WDDL, considerando os diferentes estágios de operação. Em cada gráfico, a linha tracejada caracteriza o valor médio da distribuição, enquanto a linha contínua define o valor nominal de NSD. O histograma da topologia SABL, para a fase de pré-carga, é ilustrado na Figura 42 (a). Apesar da métrica nominal estar bastante próxima do valor médio, o qual coincide com a mediana da distribuição, a topologia apresenta um formato levemente assimétrico, possuindo uma cauda maior em direção aos valores mais extremos da métrica. Dessa forma, embora os dados se dividam proporcionalmente à direita e à esquerda do valor médio, os resultados acima da métrica nominal são dispostos em um intervalo substancialmente maior, indicando que o efeito BTI pode produzir valores críticos de baixa segurança. Esse comportamento condiz com a natureza exponencial do impacto das armadilhas. Porém, por tratar-se de um circuito de alta complexidade, tais ocorrências são raras e de baixa significância estatística. Por outro lado, a Figura 42 (b) ilustra o histograma da topologia WDDL para a fase de pré-carga. Novamente, é possível observar como os valores de mediana e média se equivalem. Entretanto, em contraste à topologia SABL, a distribuição para WDDL exibe uma cauda maior em direção aos valores mais baixos da métrica. Além disso, destaca-se que a ampla maioria das observações se encontra abaixo do valor nominal, demonstrando que o efeito BTI pode ser benéfico para a segurança desta topologia.

Os histogramas das topologias SABL e WDDL, obtidos para a fase de avaliação, são exibidos nas Figuras 43 (a) e (b), respectivamente. De acordo com os gráficos, é possível observar que o estilo lógico WDDL manteve o mesmo comportamento verificado para o estágio de pré-carga. Entretanto, para a topologia SABL, nota-se que a degradação decorrente do efeito BTI, durante a etapa de avaliação, resulta no agravamento da redução da segurança, considerando que todas as observações encontram-se acima do valor nominal de NSD.

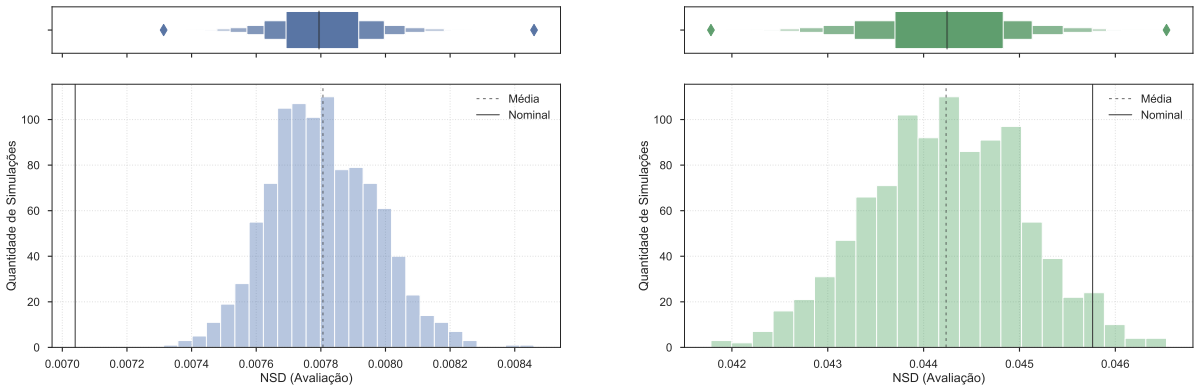


(a)



(b)

Figura 42 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica AND/NAND implementada nas topologias (a) SABL e (b) WDDL.

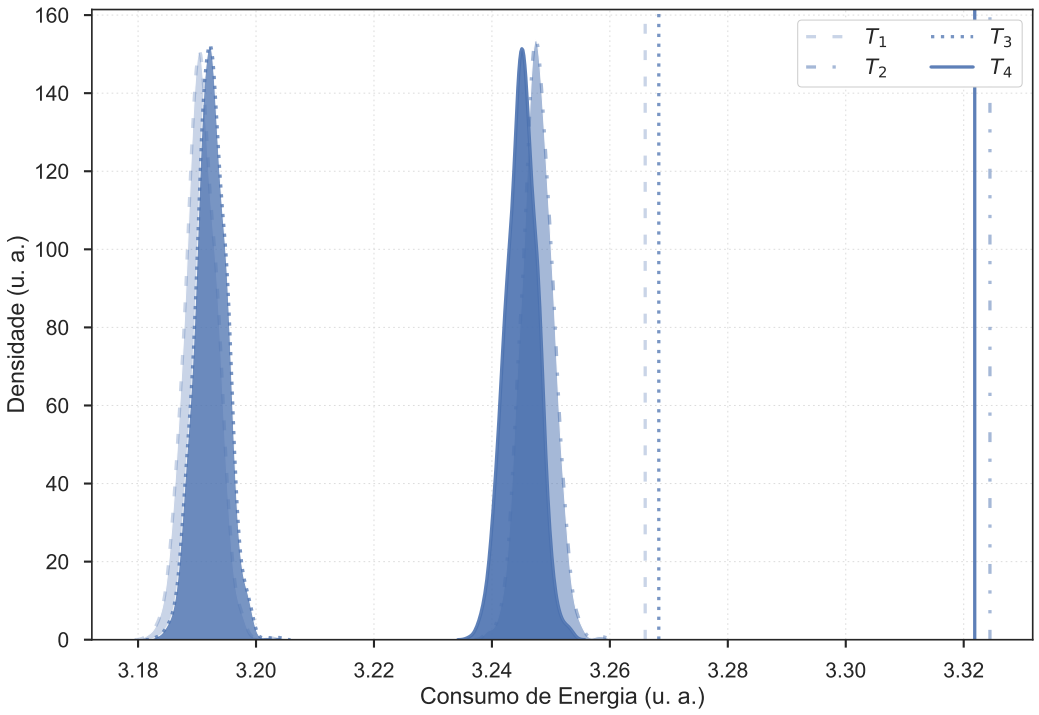


(a) (b)

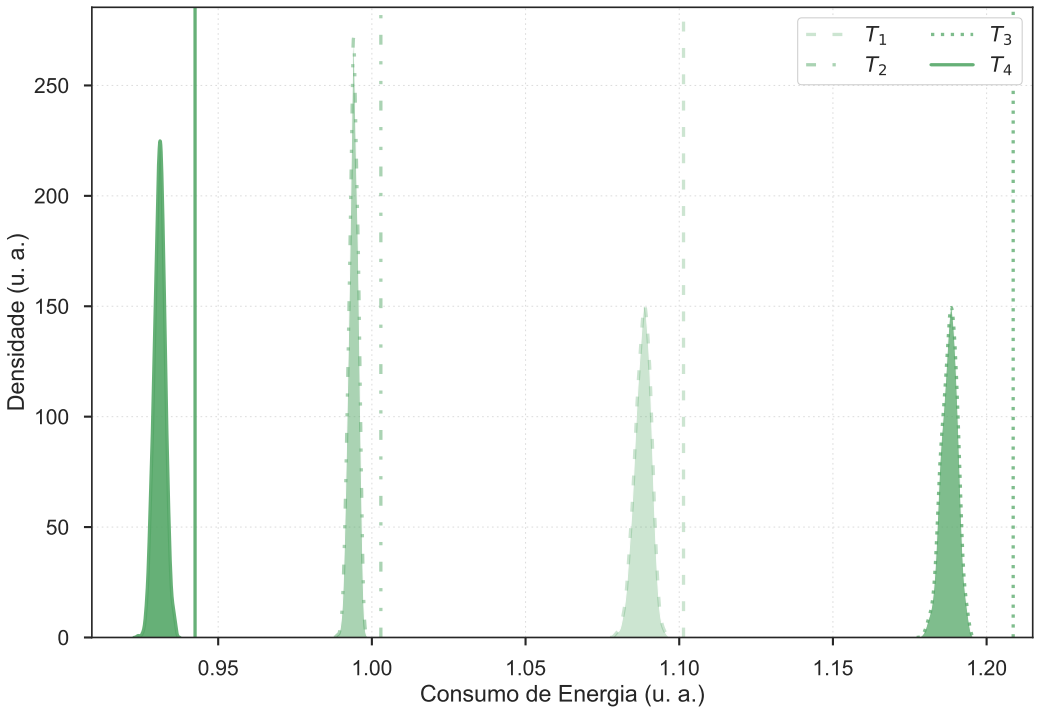
Figura 43 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica AND/NAND implementada nas topologias (a) SABL e (b) WDDL.

O comportamento exibido pelas distribuições acima pode ser parcialmente justificado, analisando-se a variação da energia em cada arco de transição. Conforme supracitado, os arcos de transição expressam as possíveis alterações de estado na saída do circuito. A Figura 44 ilustra o consumo de energia observado nas transições das respectivas topologias apresentadas na Figura 42, considerando a etapa de pré-carga. As linhas verticais expressam o valor nominal do consumo de energia medido para arco de transição. Examinado as distribuições para a topologia SABL, expostas na Figura 44 (a), nota-se a ocorrência de sobreposição entre as curvas de energia e um elevado distanciamento destas em relação aos seus respectivos valores nominais. Assim, embora as transições apresentem um grau de variação bastante similar, a diminuição do valores de energia para cada arco acarreta no decréscimo do valor médio de consumo e, consequentemente, no potencial aumento do resultado da métrica NSD. Por outro lado, a distribuição da energia extraída para os arcos da contramedida WDDL é demonstrada na Figura 44 (b). Em contraste à topologia SABL, as curvas de energia para a WDDL são dispostas de maneira afastada entre si, mas extremamente próximas aos seus respectivos valores nominais. Ademais, o gráfico permite observar que os arcos de consumo energético mais elevado (T_3 e T_1) obtiveram uma redução no valor consideravelmente maior que os demais (T_2 e T_4), resultando no impacto positivo verificado para a métrica NSD.

Os dados obtidos para a porta lógica XOR/XNOR apontam características semelhantes às expostas para a célula AND/NAND, com as topologias demonstrando um nível moderadamente mais elevado de variação nos pontos, conforme pode ser observado na Figura 45. Complementarmente, a distribuição das topologias em relação aos valores nominais reafirma a influência heterogênea do fenômeno BTI nas métricas de segurança. Com exceção do estilo lógico SABL, cujo valor nominal calculado é zero e, por definição, a dispersão exibida pelas métricas é apenas prejudicial; o impacto



(a)



(b)

Figura 44 – Distribuição da densidade de probabilidade do consumo de energia observado para as transições da porta lógica AND/NAND implementada nas topologias (a) SABL e (b) WDDL durante a etapa de pré-carga.

do efeito BTI propagou-se de maneira inconstante entre as topologias, apresentando cenários tanto positivos quanto negativos para a segurança das contramedidas.

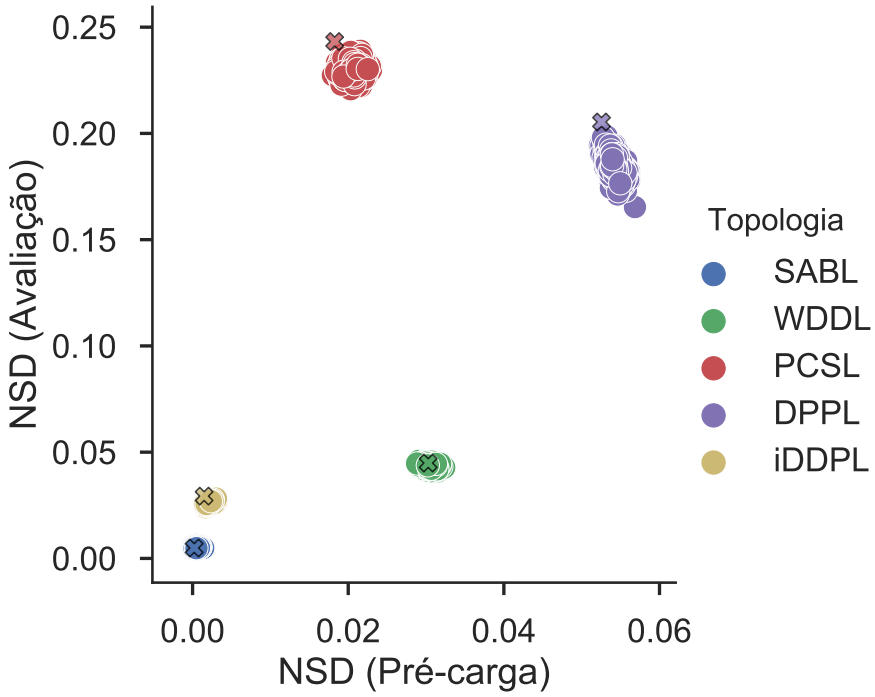


Figura 45 – Gráfico de dispersão para as 1000 simulações MC, avaliando a métrica NSD para a porta XOR/XNOR, durante as fases de pré-carga e avaliação.

A investigação particular das topologias corrobora o caráter ambíguo do impacto do fenômeno BTI nas métricas de segurança. As Figuras 46 (a) e (b) apresentam a distribuições de frequência da métrica NSD obtidas para a topologia PCSL, durante as fases de pré-carga e avaliação, respectivamente. Embora ambas as distribuições exibam uma formato simétrico em torno do valor mediano, a disposição das curvas em relação ao valor nominal se apresenta de maneira completamente oposta. Enquanto os dados de pré-carga estão agrupados acima do valor nominal, os resultados da etapa de avaliação se concentram inteiramente abaixo deste. Esse comportamento ressalta que o efeito BTI pode causar um impacto negativo na correlação dos dados com a potência do dispositivo, atuando de forma benéfica para a segurança do circuito integrado.

O comportamento irregular manifestado pela topologia PCSL é replicado na análise da porta XOR/XNOR implementada para a topologia iDDPL, conforme pode ser visualizado nas Figuras 47 (a) e (b). Apesar da topologia iDDPL exibir valores notavelmente menores e uma distribuição assimétrica positiva para a fase de pré-carga, contrastando com o formato gaussiano exposto pela topologia PCSL, ambas as contramedidas apresentam a mesma divergência acerca dos resultados nominais das métricas entre os diferentes estágios de operação. Semelhantemente ao estilo lógico PCSL, durante a fase de avaliação da topologia iDDPL observa-se uma tendência ao

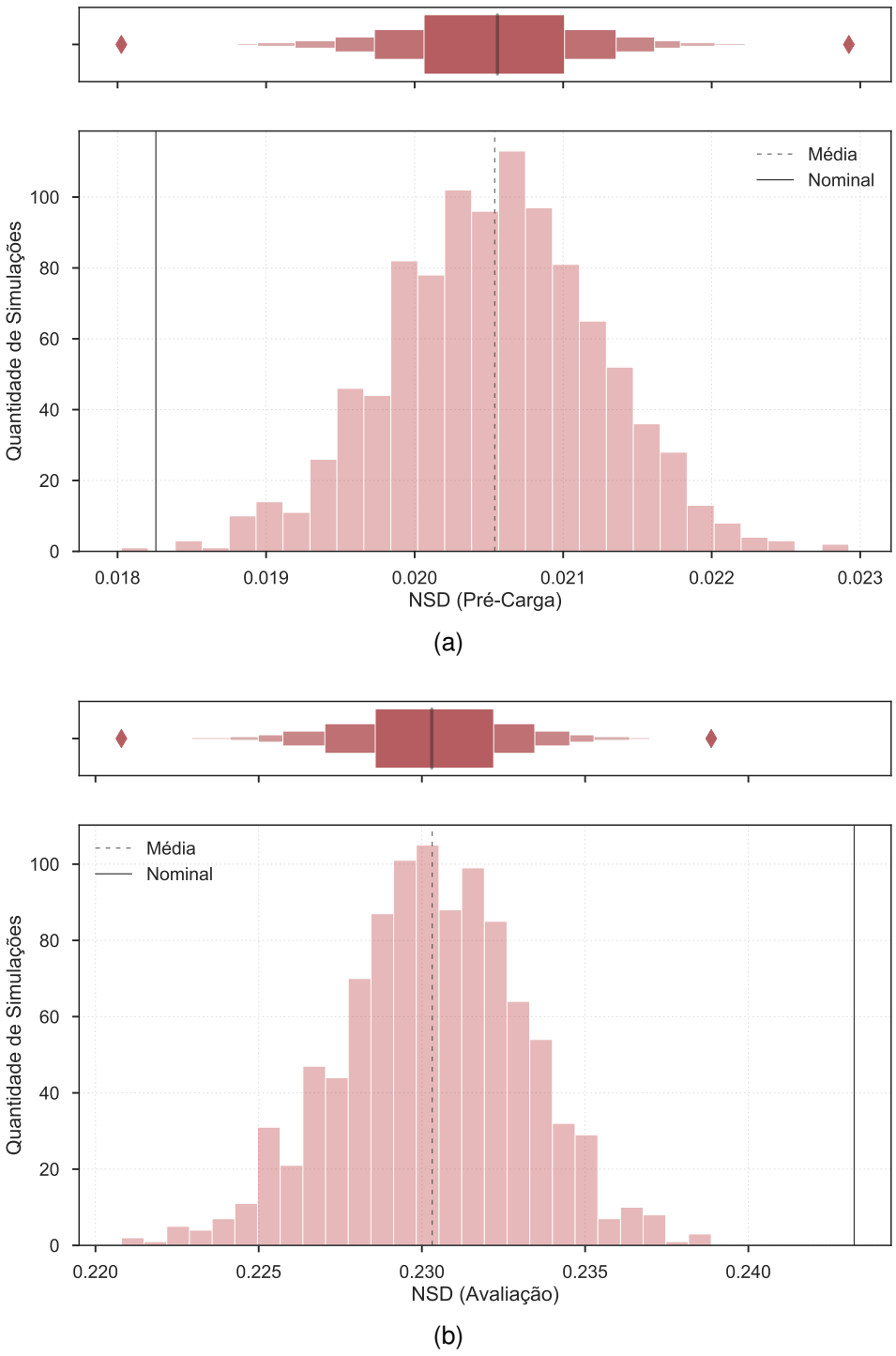


Figura 46 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica XOR/XNOR implementada na topologia PCSL, durante as fases de (a) pré-carga e (b) avaliação.

aumento da segurança decorrente do efeito BTI. Essa característica demonstra que mesmo para os circuitos implementados nas topologias mais seguras, a consequência do fenômeno BTI pode ser vantajosa em termos de segurança. Embora assuma-se que tais circuitos apresentariam uma maior vulnerabilidade ao efeito, considerando a alta uniformidade presente nos arcos e, por conseguinte, o maior potencial de re-

sultar em desequilíbrio; a análise dos dados contrapôs parcialmente essa hipótese. O comportamento observado nos resultados pode ser atribuído à estrutura extremamente balanceada destas células, a qual faz com que todos os arcos degradem-se de maneira similar.

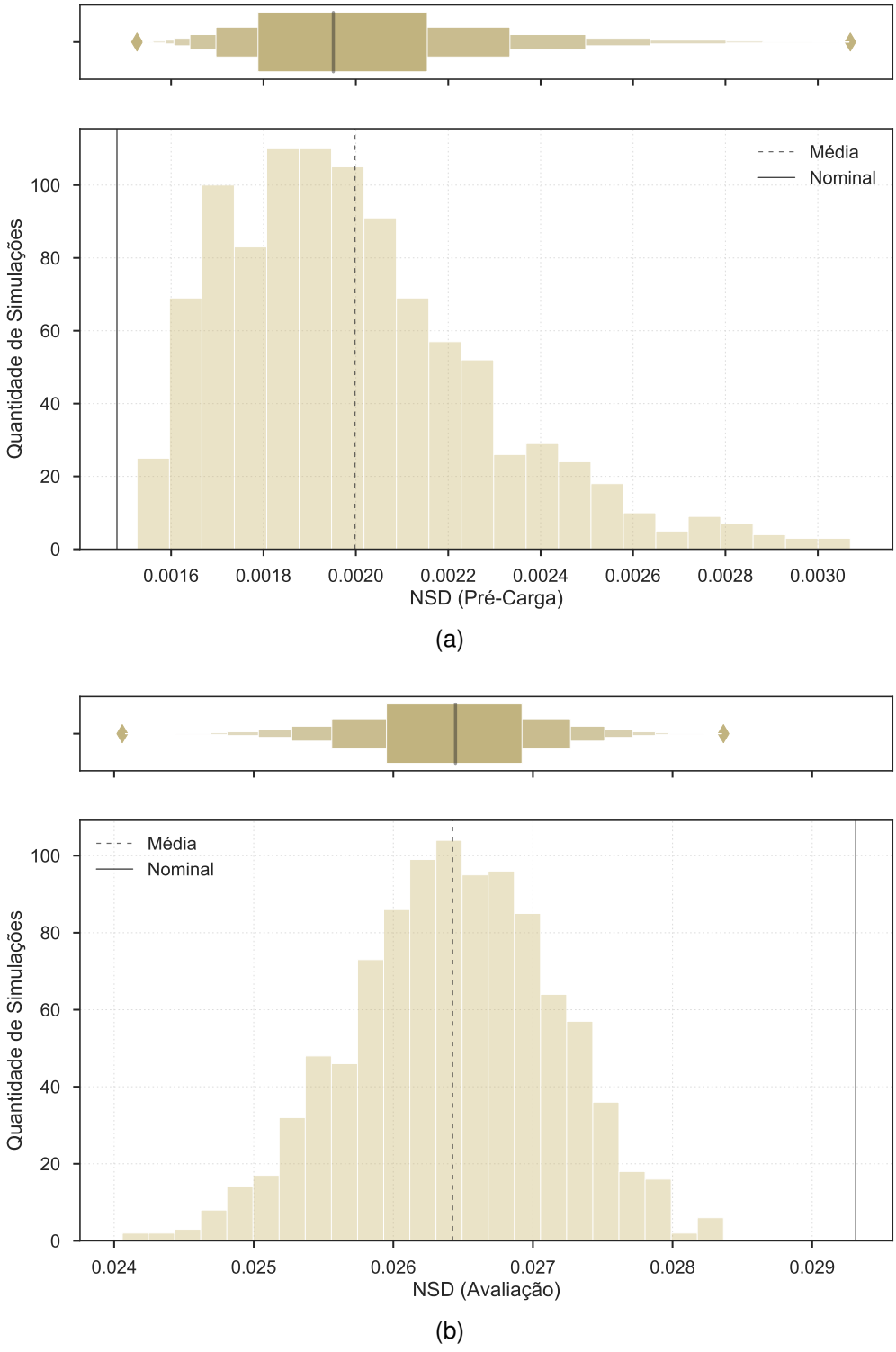


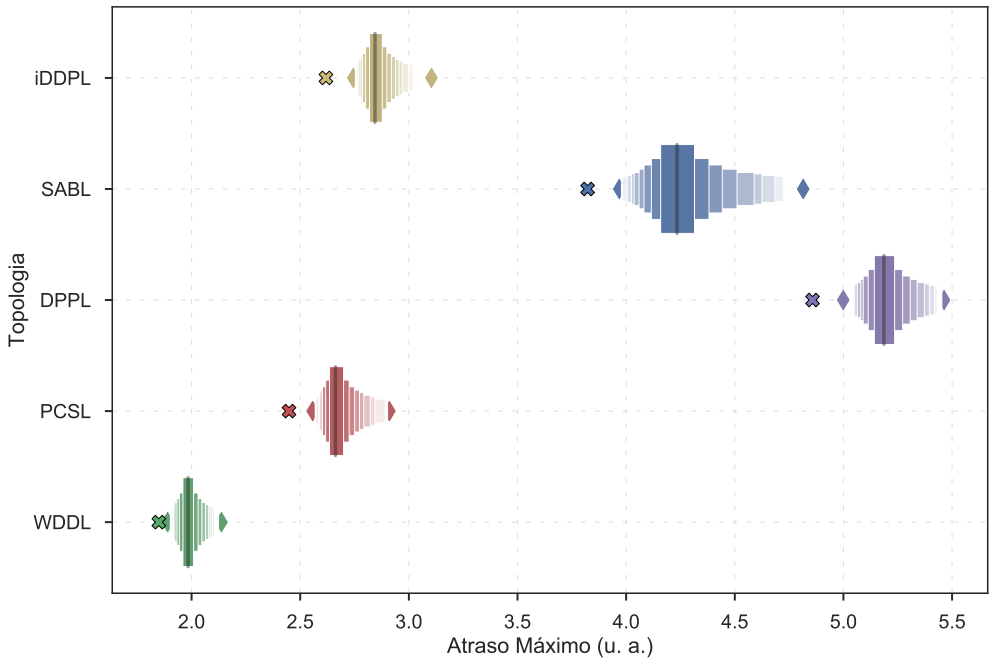
Figura 47 – Distribuição de frequência para as 1000 observações de NSD obtidas para a porta lógica XOR/XNOR implementada na topologia iDDPL, durante as fases de (a) pré-carga e (b) avaliação.

A alta heterogeneidade observada nos resultados inviabiliza uma inferência mais abrangente acerca do impacto do efeito BTI na proteção apresentada pelas contramedidas. A análise dos dados enfatiza as alterações exibidas no comportamento elétrico dos circuitos, resultantes da degradação dos transistores pelo fenômeno. Entretanto, a irregularidade das alterações propagadas na potência dos arcos permite que as métricas tanto se aproximem quanto se afastem das condições nominais. Assim, embora tenha-se evidenciado que o efeito BTI afeta a segurança das topologias, a consequência decorrente do fenômeno não implica, necessariamente, em perda de segurança, conforme demonstrado pelos cenários em que os valores da métricas diminuem. Ademais, devido à estrutura complexa das portas analisadas, associada à forte dependência do efeito ao ciclo de trabalho, torna-se inexequível determinar como o fenômeno influenciará o resultado das métricas de segurança.

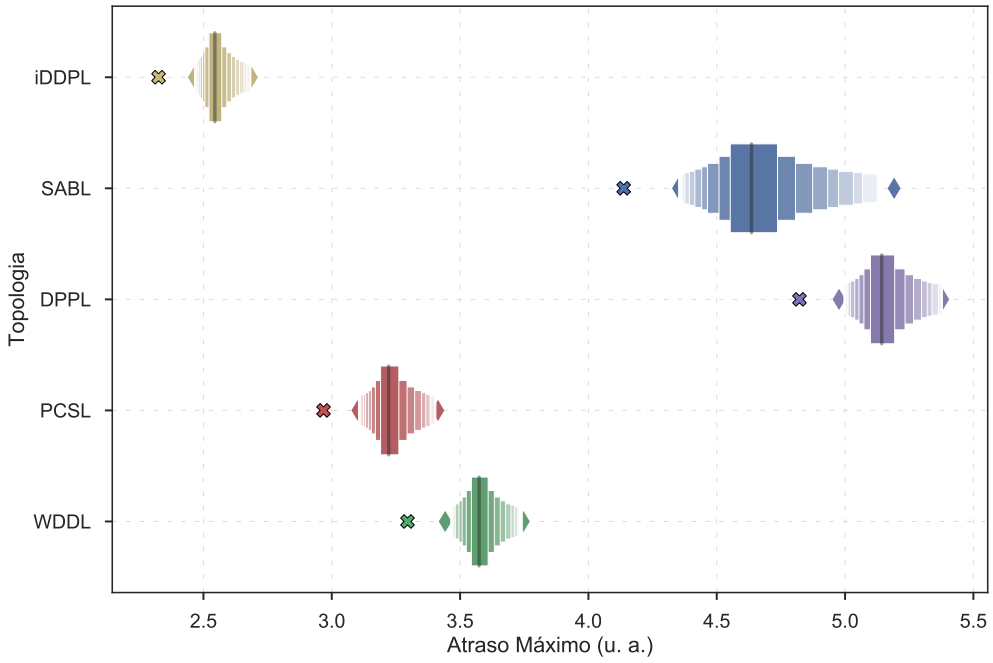
De forma análoga à seção anterior, priorizou-se a apresentação de uma parcela mais significativa dos resultados para a análise do efeito BTI. Entretanto, os dados específicos obtidos para cada porta e topologia podem ser visualizados no Apêndice D deste trabalho.

5.2.1 Impacto no Atraso de Propagação dos Circuitos

Conforme supracitado, o propósito deste trabalho consiste na investigação do impacto de fatores de confiabilidade no nível de proteção fornecido pelas topologias de contramedidas. Entretanto, de maneira análoga à análise de variabilidade de processo, também verificou-se a influência do efeito BTI no desempenho dos circuitos, considerando o atraso de propagação das portas lógicas. As Figuras 48 (a) e (b) apresentam os gráficos LV para as distribuições do atraso de propagação máximo extraído para as portas AND/NAND e XOR/XNOR, respectivamente. Os pontos simbolizados pelo marcador ‘X’ representam o valor do atraso de propagação nominal observado para cada topologia. Analisando os gráficos, é possível observar que todas as topologias exibem suas distribuições à direita dos valores nominais, independentemente da célula examinada. Esse comportamento reflete a degradação causada pelo fenômeno BTI na tensão de limiar dos transistores, a qual, por sua vez, implica no aumento observado no atraso dos circuitos. Ademais, as distribuições das topologias exibem um formato assimétrico positivo, indicando a ocorrência de uma longa cauda em direção aos valores mais extremos de atraso.



(a) AND/NAND



(b) XOR/XNOR

Figura 48 – Distribuição do atraso de propagação máximo extraído para todas as topologias implementadas nas portas lógicas (a) AND/NAND e (b) XOR/XNOR.

6 CONCLUSÃO

Ataques por canais laterais que monitoram a dissipação de potência ou a emissão eletromagnética emitida por um circuito representam uma severa ameaça à segurança de sistemas criptográficos, devido à dependência inerente dos dados a tais propriedades elétricas. Com o intuito de impedir a exploração dessa relação, diferentes contramedidas são propostas para mitigar a ação dos ataques. Neste cenário, técnicas que propõem o projeto de circuitos que buscam a homogeneização do consumo de energia são consideradas as melhores alternativas à prevenção aos ataques DPA.

A despeito da maior segurança concedida pelas contramedidas, os circuitos que as implementam baseiam-se em propriedades que estão suscetíveis a variações, as quais acarretam em alterações no comportamento dos CIs. Essas variações podem ser decorrentes de limitações do processo de fabricação e da natureza discreta da matéria ou, ainda, de fatores que emergem gradualmente ao longo da operação dos circuitos. Sob esse contexto, o objetivo desta dissertação consistiu na investigação da influência de fenômenos de variabilidade na proteção fornecida por técnicas de contramedidas de ocultação.

O desenvolvimento do trabalho dividiu-se, essencialmente, em dois estudos: análise da variabilidade de processo e análise dos efeitos temporais. Ambos os estudos fundamentaram-se em simulações elétricas e estatísticas, adotando os respectivos modelos de variabilidade. Complementarmente, em ambas as análises avaliou-se um conjunto de diferentes contramedidas implementadas ao nível de transistor, buscando abranger as variadas abordagens propostas para proteção aos ataques DPA. Para a variabilidade de processo, verificou-se a consequência oriunda de efeitos locais e globais na proteção das contramedidas mencionadas, a partir da análise de métricas de segurança. A respeito da variabilidade temporal, concentrou-se no impacto causado pelo efeito BTI.

A investigação da variabilidade de processo demonstrou que à medida que o nodo tecnológico diminui, e os fenômenos de variabilidade local assumem maior relevância, a variabilidade dos transistores aumenta, acarretando no maior desequilíbrio de potência observado entre os arcos de uma porta lógica e, consequentemente, na fabricação

de um circuito menos seguro. A variabilidade verificada nos transistores propagou-se para as métricas de segurança em todas as contramedidas estudadas, ressaltando que a variabilidade de processo deve ser considerada no projeto de um sistema seguro. Ademais, notou-se um impacto maior nas topologias mais seguras, as quais apresentaram uma distribuição com uma cauda pesada à direita, deslocando os resultados das métricas para valores substancialmente maiores que os esperados por uma simulação nominal, indicando que a variabilidade impõe um limite na segurança dessas contramedidas. Adicionalmente, a análise de *corners* revelou-se ineficaz na avaliação do impacto da variabilidade de processo na segurança dos circuitos, reforçando a necessidade do emprego de simulações estatísticas.

A análise acerca da influência do fenômeno BTI indicou que as métricas de segurança não manifestam grandes alterações no seu comportamento. Observou-se o efeito BTI apresenta-se de maneira divergente, exibindo casos em que a eficácia da contramedida foi comprometida, mas também situações nas quais os resultados mostraram-se aprimorados após a aplicação de uma condição de estresse. Dessa forma, em termos de segurança, o efeito de BTI não representou um problema que justifique dedicação adicional durante o projeto de um sistema, sendo significativamente menos relevante do que a variabilidade de processo. Entretanto, examinando o desempenho das portas lógicas do ponto de vista do atraso apresentado, concluiu-se que o impacto de BTI não pode ser negligenciado, devendo ser avaliado durante o projeto de circuitos seguros da mesma maneira que deve ser considerado no projeto de circuitos tradicionais.

Como trabalhos futuros, pretende-se expandir os estudos de variabilidade efetuados nesta dissertação, em portas lógicas, para módulos criptográficos que implementam o protocolo AES, permitindo, então, a realização de ataques a estes circuitos. Acerca do efeito BTI, propõe-se a aplicação do fenômeno como uma técnica de ataque, degradando o circuito de maneira não uniforme. Para isso, sugere-se investigar o desequilíbrio causado no consumo de energia, ao manter o circuito operando sob condições de estresse por um determinado período, continuadamente, mas para uma mesma entrada.

REFERÊNCIAS

AGARWAL, K.; NASSIF, S. Characterizing Process Variation in Nanometer CMOS. In: ANNUAL DESIGN AUTOMATION CONFERENCE, 44., 2007, New York, NY, USA. **Anais...** ACM, 2007. p.396–399. (DAC '07).

ALAM, M.; MAHAPATRA, S. A comprehensive model of PMOS NBTI degradation. **Microelectronics Reliability**, [S.l.], v.45, n.1, p.71 – 81, 2005.

ALIOTO, M. et al. Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations. **IEEE Transactions on Circuits and Systems I: Regular Papers**, [S.l.], v.61, n.2, p.429–442, 2014.

ASENOV, A.; KAYA, S.; BROWN, A. R. Intrinsic parameter fluctuations in decananometer MOSFETs introduced by gate line edge roughness. **IEEE Transactions on Electron Devices**, [S.l.], v.50, n.5, p.1254–1260, May 2003.

BANSAL, A.; RAO, R. M. Variations: Sources and Characterization. In: BHUNIA, S.; MUKHOPADHYAY, S. (Ed.). **Low-Power Variation-Tolerant Design in Nanometer Silicon**. Boston, MA: Springer US, 2011. p.3–39.

BARENGHI, A.; BREVEGLIERI, L.; KOREN, I.; NACCACHE, D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. **Proceedings of the IEEE**, [S.l.], v.100, n.11, p.3056–3076, Nov 2012.

BELLIZIA, D. et al. Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications. **IEEE Transactions on Emerging Topics in Computing**, [S.l.], v.5, n.3, p.329–339, July 2017.

BELLIZIA, D.; SCOTTI, G.; TRIFILETTI, A. TEL Logic Style as a Countermeasure Against Side-Channel Attacks: Secure Cells Library in 65nm CMOS and Experimental Results. **IEEE Transactions on Circuits and Systems I: Regular Papers**, [S.l.], v.65, n.11, p.3874–3884, Nov 2018.

BERNSTEIN, K. et al. High-performance CMOS variability in the 65-nm regime and beyond. **IBM Journal of Research and Development**, [S.l.], v.50, n.4.5, p.433–449, July 2006.

BHUSHAN, M.; KETCHEN, M. B. Variability. In: **CMOS Test and Evaluation**: A Physical Perspective. [S.l.]: Springer, 2015. p.201–239.

BNDES. **Relatório do Plano de Ação – Iniciativas e Projetos Mobilizadores**. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERESCVID=m0jDUok>. Acesso em: 17-04-2020.

BÖHM, C.; HOFER, M. Sources of Mismatch and Errors. In: PHYSICAL UNCLONABLE FUNCTIONS IN THEORY AND PRACTICE, 2013, New York, NY. **Anais...** Springer New York, 2013. p.105–130.

BONGIOVANNI, S.; CENTURELLI, F.; SCOTTI, G.; TRIFILETTI, A. Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks. **Journal of Cryptographic Engineering**, [S.l.], v.5, n.4, p.269–288, Nov 2015.

BOTH, T. H.; FURTADO, G. F.; WIRTH, G. I. Modeling and simulation of the charge trapping component of BTI and RTS. **Microelectronics Reliability**, [S.l.], v.80, p.278 – 283, 2018.

BROWN, A. R.; ROY, G.; ASENOV, A. Poly-Si-Gate-Related Variability in Decananometer MOSFETs With Conventional Architecture. **IEEE Transactions on Electron Devices**, [S.l.], v.54, n.11, p.3056–3063, Nov 2007.

BUCCI, M.; GIANCANE, L.; LUZZI, R.; TRIFILETTI, A. Three-Phase Dual-Rail Precharge Logic. In: CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2006, 2006, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2006. p.232–241.

BURLESON, W.; MUTLU, O.; TIWARI, M. Invited: Who is the major threat to tomorrow's security? You, the hardware designer. In: ACM/EDAC/IEEE DESIGN AUTOMATION CONFERENCE (DAC), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p.1–5.

CHAMPAC, V.; GARCIA GERVACIO, J. **Timing Performance of Nanometer Digital Circuits Under Process Variations**. Cham: Springer International Publishing, 2018. 1–17p.

CHEN, K.-L.; SALLER, S. A.; GROVES, I. A.; SCOTT, D. B. Reliability Effects on MOS Transistors Due to Hot-Carrier Injection. **IEEE Journal of Solid-State Circuits**, [S.l.], v.20, n.1, p.306–313, Feb 1985.

CHIANG, C.; KAWA, J. Variability Parametric Yield. In: **Design for Manufacturability and Yield for Nano-Scale CMOS**. [S.l.]: Springer, 2007. p.151–168.

CHONG, K. et al. Counteracting differential power analysis: Hiding encrypted data from circuit cells. In: IEEE INTERNATIONAL CONFERENCE ON ELECTRON DEVICES AND SOLID-STATE CIRCUITS (EDSSC), 2015., 2015. **Anais...** [S.l.: s.n.], 2015. p.297–300.

CISCO. **Cisco Annual Internet Report (2018–2023)**. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>. Acesso em: 17-04-2020.

CLAVIER, C.; CORON, J.-S.; DABBOUS, N. Differential Power Analysis in the Presence of Hardware Countermeasures. In: CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS — CHES 2000, 2000, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2000. p.252–263.

CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; STEIN, C. **Introduction to Algorithms, 3rd Edition**. [S.l.]: MIT Press", 2009. 1–1292p.

DADGOUR, H. F.; ENDO, K.; DE, V. K.; BANERJEE, K. Grain-Orientation Induced Work Function Variation in Nanoscale Metal-Gate Transistors—Part I: Modeling, Analysis, and Experimental Validation. **IEEE Transactions on Electron Devices**, [S.l.], v.57, n.10, p.2504–2514, Oct 2010.

DINU, D.; KIZHVATOV, I. EM Analysis in the IoT Context: Lessons Learned from an Attack on Thread. **IACR Transactions on Cryptographic Hardware and Embedded Systems**, [S.l.], v.2018, n.1, p.73–97, Feb. 2018.

FUJINO, T.; KUBOTA, T.; SHIOZAKI, M. Tamper-Resistant Cryptographic Hardware. **IEICE Electronics Express**, [S.l.], v.14, n.2, p.1–13, 2017.

GADLAGE, M. J. et al. Single event transient pulse widths in digital microcircuits. **IEEE Transactions on Nuclear Science**, [S.l.], v.51, n.6, p.3285–3290, Dec 2004.

GRASSER, T. et al. The Paradigm Shift in Understanding the Bias Temperature Instability: From Reaction–Diffusion to Switching Oxide Traps. **IEEE Transactions on Electron Devices**, [S.l.], v.58, n.11, p.3652–3666, 2011.

GRASSER, T. et al. A unified perspective of RTN and BTI. In: IEEE INTERNATIONAL RELIABILITY PHYSICS SYMPOSIUM, 2014., 2014. **Anais...** [S.l.: s.n.], 2014. p.4A.5.1–4A.5.7.

GUO, X. et al. Simulation and analysis of negative-bias temperature instability aging on power analysis attacks. In: IEEE INTERNATIONAL SYMPOSIUM ON HARDWARE ORIENTED SECURITY AND TRUST (HOST), 2015., 2015. **Anais...** [S.l.: s.n.], 2015. p.124–129.

HOFMANN, H.; WICKHAM, H.; KAFADAR, K. Letter-Value Plots: Boxplots for Large Data. **Journal of Computational and Graphical Statistics**, [S.l.], v.26, n.3, p.469–477, 2017.

JACOB, A. P. et al. Scaling Challenges for Advanced CMOS Devices. **International Journal of High Speed Electronics and Systems**, [S.l.], v.26, n.01n02, p.1740001, 2017.

JEPPSON, K. O.; SVENSSON, C. M. Negative bias stress of MOS devices at high electric fields and degradation of MNOS devices. **Journal of Applied Physics**, [S.l.], v.48, n.5, p.2004–2014, 1977.

KACZER, B. et al. Recent Trends in Bias Temperature Instability. **Journal of Vacuum Science Technology B: Microelectronics and Nanometer Structures**, [S.l.], v.29, 01 2011.

KANNO, M. et al. Empirical Characteristics and Extraction of Overall Variations for 65-nm MOSFETs and Beyond. In: IEEE SYMPOSIUM ON VLSI TECHNOLOGY, 2007., 2007. **Anais...** [S.l.: s.n.], 2007. p.88–89.

KARIMI, N.; MOOS, T.; MORADI, A. Exploring the Effect of Device Aging on Static Power Analysis Attacks. **IACR Transactions on Cryptographic Hardware and Embedded Systems**, [S.l.], v.2019, n.3, p.233–256, May 2019.

KASPER, T.; OSWALD, D.; PAAR, C. Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation. In: RFID. SECURITY AND PRIVACY, 2012, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2012. p.61–77.

KERBER, A.; CARTIER, E. Bias Temperature Instability Characterization Methods. In: BIAS TEMPERATURE INSTABILITY FOR DEVICES AND CIRCUITS, 2014, New York, NY. **Anais...** Springer New York, 2014. p.3–31.

KERBER, A.; NIGAM, T. Bias temperature instability in scaled CMOS technologies: A circuit perspective. **Microelectronics Reliability**, [S.l.], v.81, p.31 – 40, 2018.

KOCHER, P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: ADVANCES IN CRYPTOLOGY — CRYPTO '96, 1996, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 1996. p.104–113.

KOCHER, P.; JAFFE, J.; JUN, B. Differential Power Analysis. In: ADVANCES IN CRYPTOLOGY — CRYPTO' 99, 1999, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 1999. p.388–397.

K.SAHA, S. Modeling Process Variability in Scaled CMOS Technology. **IEEE Design Test of Computers**, [S.l.], v.27, n.2, p.8–16, March 2010.

KUHN, K. et al. **Managing process variation in Intel's 45 nm CMOS technology**. 93-109p. v.12.

LEWYN, L. L.; YTTERDAL, T.; WULFF, C.; MARTIN, K. Analog Circuit Design in Nanoscale CMOS Technologies. **Proceedings of the IEEE**, [S.l.], v.97, n.10, p.1687–1714, Oct 2009.

LIEBMANN, L. W. et al. TCAD development for lithography resolution enhancement. **IBM Journal of Research and Development**, [S.l.], v.45, n.5, p.651–665, Sep. 2001.

LIN, L.; BURLESON, W. Analysis and Mitigation of Process Variation Impacts on Power-Attack Tolerance. In: ANNUAL DESIGN AUTOMATION CONFERENCE, 46., 2009, New York, NY, USA. **Proceedings...** Association for Computing Machinery, 2009. p.238–243. (DAC '09).

LUO, C.; FEI, Y.; KAELI, D. Effective Simple-Power Analysis Attacks of Elliptic Curve Cryptography on Embedded Systems. In: IEEE/ACM INTERNATIONAL CONFERENCE ON COMPUTER-AIDED DESIGN (ICCAD), 2018., 2018. **Anais...** [S.l.: s.n.], 2018. p.1–7.

MAHAPATRA, S.; GOEL, N.; MUKHOPADHYAY, S. Introduction: Bias Temperature Instability (BTI) in N and P Channel MOSFETs. In: FUNDAMENTALS OF BIAS TEMPERATURE INSTABILITY IN MOS TRANSISTORS: CHARACTERIZATION METHODS,

PROCESS AND MATERIALS IMPACT, DC AND AC MODELING, 2016, New Delhi. **Anais...** Springer India, 2016. p.1–42.

MAHMOODI, H.; MUKHOPADHYAY, S.; ROY, K. Estimation of delay variations due to random-dopant fluctuations in nanoscale CMOS circuits. **IEEE Journal of Solid-State Circuits**, [S.l.], v.40, n.9, p.1787–1796, Sep. 2005.

MANGARD, S.; OSWALD, E.; POPP, T. **Power Analysis Attacks**: Revealing the Secrets of Smart Cards (Advances in Information Security). Berlin, Heidelberg: Springer-Verlag, 2007.

MARICAU, E.; GIELEN, G. CMOS reliability overview. In: **Analog IC Reliability in Nanometer CMOS**. [S.l.]: Springer, 2013. p.15–35.

MARKOV, S.; CHENG, B.; ZAIN, A.; ASENOV, A. Understanding variability in complementary metal oxide semiconductor (CMOS) devices manufactured using silicon-on-insulator (SOI) technology. In: KONONCHUK, O.; NGUYEN, B.-Y. (Ed.). **Silicon-On-Insulator (SOI) Technology**. [S.l.]: Woodhead Publishing, 2014. p.212 – 242.

MOORE, G. E. Cramming more components onto integrated circuits. **Electronics**, [S.l.], v.38, n.8, April 1965.

MULDER, E. D. et al. Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem. In: EUROCON 2005 - THE INTERNATIONAL CONFERENCE ON "COMPUTER AS A TOOL", 2005. **Anais...** [S.l.: s.n.], 2005. v.2, p.1879–1882.

MULDER, E. D.; GIERLICHS, B.; PRENEEL, B.; VERBAUWHEDE, I. Practical DPA attacks on MDPL. In: FIRST IEEE INTERNATIONAL WORKSHOP ON INFORMATION FORENSICS AND SECURITY (WIFS), 2009., 2009. **Anais...** [S.l.: s.n.], 2009. p.191–195.

MURESAN, R.; GREGORI, S. Protection Circuit against Differential Power Analysis Attacks for Smart Cards. **IEEE Transactions on Computers**, [S.l.], v.57, n.11, p.1540–1549, Nov 2008.

ÖRS, S. B.; GüRKAYNAK, F.; OSWALD, E.; PRENEEL, B. Power-Analysis Attack on an ASIC AES Implementation. In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING (ITCC'04) VOLUME 2 - VOLUME 2, 2004, USA. **Proceedings...** IEEE Computer Society, 2004. p.546. (ITCC '04).

PAAR, C.; PELZL, J. **Understanding Cryptography**: A Textbook for Students and Practitioners. 1st.ed. [S.l.]: Springer Publishing Company, Incorporated, 2009.

PANDIT, S.; MANDAL, C.; PATRA, A. **Nano-scale CMOS analog circuits**: Models and CAD techniques for high-level design. [S.l.]: CRC Press, 2014. 1-368p.

PANG, X.; WANG, J.; WANG, C.; WANG, X. A DPA resistant dual rail Préchargé logic cell. In: IEEE 11TH INTERNATIONAL CONFERENCE ON ASIC (ASICON), 2015., 2015. **Anais...** [S.l.: s.n.], 2015. p.1–4.

PUSCHKARSKY, K. et al. Understanding BTI in SiC MOSFETs and Its Impact on Circuit Operation. **IEEE Transactions on Device and Materials Reliability**, [S.l.], v.18, n.2, p.144–153, 2018.

QUISQUATER, J.-J.; SAMYDE, D. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In: SMART CARD PROGRAMMING AND SECURITY, 2001, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2001. p.200–210.

RABAEY, J. M.; CHANDRAKASAN, A.; NIKOLIC, B. **Digital Integrated Circuits**. 3rd.ed. USA: Prentice Hall Press, 2008.

REIS, R.; WIRTH, G.; CAO, Y. **Circuit design for reliability**. [S.l.]: Springer New York, 2015.

RENAULD, M. et al. A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices. In: ADVANCES IN CRYPTOLOGY – EUROCRYPT, 2011, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2011. p.109–128.

RöMER, T.; SEIFERT, J.-P. Information Leakage Attacks against Smart Card Implementations of the Elliptic Curve Digital Signature Algorithm. In: SPRINGER BERLIN HEIDELBERG, 2001. **Anais...** [S.l.: s.n.], 2001. v.2140, p.211–219.

SAKIYAMA, K.; SASAKI, Y.; LI, Y. **Security of Block Ciphers**: From Algorithm Design to Hardware Implementation. 1st.ed. [S.l.]: Wiley Publishing, 2015.

SAXENA, S. et al. Variation in Transistor Performance and Leakage in Nanometer-Scale Technologies. **Electron Devices, IEEE Transactions on**, [S.l.], v.55, p.131 – 144, 02 2008.

SCHRODER, D. K.; BABCOCK, J. A. Negative bias temperature instability: Road to cross in deep submicron silicon semiconductor manufacturing. In: 2003. **Anais...** AIP, 2003. v.94, n.1, p.1–18.

SEDRA, A. S.; SMITH, K. C. **Microelectronic Circuits Revised Edition**. 5th.ed. USA: Oxford University Press, Inc., 2007.

SPREITZER, R.; MOONSAMY, V.; KORAK, T.; MANGARD, S. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. **IEEE Communications Surveys Tutorials**, [S.l.], v.20, n.1, p.465–488, Firstquarter 2018.

SUTHERLAND, I.; SPROULL, B.; HARRIS, D. **Logical Effort**: Designing Fast CMOS Circuits. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1999.

TILBORG, H. C. A. van (Ed.). **Encyclopedia of Cryptography and Security**. [S.l.]: Springer, 2005.

TIRI, K.; AKMAL, M.; VERBAUWHEDE, I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In: EUROPEAN SOLID-STATE CIRCUITS CONFERENCE, 28., 2002. **Proceedings...** [S.l.: s.n.], 2002. p.403–406.

TIRI, K.; VERBAUWHEDE, I. Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology. In: CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES, 2003. **Anais...** Springer, 2003. p.125–136.

TIRI, K.; VERBAUWHEDE, I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: DESIGN, AUTOMATION AND TEST IN EUROPE CONFERENCE AND EXHIBITION, 2004. **Proceedings...** [S.l.: s.n.], 2004. v.1, p.246–251 Vol.1.

TOLEDANO-LUQUE, M. et al. Response of a single trap to AC negative Bias Temperature stress. In: INTERNATIONAL RELIABILITY PHYSICS SYMPOSIUM, 2011., 2011. **Anais...** [S.l.: s.n.], 2011. p.4A.2.1–4A.2.8.

TU, K. N. Recent advances on electromigration in very-large-scale-integration of interconnects. **Journal of Applied Physics**, [S.l.], v.94, n.9, p.5451–5473, 2003.

VELAMALA, J. B. et al. Compact Modeling of Statistical BTI Under Trapping/Detrapping. **IEEE Transactions on Electron Devices**, [S.l.], v.60, n.11, p.3645–3654, 2013.

WANG, X. et al. Statistical Threshold-Voltage Variability in Scaled Decananometer Bulk HKMG MOSFETs: A Full-Scale 3-D Simulation Scaling Study. **IEEE Transactions on Electron Devices**, [S.l.], v.58, n.8, p.2293–2301, Aug 2011.

WEGLARCZYK, S. Kernel density estimation and its application. **ITM Web Conf: XLVIII Seminar of Applied Mathematics.**, [S.l.], v.23, p.1–8, 2018.

WESTE, N. H. E.; ESHRAGHIAN, K. **Principles of CMOS VLSI Design**: A Systems Perspective. USA: Addison-Wesley Longman Publishing Co., Inc., 1985.

WIRNSHOFER, M. Sources of Variation. In: **Variation-Aware Adaptive Voltage Scaling for Digital CMOS Circuits**. Dordrecht: Springer Netherlands, 2013. p.5–14.

WIRTH, G. et al. Charge Trapping in MOSFETS: BTI and RTN Modeling for Circuits. In: BIAS TEMPERATURE INSTABILITY FOR DEVICES AND CIRCUITS, 2014, New York, NY. **Anais...** Springer New York, 2014. p.751–782.

WIRTH, G.; SILVA, R. da. Charge Trapping Phenomena in MOSFETS: From Noise to Bias Temperature Instability. In: CIRCUIT DESIGN FOR RELIABILITY, 2015, New York, NY. **Anais...** Springer New York, 2015. p.21–46.

WIRTH, G.; SILVA, R.; KACZER, B. Statistical Model for MOSFET Bias Temperature Instability Component Due to Charge Trapping. **Electron Devices, IEEE Transactions on**, [S.l.], v.58, p.2743 – 2751, 09 2011.

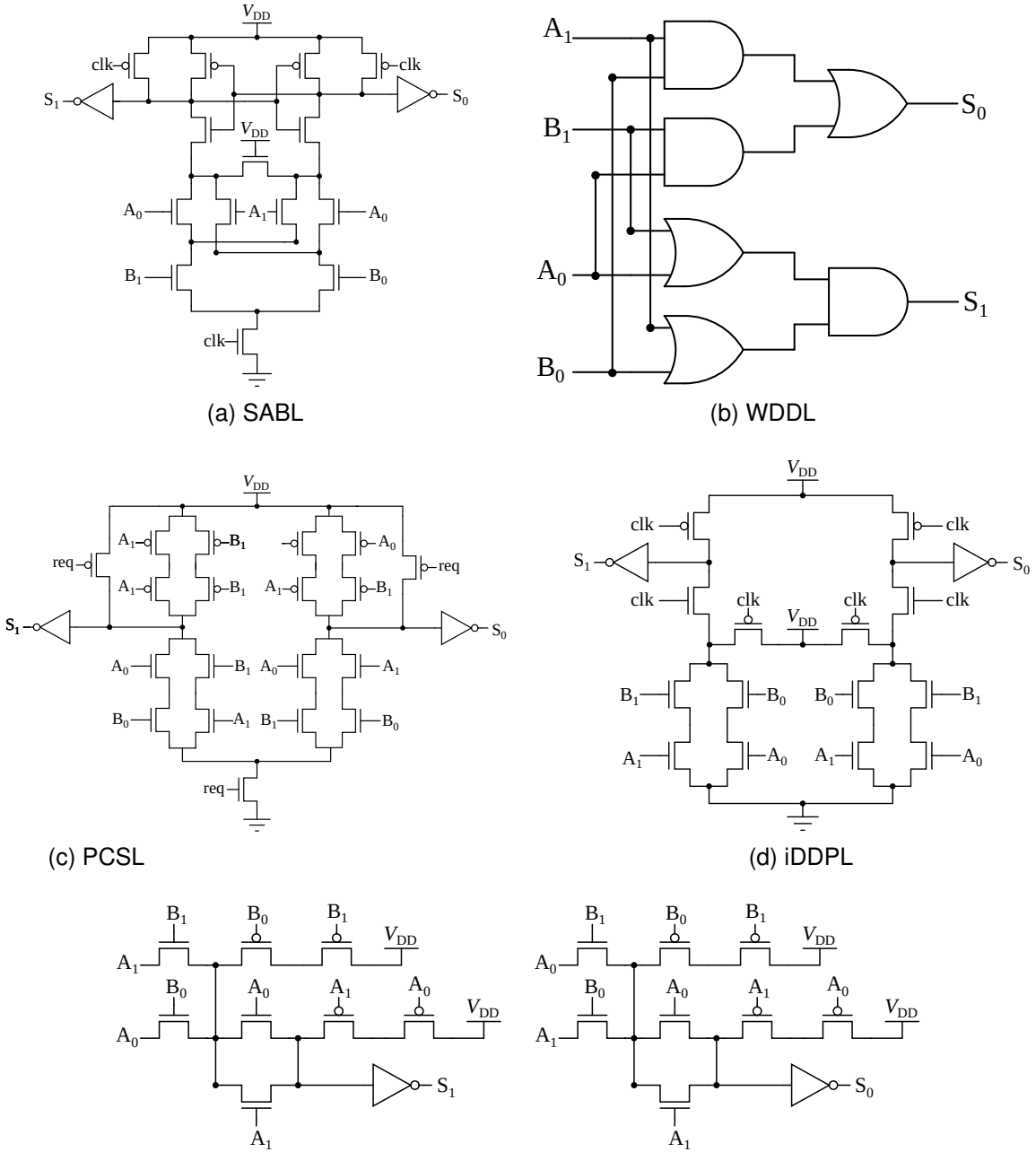
YE, Y. et al. Statistical Modeling and Simulation of Threshold Variation Under Random Dopant Fluctuations and Line-Edge Roughness. **IEEE Transactions on Very Large Scale Integration (VLSI) Systems**, [S.l.], v.19, n.6, p.987–996, June 2011.

YU, W.; KöSE, S. Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures. **IEEE Transactions on Emerging Topics in Computing**, [S.l.], v.6, n.2, p.244–257, 2018.

ZHANG, L.; VEGA, L.; TAYLOR, M. Power Side Channels in Security ICs: Hardware Countermeasures. , [S.l.], 05 2016.

Apêndices

APÊNDICE A – Arranjo de Transistores da Porta Lógica XOR/XNOR para as Topologias Analisadas



(a) SABL

(b) WDDL

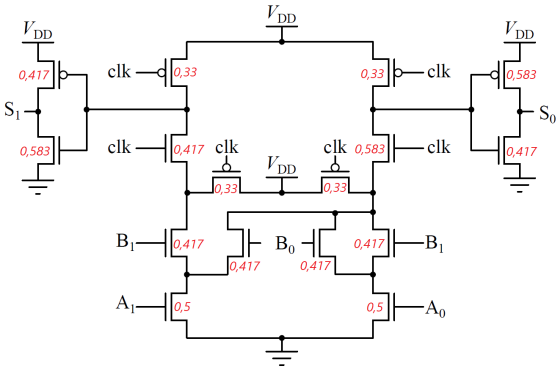
(c) PCSL

(d) iDDPL

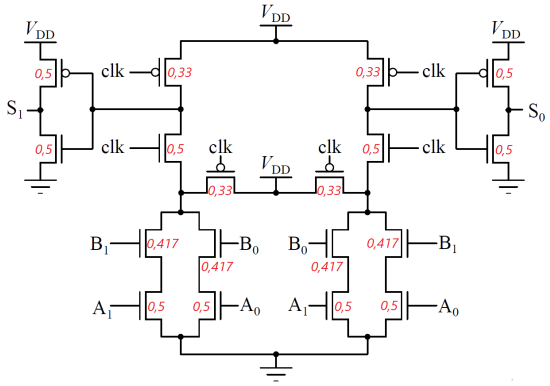
(e) DPPL

Figura A-1 – Esquemático da porta lógica XOR/XNOR para as topologias: (a) SABL, (b) WDDL, (c) PCSL, (d) iDDPL, (e) DPPL.

APÊNDICE B – Resultados do Cálculo de DF para o Arranjo de Transistores das Portas Lógicas Analisadas

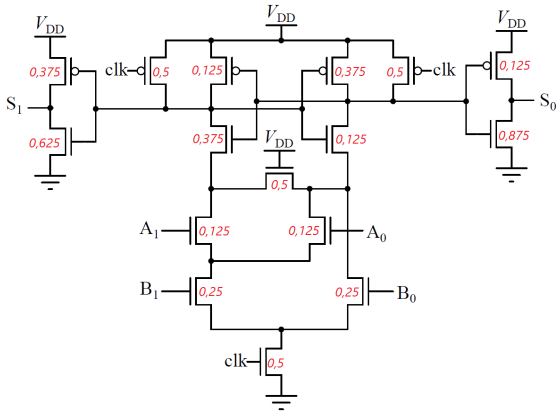


(a) AND/NAND – iDDPL

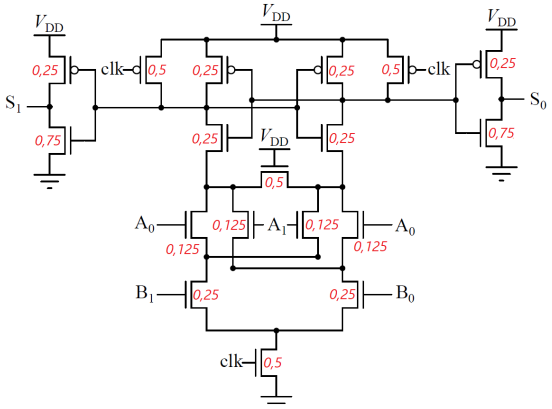


(b) XOR/XNOR – iDDPL

Figura B-1 – Valores de DF para o arranjo de transistores das portas lógicas (a) AND/NAND e (b) XOR/XNOR, implementadas na topologia iDDPL.

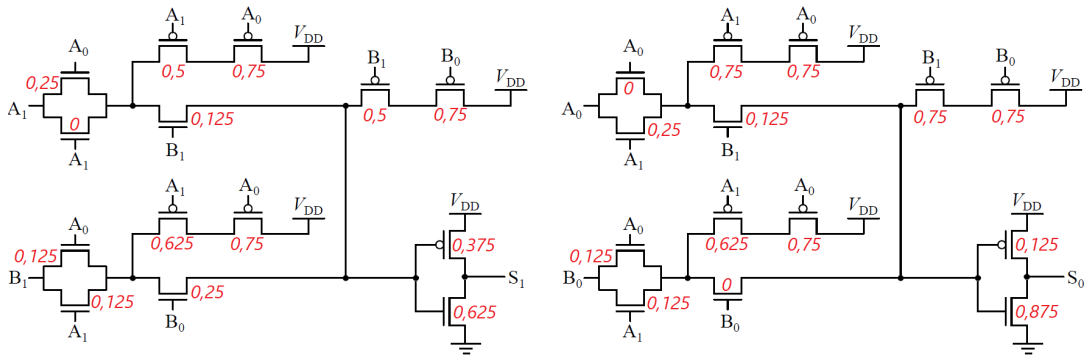


(a) AND/NAND – SABL

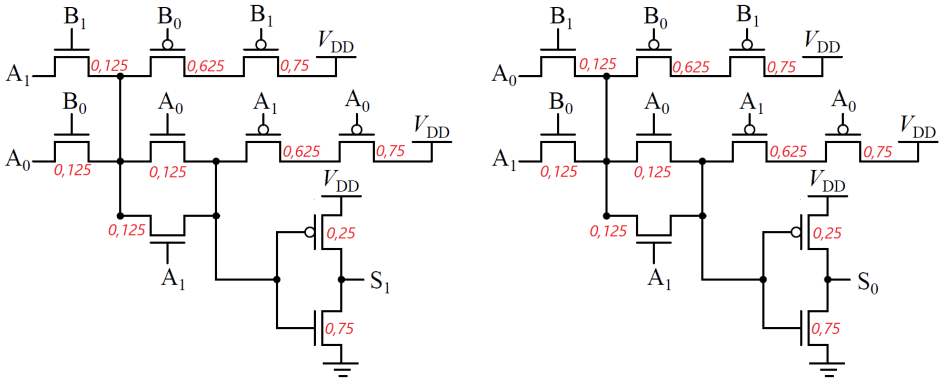


(b) XOR/XNOR – SABL

Figura B-2 – Valores de DF para o arranjo de transistores das portas lógicas (a) AND/NAND e (b) XOR/XNOR, implementadas na topologia SABL.

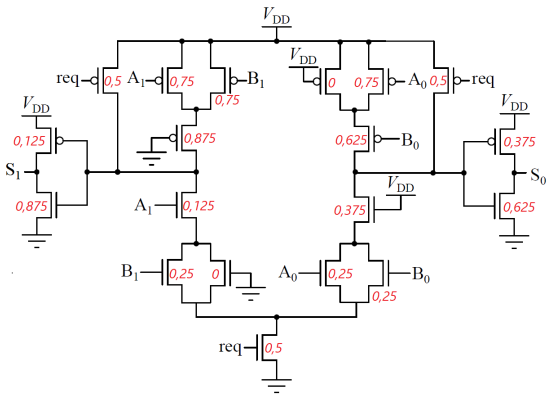


(a) AND/NAND – DPPL

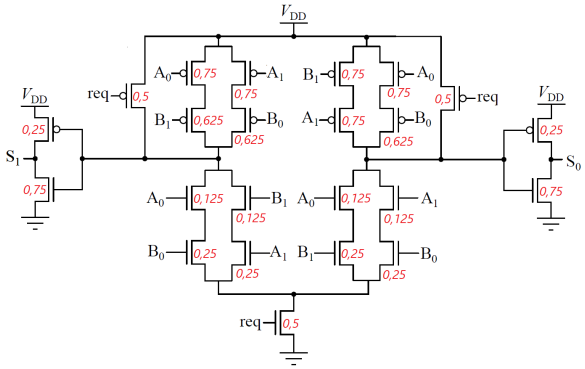


(b) XOR/XNOR – DPPL

Figura B-3 – Valores de DF para o arranjo de transistores das portas lógicas (a) AND/NAND e (b) XOR/XNOR, implementadas na topologia DPPL.

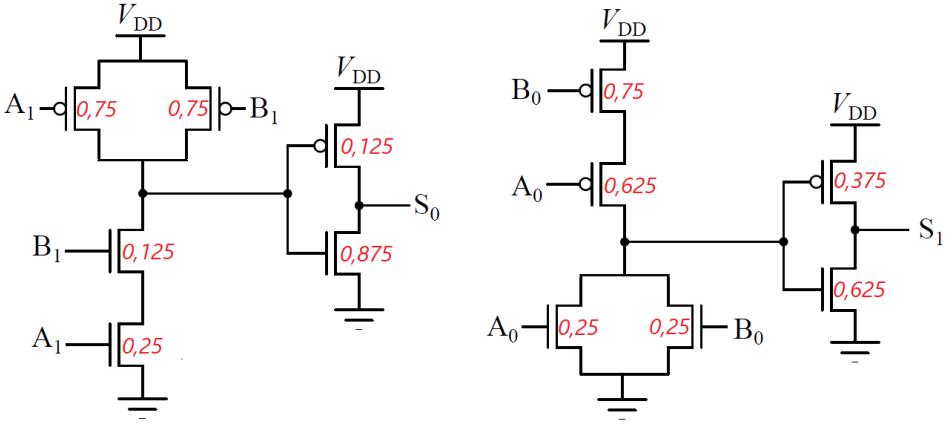


(a) AND/NAND – PCSL

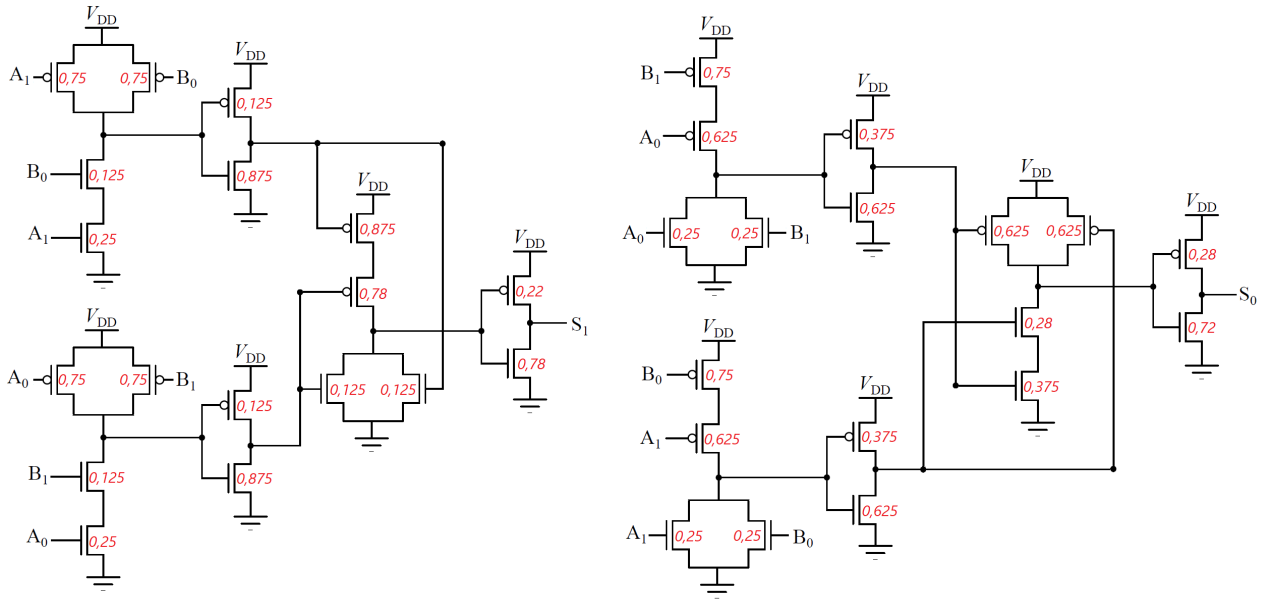


(b) XOR/XNOR – PCSL

Figura B-4 – Valores de DF para o arranjo de transistores das portas lógicas (a) AND/NAND e (b) XOR/XNOR, implementadas na topologia PCSL.



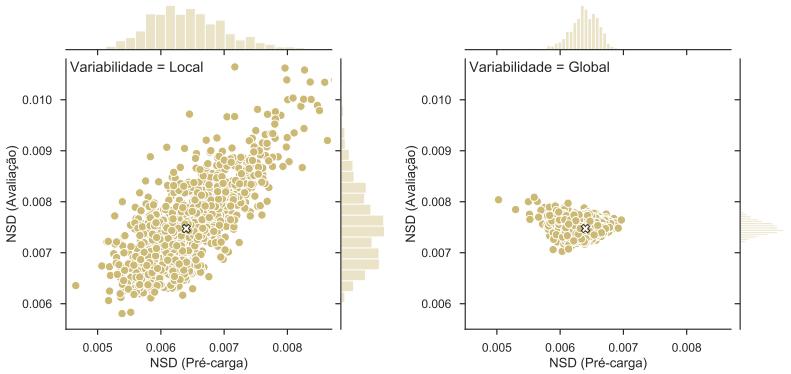
(a) AND/NAND – WDDL



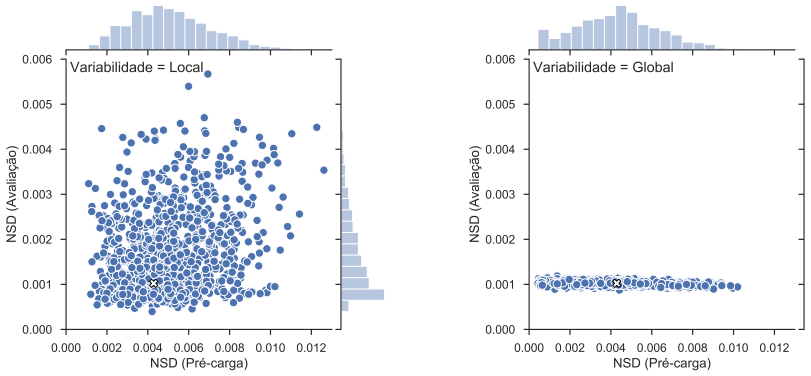
(b) XOR/XNOR – WDDL

Figura B-5 – Valores de DF para o arranjo de transistores das portas lógicas (a) AND/NAND e (b) XOR/XNOR, implementadas na topologia WDDL.

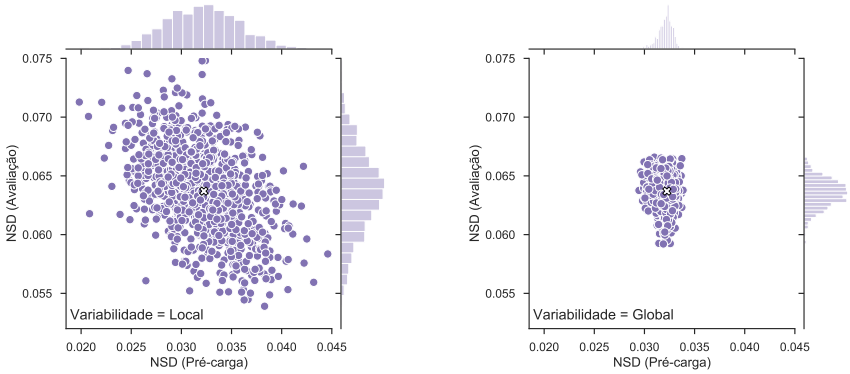
APÊNDICE C – Resultados para a Variabilidade de Processo



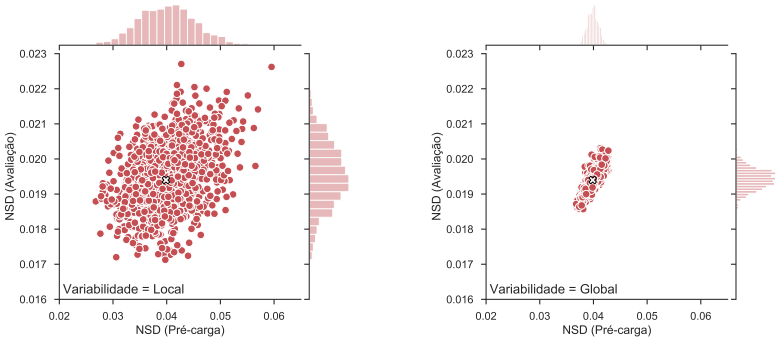
(a) AND/NAND – iDDPL



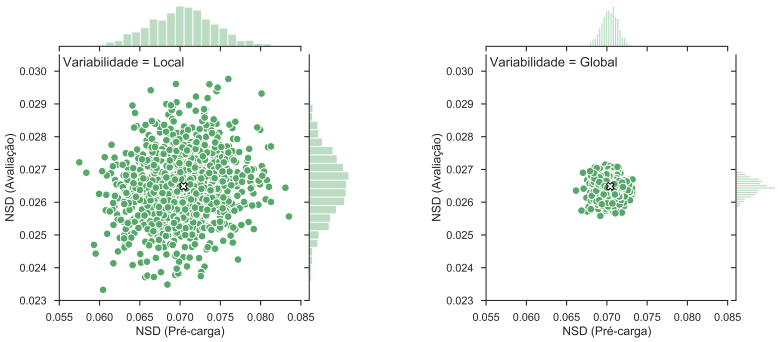
(b) AND/NAND – SABL



(c) AND/NAND – DPPL

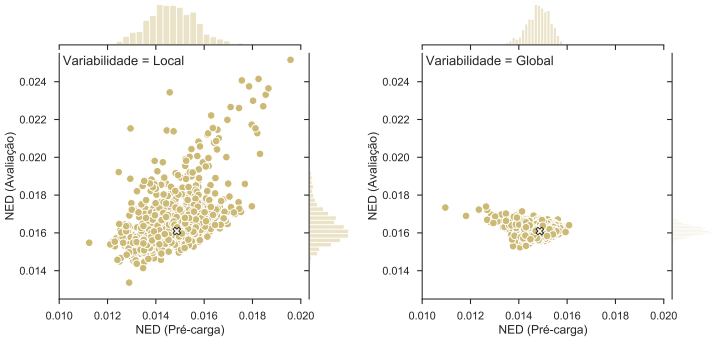


(d) AND/NAND – PCSL

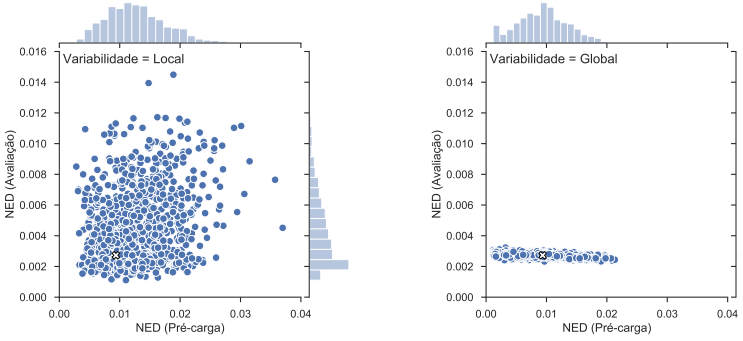


(e) AND/NAND – WDDL

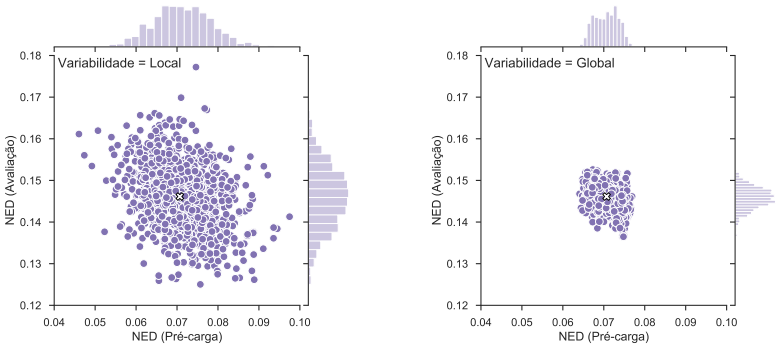
Figura C-1 –Distribuição dos resultados de NSD, avaliando efeitos locais e globais, para a porta AND/NAND implementada nas topologias (a) iDDPL, (b) SABL, (c) DPPL, (d) PCSL, (e) WDDL. Os pontos com o marcador 'X' representam os valores nominais.



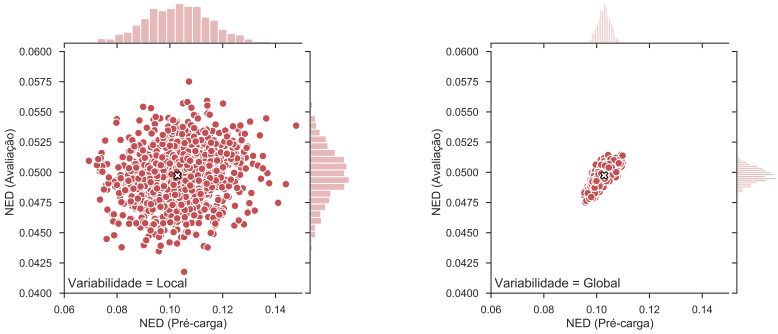
(a) AND/NAND – iDDPL



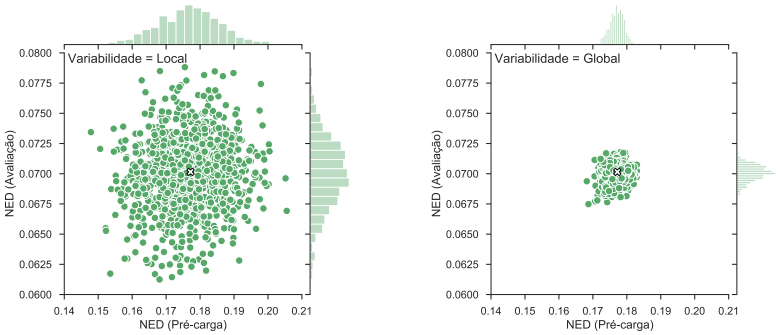
(b) AND/NAND – SABL



(c) AND/NAND – DPPL

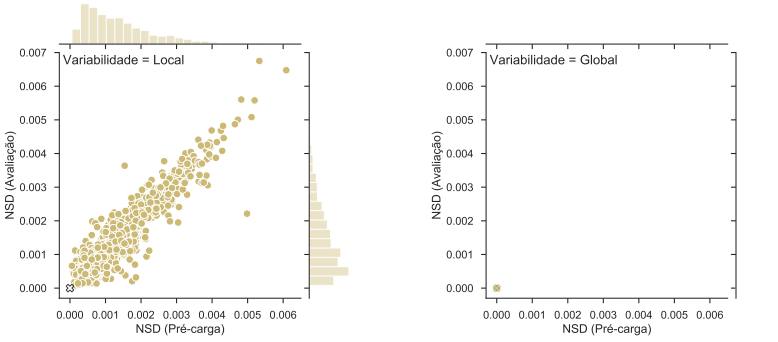


(d) AND/NAND – PCSL

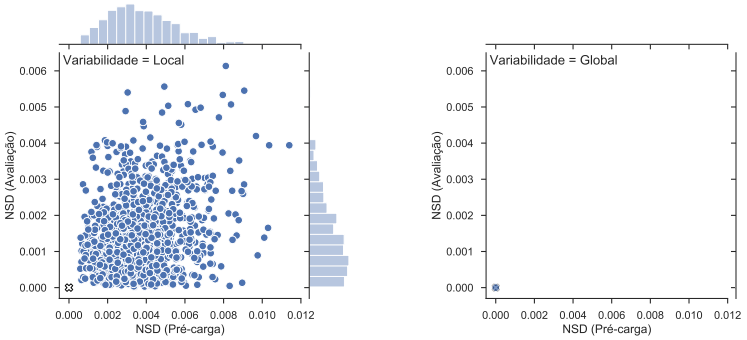


(e) AND/NAND – WDDL

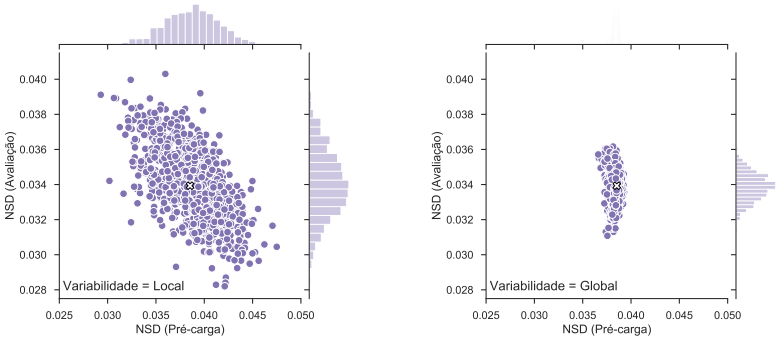
Figura C-2 –Distribuição dos resultados de NED, avaliando efeitos locais e globais, para a porta AND/NAND implementada nas topologias (a) iDDPL, (b) SABL, (c) DPPL, (d) PCSL, (e) WDDL. Os pontos com o marcador 'X' representam os valores nominais.



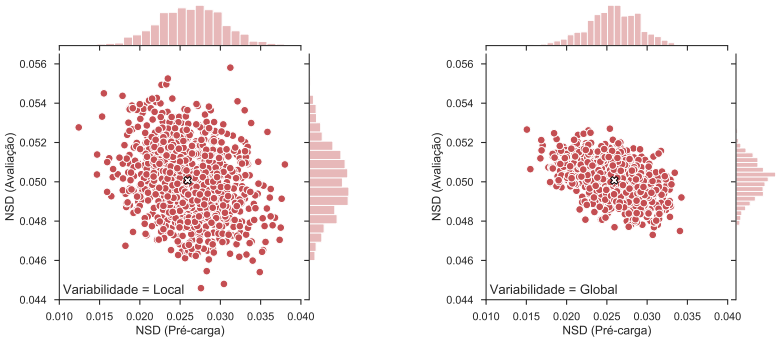
(a) XOR/XNOR – iDDPL



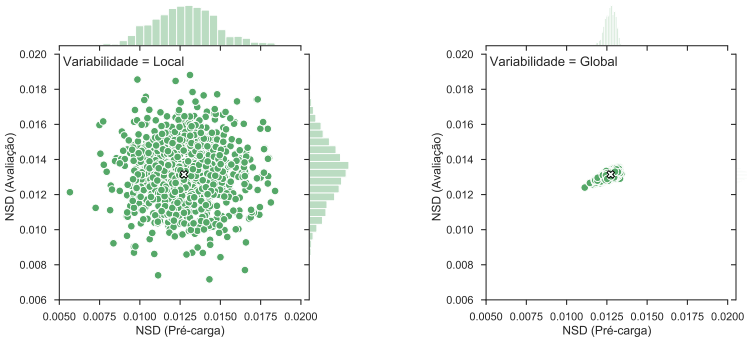
(b) XOR/XNOR – SABL



(c) XOR/XNOR – DPPL

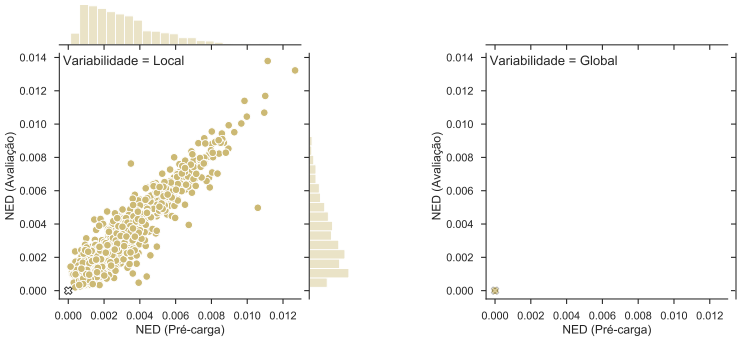


(d) XOR/XNOR – PCSL

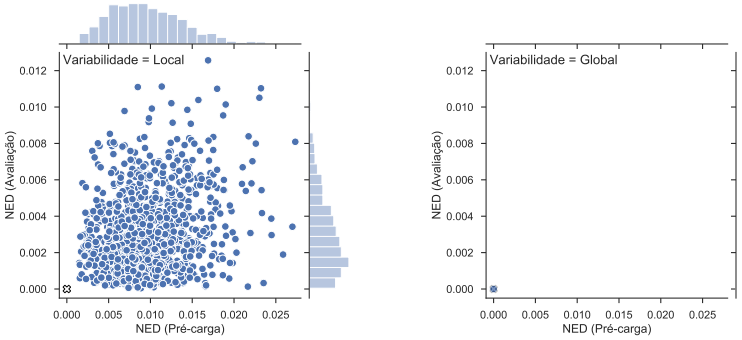


(e) XOR/XNOR – WDDL

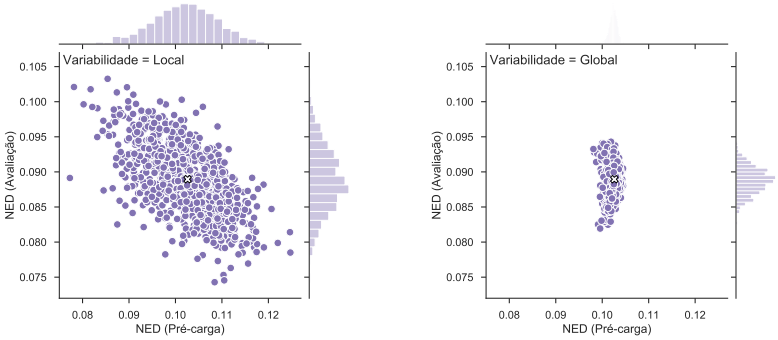
Figura C-3 – Distribuição dos resultados de NSD, avaliando efeitos locais e globais, para a porta XOR/XNOR implementada nas topologias (a) iDDPL, (b) SABL, (c) DPPL, (d) PCSL, (e) WDDL. Os pontos com o marcador 'X' representam os valores nominais.



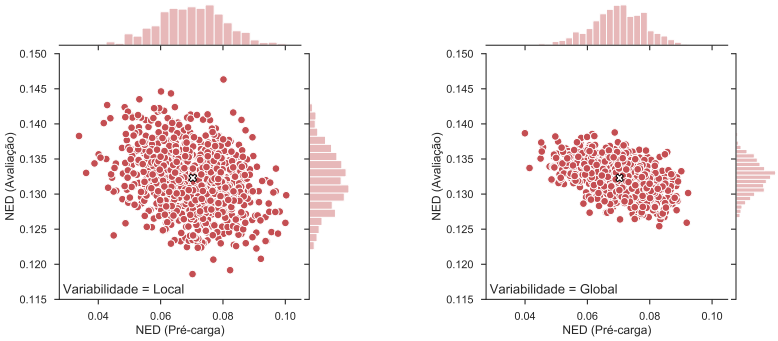
(a) XOR/XNOR – iDDPL



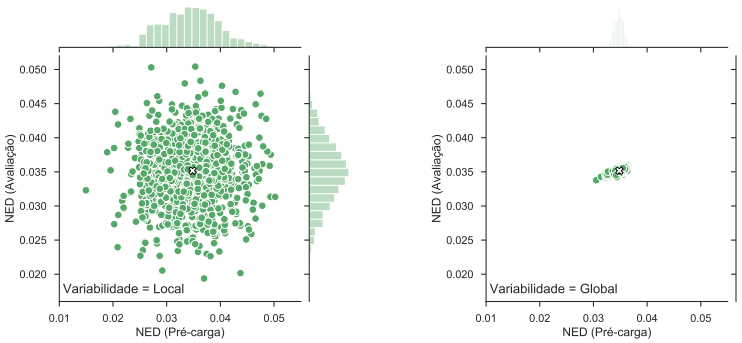
(b) XOR/XNOR – SABL



(c) XOR/XNOR – DPPL



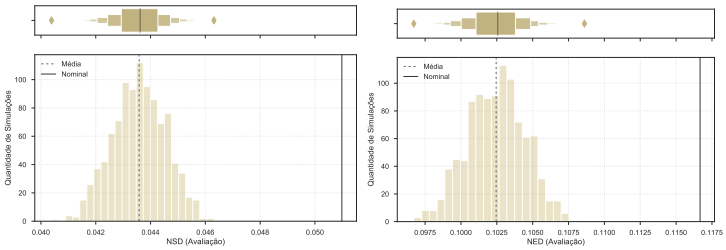
(d) XOR/XNOR – PCSL



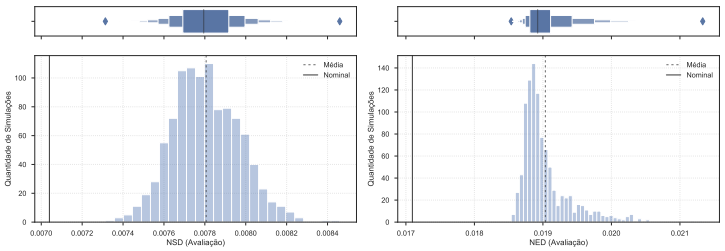
(e) XOR/XNOR – WDDL

Figura C-4 –Distribuição dos resultados de NED, avaliando efeitos locais e globais, para a porta XOR/XNOR implementada nas topologias (a) iDDPL, (b) SABL, (c) DPPL, (d) PCSL, (e) WDDL. Os pontos com o marcador 'X' representam os valores nominais.

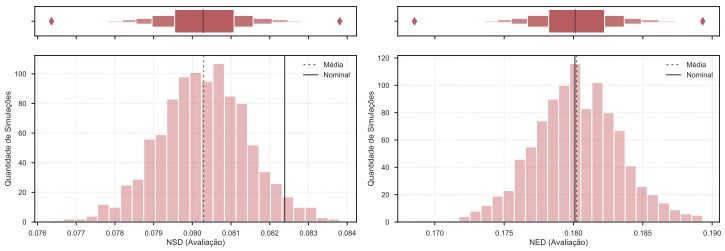
APÊNDICE D – Resultados para o Efeito BTI



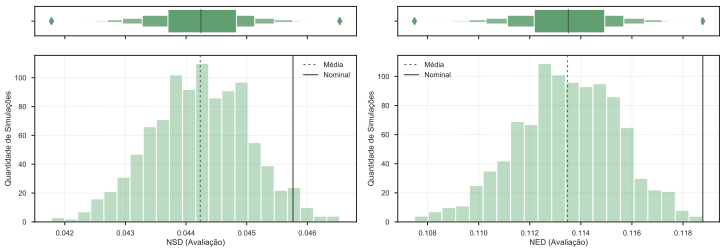
(a) AND/NAND – iDDPL



(b) AND/NAND – SABL

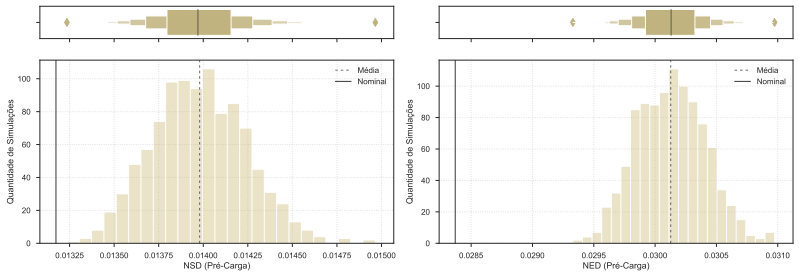


(c) AND/NAND – PCSL

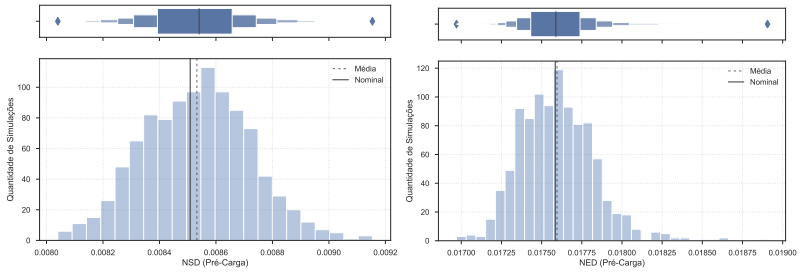


(d) AND/NAND – WDDL

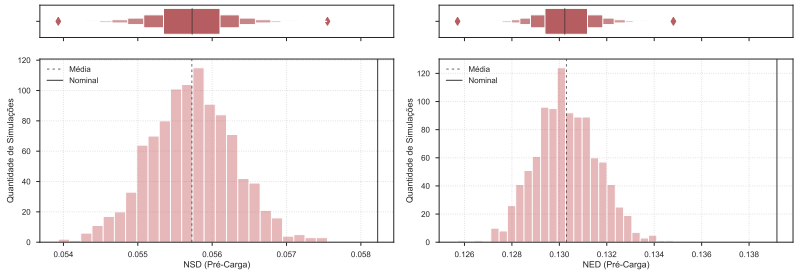
Figura D-1 – Distribuição de frequência para as métricas de segurança NSD e NED, obtidas durante a fase de avaliação para a porta lógica AND/NAND implementada nas topologias (a) iDDPL, (b) SABL, (c) PCSL, (d) WDDL.



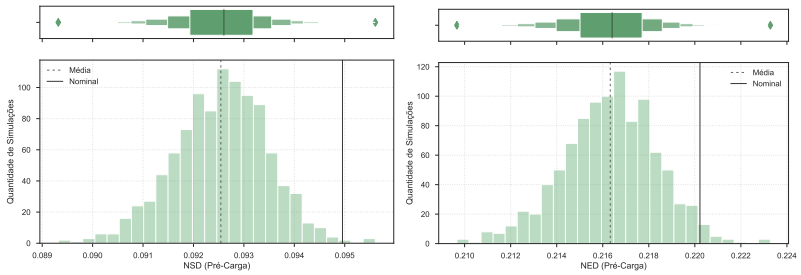
(a) AND/NAND – iDDPL



(b) AND/NAND – SABL

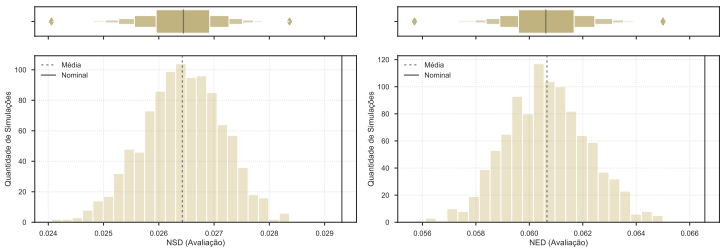


(c) AND/NAND – PCSL

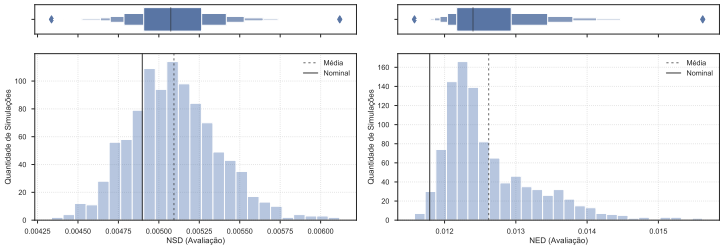


(d) AND/NAND – WDDL

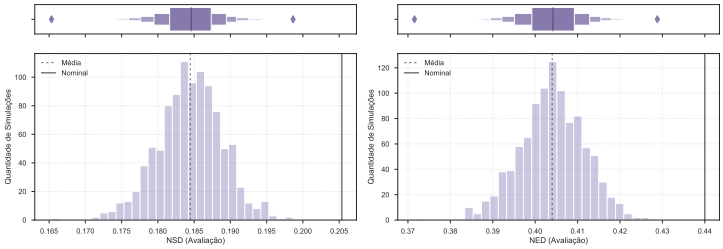
Figura D-2 – Distribuição de frequência para as métricas de segurança NSD e NED, obtidas durante a fase de pré-carga para a porta lógica AND/NAND implementada nas topologias (a) iDDPL, (b) SABL, (c) PCSL, (d) WDDL.



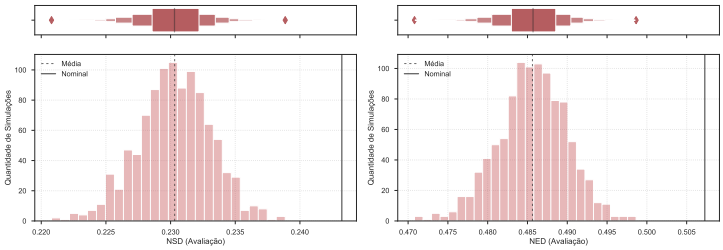
(a) XOR/XNOR – iDDPL



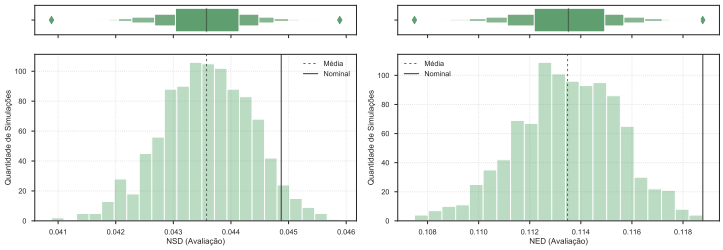
(b) XOR/XNOR – SABL



(c) XOR/XNOR – DPPL

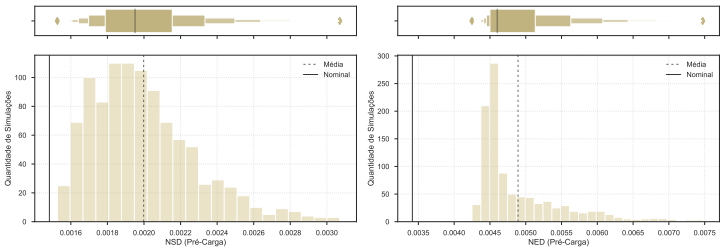


(d) XOR/XNOR – PCSL

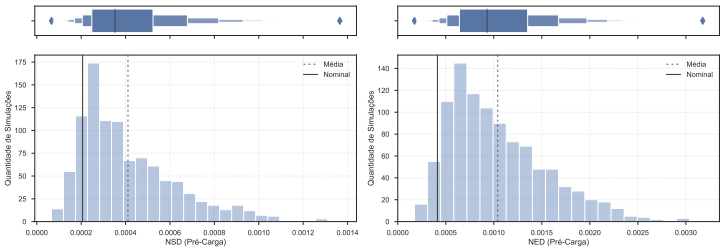


(e) XOR/XNOR – WDDL

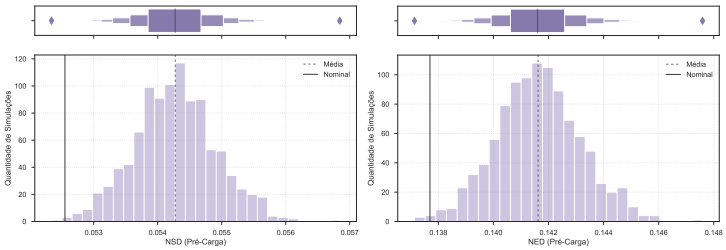
Figura D-3 – Distribuição de frequência para as métricas de segurança NSD e NED, obtidas durante a fase de avaliação para a porta lógica XOR/XNOR implementada nas topologias (a) iDDPL, (b) SABL, (c) DPPL, (d) PCSL, (e) WDDL.



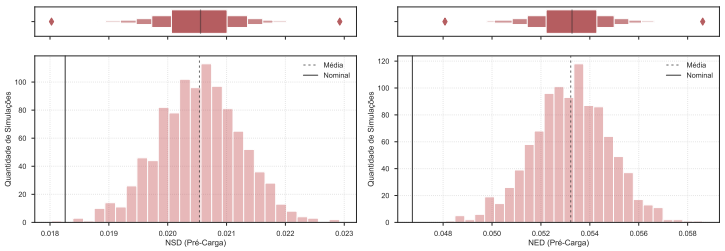
(a) XOR/XNOR – iDDPL



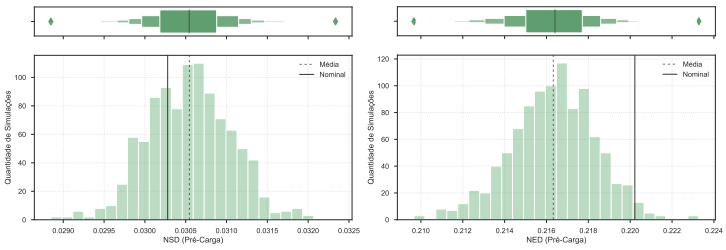
(b) XOR/XNOR – SABL



(c) XOR/XNOR – DPPL



(d) XOR/XNOR – PCSL



(e) XOR/XNOR – WDDL

Figura D-4 – Distribuição de frequência para as métricas de segurança NSD e NED, obtidas durante a fase de pré-carga para a porta lógica XOR/XNOR implementada nas topologias (a) iDDPL, (b) SABL, (c) DPPL, (d) PCSL, (e) WDDL.