Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability

Peter Pessl, Stefan Mangard
IAIK, Graz University of Technology, Austria

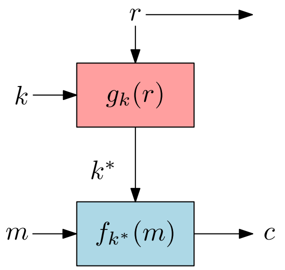
CT-RSA 2016, San Francisco, 3rd March 2016

Overview

- New side-channel attack on Fresh Re-Keying and binary-field multiplication
  - Relation to Learning Parity with Noise (LPN) problem
  - Extensive use of bit reliabilities in order to decrease runtime
- Attack a protected Fresh Re-Keying implementation
  - Using only 512 traces
  - With reasonable runtime

Fresh Re-Keying [MSGR10, MPR$^+$11]

- Goal: SCA protection for low-cost devices
- Combine an encryption function f
- With a re-keying function g
- *Fresh* session key k^* per invocation
  - f is SPA secure
  - g is DPA secure, but not *cryptographically strong*



Re-Keying Function

- Polynomial multiplication modulo $y^{16} + 1$ over GF(2^8)
  - Good diffusion
  - Easy to protect (masking, shuffling)
- Rewrite as matrix-vector product over bytes and bits
  - Linear equation in master-key bits

$$\begin{pmatrix} r_0 & r_{15} & r_{14} & \cdots & r_1 \\ r_1 & r_0 & r_{15} & \cdots & r_2 \\ r_2 & r_1 & r_0 & \cdots & r_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{15} & r_{14} & r_{13} & \cdots & r_0 \end{pmatrix} \begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ \vdots \\ k_{15} \end{pmatrix} = \begin{pmatrix} k_0^* \\ k_1^* \\ k_2^* \\ \vdots \\ k_{15}^* \end{pmatrix}$$

SCA of Binary-Field Multiplication

Attacks of Belaïd et al. [BFG14, BCF+15]

- Multiplication in $GF(2^n)$
  - Constant secret $\times$ public random value
- Noisy Hamming weight of each n-bit product
  - With, e.g., $n = 128$
  - Round to either 0 or $2^n - 1$
- Linear equations in bits, but with errors

LPN - Learning Parity with Noise

Definition: Learning Parity with Noise

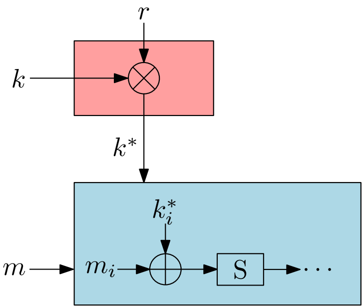
- ν equations $b_i = \langle \mathbf{a}_i, \mathbf{k} \rangle + e_i$
- Secret **k**, public random $\mathbf{a}_i$ (bit vectors), $\mathrm{P}(e_i = 1) = \epsilon$
- find **k**

Solving algorithms

- BKW-based (high ν, sub-exponential runtime) (used by Belaïd et al.)
- Linear decoding (low ν, exponential runtime)

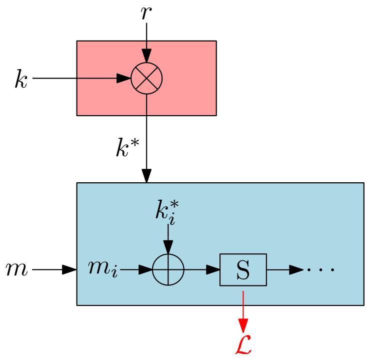
Our Attack

Chosen Target



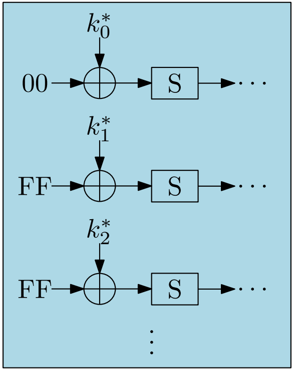
- Protected Fresh Re-Keying implementation (8-bit software) [MPR+11]
- Multiplication: masked and shuffled
- AES: shuffled

Template Attack on the S-box



- Product k^* is used in AES
  - AES *only* SPA secure
- Templates on S-box
- Probability vector for key-bytes
- Turn them into bit-wise probabilities

Countering the Shuffling



- Application: challenge-response auth.
  - Reader choses plaintexts
- Chosen fixed plaintext: $(00)||(FF)^{15}$
- Templates for both cases
  - Reveal one position
  - Independent of permutation generation

Outcome of the physical attack

- Vector of probabilities for session-key bits b
  - $p_b = \mathrm{P}(b = 1)$, bias $\tau_b = |p_b - 0.5|$
  - Classification: $b = \lfloor p_b \rceil$, $\epsilon_b = 0.5 - \tau_b$
- Each entry a LPN sample
  - but with additional information (ϵ_b)

A New LPN Variant

Definition: Learning Parity with Variable Noise

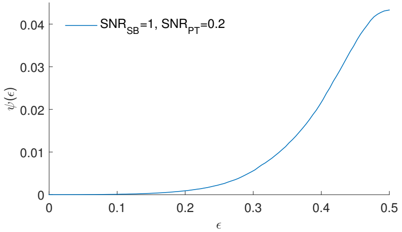
- ν equations $b_i = \langle \mathbf{a}_i, \mathbf{k} \rangle + e_i$
- Secret **k**, public random **a** (bit vectors)
- $P(e_i = 1) = \epsilon_i$, ϵ_i sampled from meta-distribution ψ
- Find **k**

Incorporation of ϵ_i might lead to faster algorithms.

Our LPVN algorithm

Filtering

- Discard samples with high ϵ_b
- Similar to Belaïd et al., but bit-wise



Linear Decoding

- Tweaked algorithm incorporating probabilities

LPN and Decoding

Decoding problem:

- Given a generator matrix $\mathbf{G}$ and noisy word $\mathbf{y} = \mathbf{G}' \cdot \mathbf{k} + \mathbf{e}$
- find $\mathbf{e}$ or $\mathbf{k}$

Syndrome decoding:

- Check matrix $\mathbf{H}$ and syndrome $\mathbf{s} = \mathbf{Hy} = \mathbf{He}$
- Search for $\mathbf{e}$ (w columns of $\mathbf{H}$ with sum $\mathbf{s}$)

Stern's Algorithm

- Randomly partition columns of **H** into sets $\mathcal{Q}, \mathcal{I}$
- Transform $\mathcal{I}$ to identity, search for errors of particular form
- Optimization: swap columns between $\mathcal{Q}$ and $\mathcal{I}$ [BLP08]

$$\mathbf{H}_p = (\mathcal{Q}|\mathcal{I}) = \left(\begin{array}{ccc|c} \overbrace{1\ \ 0\ \ 0 \cdots}^{k/2:\ p \text{ err.}} & \overbrace{\cdots 0\ \ 1\ \ 0}^{k/2:\ p \text{ err.}} & \overbrace{1 \quad\quad}^{\ell:\ 0 \text{ err.}} & \\ 1\ \ 1\ \ 0 \cdots & \cdots 0\ \ 0\ \ 0 & \quad 1 & \\ 0\ \ 1\ \ 1 \cdots & \cdots 1\ \ 1\ \ 1 & \quad\quad 1 & \\ \vdots & \vdots & & \ddots \\ 0\ \ 1\ \ 1 \cdots & \cdots 1\ \ 0\ \ 1 & & \quad 1 \end{array}\right)$$

Tweaked Stern

- Each entry of **e** / column of **H** corresponds to LPN sample
  - with attached probability
- Reliability-guided swapping of columns
  - Keep number of errors in $\mathcal{Q}$ low
  - While still behaving randomly

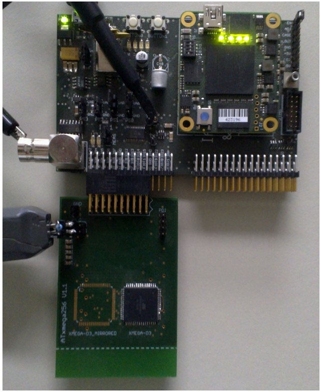
Attack Results

Simulation

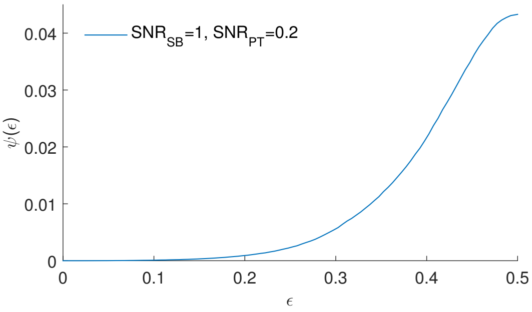
- 8-bit with shuffling countermeasure
- Noisy Hamming weights

Real device

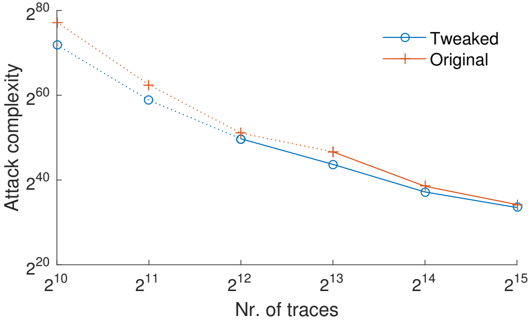
- Power measurements
- Profiling



Results - Simulation

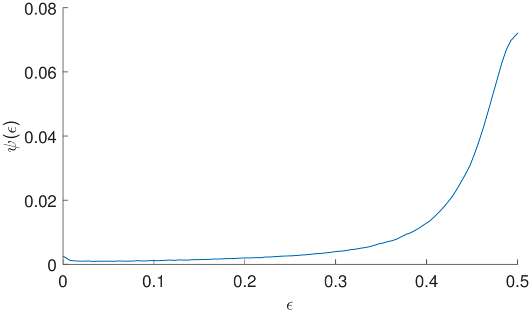


Meta-probability $\psi(\epsilon)$

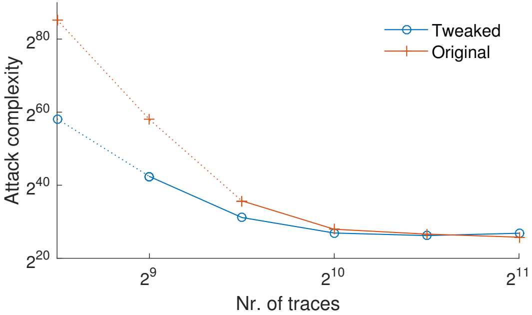


Runtime complexity

Results - Real Device



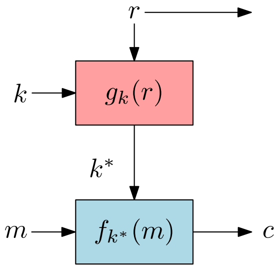
Meta-probability $\psi(\epsilon)$



Runtime complexity

Conclusions

- Attack with small trace count and reasonable runtime
  - Without violating the constraints (AES still SPA secure)
- Implications for Fresh Re-Keying
  - Separations of responsibilities not trivial
  - Protect re-keying output in all stages



S C I E N C E ▪ P A S S I O N ▪ T E C H N O L O G Y

Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability

Peter Pessl, Stefan Mangard
IAIK, Graz University of Technology, Austria

CT-RSA 2016, San Francisco, 3rd March 2016

Bibliography I

[BCF+15] Sonia Belaïd, Jean-Sébastien Coron, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, and Emmanuel Prouff. Improved Side-Channel Analysis of Finite-Field Multiplication. *IACR Cryptology ePrint Archive*, 2015:542, 2015. note: to appear at CHES 2015.

[BFG14] Sonia Belaïd, Pierre-Alain Fouque, and Benoît Gérard. Side-Channel Analysis of Multiplications in GF(2^{128}) - Application to AES-GCM. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014*, volume 8874 of *Lecture Notes in Computer Science*, pages 306–325. Springer, 2014.

[BLP08] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Attacking and Defending the McEliece Cryptosystem. In Johannes A. Buchmann and Jintai Ding, editors, *Post-Quantum Cryptography, Second International Workshop, PQCrypto 2008*, volume 5299 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2008.

[MPR+11] Marcel Medwed, Christophe Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert. Fresh Re-keying II: Securing Multiple Parties against Side-Channel and Fault Attacks. In Emmanuel Prouff, editor, *Smart Card Research and Advanced Applications - 10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011*, volume 7079 of *Lecture Notes in Computer Science*, pages 115–132. Springer, 2011.

[MSGR10] Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni. Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. In Daniel J. Bernstein and Tanja Lange, editors, *Progress in Cryptology - AFRICACRYPT 2010*, volume 6055 of *Lecture Notes in Computer Science*, pages 279–296. Springer, 2010.