FIPS 140-3 Non-Invasive Attack Testing

Hirofumi Sakane[1,2] Hirofumi.Sakane@nist.gov

Caroline Scace[1] Caroline.Scace@nist.gov

[1] Security Management and Assurance Group, CSD, NIST

[2] Research Team for Hardware Security, RCIS, AIST

Non-invasive attacks

- Are side-channel attacks which exploit weak channels
  - Hidden information may leak in the form of physical phenomena:
    - Power consumption, electro-magnetic emission, photon emission, or timing
- Differ from conventional attacks
  - No physical modification required – **Inexpensive**
  - Leave no tamper evidence
    - Don’t trigger tamper response
- Classes of non-invasive attacks
  - Power Analysis Attacks
  - Electromagnetic Analysis Attacks
  - Timing Attacks

Power Analysis Attacks

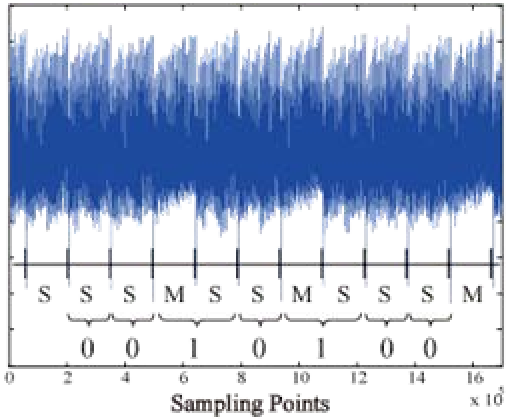
- Real-time power consumption data may contain the information of on-going crypto-operations
- Simple Power Analysis (SPA)
  - Extracts the secret key after visual inspection of a power trace
- Differential Power Analysis (DPA)
  - Extracts the secret key after statistical processing of power traces

Power trace : measured waveform of real-time power consumption

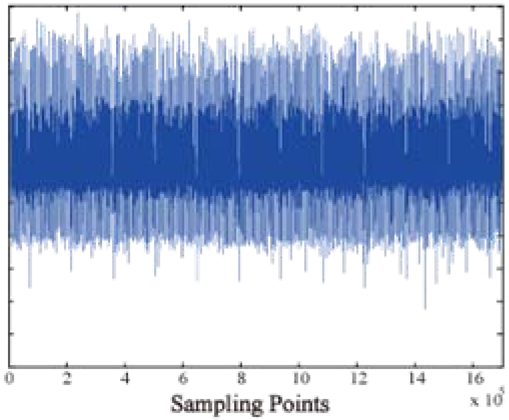
SPA on RSA

- Correct partial key = 0010100

Fail

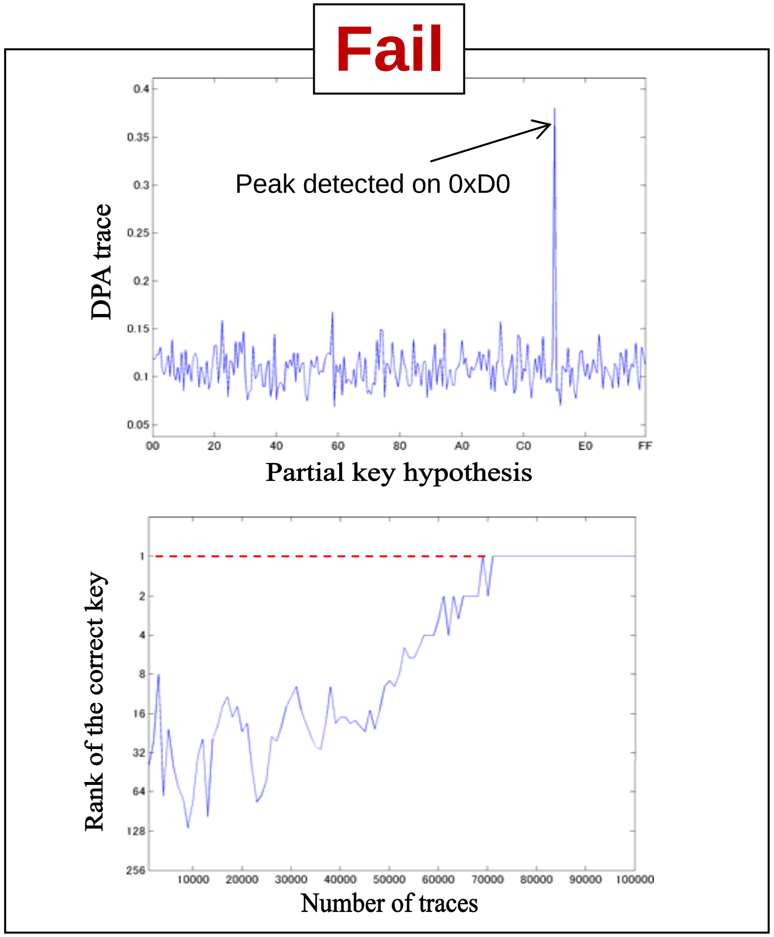


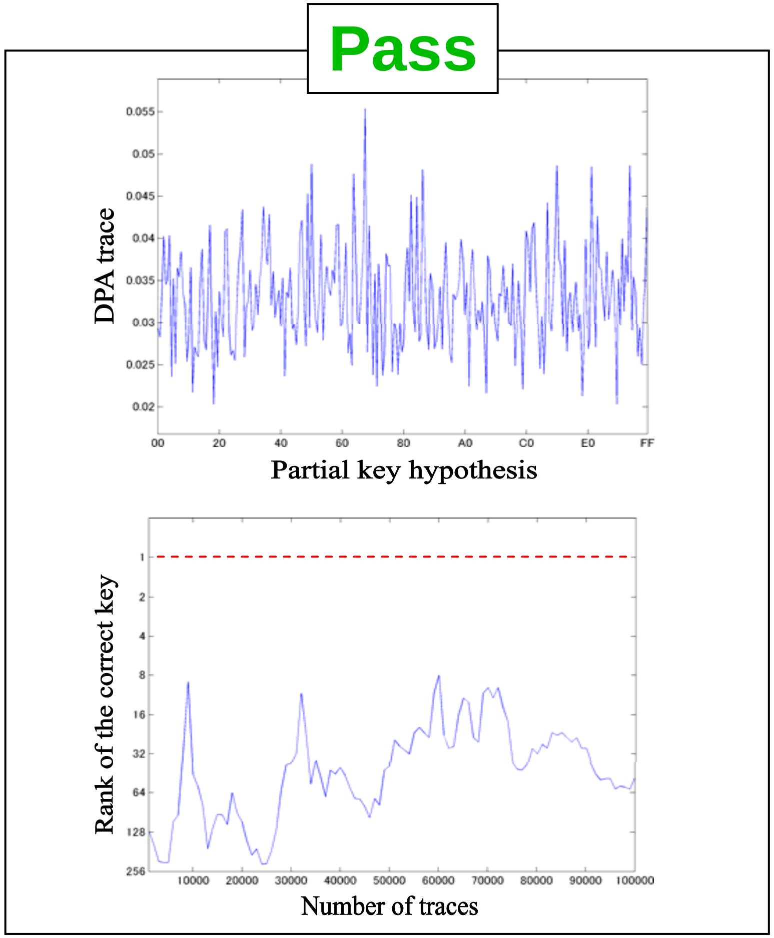
Pass



DPA on AES

- Correct partial round key = 0xD0





Research Goals

- Develop test methods
  - Support our labs to perform testing
- Determine test metrics
  - For new standard: FIPS 140-3 Security Requirements for Cryptographic Modules

Example Target: Smart Card

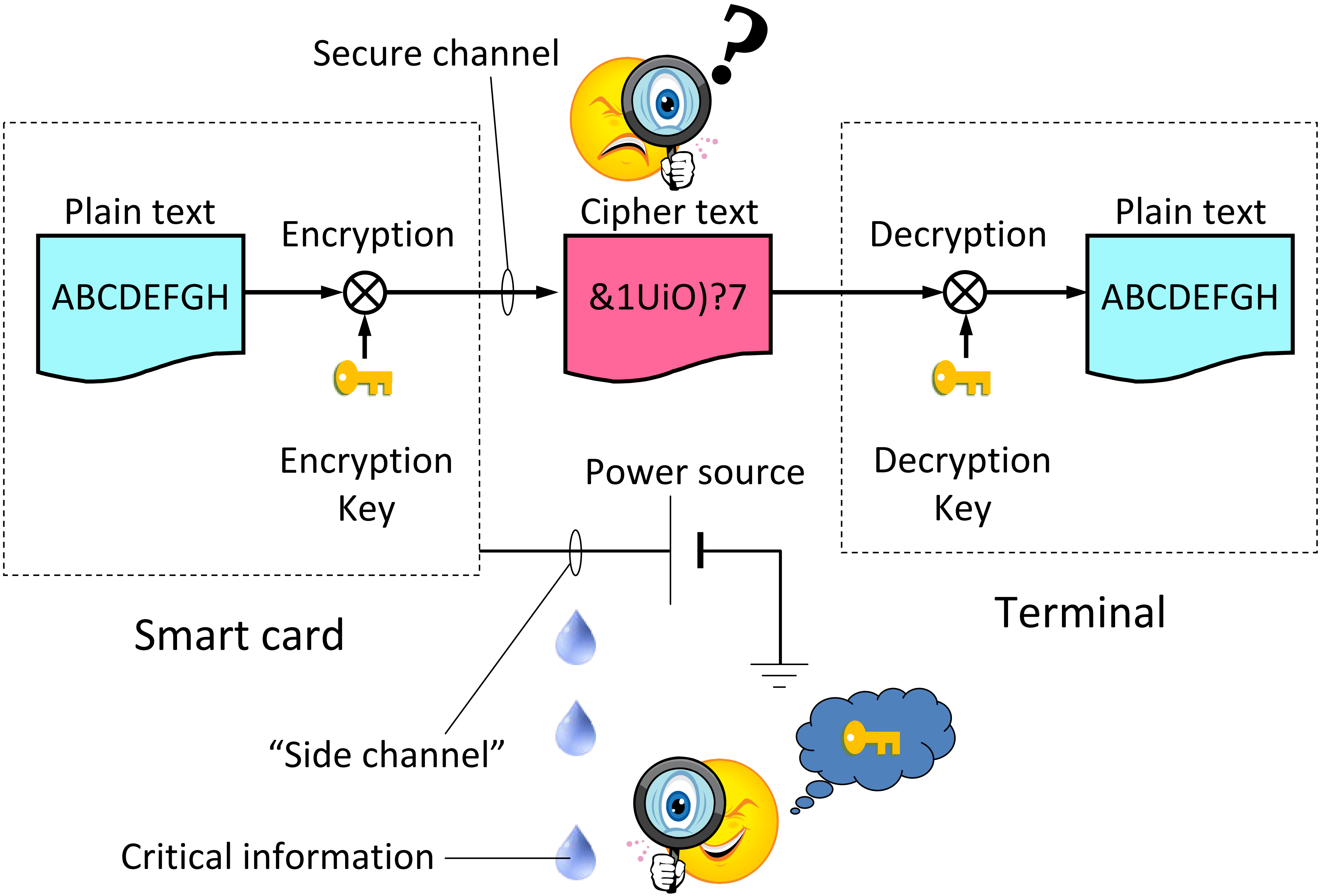
- **Governmental use**: Identification, Authentication, Electronic signature, etc.
- Commercial use: Payment card, Credit card, Transportation fare card, etc.
- Security functions protect important information (CSPs) from malicious use
  - CSP: Critical Security Parameter, such as cryptographic key and PIN
- Portable

  → Easy for attackers to possess

  → Easy to observe side channels

  → Potential weakness against non-invasive attacks

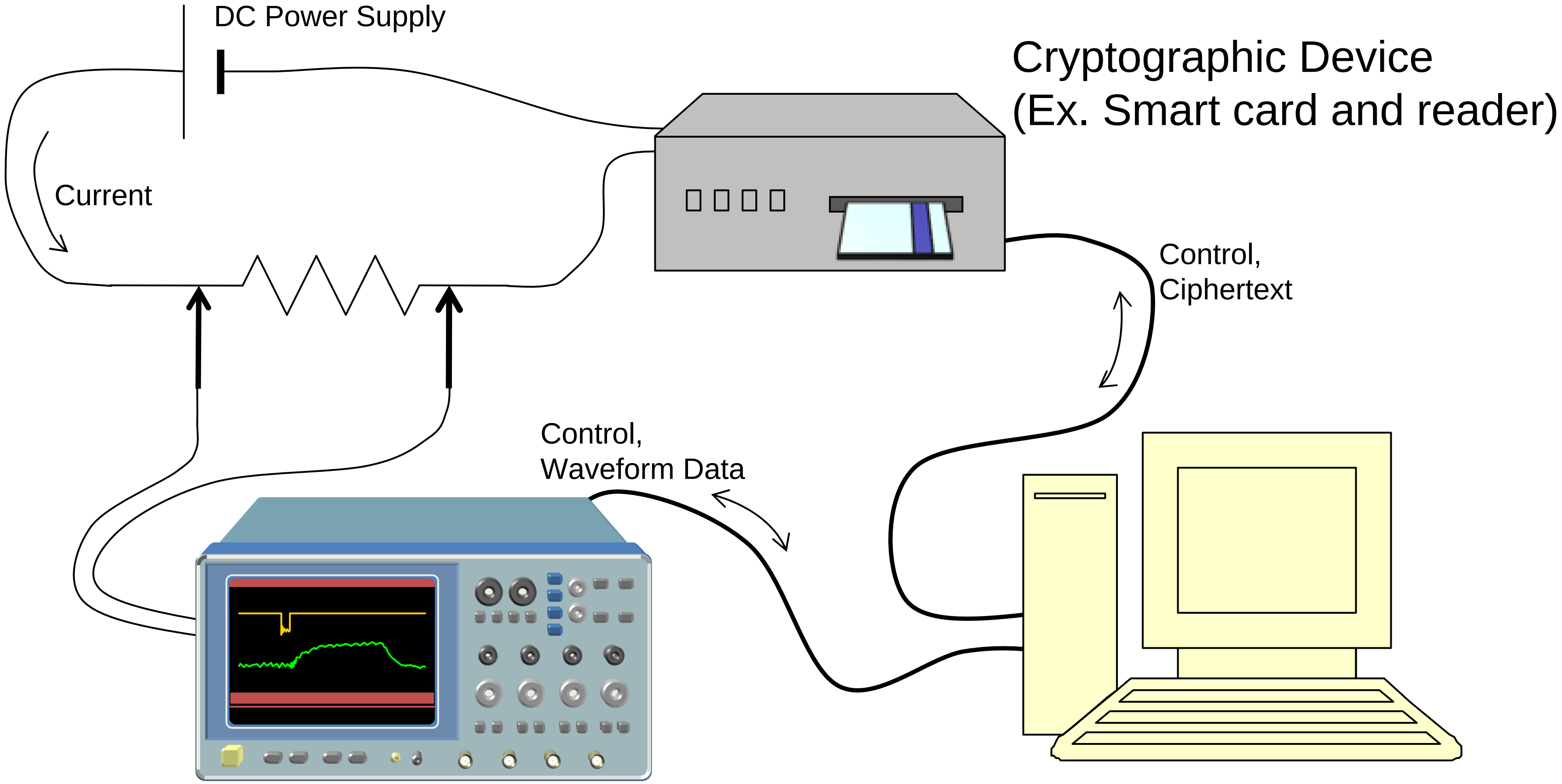
Is Your Smart Card Secure?



Example: PIV Card

- What if your PIV card is vulnerable against Non-Invasive side-channel attacks?
  - Someone may pick up your card on the street
  - He may be able to:
    - Enter your building
    - Access your email
    - Electronically sign a purchase contract
- Prevention measure:
  - FIPS 140-3 validation
    - Effective testing to fail a vulnerable module

A Test Bench for Power Analysis



DC Power Supply

Cryptographic Device
(Ex. Smart card and reader)

Current

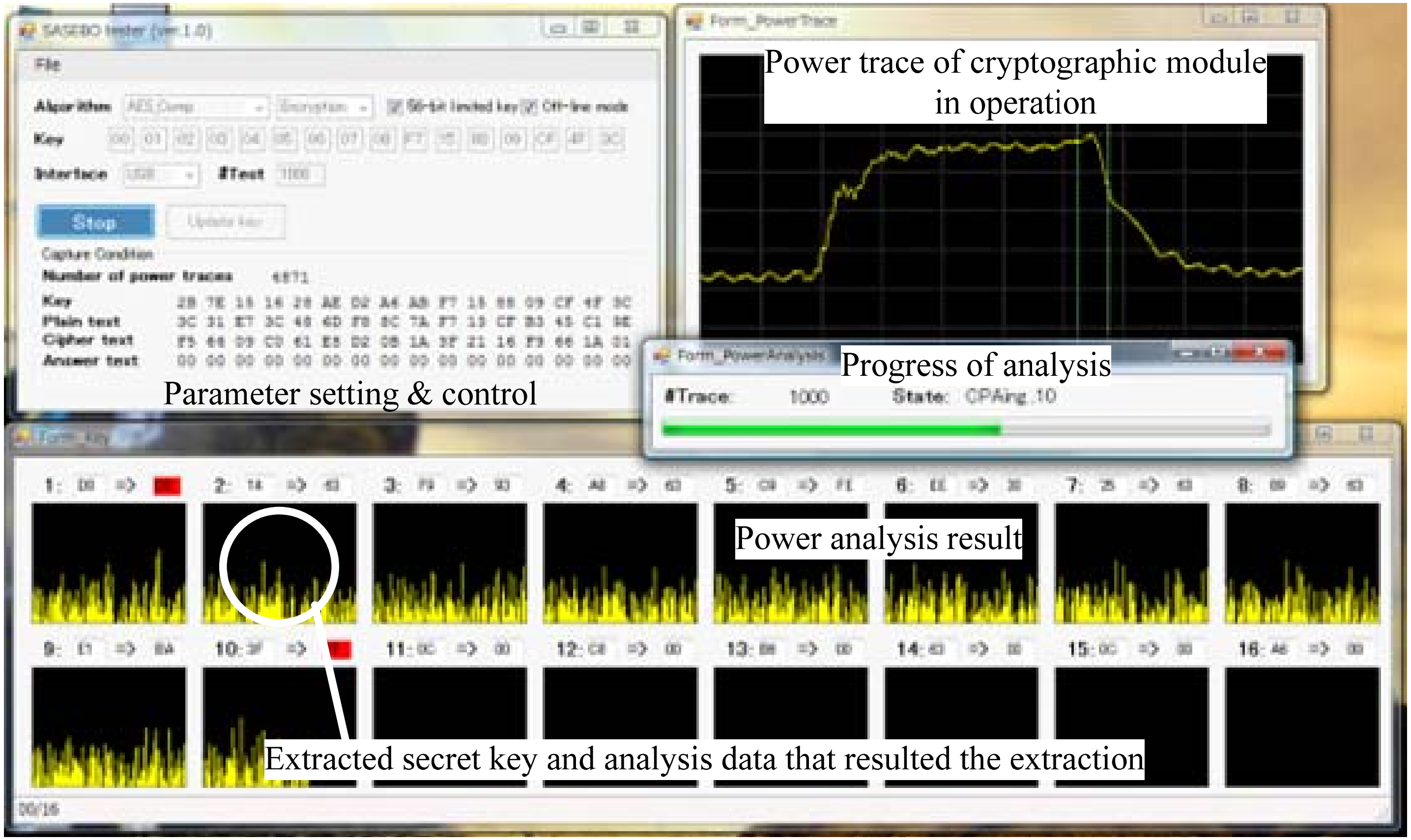
Control,
Ciphertext

Control,
Waveform Data

Power Consumption Measurement

Data Analysis

Example Test Tool Interface



Algorithm: AES Comp, Encryption ☑ 56-bit limited key ☑ Off-line mode
Key: 00 01 02 03 04 05 06 07 08 F7 15 88 09 CF 4F 3C
Interface: USB #Test: 1000

Capture Condition

```
Number of power traces   4871
Key            2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Plain text     3C 31 E7 3C 48 6D F8 8C 7A F7 13 CF B3 45 C1 9E
Cipher text    F5 66 09 C0 61 E5 D2 0B 1A 3F 21 16 F9 66 1A 31
Answer text    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Parameter setting & control

Power trace of cryptographic module in operation

#Trace: 1000 State: CPAing 10

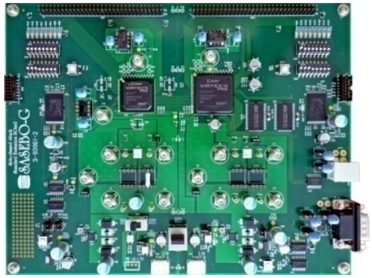
Progress of analysis

Power analysis result

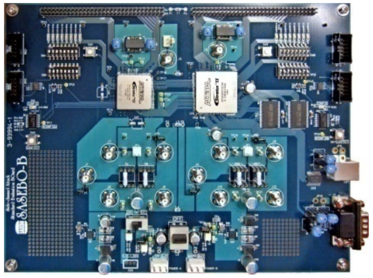
Extracted secret key and analysis data that resulted the extraction

SASEBO

- **S**ide-channel **A**ttack **S**tandard **E**valuation **BO**ard
  - Developed by Tohoku University and AIST
  - Convenient for power consumption measurement
  - Suitable for fundamental research due to its known and controllable characteristics
- Purposes
  - Common platform for side-channel attack research
  - Training for test labs
  - Hardware artifact for test tool calibration and certification
  - Development of FIPS 140-3 Non-Invasive Attack test methods and metrics



SASEBO-G



SASEBO-B

SASEBO-R

SASEBO-GII

http://www.rcis.aist.go.jp/special/SASEBO/index-en.html