ESTUDO DE DIMENSIONAMENTO PARA AUMENTO DE SEGURANÇA A ATAQUES POR CANAIS LATERAIS EM CIRCUITOS INTEGRADOS CRIPTOGRÁFICOS

VINÍCIUS RENATO ROCHA GERALDO[1]; PLÍNIO FINKENAUER JUNIOR[2]; RAFAEL IANKOWSKI SOARES[3]; VINÍCIUS VALDUGA DE ALMEIDA CAMARGO[4]

{vrrgeraldo[1], pfinkenauer[2], rafael.soares[3], vvacamargo[4]}@inf.ufpel.edu.br
Grupo de Arquitetura e Circuitos Integrados - GACI
Universidade Federal de Pelotas - UFPel

1. INTRODUÇÃO

Com o avanço tecnológico e a expansão do acesso à informação, o sigilo de dados torna-se essencial. A popularização de dispositivos IoT (Internet das Coisas, do inglês *Internet of Things)* também reforça a necessidade por sistemas digitais capazes de operar de maneira segura. Com esse intuito, os algoritmos criptográficos são usados para ocultar os dados e protegê-los contra possíveis agentes maliciosos. Por outro lado, diferentes métodos de ataques aos sistemas criptográficos foram desenvolvidos com o propósito de conseguir acesso às informações confidenciais. Os ataques por canais laterais (*Side Channel Attacks – SCA*) são metodologias que utilizam propriedades físicas dos sistemas para obter os dados sigilosos. Entre as propriedades exploradas pelos SCA estão o consumo de energia, emissão de radiação eletromagnética e tempo de processamento.

A Análise Diferencial de Potência (*Differential Power Analysis* – DPA) é um ataque SCA que investiga o consumo de energia durante o processamento do dado pelo algoritmo criptográfico (KRIS e VERBAUWHEDE, 2003). DPA é muito utilizado por ser um ataque não-invasivo, ou seja, não deixa vestígios do ataque no sistema. Além disso, DPA revela-se eficiente mesmo com sinais ruidosos para realizar o ataque (KRIS e VERBAUWHEDE, 2004). Para reduzir a ação desses ataques, são desenvolvidas estratégias, conhecidas como contramedidas, que buscam minimizar as vulnerabilidades exploradas pelos SCA.

Uma estratégia de contramedida adotada para reduzir a eficácia do DPA, visa a uniformização de consumo, tornando-o independente do dado processado. No nível de implementação dos circuitos, dois estilos lógicos são empregados para equalizar o consumo: Trilha dupla (*Dual Rail* – DR) e lógica de pré-carga. DR é um esquemático de codificação onde um bit de informação é construído em duas trilhas, de forma que ambas sejam logicamente complementares (SOKOLOV et al., 2005). A lógica de pré-carga é um modelo de projeto que adiciona uma fase extra para o cálculo dos dados. Assim, a lógica de pré-carga em trilha dupla (*Dual-Rail Pre-Charge Logic* – DPL) é desenvolvida a partir da união de uma topologia de trilha dupla com lógica de pré-carga. Nesses circuitos, a fase adicional é responsável por conduzir todo o circuito para o mesmo estado inicial e, dessa forma, escondendo os comportamentos elétricos desde o último cálculo (DANGER et al., 2009). *Wave Dynamic Differential Logic* (WDDL) consiste em umas das topologias pioneiras a implantar o estilo lógico DPL como contramedida aos ataques DPA e se caracteriza pela sua implementação por meio de uma biblioteca de células padrão (HWANG et al., 2006).

Na etapa de síntese lógica de um projeto, o tamanho definido para os transistores afeta o comportamento elétrico dos circuitos, e consequentemente, a dissipação de potência destes. Um dos métodos mais populares na literatura para

definição do dimensionamento dos transistores é o *Logical Effort* (LE). Essa técnica busca otimizar o tempo de atraso associado às redes de *pull-up* e *pull-down* de circuitos baseados em lógica CMOS, desconsiderando área e potência (SINGH et al., 2018). Assim, dado o panorama apresentado, esse trabalho propõe uma investigação do impacto da variação dos parâmetros de dimensionamento do LE nas métricas de segurança associadas a dissipação de energia em circuitos criptográficos WDDL.

2. METODOLOGIA

A topologia WDDL é desenvolvida a partir da utilização de uma biblioteca de células padrão CMOS. A biblioteca de células é constituída por um conjunto de portas lógicas projetadas e verificadas anteriormente. Por utilizar DPL, uma porta WDDL consiste em uma combinação de duas portas logicamente complementares.

A topologia requer uma fase de pré-carga e uma fase de avaliação. Na fase de pré-carga, ambas as entradas, verdadeira e falsa, são fixadas em '0' lógico, encaminhando a saída de todas as portas ao mesmo valor – '0'. Esse valor é propagado para entrada da próxima porta. Na fase de avaliação, as entrada são complementares e a porta WDDL calcula o diferencial dinâmico para a saída (HWANG et al., 2006). A Figura 1 apresenta as portas NAND, NOR e XOR, implementadas no modelo WDDL, expondo a lógica original e complementar.

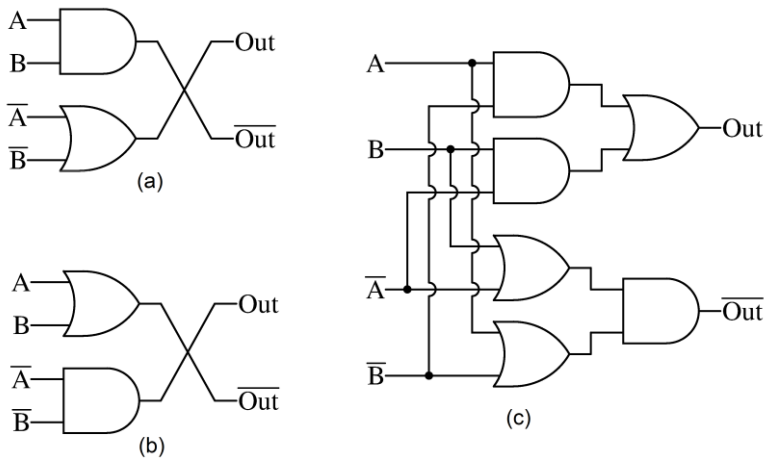

Figura 1 – Descrição das portas lógicas da topologia WDDL: (a) NAND, (b) NOR, (c) XOR.

No projeto de circuitos integrados baseados na utilização da técnica de LE, busca-se identificar o valor para o parâmetro lambda (λ) que equilibre os tempos de chaveamento existentes no circuito. Esse parâmetro é necessário para o dimensionamento da rede PMOS no projeto do circuito. A escolha do lambda pode impactar diretamente a segurança do circuito em relação à potência dissipada nas transições das entradas com as saídas para a porta desejada. Visando identificar o valor mais adequado para a segurança, realizou-se uma análise do vazamento de informações associado a cada porta, considerando a variação do lambda, por meio de métricas para quantificar a vulnerabilidade dos circuitos.

Para a extração dos valores de consumo, são realizadas simulações SPICE nas quais obtêm-se o comportamento elétrico do circuito. O modelo de transistores utilizado para a obtenção dos resultados é baseado na tecnologia preditiva 45-nanômetros (Free PDK – 45 nm). Na simulação dos circuitos é empregada a técnica de *fan-out of 4* (FO4) inversores, a qual consiste em 4 inversores na saída do

circuito, com o intuito de simular o comportamento capacitivo das portas lógicas conectadas às saídas deste circuito. Além disso, 2 inversores em série são utilizados como *fan-in,* a fim de obter sinais de entradas realistas.

As métricas utilizadas para a avaliação são o Desvio Padrão de Energia Normalizado (NED), expressa pela Equação (1), e o Desvio Padrão Normalizado (NSD), demonstrada na Equação (2) (MONTEIROA, TAKAHASHIB, SEKINEB, 2013). Ambas as métricas são calculadas para um conjunto de valores de energia (*E*), contendo todas as possíveis transições de um dado circuito. No caso das portas lógicas baseadas na topologia WDDL, isso implicará que portas NAND e NOR possuirão mesmas métricas NED e NSD.

$$NED = \frac{\max(E) - \min(E)}{\max(E)} \quad (1)$$

$$NSD = \frac{\sigma(E)}{\bar{E}} \quad (2)$$

3. RESULTADOS E DISCUSSÃO

A metodologia aplicada para as simulações considerou o lambda estimado pelo LE (λ = 1,2). Esse valor foi verificado como o mais adequado para otimização dos tempos do circuito. Para verificar o impacto na segurança, diferentes simulações SPICE foram executadas variando o valor de lambda (λ = 0,2 a λ = 5, incrementando uma casa decimal após a vírgula em cada simulação). A Figura 2 apresenta os resultados das métricas NSD e NED para as fases de pré-carga e avaliação nas portas NAND e XOR.

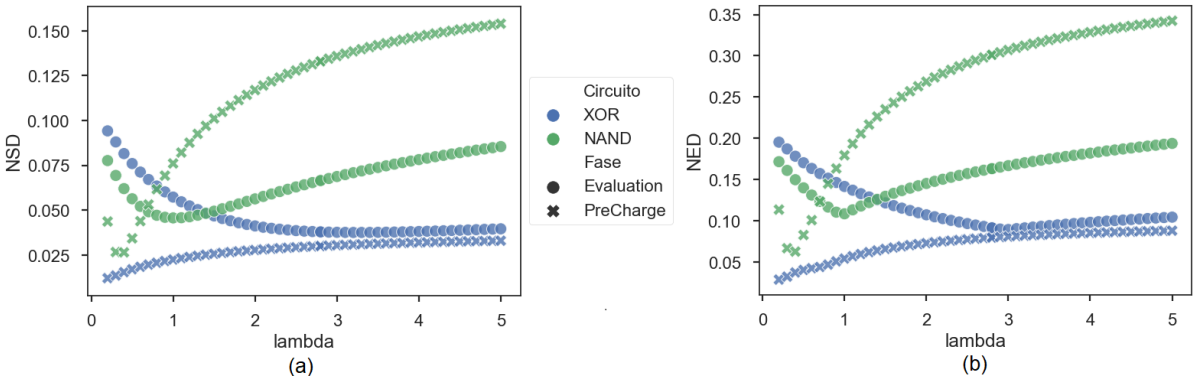

Figura 2 – Métricas de segurança para as portas NAND e XOR: (a) NSD e (b) NED.

Visto que os ataques podem ser realizados nas duas fases de computação dos dados, busca-se o resultado que seja menor e mais homogêneo entre as fases para escolha do parâmetro. Tanto para portas NAND quanto para portas XOR, fica evidente que o melhor lambda para o equilíbrio do consumo acontece em um ponto diferente do valor 1,2, mostrando que o lambda estimado pelo LE não é otimizado para a segurança.

A escolha do valor do lambda pode ser feita visando minimizar as métricas NED e NSD nas portas NAND e NOR, largamente utilizadas na construção de circuitos criptográficos em detrimento das portas XOR, de uso mais restrito e

naturalmente mais seguras. Seguindo esta estratégia valores de lambda entre 0,7 e 0,8 são considerados potenciais escolhas, dado que os resultados de NSD e NED das fases de pré-carga e avaliação se interceptam ou são bastante próximos gerando um ponto de mínimo relativo. Outra estratégia de dimensionamento possível seria buscar minimizar as métricas NED e NSD de todas as possíveis portas em ambos os ciclos. Neste caso, o ponto de mínimo ocorre quando a fase de avaliação da XOR cruza com a fase de pré-carga da NAND, em lambda aproximadamente igual a 0,8 para ambos NED e NSD.

4. CONCLUSÕES

Esse trabalho apresenta um estudo da variação do parâmetro lambda, estimado para o dimensionamento de circuitos, em busca da identificação do resultado mais apropriado para a homogeneização do consumo de energia. A análise dos resultados obtidos permite concluir que o valor definido para o parâmetro tem grande influência no consumo de energia dos circuitos analisados e, consequentemente, na segurança proporcionada por estes. Além disso, os resultados indicam que o valor definido via LE não corresponde ao lambda mais apropriado para segurança dos circuitos, sendo o lambda mais adequado inferior ao definido por LE. Como trabalhos futuros, pretende-se investigar o impacto do parâmetro em diferentes topologias de contramedidas e propagar estes estudos para circuitos criptográficos completos.

5. REFERÊNCIAS BIBLIOGRÁFICAS

KRIS, T. e VERBAUWHEDE, I. “Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology”. Em: Int. Work. on Crypt. Hard. e Emb. Systems., 2003, pg. 125-136.

TIRI, K. e VERBAUWHEDE, I. “Place and Route for Secure Standard Cell Design,” em: Smart Card Research and Advanced Applications VI, 2004, pp. 143–158.

DANGER, J.L., GUILLEY, S., BASHIN, S., NASSAR, M. e SAUVAGE, L. "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors". 2009 3rd International Conference on Signals, Circuits and Systems (SCS), Medenine, 2009, pp. 1-8.

SINGH, K., JAIN, A., MITTAL, A., YADAV, V., SINGG, A. A., JAIN, A. K., & Gupta, M. (2018). Optimum transistor sizing of CMOS logic circuits using logical effort theory and evolutionary algorithms. Integration, the VLSI Journal, 60, 25–38.

D. D. HWANG *et al*., "AES-Based Security Coprocessor IC in 0.18-*muhbox m*CMOS With Resistance to Differential Power Analysis Side-Channel Attacks," in IEEE Journal of Solid-State Circuits, vol. 41, no. 4, pp. 781-792, April 2006.

MONTEIROA, C., TAKAHASHIB, Y., SEKINEB, T. “Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level”. Microelectronics Journal. V. 44 I. 6. Pg. 496-503, 2013