CHES 2006 *October 12, 2006*

High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching

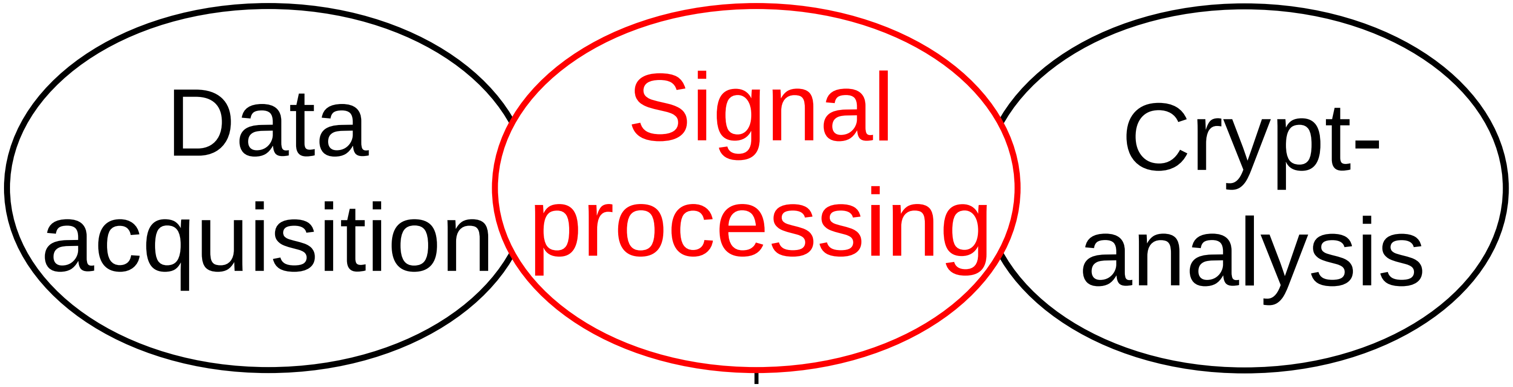
Naofumi HOMMA[†], Sei NAGASHIMA[†], Yuichi IMAI[†]
Takafumi AOKI[†] and Akashi SATOH[‡]

[†]Tohoku University, Japan
[‡]IBM Research, Tokyo Research Laboratory

Outline

- Why waveform matching?
- Phase-based waveform matching
- Application for side-channel attacks
- Conclusions and future prospects

Side-channel attack

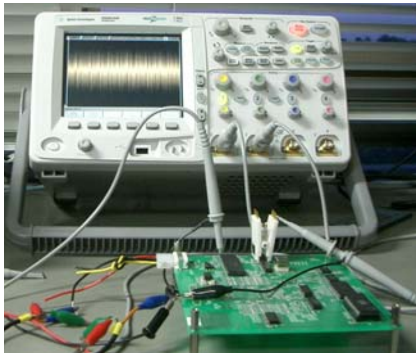


Data acquisition

Signal processing

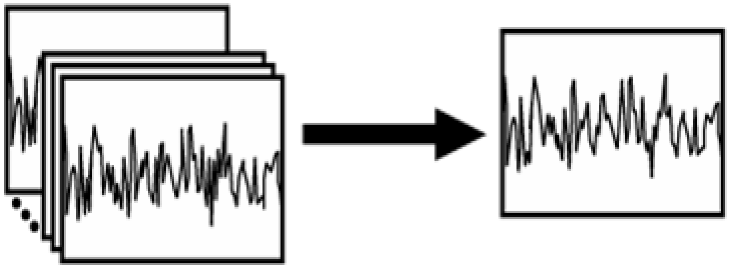
Crypt-analysis

Power dissipation
EM radiation
Operating times



Digital oscilloscope
(Side-channel information→waveform)

Noise reduction
Information extraction



Secret information extraction

Displacement problem

Assumption:

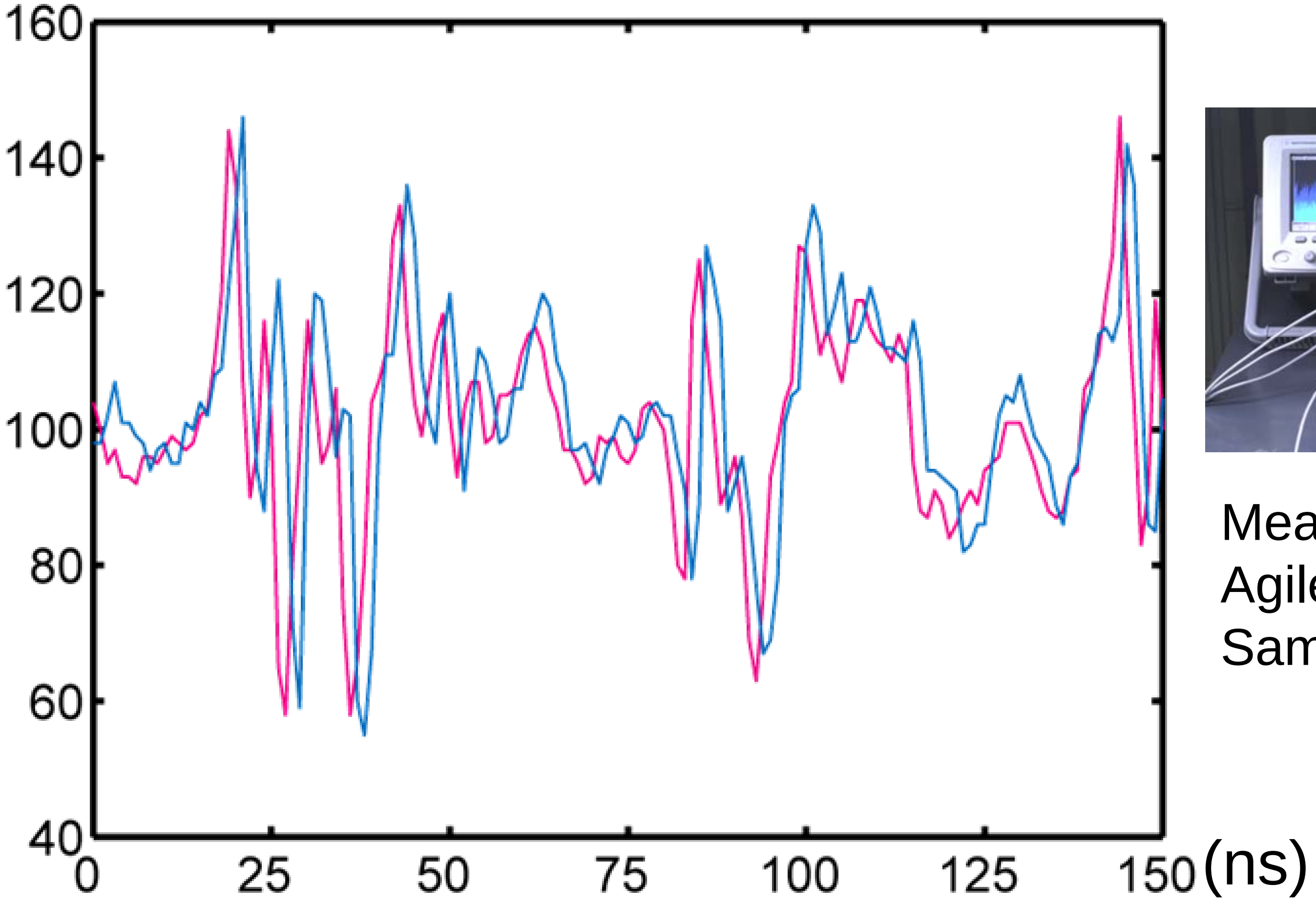
Each waveform can be captured at the exact moment as the cryptographic computation.

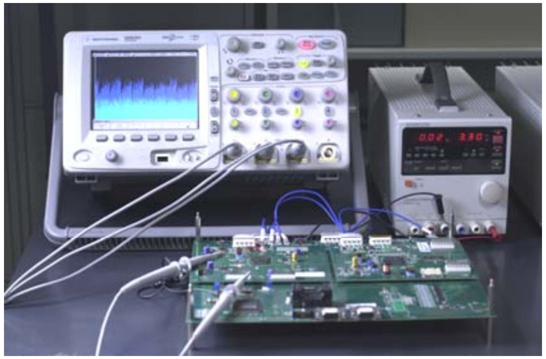
Reality:

Captured waveforms include displacement errors.

- No exact trigger signal
- Trigger jitter
- Randomly inserted displacement
  - Countermeasures creating distorted waveforms

Displacement in waveforms

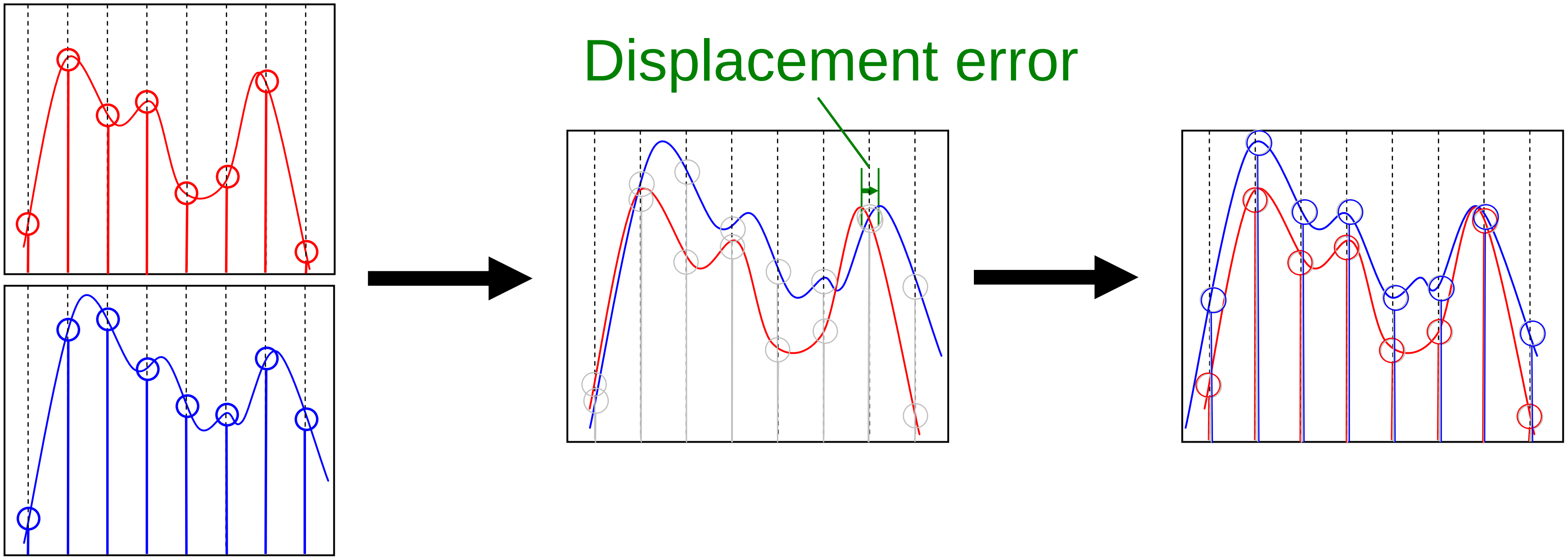




Measuring device:
Agilent DSO6104A
Sampling rate: 1GHz

Displacement errors cause significant loss of the secret information when the waveforms are averaged together.

Waveform matching



Displacement error

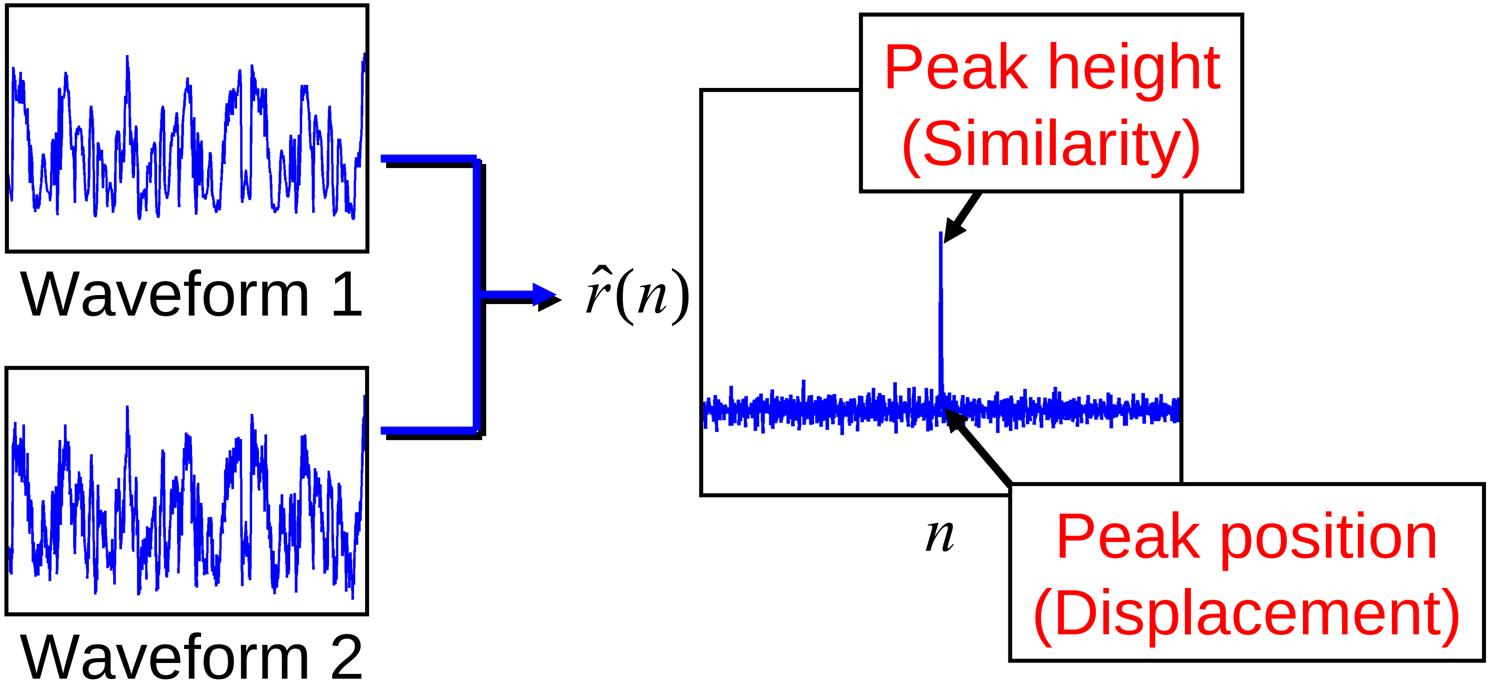
Requirements:

- To handle distorted waveforms → High noise tolerance
- To match waveforms captured by a digital measuring device
  → Higher accuracy beyond the sampling resolution

Phase-based waveform matching

- Phase-Only Correlation (POC) function

K. Takita et al. IEICE Trans. Fundamentals, E86-A, No. 8, 2003



Waveform 1

Waveform 2

$\hat{r}(n)$

n

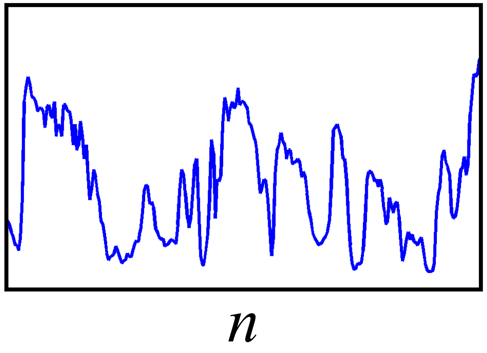
Peak height (Similarity)

Peak position (Displacement)

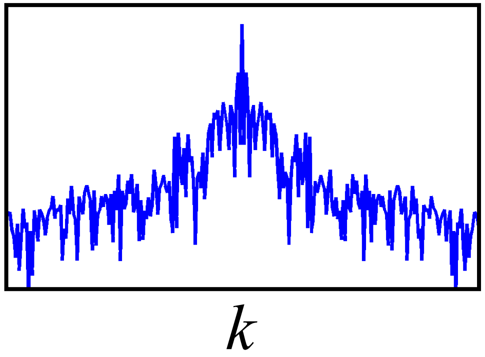
POC function has a sharp peak like a delta function.
Peak position: Translational displacement
Peak height: Similarity of waveforms

Basic computation flow for POC

Time Domain



Frequency Domain



Two input waveforms $f(n)$ $g(n)$

DFT →

$$F(k) = A_F(k)e^{j\theta_F(k)}$$

$$G(k) = \underbrace{A_G(k)}_{\text{Amplitude}}\underbrace{e^{j\theta_G(k)}}_{\text{Phase}}$$

POC function

$\hat{r}(n)$

← IDFT

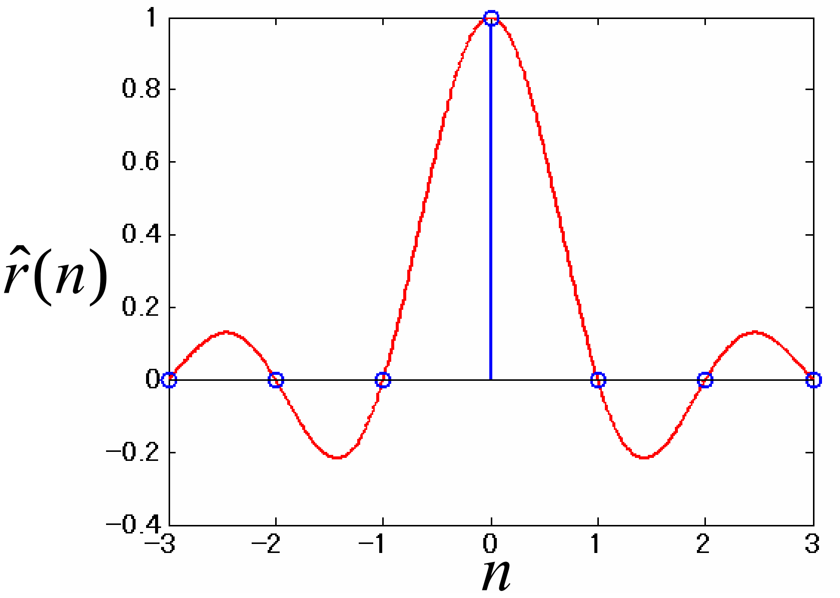
Cross-phase spectrum

$$\hat{R}(k) = \frac{F(k)}{|F(k)|} \cdot \frac{\overline{G(k)}}{|\overline{G(k)}|}$$

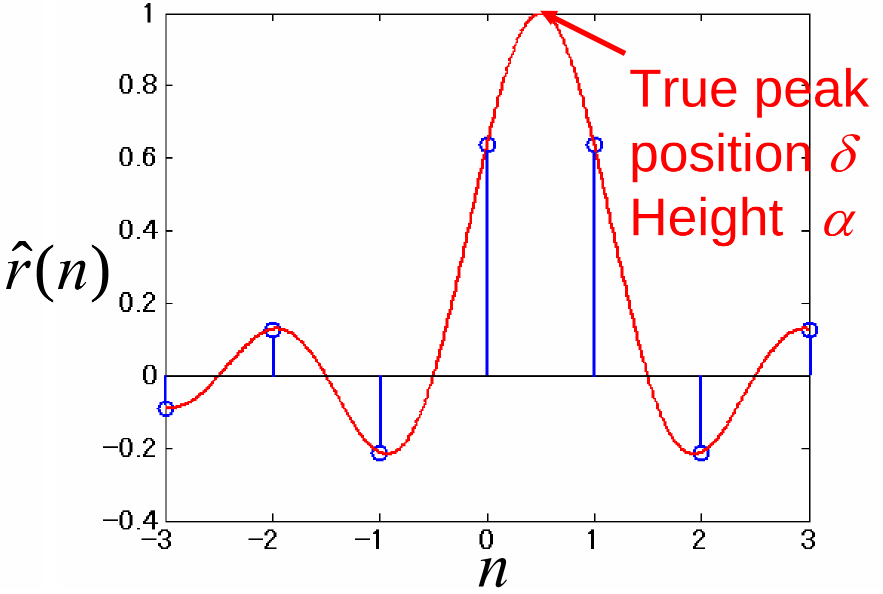
$$= e^{j\{\theta_F(k) - \theta_G(k)\}}$$

Displacement estimation

POC computation produces N data values.



Peak position $\delta = 0$



True peak position δ

Height α

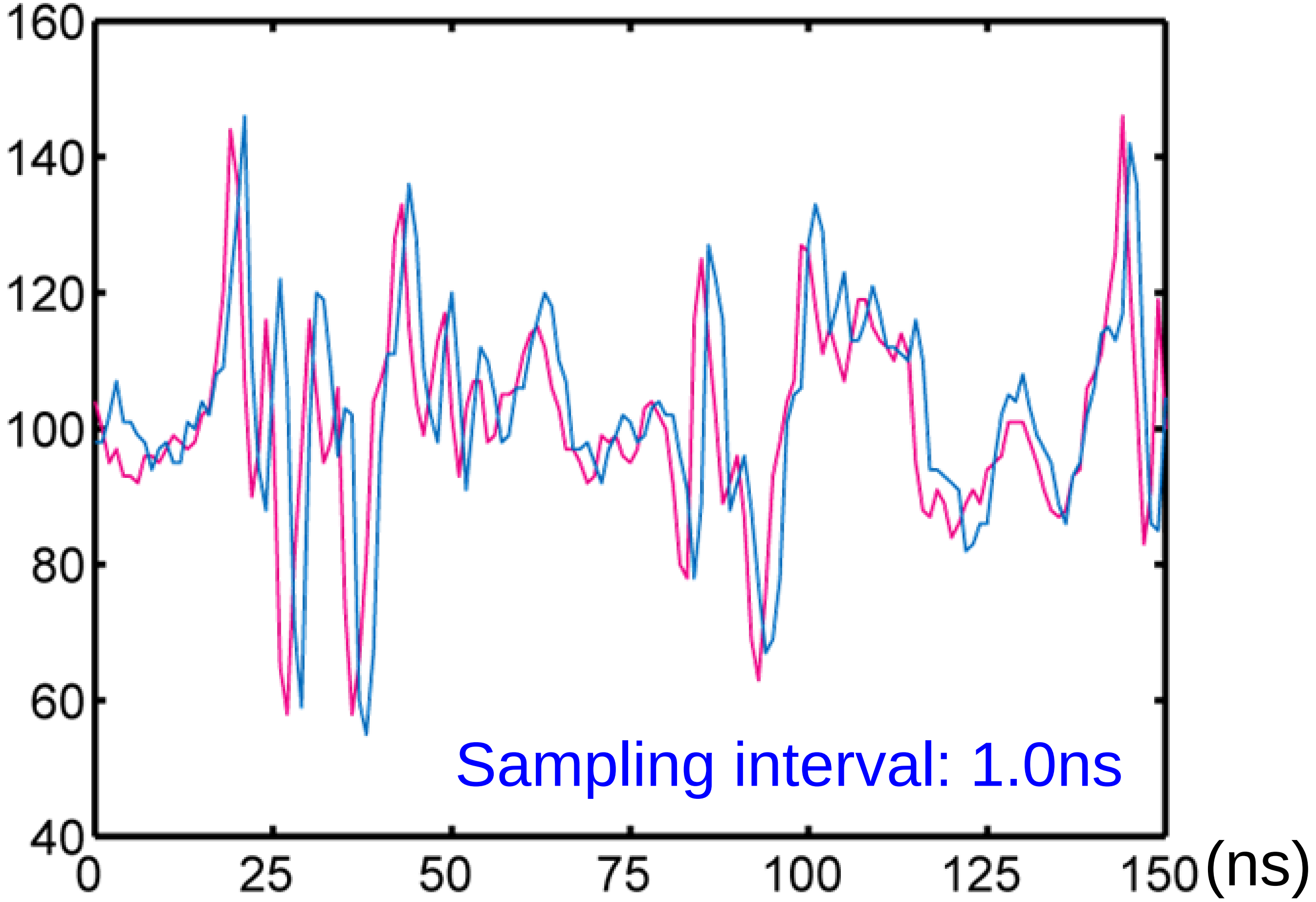
Peak position $\delta = 0.5$

Correlation peak model

$$\hat{r}(n) \approx \frac{\alpha}{N} \frac{\sin\{(n+\delta)\pi\}}{\sin\{(n+\delta)\frac{\pi}{N}\}}$$

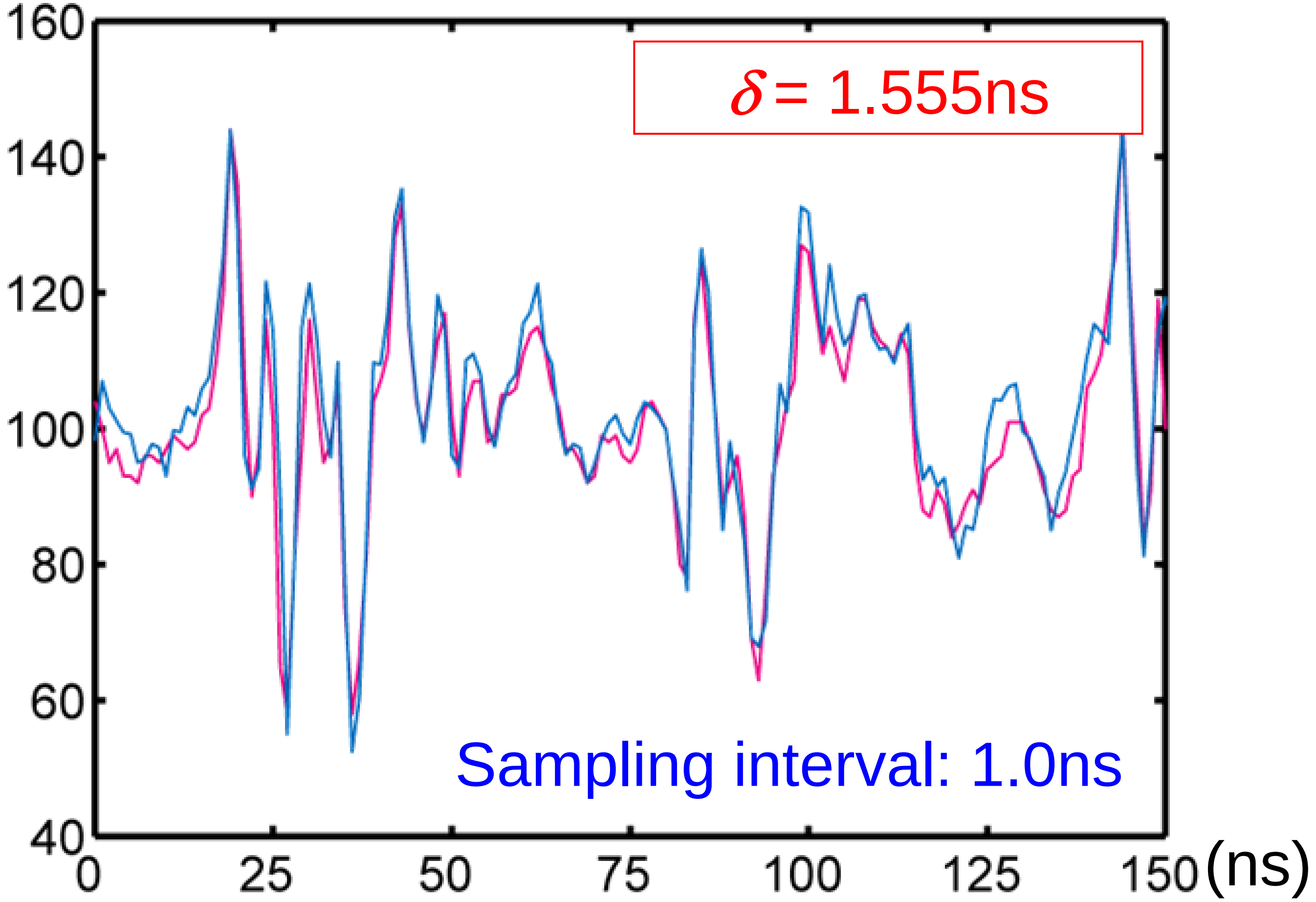
α, δ : fitting parameters

Example of waveform matching



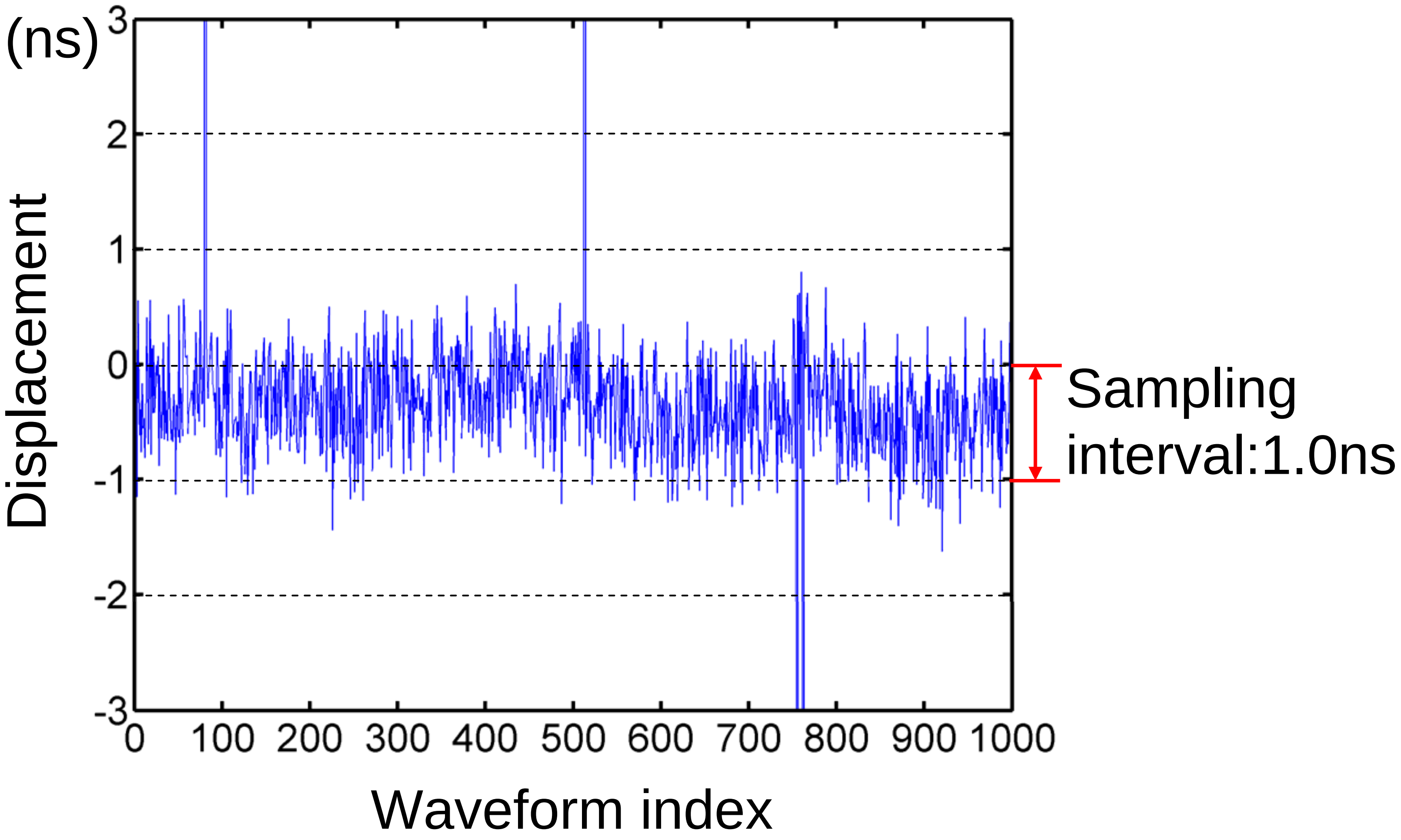
Before matching

Example of waveform matching



After matching

Estimated displacements

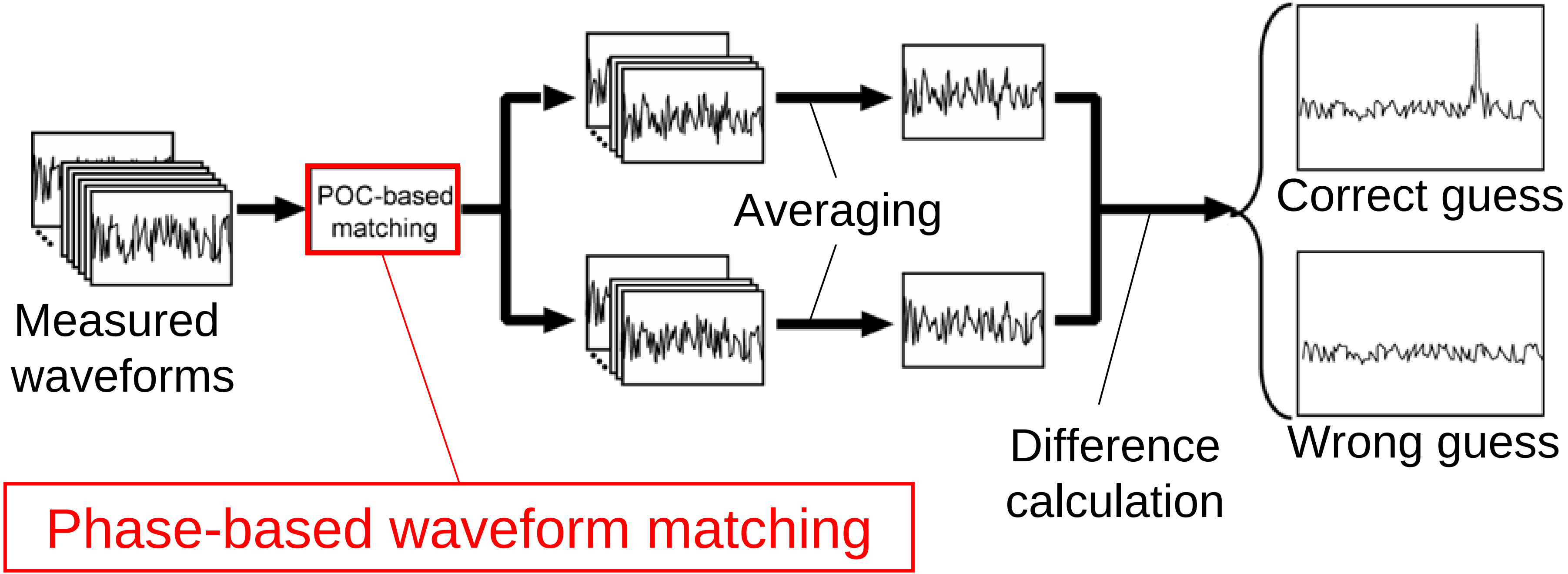


The waveforms contain displacement errors even though they were captured by using a trigger signal.

Side-channel attacks with phase-based waveform matching

- Phase-based waveform matching:
  a pre-processing step followed by waveform analysis

Proposed differential analysis



Measured waveforms

POC-based matching

Averaging

Difference calculation

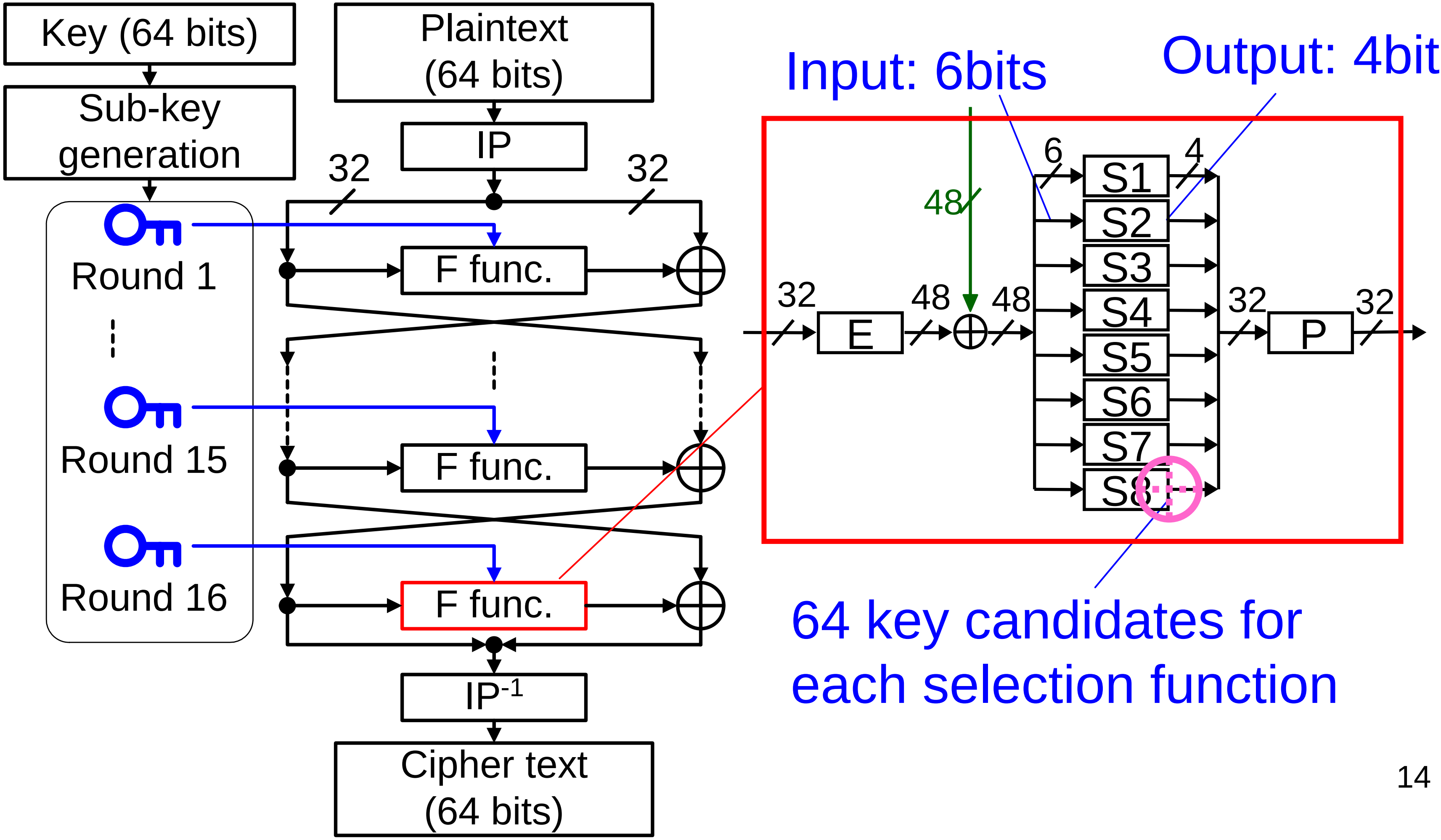
Correct guess

Wrong guess

Phase-based waveform matching

Experiment

- DPA and DEMA against DES module



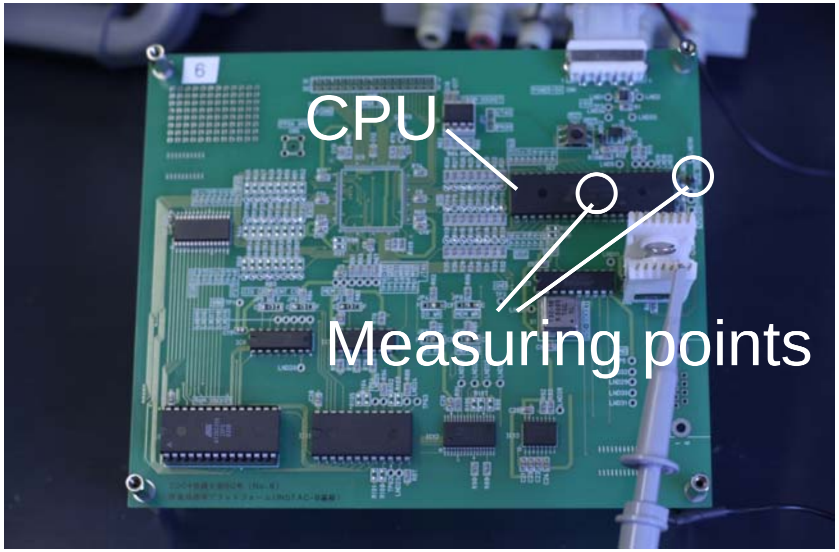
Input: 6bits

Output: 4bits

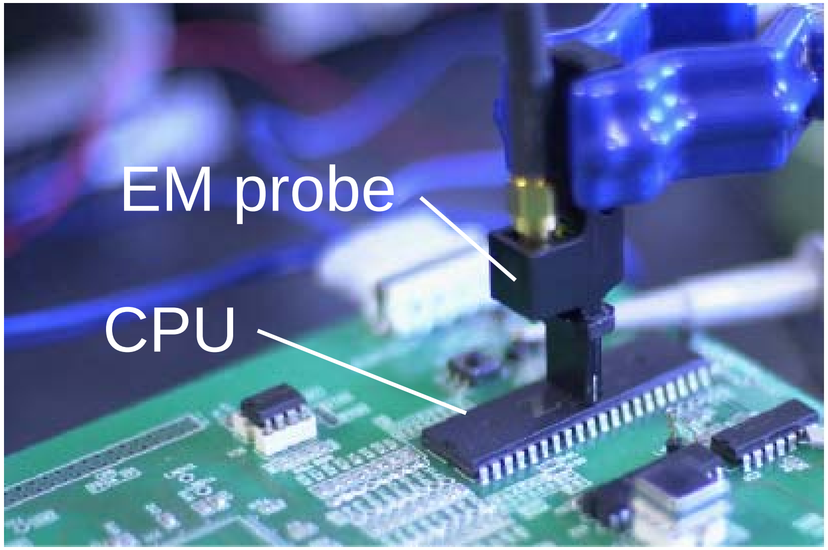
64 key candidates for each selection function

Experimental condition

- DES software implementation on a microprocessor
- Clock frequency: 8MHz
- Trigger signal at the beginning of Round 15
- Four sampling frequencies:
  100MHz, 200MHz, 400MHz, 1GHz

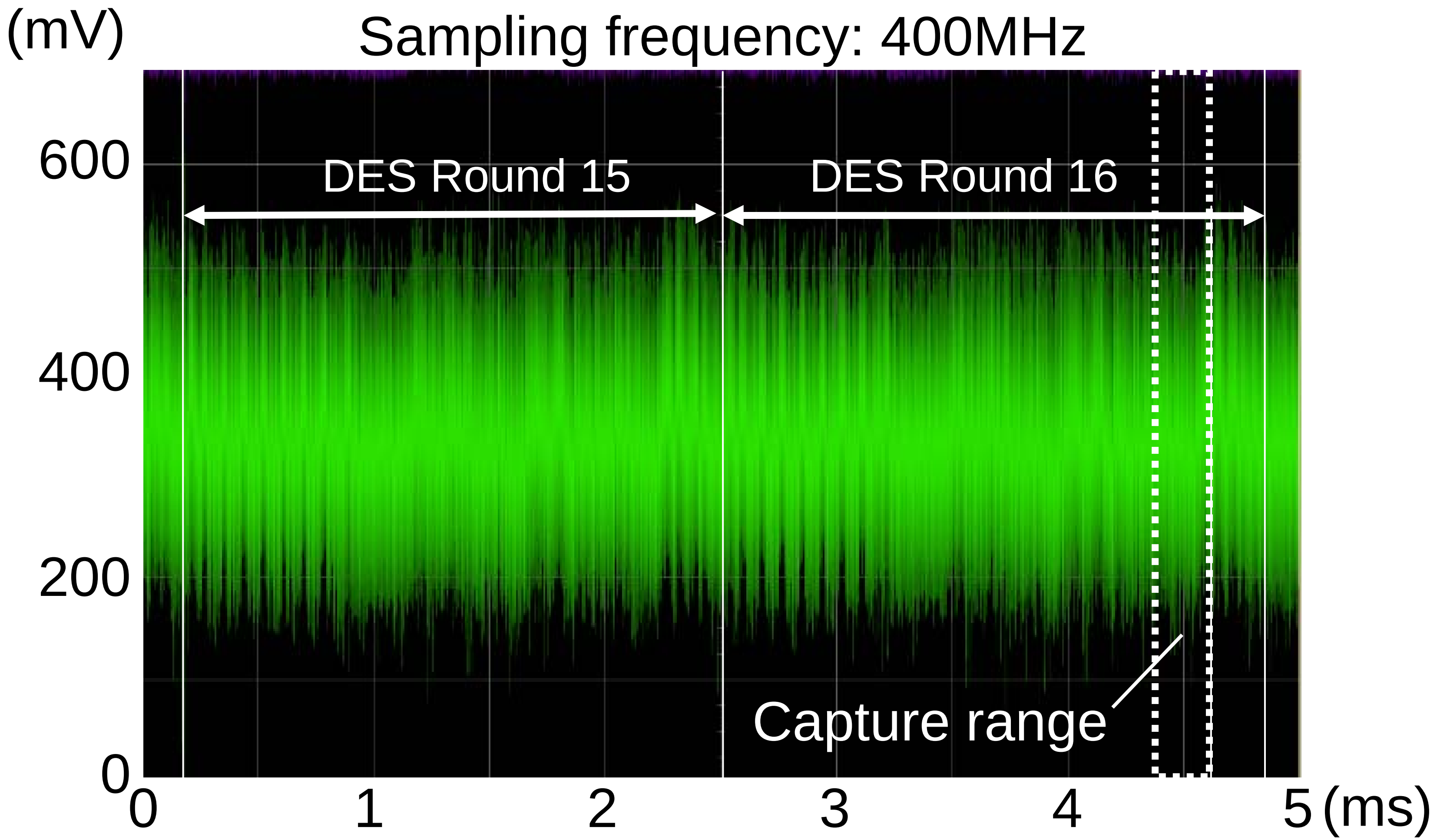


Evaluation board (INSTAC-8)



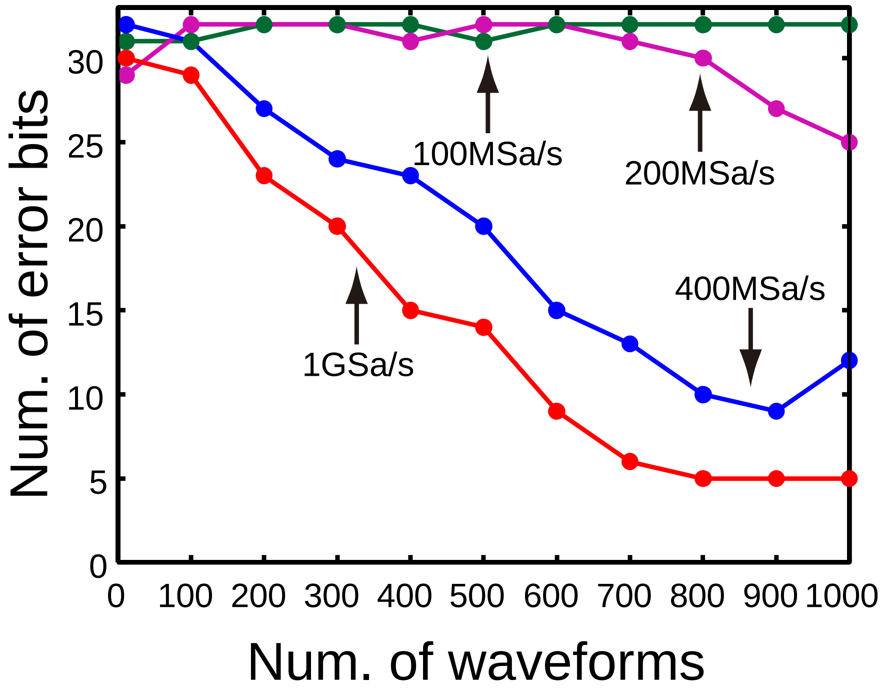
EM probing

Example of power trace

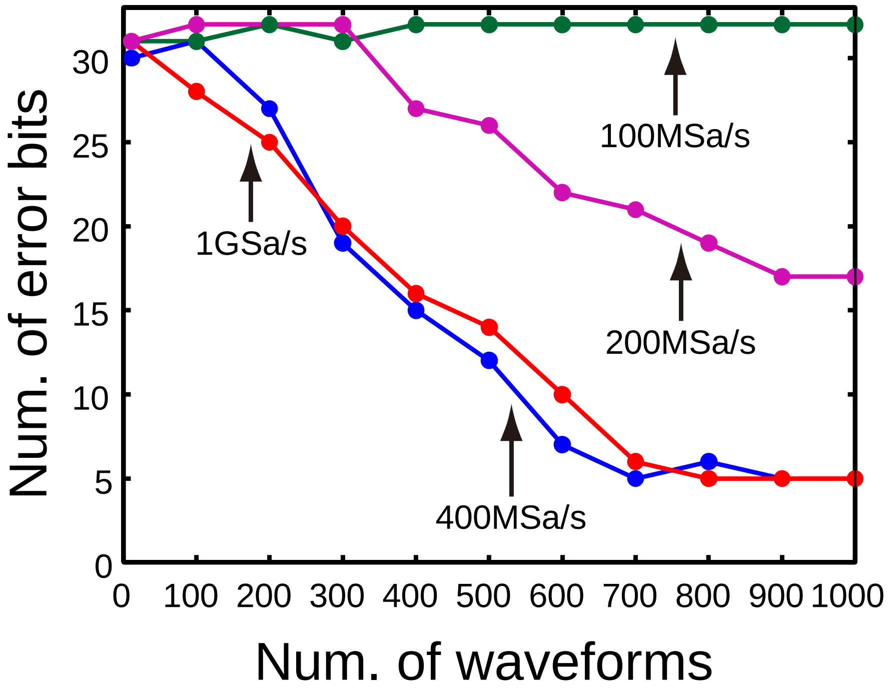


<span style="color:red">1000 waveforms</span> were measured during encryption of 1000 random plaintexts for each sampling frequency.

Error rates of DPAs



Conventional DPA

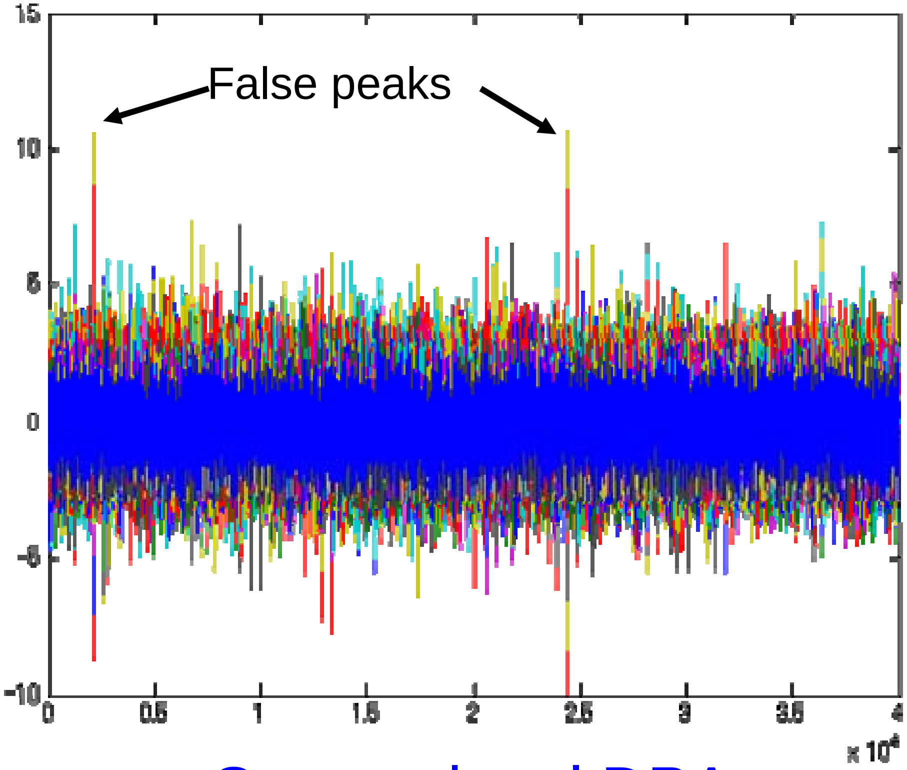


Proposed DPA

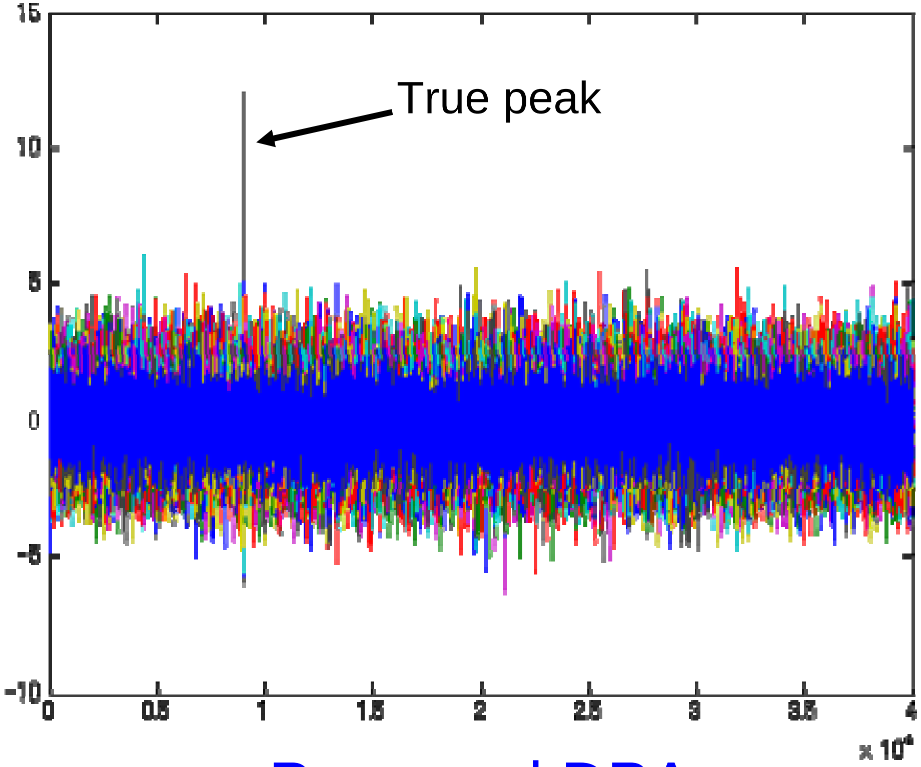
The proposed DPA improved the error rates of finding correct subkeys in comparison with the conventional DPA.

Example of DPAs

Sampling rate: 200MHz, Number of waveforms: 1000



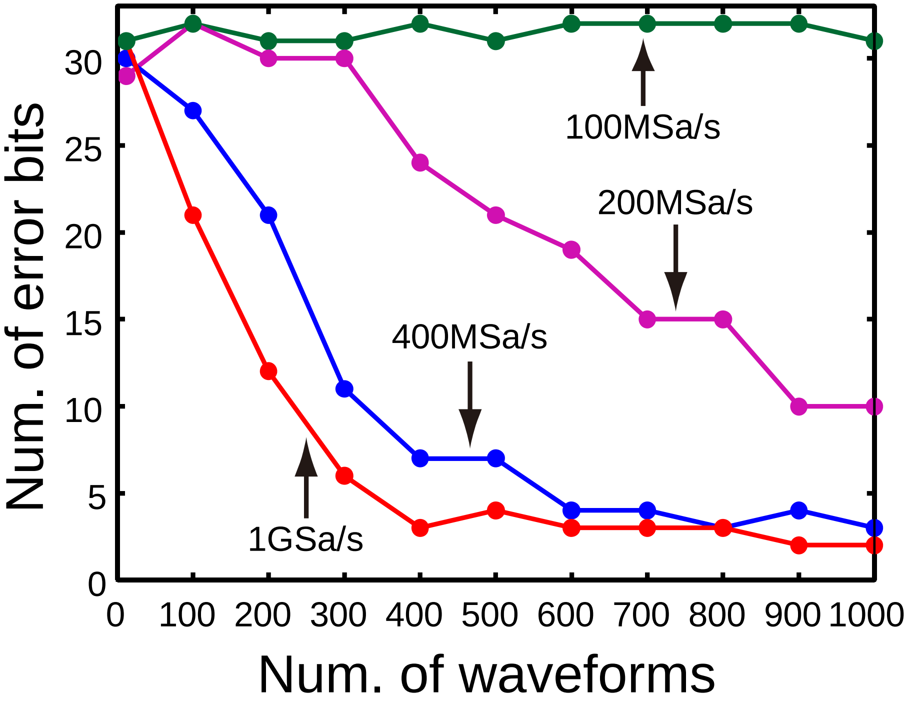
Conventional DPA



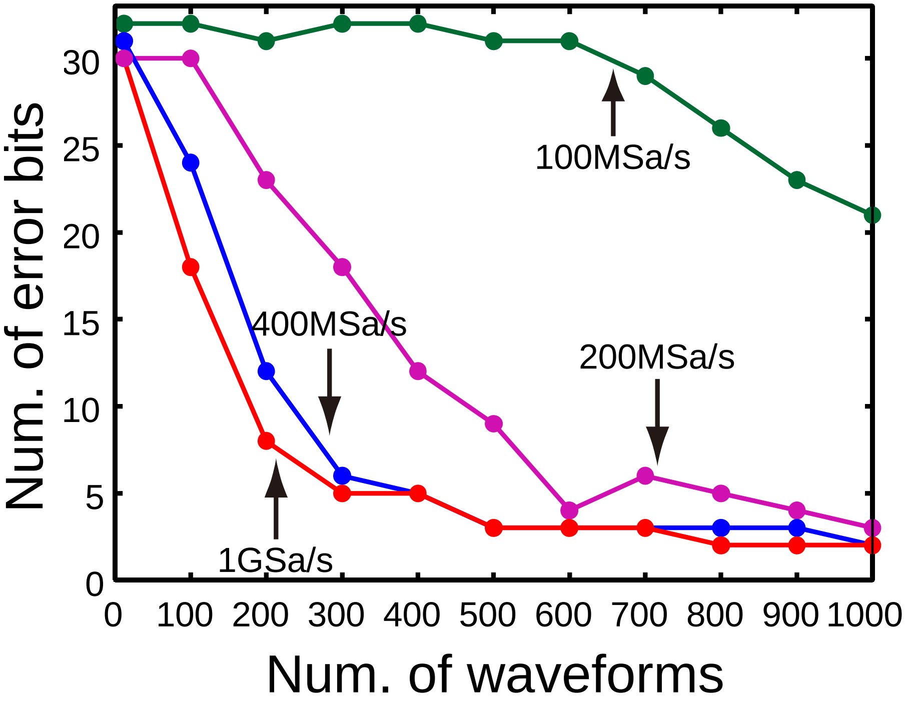
Proposed DPA

The proposed attack succeeded at a low sampling rate while the conventional attack failed.

Error rates of DEMAs



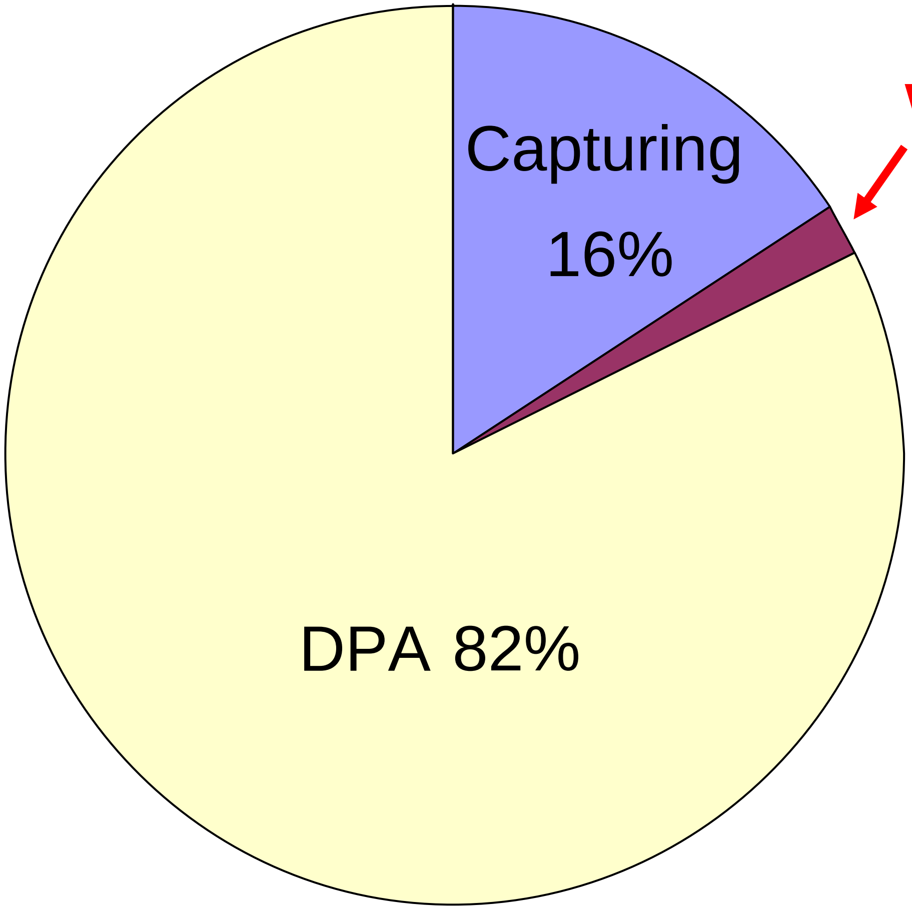
Conventional DEMA



Proposed DEMA

Proposed waveform matching can also be effective for DEMA.

Computation cost



Waveform matching: 2%

Total 251 minutes

Measuring device
Oscilloscope:
Agilent DSO6104A
Sampling rate: 200M Sa/s
# of waveforms: 1000

PC environment
CPU: Pentium4 3.2GHz
Memory: 2GB
OS: Windows XP
Software: MATLAB 7.1

Conclusions

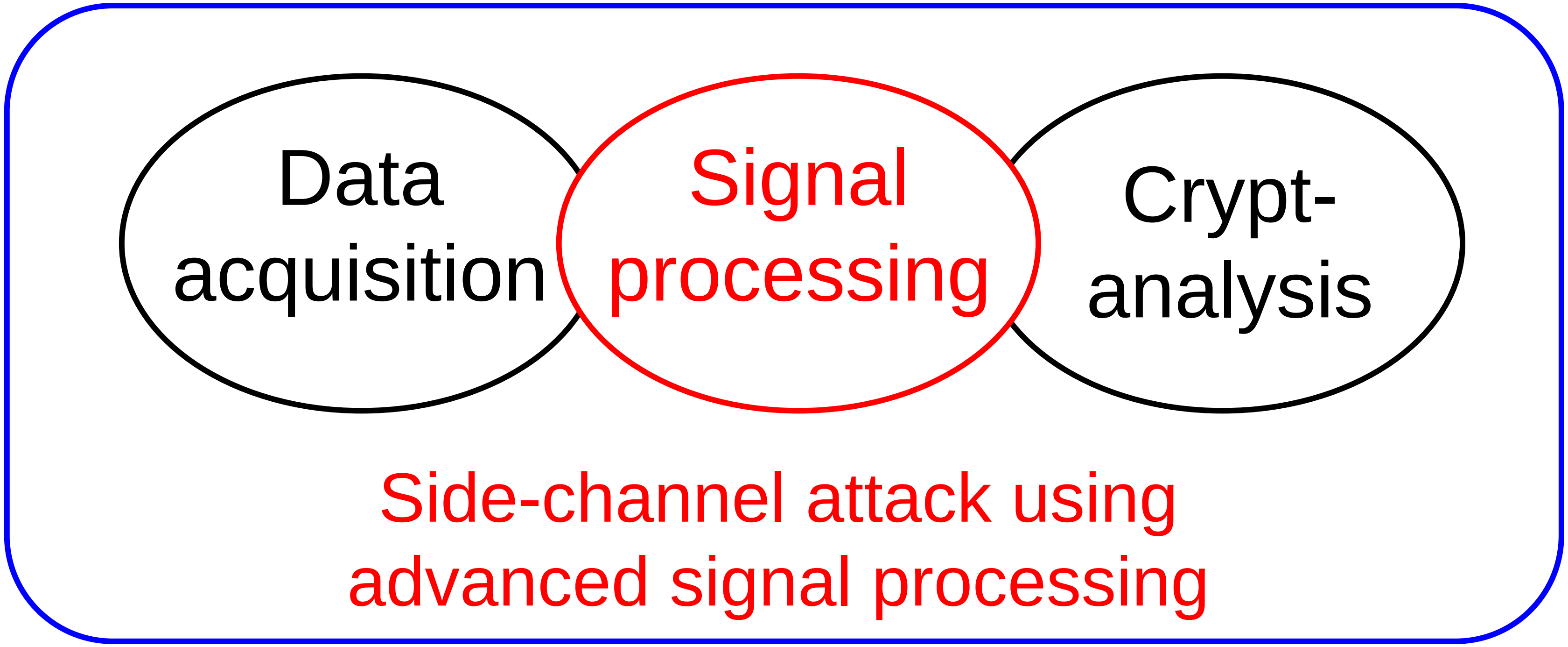
High-resolution side-channel attacks using phase-based waveform matching

- Detect displacement errors with higher resolution than the sampling resolution

- Improve the accuracy of differential analysis
  - Additional computation cost is less than 3%.

- Have high availability
  - POC pre-process is simply applied to captured waveforms before cryptanalysis.

Future prospects



Data acquisition

Signal processing

Crypt-analysis

Side-channel attack using advanced signal processing

- Independent of cipher algorithms, implementations, and kind of side-channel information
- Efficient for attacking actual cryptographic modules
- Defeat some hardware countermeasures