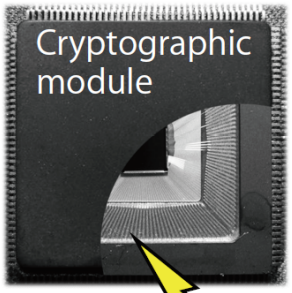
Information Security Engineering Laboratory

Cryptographic algorithm

Encryption: $C = P^E \mod N$

Decryption: $P = C^D \mod N$

P: Plaintext, C: Ciphertext
E, N: Public keys
D: Secret key



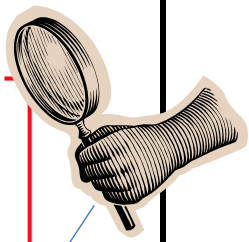
Theme 1: Hardware Implementation of Crypt. Algorithm (RSA)

Side Channel Information


Timing

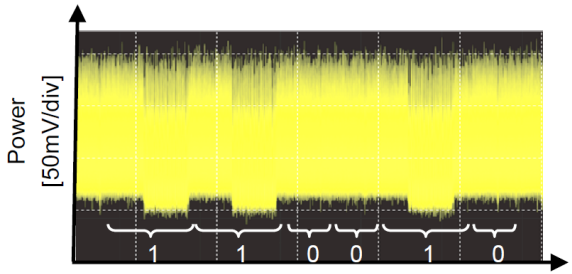

Power consumption


EM radiation

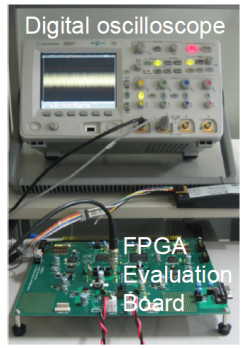


Measurement of leakage information from cryptographic module

Theme 2: Cryptanalysis based using Side-Channel Information from Crypto. Module



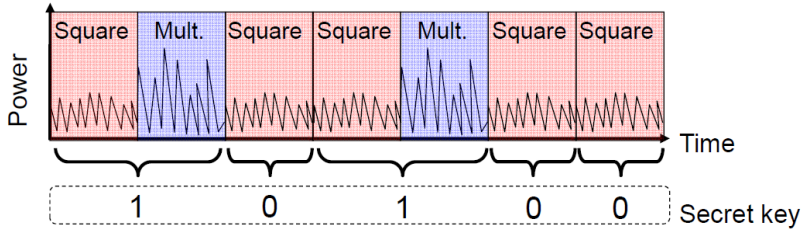
Measured power waveform



Measurement

Waveform patterns clearly showed secret key information

Simple Power/EM Analysis reveals secret information directly using one or a few power waveforms



Secret key information is estimated by waveform patterns