Differential Power Analysis of the HMAC Algorithm

Robert P. McEvoy, Michael Tunstall, Claire Whelan, Neil Hanley, Colin C. Murphy and William P. Marnane

Coding & Cryptography Research Group, Department of Electrical & Electronic Engineering, University College Cork, IRELAND

E-mail: {robertmce, miket, clairew, neilh, cmurphy, liam}@eleceng.ucc.ie

1. The HMAC Algorithm

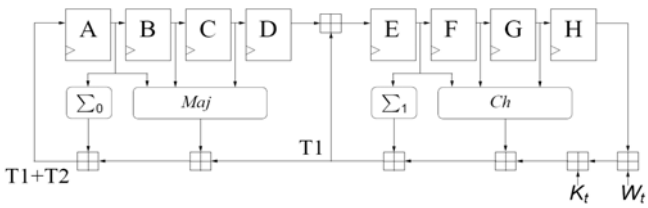
- HMAC = keyed-**H**ash **M**essage **A**uthentication **C**ode
- Used in IPSec & TLS protocols for authentication & integrity
- Hash functions are not usually considered as targets for side-channel attacks, as they are mostly used to process non-secret information. However, HMAC handles the secret key:

$$HMAC_k(x) = H((k \oplus opad) \,||\, H((k \oplus ipad) \,||\, x))$$

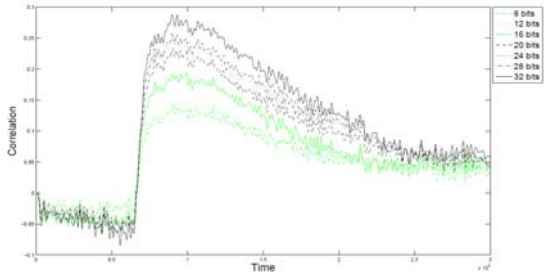
- k = secret key
  ipad, opad = fixed public paddings
  x = message to be authenticated (variable)
- In the hash function H, **known variable** data mixes with **fixed unknown** data → DPA attack is theoretically possible
- Attack would signatures for chosen messages to be forged
- Here, we present practical 1st-order attacks on HMAC-SHA-2 and HMAC-Whirlpool, and design countermeasures

2. Attacking HMAC-SHA-2

- SHA-2 family (**S**ecure **H**ash **A**lgorithm) is a well-known set of dedicated hash functions, standardised by NIST
- SHA-2 Compression Core:



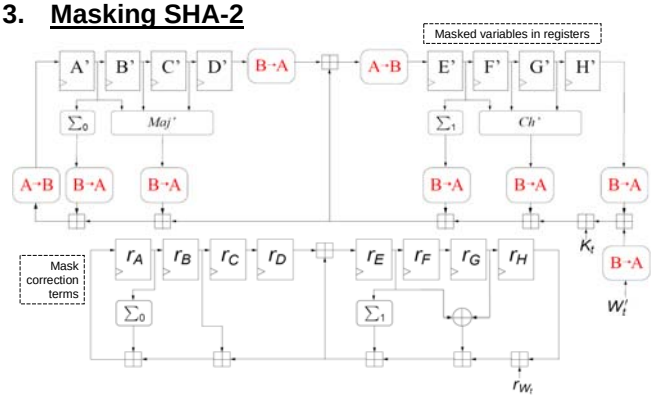
- Goal of DPA attack on HMAC-SHA-2 is to recover fixed intermediate hash of $(k \oplus ipad)$, i.e.
  Fixed unknown data: initial states of registers A, B, C, …, H
  Known variable data: message schedule W_t
- A – H can be recovered using seven DPA attacks [1]
  However, in SHA-256 the variables are 32-bit, and in SHA-512 the variables are 64-bit
  → Attack is difficult in practice
- Attack is simplified using **Partial Correlation** technique [2, 3]



Correlation and partial correlations between the power consumption and hypothesis for E, given the correct prediction of D and the previous state of E.

- **Partial Correlation:**
  Predict 32 bits → Correlation = ρ
  Predict n bits → Correlation = $\rho\sqrt{n/32}$
  → Can make hypotheses on smaller sets of bits at a time
- Keep only those hypotheses with highest partial correlations (extend-and-prune approach)
- Build up partial correlations from 4 → 32 bits; much less computation than attempting immediate full 32-bit correlation.

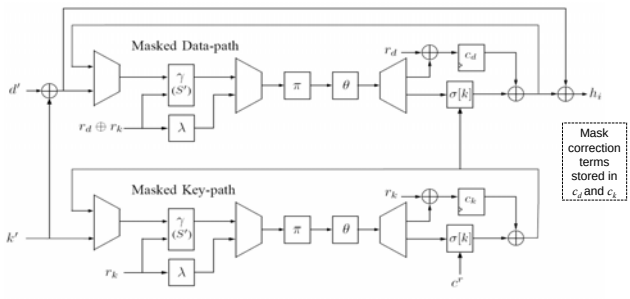
3. Masking SHA-2



- Masked circuits designed for *Ch* and *Maj* functions [1]
- Boolean-to-Arithmetic and Arithmetic-to-Boolean conversions optimised for FPGA using dedicated **carry chain**

4. HMAC-Whirlpool: Attack & Masking

- Whirlpool hash function recommended in *NESSIE* portfolio. Block cipher-based, similar to AES
- Similar attack goal to HMAC-SHA-2 case: recover secret intermediate chaining state
- Attack is less complex due to Whirlpool S-box:
  Processes each byte of the 512-bit state independently
  → Can focus on 8-bit intermediate variables in the DPA attack
- Masked circuit [4]:



- Masked S-box S' = 5 masked 4-bit pre-computed look-up tables. Re-use of round function transformations to compute mask correction → negligible area impact
- **Future work**: Consider template attacks & higher order attacks
  Future hash functions? (NIST Hash Function Competition)

References

[1] R. McEvoy, M. Tunstall, C. C. Murphy, and W. P. Marnane. Differential Power Analysis of HMAC based on SHA-2, and Countermeasures. In *Workshop on Information Security Applications, WISA 2007*
[2] E. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems — CHES 2004, 6th International Workshop*
[3] M. Tunstall, N. Hanley, R. McEvoy, C. Whelan, C. C. Murphy and W. P. Marnane. Correlation Power Analysis of Large Word Sizes. In *Irish Signals and Systems Conference, ISSC 2007.*
[4] R. McEvoy, M. Tunstall, N. Hanley, C. C. Murphy and W. P. Marnane. Protecting HMAC-Whirlpool Against Differential Power Analysis Attacks. In preparation.

Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 2007

Supported in part by: embarkinitiative Investing in People and Ideas