Strategy and Synergy for Security

Side Channel Attack Evaluation

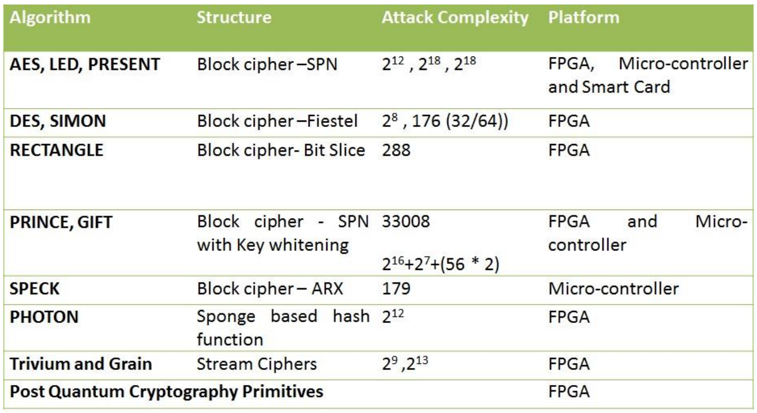
Towards Securing Crypto Modules

Overview

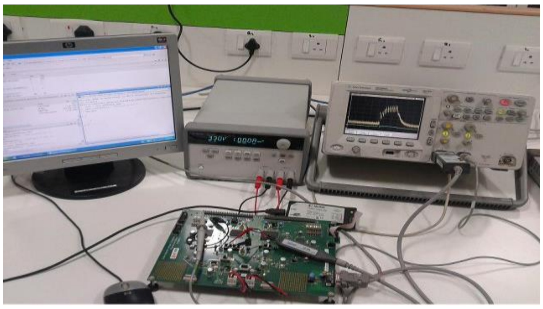
Side channel attacks exploit the information leakage through physical medium to reveal the secret key/information of the cryptography device. Side channel attacks are an important concern for the security of cryptographic implementations. Many security standards such as FIPS 140-3, Common Criteria mandating cryptographic devices and modules to resist side channel attacks such as timing analysis, simple and differential power/electromagnetic analysis.

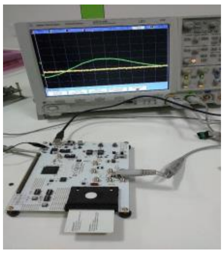
Evaluation of crypto primitives @ SETS

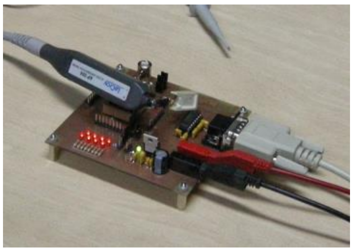
SETS has established differential power analysis measurement and analysis set-up on Field Programmable Gate Array (FPGA) and micro-controller. Using the set-up, varieties of crypto modules have been evaluated and appropriate countermeasures have also been developed.



Algorithm	Structure	Attack Complexity	Platform
AES, LED, PRESENT	Block cipher –SPN	2^{12} , 2^{18} , 2^{18}	FPGA, Micro-controller and Smart Card
DES, SIMON	Block cipher –Fiestel	2^{8} , 176 (32/64))	FPGA
RECTANGLE	Block cipher- Bit Slice	288	FPGA
PRINCE, GIFT	Block cipher - SPN with Key whitening	33008 $2^{16}+2^{7}+(56 * 2)$	FPGA and Micro-controller
SPECK	Block cipher – ARX	179	Micro-controller
PHOTON	Sponge based hash function	2^{12}	FPGA
Trivium and Grain	Stream Ciphers	2^{9} ,2^{13}	FPGA
Post Quantum Cryptography Primitives			FPGA







Evaluation and Design

Evaluation of security products are important for the systems that are used for protecting critical information infrastructure.

- Components like pseudo random number generator, symmetric key algorithms, public key algorithms can be evaluated for a specific threat model.
- Countermeasures resist the security product from side channel attack. SETS has home-grown expertise in the development of efficient countermeasure techniques. SETS will provide
  - Architecture and implementation of secure component for crypto systems
  - Secure implementation practices.

Contact

Society for Electronic Transactions and Security (SETS)
MGR Knowledge City, Taramani, Chennai – 600113
Phone : 044-66632503 **Fax** : 044-66632501
contact@setsindia.net
website:www.setsindia.in