Signal pre-processing to increase DPA success on GALS architectures

Autores:

Marcelo fay

Luciano Loder

Adão de Sousa Junior

Rafael Soares

SUMÁRIO

- Introdução
- Trabalhos relacionados
- Objetivos
- Técnicas de pré-processamento
- Experimentos realizados
- Conclusões e trabalhos futuros

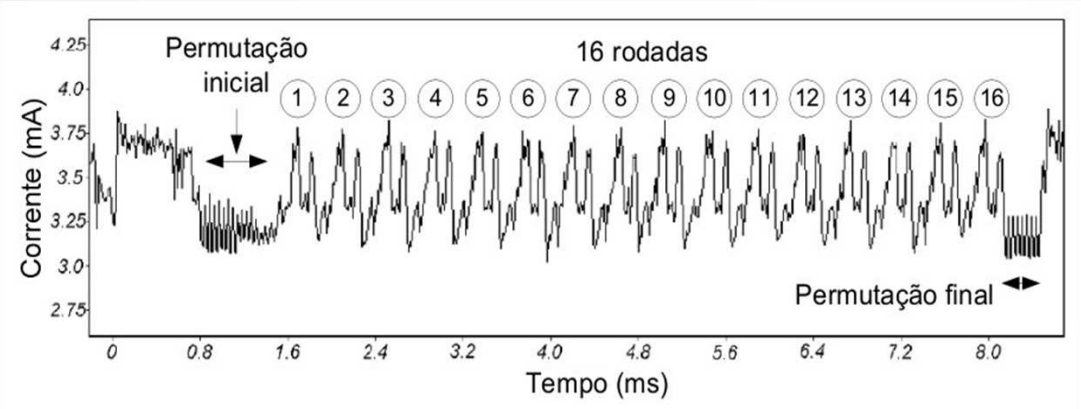
INTRODUÇÃO

- Evolução da Criptografia → Algoritmos robustos à violação de informações
- Criptoanálises (Ataques)
  - ciência de quebrar *textos encriptados*
    - explora falhas na lógica de algoritmos

- Nova classe de ataques → Kocher et al. 1996
  - Ataques por canais laterais (**Side Channel Attacks - SCAs)**
  - Correlacionam dados com grandezas físicas radiadas por dispositivos eletrônicos
    - Consumo de Potência: Differential Power Analysis – DPA
    - Radiação Eletromagnética: Differential ElectroMagnetic Analysis – DEMA
    - Tempo de computação: Timing Analysis - TA

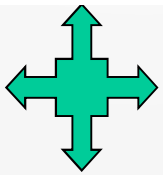
INTRODUÇÃO

Principais fatores que provocam a *fuga de informações* dos circuitos à SCA (vulnerabilidades)



Execução Síncrona do algoritmo DES

- Tecnologia de fabricação CMOS
  - Consumo de potência sensível a dados

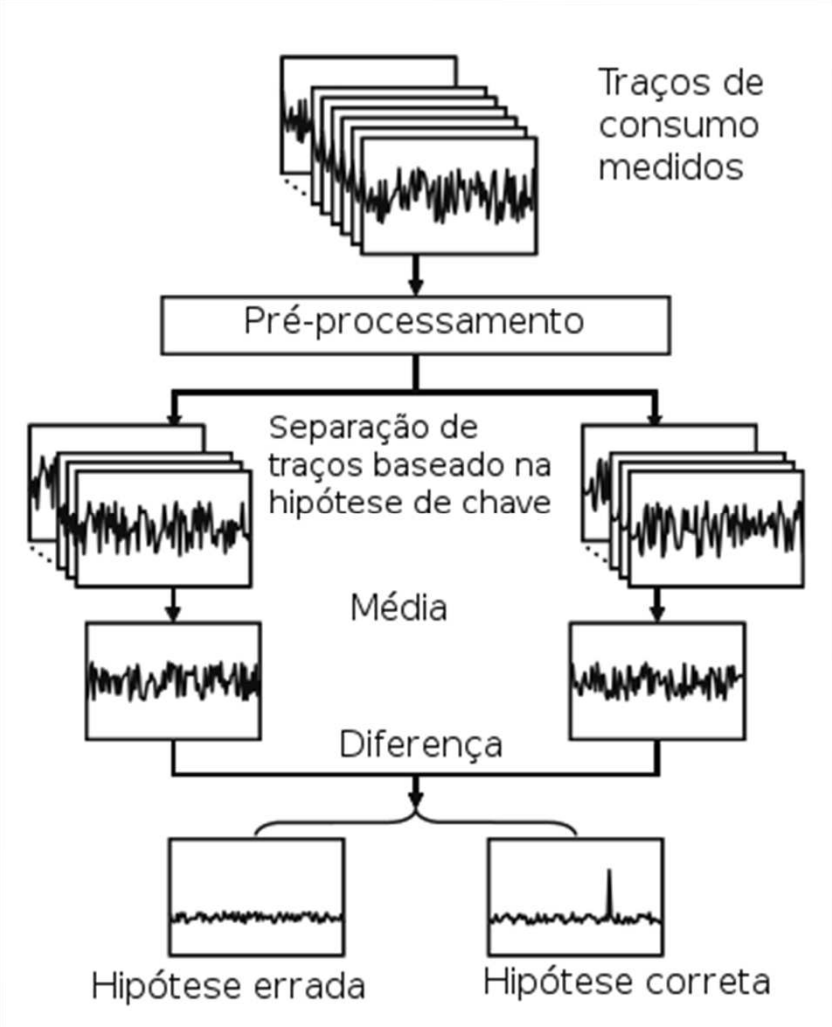


- Síntese Física (Place & Route)
  - Desequilíbrios no caminho de dados (capacitâncias parasitas)

- Paradigma síncrono
  - Operações sincronizadas (sinal global de relógio)

ATAQUES DPA

- Composto dos seguintes passos:
  - Medição dos traços de consumo de potência
  - Etapa de pré-processamento (opcional)
  - Separação dos traços de acordo com um valor intermediário
  - Média dos traços em cada grupo
  - Diferença entre a média dos grupos
  - Determinação da hipótese correta, de acordo com o pico de consumo de potência



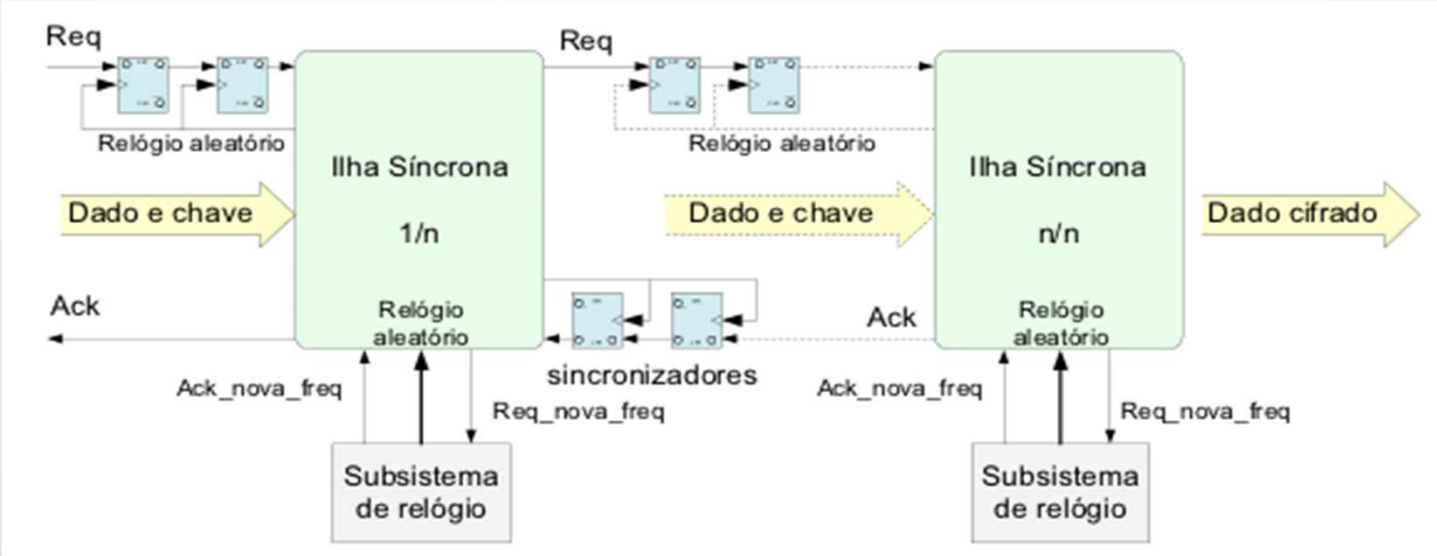
TRABALHOS RELACIONADOS

- Contramedidas a ataques DPA:
  - *Random Delay Insertion* – RDI:
  - caracterizado por Clavier et al. 2000
  - implementado em hardware por Lu et al. 2008
  - Variação da frequência de relógio do circuito por Avirneni et al. 2013

- Ataques DPA com alinhamento de traços:
  - Correlação de fase (POC) Nagashima et al. 2007
  - Correção estática de amplitude Real et al. 2008

ARQUITETURAS GALS PIPELINE

- Composta de “N” *ilhas síncronas* comunicando-se assincronamente (GALS)
- Cada ilha computa 1 ou mais rodadas do algoritmo de criptografia
- Frequências de relógio distintas e escolhidas randomicamente
- Introduzem atrasos no domínio do tempo e alteram a amplitude
- Processamento paralelo (Pipeline)



OBJETIVOS

- Investigar a vulnerabilidade das arquiteturas GALS pipeline a ataques DPA
- Avaliar o uso da etapa de pré-processamento para alinhamento de traços
- Avaliar a aplicação de filtro para aumentar a efetividade de ataques DPA.

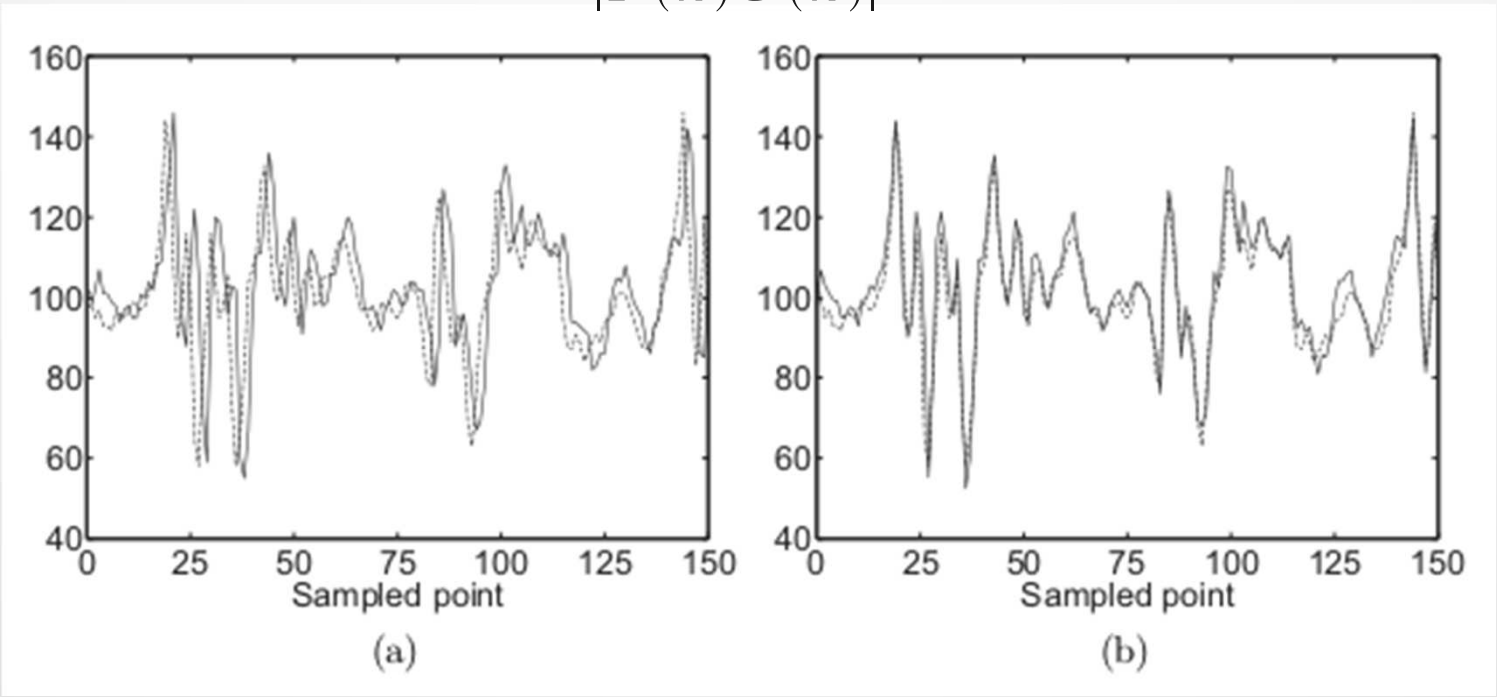
TÉCNICAS DE PRÉ-PROCESSAMENTO

- Analisar e classificar traços com mesma frequência de operação
- Domínio do tempo → Domínio de frequência
  - Aplicação da Transformada de Fourier (FFT): determinar a frequência de relógio da ilha sob ataque
  - Uso de janelamento do sinal evita o efeito de bordas (maior precisão da FFT)
    - Janelas de Hanning
    - Janelas de Hamming

TÉCNICAS DE PRÉ-PROCESSAMENTO

- Alinhamento por correlação de fase – POC:
- Avalia a diferença de fase entre traços

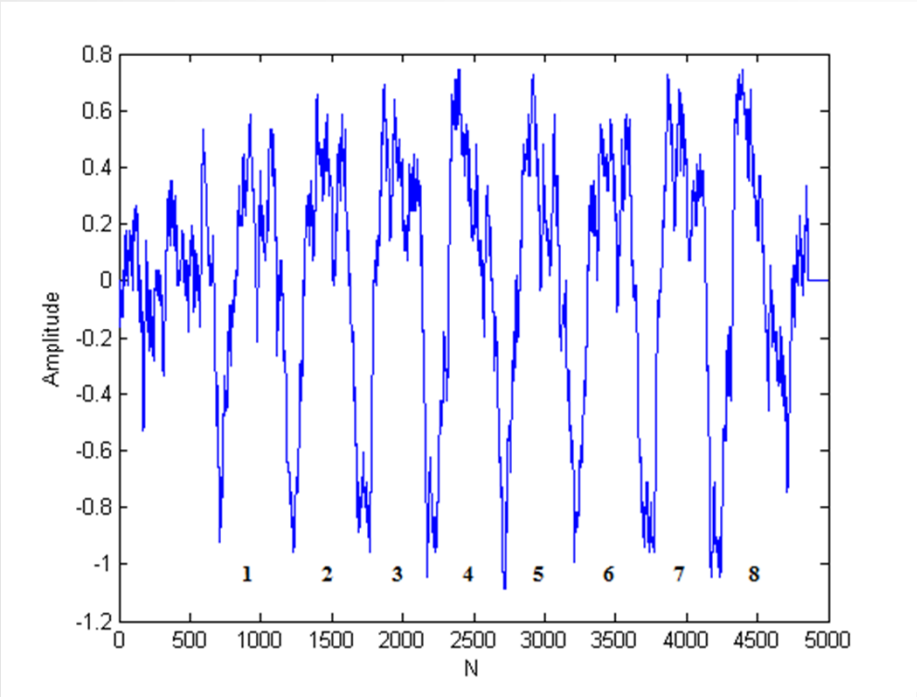
$$R_{FG}(k) = \frac{F(k)\overline{G(k)}}{|F(k)\overline{G(k)}|} \quad e^{j\frac{2\pi}{L}k\delta}$$

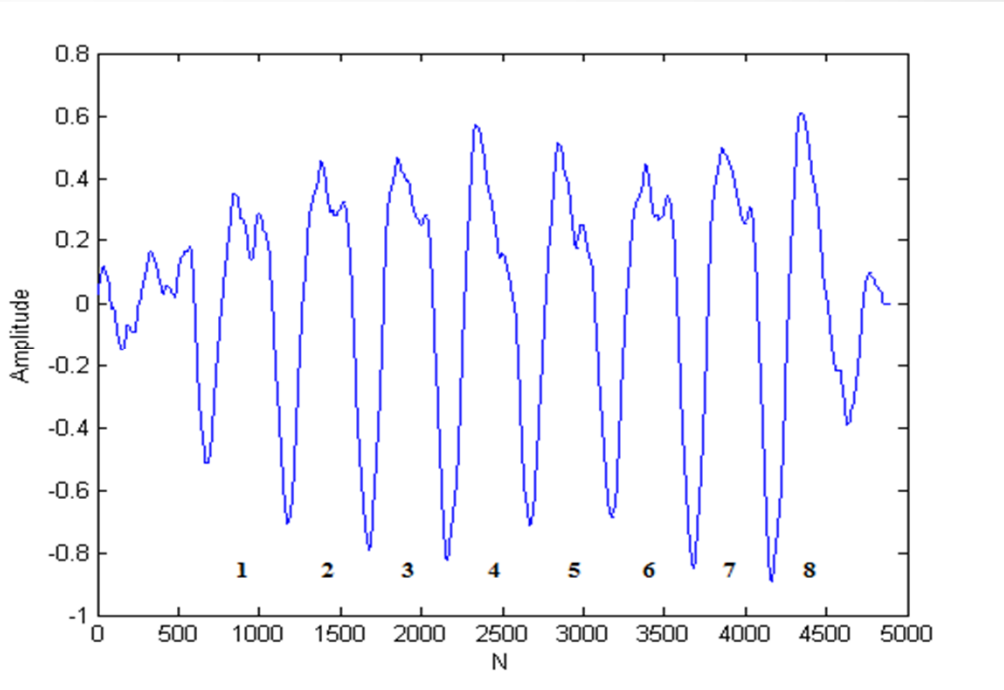


TÉCNICAS DE PRÉ-PROCESSAMENTO

- Filtro de médias móveis:
  - Filtro FIR passa-baixas:
  - Útil para redução do ruído

$$y[n] = \frac{1}{N} \sum_{k=0}^{N-1} x[n-k]$$





EXPERIMENTOS REALIZADOS

Resultados preliminares

(A) DPA sem pré-processamento							
sbox1	sbox2	sbox3	sbox4	sbox5	sbox6	sbox7	sbox8
24	63	33	51	09	54	53	61
21	03	13	20	53	35	33	42
40	21	31	08	61	25	32	5
-	-	-	-	-	-	-	-

- Arquiteturas GALS PIPE 2 estágios
- Prototipada em Xilinx Spartan3
- 100 mil traços adquiridos previamente
- MATLAB

(B) DPA com POC							
sbox1	sbox2	sbox3	sbox4	sbox5	sbox6	sbox7	sbox8
24	63	33	51	09	54	53	61
24	63	33	51	11	54	53	26
01	01	01	01	01	01	01	56
6943	**22130**	**29752**	**12211**	**27238**	**15987**	**33511**	**-**

(C) DPA com POC e filtro de médias móveis							
sbox1	sbox2	sbox3	sbox4	sbox5	sbox6	sbox7	sbox8
24	63	33	51	09	54	53	61
24	63	33	51	09	54	53	38
01	01	01	01	01	01	01	22
1290	**12932**	**18836**	**4790**	**21516**	**15987**	**13886**	**-**

CONCLUSÕES E TRABALHOS FUTUROS

Conclusões

- Aplicação de técnicas DSP mostram-se eficientes para alinhar traços
- Traços com frequências iguais ou próximas, alinhadas por correlação de fase aumentam a taxa de sucesso de DPA
- Redução de ruídos de alta frequência também apresentou redução no número de traços necessário para o sucesso de DPA.

Trabalhos futuros

- Avaliar o alinhamento de amplitude dos traços (frequências ≠s)
- Avaliar a frequência de corte do filtro FIR
- Revisar outras técnicas de alinhamento de traços