Algebraic Side Channel Cryptanalysis

Christopher Goyet

Academic Advisors : Jean-Charles Faugère and Guénaël Renault
Industrial Advisor : Olivier Orcière

PolSys - LIP6
LCH - Thales Communications and Security

November 7, 2012

THALES Communications & Security
UPMC SORBONNE UNIVERSITÉS
informatiques mathématiques

Cryptology

Cryptography is the discipline related to data protection and communications

General cryptanalysis methods

- Linear cryptanalysis
- Differential cryptanalysis
- Algebraic cryptanalysis
- ...

Algebraic cryptanalysis

Cryptographic Algorithm (AES, DSA, ...)

Modeling

$$\begin{cases} x_1x_2 + x_1k_2 + x_1 + x_2k_1 + x_3 + x_4s_4 + \\ \quad s_1s_4 + s_3s_4 + s_3 + s_4k_4 + s_4 + k_1k_2 + k_1 + k_3, \\ x_4 + s_1s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_{21} + s_{52}y_{124} + s_3y_{124} + y_{121}y_{124} + y_{121} + \\ \quad y_{123}y_{124} + y_{124}k_{122} + y_{124}k_{123} + y_{124} + k_{121} \end{cases}$$

Solving

$$\begin{cases} k_1 = 1, \\ k_2 = 0, \\ k_3 = 1, \\ \vdots \end{cases}$$

Secret (key, message, ...)

Algebraic cryptanalysis

- Security $\Rightarrow$ hardness of solving these polynomial systems

Algebraic cryptanalysis with additional information

Cryptographic
Algorithm
(AES, DSA, ...)

$\xrightarrow{\text{Modeling}}$

$$
\begin{cases}
x_1x_2 + x_1k_2 + x_1 + x_2k_1 + x_3 + x_4s_4 + \\
\quad s_1s_4 + s_3s_4 + s_3 + s_4k_4 + s_4 + k_1k_2 + k_1 + k_3, \\
x_4 + s_1s_3 + s_2 + s_4 + k_4 + 1, \\
\vdots \\
s_{21} + s_{52}y_{124} + s_3y_{124} + y_{121}y_{124} + y_{121} + \dots \\
s_1s_2 + s_1s_3 + s_1s_4 + \dots \\
s_{124}s_{125} + s_{124}s_{126} + \dots
\end{cases}
$$

additional
information
on secret data

Solving
in practice ?

Algebraic cryptanalysis with additional information

Cryptographic Algorithm (AES, DSA, ...) $\xrightarrow{\text{Modeling}}$

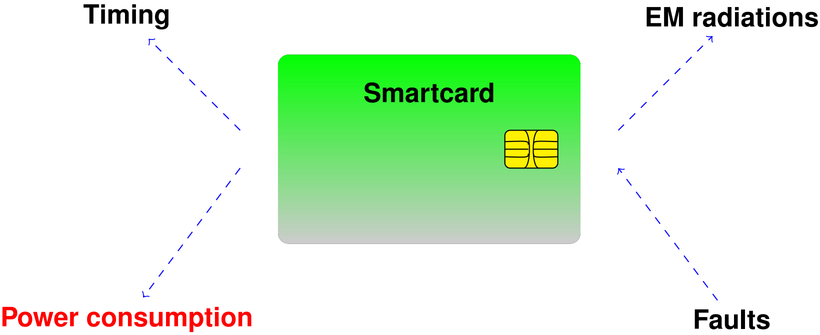
$$\begin{cases} x_1x_2 + x_1k_2 + x_1 + x_2k_1 + x_3 + x_4s_4 + \\ \quad s_1s_4 + s_3s_4 + s_3 + s_4k_4 + s_4 + k_1k_2 + k_1 + k_3, \\ x_4 + s_1s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_{21} + s_{52}y_{124} + s_3y_{124} + y_{121}y_{124} + y_{121} + \dots \\ s_1s_2 + s_1s_3 + s_1s_4 + \dots \\ s_{124}s_{125} + s_{124}s_{126} + \dots \end{cases}$$

Solving in practice ?

additional information on secret data

Side Channel Analysis

Cryptographic algorithms implementation (smartcard, FPGA, Microcontroller, ...) $\rightsquigarrow$ physical leakage of information



“A correct implementation of a strong protocol is not necessarily secure” (Kocher, 1999)

Solving methods

Symmetric-key cryptography:

AES, PRESENT

↓

Small Characteristic Field ($\mathbb{F}_2$)

↓

SAT solver & Gröbner Basis

Public-key cryptography:

(EC)DSA

↓

Large Characteristic or Integer

↓

Lattice reduction (LLL)

Solving methods

Symmetric-key cryptography:

AES, PRESENT

$\downarrow$

Small Characteristic Field ($\mathbb{F}_2$)

$\downarrow$

SAT solver & Gröbner Basis

Public-key cryptography:

(EC)DSA

$\downarrow$

Large Characteristic or Integer

$\downarrow$

Lattice reduction (LLL)

Contributions

Symmetric-key cryptography:

- leakage models
- HW, HD, ...
- criterion of success
- complexity upper-bounded
- resistant cryptosystems

Faugère, Goyet, Renault, A new Criterion for Effective Algebraic Side Channel Attacks, COSADE 2011

Carlet, Faugère, Goyet, Renault, An Analysis of Algebraic Side Channel Attacks, February 2012, Journal of Cryptographic Engineering

Public-key cryptography:

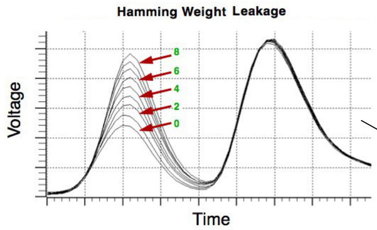
- New situation to attack (EC)DSA
- Implicit information
- unknown shared bits (locked register)

Faugère, Goyet, Renault, Attacking (EC)DSA Given Only an Implicit Hint, SAC 2012

Algebraic Side Channel Attack on block ciphers

Algebraic Side Channel Attacks (ASCA)

Attacks against block ciphers proposed by Renauld, Standaert and Veyrat-Charvillon (CHES 2009, Inscrypt2009)



$$\left\{\begin{array}{l} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \dots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \end{array}\right.$$

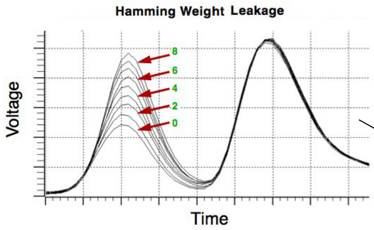
$$\left\{\begin{array}{l} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \\ \vdots \\ s_{121} s_{122} + s_{121} s_{123} + s_{121} s_{124} + \dots \end{array}\right.$$

Key $\longleftarrow$ SAT solver

Interesting aspects:

Nb observations:	1 for ASCA	/	> 1000 DPA
Solving step:	1s with HW	/	∞ without

Main goal: analysis of algebraic phase



$$\begin{cases} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \dots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \end{cases}$$

$$\begin{cases} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \\ \vdots \\ s_{121} s_{122} + s_{121} s_{123} + s_{121} s_{124} + \dots \end{cases}$$

$$\text{Key} \xleftarrow[\cancel{\text{SAT solver}}]{\text{Gröbner Basis}}$$

Our goal : analysis of algebraic phase

- Explain the efficiency (solving complexity)
- Resistant Cryptosystems

Gröbner Basis Algorithm

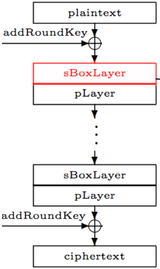
$$\left\{\begin{array}{l} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ \quad\vdots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \ldots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \ldots \end{array}\right. \xrightarrow[\text{Algorithm}]{\text{Gröbner Basis}} \left\{\begin{array}{r} g_1(k_{128}, k_{127}, \ldots, x_2, x_1) \\ \vdots \\ g_{s-i}(x_2, x_1) \\ \vdots \\ g_{s-1}(x_2, x_1) \\ g_s(x_1) \end{array}\right.$$

Complexity

- Degree of equations during computation
- Intrinsic to input problem

System modeling a block cipher

- S-boxes are the only nonlinear part of many block ciphers
- They give the resistance against algebraic attacks

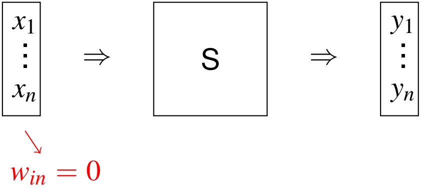


$$\left\{\begin{array}{l} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ \boxed{\begin{array}{l} s_1 s_2 + s_1 s_3 + s_1 s_4 + \dots \\ s_{121} s_{122} + s_{121} s_{123} + s_{121} s_{124} + \dots \end{array}} \\ \vdots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \dots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \end{array}\right.$$

$\Rightarrow$ S-boxes + HW leakages ?

Trivial example: $w_{in} = 0$

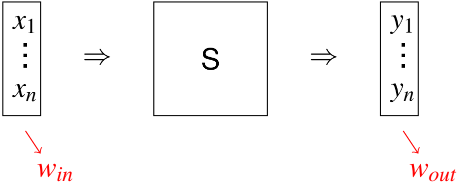
Let S an n-bit S-box.
If $w_{in} = 0$ then
$x_1 = x_2 = \cdots = x_n = 0$
and the y_i are given by



$$y_1, \ldots, y_n = S(0, \ldots, 0)$$

Influence of leakages:

- S-box completely described by $2n$ linear relations
- Degree reduced $\Rightarrow$ Algebraic resistance canceled



PRESENT S-box example, $n = 8$

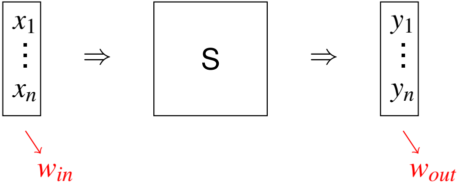
w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					16				
1					9				
2			15	15	8	13	15		
3			9	5	9	5	9		
4	16	15	14	2	11	3	12	13	16
5		13	13	2	7	10	11	13	
6		15	12	15	7	15	14		
7			13		13				
8			16						

Figure : Nb of linear relations

- Most of leakages give a lot of linear relations: $\mathbb{E}(\#AI_L) \simeq 8$
- Algebraic Immunity with Leakage: $\#AI_L(w_{in}, w_{out})$

$\Rightarrow$ system partly linearized $\Rightarrow$ solving complexity?

HW model : (w_{in}, w_{out})



PRESENT S-box example, $n = 8$

w_{in} \ w_{out}	0	1	2	3	4	5	6	7	8
0					16				
1					9				
2			15	15	8	13	15		
3			9	5	9	5	9		
4	16	15	14	2	11	3	12	13	16
5		13	13	2	7	10	11	13	
6		15	12	15	7	15	14		
7			13		13				
8			16						

Figure : Nb of linear relations

- Most of leakages give a lot of linear relations: $\mathbb{E}(\#AI_L) \simeq 8$
- Algebraic Immunity with Leakage: $\#AI_L(w_{in}, w_{out})$

$\Rightarrow$ system partly linearized $\Rightarrow$ solving complexity?

Another invariant

Definition

$\forall$ S-box $S, \forall$ leakage value $\ell = (w_{in}, w_{out})$
we define

$$N_S(w_{in}, w_{out}) = \#\{x \in \mathbb{F}_2^n \text{ s.t. } HW(x) = w_{in}, HW(S(x)) = w_{out}\}$$

Prop

Let n the bus size of S. If $N_S(w_{in}, w_{out})$ is non-zero then

$$\#AI_L(S, w_{in}, w_{out}) \geq 2n + 1 - N_S(w_{in}, w_{out})$$

$N_S(w_{in}, w_{out})$ small $\rightsquigarrow$ a lot of linear relations between input and output

Another invariant

Definition

$\forall$ S-box $S, \forall$ leakage value $\ell = (w_{in}, w_{out})$
we define

$$N_S(w_{in}, w_{out}) \quad = \quad \#\{x \in \mathbb{F}_2^n \text{ s.t. } HW(x) = w_{in}, HW(S(x)) = w_{out}\}$$

Prop

Let n the bus size of S. If $N_S(w_{in}, w_{out})$ is non-zero then

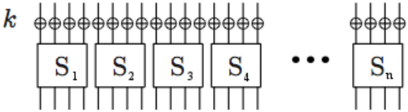
$$\#AI_L(S, w_{in}, w_{out}) \geq 2n + 1 - N_S(w_{in}, w_{out})$$

$N_S(w_{in}, w_{out})$ small $\rightsquigarrow$ a lot of linear relations between input and output

An upper bound on the complexity

If plaintext (or ciphertext) known

Plaintext

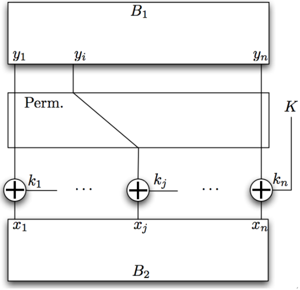


$$N_{S_1} \times N_{S_2} \times N_{S_3} \times \ldots N_{S_n}$$

$\Rightarrow$ leakages $\Rightarrow$ constraints $\Rightarrow$ exhaustive search reduced to $\prod_i N_{S_i}$
Ex. with PRESENT : $\mathbb{E}(\prod_i N_{S_i}) = 2^{29}$ (instead of 2^{64})

Unknown P/C or few consecutive leakages

- $N_S(w_{in}, w_{out})$ small $\Rightarrow$ exhaustive search reduced but must be done on 2 consecutive rounds
- $N_S(w_{in}, w_{out})$ very small (≤ 6) $\Rightarrow$ fixed input/output bits!



$\rightsquigarrow$ subkey bits deduced without knowing plaintext/ciphertext

Experiments

Implementation:

- algebraic cryptanalysis library (systems generator)
- ASCA in MAGMA

Experiments performed against PRESENT and AES

Analysis supported by experiments:

	GB (F4)
reject of leakages with large N_S	✓
reject of leakages with small N_S	✗
no consecutive rounds with leakages	✗

Experiments

Implementation:

- algebraic cryptanalysis library (systems generator)
- ASCA in MAGMA

Experiments performed against PRESENT and AES

Analysis supported by experiments:

	GB (F4)	SAT-solvers
• reject of leakages with large N_S	✓	✓($<$3h)
• reject of leakages with small N_S	✗	✗($>$3h)
• no consecutive rounds with leakages	✗	✗($>$3h)

Analysis seems valid with both Gröbner basis and SAT-solver

ASCA Resistant S-Boxes ?

Are there ASCA resistant S-Boxes ?

Requirements:

- few fixed input/output bits
- few linear relations

$\rightsquigarrow$ N_S large for a lot of leakages

A first class: N_S max for all leakages

$$N_S(w_{in}, w_{out}) = \#(HW^{-1}(w_{in}) \bigcap S^{-1}(HW^{-1}(w_{out})))$$

Then, S must satisfy

$$HW^{-1}(w_{in}) = S^{-1}(HW^{-1}(w_{out}))$$

and

$$w_{in} = w_{out} \text{ or } w_{in} = n - w_{out}$$

Resistant S-Boxes ?

Characterization:

$$S(x) = \pi(x) \oplus f(HW(x))(1, ..., 1)$$

- $\pi(x)$ = permutation stable under HW (i.e. $HW(x) = HW(\pi(x))$)
- f = boolean function s.t. $\forall x \in \{0, \ldots, n\}, f(x) = f(n - x)$

Example of such 4-bit S-box:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	0	B	D	C	E	6	9	8	7	5	3	1	A	2	4	F

$w_{in} = w_{out}$ or $w_{in} = n - w_{out}$

Experiments

Experiments performed against PRESENT and AES

Analysis supported by experiments:

	GB	SAT-solver
reject of leakages with large N_S	✓	✓
reject of leakages with small N_S	✗	✗
no consecutive leaked rounds	✗	✗
with resistant S-boxes	✗	✗

Resistant S-Boxes ?

Proposition:

Let S an n-bit optimally ASCA-resistant S-Box.
Then we have

$$n \text{ even } \Rightarrow \text{nonlinearity}(S) = 0$$

Proof:

$$w_{in} = w_{out} \text{ or } w_{in} = n - w_{out}$$

then $\quad w_{in} + w_{out} \equiv 0 \pmod 2$ because n is even,
and $\quad \forall x \in \mathbb{F}_2^n, \quad \langle x|(1,\dots,1)\rangle + \langle S(x)|(1,\dots,1)\rangle \equiv 0 \pmod 2$

$$\text{Lin}(S) = \max_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^n\setminus\{0\}} \left| \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle x|a\rangle + \langle S(x)|b\rangle} \right| = 2^n$$

$\square$

Perspectives

Open problem:

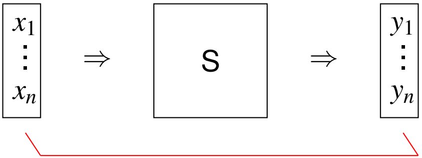
(optimally) ASCA-resistant + strong against linear cryptanalysis ?

Perspectives:

- Other leakage models
- Leakages with noise/errors

Some other leakage models

Example 1 : Hamming Distance Leakage Model



$$HD(x, y) = HW(x \oplus y)$$

HD model :

- $\mathbb{E}(\#AI_L) = 2,3$, $\mathbb{E}(N_S) \simeq 2^{5,9}$

Upper bound (first round):

- PRESENT: $E(N_S)^8 \simeq 2^{47}$ $\Rightarrow$ ✓ $\simeq 70\%$ ($<$ 3h)
- AES: $E(N_S)^{16} \simeq 2^{90}$ ✗

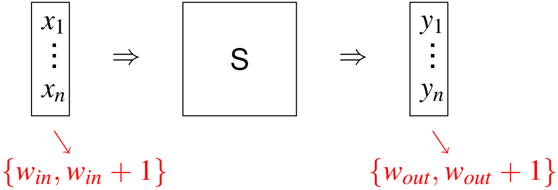
d	0	1	2	3	4	5	6	7	8
$N_S(d)$	0	0	16	56	81	64	30	8	1
$\#AI_L(S, d)$	0	0	10	3	1	1	1	9	16
fixed bits	0	0	0	0	0	0	0	0	16

Figure : HD model and PRESENT S-Box

Perspectives:

- better leakages exploitation / using more HD

Example 2 : uncertain Hamming Weight



Observations :

- $\mathbb{E}(lin.\ eq.) = 2,6$
- $\mathbb{E}(N_S) \simeq 2^5$
- Upper bound (first round) PRESENT: $\mathbb{E}(N_S)^8 \simeq 2^{41}$ ✓(SAT solver)

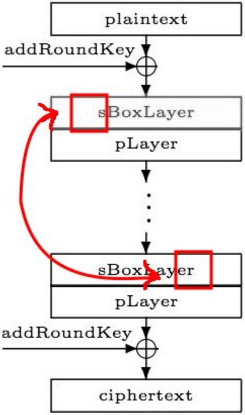
Perspectives:

- on AES
- larger error rate

Example 3 : Side Channel Collision Attacks

Side Channel Collision Attacks seen as ASCA

Assumptions : equalities between intermediate bits



Experiments with SAT-solver :

1. with extremal rounds ✓
2. without extremal rounds ✗

Perspectives:

- Criterion of success (complexity)?
- Exploit new collisions (e.g. middle rounds) ?

Example 4 : fault attack with algebraic methods

faulty ciphertexts

$$\begin{cases} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ \vdots \\ s_3 y_{124} + y_{121} y_{124} + y_{121} + \dots \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \end{cases}$$

$$\begin{cases} x_4 + s_1 s_3 + s_2 + s_4 + k_4 + 1, \\ y_{124} k_{122} + y_{124} k_{123} + y_{124} + k_{121} + \dots \\ \vdots \\ s_{121} s_{122} + s_{121} s_{123} + s_{121} s_{124} + \dots \end{cases}$$

Experiment on AES:

1. Piret and Quisquater DFA (round 7) ✓

Perspectives:

1. faults on other rounds
2. Other fault models (Chong Hee Kim, 2011) /
3. Other cryptosystems: DES (Courtois2010), . . .
4. Criterion of success (complexity) ?

On public-key cryptography : Attacking (EC)DSA with only an implicit hint

Algebraic cryptanalysis with additional information

Cryptographic Algorithm (signature schemes) $\xrightarrow{\text{Modeling}}$

$$\begin{cases} k_1 s_1 & = & h_1 + a r_1 \mod q \\ k_2 s_2 & = & h_2 + a r_2 \mod q \\ \vdots & & \vdots \\ k_i & = & \dots \\ k_j & = & \dots \end{cases}$$

Solving in practice ?

additional information on secret data

Possible scenarios:

- power analysis (known bits) $\Rightarrow$ Howgrave-Graham and Smart (2001), ...
- fault attacks $\Rightarrow$ Bao (1996), Giraud and Knudsen (2004), ...
- locked register (RSA) $\Rightarrow$ Implicit Factoring, May Ritzenhofen (2009)
- with DSA-like schemes ?

With only an implicit hint: the case of (EC)DSA

Framework:

Let (M_i, S_i) be given signed messages with DSA-like schemes.
Assumption: nonces share a portion of their (unknown) bits

Our results:

- secret key found in polynomial time
- positions for shared bits: MSB, LSB, Middle, etc
- implicit hint is exploited by lattice method (shortest vector)
- required shared bits/signatures comparable to explicit methods (e.g. ≈ 3 shared bits on 100 signed messages)
- efficient with 1 shared bit/400 signatures

DSA-like schemes

We recall the DSA-style signature scheme:

- DLP instance:
  - G group of prime order q ($2^{N-1} \leq q < 2^N$)
  - private key is an integer $a \in \{1, \ldots, q-1\}$
  - public key is $g^{\mathbf{a}} \in G$, where g is a generator of G
- Signature:
  - to sign a message m, the signer computes $h = HASH(m)$ and
  - chooses a random number $\mathbf{k} \in \{1, \ldots, q-1\}$ called the ephemeral key or nonce
  - the signature is the pair (r, s) given by

$$r = g^k \bmod q \quad \text{and} \quad s = k^{-1}(h + ar) \bmod q$$

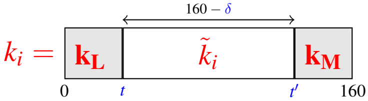
Our assumptions

To simplify, we choose the size of q equals to $N = 160$ bits (thus a and k_i are $< 2^{160}$)

Attackers has messages m_i with associated signatures (r_i, s_i) $i = 1, \ldots, n$

Implicit Hint

all ephemeral keys k_i used to signed m_i shared δ bits between their MSB/LSB:



Notice that k_i, $\tilde{k}_i$, $\mathbf{k_L}$ and $\mathbf{k_M}$ are unknown

Shared MSB and LSB: first lattice

Implicit hypothesis:

$$k_i = \boxed{\mathbf{k_L}}\overbrace{\boxed{\quad\tilde{k}_i\quad}}^{160-\delta}\boxed{\mathbf{k_M}}$$

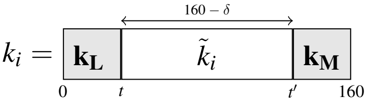
0 t t' 160

Polynomial system modeling (two signatures):

$$\mathcal{S} : \begin{cases} k_1 s_1 = h_1 + a r_1 \mod q \\ k_2 s_2 = h_2 + a r_2 \mod q \\ \\ k_1 = k_L + 2^t \tilde{k}_1 + 2^{t'} k_M \\ k_2 = k_L + 2^t \tilde{k}_2 + 2^{t'} k_M \end{cases}$$

Shared MSB and LSB: first lattice

Implicit hypothesis:

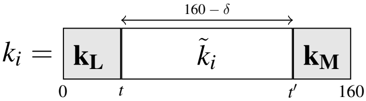


Polynomial system modeling (two signatures):

$$\mathcal{S} : \begin{cases} (k_L + 2^t \tilde{k}_1 + 2^{t'} k_M) s_1 = h_1 + a r_1 \mod q \\ (k_L + 2^t \tilde{k}_2 + 2^{t'} k_M) s_2 = h_2 + a r_2 \mod q \end{cases}$$

Shared MSB and LSB: first lattice

Implicit hypothesis:



Polynomial system modeling (two signatures):

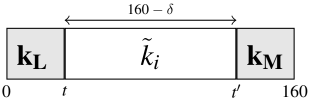
$$\mathcal{S} : \begin{cases} (k_L + 2^t \tilde{k_1} + 2^{t'} k_M) s_1 & = & h_1 + a r_1 \mod q \\ (k_L + 2^t \tilde{k_2} + 2^{t'} k_M) s_2 & = & h_2 + a r_2 \mod q \end{cases}$$

Elimination of the variables k_L and k_M:

$$2^{-t}(s_1^{-1} h_1 - s_2^{-1} h_2) + 2^{-t} a (s_1^{-1} r_1 - s_2^{-1} r_2) - (\tilde{k_1} - \tilde{k_2}) = 0 \mod q$$

Shared MSB and LSB: first lattice

Implicit hypothesis:

$k_i =$ 

Polynomial system modeling (two signatures):

$$2^{-t}(s_1^{-1}h_1 - s_2^{-1}h_2) + 2^{-t}a(s_1^{-1}r_1 - s_2^{-1}r_2) - (\tilde{k}_1 - \tilde{k}_2) = 0 \mod q$$

$$\boxed{F(x_0, x_1, x_2) = x_0\alpha + x_1\beta - x_2 \in \mathbb{F}_q[x_0, x_1, x_2] \text{ verifies } F(1, a, \kappa_{1,2}) = 0}$$

- $\alpha = 2^{-t}(s_1^{-1}h_1 - s_2^{-1}h_2) \mod q$
- $\beta = 2^{-t}(s_1^{-1}r_1 - s_2^{-1}r_2) \mod q$
- $\kappa_{1,2} = (\tilde{k}_1 - \tilde{k}_2)$

Shared MSB and LSB: first lattice

Implicit hypothesis:

$160 - \delta$

$$k_i = \boxed{\mathbf{k_L}}\boxed{\quad \tilde{k}_i \quad}\boxed{\mathbf{k_M}}$$

$0 \quad t \quad t' \quad 160$

Polynomial system modeling (two signatures):

$$\boxed{F(x_0, x_1, x_2) = x_0\alpha + x_1\beta - x_2 \in \mathbb{F}_q[x_0, x_1, x_2] \text{ verifies } F(1, a, \kappa_{1,2}) = 0}$$

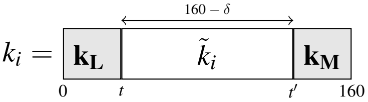
The set of solutions L of F forms a lattice :

$$\boxed{L = \{(x_0, x_1, x_2) \in \mathbb{Z}^3 \ : \ x_0\alpha + x_1\beta - x_2 = 0 \mod q\}}$$

with $v_0 = (1, a, \kappa_{1,2}) \in L$

Shared MSB and LSB: first lattice ($n > 2$ signatures)

Implicit hypothesis:



Polynomial system modeling ($n > 2$ signatures):

$$\begin{cases} \alpha_2 + a\beta_2 - \kappa_{1,2} & \equiv & 0 & \pmod q \\ \alpha_3 + a\beta_3 - \kappa_{1,3} & \equiv & 0 & \pmod q \\ \vdots \quad \vdots & & \vdots & \vdots \\ \alpha_n + a\beta_n - \kappa_{1,n} & \equiv & 0 & \pmod q \end{cases}$$

$\alpha_i = 2^{-t}(s_1^{-1}m_1 - s_i^{-1}m_i) \bmod q$, $\beta_i = 2^{-t}(s_1^{-1}r_1 - s_i^{-1}r_i) \bmod q$, $\kappa_{i,j} = \tilde{\mathbf{k}}_i - \tilde{\mathbf{k}}_j$

$$\boxed{\begin{array}{c} L = \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} : x_0\alpha_i + x_1\beta_i - x_i = 0 \mod q\,(i = 2, \ldots, n)\} \\ \text{with } v_0 = (1, a, \kappa_2, \ldots, \kappa_n) \in L \end{array}}$$

Shared MSB and LSB: first lattice ($n > 2$ signatures)

$$L = \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} : x_0\alpha_i + x_1\beta_i - x_i = 0 \mod q\,(i = 2, \ldots, n)\}$$
with $v_0 = (1, a, \kappa_2, \ldots, \kappa_n) \in L$

The lattice L is generated by the row-vectors of the matrix

$$M = \begin{pmatrix} 1 & 0 & \alpha_2 & \ldots & \alpha_n \\ 0 & 1 & \beta_2 & \ldots & \beta_n \\ 0 & 0 & q & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & q \end{pmatrix}$$

and $(1, \mathbf{a}, \lambda_2, \ldots, \lambda_n) \cdot M = v_0$ for some λ_i.

Shared MSB and LSB: first lattice, first result

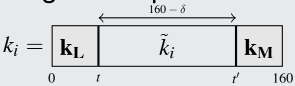
Gaussian Assumption

If $||v_0||^2$ is smaller than $\frac{d}{2\pi e}\,\mathrm{Vol}(L)^{\frac{2}{d}}$ then v_0 is a shortest vector of L.
Here the dimension is $d = n+1$.

Theorem 1

Let be given n signatures (r_i, s_i). Under the following assumptions

- Gaussian Assumption
- $2^{159-\delta} \leq a < 2^{160-\delta}$
- Implicit hint: nonces k_i share δ bits (LSB/MSB)



Then the vector v_0 is a shortest vector in L as soon as

$$\delta \geq \frac{320 + (n-1)}{n+1} + \frac{1 + \log_2(\pi e) - \log_2(\frac{n+1}{n})}{2}$$

ex: 32 bits shared $\Rightarrow$ 10 signatures needed

Shared MSB and LSB: improvement

The lattice L is generated by the row-vectors of the matrix

$$M = \begin{pmatrix} 1 & 0 & \alpha_2 & \dots & \alpha_n \\ 0 & 1 & \beta_2 & \dots & \beta_n \\ 0 & 0 & q & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & q \end{pmatrix}$$

and the vector $(1, \mathbf{a}, \lambda_2, \dots, \lambda_n) \cdot M = (1, a, \kappa_2, \dots, \kappa_n) = v_0$.

$\Rightarrow$ Cancel the second coefficient of v_0

$\Rightarrow$ Considering a new lattice L.

Shared MSB and LSB: improvement

Let L' (dimension n) generated by the row-vectors of the matrix

$$M' = \begin{pmatrix} 1 & \alpha_2 & \dots & \alpha_n \\ 0 & \beta_2 & \dots & \beta_n \\ 0 & q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & q \end{pmatrix}$$

and the vector $(1, \mathbf{a}, \lambda_2, \dots, \lambda_n) \cdot M' = (1, \kappa_2, \dots, \kappa_n) = v_0'$.

$\Rightarrow$ The secret a is no more contained in v_0'

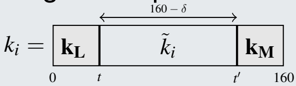
$\Rightarrow$ The matrix M do not form a basis of the lattice

Shared MSB and LSB: improvement

Theorem 2

Let be given n signatures (r_i, s_i). Under the following assumptions

- Gaussian Assumption
- $\cancel{2^{159-\delta} \leq a < 2^{160-\delta}}$
- Implicit hint: nonces k_i share δ bits (LSB/MSB)



Then the vector v'_0 is a shortest vector in L' as soon as

$$\delta \geq \frac{320 + (n-2)}{n} + \frac{1 + \log_2(\pi e) - \log_2(\frac{n}{n-1})}{2}$$

ex: 32 bits shared $\Rightarrow$ 11 signatures needed

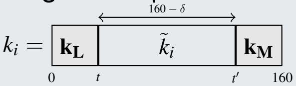
Shared MSB and LSB: improvement *bis*

$\Rightarrow v_0' = (1, \kappa_2, \ldots, \kappa_n)$, using weighted norm

$$\langle (x_0, \ldots, x_n), (y_0, \ldots, y_n) \rangle := \sum_{i=0}^{n} x_i y_i 2^{2(160 - \lceil \log_2(v_{0,i}) \rceil)}$$

Theorem 3

Let be given n signatures (r_i, s_i). Under the following assumptions

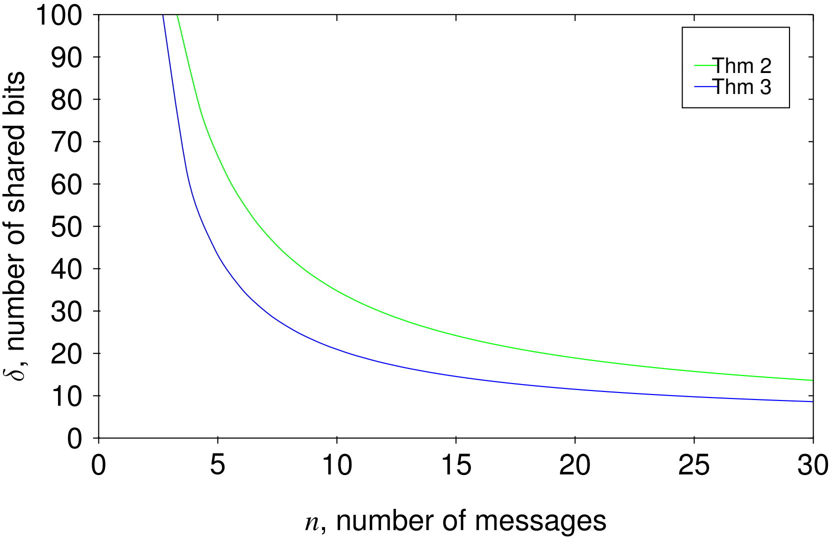


- Gaussian Assumption
- $\cancel{2^{159-\delta} \leq a < 2^{160-\delta}}$
- Implicit hint: nonces k_i share δ bits (LSB/MSB)

Then the vector v_0' is a shortest vector in L' as soon as

$$\delta \geq \frac{160 + (n-2)}{n-1} + \frac{n(1 + \log_2(\pi e))}{2(n-1)} \qquad (1)$$

Theoretical comparison



ex: 32 bits shared $\Rightarrow$ 7 signatures needed

Performing the computations

Computation of a shortest vector

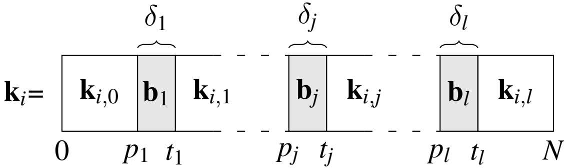
This is an NP-hard problem ! The complexity is

- Exponential in d by using Kannan's algorithm
- Polynomial in d if v_0 can be found with LLL (Polynomial complexity but approximate (exponential 2^d) shortest vector)

$\Rightarrow$ Experimented using LLL: we always obtain the private key
$\Rightarrow$ The computational time is not more than one minute (Magma 2.17)
$\Rightarrow$ In practice, the attack can be mounted with $\delta < 3$

Generalization: shared blocks

General implicit hint:



$\Rightarrow$ More technical but comparable results

ex with 3 blocks: 7 signatures $\rightarrow$ 37 shared bits need

Perspectives

Remarks:

- ECDSA implicit attack can be applied *mutatis mutandis* on ElGamal or Schnorr signatures
- Backdoor in PRNG using such implicit hint are undetectable with Dieharder/STS

Perspectives:

- Implicit hints in other cryptosystems?
- Other kind of implicit hints ? (linear, polynomial relations, ...)
- New statistical tests ?

Conclusion

- Additional information (even implicit) exploited with algebraic method on both symmetric and asymmetric cryptographic systems
- equivalent leakage models ?
- ex: implicit hint (DSA) $\Longleftrightarrow$ collisions (ASCA)

Faugère, Goyet, Renault, A new Criterion for Effective Algebraic Side Channel Attacks, COSADE 2011

Carlet, Faugère, Goyet, Renault, An Analysis of Algebraic Side Channel Attacks, February 2012, Journal of Cryptographic Engineering

Faugère, Goyet, Renault, Attacking (EC)DSA Given Only an Implicit Hint, SAC 2012