BSTTL: Aperfeiçoamento da Lógica Segura em Trilha Tripla - STTL

Vitor Lima[1]; Rodrigo Nuevo[2]; Junior Finkenaur[3]; Leomar Júnior[4]; Felipe Marques[5]; Rafael Soares[6].

[1]Universidade Federal de Pelotas – vgdlima@inf.ufpel.edu.br 1
[2]Universidade Federal de Pelotas – m.lellis@inf.ufpel.edu.br 2 (se houver)
[3]Universidade Federal de Pelotas – pfinkenaur@inf.ufpel.edu.br 3 (se houver)
[4]Universidade Federal de Pelotas – leomarjr@inf.ufpel.edu.br 4 (se houver)
[5]Universidade Federal de Pelotas – felipem@inf.ufpel.edu.br 5 (se houver)
[6]Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br 6 (se houver)

1. INTRODUÇÃO

Com o avanço das tecnologias e a globalização da informação é cada vez mais importante garantir o sigilo dos dados, tanto no armazenamento quanto nas transferências em diversos tipos de sistemas. Focando nisso, algoritmos criptográficos são utilizados para ocultar informações confidenciais dos usuários. Diversas estratégias de ataques, em nível de software, foram desenvolvidas ao longo do tempo. Contudo, atualmente essa não é a única técnica utilizada para quebrar a segurança fornecida por sistemas criptográficos. Outras metodologias foram desenvolvidas para atacar esses sistemas correlacionando o processamento do algoritmo com características físicas dos chips que convergem às informações sigilosas.

Esses ataques são conhecidos como ataques por canais laterais (*Side Channel Attacks* – SCA) e foram primeiramente propostos por KOCHER (1996). Um exemplo de SCA são os ataques que exploram as características do consumo de energia ao computar o algoritmo para criptografar os dados. Esse ataque é conhecido como ataque por variação de energia (*Differential Power Analysis* – DPA).

DPA são ataques amplamente utilizados na atualidade, pois possuem características muito atrativas para os atacantes. Os principais benefícios são: (1) ataques com baixos custos – esses ataques necessitam apenas de osciloscópio, dispositivo criptográfico e software para análise estatística, (2) são ataques não invasivos, ou seja, são ataques que apenas monitoram o dispositivo atacado e não deixam rastros sobre o ataque e (3) alta efetividade, explora características intrínsecas dos dispositivos digitais, o que torna muito complexo eliminar essas vulnerabilidades de forma efetiva.

Os dispositivos com algoritmos criptográficos possuem alta suscetibilidade para ataques SCA, assim, é notório a necessidade de aprimoramento nos dispositivos, de forma que garanta que os mesmos sejam imunes aos ataques. Existem diversas estratégias na literatura que visam inviabilizar os ataques DPA, essas estratégias são denominadas de contramedidas. Exemplos de contramedidas: (1) trilha-dupla (*Dual-Rail* – DR), cada bit de informação do circuito é representado por duas trilhas, a lógica direta e o valor complementar. Dessa maneira sempre haverá transições 0~1 e 1~0, reduzindo a fuga de informações. (2) trilha-dupla com lógica complementar (*Dual-Rail Precharge Logic* – DPL) é uma metodologia muito utilizada e é baseada no DR que concentra toda a lógica em um único plano, isso evita as diferenças de consumo intrínsecas de cada plano. Para que a DPL funcione, é necessário inserir uma etapa extra de pré-carregamento para cada processamento do componente, como não possui arranjo complementar, essa etapa é responsável por levar o circuito para um estado inicial.

Em 2007 foi realizado um trabalho por RAZAFINDRAIBE, ROBERT e MAURINE (2007) com o intuito de uniformizar o consumo de energia. Essa contramedida é chamada de lógica segura em trilha tripla (*Secure Tripple Track Logic* – STTL). Essa topologia baseada em DPL adiciona uma trilha de validação que garante que o próximo estágio de transistores do circuito só propagará quando o sinal estiver estável. Isso evita diferenças nos consumos de energia ocasionado pelo *hazard* de propagação antecipada proveniente dos circuitos combinacionais.

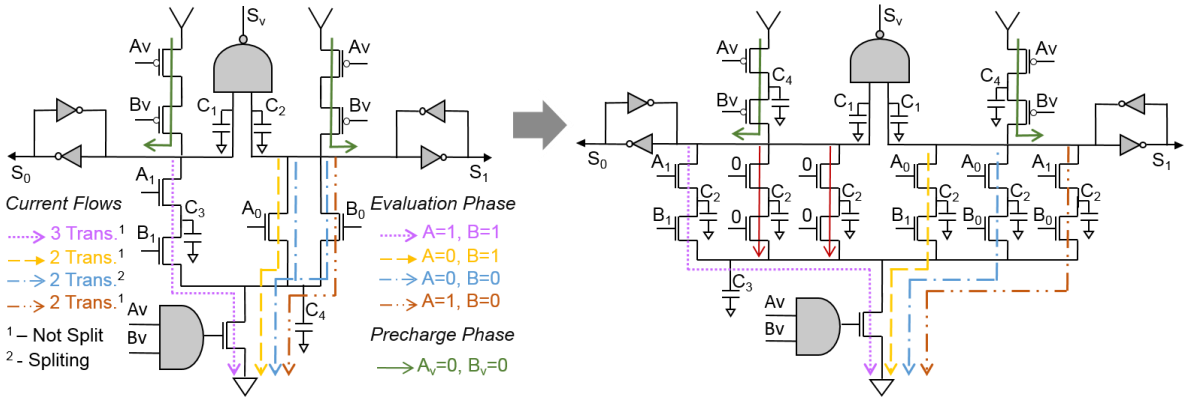
Os ataques DPA exploram a correlação entre o consumo de energia com as operações que os dispositivos realizam. Quanto maior for a variação e as discrepâncias nos traços de consumo, mais suscetível ele estará aos atacantes. Dessa maneira, se houvesse uma contramedida que homogeneizasse completamente o consumo, independente das entradas do circuito, não seria possível fazer ataques DPA.

Esse trabalho constatou que a topologia STTL possui uma estratégia poderosa como contramedida DPA, porém possui um arranjo de transistores desbalanceado. A metodologia proposta é chamada de lógica segura em trilha tripla balanceada (*Balanced Secure Tripple Track Logic* - BSTTL) e consiste em adicionar componentes nas portas lógicas que beneficiem o balanceamento das mesmas,. Para isso, são inseridos elementos que não farão, necessariamente, parte da lógica do circuito. Dessa maneira, serão inseridos componentes que contribuam com o balanceamento das portas, consequentemente, com a uniformização do consumo, independentemente de adicionar custos extras. Alguns possíveis custos, são: (1) área, (2) consumo energético e (3) frequência de operação do circuito.

2. METODOLOGIA

Esse trabalho propõe uma nova contramedida baseada. Essa estratégia é chamada de BSTTL e herda os benefícios da STTL e minimiza as suas desvantagens. Para alcançar isso, é proposto um novo arranjo de transistores que garante a simetria do caminho elétrico. A **Erro! Fonte de referência não encontrada.** demonstra as características da STTL e BSTTL, onde: (1) as capacitâncias intrínsecas penduradas nos fios, representada pelas letras C, (2) os fluxos de corrente para cada entrada estão representadas pelas linhas coloridas pontilhadas, (3) portas CMOS tradicionais utilizadas na lógica estão representadas pelas portas com fundo cinza e (4) Sx expressam as saídas, Ax e Bx são as entradas, onde x pode expressar: 1 lógica direta; 0 lógica complementar e v sinal de validação. Analisando a **Erro! Fonte de referência não encontrada.** (a) é observável que o arranjo possui quatro diferentes capacitâncias internas, a corrente percorre por diferentes números de caminhos e transistores. A **Erro! Fonte de referência não encontrada.** (b) representa a BSTTL proposta, sendo observável, que ela não apresenta nenhum dos problemas citados para STTL, através da adição e rearranjando dos transistores da lógica.

Para que seja possível quantificar a vulnerabilidade de um circuito sem realizar ataques, é necessário analisar as características de consumo, as mesmas características exploradas pelos ataques. Algumas métricas já são consolidadas para mensurar tais vulnerabilidades. Em BUCCI et al (2006) é utilizado a energia consumida pelas portas lógicas e também por um módulo composto por portas lógicas durante a computação de todas as possibilidades de dados de entrada. A partir destas energias, seus desvios padrões e variâncias é possível estimar sua vulnerabilidade aos ataques. As Equações 1, 2 e 3 utilizadas por Bucci et al. são apresentadas.



(a) (b)

Figura 1 - Representação NANDS 2: (a) STTL e (b) proposta BSTTL. Destacando: fluxos de correntes, capacitâncias intrínsecas, estímulos de entradas, arranjo transistores e desbalanceamento STTL

$$E = V_{dd} \int_0^t I_{dd}(t) d_t \quad (01)$$

$$NED = \frac{\max(E) - \min(E)}{\max(E)} \quad (02)$$

$$NSD = \frac{\sigma E}{\overline{E}} \quad (03)$$

A equação (01) representa a energia consumida para computar a operação, se aplicando tanto para a fase de carregamento, quanto para a fase de carregamento. As equações (02) e (03) representam duas métricas utilizadas pela literatura para determinar a robustez contra ataques DPAs. Onde, NED representa a Variação de Energia Normalizada (Normalized Energy Deviation) e NSD representa a Variação Padrão Normalizada (Normalizaded Standard Deviation). O atributo $\max(E)$ representa o consumo máximo entre os arcos e $\min(E)$ expressa o consumo mínimo, σE representa o desvio padrão de consumo de energia dos arcos e $\overline{E}$ calcula a média aritmética de consumo dos arcos.

As simulações serão realizadas utilizando FreePdk com tecnologia VLSI com canal do transistor de @45nm.

3. RESULTADOS E DISCUSSÃO

Este trabalho propõe uma nova topologia baseada em STTL que objetiva eliminar as discrepâncias e assimetrias que a mesma possui. Buscando confirmar as melhorias que a simetria provê no circuito, esse trabalho utiliza as métricas NSD e NED. Em três distintos cenários: (1) portas lógicas And2/Nand2, (2) AES Serpent SBox (Großschadl, Tilich, Rechberger, 2006) e (3) DES Sbox 1 (Biham, Shamir, 2007). A Tabela 1 representa esses dados, expondo a frequência de operação, o nível de segurança em NSD e NED e o consumo para cada um dos cenários descritos e fase lógica.

Os resultados demonstram que o balanceamento representa uma estratégia muito efetiva para homogeneização do consumo de energia. Considerando segurança, a BSTTL perde para STTL apenas na fase de processamento em 20%, enquanto representa melhoria em todos os outros cenários com ganhos variando entre 60% e 250%. Adicionalmente, a metodologia proposta é mais rápida na etapa

de pré-carregamento e mais lenta na etapa de processamento, enquanto ambas as topologias possuem um consumo similares.

Tabela 1 – Comparação entre BSTTL e STTL considerando: (1) frequência de operação, (2) NED, (3) NSD e (4) consumo de energia nas fases de pré-carregamento e processamento

circuito	Proporção BSTTL x STTL						Frequência (GHz)			
	Precarreg.			Process.			Precarreg.		Process.	
	NED	NSD	$\overline{E}$	NED	NSD	$\overline{E}$	BSTTL	STTL	BSTTL	STTL
And2	2.2	2.2	1.8	-1.2	-1.1	-1.6	20.5	19.2	10.6	18.8
AES	2.8	2.7	1.4	3.2	3.0	-1.2	3.4	2.9	1.4	1.8
DES	1.6	1.7	1.1	3.4	3.5	-1.1	1.2	1.0	0.5	0.6

4. CONCLUSÕES

Uma estratégia chamada BSTTL resistente a DPA foi introduzida e comparada com a antecessora STTL. O trabalho propõe um rearranjo em nível de transistores que foca na equalização e na uniformização no fluxo de corrente. Resultados experimentais confirmaram que a topologia proposta possui uma significativa melhora na homogeneização no consumo de energia.

Como trabalho futuro, pretende-se estender o balanceamento para diferentes circuitos, investigando a relação entre o consumo de energia e robustez contra ataques DPA. Adicionalmente, será investigada a relevância da estratégia de dimensionamento e balanceamento para diferente topologias.

5. REFERÊNCIAS BIBLIOGRÁFICAS

Biham, E., Shamir, A. “Differential Cryptanalysis of the Data Encryption Standard”. 1st ed., vol.1. Springer-Verlag: New York, 1993.

Großschadl, J., Tilich, S., Rechberger, C. “Energy Evaluation of Software Implementations of Block Ciphers under Memory Constraints”. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2007.

M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti. “Three-Phase Dual-Rail Pre-charge Logic”. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg, 2006.

P.C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and others Systems,” In 16th Annual International Conference on Advances in Cryptology, 1996, pp. 104-113.

RAZAFINDRAIBE, A., ROBERT, M., MAURINE, P. “Improvement of Dual Rail Logic as a Countermeasure Against DPA”. In: IFIP International Conference on Very Large Integration, 2007.