

Certifying DPA Resistance



Cryptography Research, Inc.
www.cryptography.com

575 Market St., 11th Floor, San Francisco, CA 94105

© 1998-2009 Cryptography Research, Inc. Protected under issued and/or pending US and/or international patents. All trademarks are the property of their respective owners. The information contained in this presentation is provided for illustrative purposes only, and is provided without any guarantee or warranty whatsoever, and does not necessarily represent official opinions of CRI or its partners. Unauthorized copying, use or redistribution is prohibited.





Certifying DPA Resistance

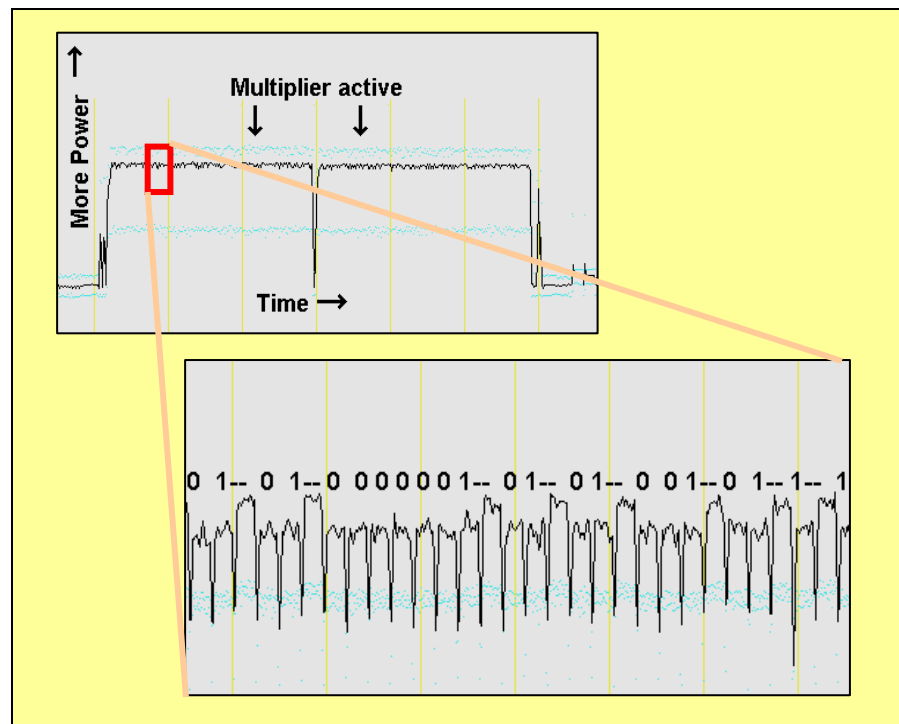
- DPA and Certification
- Example Certifications & Requirements
- Testing Approaches
- Introduction to CRI DPA Countermeasure Validation Program

DPA and Certification



Power Analysis Attacks - SPA

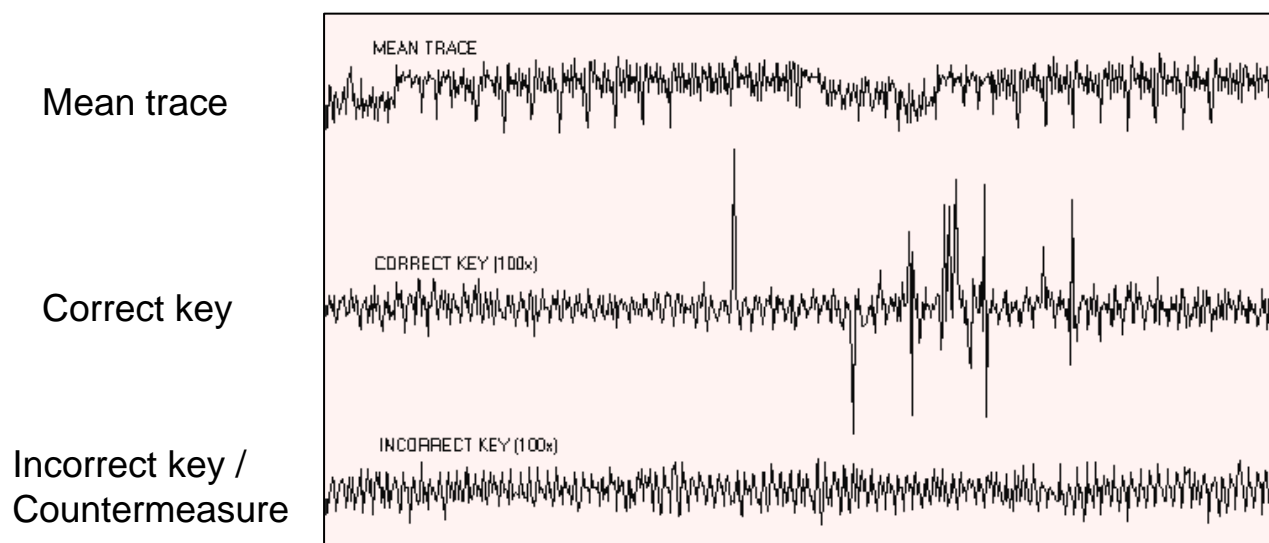
- Simple Power Analysis (SPA)
 - IC power consumption depends on activity of transistors
 - Measurements of device operation can directly reveal keys and other secrets





Power Analysis Attacks - DPA

- Differential Power Analysis (DPA)
 - Observe a series of cryptographic transactions
 - Apply statistical tests that identify statistical correlations in computational intermediates
 - Apply these tests to recover portions of the key
 - Repeat tests to recover entire key





Why are power analysis attacks important?

- Opportunity
 - Basic equipment is readily available
 - Attack is well known (not new anymore!)
- Execution
 - Non invasive + leaves no trace
 - Attackers have physical access to devices
- Defense
 - Products can be vulnerable at many levels (H/W, S/W, interface)
 - High skill needed to deploy effective countermeasures
- Exploitation
 - Consequences of a successful attack can be devastating
 - Opportunity to commit fraud, piracy, data compromise etc.



Are today's products secure?

- Industry has been aware of SPA and DPA for many years
 - Cryptography Research team discovers SPA and DPA in mid 90's, quietly informs smart card vendors

- Many leading vendors now implement SPA/DPA countermeasures
 - Cryptography Research countermeasures used in many devices
 - But many products remain vulnerable to attack

- Next challenge: Evaluating products
 - Leading evaluation facilities can devote up to 70% of lab time on side channel attacks
 - Quality of products varies widely



DPA Certification Challenges

- Many certification processes based on traditional design assumptions
 - Designers + evaluators focus on attacks they know best
 - But many serious weaknesses come from other problems!
- Standards beginning to address issues like DPA
 - Current processes valuable, but not complete
- A continuing CRI effort
 - With customers, standards efforts, testing labs, industry associations, research groups
 - Challenges: High-assurance, consistency, robustness, ...



Leakage Analysis

- Leakage is not binary!
 - Leakage cannot be entirely masked
 - ...but it can be characterized
 -and tolerated if factored into design
- Testing should use a leakage analysis approach
 - Identify sources of leakage
 - Evaluate effectiveness of countermeasures
- Leakage analysis can even deliver provable security
 - Tolerable leakage rates can be quantified
 - Actual leakage rates demonstrated within threshold with sufficient safety margin



Equipping Testing Labs

- DPA evaluation involves expertise in areas where labs were traditionally weak
 - Cryptography (public key & symmetric)
 - Signal processing, statistics
 - Scientific instrumentation
 - Smart card technology & protocols
- DPA testing knowledge is growing
 - Via conferences (CHES), industry associations, published security profiles (CC), standards updates (FIPS), ...

Challenge: Testing consistency and quality

DPA Certifications / Requirements

Example Approaches



Certification Schemes Strategies

- **Validation Approach** – e.g. FIPS 140-2
 - Demonstrate conformance to specification
 - Structured test/check methodology
 - Critical dependence on quality and relevance of specification and procedure definition

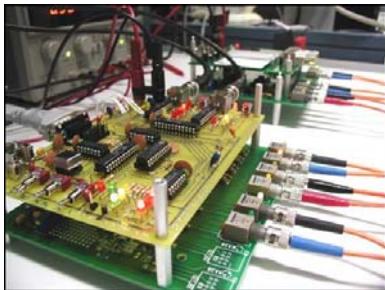
- **Evaluation Approach** – e.g. Common Criteria
 - Defined
 - Security environment
 - Threat model
 - Flexible methodology
 - Intrinsic risk assessment



Validation vs. Evaluation

Each approach has particular strengths and weaknesses

Validation

- + Defined tasks
 - + Lab consistency
 - + Cost effective
- 
- New vulnerabilities not addressed
 - Lack of penetration testing
 - Only as good as spec and test plan coverage

Evaluation

- + Threat based analysis
 - + Best use of lab expertise
 - + Flexibility
 - + Risk assessment
- Limited by lab expertise
 - Potential inconstancy of evaluations
 - Higher cost

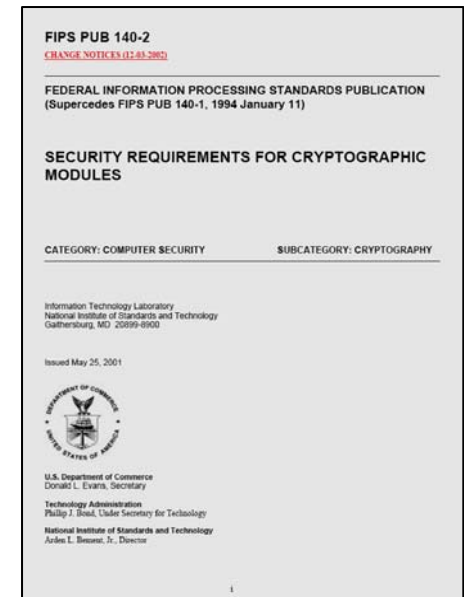
Example: FIPS 140-2



4.11 Mitigation of Other Attacks

Cryptographic modules may be susceptible to other attacks for which testable security requirements were not available at the time this version of the standard was issued (e.g., power analysis, timing analysis, and/or fault induction) or the attacks were outside of the scope of the standard (e.g., TEMPEST). Susceptibility of a cryptographic module to such attacks depends on module type, implementation, and implementation environment. Such attacks may be of particular concern for cryptographic modules implemented in hostile environments (e.g., where the attackers may be the authorized operators of the module). Such types of attacks generally rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and CSPs within the cryptographic module. Brief summaries of currently known attacks are provided below.

Power Analysis: Attacks based on the analysis of power consumption can be divided into two general categories, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). SPA involves a direct (primarily visual) analysis of electrical power consumption patterns and timings derived from the execution of individual instructions carried out by a cryptographic module during a cryptographic process. The patterns are obtained through monitoring the variations in electrical power consumption of a cryptographic module for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently values of cryptographic keys. DPA has the same goals but utilizes advanced statistical methods and/or other techniques to analyze the variations of the electrical power consumption of a cryptographic module. Cryptographic modules that utilize external power (direct current) sources appear to be at greatest risk. Methods that may reduce the overall risk of Power Analysis attacks include the use of capacitors to level the power consumption, the use of internal power sources, and the manipulation of the individual operations of the algorithms or processes to level the rate of power consumption during cryptographic processing.



FIPS PUB 140-2 (Section 4.11)
NIST, May 25, 2001

FIPS 140-2: "Mitigation of Other Attacks"

DPA resistance investigated only if vendor specifies DPA in module security policy. Testing process unspecified.

Example: US Passport (Contactless Chip)



- Specific Capabilities:

- (72) Protection against Power line emanations: Minimum information leakage measure; functional information being leaked out of the power lines should be at least 50% masked with random power fluctuations.
- (73) Ability to sense input power voltages outside (both over and under) of its normal operating range. Upon detection of an out of range condition, the IC shall reset to include overwriting of the random access memory (RAM).

ABSTRACT OF CONCEPT OF OPERATIONS
FOR THE INTEGRATION
OF CONTACTLESS CHIP IN THE U.S.
PASSPORT



Abstract of
Document Version
2.0
26 April, 2004

Abstract of Concept of Operations for the Integration
of Contactless Chip in the US Passport
April 26, 2004

Requires specific DPA CM (what about other types of DPA CM?)

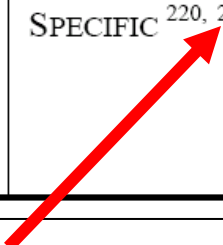
Concern: Vague requirements for DPA resistance yield inconsistent (insecure) results.

Example: Global Platform (Payment)

5.12.1 Tamper Resistance Security Feature

The *Tamper Resistance Security Feature* provides general protection against physical attack.

Operation(s)	Input Object(s)	Output Object(s)
Any unauthorized operation that attempts to read and/or modify data either via direct physical contact and/or without making physical contact with the IC ²¹⁹	PLATFORM IMPLEMENTATION SPECIFIC ^{220, 221}	PLATFORM IMPLEMENTATION SPECIFIC



²²¹ Other mechanisms, which are becoming established as being defenses against DPA attacks, should be included here. Note that these defenses might be a mixture of hardware and software. Also included would be the technique of making sure that whichever branch is taken inside a program that performs operations on cryptographic keys (such as modular exponentiation/multiplication) each alternative branch does equivalent work.

Requires specific DPA CM (what about other types of DPA CM?)

Example: Smartcard IC Platform Protection Profile



Standard Threats (referring to SC1 and SC2)

100 The TOE shall avert the threat “Inherent Information Leakage (T.Leak-Inherent)” as specified below.

T.Leak-Inherent Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Smartcard in order to disclose confidential data (User Data or TSF data).

No direct contact with the Smartcard internals is required here.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is the Differential Power Analysis (DPA). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements (Numbers 6 and 7 in Figure 8) or measurement of emanations (Number 5 in Figure 8) and can then be related to the specific operation being performed.



Smartcard IC Platform Protection Profile
Version 1.0, July 2001

Threat defined, testing methodology at lab discretion

Example: Common Criteria CEM



15.2.4 Evaluation of sub-activity (AVA_VAN.4)

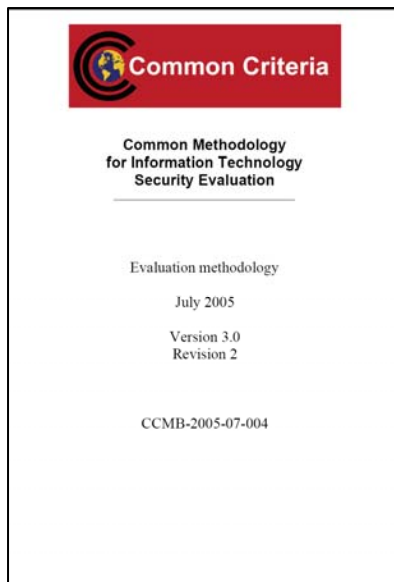
15.2.4.1 Objectives

1814 The objective of this sub-activity is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attackers possessing moderate attack potential.

15.2.5 Evaluation of sub-activity (AVA_VAN.5)

1864 There is no general guidance; the scheme should be consulted for guidance on this sub-activity.

Threat currently defined up to moderate attack potential in Common Criteria V 3.0

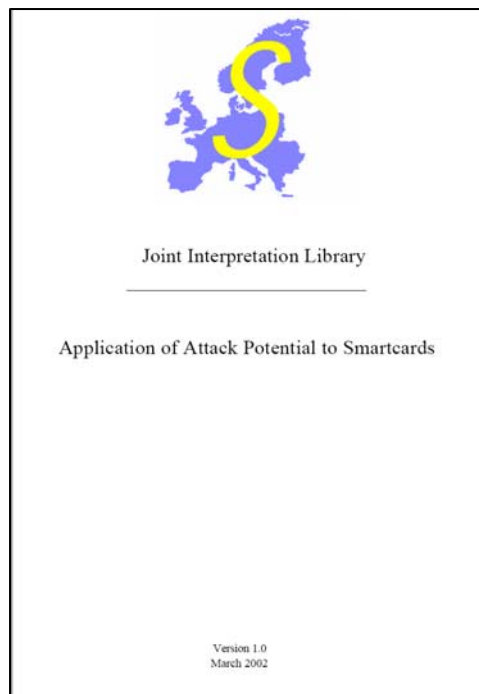


Common Methodology for Information
Technology Security Evaluation
Evaluation methodology
July 2005 Version 3.0 Revision 2

Example: Joint Interpretation Library (JIL)



Interpretation of CEM part 2, annex B.8. specifically for Smartcard evaluation. Based on Smartcard CC evaluation experience and input from smartcard industry through International Security Certification Initiative (ISCI).



Joint Interpretation Library
Version 2.1 2006

Recognition outside Europe is limited.
Updated version 2.1 released April 2006

Additional documents address the particular challenges associated with smart card evaluations including guidelines in application of attack potential in Common Criteria Evaluations

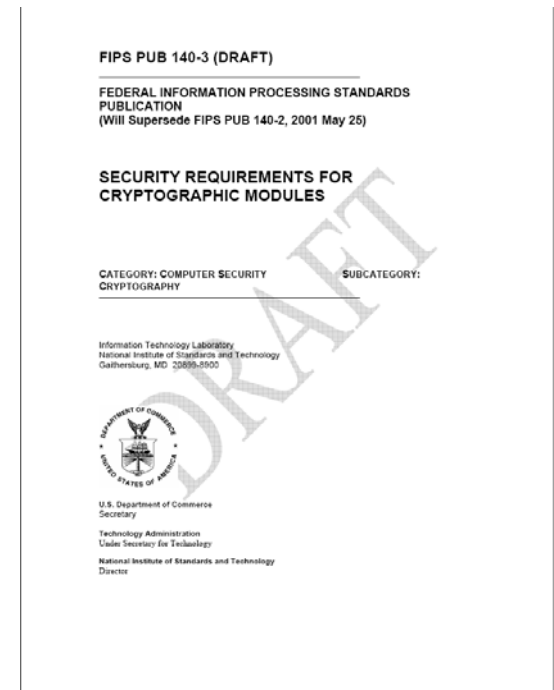
Comprehensive guidance and metrics to evaluate attack potential for Smartcards

Covers all "currently known" attack methods – including SPA/DPA



FIPS 140-3

- FIPS 140-3 currently under development by NIST
- 1st draft published July 2007
- Introduces requirements to protect against non invasive attacks such as SPA, DPA and Timing Analysis into the core of the specification

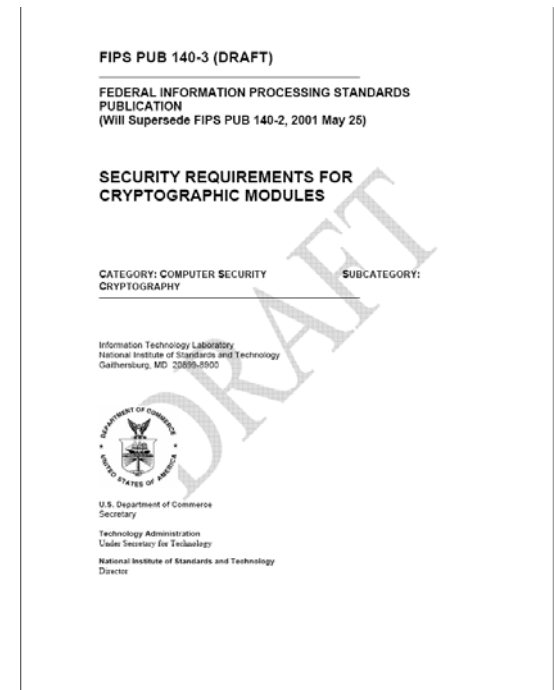


FIPS PUB 140-3 draft



FIPS 140-3 – changes vs FIPS 140-2

- Major new sections
 - 4.4 Software security
 - 4.7 Physical security – non invasive attacks
- Security Levels
 - New Level 5 added
 - Levels 1-4 comparable to those in FIPS 140-2
- Major modifications
 - 4.8 sensitive security parameter SSP replaces references to 'Keys'
 - 4.8 EMI/EMC removed as separate section
 - 4.10 Life cycle assurance replaces design assurance + expands scope



FIPS PUB 140-3 draft



FIPS 140-3 – non invasive attacks

- 4.7 Physical security – non invasive attacks
 - Simple Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Emanation (EME) and Timing Analysis (TA)
- Proposed Security Levels
 - Level 3 – cryptographic module shall protect the module's CSPs against TA attacks. Documentation shall specify the mitigation techniques against applicable TA attacks
 - Level 4 - cryptographic module shall protect the CSPs against SPA & DPA attacks. Documentation shall specify the mitigation techniques against applicable SPA & DPA attacks
 - Level 5 - cryptographic module shall protect the module's CSPs against EME. Documentation shall specify the mitigation techniques against applicable EME attacks



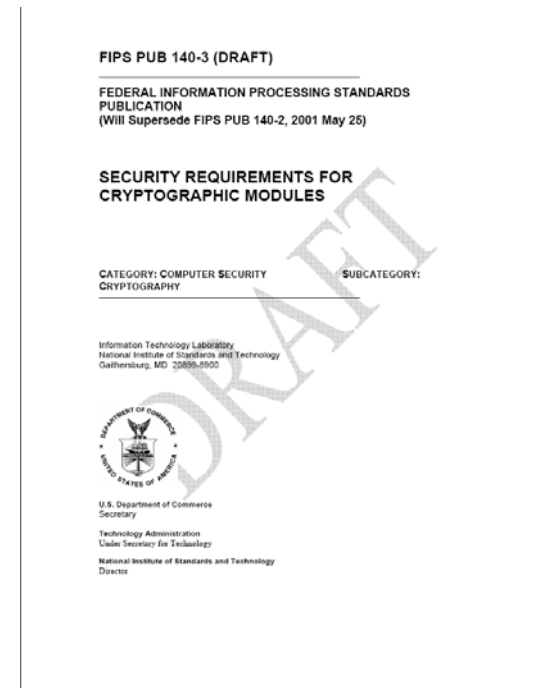
FIPS 140-3 – CRI comments

- CRI comments and feedback to NIST on FIPS 140-3
 - Modify the level at which cryptographic module should protect against SPA and DPA attacks as follows
- Level 2
 - SPA and simple DPA (< 1000 traces, simple data sorting)
- Level 3
 - 'Normal' DPA (< 50,000 traces, basic signal processing)
- Level 4
 - High order DPA (>100,000 traces, extensive signal processing, high-order analysis, chosen message attacks, and methods using advanced data acquisition and collection hardware)



FIPS 140-3 - schedule

- Time frame
 - July 2007 – 1st draft published
 - Nov 2008 - Development of FIPS 140-3 moved to the NIST Computer Security Division
 - TBD – 2nd draft released for public comment
 - TBD - FIPS 140-3 presented to the Secretary of the Department of Commerce for signature
 - + 6 mths – FIPS 140-3 becomes affective, Derived Test Requirements published
 - + 6 mths – FIPS 140-2 retired



FIPS PUB 140-3 draft

Testing Approaches



Black Box DPA Testing

- Black box evaluations are a common approach
 - Use power traces to (a) infer information about the design and (b) extract keys.
 - Approach: Form hypotheses then use traces to test them

- Many challenges:
 - Tester must have a deep understanding of the range of possible implementation techniques & countermeasures
 - Effectiveness depends on lab expertise & capabilities
 - Can miss problems
 - Black box testing does not provide positive, verifiable evidence of security

- Black box testing has limitations, but often finds flaws and is useful for differentiating products with a moderate level of protection from those that are highly vulnerable



Clear Box DPA Testing

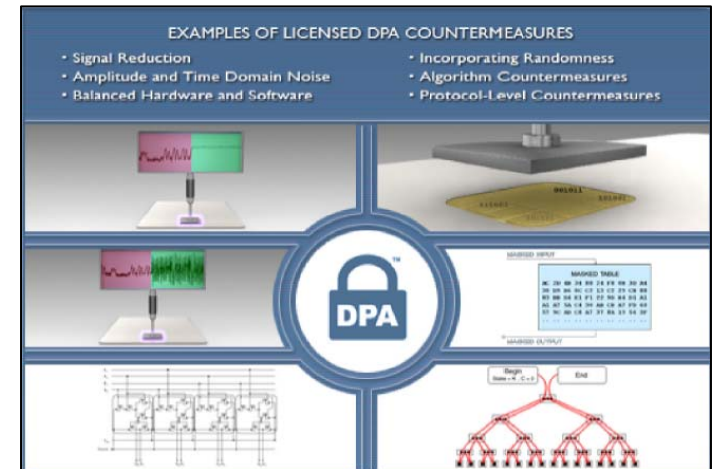
- Evaluator has comprehensive design information
 - Necessary to obtain higher levels of confidence
 - Makes more efficient use of testing resources
 - Avoids wasteful trial & error guesswork to infer design
 - Security requirements allow lab to focus on meaningful testing
 - Places greater burden on designer (must document claims)
 - Lab does not need to look for every possible design strategy or countermeasure, only validate those deployed

- Products that perform well in a comprehensive clear box evaluation much less likely to reveal unpleasant surprises in the field

Countermeasure-Based Validation



- Countermeasure design & implementation
 - Well designed countermeasures will be matched to device leakage characteristics
 - Vendor provides countermeasure rationale to explain implementations choices
- Typical laboratory evaluation process
 - Validate countermeasure rationale & implementation
 - Validate effectiveness of countermeasures
 - Testing of device with countermeasures enabled and disabled
 - Leakage characterization based analysis





High Assurance Validation Strategy

- If protocols can tolerate some leakage, the validation needs to demonstrate that actual leakage rate is within tolerance range
 - Verify that the protocols have the claimed properties
 - Conventional crypto evaluation
 - Verify that the hardware leaks less than the survivable leakage, with a suitable safety margin
 - Hardware analysis

- If protocols require zero leakage, high assurance validation likely to be impossible
 - Leakage cannot be entirely eliminated by masking countermeasures

Introduction to DPA Countermeasure Validation Program



DPA Countermeasure Validation Program



- Cryptography Research 'DPA Countermeasure Validation Program'
 - Evaluation of smart cards against power analysis attacks
 - Combines best elements of 'validation' and 'evaluation' methodologies
 - 'Clear box' testing by accredited, independent laboratories
 - Defines testing framework for consistent evaluations
 - Defines 2 levels of assurance
 - DPA Approved
 - DPA Approved – High Assurance
 - Compatible with and complementary to existing industry certification schemes



Evaluation Guidelines

- Countermeasure Testing

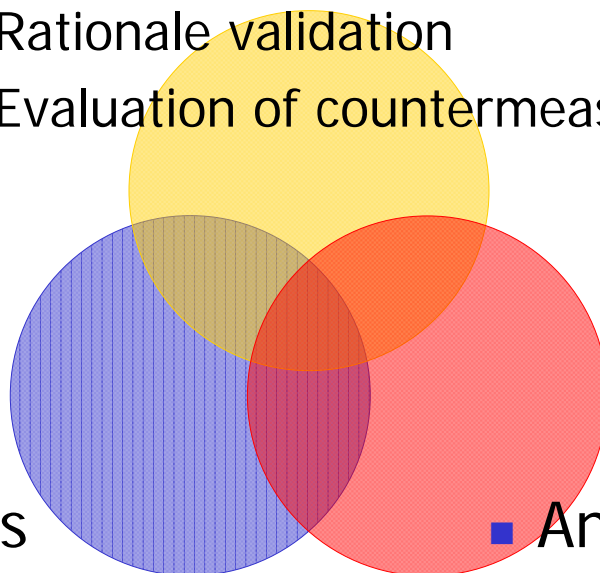
- Rationale validation
- Evaluation of countermeasure effectiveness

- Leakage Sources

- Core function
- Cryptographic processing
- Application-specific

- Analysis Techniques

- Data collection methods
- SPA/DPA methodology





Process Overview

- Study vendor documentation and usage model
- Initial testing to confirm understanding of function
- Evaluation of countermeasure rationale & effectiveness
 - Rationale validation
 - Countermeasure testing
- Leakage testing of selected functions
 - Potential leakage in core function and cryptographic processing
 - Use of appropriate analysis techniques
- Report preparation
 - Feedback to vendor
 - Evaluation Conclusion Report to CRI



Summary & Conclusion

- DPA certifications and requirements
 - Variety of approaches currently used
 - Scope for improvement in many instances
- Testing approaches
 - Most effective approaches focus on leakage analysis
- CRI DPA Countermeasure Validation Program
 - Specific testing methodology for DPA assurance
 - Combining many of the best practices from existing programs
 - Compatible and complementary to current industry schemes

For More Information

Papers and Technical Information

www.cryptography.com/dpa

*Testing, Certification and DPA
Workstation*

Ken Warren

ken@cryptography.com

Tel: +44 1494 766271

Licensing

Kit Rodgers

kit@cryptography.com

Tel: +1 415 957 2601

