Attacking ECDSA leaking discrete bits with a more efficient lattice

Shuqin Fan, Xianhui Lu, Shuaigang Li

Speaker: Shuaigang Li

CONTENTS

01 Attacking ECDSA with lattice reduction algorithms

02 Previous works

03 Our improvement

1. Attacking ECDSA with lattice reduction algorithms

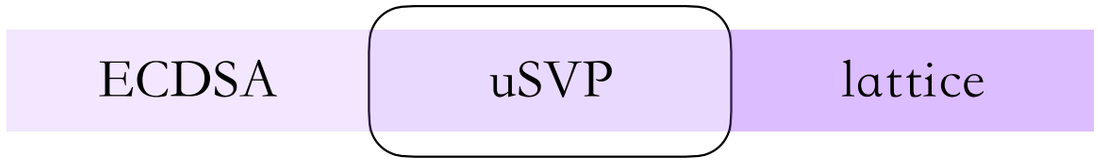
Elliptic curve: E, a fixed point $G \in E$ of a big prime order q.

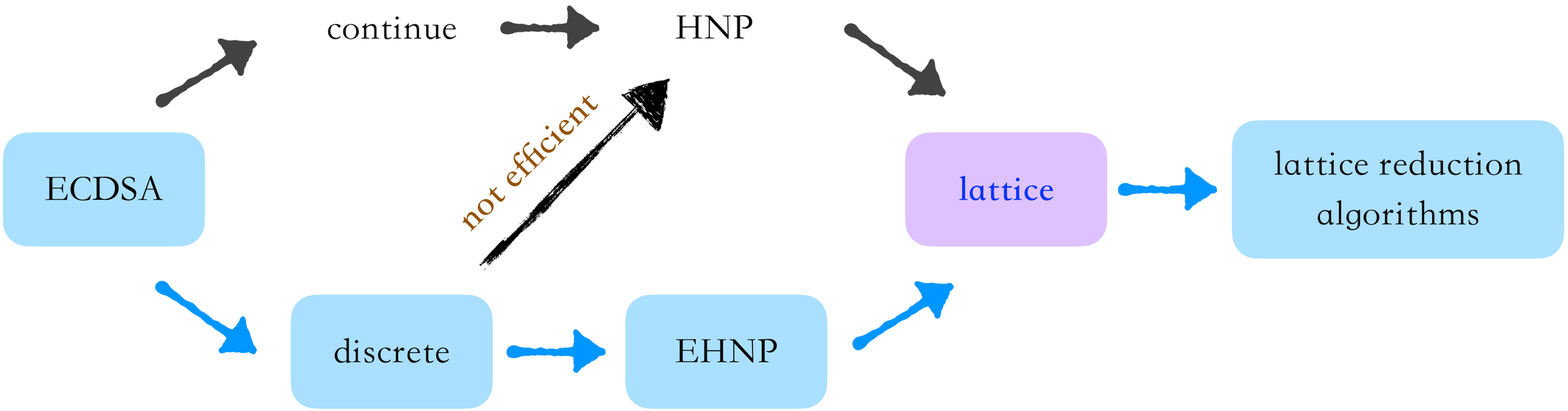
secret key: α, point: $Q = \alpha \cdot G$, hash function: H, message: m

- $k \xleftarrow{\$} \mathbb{Z}_q^*$, $k \cdot G \triangleq (r, y)$, if $r = 0$, restart
- compute $s = k^{-1}(H(m) + \alpha r) \mod q$, if $s = 0$, return the first step
- return signature (r, s)

For attackers: $sk - \alpha r - H(m) = 0 \mod q$

1. Attacking ECDSA with lattice reduction algorithms





continue: 1 1 0 1 0 0 1 0 1 1 1 0

discrete: 1 1 0 1 0 0 1 0 1 1 1 0

$$sk - \alpha r - H(m) = 0 \mod q, \text{ the situation: } k = \sum_i 2^{\lambda_i} k_i$$

1. Attacking ECDSA with lattice reduction algorithms

$$sk - \alpha r - H(m) = 0 \mod q, \text{ the situation: } k = \sum_i 2^{\lambda_i} k_i$$

Example

$$s_0 k_0 - \alpha r_0 - H(m_0) = 0 \mod q$$

$$s_1 k_1 - \alpha r_1 - H(m_1) = 0 \mod q$$

Eliminate α

$$r_1 s_0 k_0 - r_0 s_1 k_1 + (r_0 H(m_1) - r_1 H(m_0)) = 0 \mod q$$

Substitute k_i

$$r_1 s_0 (k_{00} + 2^{l_0} k_{01}) - r_0 s_1 (k_{10} + 2^{l_1} k_{11}) + \beta + hq = 0$$

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1) \begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

$$= (0, k_{00} + \beta_1, k_{01} + \beta_2, k_{10} + \beta_3, k_{11} + \beta_4, 1) \triangleq \mathbf{w}$$

ECDSA ⇨ uSVP

1. Attacking ECDSA with lattice reduction algorithms

How to construct a more efficient lattice

$$r_1 s_0(k_{00}+2^{l_0}k_{01}) - r_0 s_1(k_{10}+2^{l_1}k_{11}) + \beta + hq = 0$$

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

target vector:

$$\mathbf{w} = (0, k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

The methods

- Reducing the dimension of the lattice
- Reducing the value of $\delta_0 = (\frac{\|\mathbf{w}\|}{det^{\frac{1}{n}}(\Lambda)})^{\frac{1}{n}}$
- Reducing the number of the lattice vectors shorter than the target vector

2. Previous works

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

target vector:

$$\mathbf{w} = (0, k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

Optimization methods

- Eliminating the secret key α
- Merging the elements k_{ij}'s
- Recovering/Enumerating the MSD

⇩

Effectively reduce the dimension of the lattice

[FWC16] Fan, S., Wang, W., Cheng, Q.: Attacking openssl implementation of ECDSA with a few signatures. In: CCS. pp. 1505 – 1515. ACM (2016)

2. Previous works

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

target vector:

$$\mathbf{w} = (0, k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

Optimization methods

- Selecting signatures with a certain feature (Reducing $\|\mathbf{w}\|$)
- Attackers can recover the secret even if there is a small amount of erroneous information

[MPP20] Micheli, G.D., Piau, R., Pierrot, C.: A tale of three signatures: Practical attack of ECDSA with wnaf. In: AFRICACRYPT. Lecture Notes in Computer Science, vol. 12174, pp. 361 – 381. Springer (2020)

2. Previous works

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

target vector:

$$\mathbf{w} = (0, k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

Problems

- The $N-1$ zeros in the target vector $\mathbf{w}$ increase the dimension of the lattice, however, they can't be used to recover α
- The information of k_{ij}'s isn't fully utilized, which makes the value of $\mathbf{w}_i^2$ (e.g., $\mathbf{w}_1 = k_{00}+\beta_1$) not small enough

3. Our improvement

Reducing the dimension of the lattice ($N-1$)

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

target vector:

$$\mathbf{w} = (0, k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

$$r_1 s_0 (k_{00} + 2^{l_0} k_{01}) - r_0 s_1 (k_{10} + 2^{l_1} k_{11}) + \beta + hq = 0$$

$$k_{00} = a k_{01} + b k_{10} + c k_{11} + d + eq$$

$$\mathbf{w} = (e, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & \\ a & 1 & & & \\ b & 0 & 1 & & \\ c & 0 & 0 & 1 & \\ d+\beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

$$= (k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

3. Our improvement

Reducing the length $\|\mathbf{w}\|$ of the target vector

$$\mathbf{w} = (e, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & \\ a & 1 & & & \\ b & 0 & 1 & & \\ c & 0 & 0 & 1 & \\ d+\beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

$$= (k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

$$S_p = x_0 + 2^4 \cdot x_1 + \cdot + 2^{4p} \cdot x_p, x_p \in \{0,1,2,3,4,5,6,7\}$$

For $k_{00} \in S_p \in [0, 7 \cdot 2^{4p}]$, [CCS16] chose $\beta_1 = -4 \cdot 2^{4p}$ to balance k_{00}

β_1 is only related to the information of x_p and doesn't balance x_p

Therefore, β_i can't minimize $E(\|\mathbf{w}\|^2)$

3. Our improvement

A simple example of minimizing $E(\|\mathbf{w}\|)^2 = E(\sum_i \mathbf{w}_i^2)$

For $\mathbf{w}_1 = k_{00} + \beta_1$, assuming that $k_{00} \in S = \{1,3,5,7,11,15\}$, we provide a method to minimize the mean of $\mathbf{w}_1^2$ by the following two steps:

- substituting k_{00} with the integer $k'_{00} = \frac{k_{00}-1}{d} \in \{0,1,2,3,5,7\}$, where $d = gcd(3-1,\cdots,15-11)$

- Setting $\beta_1 = -E(k'_{00}) = -3$ to recenter $\mathbf{w}_1$

the new $\mathbf{w}_1 \in \{-3,-2,-1,2,4\}$

3. Our improvement

Adjusting the method of merging in [FWC16]

$$(h, k_{00}, k_{01}, k_{10}, k_{11}, 1)\begin{pmatrix} q & & & & & \\ r_1 s_0 & 1 & & & & \\ 2^{l_0} r_1 s_0 & 0 & 1 & & & \\ -r_0 s_1 & 0 & 0 & 1 & & \\ -2^{l_1} r_0 s_1 & 0 & 0 & 0 & 1 & \\ \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 & 1 \end{pmatrix}$$

$$= (0, k_{00}+\beta_1, k_{01}+\beta_2, k_{10}+\beta_3, k_{11}+\beta_4, 1)$$

$$(h, k_{00}+2^{l_0}k_{01}, k_{10}+2^{l_1}k_{11}, 1)\begin{pmatrix} q & & & \\ r_1 s_0 & 1 & & \\ -r_0 s_1 & 0 & 1 & \\ \beta & \beta'_1 & \beta'_2 & 1 \end{pmatrix}$$

$$= (0, k_{00}+2^{l_0}k_{01}+\beta'_1, k_{10}+2^{l_1}k_{11}+\beta'_2, 1)$$

Merging decreases the dimension of the lattice, but increase the length of the target vector

By adjusting the number of merged $k_{i,j}$'s, we improve the success probability

3. Our improvement

Attack	N	Technique-1	Technique-2	block	probability
[7]	4	Yes	No	25	8%
[7] + our techniques	3	Yes	No	35	0.2%
[14]	4	No	No	35	4%
[14] + our techniques	4	No	No	35	14.6%
[14]	3	No	Yes	35	0.2%
[14] + our techniques	3	No	Yes	35	4.1%

[7]: [FWC16], [14]: [MPP20]

"Technique-1": the techniques (MSD recovering and enumer- ation) introduced in [7]

"Technique-2": the technique of selecting the signatures with a certain feature introduced in [14].

"block": the important parameter determining the time complexity of lattice reduction algorithms for a given lattice basis

THANKS !!!