1. The HMAC Algorithm

- HMAC = keyed-hash Message Authentication Code
- 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:

\[
\text{HMAC}_k(x) = H((k \oplus \text{ipad}) \parallel H((k \oplus \text{ipad}) \parallel x))
\]

- \(k\) = 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 \(\Rightarrow\) 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 (Secure Hash Algorithm) is a well-known set of dedicated hash functions, standardised by NIST
- SHA-2 Compression Core:

\[
\begin{align*}
\Sigma_c & = \text{Maj} \\
\Sigma_r & = \text{Ch} \\
K_1 & = \text{ipad} \\
W_t & = \text{msg schedule}
\end{align*}
\]

- Goal of DPA attack on HMAC-SHA-2 is to recover fixed intermediate hash of \((k \oplus \text{ipad})\), 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]

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 \(\Rightarrow\) negligible area impact
- Future work: Consider template attacks & higher order attacks

References

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