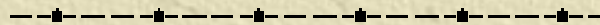




# *Cryptographic Testing, Validation & Certification*

**Assoc. Prof. Ahmet Koltuksuz, Ph. D.**  
ahmetkoltuksuz@iyte.edu.tr

Izmir Institute of Technology  
Department of Computer Engineering  
Information Systems Strategy & Security Lab.  
<http://is3.iyte.edu.tr>



# *AGENDA*

- #1 Introduction
- #2 Standards and NIST
- #3 Cryptographic Algorithm Test & Validation
- #4 Cryptographic Module Test & Validation
- #5 FIPS 140-2 Security Requirements For Cryptographic Modules
- #6 Side Channel Attacks
- #7 FIPS 140-2 & Common Criteria (CC) Relation
- #8 Common Criteria (CC)
- #9 How to be an approved CMT Lab
- #10 Recommendations

# *Section #1: Introduction*

- ✧ Cryptography and Standards
- ✧ Cryptographic Security Testing & Metrics

# *Cryptography*

- ✦ The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31]
- ✦ Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]



# *Cryptographic Security Testing & Metrics*

- ✦ Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas.
- ✦ At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication.

# *Cryptographic Security Testing & Metrics*

- ✦ Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render the product insecure and place highly sensitive information at risk.
- ✦ Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

## *Section #2: Standards & NIST*

- ✦ NIST & CSE
- ✦ Cryptographic Module Validation Program (CMVP)
- ✦ Cryptographic Algorithm Validation Program (CAVP)
- ✦ Cryptographic and Security Testing (CST) Laboratories  
(Cryptographic Module Testing (CMT) Labs.)

# *NIST*

- ✦ NIST: National Institute for Standards and Technology.
- ✦ Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce.
- ✦ NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.



# *NIST*

- ✦ NIST's FY 2008 resources total \$931.5 million. The agency operates in two campuses: Gaithersburg, Md. and Boulder, Colo.
- ✦ NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel.
- ✦ NIST hosts about 2,600 associates and facility users from academia, industry, and other government agencies.
- ✦ Check the web address of <http://www.nist.gov>

# *NIST & CSEC: CMVP*



✦ Cryptographic Module Validation Program (CMVP)

✦ <http://csrc.nist.gov/groups/STM/cmvp/index.html>

# *NIST & CSEC: CMVP*



✧ On July 17, 1995, the National Institute of Standards and Technology (NIST) established the [Cryptographic Module Validation Program \(CMVP\)](#) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards.

✧ The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC).

✧ FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 and supersedes FIPS 140-1.



# *NIST & CSEC: CMVP*



✱ The CMVP is a program under which National Voluntary Laboratory Accreditation Program (NVLAP) accredited Cryptographic Module Testing (CMT) laboratories test cryptographic modules for conformance to Federal Information Processing Standard Publication (FIPS) 140-2, Security Requirements for Cryptographic Modules.

✱ In addition, this program covers the testing of Approved security functions, including the Advanced Encryption Standard, Data Encryption Algorithm, Digital Signature Algorithm, Secure Hash Algorithm, and Skipjack Algorithm.



# *NIST & CSEC: CAVP*



✦ Cryptographic Algorithm Validation Program (CAVP)

✦ <http://csrc.nist.gov/groups/STM/cavp/index.html>

# *NIST & CSEC: CAVP*



- ✦ The [Cryptographic Algorithm Validation Program \(CAVP\)](#) encompasses validation testing for FIPS approved and NIST recommended cryptographic algorithms.
- ✦ Cryptographic algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP).
- ✦ The CAVP was established by NIST and the Communications Security Establishment Canada (CSEC) in July 1995.

# *CMT Labs: CMVP & CAVP Testing*



✳ Vendors of cryptographic modules (CMVP) and cryptographic algorithms (CAVP) use independent, accredited [Cryptographic Module Testing \(CMT\)](#) laboratories to test their modules as well as algorithms.

✳ All of the third-party laboratories that are accredited as [Cryptographic Module Testing \(CMT\) laboratories](#) are accredited by the National Voluntary Laboratory Accreditation Program (NVLAP).

✳ Vendors interested in validation testing of their algorithm implementation may select any of the accredited laboratories.



# CST-CMT Labs: Who does, What?

## CMVP

### FIPS 140-2 (140-3 draft)

## CAVP

### Symmetric Algorithms

- **FIPS 197:** *Advanced Encryption Standard (AES).*
- **FIPS 46-3 & FIPS 81:** *Data Encryption Standard (DES & Triple DES) and DES Modes of Operation.*
- **FIPS 185:** *Escrowed Encryption Standard (EES)*

### Asymmetric Algorithms

- **FIPS 186.2:** *Digital Signature Standard (DSS); DSA, RSA, and ECDSA.*

### Hash Algorithms

- **FIPS 180-2:** specifying **SHA-1, SHA 224-256-384-512**

### Random Number Generator Algorithms

- **FIPS 186-2:** Specifies the RNG for the DSA algorithm.
- **ANSI X9.31:** Specifies the RNG for the RSA algorithm.
- **ANSI X9.62:** Specifies the RNG for the ECDSA algorithm.

### Deterministic Random Bit Generator (DRBG) Algorithms

- **SP 800-90:** Specifies four algorithms for RNG using DRBGs.

### Message Authentication Algorithms

- **SP 800-38B:** *Recommendation for Block Cipher Modes of Operation*
- **SP 800-38C:** *Counter with Cipher Block Chaining - MAC (CCM).*
- **FIPS 198:** *Keyed-Hash Message Authentication Code (HMAC).*
- **FIPS 113:** *Computer Data Authentication*

## CMT TESTING LABORATORIES

**ÆGISOLVE, INC.** (USA - CA)

**Aspect Labs, a division of BKP Security, Inc.** (USA - CA)

**Atlan Laboratories** (USA - VA)

**atsec Information Security Corporation** (USA - TX)

**BT Cryptographic Module Testing Laboratory** (United Kingdom)

**CEAL: a CygnaCom Solutions Laboratory** (USA - VA)

**COACT Inc. CAFE Laboratory** (USA - MD)

**DOMUS IT Security Laboratory** (Canada)

**EWA - Canada IT Security Evaluation & Test Facility** (Canada)

**ICSA Labs, An Independent Division of Verizon Business** (USA - PA)

**InfoGard Laboratories, Inc.** (USA - CA)

**Science Applications International Corporation (SAIC)** (USA - MD)

**TÜV Informationstechnik GmbH** (Germany)





## Your Solution for Security Compliance

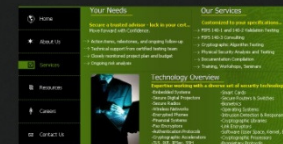


## Delivering the Right Assurance

➤ SERVICES   ➤ CAPABILITIES   ➤ EXPERIENCE



**CYGNACOM**  
SOLUTIONS



[Home](#) [About us](#) [Contact](#) [Legal Information](#) [Privacy](#) [Search](#) [Sitemap](#) [English](#)

IT Security IT Quality Certification Test Marks

Validation of crypto modules according to FIPS PUB 140-2



the information security provider

INFO | GARD

## Security Assurance

*Independence. Integrity. Trust.*



## *Section #3: Cryptographic Algorithm Test & Validation (CAVP)*

- ✦ How does a CST (CMT) Lab do it?
- ✦ Examples for testing & validation of DES

## *CMT Labs: Who does, How?*

✦ Currently the CAVP provides validation testing for the following algorithms:

1. Advanced Encryption Algorithm (AES),
2. Triple Data Encryption Algorithm (Triple-DES),
3. Data Encryption Algorithm (DES),
4. Digital Signature Algorithm (DSA),
5. Secure Hash Algorithm (SHA),
6. Random Number Generator (RNG),
7. Reversible Digital Signature Algorithm (RSA),
8. Elliptic Curve Digital Signature Algorithm (ECDSA),
9. Keyed-Hash Message Authentication Code (HMAC),
10. Counter with Cipher-Block Chaining-Message Authentication (CCM)
11. CMAC Algorithm (CMAC)



## *CMT Labs: Who does, How?*

### ✧ Testing and Validation of DES

NIST Special Publication 800-17  
Modes of Operation Validation System  
(MOVS): Requirements and Procedures

#### **Works for DES and SKIPJACK**

The MOVS for the DES and Skipjack algorithms consists of two types of tests, the **Known Answer tests (KATs)** and the **Modes tests (MTs)**.

The MOVS provides conformance testing for the individual components of an implementation under test (IUT) of the DES algorithm and analyzes IUTs of the DES and Skipjack algorithms for apparent operational errors.



## *CMT Labs: Who does, How?*

### ✧ Testing and Validation of DES

NIST Special Publication 800-17  
Modes of Operation Validation System  
(MOVS): Requirements and Procedures

#### **The Known Answer Tests**

The Known Answer tests are based on the standard DES test set discussed in SP500-20. When applied to IUTs of the DES algorithm, the Known Answer tests verify that the IUT correctly performs the algorithm. The tests also provide conformance testing for the following components of an IUT of the DES algorithm: the initial permutation IP, the inverse permutation  $IP^{-1}$ , the expansion matrix E, the data permutation P, the key permutations PC1 and PC2, and the substitution tables  $S$ ,  $S$ , ...,  $S$ . When applied to IUTs of the Skipjack algorithm, these same tests verify that the implemented algorithm produces the correct results, i.e., given known input, the correct results are produced.

## *CMT Labs: Who does, How?*

### ✧ Testing and Validation of DES

NIST Special Publication 800-17  
Modes of Operation Validation System  
(MOVS): Requirements and Procedures

#### **The Modes Test**

The Modes test is the second type of validation test required to validate IUTs of the DES and Skipjack algorithms. The Modes test is based on the Monte-Carlo test discussed in SP500-20.

They are designed to use pseudo-random data to verify that the IUT has not been designed just to pass the Known Answer tests. A successful series of Modes tests gives some assurance that an anomalous combination of inputs does not exist that would cause the test to end abnormally for reasons not directly related to the implementation of the algorithm. An additional purpose of the Modes test is to verify that no undesirable condition within the IUT will cause the key or plaintext to be exposed due to an implementation error. This test also checks for the presence of an apparent operational error.

## *CMT Labs: Who does, How?*

### ✧ Testing and Validation of DES

#### **The Variable Plaintext Known Answer Test - ECB Mode**

MOVS: Initialize KEY:

    If DES, KEY=0101010101010101 (odd parity set)

    If Skipjack, KEY=000000000000000000000000

    PT<sub>1</sub>= 800000000000000000000000

    Send KEY, PT<sub>1</sub>

IUT: FOR i = 1 to 64 {

    IB<sub>i</sub> = PT<sub>i</sub>

    Perform algorithm in encrypt state, resulting in CT<sub>i</sub>

    Send i, KEY, PT<sub>i</sub> , CT<sub>i</sub>

    PT<sub>i+1</sub> = basis vector where single "1" bit is in position I+1

}

MOVS: Compare results from each loop with known answers

If DES, use Appendix B, Table 1. If Skipjack, use Appendix B, Table 5.

## *CMT Labs: Who does, How?*

### ✦ Testing and Validation of DES

#### Appendix B Tables of Values for the Known Answer Tests

Table 1 Resulting Ciphertext from the Variable Plaintext Known Answer Test for DES

*(NOTE: KEY = 01 01 01 01 01 01 01 01 (odd parity set))*

ROUND	PLAINTEXT	CIPHERTEXT
0	80 00 00 00 00 00 00 00	95 F8 A5 E5 DD 31 D9 00
1	40 00 00 00 00 00 00 00	DD 7F 12 1C A5 01 56 19
2	20 00 00 00 00 00 00 00	2E 86 53 10 4F 38 34 EA
3	10 00 00 00 00 00 00 00	4B D3 88 FF 6C D8 1D 4F
4	08 00 00 00 00 00 00 00	20 B9 E7 67 B2 FB 14 56
5	04 00 00 00 00 00 00 00	55 57 93 80 D7 71 38 EF
.	.....	.....
.	.....	.....
.	.....	.....
63	00 00 00 00 00 00 00 01	16 6B 40 B4 4A BA 4B D6



## *CMT Labs: Who does, **How?***

✦ The complete resources are at

<http://csrc.nist.gov/groups/STM/cavp/documents/>

## *Section #4: Cryptographic Module Test & Validation (CMVP)*

- ✧ Challenges in FIPS 140-2 Validation
- ✧ A Road Map to FIPS 140-2 Certification
- ✧ CMVP Revisited
- ✧ Derived Test Requirements (DTRs)
- ✧ Implementation Guide
- ✧ Briefly...

## *Challenges in FIPS 140-2 Validation*

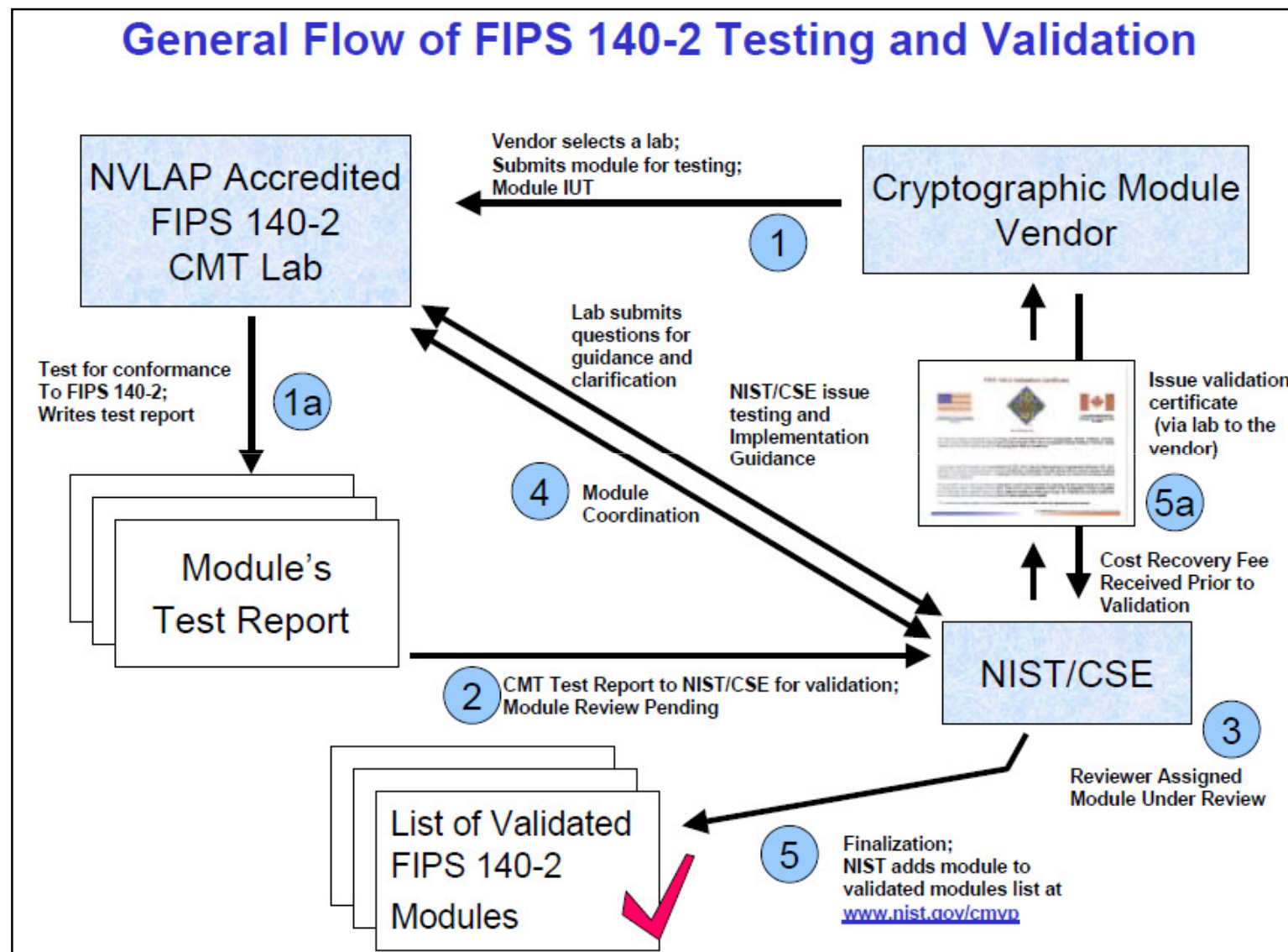
- ✧ Building to the FIPS 140-2 standard is complicated
- ✧ Increased need for in-house security expertise
- ✧ Evolving FIPS standards that require continual monitoring
- ✧ Platform specificity of each FIPS validation
- ✧ Requirement for re-validation when any feature changes are introduced into FIPS Validated product.





## A road map to FIPS 140-2 certification

S. #4



## *CMVP: Revisited*

To receive FIPS 140-2 validation, a cryptographic module must:

- ✱ have a well-defined “crypto boundary” so that all sensitive security information remains within the cryptographic core of the product.
- ✱ use at least one “FIPS-approved algorithm” with correct implementation and an intact crypto boundary.



## *CMVP: Revisited*

### NIST/CSE

- ✱ Review reports and issue validation certificates
- ✱ Issue CMVP policy
- ✱ Issue guidance and clarifications of FIPS 140-2
- ✱ Assist NVLAP and PALCAN in lab assessments

### NVLAP/PALCAN

- ✱ Accredite labs for quality and competence
- ✱ Perform periodic reassessments

### Vendors

- ✱ Provide necessary and required info and docs to the lab
- ✱ Review DTRs, policy and Implementation Guidance

### CST-CMTs

- ✱ Perform FIPS 140-2 and algorithm testing
- ✱ Intermediate between vendors and NIST/CSE



## *Derived Test Requirements (DTRs)*

### **Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules***

- ✱ The purpose of this document is to describe the methods that will be used by accredited laboratories to test whether the cryptographic module conforms to the requirements of FIPS PUB 140-2.
- ✱ It includes detailed procedures, inspections, and tests that the tester must follow, and the expected results that must be achieved for the cryptographic module to satisfy the FIPS PUB 140-2 requirements.
- ✱ Vendors may use this document as a guide in trying to determine if their cryptographic modules meet the security requirements of FIPS PUB 140-2 **before they apply to the laboratory for testing.**

## *Derived Test Requirements (DTRs)*

### **Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules***

- Cryptographic module testing is performed using the DTR
- Assertions in the DTR are directly traceable to requirements in FIPS 140-1 and FIPS 140-2
- FIPS 140-1 DTR assertions are either
  - Direct quotes from the standard or
  - Directly derivable from the requirements
- FIPS 140-2 DTR assertions map directly to FIPS 140-2 requirements

## *Derived Test Requirements (DTRs)*

### **Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules***

- All FIPS 140-2 requirements will be included in the DTR as assertions
  - Provides for one-to-one correspondence between the FIPS and the DTR
- Each assertion will include requirements levied on the
  - Cryptographic module vendor
  - Tester of the cryptographic module
- Modules tested against FIPS 140-2 will use the associated DTR



## *Derived Test Requirements (DTRs)*

### **Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules***

- DTRs are directly traceable to FIPS 140-1&2
- AS<reqmt\_no>.<assertion\_sequence\_no>
  - reqmt\_no - corresponding area in FIPS 140-1&2
  - assertion\_sequence\_no - sequential identifier for assertions within a section
  - Assertions map directly to requirements in FIPS 140-2
  - Example: AS03.13: Documentation shall provide a complete specification of all of the authorized roles supported by the module (1, 2, 3, and 4)

## *Derived Test Requirements (DTRs)*

### **Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules***

- **VE<reqmt\_no>.<assertion\_sequence\_no>.<sequence\_no>**
  - reqmt\_no - corresponding area in FIPS 140-1&2
  - assertion\_sequence\_no - sequential identifier for assertions within a section
  - sequence\_no - a sequential identifier for vendor requirements within the assertion
  - Example: VE03.01.01: Vendor documentation shall specify each distinct authorized role, including its name, purpose, and the services that are performed in the role

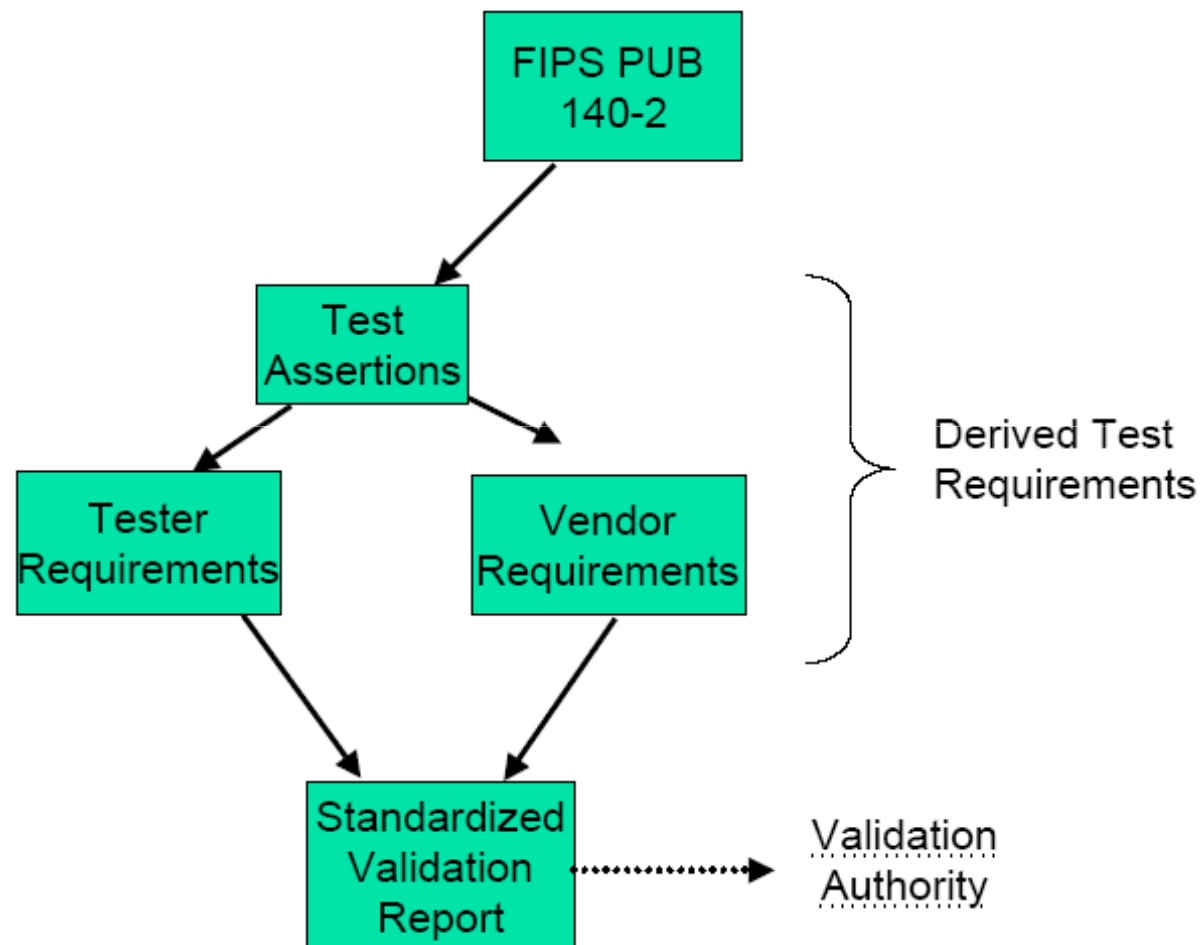
## *Derived Test Requirements (DTRs)*

### **Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules***

- TE<reqmt\_no>.<assertion\_sequence\_no>.<sequence\_no>
  - reqmt\_no - corresponding area in FIPS 140-1&2
  - assertion\_sequence\_no - sequential identifier for assertions within a section
  - sequence\_no - a sequential identifier for tester requirements within the assertion
  - Example: TE03.01.02: The tester shall assume each of the authorized roles described in the vendor documentation and verify that each of them can be assumed.



## Derived Test Requirements Development



## *Implementation Guide*

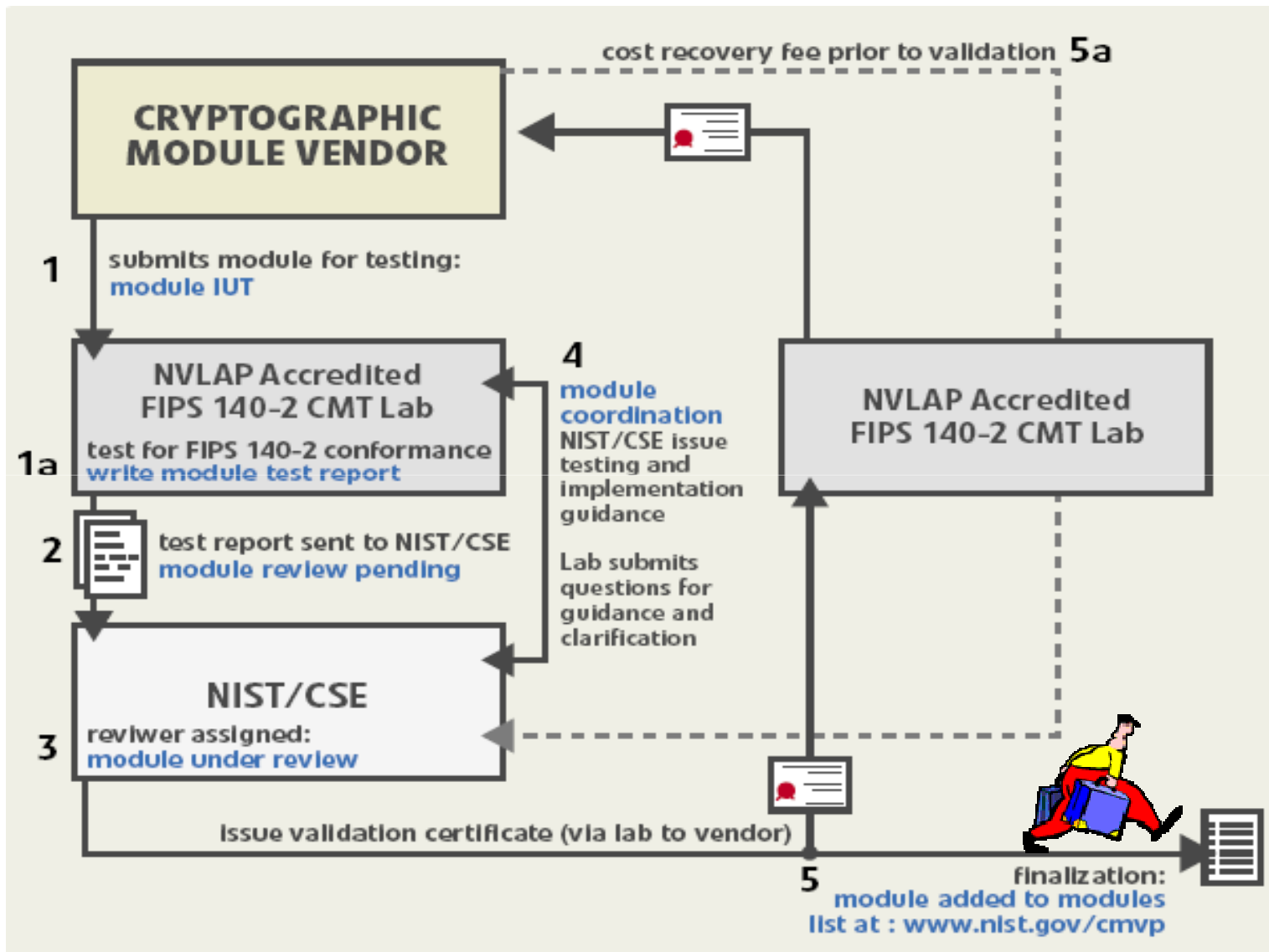
### **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**

✱ This document is intended to provide clarifications of the CMVP, and in particular, clarifications and guidance pertaining to the *Derived Test Requirements for FIPS PUB 140-2 (DTR)*, which is used by CMT laboratories to test for a cryptographic module's conformance to FIPS 140-2.

✱ Guidance presented in this document is based on responses issued by NIST and CSE to questions posed by the CMT labs, vendors, and other interested parties.

*In short...*

S. #4



*Dr. A. Koltuksuz*



*In short...*

## **The relationship of an algorithm validation to the FIPS 140-2 module validation**

- ✱ A cryptographic module validated to FIPS 140-2 shall implement at least one Approved security function used in an Approved mode of operation.
- ✱ For an algorithm to be listed on a module validation certificate as an Approved security function, the algorithm implementation must meet all the requirements of FIPS 140-2 and must have received an algorithm validation certificate.
- ✱ A product or implementation does not meet the FIPS 140-2 applicability requirements by simply implementing an Approved security function and acquiring algorithm validation certificates.

## *Section #5: FIPS 140-2 Security Requirements for Cryptographic Modules*

- ✧ Why FIPS 140-2
- ✧ A Short History
- ✧ An Umbrella Standard
- ✧ 4 Levels of Security
- ✧ 11 Requirements
- ✧ A Finite State Model Example
- ✧ Security Levels and Requirements Relations
- ✧ Appendices and Annexes

## *Why FIPS 140-2 ?*

### ✦ Help Non-Experts

- Commercial Off-The-Shelf Technology
- Thorough & Applicable
- Verified, Easy To Validate
- A Standard Approach To Standards





## *FIPS 140-2, A Short History*

- ✦ Federal Standard 1027 (General Reqs. for Equipment using DES)
  - Very HW oriented
  - Restrictive
  
- ✦ FIPS 140 (Only the cover changed)
  
- ✦ FIPS 140-1 (11 Jan 1994)
  - Giving flexibility to vendors
  - Still HW oriented
  - Recognizing SW modules
  
- ✦ FIPS 140-2 (25 May 2001)
  - Clarified some reqs.
  - Incorporation of refinements contained in Implementation Guidance
  - Introduction of Design Assurance



*FIPS 140-2:*  
*“An Umbrella Cryptographic Standard”*



- ✦ The Basic Federal Standard
- ✦ We can “Fill In The Blanks”
- ✦ Choice of “4 Security Levels”
- ✦ Covers “11 Security Requirements”

## Security Levels and Requirements Relations

S. #5

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Dr. A. Koltuksuz



## *FIPS 140-2 Offers 4 Levels of Security*

- ✦ Level 1 to Level 4
- ✦ Most Secure Is 4
- ✦ Requirements Are Cumulative
- ✦ Varies Among Requirements
- ✦ We Can Set Level



## *FIPS 140-2 Security Levels*

- ✦ **Security Level #1** provides the lowest level of security. It specifies basic security requirements for a cryptographic module (for software implementation only).
- ✦ **Security Level #2** improves the physical security of a Security Level 1 cryptographic module by adding the requirement for tamper evident coatings or seals, or for pick-resistant locks.

## *FIPS 140-2 Security Levels*

- ✦ **Security Level #3** requires enhanced physical security, attempting to prevent the intruder from gaining access to critical security parameters held within the module.
- ✦ **Security Level #4** provides the highest level of security. Level 4 physical security provides an envelope of protection around the cryptographic module to detect a penetration of the device from any direction



## *FIPS 140-2 Addresses 11 Requirements*

1. Cryptographic Module Specification
2. Ports & Interfaces
3. Roles, Services & Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. EMI/EMC
8. Key Management
9. Self-Tests
10. Design Assurance
11. Mitigation Of Other Attacks

And Useful Appendices

## Requirement #1

### *CRYPTOGRAPHIC MODULE SPECIFICATION GIVES BOUNDARIES & ALGORITHMS*

- ✦ Boundary Scopes What Is Included
  - Closed Surface Includes Everything
  - Small Facilitates Module Reuse
  
- ✦ Algorithms From Approved List
  - Established Security
  - All Our Algorithms There
  - “Annex A” To FIPS 140-2

## Requirement #2

S. #5

### *PORTS AND INTERFACES SPECIFY INPUT AND OUTPUT*

- ✦ Define How Data Crosses the Boundary
- ✦ Physical Ports/Logical Interfaces
- ✦ Data Differs From Control
- ✦ Four Interfaces
  - Data In
  - Data Out
  - Control In
  - Status Out

## Requirement #3

S. #5

### *ROLES, SERVICES, & AUTHENTICATION GOVERN USERS*

- ✦ Roles: User, Maintenance, Crypto-Officer
- ✦ Services Describe CM Capabilities
  - Perform Approved Security Function
  - Display Status
  - Self-Test
  - May Support Bypass
- ✦ May Authorize Action By Role Or ID
  - Authentication Strength Varies By Level



## Requirement #4

S. #5

*FINITE STATE MODEL TELLS WHAT THE MODULE IS DOING*

- ✦ ID All Operational & Error States
  - Power On, Testing
  - Maintenance, Key Change
  - Error, Bypass, Others
- ✦ ID Conditions For State Change

## Requirement #5

### *PHYSICAL SECURITY CONTROLS TAMPER FOR 3 PHYSICAL EMBODIMENTS*

- ✦ Single Chip
- ✦ Multi-Chip (Embedded)
- ✦ Multi-Chip (Stand-Alone)
- ✦ Prevent, Detect, Evidence Tamper
- ✦ Depends On Security Level, Embodiment
- ✦ Automatic Re-zero On Maintenance
- ✦ Environmental Failure Protection (Lev. 4)

## Requirement #6

### *OPERATIONAL ENVIRONMENT RELATES TO COMPUTER OS*

- ✦ OS = Operating System
- ✦ OS Can Weaken Security
- ✦ OS May Be Fixed Or Variable
- ✦ Details Tied To CC Evaluation Level

## Requirement #7

S. #5

*KEY MANAGEMENT TELLS HOW TO MAKE, STORE  
& PASS KEYS*

### ✦ Focus On Key Life Cycle

- Good Random Number Generator
- Key Generation/Establishment
- Key Entry/Output
- Key Storage, Assigned By User
- Key Zeroization



## Requirement #8

S. #5

### *EMI/EMC COVERS ELECTROMAGNETIC INTERFERENCE*

- ✦ Comply with 47 Code of Fed Regs. Class A (Lev. 1 & 2)
- ✦ Comply with 47 Code of Fed Regs. Class B (Lev. 3 & 4)
- ✦ No TEMPEST Protection
- ✦ No RADAR Protection

## Requirement #9

S. #5

***SELF-TESTS** ASSURE THE MODULE IS OPERATING RIGHT*

- ✦ Power-Up Tests Automatically
  - Cryptographic Algorithm Test
  - SW/FW Integrity Test
  - Critical Function Test
  
- ✦ Conditional Tests
  - Pair-wise Consistency Test
  - SW/FW Load Test
  - Manuel Key Entry Test
  - Continous RNG Test
  - By-Pass Test

## Requirement #10

S. #5

### *DESIGN ASSURANCE ASSURES GOOD INSTALLATION & OPERATION*

- ✦ Configuration Management Assures Meeting Requirements
- ✦ Secure Delivery & Operation
- ✦ Proper Development
- ✦ Guidance Documents

## Requirement #11

S. #5

### *MITIGATION OF OTHER ATTACKS*

✦ Attacks for which NIST certified tests are currently **unavailable**

- Power Analysis
  - Timing Analysis
  - Fault Induction
  - TEMPEST
- } Side Channel Attacks



## Requirement #4: A Finite State Model Example

S. #5



**Cryptographic Equipment  
Assessment Laboratory (CEAL)**

- ✦ The CryptoGarage 900 is a FIPS 140-2 level 1 compliant cryptographic garage door controller.
- ✦ The CryptoGarage 900 is featuring all the amenities of the 800 series, cryptographic user authentication, state-of-the art door interlock safety control, automatic shop light, and pretty flashing LEDs.
- ✦ All communication with the remote device is cryptographically protected to prevent sophisticated thieves from intercepting your private communications with your CryptoGarage 900.

## Requirement #4: A Finite State Model Example

S. #5



**Cryptographic Equipment  
Assessment Laboratory (CEAL)**

- ✦ The CryptoGarage must be activated with the radio frequency remote control.
- ✦ Activation uses a challenge response with SKIPJACK encryption using symmetric keys.
- ✦ Once activated, the door can be raised and lowered until it is deactivated.
- ✦ Deactivation is either explicit using the remote, or implicit using a one-minute timeout circuit.

## Requirement #4: A Finite State Model Example

S. #5



Cryptographic Equipment  
Assessment Laboratory (CEAL)

### States

- |               |                  |
|---------------|------------------|
| ✦ Power-Up    | ✦ Down           |
| ✦ Power-Down  | ✦ Moving on Up   |
| ✦ No Key      | ✦ Moving on Down |
| ✦ Deactivated | ✦ Safety Error   |
| ✦ Activated   | ✦ Security Error |
| ✦ Up          | ✦ Self-Destruct  |

## Requirement #4: A Finite State Model Example

S. #5

**CYGNACOM**  
SOLUTIONS

Cryptographic Equipment  
Assessment Laboratory (CEAL)

### State Transitions

•	<u>Current State</u>	<u>Input</u>	<u>Output</u>	<u>Next State</u>
•	Power, Up	No Skipjack Key	No Key LED lit	No Key
•	Power Up	Skipjack Key Loaded	Pretty LEDs lit	Deactivated
•	Power Down	Self-destruct Command	Boom	Self Destruct
•	Self Destruct	Any Command	Boom	Self Destruct
•	No Key	Successful Key Entry	Pretty LEDs lit & flash	Deactivated
•	Deactivated	Successful Challenge	Pretty LEDs lit	Activated
•	Activated	Door is closed	All LEDs lit	Up
•	Activated	Door is open	All LEDs off	Down
•	Activated	Timer Off	Pretty LEDs lit	Deactivated
•	Activated	Deactivate Command	Pretty LEDs lit	Deactivated
•	Up	Close Command	Pretty LEDs lit	Moving on Down
•	Up	ACSC	LEDs flash	Safety Error
•	Down	Open Command	Pretty LEDs lit	Moving on Up
•	Down	ACSC	LEDs flash	Safety Error
•	Moving on Up	Close Command	Pretty LEDs lit	Moving on Down
•	Moving on Up	ACSC	LEDs flash	Safety Error
•	Moving on Up	Reached Top	All LEDs lit	Up
•	Moving on Down	Open Command	Pretty LEDs lit	Moving on Up
•	Moving on Down	ACSC	LEDs flash	Safety Error
•	Moving on Down	Reached Bottom	All LEDs off	Down
•	Safety Error	ACSC off	Pretty LEDs	Self Test
•	Safety Error	ACSC	LEDs flash	Safety Error
•	Any State	Bad Encryption	LEDs flash	Security Error
•	Security Error	Auto Transition	All LEDs flash	Deactivated

*Dr. A. Koltuksuz*



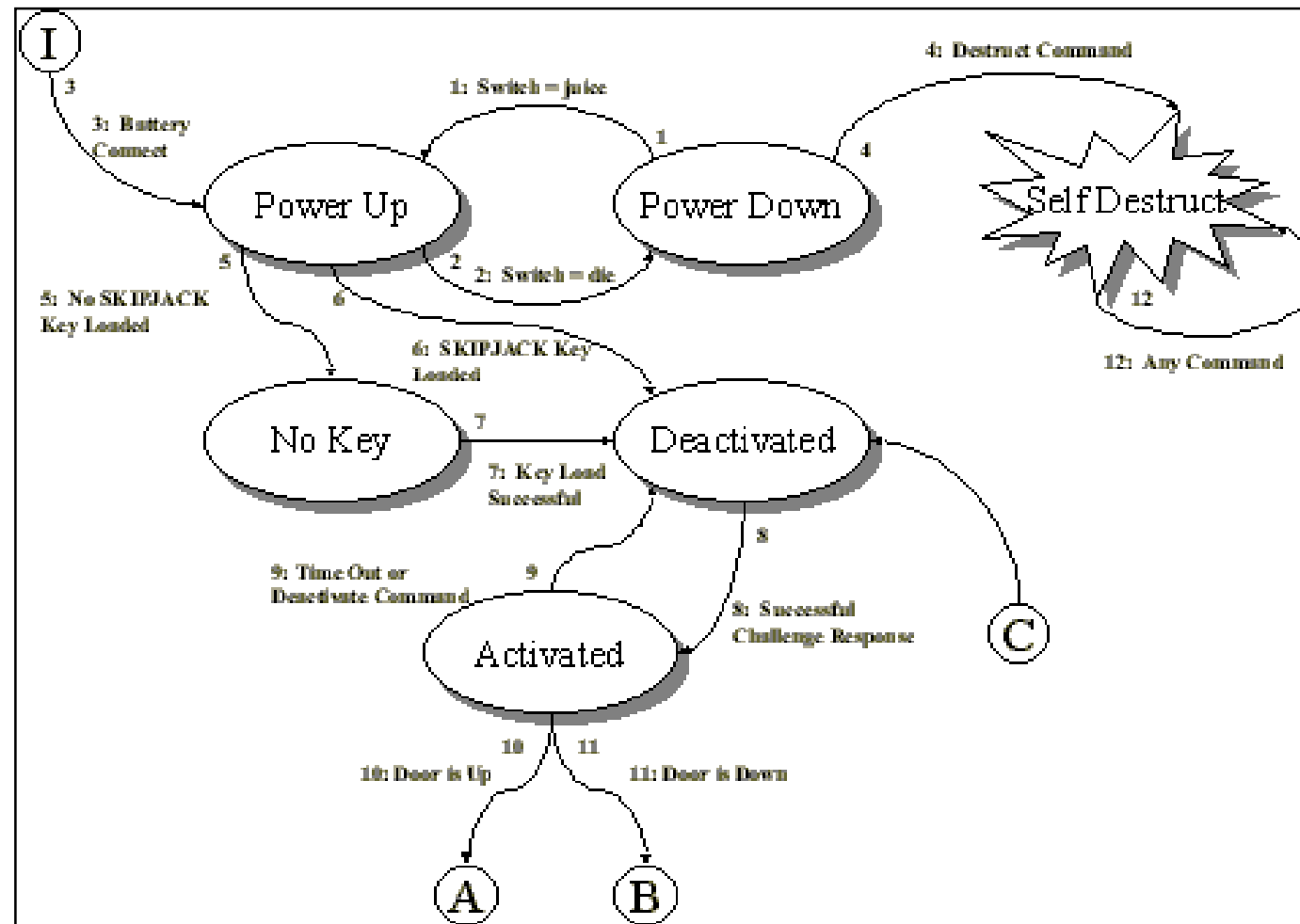
## Requirement #4: A Finite State Model Example

S. #5

**CYGNACOM**  
SOLUTIONS

Cryptographic Equipment  
Assessment Laboratory (CEAL)

### Finite State Diagram



Dr. A. Koltuksuz

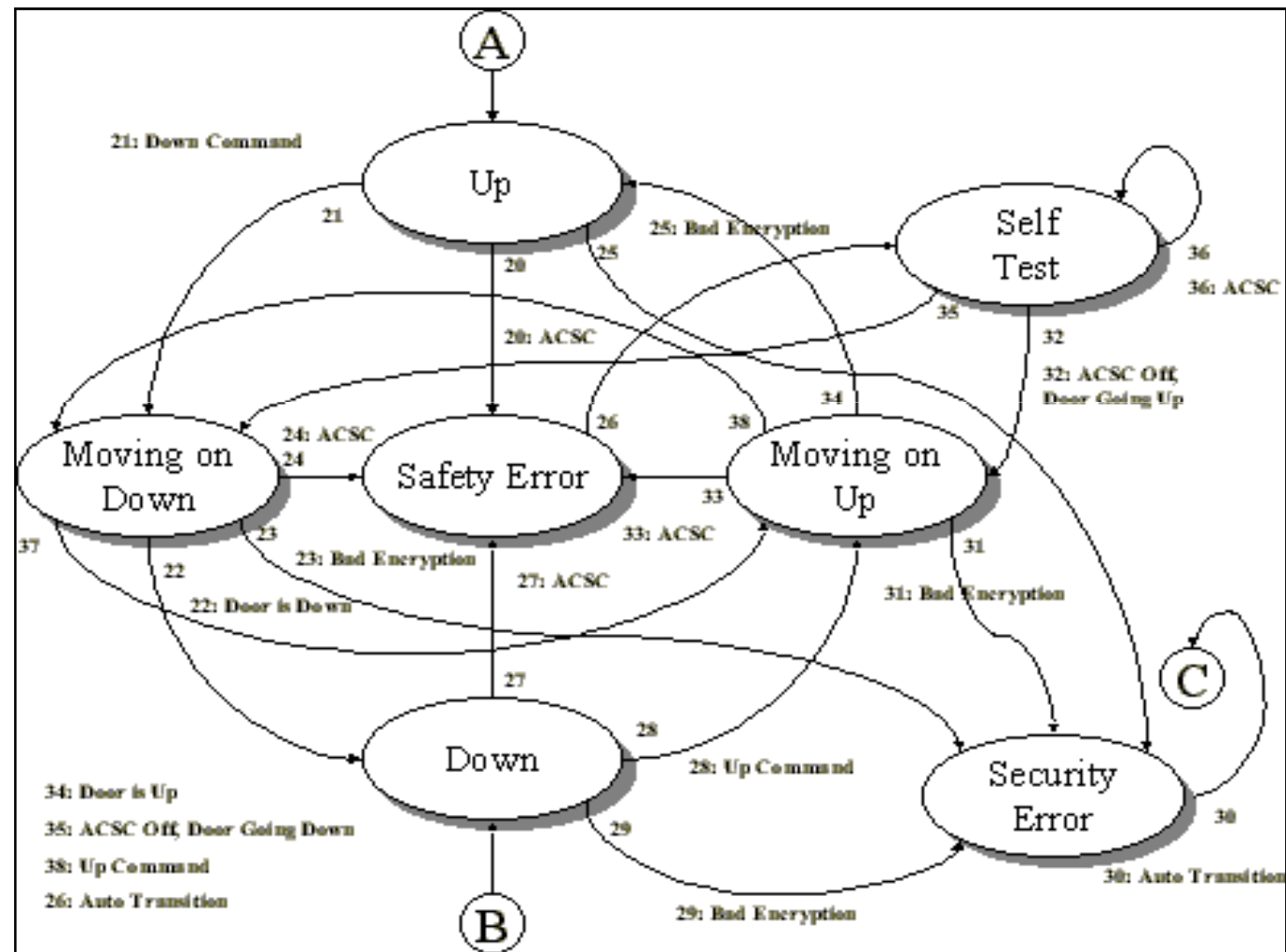
## Requirement #4: A Finite State Model Example

S. #5

**CYGNACOM**  
SOLUTIONS

Cryptographic Equipment  
Assessment Laboratory (CEAL)

### Finite State Diagram



## Security Levels and Requirements Relations

S. #5

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Dr. A. Koltuksuz

## *APPENDICIES HAVE USEFUL IDEAS & INFORMATION*

- ✧ Documentation Requirements
- ✧ Software Writing Recommendations
- ✧ Cryptographic Security Policy
- ✧ References



## *ANNEXES HAVE APPROVED TECHNICAL OPTIONS*

- ✧ Security Functions
- ✧ Protection Profiles (CC)
- ✧ Random Number Generators
- ✧ Key Establishment Techniques

## *Section #6: Side Channel Attacks*

- ✧ DLP
- ✧ DLP & DHKE
- ✧ EC
- ✧ EC & ECDLP
- ✧ Solutions to ECDLP
  - Timing attack (TA)
  - Simple power analysis (SPA)
  - Differential power analysis (DPA)
  - Fault induction attack (DFA)

M.Ciet, UCL Cryptogroup

## *The Problem*

- ✦ ECDLP: Elliptic Curve Discrete Logarithm Problem
- ✦ Knowing  $E(K)$  an elliptic curve defined over  $K$ ,  $P$  and;  $Q := kP$  two points of the curve, ECDLP consists of finding  $k$ .

## *Methods to Solve the ECDLP*

### ✧ General

- Giant Step, Baby Step
- Pollard  $\rho$
- Pohlig-Hellman
- Index Calculus

### ✧ Specific to the curve

- MOV Attack
- Weil Descent

### ✧ Implementation dependent

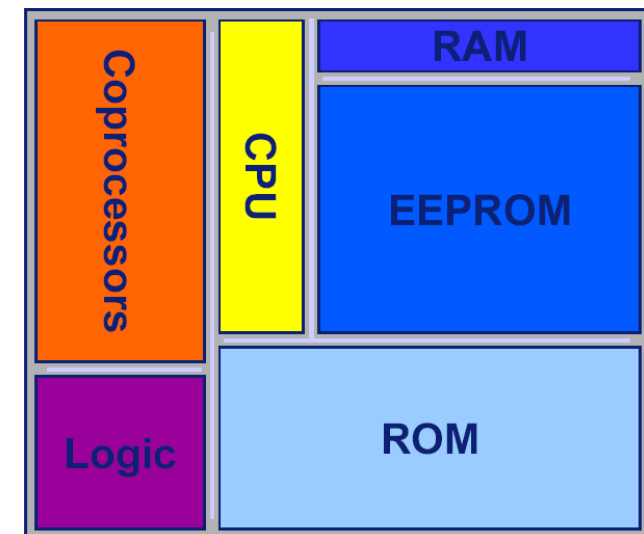
- Timing Attack
- Simple/Differential Analysis
- Fault Attack

Side Channel  
Attacks



## *Smart Card: A very basic structure*

- ✦ Complete area is less than 25mm<sup>2</sup>.
- ✦ FameXE (ECC) (in 2002 by Philips)
  - 1024 bit RSA, 100 ms
  - Optimized for ECC based algorithms
  - GF(2<sup>m</sup>), scalable length of operands

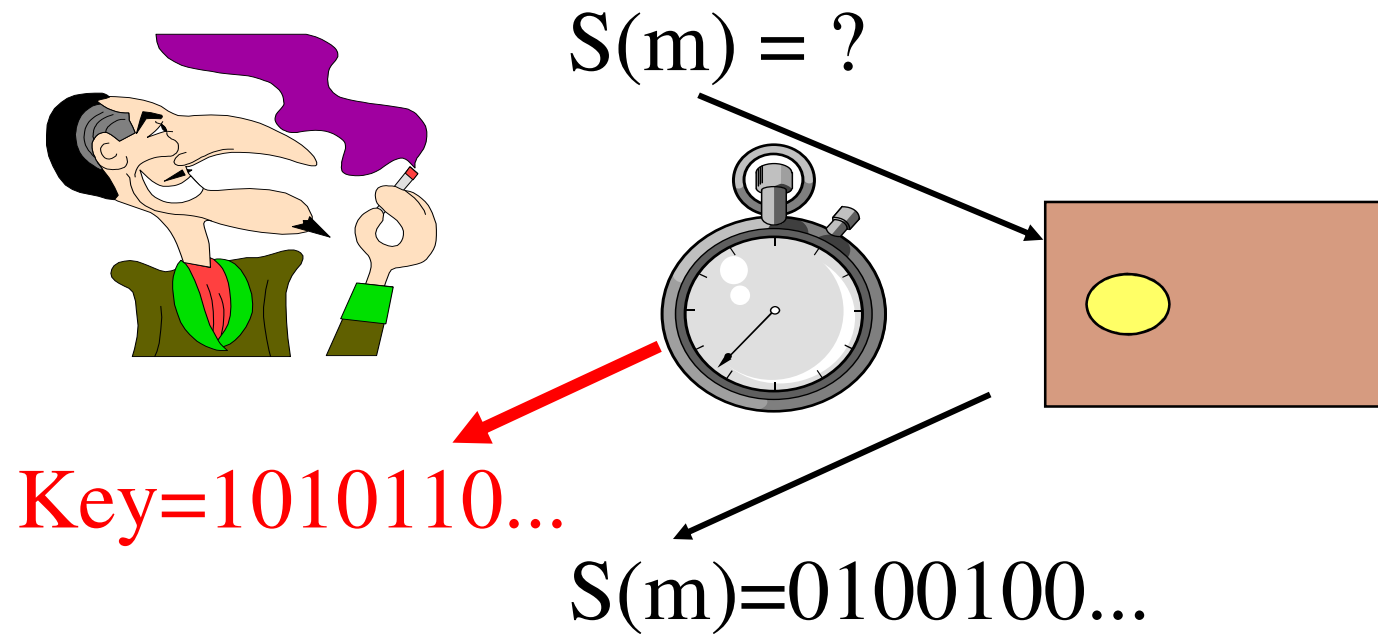


## *Leakages*

- ✦ Most known attacks against smart cards:
  - Timing Attack [Kocher]
  - SPA/DPA [Kocher, Jaffe and Jun]
  - Faults Insertions [Boneh]
  - Electromagnetic Analysis [Quisquater and Samyde, Gandolfi, Mourtel and Olivier]

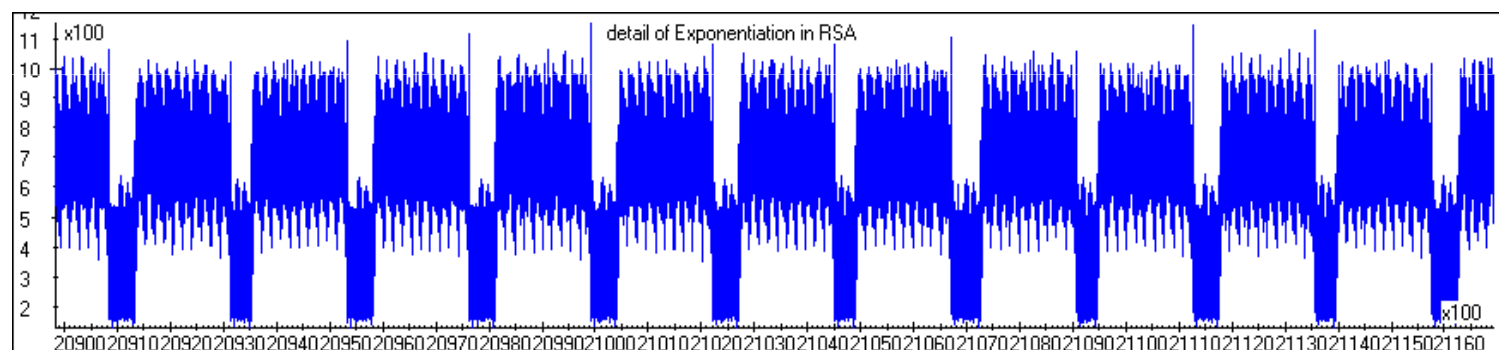
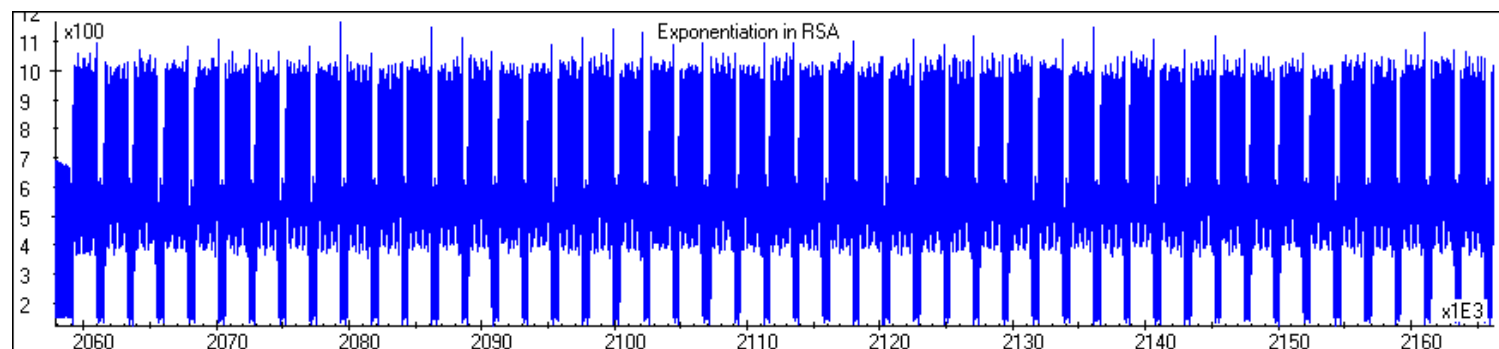
External leakages can be used to retrieve the  
secrete key

## Timing Attack



Times for addition and duplication operations are not the same!!!

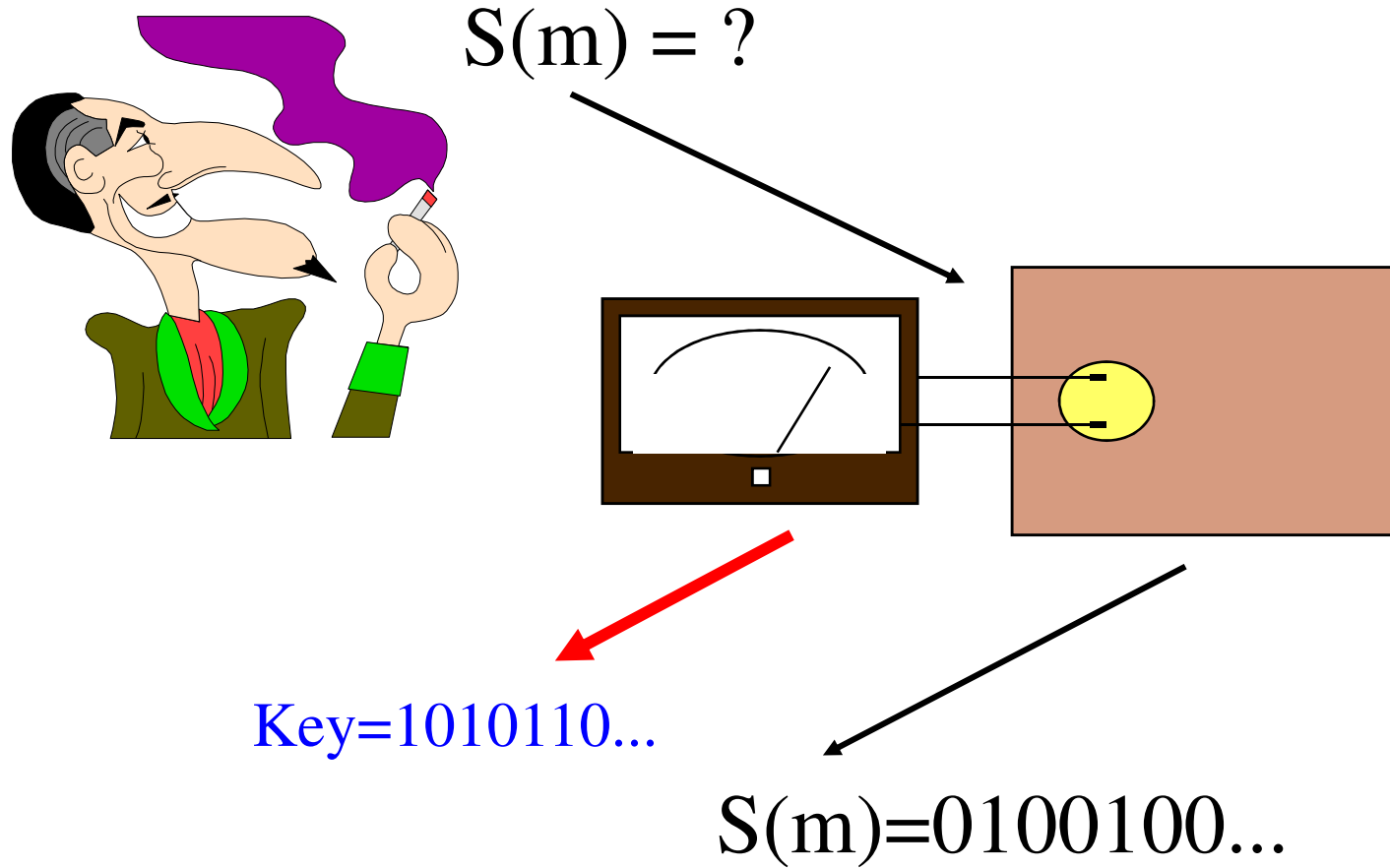
## Timing Attack on RSA



1 0 0 0 1 1 1



# Power Analysis Attack



## *Time/Power Analysis*

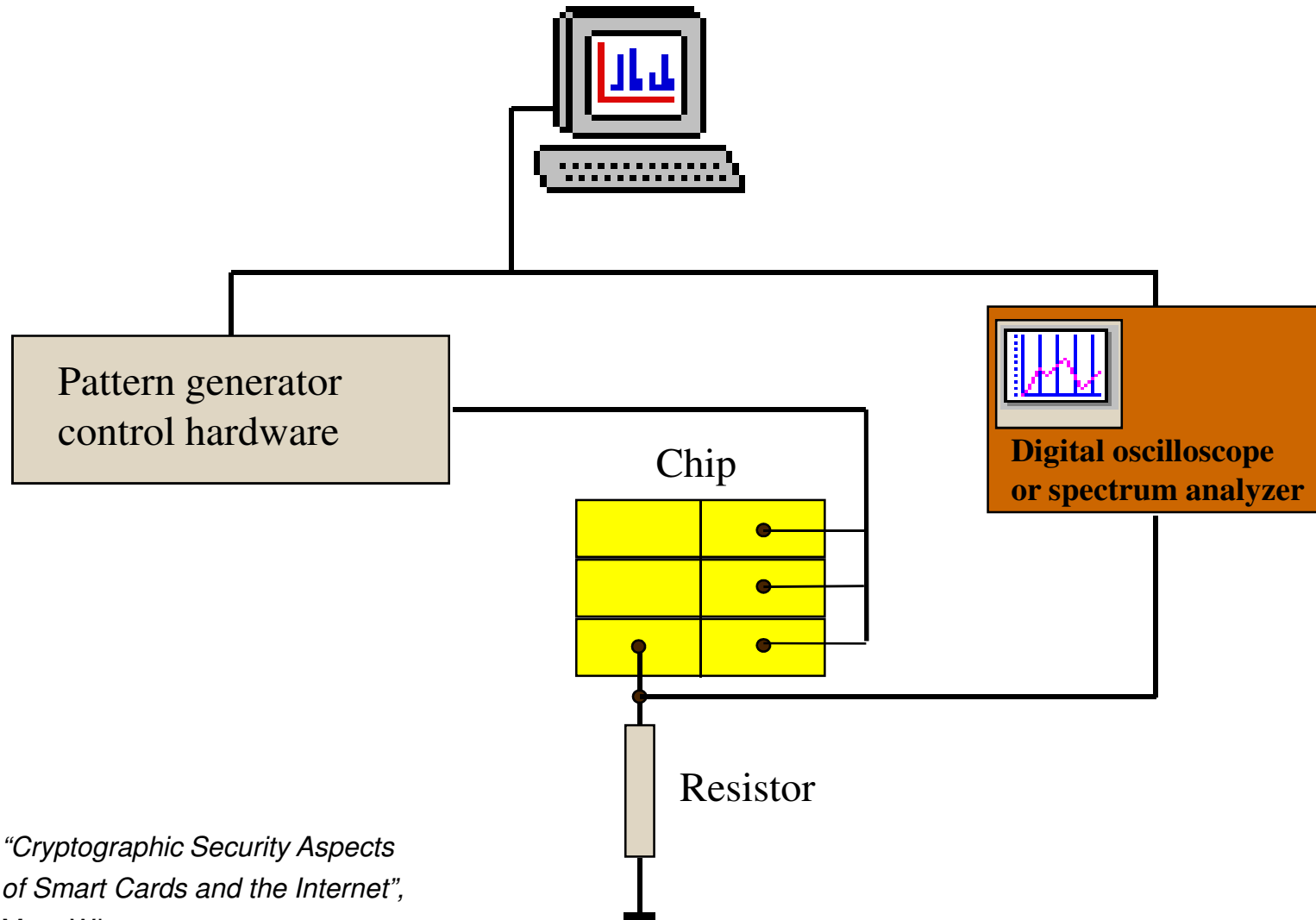
### ✦ Measure

- duration of operations.
- power consumption during operation
- duration of partial power traces

### ✦ Analyse

- role of time within an algorithm
- hamming weight of processed data
- instruction signature and program code structure
- statistical differences between power traces

# Power analysis configuration



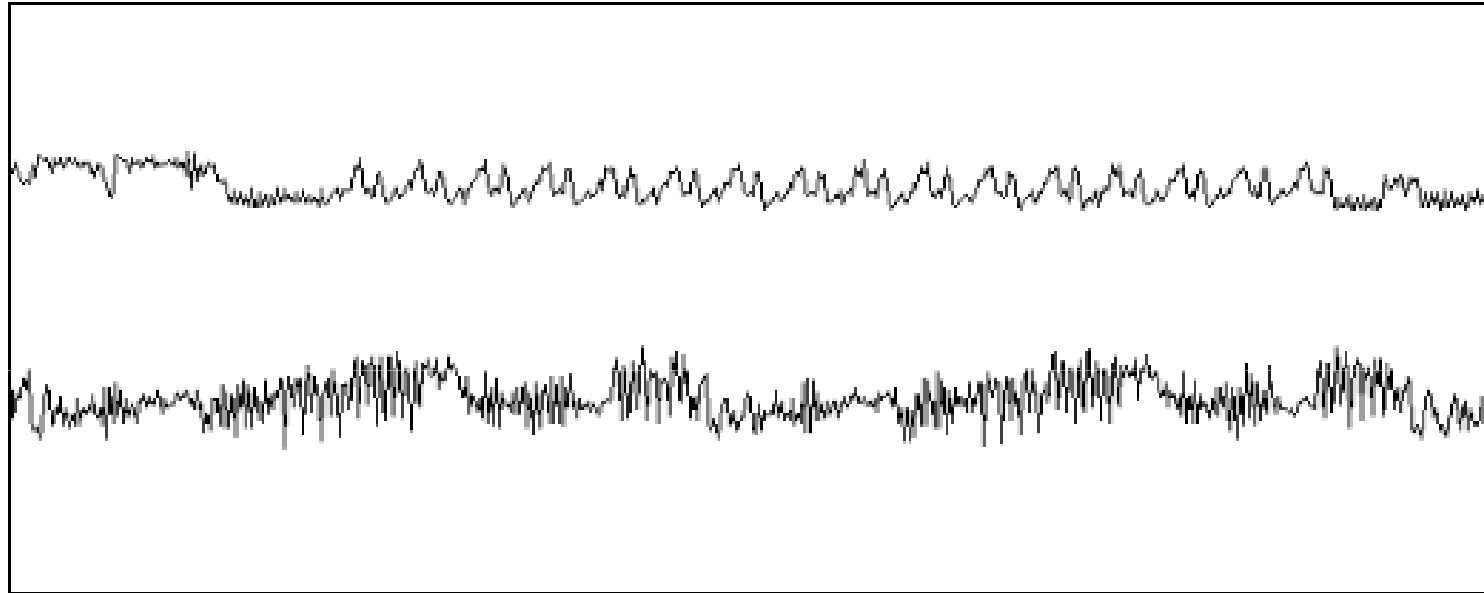
*"Cryptographic Security Aspects  
of Smart Cards and the Internet",  
Marc Witteman*

## *Simple Power Analysis*

- ✦ Depending on
  - the operations it performs
  - the data it handles
- ✦ smart card's energy needs will vary.
- ✦ Therefore, if we monitor energy needs, we will have something about data.
- ✦ Better in the case of asymmetric schemes



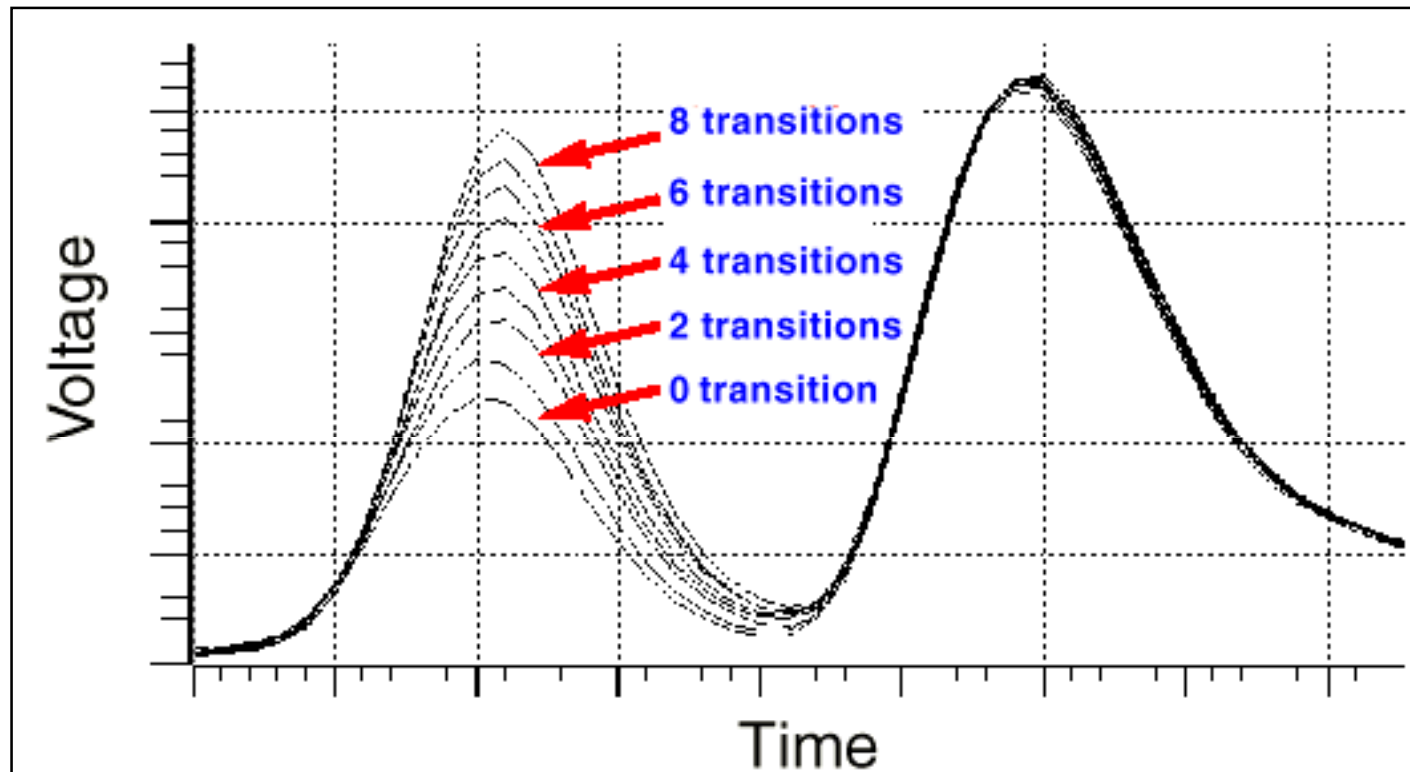
## *Operation-dependent variation*



DES: initial permutation, 16 rounds, final permutation

Paul Kocher,  
Introduction to DPA and Related Attacks

## *Data-dependent variation*



Power consumption shows *how many* bits have changed.

Th.S. Messerges, E.A. Dabbish & R.H. Sloan  
[CHES '99]

## *Differential power analysis*

### ✦ Simple power analysis:

- monitor power consumption of one computation
- very detailed knowledge of implementation needed

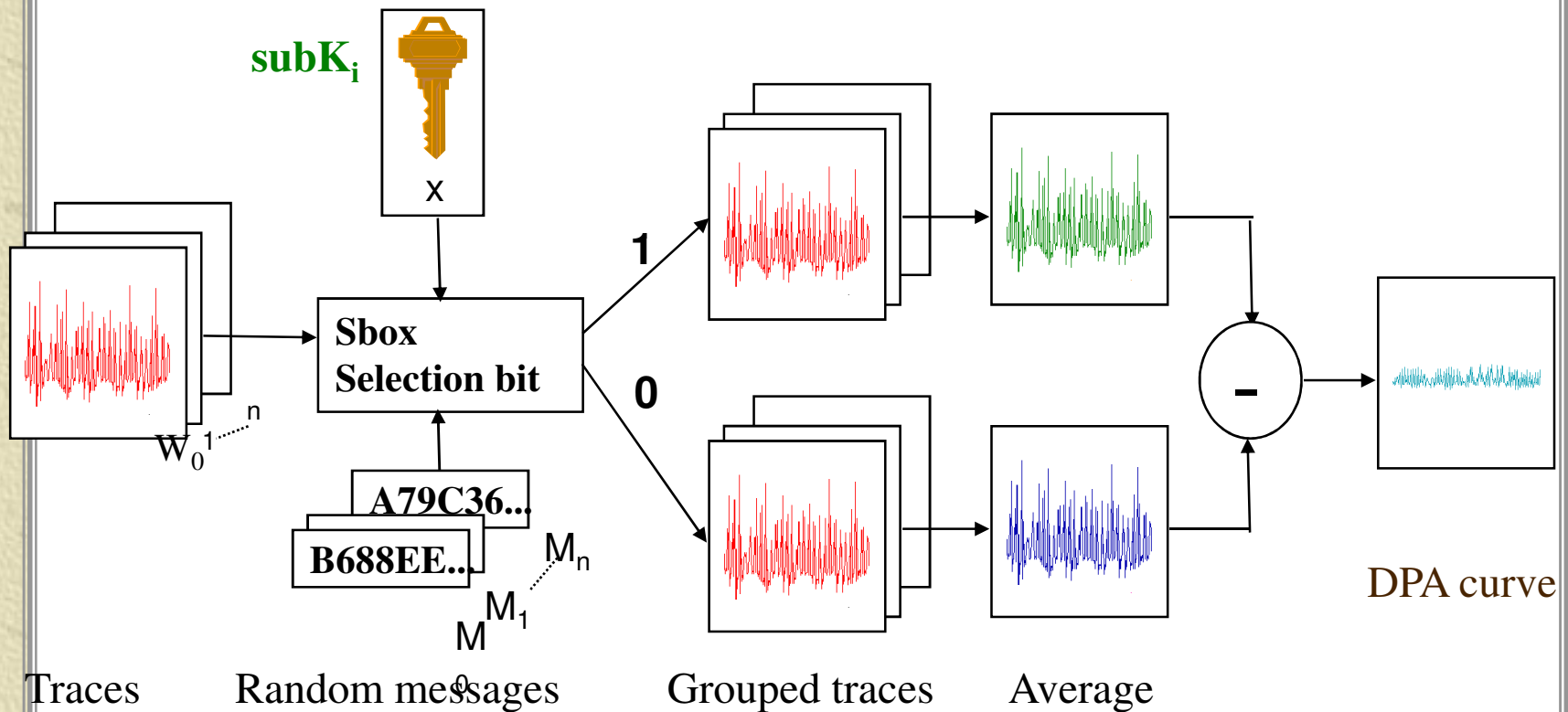
### ✦ Differential power analysis:

- monitor consumption difference between several computations
- almost no knowledge of implementation needed
- Independent of the architecture

# Differential Power Analysis

## ✦ DPA on DES [Kocher]

- 1<sup>st</sup> round : 1 selection bit on each of 8 Sbox output
- Test 64  $\text{subK}_i$  guesses (input 6 bits: 0 to 63) with 64 DPA curves

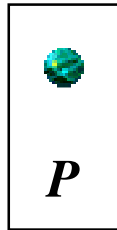


Gandolfi, Mourtel and Olivier [CHES 2001]

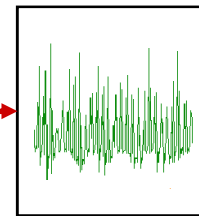
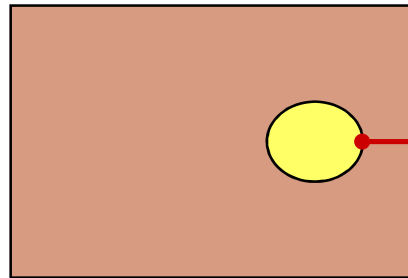


## *DPA: Elliptic Curves*

$P$  be the public  
point



$k$  the secret  
key



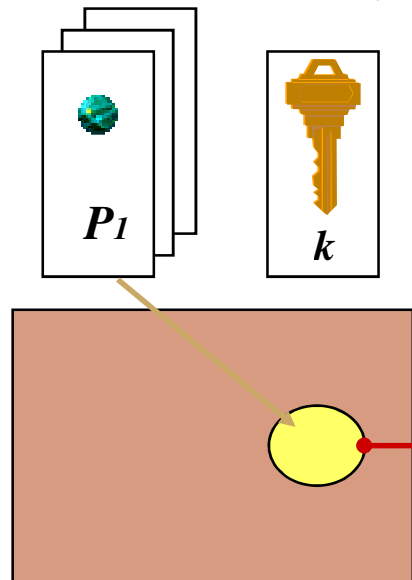
Power consumption  
associated to the  
computation of  $kP$

$kP$

## DPA: Elliptic Curves

$P_1 \dots P_e$  be  $e$  random points

$k$  the secret key



$C_i(t)$  be the side channel information

Power consumption associated to the computation of  $k_i P$

$$Q_i = kP_i$$

## *DPA: Elliptic Curves*

Let  $k = (k_{l-1}, \dots, k_0)$  be the binary representation of  $k$

We know that  $k_{l-1} = 1$

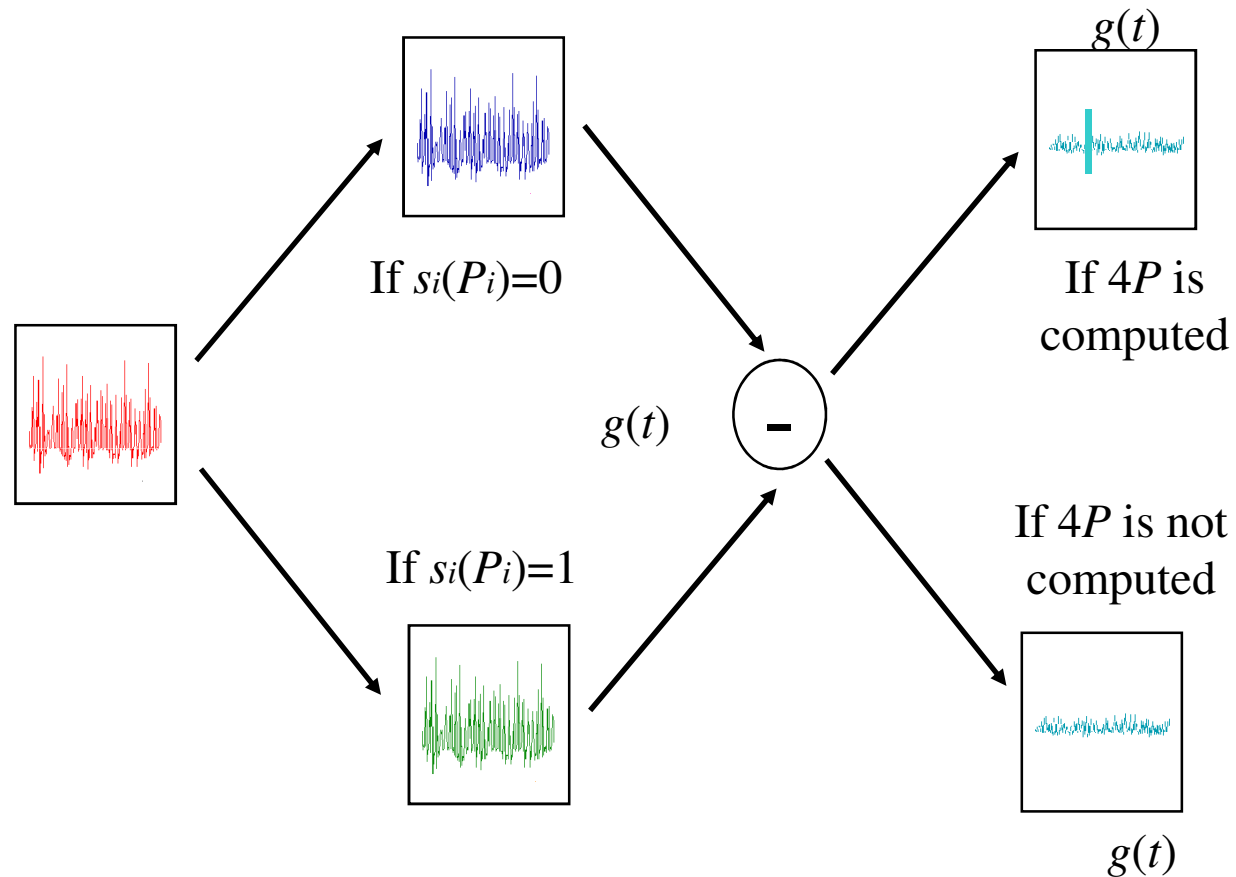
$k_{l-2} = 0 \longrightarrow 4P$  is computed


$k_{l-2} = 1 \longrightarrow 4P$  is **NEVER** computed

$k_{l-2} = 0 \longrightarrow 4P_i$  are computed

$k_{l-2} = 1 \longrightarrow 4P_i$  are **NEVER** computed

## DPA: Elliptic Curves



 The value of  $k_{l-2}$  is obtained, and the process is repeated with  $k_{l-3}$  and  $12P$  ...



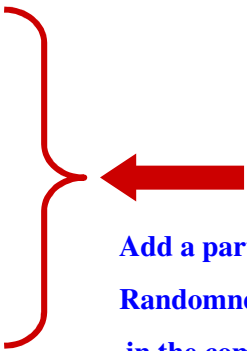
# *DPA Countermeasures*

## ✧ Hardware

- reduce signal by equalising the power
- add amplitude noise
- use variable clock

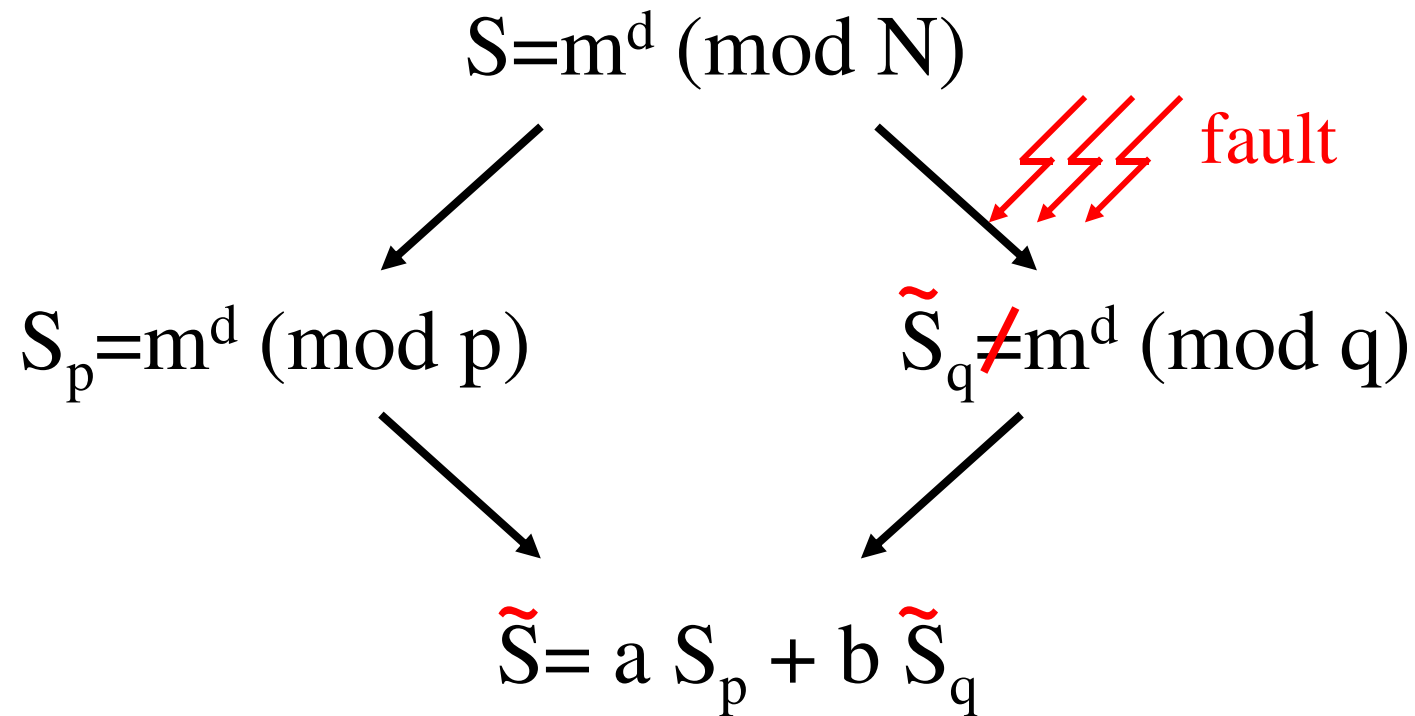
## ✧ Software

- eliminate timing relation with processed data
- reduce signal by random ordering of processes
- add random delays
- blind intermediate values with random values



Add a part of  
Randomness  
in the computation

## *Fault attacks on CRT*



where:

$$a = 1 \pmod{p}$$

$$a = 0 \pmod{q}$$

$$b = 0 \pmod{p}$$

$$b = 1 \pmod{q}$$

## *Without fault*

✧  $S = a S_p + b S_q$       where:  $a \equiv 1 \pmod{p}$ ,  $a \equiv 0 \pmod{q}$   
 $b \equiv 0 \pmod{p}$ ,  $b \equiv 1 \pmod{q}$

✧ thus,

$$\begin{aligned} S^e \pmod{p} &= S_p^e \pmod{p} \\ &= m^{de} \pmod{p} \\ &= m \pmod{p} \end{aligned}$$

✧ same  $\pmod{q}$

*With fault*

$$\star S = a S_p + b \tilde{S}_q \text{ where, } a \equiv 1 \pmod{p}, a \equiv 0 \pmod{q} \\ b \equiv 0 \pmod{p}, b \equiv 1 \pmod{q}$$

thus,

$$\star S^e \pmod{p} = S_p^e \pmod{p} \\ = m^{de} \pmod{p} \\ = m \pmod{p}$$

$$\star \text{ same } \pmod{q}$$

$$S^e \not\equiv m \pmod{q}$$



## *With fault*

✦ In other words, we have that

$$\tilde{S}^e - m = 0 \pmod{p}$$

$$\tilde{S}^e - m \neq 0 \pmod{q}$$

✦ or

$$p \mid (\tilde{S}^e - m)$$

$$q \nmid (\tilde{S}^e - m)$$

✦ as  $N \neq p q$ , we get

$$\gcd((\tilde{S}^e - m), N) = p$$

## *Section #7: FIPS 140-2 & Common Criteria (CC) Relation*

- ✦ Some considerations
- ✦ A generalized figure

## *FIPS 140-2 and Common Criteria (CC) Relation*

- ✦ If the operational environment is a modifiable operational environment, the operating system requirements of the Common Criteria are applicable at Security Levels 2 and above.
- ✦ FIPS 140-1 required evaluated operating systems that referenced the Trusted Computer System Evaluation Criteria (TCSEC) classes C2, B1 and B2.
- ✦ However, TCSEC is no longer in use and has been replaced by the Common Criteria. Consequently, FIPS 140-2 now references the Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 15408:1999.

## *FIPS 140-2 and Common Criteria (CC) Relation*

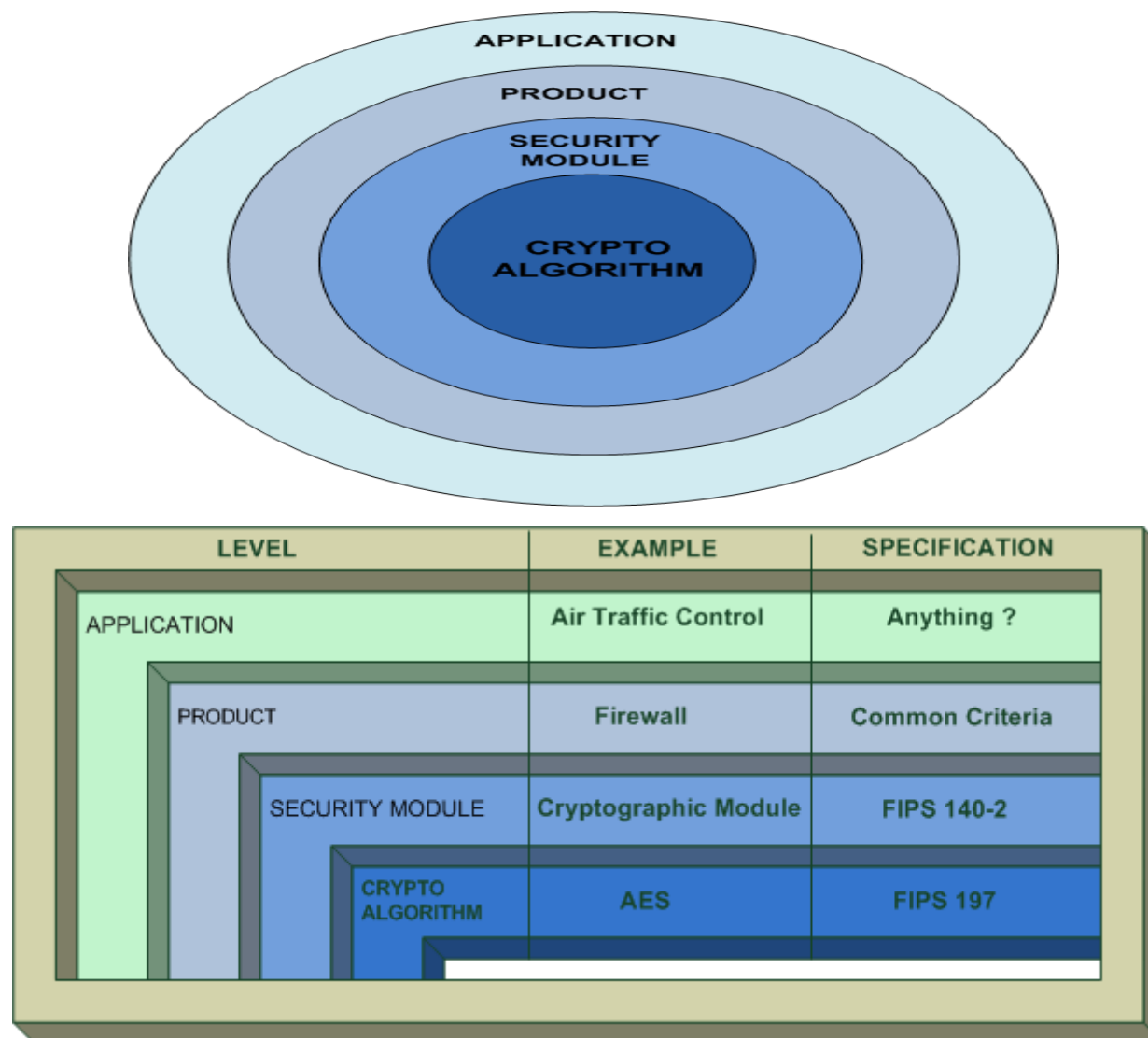
- ✦ The Common Criteria (CC) and FIPS 140-2 are different in the abstractness and focus of tests.
- ✦ FIPS 140-2 testing is against a defined cryptographic module and provides a suite of conformance tests to four security levels.
- ✦ FIPS 140-2 describes the requirements for cryptographic modules and includes such areas as physical security, key management, self tests, roles and services, etc. The standard was initially developed in 1994 - prior to the development of the CC.



## *FIPS 140-2 and Common Criteria (CC) Relation*

- ✦ CC is an evaluation against a created protection profile (PP) or security target (ST). Typically, a PP covers a broad range of products.
- ✦ A CC evaluation does not supersede or replace a validation to either FIPS 140-1 or FIPS 140-2.
- ✦ The four security levels in FIPS 140-1 and FIPS 140-2 do not map directly to specific CC EALs or to CC functional requirements.
- ✦ A CC certificate cannot be a substitute for a FIPS 140-1 or FIPS 140-2 certificate.

## *FIPS 140-2 and Common Criteria (CC) Relation*



## *Section #8: Common Criteria (CC)*

- ✦ Basic Concepts
- ✦ Protection Profile
- ✦ Security Target

## *CC: Basic Concepts*

- ✦ **Target Of Evaluation (TOE)** - the product or system that is the subject of the evaluation.
- ✦ **Protection Profile (PP)** - a document, typically created by a user or user community, which identifies security requirements for a class of security devices relevant to that user for a particular purpose.
- ✦ **Security Target (ST)** - the document that identifies the security *properties* of the target of evaluation. It may refer to one or more PPs. The TOE is evaluated against the SFRs established in its ST.
- ✦ **Security Functional Requirements (SFRs)** - specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions.



## *CC: Basic Concepts*

✱ **Security Assurance Requirements (SARs)** - descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.

✱ **Evaluation Assurance Level (EAL)** - the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic and EAL 7 being the most stringent .

## *CC: Protection Profile - PP*

- ✱ The PP contains a set of security requirements either from this International Standard, or stated explicitly, which should include an EAL (possibly augmented by additional assurance components).
- ✱ The PP permits the implementation independent expression of security requirements for a set of TOEs that will comply fully with a set of security objectives.
- ✱ A PP is intended to be reusable and to define TOE requirements that are known to be useful and effective in meeting the identified objectives, both for functions and assurance.
- ✱ A PP also contains the rationale for security objectives and security requirements.
- ✱ A PP gives consumers a means of referring to a specific set of security needs and facilitates future evaluation against those needs.

## *CC: Security Target - ST*

- ✱ ST contains a set of security requirements that may be made by reference to a PP, directly by reference to ISO/IEC 15408 functional or assurance components, or stated explicitly.
- ✱ ST permits the expression of security requirements for a specific TOE that are shown, by evaluation, to be useful and effective in meeting the identified objectives.
- ✱ ST contains the TOE summary specification, together with the security requirements and objectives, and the rationale for each.
- ✱ ST is the basis for agreement between all parties as to what security the TOE offers.

## *Section #9: How to be an Approved CST Lab?*

- ✦ What is NVLAP
- ✦ Requirements
- ✦ For the Assessors
- ✦ How to Apply





✦ NVLAP is part of the Standards Services Division within NIST's Technology Services.

✦ <http://ts.nist.gov/standards/accreditation/index.cfm>



✦ All of the third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories are accredited by the National Voluntary Laboratory Accreditation Program (NVLAP).

✦ The National Voluntary Laboratory Accreditation Program (NVLAP) provides third-party accreditation to testing and calibration laboratories. NVLAP's accreditation programs are established in response to Congressional mandates or administrative actions by the Federal Government or from requests by private-sector organizations.

✦ NVLAP is in full conformance with the standards of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), including ISO/IEC 17025 and ISO/IEC 17011.

# NVLAP<sup>®</sup> Requirements

✱ NIST Handbook 150:2006, *NVLAP Procedures and General Requirements*, which contains the general procedures and requirements under which NVLAP operates as an unbiased third-party accreditation body.

✱ NIST Handbook 150-xx program-specific handbooks, which supplement NIST Handbook 150 by providing additional requirements, guidance, and interpretive information applicable to specific NVLAP laboratory accreditation programs (LAPs).

# NVLAP<sup>®</sup> Requirements

✱ NIST Handbook 150:2006, *NVLAP Procedures and General Requirements*

✱ NIST Handbook 150-17:2008  
NVLAP Cryptographic and Security Testing

✱ And two related lab bulletins

➤ Lab Bulletin LB-30-2007:  
Addition of Security Content Automation Protocol (SCAP)  
Validation Program Test Methods to the NVLAP Cryptographic and  
Security Testing LAP

➤ Lab Bulletin LB-15-2006:  
Addition of Personal Identification Verification Test Methods to the  
NVLAP Cryptographic Module Testing LAP



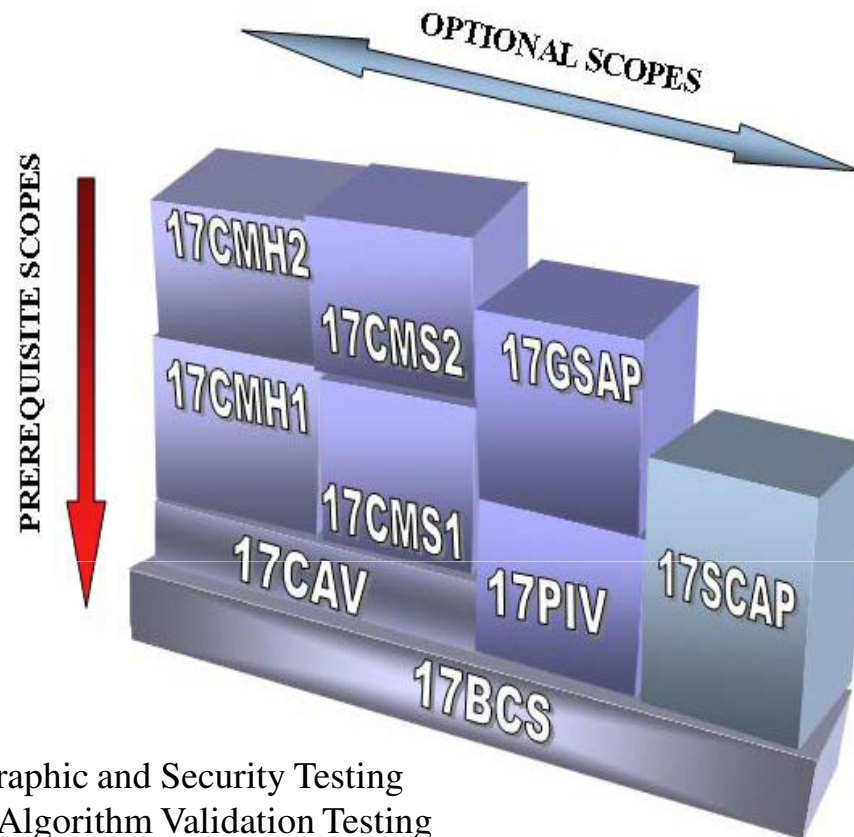
# **NVLAP<sup>®</sup>** *For the Assessors*

- ✦ NIST Handbook 150 Check List
- ✦ Program Specific Check Lists
  - CMT LAP Specific Operations Check List

# **NVLAP**<sup>®</sup> *How to Apply*

1. Fill out General Application Form
2. Fill out program Specific Application Form: Information Technology Security Testing, Test Method Selection List
  - i. Cryptographic And Security Testing
  - ii. Common Criteria Testing
3. Determine the fee by fee schedule and Pay
4. Wait for the Assessment Day!

2. i. Information technology security testing, test method selection list – cryptographic and security testing



17BCS = Basic Cryptographic and Security Testing  
17CAV = Cryptographic Algorithm Validation Testing  
17CMS1 = Cryptographic Modules – Software 1 Testing (Security Levels 1 to 3)  
17CMS2 = Cryptographic Modules – Software 2 Testing (Security Levels 4 and above)  
17CMH1 = Cryptographic Modules – Hardware 1 Testing (Security Levels 1 to 3)  
17CMH2 = Cryptographic Modules – Hardware 2 Testing (Security Levels 4 and above)  
17PIV = Personal Identity Verifier Testing  
17GSAP = GSA-Precursor Testing  
17SCAP = Security Content Automation Protocol Testing



3. Fee Calculation

S. #9

**FEE SCHEDULE (Effective October 1, 2008)**  
**NVLAP FEE SCHEDULE (REV. 2008-09-24)**

**PROGRAM/Field:**

**INFORMATION AND TECHNOLOGY SECURITY TESTING**

Common Criteria Testing

Cryptographic Security Testing

**ADMINISTRATIVE/ TECHNICAL SUPPORT FEE: \$ 4,930 (annually)**

**INITIAL APPLICATION FEE: \$750 (once only)**

**ON-SITE ASSESSMENT FEE: Variable**

**PROFICIENCY TESTING FEE : Not applicable**

**Payable to NIST-NVLAP**

*Dr. A. Koltuksuz*



## *Section #10: Recommendations*

- ✦ Know FIPS 140-2 by heart!
- ✦ Make sure that your design complies with FIPS 140-2
- ✦ Know testing standards by heart
- ✦ Evaluate your product by testing standards before submitting to any CMT lab.



Thank you very much for your  
time & attention...