FIPS 140-3 Security Requirements for Cryptographic Modules Non-Invasive Attack Testing

Research Goals:

-Develop test methods

Support our labs to perform testing

-Determine test metrics

For new FIPS 140-3 standard

FIPS 140-3 Is Coming

- 11 Security Requirement Areas for **Cryptographic Modules**

4. SECURITY REQUIREMENTS

4.1 Cryptographic Module Specification
4.2 Cryptographic Module Interfaces
4.3 Roles, Authentication and Services
4.4 Software/Firmware Security
4.5 Operational Environment
4.6 Physical Security
4.7 Physical Security – Non-Invasive Attacks
4.8 Sensitive Security Parameter Management
4.9 Self-Tests
4.10 Life-Cycle Assurance
4.11 Mitigation of Other Attacks

New!

Non-Invasive Attacks

- do not make any physical contact with the target module
- Exploit side-channel leaks
- Classes:

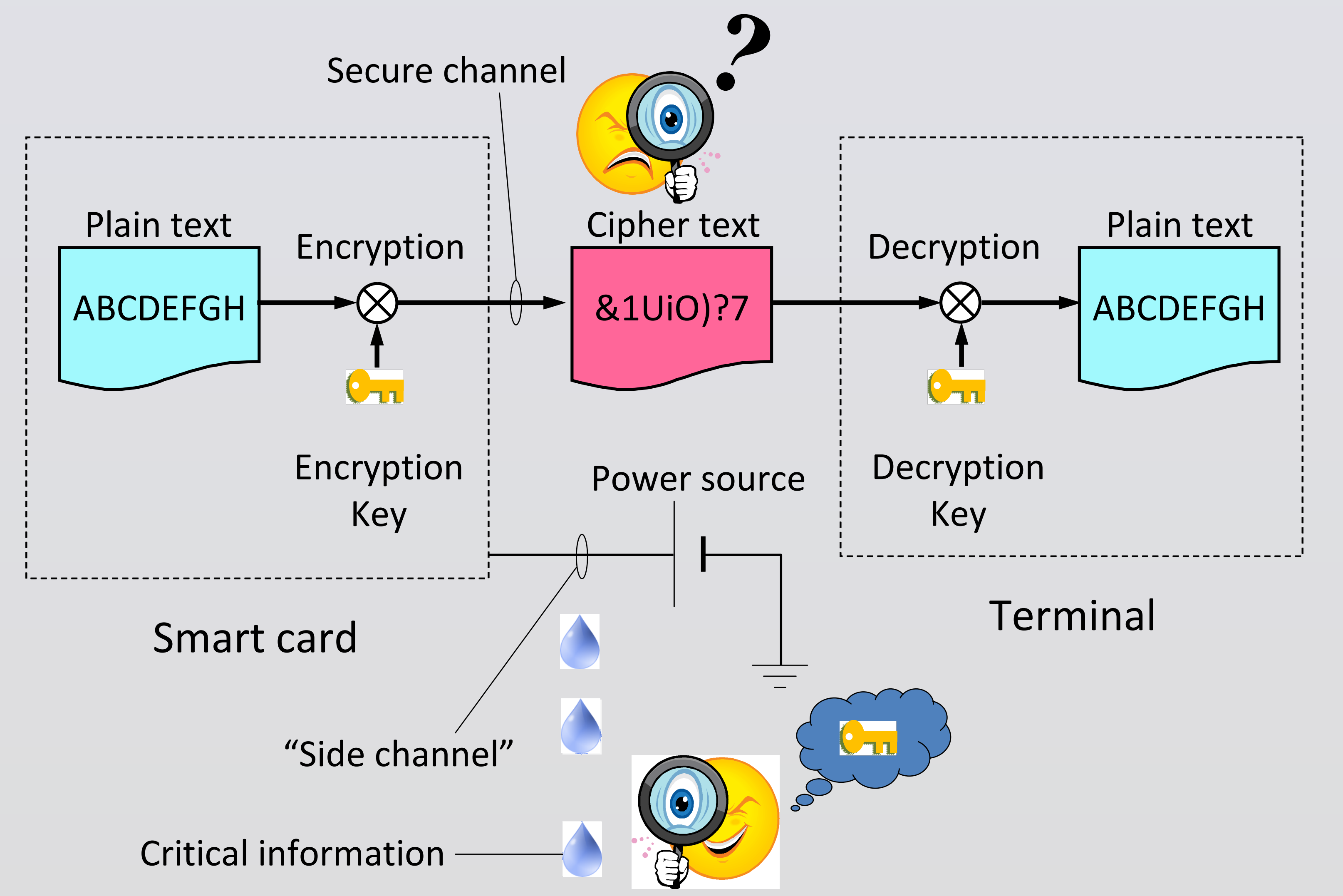
Power Analysis Attacks

Electromagnetic Analysis Attacks

Timing Attacks

Side-channel : A path for possible leak of information other than secured channels

Is Your Smart Card Secure?



Example: 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 PIN

-Portable → Easy for attackers to possess

→ Easy to observe side channels

→ Potential weakness against non-invasive attacks

Example: PIV Card

Are PIV cards secure against non-invasive side-channel attacks?

-FIPS 140-3 validation

-Effective testing to fail a vulnerable module

What if your PIV card is vulnerable?

-Someone picked up your card on the street

-He may be able to:

- Enter your building
- Access your email
- Electronically sign a purchase contract