A Stochastic Approach in Side-Channel Analysis in the Presence of Masking

W. Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany

Barcelona, May 22, 2007
Power attacks on a block cipher implementation protected by masking

- (Classical) template attacks: most powerful attack, but gigantic workload (= # of measurements) for profiling
- Second order DPA: no profiling, but only little efficient
The Stochastic Approach
(Example: Power attack on AES)

\[ x \in \{0,1\}^8 \text{ (known) part or the plaintext or ciphertext} \]
\[ z \in \{0,1\}^8 \text{ masking value} \]
\[ k \in \{0,1\}^8 \text{ subkey} \]
\[ t \text{ time} \]

**Time t:** \[ I_t(x,z;k) = h_t(x,z;k) + R_t \]

- Random variable (depends on \( x,z,k \))
- Deterministic part (depends on \( x,z,k \))
- Random variable \( E(R_t) = 0 \)
- Noise

quantifies the randomness of the side-channel signal at time \( t \)
Naïve Approach: Estimate $h_t(x,z;k) = \mathbb{E}(I_t(x,z;k))$

independently for each triple $(x,z;k) \in \{0,1\}^8 \times \{0,1\}^8 \times \{0,1\}^8$

for all $t \in \{t_1, t_2, \ldots, t_m\}$ (relevant instants)

Drawback: Gigantic number of measurements
For any fixed subkey $k$ interpret the function $h_{t;k}(\cdot,\cdot): \{0,1\}^8 \times \{0,1\}^8 \rightarrow \mathbb{R}$, $h_{t;k}(\cdot,\cdot) = h_t(\cdot,\cdot;k)$, as an element of a real vector space $F$. Approximate $h_{t;k}(\cdot,\cdot)$ by its image $h^*_{t;k}$ under the orthogonal projection onto a suitably chosen low-dimensional vector subspace $F_{u;t}$. geometric visualization
r (clou) The image $h^*_{t;k}$ minimizes a functional on the vector subspace $F_{u;t}$

$h^*_{t;k}$ can be determined without knowing $h(.,.,.,k)$

r (Qualitative) conjectures on the reasons for the leakage signal $\rightarrow$ subspace $F_{u;t}$

r Typical vector space dimensions ($\rightarrow$ Example)
  r $\dim(F) = 2^{16}$
  r $\dim(F_{u;t}) = 9$ or $17$
Comparison with Template Attacks

Non-masking case:
- introduced by Schindler, Lemke, Paar (CHES 2005)
- extensive experimental studies by Gierlichs, Lemke, Paar (CHES 2006)
  - Compared to template attacks: reduces the number of measurements in the profiling phase up to factor 50

Masking case:
The advantages of the stochastic approach are even by an order of magnitude larger than in the non-masking case.
Summary

The stochastic approach

- reduces the profiling workload by order(s) of magnitude
- combines engineer’s insight into the reasons for the leakage (→ suitability of the subspace $F_{u;t}$) with precise stochastic methods (→ optimal approximator in $F_{u;t}$)
- identifies and quantifies those properties that have significant impact on the side-channel signal
- supports constructively the design of security implementations
Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Werner Schindler  
Godesberger Allee 185-189  
53175 Bonn

Tel: +49 (0)3018-9582-5652  
Fax: +49 (0)3018-10-9582-5652

Werner.Schindler@bsi.bund.de  
www.bsi.bund.de  
www.bsi-fuer-buerger.de
A Stochastic Model for Particular Designs of Physical RNGs with Robust Entropy Estimators

Wolfgang Killmann $^1$, Werner Schindler $^2$

$^1$ T-Systems GEI GmbH
Bonn, Germany

$^2$ Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bonn, Germany

Barcelona, May 22, 2007
Generic Design

\[ r_{n+1} = r_n + sw(n+1) \pmod{2} \]

\# switches in time period \( n+1 \)
Summary

- Goal: Determine the conditional entropy
  \[ H(R_{n+1} \mid R_1, \ldots, R_n) \]
- We formulated and analysed a stochastic model of the noise source.
- We derived robust entropy estimators, yielding practically useful lower entropy bounds.

Practical experiments:
10^5 random bits / sec (limitations by the USB interface)
entropy / random bit > 1 - 10^{-5}
Contact

Wolfgang Killmann
T-Systems, GEI GmbH,
Bonn, Germany
wolfgang.killmann@t-systems.com

Werner Schindler
Bundesamt für Sicherheit in der
Informationstechnik (BSI),
Bonn, Germany
Werner.Schindler@bsi.bund.de