Attacking (EC)DSA Given Only an Implicit Hint

SAC 2012

Jean-Charles Faugère[1], Christopher Goyet[1,2] Guénaël Renault[1]

[1]: UPMC, INRIA, CNRS, LIP6

[2]: Thales Communications and Security

August 2012

THALES Communications & Security

UPMC SORBONNE UNIVERSITÉS LIP6 CNRS INRIA informatiques mathématiques

Part I

Introduction

Recovering the whole secret key in polynomial time

Partial exposure of the secret key:

- RSA: $N = pq$ can be factored given some bits of p
  - Rivest and Shamir (Eurocrypt 1985)
  - Coppersmith (Eurocrypt 1996)
  - Boneh *et al.* (Asiacrypt 1998)
  - ...
  - Herrmann and May (Asiacrypt 2008)
- DSA: discrete logarithm of g^k given small number of bits of k
  - Howgrave-Graham and Smart (2001)
  - Nguyen and Shparlinski (2002)
  - ...

☞ Take care to power analysis, fault attacks, protocol failures, etc.

Recovering the whole secret key in polynomial time

Partial exposure of the secret key:

- RSA: $N = pq$ can be factored given some bits of p
  - Rivest and Shamir (Eurocrypt 1985)
  - Coppersmith (Eurocrypt 1996)
  - Boneh *et al.* (Asiacrypt 1998)
  - ...
  - Herrmann and May (Asiacrypt 2008)
- DSA: discrete logarithm of g^k given small number of bits of k
  - Howgrave-Graham and Smart (2001)
  - Nguyen and Shparlinski (2002)
  - ...

☞ Take care to power analysis, fault attacks, protocol failures, etc.

Nowadays ?

Countermeasures development:

- unlikely that attacker can determine a set of bits
- too strong assumption
- but . . .

does an attacker really need to explicitly know some bits ?

Nowadays ?

Countermeasures development:

- unlikely that attacker can determine a set of bits
- too strong assumption
- but . . .

does an attacker really need to explicitly know some bits ?

With only an implicit hint: the case of RSA

Implicit factorization

- introduced by May and Ritzenhofen (PKC 2009)
- **not required to explicitly know some bits**
- an implicit hint may be enough $\Rightarrow$ polynomial factorization

Let $N_i = p_i q_i$ be given RSA moduli.
Implicit Hint was the suspicion that:
number of p_i's **share enough bits**

☞ Many practical scenarii proposed (side-channel, design, ...)

With only an implicit hint: the case of RSA

Implicit factorization

- introduced by May and Ritzenhofen (PKC 2009)
- **not required to explicitly know some bits**
- an implicit hint may be enough $\Rightarrow$ polynomial factorization

Let $N_i = p_i q_i$ be given RSA moduli.
Implicit Hint was the suspicion that:
number of p_i's **share enough bits**

☞ Many practical scenarii proposed (side-channel, design, ...)

What about (EC)DSA ?

☞ application of the May-Ritzenhofen trick to DSA scenario

Proposed Problematic:

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

- evaluate the complexity to find the secret key
- possible positions for shared bits? (MSB, LSB, Middle, etc)

Possible applications:

- fault attacks (unknown bits modification)
- destroyed register (like in May-Ritzenhofen 2009)
- malicious modification of random generators (e.g. smart card)

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

Our results:

- 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 down to 1 shared bit/400 signatures
- malicious PRNG undetectable (DieHarder & STS testing suite)

DSA-like schemes

We recall the DSA-style signature scheme:

- DLP instance:
  - let G be a multiplicative group of prime order q (elements of G are seen as integers)
  - with $2^{N-1} \leq q < 2^N$, N at least 160
  - private key is an integer $a \in \{1, \ldots, q-1\}$
  - public key is $g^{\mathbf{a}} \in G$, where g is a publicly known 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

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

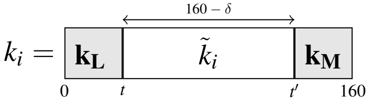
Our assumptions

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

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

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
but the positions t and t' are known

Part II

Lattice Attack

Implicit hypothesis:

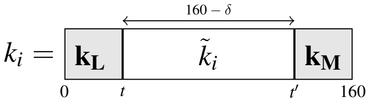
$$k_i = \boxed{\mathbf{k_L}}_{\,0 \,\to\, t}\ \overbrace{\boxed{\quad \tilde{k}_i \quad}}^{160-\delta}_{\,t \,\to\, t'}\ \boxed{\mathbf{k_M}}_{\,t' \,\to\, 160}$$

Polynomial system modeling (two signatures):

$$\mathcal{S} : \begin{cases} k_1 s_1 = h_1 + a r_1 \mod q \\ k_2 s_2 = h_2 + a r_2 \mod q \end{cases}$$

Shared MSB and LSB: first lattice

Implicit hypothesis:

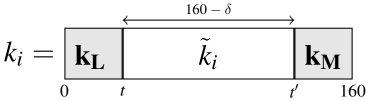


Polynomial system modeling (two signatures):

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

Shared MSB and LSB: first lattice

Implicit hypothesis:



Polynomial system modeling (two signatures):

$$f_i(k_L, k_i, k_M, a) = h_i + ar_i - (k_L + 2^t \tilde{k}_i + 2^{t'} k_M) s_i$$

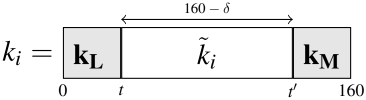
$$\mathcal{S} : \begin{cases} f_1(k_L, k_1, k_M, a) & = & 0 \mod q \\ f_2(k_L, k_2, k_M, a) & = & 0 \mod q \end{cases}$$

Elimination of the variables k_L and k_M:

$$2^{-t} s_1^{-1} f_1 - 2^{-t} s_2^{-1} f_2 = 2^{-t}(s_1^{-1} h_1 - s_2^{-1} h_2) + 2^{-t} a (s_1^{-1} r_1 - s_2^{-1} r_2) - (\tilde{k_1} - \tilde{k_2})$$

Shared MSB and LSB: first lattice

Implicit hypothesis:



Polynomial system modeling (two signatures):

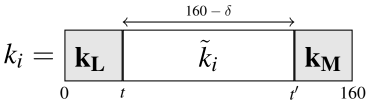
$$2^{-t}s_1^{-1}f_1 - 2^{-t}s_2^{-1}f_2 = 2^{-t}(s_1^{-1}h_1 - s_2^{-1}h_2) + 2^{-t}a(s_1^{-1}r_1 - s_2^{-1}r_2) - (\tilde{k_1} - \tilde{k_2})$$

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

- $\alpha = 2^{-t}(s_1^{-1}h_1 - s_2^{-1}h_2) \mod q$
- $\beta = 2^{-t}(s_1^{-1}r_1 - s_2^{-1}r_2) \mod q$
- $\kappa = (\tilde{k_1} - \tilde{k_2})$

Shared MSB and LSB: first lattice

Implicit hypothesis:



Polynomial system modeling (two signatures):

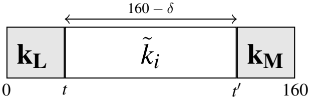
$$\boxed{F(x_0, x_1, x_2) = x_0\alpha + x_1\beta - x_2 \in \mathbb{F}_q[x_0, x_1, x_2] \text{ verifies } F(1, a, \kappa) = 0}$$

The set of solutions L of F forms a lattice :

$$\boxed{v_0 = (1, a, \kappa) \in L = \{(x_0, x_1, x_2) \in \mathbb{Z}^3 \ : \ x_0\alpha + x_1\beta - x_2 = 0 \mod q\}}$$

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

Implicit hypothesis:

$k_i =$ 

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

$$\begin{cases} \alpha_2 + a\beta_2 - \kappa_2 & \equiv & 0 & \pmod{q} \\ \alpha_3 + a\beta_3 - \kappa_3 & \equiv & 0 & \pmod{q} \\ \vdots \quad \vdots \quad \vdots & \vdots & & \vdots \\ \alpha_n + a\beta_n - \kappa_n & \equiv & 0 & \pmod{q} \end{cases}$$

$\alpha_i = 2^{-t}(s_1^{-1}m_1 - s_i^{-1}m_i) \bmod q$, $\beta_i = 2^{-t}(s_1^{-1}r_1 - s_i^{-1}r_i) \bmod q$, $\kappa_i = \tilde{\mathbf{k}}_1 - \tilde{\mathbf{k}}_i$

$$v_0 = (1, a, \kappa_2, \ldots, \kappa_n) \in L$$

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

Is v_0 a shortest vector in L?

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

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

Is v_0 a shortest vector 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 ($n > 2$ signatures)

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

Is v_0 a shortest vector in L?

GA: Gaussian Assumption

Let L be a lattice of dimension d and $v_0 \in L$. If $||v_0||^2$ is smaller than $\frac{d}{2\pi e} \operatorname{Vol}(L)^{\frac{2}{d}}$ then v_0 is a shortest vector of L.

☞ Assumption generally verified in practice (in particular during our experiments).

☞ Find conditions on n and δ to be under the GA.

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

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

GA: 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 dimension $d = n + 1$.

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

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

$$\boxed{\mathrm{Vol}(L) = q^{n-1} \geq 2^{159(n-1)} \Rightarrow \mathrm{Vol}(L)^{\frac{2}{n+1}} \geq 2^{318\frac{n-1}{n+1}}}$$

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

GA: Gaussian Assumption

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

$$\boxed{\operatorname{Vol}(L) = q^{n-1} \geq 2^{159(n-1)} \Rightarrow \operatorname{Vol}(L)^{\frac{2}{n+1}} \geq 2^{318\frac{n-1}{n+1}}}$$

The vector $v_0 \in L$ is given by

$$v_0 = (1, a, \kappa_2, \ldots, \kappa_n)$$

$$\boxed{||v_0||^2 \geq a^2 \geq 2^{318}}$$

$\Rightarrow$ v_0 has not a high chance to be short!

☞ We can suppose a smaller (exhaustive search):

$$2^{159-\delta} \leq a < 2^{160-\delta}$$

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

GA: 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 dimension $d = n + 1$.

$$\boxed{\mathrm{Vol}(L) = q^{n-1} \geq 2^{159(n-1)} \Rightarrow \mathrm{Vol}(L)^{\frac{2}{n+1}} \geq 2^{318\frac{n-1}{n+1}}}$$

The vector $v_0 \in L$ is given by

$$v_0 = (1, a, \kappa_2, \ldots, \kappa_n)$$

$$\boxed{||v_0||^2 \geq a^2 \geq 2^{318}}$$

$\Rightarrow$ v_0 has not a high chance to be short!
☞ We can suppose a smaller (exhaustive search):

$$2^{159-\delta} \leq a < 2^{160-\delta}$$

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

GA: 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 dimension $d = n + 1$.

$$\boxed{\mathrm{Vol}(L) = q^{n-1} \geq 2^{159(n-1)} \Rightarrow \mathrm{Vol}(L)^{\frac{2}{n+1}} \geq 2^{318\frac{n-1}{n+1}}}$$

The vector $v_0 \in L$ is given by

$$v_0 = (1, a, \kappa_2, \ldots, \kappa_n)$$

We have $2^{159-\delta} \leq a < 2^{160-\delta}$ and $2^{159-\delta} \leq \kappa_i < 2^{160-\delta}$, thus

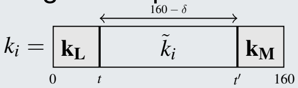
$$\boxed{||v_0||^2 \leq n \cdot 2^{2(160-\delta)} = 2^{320-2\delta+\log_2(n)}}$$

Shared MSB and LSB: first lattice, first result

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 secret a can be computed in time $\mathcal{C}(n+1, \frac{1}{2}\log_2(n-1)+160)$ as soon as

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

Notation

We denote by $\mathcal{C}(d, B)$ the time complexity of computing a shortest vector of a d-dimensional lattice L defined by vectors with norm of bit-size bounded by B.

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

☞ Cancel the second coefficient of v_0

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

☞ The secret a is no more read in the vector v_0 but in the transformation matrix.

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

We have

$$\boxed{||v_0||^2 \leq (n-1) \cdot 2^{2(160-\delta)} = 2^{320-2\delta+\log_2(n-1)}}$$

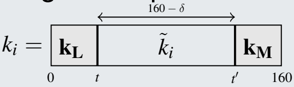
and by considering the sublattice $S \subset L'$ of index q and volume q^{n-1} generated by the first and the last $n-1$ row of M' we deduce

$$\boxed{\mathrm{Vol}(L') = [L' : S]^{-1}\,\mathrm{Vol}(S) = q^{n-2} \geq 2^{159(n-2)} \Rightarrow \mathrm{Vol}(L')^{\frac{2}{n}} \geq 2^{318\frac{n-2}{n}}}$$

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 secret a can be computed in time $\mathcal{C}(n, \frac{1}{2}\log_2(n-1) + 160)$ as soon as

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

Notation

We denote by $\mathcal{C}(d, B)$ the time complexity of computing a shortest vector of a d-dimensional lattice L defined by vectors with norm of bit-size bounded by B.

Shared MSB and LSB: improvement *bis*

By using weighted norm we obtain a better result

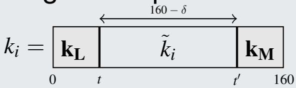
$$\langle (x_0, \ldots, x_n), (y_0, \ldots, y_n) \rangle := \sum_{i=0}^{n} x_i y_i 2^{2(160 - \lceil \log_2(v_{0,i}) \rceil)}$$

☞ drastically reduce the required number of shared bits δ in practice

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 secret a can be computed in time $\mathcal{C}(n, \frac{1}{2}\log_2(n-1) + 160\delta)$ 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

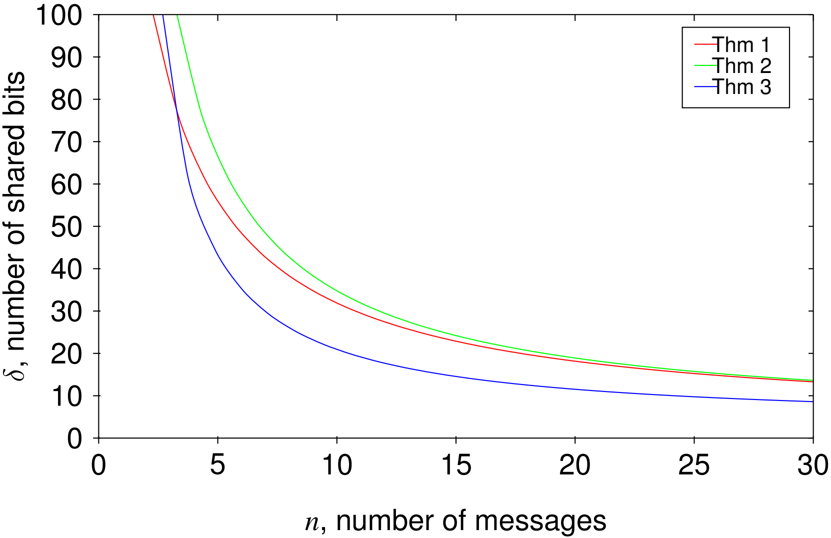
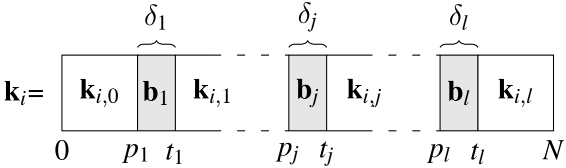


Figure : Theoretical bounds of Theorems

Generalization: shared blocks

General implicit hint:



☞ More technical but comparable results (see the paper)

Part III

Experimental Results

Performing the computations

Computation of a shortest vector

This is an NP-hard problem ! The complexity $\mathcal{C}(d, B)$ is

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

☞ We experimented our attack using LLL: we always obtain the shortest vector, even for large dimension!
☞ The computational time is not more than one minute (Magma 2.17)

Success rates

δ	n, Number of messages								
	3	4	5	6	7	8	9	10	11
40	0	0	80	100	100	100	100	100	100
30	0	0	0	3	100	100	100	100	100
20	0	0	0	0	0	0	83	100	100
Time (s)	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	0.1	0.1
δ	n, Number of messages								
	170	180	190	200	250	300	400	500	600
2	73	80	85	100	100	100	100	100	100
1	0	2	8	10	35	56	91	99	99
Time (s)	3.5	3.8	4.1	4.2	6.3	8.5	15	27	44

Table : Success rate of LSB attack

Lines with 100 correspond to theoretical minimal values of δ for a given number of messages (columns).

☞ The second table shows that the attack behaves better in practice! (In theory an attack can not be mount with $\delta < 3$).

Part IV

Conclusion

Results and Concluding Remarks

Summary of the results:

- ☞ Lattice attack on (EC)DSA using an implicit hint on the nonces
- ☞ Success rate of 100% for our theoretical results using LLL ($\Rightarrow$ heuristic polynomial time attack)
- ☞ Attack behaves better in practice
- ☞ The knowledge of the shared bits is not necessary (comparable results in both cases)

Concluding remarks:

- ☞ Backdoor in PRNG using such implicit hint are undetecteble with Dieharder/STS (see the paper)
- ☞ This attack can be applied *mutatis mutandis* on ElGamal or Schnorr signatures
- ☞ Is it possible to use implicit hints in other cryptosystems?