

11th IAC 2010
September 21-23, Antalya/TURKEY

Guidance for Side Channel Analysis of Elliptic Curve Cryptography Implementation.

Wolfgang Killmann, Wolfgang Thumser, Guntram Wicke – T-Systems
Manfred Lochter - Bundesamt für Sicherheit in der Informationstechnik

The Guidance Document

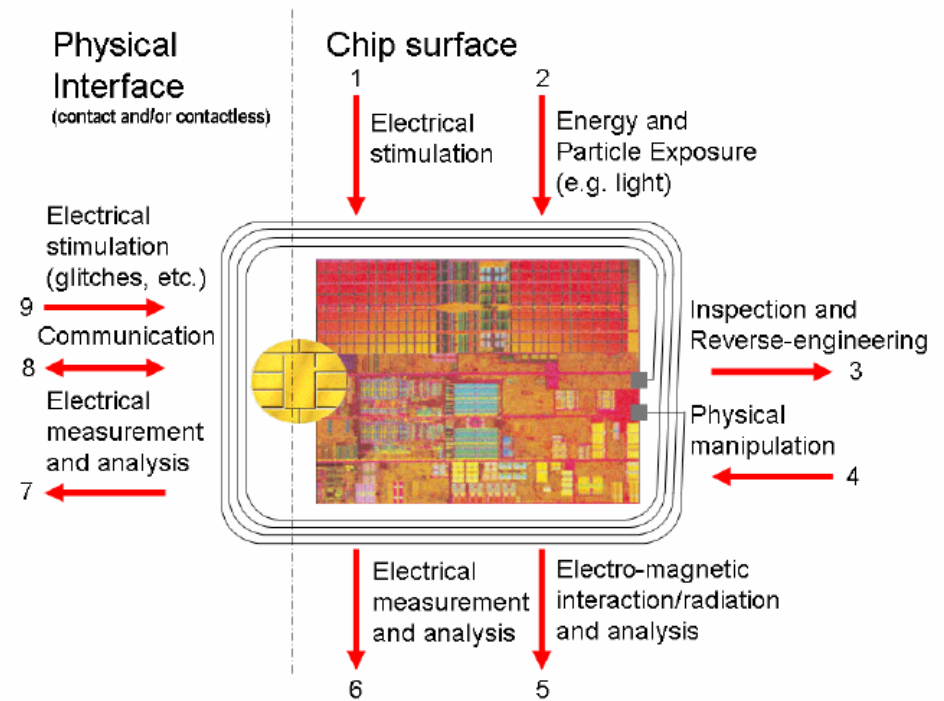
- Title of the document:
Minimal Requirements for Evaluating Side-Channel-Attack Resistance of Elliptic Curve Implementations
- Authors:
 - Wolfgang Killmann, Wolfgang Thumser, Guntram Wicke, T-Systems GEI GmbH
 - Tanja Lange, Technische Universiteit Eindhoven
- Project leader of BSI and co-author of this presentation
 - Manfred Lochter
- Goal of the document
 - Guideline for security evaluators to analyse and test smartcard implementations of elliptic-curve cryptography over $GF(p)$ for resistance against side-channel attacks with high (and other) attack potential according to Common Criteria (CC), version 3.1.



Side Channel Analysis (SCA)

Definition

- **Side channel** = unintended information flow about internal data, states or processes through physical observable signals.
- Relevant for all TOE depending on the available information in the signals
 - includes but is not limited to data exchanged through the logical interfaces
 - SCA aims on reduction of entropy of secrets like private keys or clear text
 - SCA may enable or support other attacks like perturbation



Threat model for smart cards (s. PP-BSI-0035)

5 to 8 are directly linked to SCA



Side Channel Analysis (SCA)

CC context

- Side-channel analysis (in context of CC evaluation)
Method of vulnerability analysis in order to assess the resistance of the TOE against attacks exploiting side-channels.
- Side-channel analysis may be classified by
 - Physical observables and their combination
 - output, power consumption, electromagnetic emanation
 - timing of the signals
 - Method of analysis
 - analysis of TOE hardware/software
 - method of signal analysis: single event, statistical analysis, pattern analysis, ...
 - Operation of the TOE
 - normal, enforced unexpected behaviour, perturbation



Side Channel Analysis (SCA)

Layering

	Functional level	Example	Source
Complexity	Communication protocol	ISO7816 commands	command response, timing
	Cryptographic protocol	PACE (with ECC)	protocol input/output
	Cryptographic algorithm	$s := \frac{([k]Q)_x \cdot d_A + H(M)}{k} \bmod p$	cryptographic calculation
	ECC arithmetic GF(p)	$(P+Q)_x := \frac{y_Q - y_P}{x_Q - x_P} - x_P - x_Q \bmod p$ $([2]P)_x := (3x_P + a)^2 - 2x_P \bmod p$	routines using coprocessor, CPU, bus
	Modulo arithmetic	$z := x + y \bmod p, c := m^d \bmod n$	arithmetic coprocessor data bus
	CPU command	ADD, MUL, Jump	CPU, data bus
	Data transfer	read / write of secrets	data bus



Side Channel Analysis (SCA)

ECC arithmetic

- Elliptic curves over $GF(p)$
 - Brainpool, NIST FIPS PUB 186-2, IEEE_P1363, ANSI-X962
 - domain parameter are normally public, but may be private
 - user defined elliptic curves are not examined by evaluator but correctness checks implemented by the TOE
- ECC arithmetic is based on arithmetic in the underlying finite field
 - Huge set of algorithms for optimization of the calculations
 - scalar multiplication
 - Countermeasures address specific SCA attacks
 - all kinds of randomization (base points, coordinates, programm)
 - blinding, „dummy“ operations, „double and always add“, ...



Side Channel Analysis (SCA)

ECC algorithms and protocols

- Algorithms
 - key generation
 - ECDSA
 - ECDH, ECMQV
- Protocols
 - Password Authenticated Communication Establishment (PACE)
- SCA
 - key generation is rather simple algorithm if compared with RSA
 - uniform distribution of nonce k used in ECDSA is important
 - specific SCA for algorithms and protocols are known
 - randomization in the protocol helps SCA protection



SCA in CC Evaluation Process

Application of the Guideline

- Developer
 - guideline is helpful for TOE design and security architecture
- Lab
 - plan and development of SCA methods of the lab
 - evaluators are guided for SCA as part of the vulnerability analysis
- Certifier
 - minimum requirements for SCA as part of the vulnerability analysis of smartcards and similar devices
- Accreditation body
 - minimum requirements for labs evaluating smartcards and similar devices
- Guidance gives the base line of minimal requirements and is not comprehensive. Regular updates will keep it up to date.



SCA CC Eval.

SCA vs. EAL

- Guidance lists relevant literature for vulnerability analysis against different attack potential.
- Penetration testing includes but is not limited to the attacks described in this document.

Assurance components met	Applicability of the literature reference for attacks on a given TOE	Literature references	Remarks
AVA_VAN.1-3 AVA_VAN.2-3 AVA_VAN.3-3 AVA_VAN.4-3 AVA_VAN.5-3	Generic aspects and / or preconditions predominant	[ANSI-X962], [ANSI-X963], Fehler: Referenz nicht gefunden, [BHLM01], [CC], [CCDB-2007-09-001], [CCDB-2009-03-001], [CCDB-2009-03-003], [CCMB-2009-07-004], [CoFr05], [Coc09], [CoFr05], [Ebei07], [FIPS_PUB_186-2], [HMV03], [ISO_10118-3], [ISO_11770-3], [ISO_15946-1], [ISO_15946-2], [ISO_15946-3], [ISO_15946-4], [ISO_7816-6], [ISO_7816-8], [Knap92], [Lemk07], [MaOP07], [IEEE_P1363], [Rinn03], [Sch08], [SEC_1], [Sil86], [Sil01] , [Wash08]	Recommended basic and advanced textbooks and dissertations on the foundations for ECC, Side Channel attacks on hardware and software etc., Standards, RFCs, always relevant
	Specific aspects and / or preconditions predominant	[AIS20], [AIS31], [CMCJ04], [ECCBP05], [FIPS_PUB_180-2] [LM09], [PH78], [RFC5639] [SEC_2], [Sch99]	Standards, RFCs, AIS to the CC scheme
AVA_VAN.3-3 AVA_VAN.4-3 AVA_VAN.5-3	Generic aspects and /or preconditions predominant	[BJ02], [BMM00], [BSS05], [CJ05], [Coro99], [Ebei07], [Gou03], [IIT02], [JT01], [MO08], [Sch02], [SLP05], [TR-02102], [TR-03111]	Usually relevant for the typical TOE, typical attack paths that have to be considered or excluded, BSI TR
	Specific aspects and / or preconditions predominant	[AT05], [BDJ04], [Ber06], [BHar09], [BOS06], [FoVa03], [FLRV08], [Hasa00], [HeMe08], [IT03], [JoYe03], [KIIK08], [Mon87], [NaSS04], [NS03], [OA01], [Sma03] [Wal04], [YKMH06]	Relevant for TOEs, if specific implementations are present and / or specific preconditions on leakage behaviour are fulfilled



Table 1: Examples for relevant and applicable literature references

SCA in CC Evaluation Process

Composite Evaluation

-
- Reuse of results from base evaluation
- Type 1: The composite evaluation may **reuse directly evaluation results** described in the base ST of related to security function provided by the base TOE independent on the new components.
 - DES - / AES Coprocessor
 - Type 2: The composite evaluation shall examine whether the **application uses the base components as required in the guidance** documentation and therefore the evaluation results of the base evaluation are valid for the composite evaluation.
 - Cryptolibrary
 - Type 3: The base evaluation may **cover only typical or most common potential vulnerabilities** of specific type but the composite evaluation shall also provide **additional analysis and tests** to determine that these countermeasures are effective for the current composite TOE.
 - Perturbation countermeasures
 - Type 4: The base evaluation may **not address specific features or functions** of the (physical) base TOE used by the composite TOE.
 - Coprocessor does not implement complex ECC algorithm
- Effort of the Composite Evaluation



SCA in CC Evaluation Process

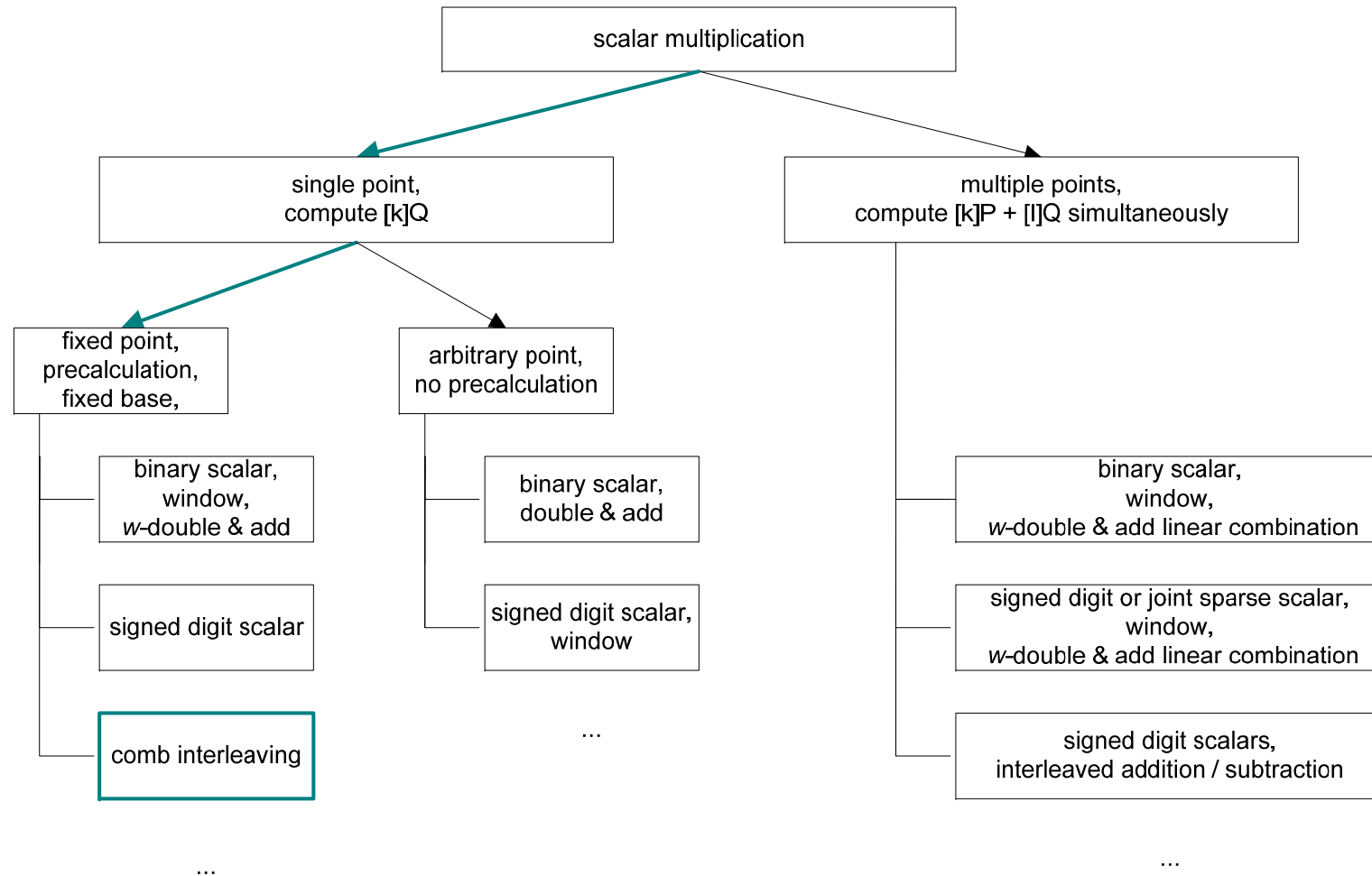
Requirements for the lab and evaluators

- **Equipment and tools**
 - CCDB-2009-03-003 Requirements to perform Integrated Circuit Evaluations (mandatory)
 - normally standard equipment for measurements
 - specialised equipment for data analysis (software)
 - non-invasive SCA maybe combined with semi-invasive and invasive attacks
- **Measurements**
 - Signal-noise ratio is important for SCA measurements
 - 1,000 to 10,000 measurements for SPA, local TA, SEMA or FA
 - 100,000 to 1,000,000 measurements for differential methods
- **Evaluator skills**
 - hardware and software analysis espacially in ECC and SCA
 - knowledge of published attacks and skills to apply / assess them for the TOE
 - training and education in ECC and SCA to extent of at least 2- 3 week per anno



Application of the Guideline (I)

Example: scalar multiplication implementation



Application of the Guideline (II)

Example: scalar multiplication evaluation

- countermeasures against side channel analysis
 - Addition of point at infinity for scalar window bits [0..0] avoided?
 - Secret-dependent conditional branches?
 - Do table point accesses leak?
 - Differentiation of points during addition?
 - Chosen point attacks (Goubin type) possible?
 - And more!
- countermeasures against fault analysis
 - Point validation, Fault attacks?
 - Invalid curve / small subgroup attacks?
 - Jump over / disable blinding?



Application of the Guideline (III)

Example: Point addition

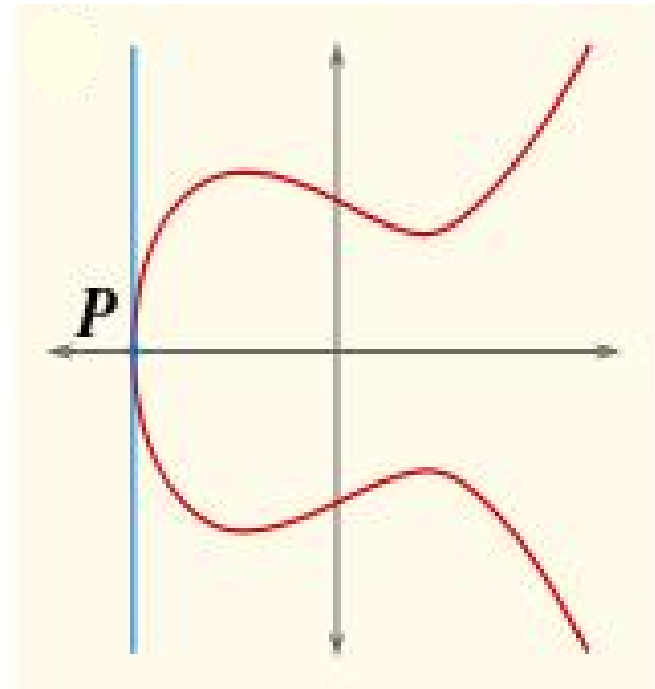
Requirements on Cofactor (NIST vs. Brainpool domain parameters):

$h = 2$ if and only if there is $P = (x, 0) \in E(F_p)$

„Proof:“ By Cauchy's theorem

$|E(F_p)| = 2 \cdot |\langle G \rangle|$ implies existence of P with $P + P = (0, 0)$ with vertical „tangent“ to meet point at infinity, hence $P(x, y) = P(x, 0)$ (qed).

Small Hamming weights are easy to detect → Situation shall be avoided!



Conclusion

- The side channel analysis is a very important, complex and quickly developing aspect of the vulnerability analysis of smartcards and similar devices.
- The guidance document defines minimum requirements for side channel analysis of ECC implementation. It can not be (and does not claim being) comprehensive but will be updated regularly.
- The guidance document support state of the art vulnerability analysis and comparability of the results.

