Differential Power Analysis

Paul Kocher, Joshua Jaffe, and Benjamin Jun
Cryptography Research, Inc.

Presented by Hyun Bin Lee

Note: If not specified, figures are borrowed from the original paper.

Motivation

- Attacks that involve multiple parts of system can create security faults when each level of system's design makes unrealistic or incomplete assumption on each other.
- Most modern cryptographic devices are implemented using semiconductor logic gates. When charge is applied to a transistor's gate, the gate consumes power and produce electromagnetic radiation.
- One can measure circuit's power consumption with "extraordinary high rates with excellent accuracy".

Simple Power Analysis (SPA)

- A technique that involves directly interpreting power consumption measurements collected during cryptographic operations

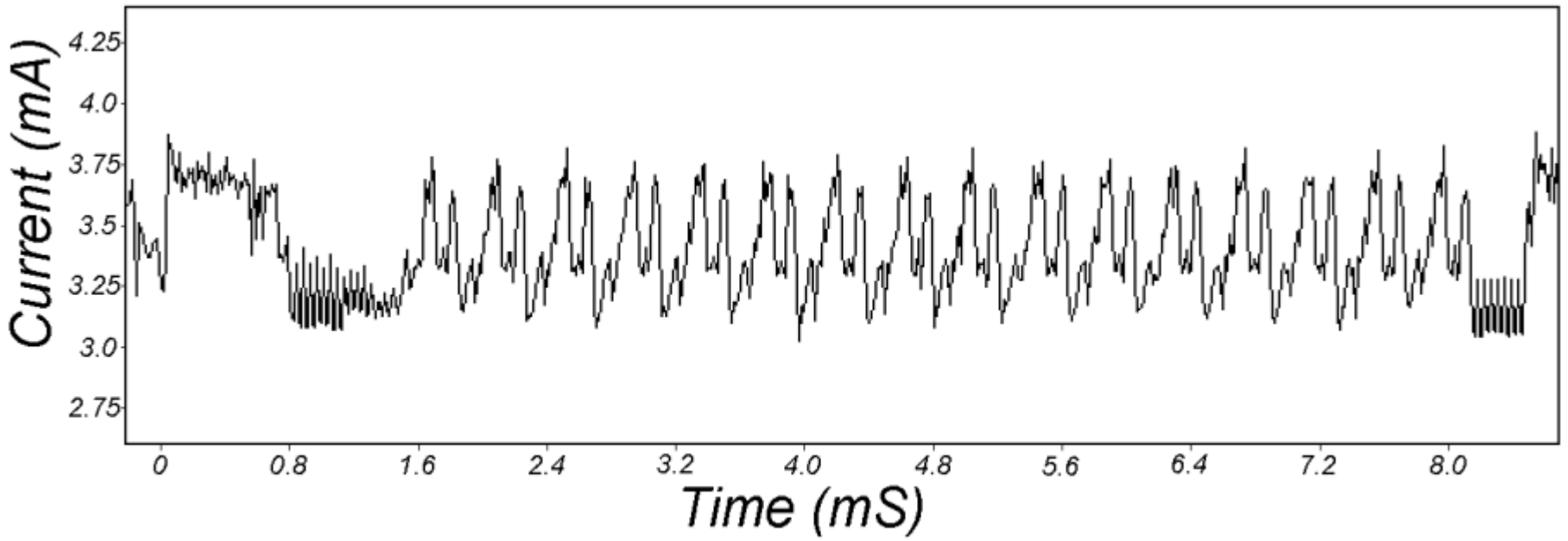


Figure 1: SPA trace showing an entire DES operation.

SPA (cont.)

- SPA can spot discernable features from power measurement traces

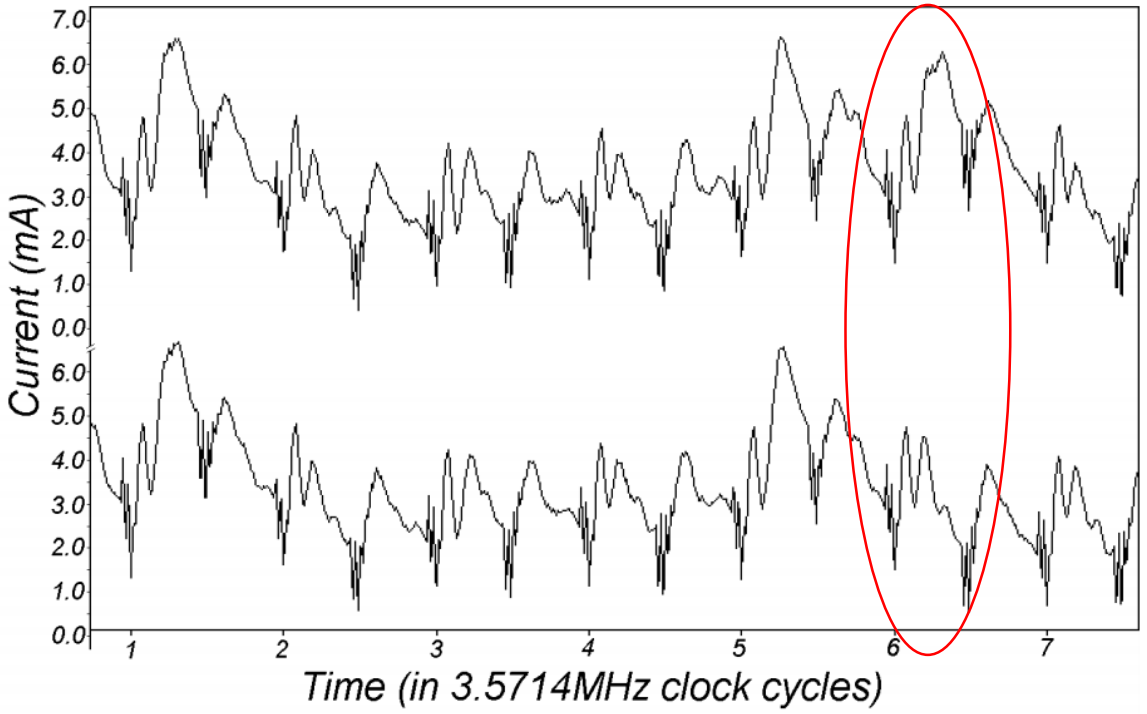


Figure 3: SPA trace showing individual clock cycles.

SPA (cont.)

- SPA can be exploited to examine DES operations

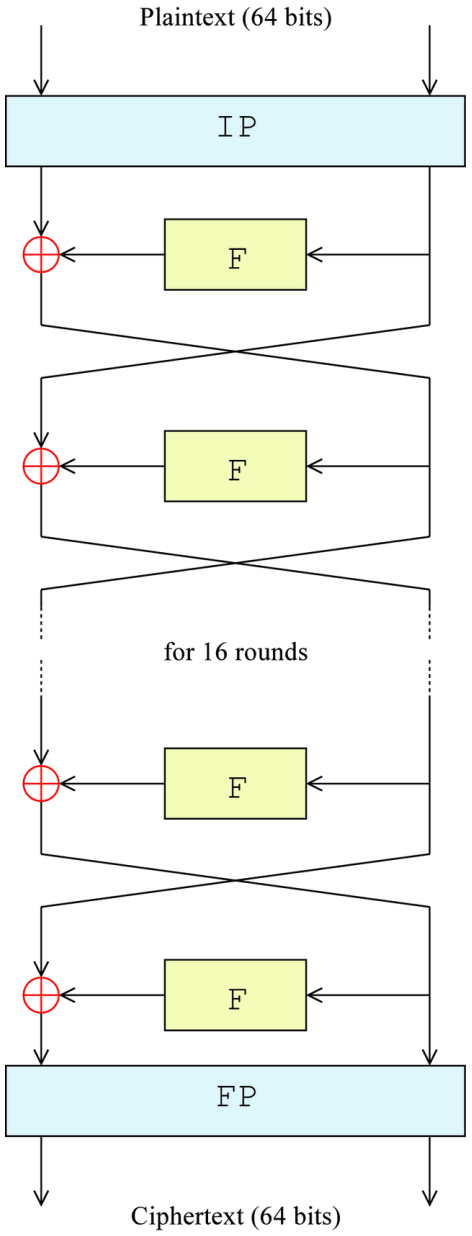
1. DES key schedule
2. DES permutations
3. Comparisons (string or memory)
4. Multipliers
5. Exponentiators

- SPA can be prevented with avoiding procedures that use secret intermediates or keys for conditional branching operations

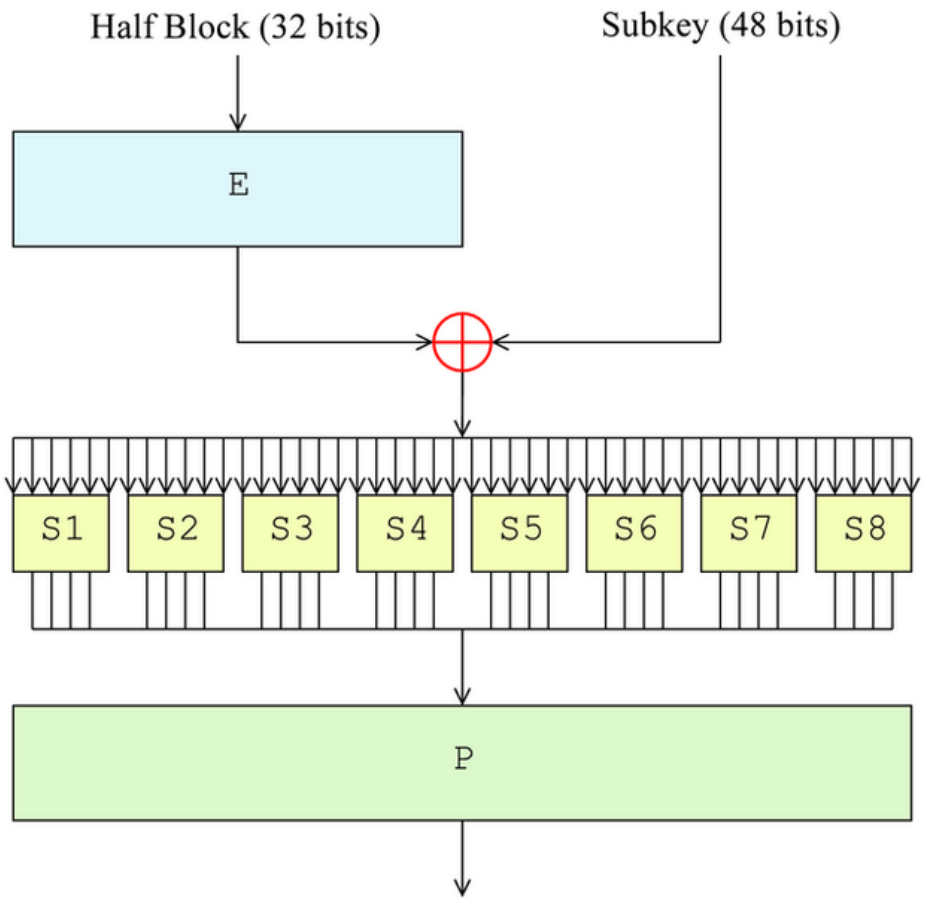
Data Encryption Standard (DES)

- A block cipher (64 bit block size & (56 + 8) bit key)
- Composed of 16 rounds of Feistel (F) function
- Feistel function is composed of

1. Expansion
2. Key mixing (with each round's subkey)
3. Substitution
4. Permutation



DES (cont.)



Differential Power Analysis against DES

The DPA selection function D(*C*, *b*, *K_s*)

- Computing bit *b* of the DES intermediate L at the beginning of 16^{th} round for Ciphertext *C*
- *K_s* refers to 6 key bits entering the S-box
- If *K_s* is incorrect, the selection function will guess correctly with probability of ½.
- If *K_s* is correct, the selection function will always guess correctly.

DPA (cont.)

- An attacker observes *m* encryption operations (*m ciphertexts)* and captures power traces with *k* samples each (T_1 … *m*[1 … *k*])
- Computes a k-sample differential trace by finding the difference between the average of the traces for which D(*C*, *b*, *K_s*) is one and the average of the traces for which D(*C*, *b*, *K_s*) is zero
- If K_s is incorrect, the bit computed using D will differ from the actual target about half of ciphertexts such that D(*C*, *b*, *K_s*) is uncorrelated to what was actually computed by the target device

$$\begin{aligned}\Delta_D[j] &= \frac{\sum_{i=1}^{m} D(C_i, b, K_s)\mathbf{T}_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))\,\mathbf{T}_i[j]}{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))} \\ &\approx 2\left(\frac{\sum_{i=1}^{m} D(C_i, b, K_s)\mathbf{T}_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} \mathbf{T}_i[j]}{m}\right).\end{aligned}$$

DPA (cont.)

- If K_s is correct, the computed value for D(*C*, *b*, *K_s*) will always be equal to the actual value of target bit.
- The correct value can be identified from the spikes in tis differential trace.
- By repeating this process for each bit, a 48-bit subkey can be recovered. Remaining 8 bits can be found by using brute-force or running additional round.

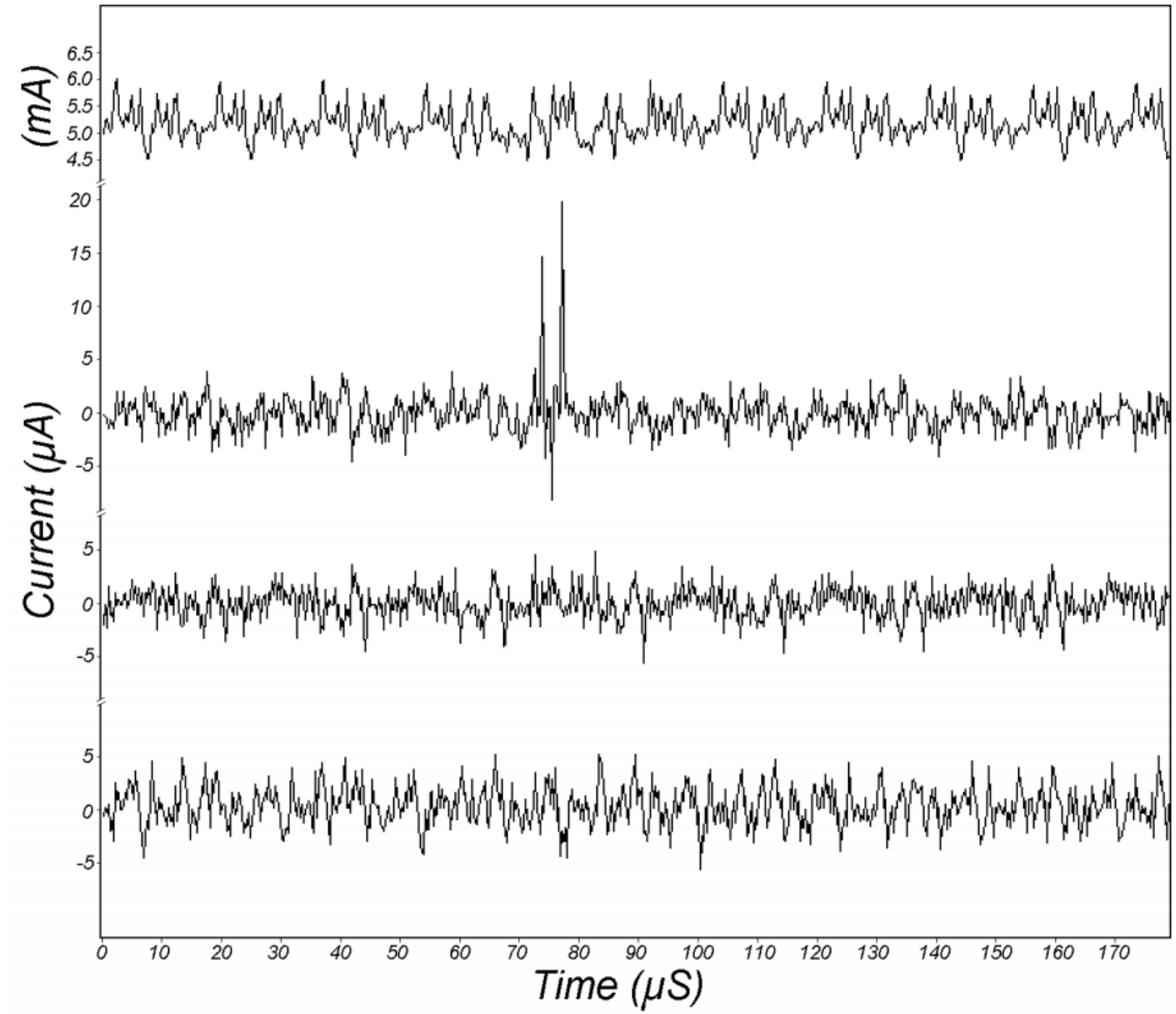


Figure 4: DPA traces, one correct and two incorrect, with power reference.

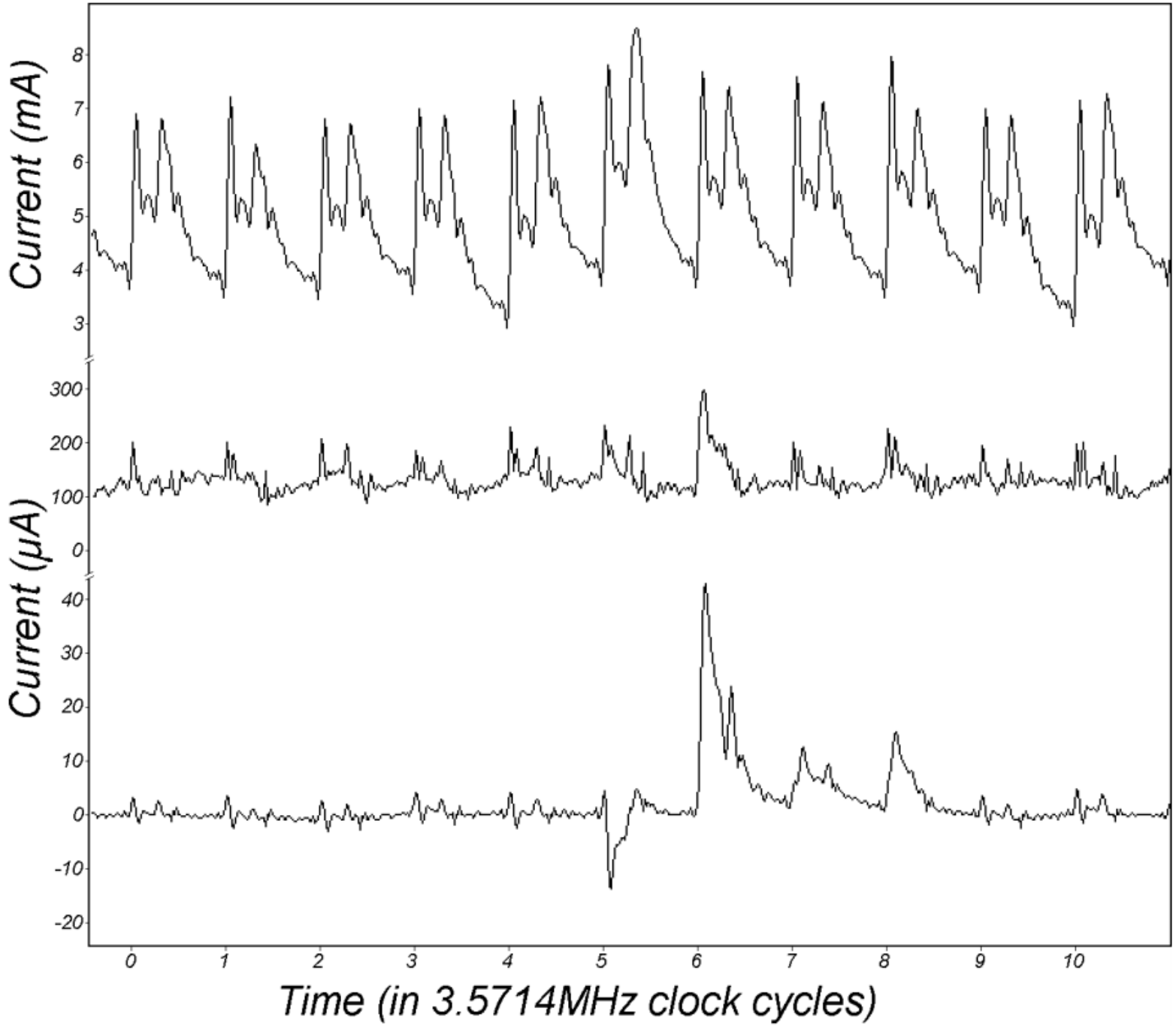


Figure 5: Quantitative DPA measurements

Challenges & Improvements

Challenges

- EM radiation
- Quantification errors due to mismatching device clocks and sample clocks
- Uncorrelated temporal misalignment of traces

Improvements

- Correct for the measurement variance (ex. automated template DPA)
- Using sophisticated selection functions (different weights to different traces, divide traces into more than two categories for instance)

Countermeasures

1. Reduce signal sizes

- using constant execution path code
- choosing operations that leak less information in their power consumption
- balancing Hamming Weights and state transitions
- physically shielding the device

attacker with an infinite number of samples will still be able to perform DPA on the “heavily-degraded” signal

Countermeasures (cont.)

2. introducing noise into power consumption measurements

→ Not plausible as there exists many methods to disable such obfuscation methods

3. designing cryptosystems with “realistic assumptions” about the underlying hardware

Questions?