ALIKE: Authenticated Lightweight Key Exchange

Sandrine Agagliate, GEMALTO Security Labs

Outline:

- Context
- Description of ALIKE
  - Generic description
  - Full specification
- Security properties
  - Chip Unforgeability and Channel Secrecy
  - Underlying PK-scheme security
- Benchmark
- Conclusion

CONTEXT: Contact-less cards (1)

- Create a Secure Channel, using a key exchange protocol
  - With no authentication: PACE (with password), DH
  - Mutual authentication: Symmetric solutions like MiFare
    - Requires embedded dedicated HW circuit for both card and reader
    - Requires a common secret to be shared between the two parties
  - Card authentication: ALIKE

- Why an asymmetrical solution?
  - When readers don’t necessarily need authentication:
    - Examples: access control, public transportation
  - Allows facilitating interoperability
    - With secret key, each system derives the keys of its cards from its own master key
    - With public key, each system chooses to trust a CA
  - Allows low-cost SAM-less reader

CONTEXT: Contact-less cards (2)

- What challenge for an asymmetrical solution?
  - Very strong time limitations :
    - Our target: The global transaction should not exceed 150 ms
    - Example: Tests on public transportation in London => traffic fluidity up to 450 ms
  - Memory is limited on smart cards
  - Pre-computation pose a number of practical problems

- ALIKE = Authenticated Lightweight Key Exchange protocol [Coron, Gouget, Paillier, Villegas, 2010]
  - Provides lightweight transactions in contact-less applications
  - Increases the security level compared to classical asymmetrical authentication scheme like RSA (80-bit security)
  - Based on the public key encryption scheme "*RSA for paranoids*" [Shamir, CryptoBytes, 1995] and on a block cipher
    - RSAP allows very fast decryption (performed inside the smart-card, where a cryptographic coprocessor is commonly available)
    - Contact-less cards commonly embed a coprocessor for a block cipher such as DES or AES

On-going Standardization

- ISO/IEC 29192 (Draft in progress) : Lightweight cryptographic mechanisms targeted for constrained environments
  - Part 1: General
  - Part 2: Block ciphers
  - Part 3: Stream ciphers
  - Part 4: Mechanisms using asymmetric techniques

- Commitee Draft 29192-4 (in progress):
  - identification scheme **cryptoGPS**
  - authenticated key exchange protocol **ALIKE**
  - ID-based signature scheme **I2R-IBS**

Functional requirements for ALIKE

Objective

ALIKE is a *very fast protocol* for contactless applications such that:

- A verifier PCD (e.g. a reader) authenticates a prover PICC (e.g. a contact-less card) relative to a certification authority CA
- Additionally, PCD and PICC establish a session key used for secure messaging

- There is no authentication of the PCD by the PICC
- Main target applications:
  - Access control, contact-less transport

PCD = Proximity Coupling Device

PICC= Proximity Integrated Circuit Card

Security requirements for ALIKE

Chip unforgeability under active attacks

- It should be “impossible” for an attacker to authenticate as a PICC without knowing that PICC’s private key

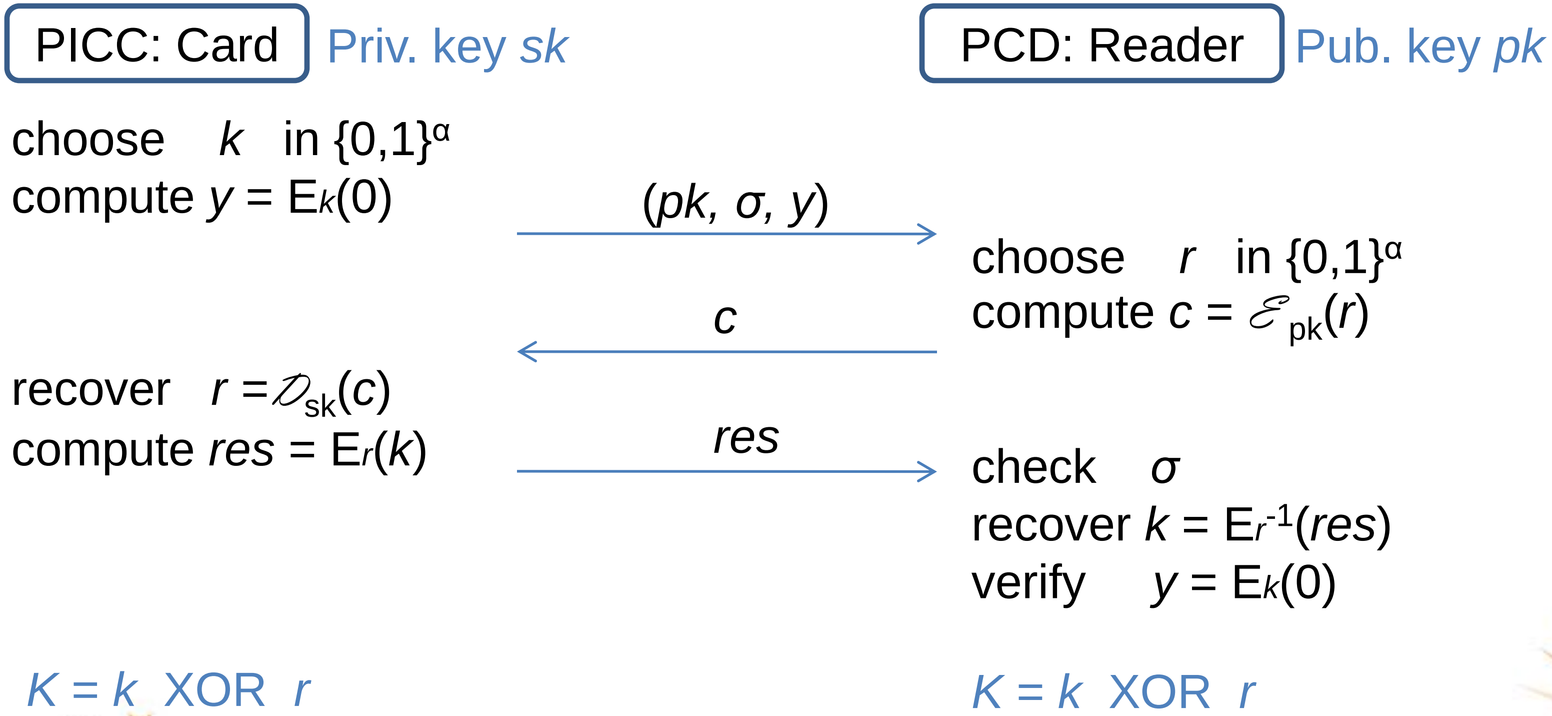
Channel secrecy under passive attacks

- It should be “impossible” for an attacker to recover the session key K of an eavesdropped transaction

- Since there is no authentication of the PCD, « channel secrecy » cannot be secure under active attacks

ALIKE protocol: generic construction

- Primitives:
  - A block-cipher: E: $\{0,1\}^{\alpha} x \{0,1\}^{\beta} \to \{0,1\}^{\beta}$, $\alpha \leq \beta$
  - A public-key encryption scheme $\mathcal{E}$
- [KeyGen] : key pair (*sk*,*pk*), certificate σ on *pk* from CA
- [Challenge-Response-Verification]:



PICC: Card Priv. key *sk*

PCD: Reader Pub. key *pk*

choose k in $\{0,1\}^{\alpha}$
compute $y = E_k(0)$

$\xrightarrow{(pk, \sigma, y)}$

choose r in $\{0,1\}^{\alpha}$
compute $c = \mathcal{E}_{pk}(r)$

$\xleftarrow{c}$

recover $r = \mathcal{D}_{sk}(c)$
compute $res = E_r(k)$

$\xrightarrow{res}$

check σ
recover $k = E_r^{-1}(res)$
verify $y = E_k(0)$

$K = k$ XOR r

$K = k$ XOR r

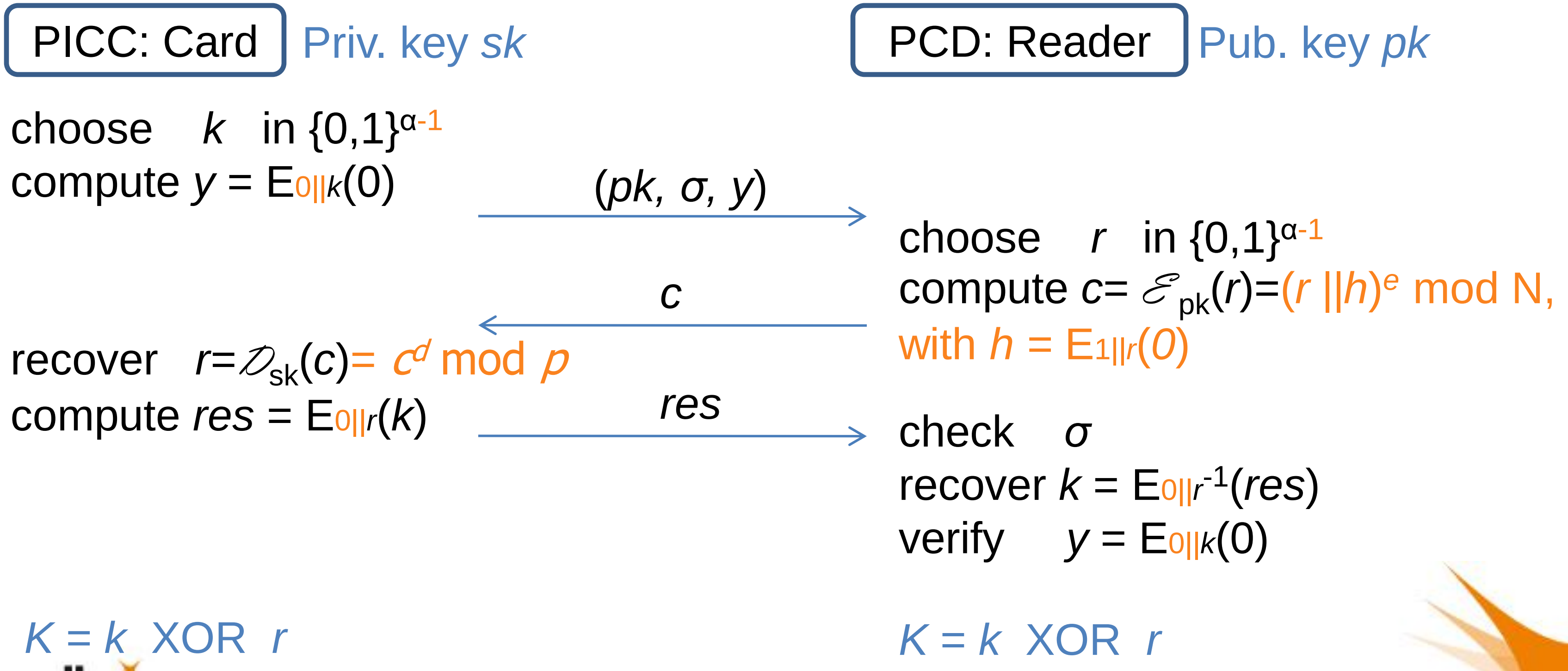
Choice for the public-key encryption scheme $\mathscr{E}$

- We revisit «RSA for paranoids»RSAP [Shamir, CryptoBytes, 1995]
  - Unbalanced modulus N = p.q
  - Decryption of ciphertexts is done only modulo the smallest prime p
  - Possibly use moduli with fixed common part, without degrading security

- [KeyGen]
  - Given the security parameter κ and a public exponent e:
    - prime p with $|p| = \kappa$ *such that* $\gcd(e,p-1)=1$
    - prime q such that $|p| \ll |q|$, and modulus N=p.q
    - private exponent $d = e^{-1} \bmod (p-1)$
- [Encryption]
  - Given m in $\{0,1\}^{\alpha}$,with $\alpha+t \leq \kappa-1$, compute $c = (m \,||\, H(m))^{e} \bmod N$ where $H: \{0,1\}^{\alpha} \rightarrow \{0,1\}^{t}$ is a hash function such that $\alpha+t \leq \kappa-1$
- [Decryption]
  - Given c, compute $x = c^{d} \bmod p$
  - Then parse x as $m||h$ where m is in $\{0,1\}^{\alpha}$ and h is in $\{0,1\}^{t}$. If the parsing fails or if $h \neq H(m)$ return error. Otherwise return m.

ALIKE protocol: full description

- Primitives:
  - A block-cipher : $E: \{0,1\}^{\alpha} x \{0,1\}^{\beta} \rightarrow \{0,1\}^{\beta}$, $\alpha \leq \beta$: AES ($\alpha=\beta=128$)
  - A public-key encryption scheme $\mathcal{E}$= variant of RSA for paranoids
    - small prime factor p + moduli with fixed common part + $E_{1||.}(0)$ as hash function
- [KeyGen] : key pair (*sk*,*pk*), certificate σ on *pk* from CA
- [Challenge-Response-Verification]:



PICC: Card Priv. key *sk*

PCD: Reader Pub. key *pk*

choose k in $\{0,1\}^{\alpha-1}$
compute $y = E_{0||k}(0)$

$(pk, \sigma, y) \rightarrow$

choose r in $\{0,1\}^{\alpha-1}$
compute $c = \mathcal{E}_{pk}(r) = (r \,||h)^{e} \bmod N$,
with $h = E_{1||r}(0)$

$\leftarrow c$

recover $r = \mathcal{D}_{sk}(c) = c^{d} \bmod p$
compute $res = E_{0||r}(k)$

$res \rightarrow$

check σ
recover $k = E_{0||r}^{-1}(res)$
verify $y = E_{0||k}(0)$

$K = k$ XOR r

$K = k$ XOR r

Security assumptions (1)

- Ideal Cipher Model (ICM)
  - Block-cipher is replaced with a publicly accessible ideal cipher, i.e. a family of random permutations parametrized by a key.
  - The attacker must query the encryption or decryption oracles attached to the IC
- ICM has been shown to be equivalent to the Random Oracle Model (ROM) [Coron,Patarin,Seurin, Crypto'2008]
  - ICM is not a stronger assumption than the ROM
- Viewing E as an ideal cipher, we proved that our construction is secure under appropriate security assumptions on $\mathcal{E}$

Security assumptions (2)

- [Bellare, Desai, Pointcheval and Rogoway, Crypto'1998]
- OW-CPA:
  - A public-key encryption scheme $\mathscr{E}$ is said to be (t,ε)-OW-CPA if no adversary running in time t, given a random public key pk and $c = \mathscr{E}_{pk}(m)$ where m is generated at random in the message space, can output m with probability better than ε
- OW-CCA:
  - Same as OW-CPA, but with access to a decryption oracle for any $c' \neq c$
- P-OW-CPA: (partially OW-CPA)
  - Same as OW-CPA, but with $c = \mathscr{E}_{pk}(m)$ where $m=m1||m2$ is generated at random in the message space, can output $m1$ with probability better than ε

Security theorems: on underlying PK-scheme assumption

Theorem 1 (Active Unforgeability)

- ALIKE is (t,ε)-secure against unforgeability under active attacks, in the ideal cipher model, assuming that that $\mathcal{E}$ is (t',ε')-OW-CCA secure.

Theorem 2 (Passive Secrecy)

- ALIKE is (t,ε)-passively secure against secrecy, in the ideal cipher model, assuming that that $\mathcal{E}$ is (t',ε')-OW-CPA secure.

Security of underlying PK-scheme

- RSAP is partially OW-CPA secure [Shamir, CryptoBytes, 1995]

- Chosen Ciphertext attack on RSAP (RSAP is not OW-CCA secure) :
  - Generate a random c in Z_N
  - Request its decryption $m = c^d \bmod p$
  - Compute $c' = m^e \bmod N$
  - Then gcd(c-c', N) disclose p with overwhelming probability

- Other Known attacks on RSAP are related to the size of the message to encrypt / decrypt
  - Known countermeasure: message size strictly < smallest prime size
  - Taken into account in ALIKE

Theorem 3 (Underlying Public Key Encryption Scheme)

- $\mathcal{E}$ = RSAP-H is (t,ε)-OW-CCA secure, assuming that RSAP is (t',ε')-P-OW-CPA secure

Real-life implementation of ALIKE (1)

- Target : at least 80-bit security

- Tuning the size of N and *p*:
  - Factoring algorithms whose running time depends on the size of N;

    The fastest such algorithm is the General Number Field Sieve (GNFS) [Lenstra, Lenstra, 1993]
  - Factoring algorithms whose running time depends on the size of p;

    The fastest such algorithm is the Elliptic Curve Method (ECM) [Lenstra, 1987]

- Tuning public exponent e:
  - Coppersmith'attack

    Attack based on Coppersmith's Theorem for finding small roots of polynomial equations. The attack applies when a small public exponent e is used.
  - Shamir's bound

    Take e such that m^e size before the modular reduction is at least twice N size

Real-life implementation of ALIKE (2)

- Tuning the number λ of non-predetermined bits in N
  - [Shamir, CryptoBytes, 1995] : RSA moduli with a fixed common part can be used without degrading the overall system security
  - allows to reduce transmissions

- Example of settings
  - λ = nb of non-predetermined bits in N;
  - t = output size of the redundancy (hash size) used in ALIKE with RSAP-H

ALIKE Security	|N|	|p|	λ	e	Block Cipher	α	β	t
80 bits	1248	352	403	11	AES-128	128	128	128
100 bits	2048	560	611	17	AES-128	128	128	128

ALIKE – benchmark (source Sec Lab's)

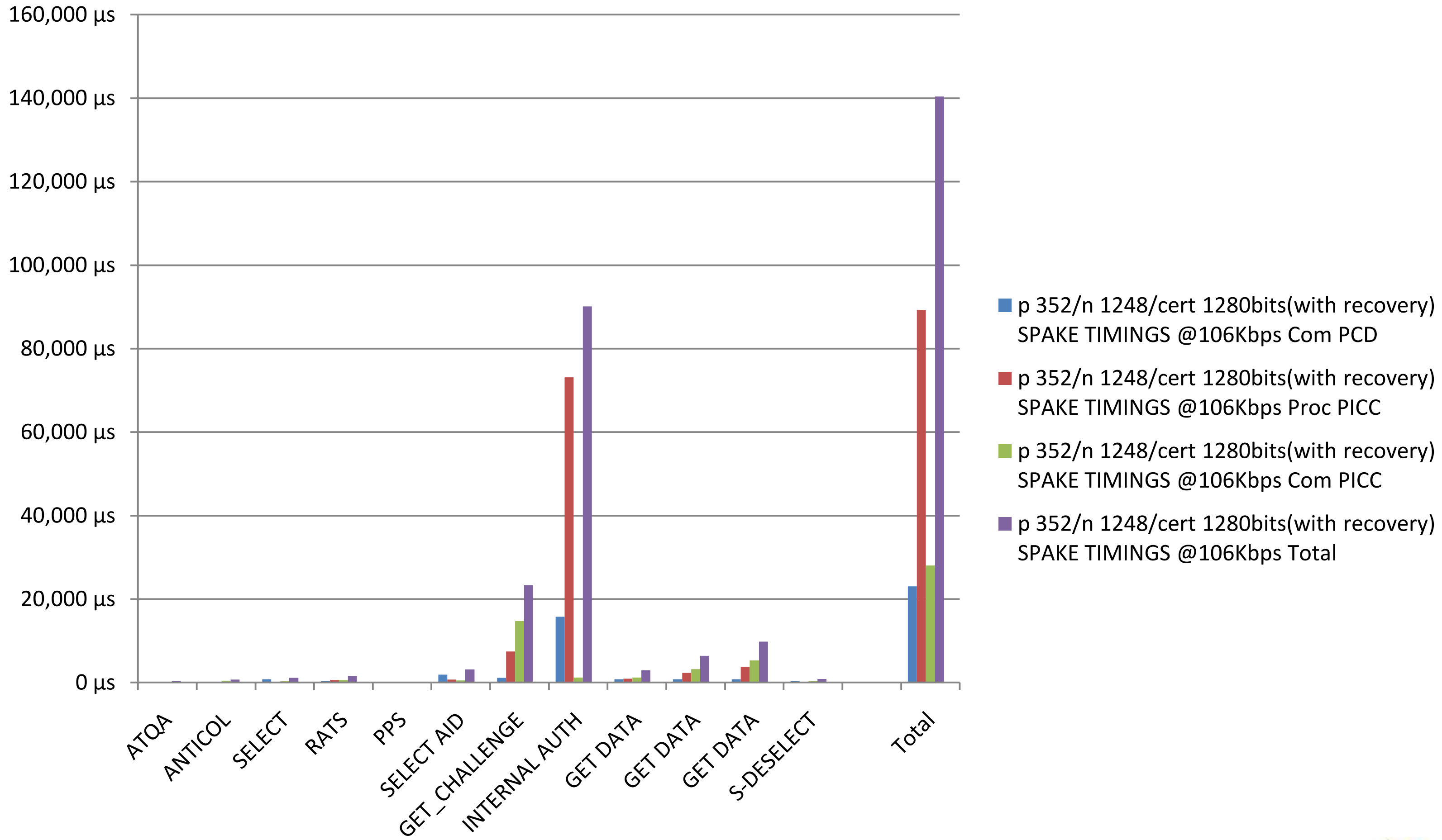
- Based on NXP's SmartMX P5CT072 platform
  - FameXE cryptoprocessor
  - DES processor

- PCD simulated on a PC via a transparent contact-less reader
  - Modular exponentiation + DES block-cipher

- Code size of our ALIKE library = 1.6 KB

- Estimation for |p| = 352, |N| = 1248 and |σ| = 1280 (80-bit security if DES is replaced by AES)
  - Total transaction time is close to 156 milliseconds
  - RAM consumption : 900 bytes
  - Non-volatile memory : 248 bytes

ALIKE (80-bit Security) - estimation



Summary

	ALIKE	
	PICC process	PCD process
Security Level [bits]	80	80
Crypto-coprocessor functionalities	Required for Modular multiplication	Not required
Functions required	- A random number generation. - Two blocks cipher executions without specific side channel and fault attacks countermeasures. - A modular exponentiation with small modulus (|p| = 352 bits)	- A random number generation. - Two blocks cipher executions - A modular exponentiation with small exponent (e≥11, |n|= 1248 bits)
Non Volatile memory	To store RSA keys for ALIKE (88 bytes to compare to 400 bytes for classical RSA) and certificates	To store public of CA
Code size	1.6 kbytes on 8051 core	
Data transferred with communication speed at 106.kb.s^{-1}	Incoming data 160 bytes⇔ 15.40 ms	Incoming data 192 bytes ⇔18.8 ms
Internal Process	- From 4 to 15 faster than classical RSA according to component - As example for 8051 core: 80 ms at 31MHz for CPU and 48 MHz for crypto-coprocessor	

Conclusion:

- ALIKE is a new key exchange protocol allowing to
  - Authenticate the smartcard relatively to a CA
  - Establish a session key (to create a secure channel between smartcard and reader)

- ALIKE specificities:
  - Allows possible interoperability
  - Requires limited hardware resources
  - Very fast: 156ms for total transaction -> RSAP is much faster than RSA
  - Secure: 80-bit security

- ALIKE is proven secure
- Proof of concept / prototype
- In right way to be standardized

References

- **ALIKE previously called SPAKE:**

  [Coron, Gouget, Paillier, Villegas, 2010] J.S.Coron1, A. Gouget, P. Paillier, K. Villegas, SPAKE: a Single-party Public-key Authenticated Key Exchange Protocol for Contact-less Applications, Financial Cryptography and Data Security (2010) 6054:107-122, January 2010

- [Bellare, Rogoway, Eurocrypt'94] M. Bellare, P. Rogaway, Optimal Asymmetric Encryption. Proceedings of EUROCRYPT 1994, pages 92-111, Springer-Verlag.
- [Bellare, Desai, Pointcheval and Rogoway, Crypto'1998] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. Proceedings of CRYPTO 1998, Springer-Verlag.
- [Coron,Patarin,Seurin, Crypto'2008] J.S. Coron, J. Patarin and Y. Seurin, The Random Oracle Model and the Ideal Cipher Model are Equivalent, Proceedings of CRYPTO 2008, Springer-Verlag.
- [Lenstra, 1987] H. W. Jr. Lenstra, Factoring Integers with Elliptic Curves, Ann. Math. 126, 649-673, 1987.
- [Lenstra, Lenstra, 1993] A. K. Lenstra and H. W. Lenstra, Jr, The development of the number field sieve. Lecture Notes in Math. (1993) 1554, Springer-Verlag.
- [Shamir, CryptoBytes, 1995] A. Shamir, RSA for paranoids, CryptoBytes 1 (1995) 1-4.