FIPS 140-3 Non-Invasive Attack Testing

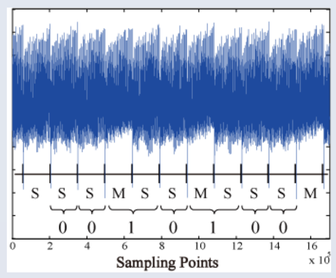
Power Analysis Attacks

- 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

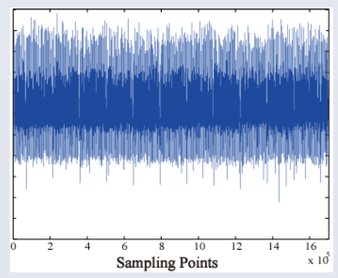
SPA on RSA

Correct partial key = 0010100

Fail



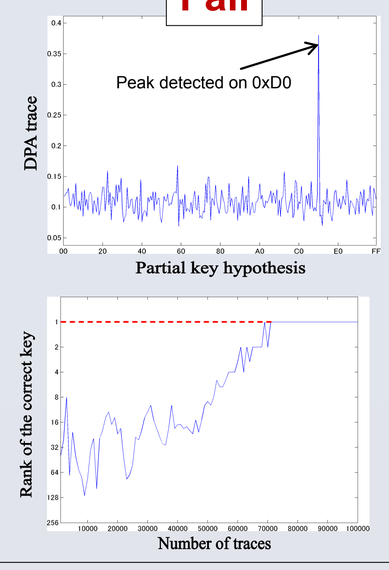
Pass



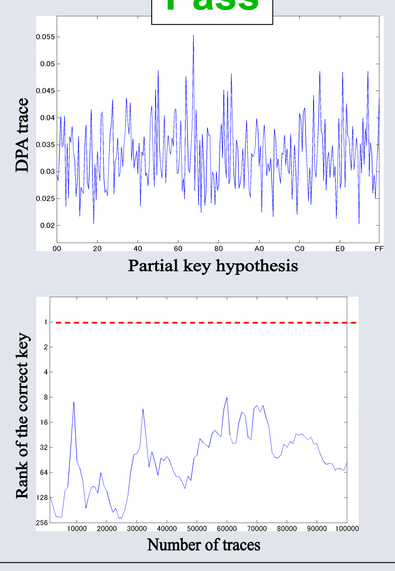
DPA on AES

Correct partial round key = 0xD0

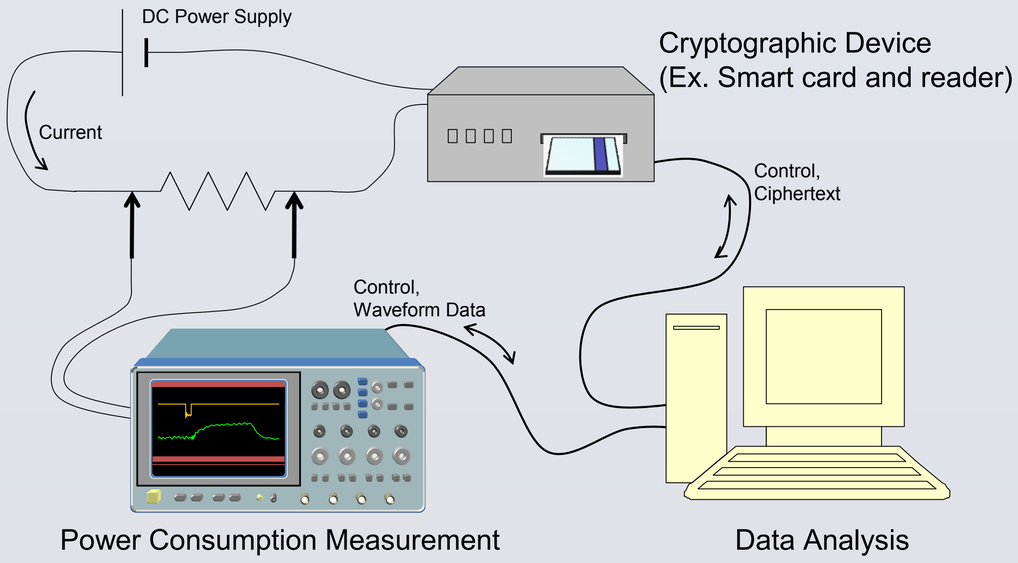
Fail



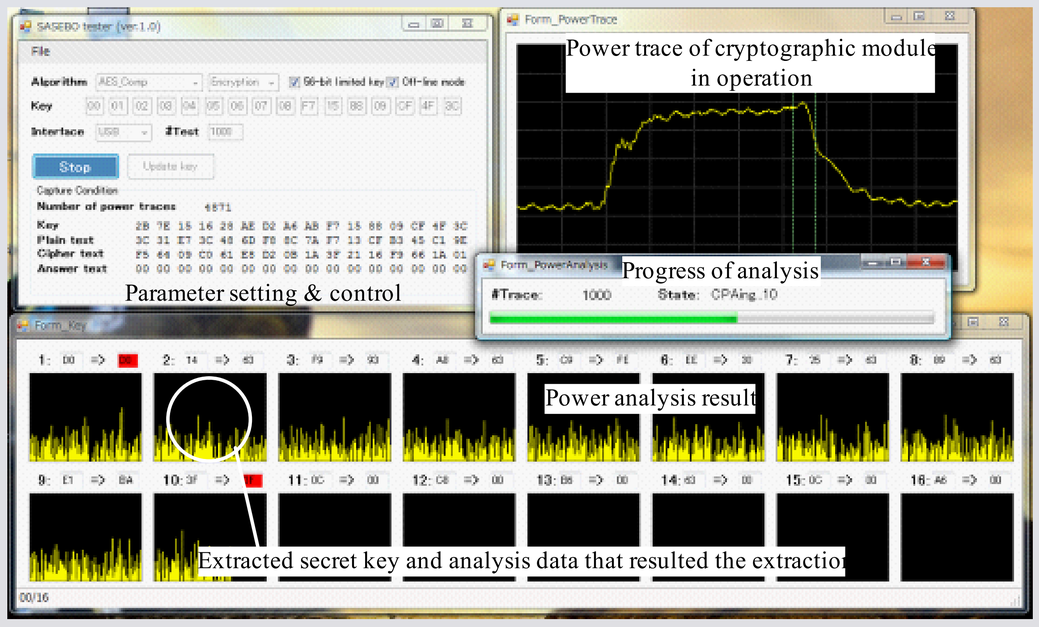
Pass



A Test Bench for Power Analysis



Example Test Tool Interface



SASEBO

Side-channel Attack Standard Evaluation BOard

- 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

NIST
National Institute of Standards and Technology
U.S. Department of Commerce