AVALIAÇÃO DA ESTRUTURA DE ATAQUE AO PADRÃO AES IMPLEMENTADO EM MICROCONTROLADORES

VINÍCIUS RENATO ROCHA GERALDO; VINÍCIUS VALDUGA DE A. CAMARGO

{vrrgeraldo, vvacamargo}@inf.ufpel.edu.br
Grupo de Arquitetura e Circuitos Integrados – GACI
Centro de Desenvolvimento Tecnológico - CDTec
Universidade Federal de Pelotas – UFPel

1. INTRODUÇÃO

Com o grande desenvolvimento das tecnologias e, consequentemente, com o aumento na troca de informações entre sistemas, principalmente por dispositivos voltados a Internet das Coisas (*Internet of Things* - IoT), a demanda por sistemas mais robustos em relação a segurança de dados ficou ainda mais evidente. Para isso, algoritmos criptográficos são uma das maneiras eficientes para proporcionar uma comunicação segura entre diferentes dispositivos. Em contrapartida, diferentes métodos de ataques aos dispositivos criptográficos foram desenvolvidos com o propósito de adquirir esses tais dados sigilosos. Devido à grande segurança oferecida pelos algoritmos a ataques computacionais, como o ataque por força bruta, técnicas de ataques em *hardware*, que se aproveitam da implementação física do algoritmo, ganharam destaque pela sua eficiência.

Ataques por canais laterais (*Side Channel Attacks* - SCA) se utilizam de propriedades físicas dos sistemas, como o consumo de energia ou emissão eletromagnética, para obtenção das informações sigilosas sem deixar rastros na invasão (KOCHER, 1999). Dentre os ataques baseados no consumo de energia, a Análise Diferencial de Potência (*Differencial Power Analysis* - DPA) foi a pioneira, este método estabelece relações estatísticas entre a potência consumida durante a execução do algoritmo e a chave secreta deste (KOCHER, 1999). Com o passar dos anos, novas técnicas de ataque foram sendo aperfeiçoadas para obter a chave secreta do circuito de maneira mais eficiente. O ataque conhecido como Análise da Correlação de Potência (*Correlation Power Analysis* - CPA), publicado por Brier (2004), é amplamente utilizado até hoje pois este reduz a quantidade de traços necessários para se estabelecer uma relação entre o consumo energético e a chave criptográfica em relação ao DPA.

O Padrão de Criptografia Avançada (*Advanced Encryption Standard* - AES), estabelecida pelo *National Institute of Standards and Technology* (NIST) em 2011, é amplamente utilizado em dispositivos criptográficos. O AES é baseado em 10, 12 ou 14 rodadas (dependendo do número de bits da chave secreta), cada uma delas passando por um bloco conhecido como sbox onde se faz a cifragem baseada na chave secreta. Como todo algoritmo criptográfico, o AES está sujeito a ataques por canais laterais. Para reduzir a eficiência desses ataques, são implementadas estratégias que visam diminuir a fuga de informações exploradas pelos SCA. Estas estratégias são denominadas contramedidas.

Este trabalho visa explorar a eficiência de duas contramedidas implementadas em microcontroladores a ataques CPA. Em microcontroladores, por não se ter acesso ao *hardware*, as contramedidas implementadas devem ter o caráter de mascaramento, visando descorrelacionar a potência e a chave secreta por meio da adição de técnicas de confusão e adição de ruído. As duas contramedidas avaliadas são descritas a seguir.

A primeira implementação realiza passos lineares para proteção por meio de um mascaramento de primeira ordem, ou seja, é utilizada uma máscara para cada rodada do AES. O método de tabela de recomputação (KOCHER, 1999) é utilizado. Um embaralhamento entre o processamento linear e o processamento das Sbox é feito. As operações *ShiftRows* e *MixColumns* são feitas em ordem randômica. No restante deste artigo, esta será referenciada como AESv1.

A segunda implementação consiste em um mascaramento voltado para a aleatoriedade das etapas realizadas do AES para encriptação, sendo tais como *AddRoundKey, SubBytes, ShiftRows* e *MixColumns*, de maneira a refazer todo o mascaramento para cada operação, sendo então uma segunda ordem de mascaramento. Detalhes desta implementação são encontrados em (FUMAROLI 2011). No restante deste artigo, esta será referenciada como AESv2.

2. METODOLOGIA

Nesse trabalho será avaliada a quantidade de amostras e traços necessárias para extração da chave secreta, e avaliar a robustez desses algoritmos com ataques do tipo CPA. As duas implementações descritas na introdução serão comparadas com uma terceira implementação sem contramedidas, referida no restante deste texto como TinyAES. A aquisição de dados de potência (traços) será feita através da placa *ChipWhisperer* (O'FLYNN, 2014). Esses traços são posteriormente transmitidos para o computador onde o ataque é realizado. A comunicação da placa com o computador feito através de um cabo USB conectado à placa de aquisição dos traços. Os traços ficam armazenados em um ambiente de programação para desenvolvimento dos ataques. A Figura 1 mostra um exemplo de traço de consumo da arquitetura TinyAES.

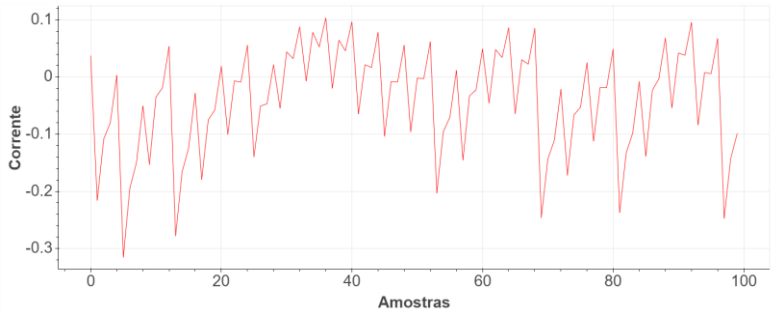

Figura 1 - Traço de consumo retirado do algoritmo AES sem contramedidas

Podemos descrever os traços por dois eixos, corrente por quantidade de amostras, onde são definidos quando realizamos a captura dos traços. No conjunto de dados retirados fazemos testes com ataques CPA de primeira ordem. Para isso, foram definidos ataques ao AES sem e com contramedidas para verificar a eficiência da segurança do sistema. O escopo de análise desenvolvido é em microcontroladores ATmega 128 bits (Atmega 128), no qual é imposto três algoritmos do AES. Avaliamos os resultados relacionados com cada configuração de experimento, dividindo em número de traços, amostras, algoritmo e tempo necessário para execução do ataque CPA.

Na definição de uma métrica para impor nos resultados empregamos adivinhação parcial de entropia (*Partial Guessing Entropy* – PGE), de tal forma que utiliza parâmetros de entropia de cada chave para realizar o seu ranqueamento para a possível chave correta, com o maior valor de correlação adota para subchave. Os valores indicados com 0 mostram o melhor ranqueamento da subchave (O'FLYNN, 2015).

3. RESULTADOS E DISCUSSÃO

A primeira avaliação realizada foi em relação ao tempo necessário para a execução de um ataque, seja esse bem sucedido ou não. Dois parâmetros são avaliados, a taxa de amostragem e o número de traços. Os resultados são sumarizados na Tabela 1. Ao avaliarmos os dados, podemos notar que o tempo de ataque independe da arquitetura atacada, porém tem um aumento com o número de traços assim como com a taxa de amostragem destes.

# Traços	*Amostras*	*Algoritmo*	*Tempo (s)*
5.000	10.000	TinyAES	1310
		AESv1	1697
		AESv2	2186
10.000	24.400	AESv1	5712
		AESv2	5891
40.000	3.160	TinyAES	4755
		AESv1	3975
		AESv2	4500
100.000	1.000	TinyAES	3875
		AESv1	4177
		AESv2	3311
100.000	316	TinyAES	4570
		AESv1	5067
		AESv2	3631
100.000	100	TinyAES	5464
		AESv1	3485
		AESv2	2896

Tabela 1 - Tempos de execuções de ataques CPA para cada configuração.

Os resultados obtidos para cada implementação são analisados em relação com a média dos PGE's da melhor hipótese de chave candidata a ser encriptada. Podemos desenvolver a fórmula da correlação com a seguinte equação:

$$\rho WH(R) = \frac{N\sum WiHi,R - \sum Wi \sum Hi,R}{\sqrt{N\sum Wi^2 - (\sum Wi)^2}\sqrt{N\sum Hi,R^2 - (\sum Hi,R)^2}} \quad (1)$$

Assim podemos definir como sendo *N* o conjunto de traços de consumo *Wi* e um *N* associado a um conjunto randômico de dados *Mi*, para assim dado um estado de referência *R* para palavras produzidas no conjunto de *N* valores pela distância Hamming *Hi,R* (BRIER, 2004).

A Figura 2 mostra a relação da média do PGE com a quantidade de traços. Assim vemos o TinyAES obteve um grande sucesso em obter a chave em comparação as duas versões com contramedidas. Em grandes amostras o TinyAES extrai a chave rapidamente em poucos traços envolvidos na simulação, assim o exemplo que podemos ver é para 24,4 mega amostras por segundo, onde utilizamos apenas 50 traços e obtemos a chave do algoritmo, e verifica-se a relação de utilizar mais amostras no traços para realização dos ataques por conter mais pontos a serem comparados, ou seja, mais informação. As implementações com contramedidas não puderam ser quebradas se mostrando seguras a ataques realizados com setup proposto e o ataque CPA de primeira ordem.

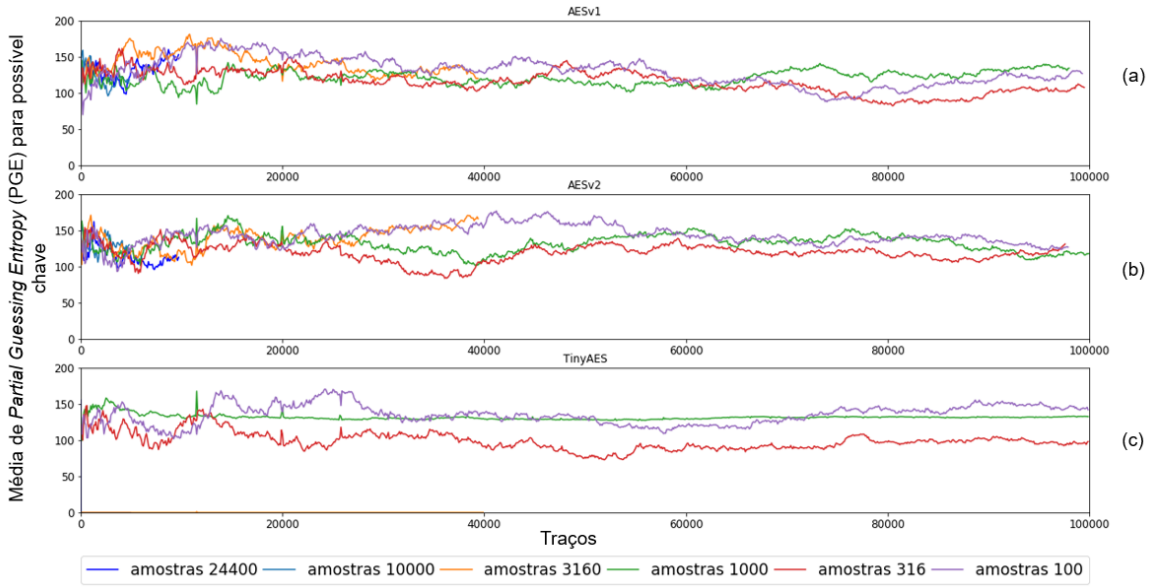

Figura 2 – Resultados para cada implementação de AES em PGE.
(a) AESv1, (b) AESv2, (c) TinyAES

4. CONCLUSÕES

Podemos notar que a eficiência dos SCA em sistema de microcontroladores contendo algoritmos criptográficos sem contramedidas. Porém vemos que ao adicionarmos contramedidas, o número de traços necessário para o sucesso do ataque aumenta, exigindo uma alta taxa de amostragem, aumentando o custo. O aumento da taxa de amostragem carrega um custo computacional na execução do ataque assim como um custo do equipamento de aquisição de dados que utiliza um conversor AD para digitalizar as informações de potência. Como trabalhos futuros serão realizados ataques CPA de ordens superiores e utilizando redes neurais para tentar quebrar as implementações com contramedidas apresentadas neste artigo.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ATMEGA128, Atmel. 8-bit Microcontroller datasheet. 2003. **USA, California: Atmel Corporation**.

BOTTINELLI, Paul; BOS, Joppe W. Computational aspects of correlation power analysis. **J. of Cryptographic Engineering**, v. 7, n. 3, p. 167-181, 2017.

BRIER, Eric; CLAVIER, Christophe; OLIVIER, Francis. Correlation power analysis with a leakage model. In: **Int. workshop on cryptographic hardware and embedded systems**. Springer, Heidelberg, 2004. p. 16-29.

FUMAROLI, Guillaume et al. Affine masking against higher-order side channel analysis. In: **Int. Workshop on Selected Areas in Cryptography**. Springer, Berlin, Heidelberg, 2010. p. 262-280.

KOCHER, Paul; JAFFE, Joshua; JUN, Benjamin. Differential power analysis. In: **Annu. int. cryptology conf.**. Springer, Heidelberg, 1999. p. 388-397.

O'FLYNN, Colin; CHEN, Zhizhang David. Chipwhisperer: An open-source platform for hardware embedded security research. In: **Int. Workshop on Constructive Side-Channel Analysis and Secure Design**. Springer, Cham, 2014. p. 243-260.

O'FLYNN, Colin; CHEN, Zhizhang David. Side channel power analysis of an AES-256 bootloader. In: **IEEE 28th Canadian Conf. on Electrical and Computer Engineering (CCECE)**. IEEE, 2015. p. 750-755.