Lattice Attacks against Elliptic-Curve Signatures with Blinded Scalar Multiplication

Dahmun Goudarzi, Matthieu Rivain, Damien Vergnaud

SAC 2016, 12 Aug, St. Johns

ENS

CryptoExperts

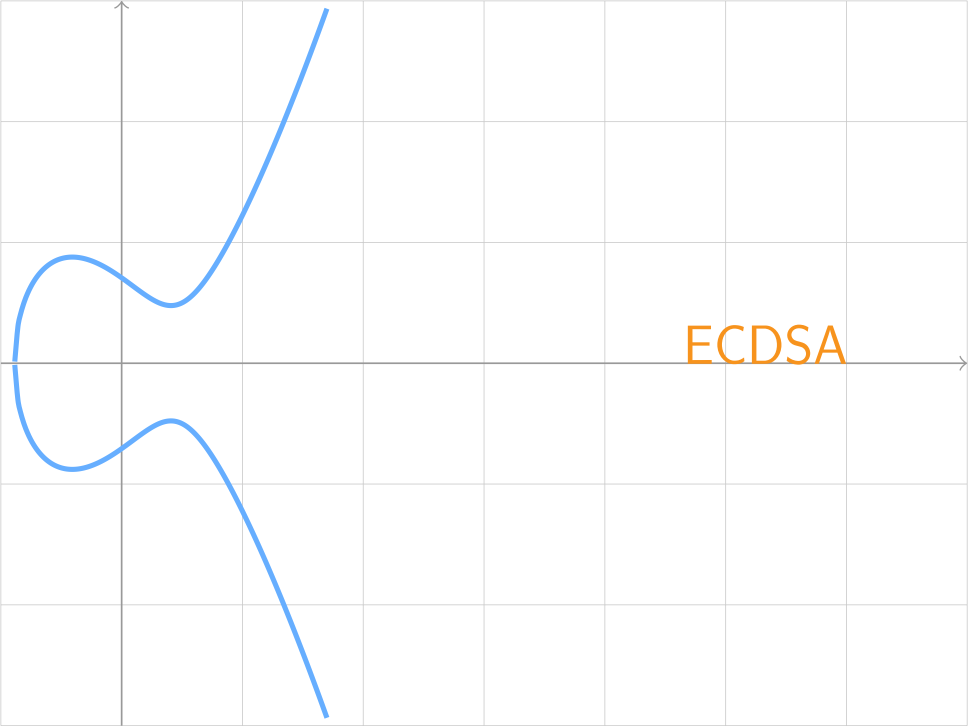
Outline

- EC signature schemes based on random nonces
  - σ computed from $[k]\boldsymbol{P}$, $k \leftarrow \$$
  - $\sigma + k \Rightarrow$ secret key
  - lattice attack: few bits of several $k_i \Rightarrow$ secret key
- Scenario:
  - implementation with countermeasures against SCA
  - blinding of the nonce
  - noisy side-channel leakage on the bits of the blinded nonce
- Issue: **noisy information** on **blinded** nonces $\Rightarrow$ lattice attack

Outline

- Approach:
  - template attack $\Rightarrow$ probability scores
  - probability scores $\Rightarrow$ bit-selection algorithm
  - selected bits $\Rightarrow$ lattice attack
  - dealing with blinding

- Presentation:
  - ECDSA
  - target implementation & leakage model
  - Howgrave-Graham and Smart lattice attack
  - bit selection
  - experimental results


ECDSA

- Key pair $(x, \boldsymbol{Q})$ with $\boldsymbol{Q} = [x]\boldsymbol{P} \in E(\mathbb{K})$

- Key pair $(x, \boldsymbol{Q})$ with $\boldsymbol{Q} = [x]\boldsymbol{P} \in E(\mathbb{K})$
- Signature of $h = H(m)$

$$k \xleftarrow{\$} [1; q] \quad (q = |E(\mathbb{K})|)$$

$$t = \mathsf{xcoord}([k]\boldsymbol{P})$$

$$s = \frac{h + t \cdot x}{k} \pmod{q}$$

- Key pair $(x, \boldsymbol{Q})$ with $\boldsymbol{Q} = [x]\boldsymbol{P} \in E(\mathbb{K})$
- Signature of $h = H(m)$

$$k \xleftarrow{\$} [1; q] \quad (q = |E(\mathbb{K})|) \qquad \Rightarrow \text{random nonce } k$$

$$t = \mathsf{xcoord}([k]\boldsymbol{P})$$

$$s = \frac{h + t \cdot x}{k} \pmod q \qquad \Rightarrow \text{signature } \sigma = (t, s)$$

- Key pair $(x, \boldsymbol{Q})$ with $\boldsymbol{Q} = [x]\boldsymbol{P} \in E(\mathbb{K})$
- Signature of $h = H(m)$

$$k \overset{\$}{\leftarrow} [1; q] \quad (q = |E(\mathbb{K})|) \qquad \Rightarrow \text{random nonce } k$$

$$t = \text{xcoord}([k]\boldsymbol{P})$$

$$s = \frac{h + t \cdot x}{k} \pmod q \qquad \Rightarrow \text{signature } \sigma = (t, s)$$

- Verification of $\sigma = (t, s)$

$$k = \frac{h + t \cdot x}{s}$$

- Key pair $(x, \boldsymbol{Q})$ with $\boldsymbol{Q} = [x]\boldsymbol{P} \in E(\mathbb{K})$
- Signature of $h = H(m)$

$$k \xleftarrow{\$} [1; q] \quad (q = |E(\mathbb{K})|) \qquad \Rightarrow \text{random nonce } k$$

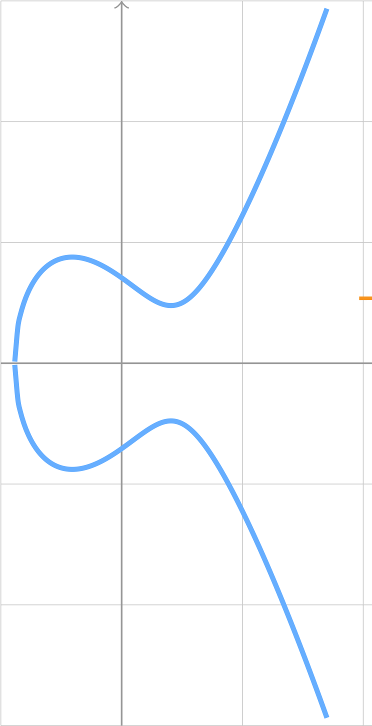
$$t = \text{xcoord}([k]\boldsymbol{P})$$

$$s = \frac{h + t \cdot x}{k} \pmod q \qquad \Rightarrow \text{signature } \sigma = (t, s)$$

- Verification of $\sigma = (t, s)$

$$k = \frac{h + t \cdot x}{s}$$

$$\underbrace{[k]\boldsymbol{P}}_{t} \stackrel{?}{=} \left[\frac{h}{s}\right]\boldsymbol{P} + \underbrace{\left[\frac{t \cdot x}{s}\right]\boldsymbol{P}}_{\left[\frac{t}{s}\right]\boldsymbol{Q}}$$



Target implementation and leakage model

Target implementation

- Regular binary algorithm (*e.g.* Montgomery ladder)
- Classical side-channel countermeasures:
  - randomization of point coordinates
  - scalar blinding

Classic blinding:

1. $r \xleftarrow{\$} [\![0, 2^\lambda - 1]\!]$
2. $a \leftarrow k + r \cdot q$
3. return $[a]\boldsymbol{P}$

Euclidean blinding:

1. $r \xleftarrow{\$} [\![1, 2^\lambda - 1]\!]$
2. $a \leftarrow \lfloor k/r \rfloor$; $b \leftarrow k \bmod r$
3. return $[r]([a]\boldsymbol{P}) + [b]\boldsymbol{P}$

Leakage model

Algorithm 1 Montgomery ladder

Input: blinded nonce a

Output: $[a]\boldsymbol{P}$

1. $\boldsymbol{P}_0 \leftarrow \mathcal{O}$; $\boldsymbol{P}_1 \leftarrow \boldsymbol{P}$
2. **for** $i = \ell - 1$ **downto** 0 **do**
3. $\quad \boldsymbol{P}_{1-a_i} \leftarrow \boldsymbol{P}_{1-a_i} + \boldsymbol{P}_{a_i}$
4. $\quad \boldsymbol{P}_{a_i} \leftarrow 2\boldsymbol{P}_{a_i}$
5. **end for**
6. **return** $\boldsymbol{P}_0$

- Loop iteration: $(\boldsymbol{P}_0, \boldsymbol{P}_1) \leftarrow f(a_i, \boldsymbol{P}_0, \boldsymbol{P}_1)$

  $\Rightarrow$ leaks $\Psi(a_i, \boldsymbol{P}_0, \boldsymbol{P}_1)$

- Gaussian leakage assumption:

$$\Psi(a_i, \boldsymbol{P}_0, \boldsymbol{P}_1) \sim \mathcal{N}(m_{a_i}, \Sigma)$$

Template attacker

- Get a side-channel trace $(\psi_{\ell-1}, \ldots, \psi_1, \psi_0)$
- For every i, use leakage templates to decide

$$\psi_i \sim \Psi(0) \quad \text{or} \quad \psi_i \sim \Psi(1)$$

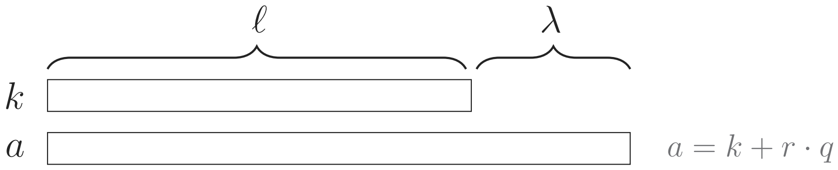
- Maximum likelihood

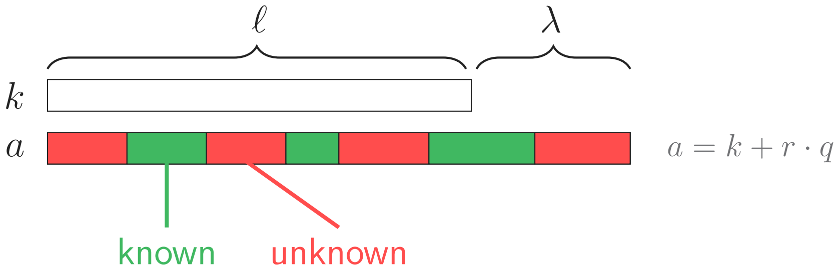
$$\Pr[a_i = 0 \mid \psi_i] = cst \cdot \exp\big(-\tfrac{1}{2}(\psi_i - m_0)^{\mathsf{t}} \cdot \Sigma^{-1} \cdot (\psi_i - m_0)\big)$$
$$\Pr[a_i = 1 \mid \psi_i] = cst \cdot \exp\big(-\tfrac{1}{2}(\psi_i - m_1)^{\mathsf{t}} \cdot \Sigma^{-1} \cdot (\psi_i - m_1)\big)$$

- We get $\Pr[a_i = 0 \mid \psi_i] \sim \mathcal{D}_\theta(a_i)$ with

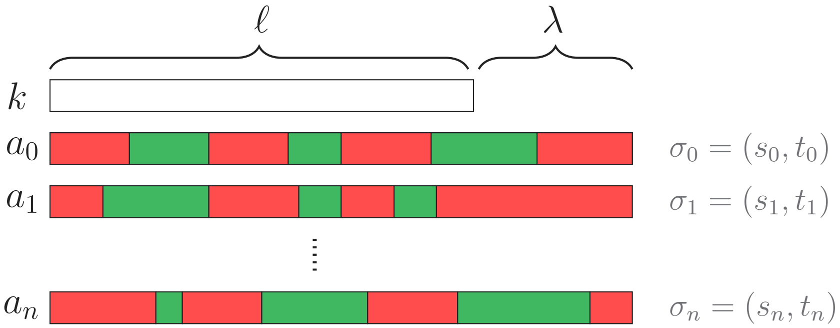
$$\underbrace{\theta = \Lambda \cdot (m_0 - m_1)}_{\text{multivariate SNR}} \quad \text{where} \quad \Lambda^{\mathsf{t}}\Lambda = \Sigma$$

Howgrave-Graham and Smart attack with blinded nonces

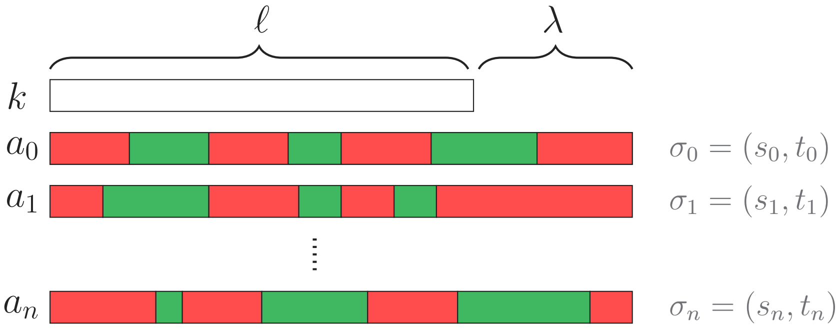

ℓ
λ
k
a
a = k + r · q



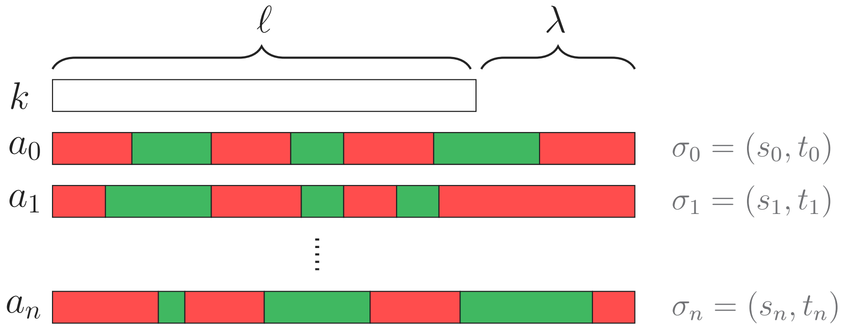
ℓ
λ
k
a
$a = k + r \cdot q$
known
unknown



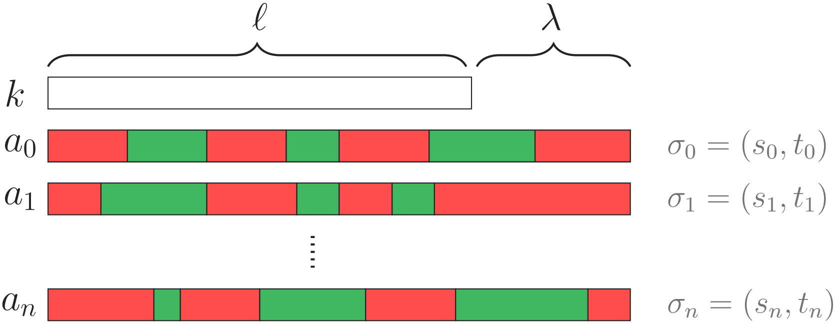
ℓ
λ
k
a_0
a_1
a_n
$\sigma_0 = (s_0, t_0)$
$\sigma_1 = (s_1, t_1)$
$\sigma_n = (s_n, t_n)$



$$x \equiv \frac{a_i \cdot s_i - h_i}{t_i} \pmod{q}$$

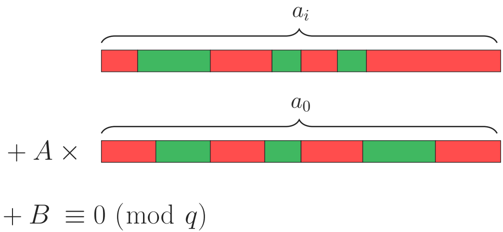


$$x \equiv \frac{a_i \cdot s_i - h_i}{t_i} \equiv \frac{a_0 \cdot s_0 - h_0}{t_0} \pmod{q}$$

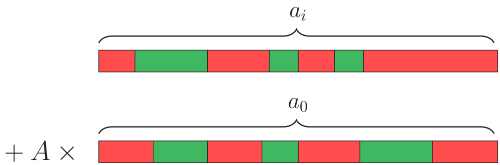


$$x \equiv \frac{a_i \cdot s_i - h_i}{t_i} \equiv \frac{a_0 \cdot s_0 - h_0}{t_0} \pmod{q}$$

$$\Leftrightarrow \quad a_i + A\, a_0 + B \equiv 0 \pmod{q}$$



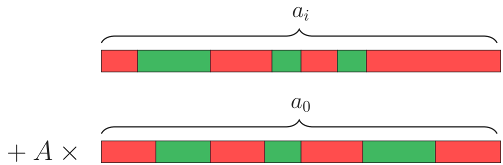
a_i
a_0
$+ A \times$
$+ B \equiv 0 \pmod{q}$



$$+ B \equiv 0 \pmod{q}$$

$$\Longleftrightarrow$$

$$x_{i,1} + \boldsymbol{\alpha_{i,2}} \cdot x_{i,2} + \boldsymbol{\alpha_{i,3}} \cdot x_{i,3} + \cdots$$
$$+ \boldsymbol{\beta_{i,1}} \cdot x_{0,1} + \boldsymbol{\beta_{i,2}} \cdot x_{0,2} + \boldsymbol{\beta_{i,3}} \cdot x_{0,3} + \cdots$$
$$+ \boldsymbol{\gamma_i} \equiv 0 \pmod{q}$$



$$+ B \equiv 0 \pmod{q}$$

$$\Leftrightarrow$$

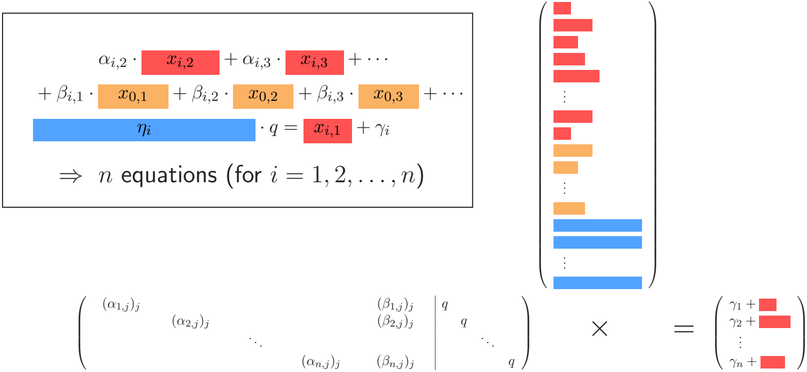
$$x_{i,1} + \boldsymbol{\alpha_{i,2}} \cdot x_{i,2} + \boldsymbol{\alpha_{i,3}} \cdot x_{i,3} + \cdots$$
$$+ \boldsymbol{\beta_{i,1}} \cdot x_{0,1} + \boldsymbol{\beta_{i,2}} \cdot x_{0,2} + \boldsymbol{\beta_{i,3}} \cdot x_{0,3} + \cdots$$
$$+ \boldsymbol{\gamma_i} = \eta_i \cdot q$$

$$x_{i,1} + \alpha_{i,2} \cdot x_{i,2} + \alpha_{i,3} \cdot x_{i,3} + \cdots$$
$$+ \beta_{i,1} \cdot x_{0,1} + \beta_{i,2} \cdot x_{0,2} + \beta_{i,3} \cdot x_{0,3} + \cdots$$
$$+ \gamma_i = \eta_i \cdot q$$

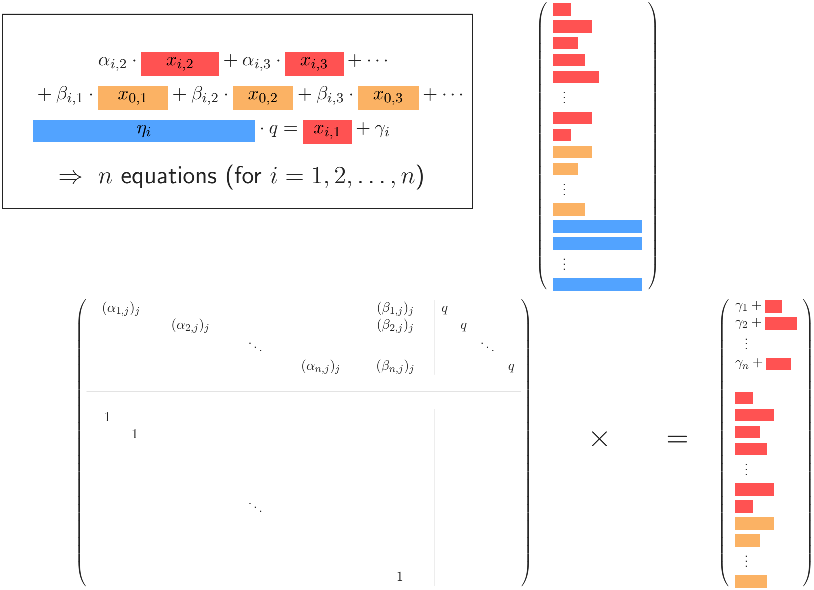
$\Rightarrow$ n equations (for $i = 1, 2, \ldots, n$)

$$
\begin{aligned}
&\alpha_{i,2} \cdot x_{i,2} + \alpha_{i,3} \cdot x_{i,3} + \cdots \\
&+ \beta_{i,1} \cdot x_{0,1} + \beta_{i,2} \cdot x_{0,2} + \beta_{i,3} \cdot x_{0,3} + \cdots \\
&\eta_i \cdot q = x_{i,1} + \gamma_i
\end{aligned}
$$

$\Rightarrow$ n equations (for $i = 1, 2, \ldots, n$)



$\alpha_{i,2} \cdot x_{i,2} + \alpha_{i,3} \cdot x_{i,3} + \cdots$
$+ \beta_{i,1} \cdot x_{0,1} + \beta_{i,2} \cdot x_{0,2} + \beta_{i,3} \cdot x_{0,3} + \cdots$
$\eta_i \cdot q = x_{i,1} + \gamma_i$
$\Rightarrow$ n equations (for $i = 1, 2, \ldots, n$)
$(\alpha_{1,j})_j$
$(\alpha_{2,j})_j$
$(\alpha_{n,j})_j$
$(\beta_{1,j})_j$
$(\beta_{2,j})_j$
$(\beta_{n,j})_j$
q
$\times$
$=$
$\gamma_1 +$
$\gamma_2 +$
$\gamma_n +$



$\alpha_{i,2} \cdot x_{i,2} + \alpha_{i,3} \cdot x_{i,3} + \cdots$
$+ \beta_{i,1} \cdot x_{0,1} + \beta_{i,2} \cdot x_{0,2} + \beta_{i,3} \cdot x_{0,3} + \cdots$
$\eta_i \cdot q = x_{i,1} + \gamma_i$
$\Rightarrow$ n equations (for $i = 1, 2, \ldots, n$)
$(\alpha_{1,j})_j$
$(\alpha_{2,j})_j$
$(\alpha_{n,j})_j$
$(\beta_{1,j})_j$
$(\beta_{2,j})_j$
$(\beta_{n,j})_j$
q
1
$\times$
$=$
$\gamma_1 +$
$\gamma_2 +$
$\gamma_n +$

Lattice problem

- There exists $\boldsymbol{y}$ st:

$$M \cdot \boldsymbol{y} = \boldsymbol{v} + \boldsymbol{x}$$

where

$$\boldsymbol{v} = (\gamma_1, \gamma_2, \ldots, \gamma_n, 0, 0, \cdots, 0)$$

$\boldsymbol{x}$ is the vector of unknown blocks

- CVP (Closest Vector Problem): $\boldsymbol{v} \Rightarrow (\boldsymbol{v} + \boldsymbol{x})$

$$\underbrace{\|(\boldsymbol{v} + \boldsymbol{x}) - \boldsymbol{v}\|}_{\|\boldsymbol{x}\|} \leq c_0 \sqrt{\dim(M)}\, \det(M)^{\frac{1}{\dim(M)}}$$

$c_0 \approx 1/\sqrt{2\pi \mathrm{e}}$ (heuristic)

Lattice attack parameters

- Sum of contributions:

$$\sum_{i=0}^{n}(\delta_i - \lambda - c_1 \cdot N_i) \geq \ell$$

where $\delta_i =$ number of known bits in a_i

$N_i =$ number of unknown blocks in a_i

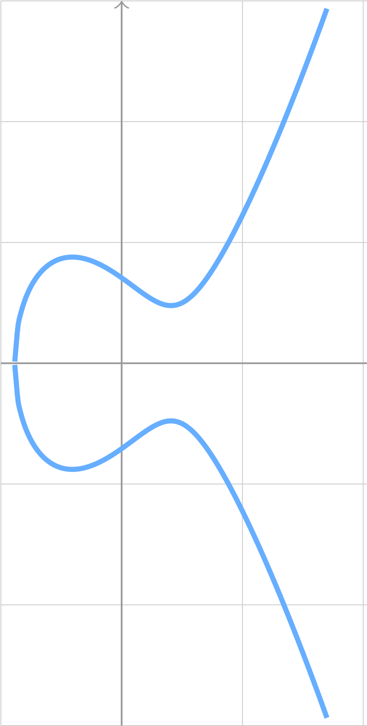
- Loss λ bits per blinded nonce
- Linear term $c_1 \cdot N_i$
  - overlooked in the original paper
  - significant in our context
  - heuristically $c_1 \approx -\log_2(c_0) \approx 2.05$
  - higher in practice

Experiments

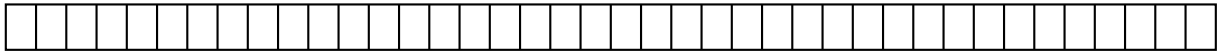
Practical c_1 values for a 95% success rate:

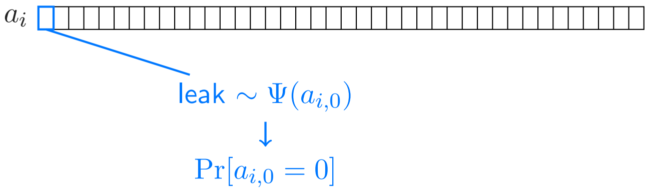
	$(n+1)=5$				$(n+1)=10$				$(n+1)=20$		
$N_b =$	5	10	25	50	10	20	50	100	20	40	100
$\lambda = 0$	3.60	2.60	2.56	2.90	4.10	3.30	3.52	3.57	4.85	4.42	4.51
$\lambda = 16$	3.40	2.60	2.40	3.02	4.20	3.15	3.40	4.20	5.25	4.77	4.96
$\lambda = 32$	3.40	2.60	2.60	2.68	3.90	3.10	3.60	n/a	4.95	4.50	n/a
$\lambda = 64$	3.20	2.80	2.36	n/a	3.70	3.55	3.68	n/a	4.80	4.60	n/a

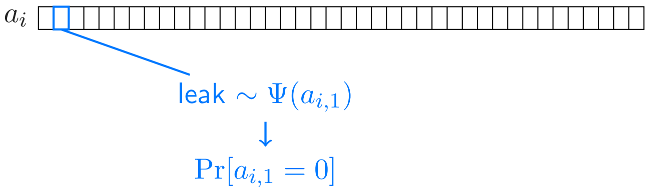
- CVP algorithm: the embedding method
- For tested parameters: $2.3 < c_1 < 5.3$



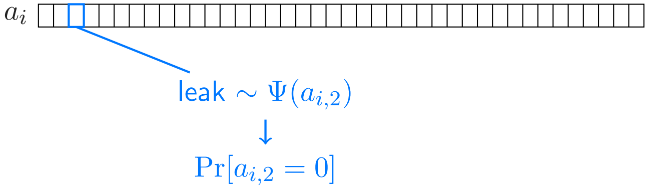
Attack on leaking implementations

a_i 

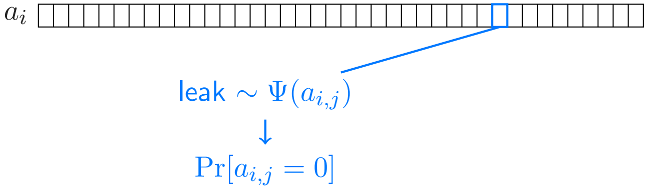

a_i
leak $\sim \Psi(a_{i,0})$
$\Pr[a_{i,0} = 0]$

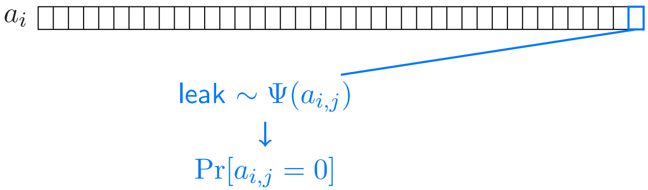


a_i
leak $\sim \Psi(a_{i,1})$
$\Pr[a_{i,1} = 0]$

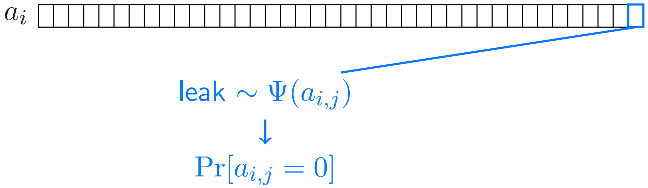


a_i
leak $\sim \Psi(a_{i,2})$
$\Pr[a_{i,2} = 0]$


a_i
leak $\sim \Psi(a_{i,j})$
$\Pr[a_{i,j} = 0]$



a_i
leak $\sim \Psi(a_{i,j})$
↓
$\Pr[a_{i,j} = 0]$



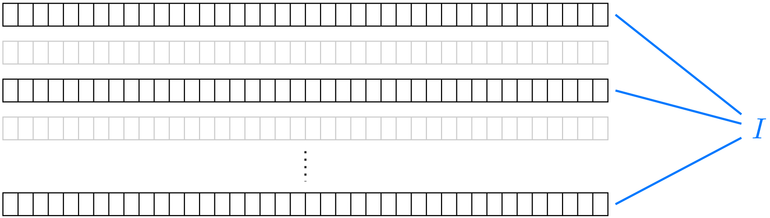
- Guess

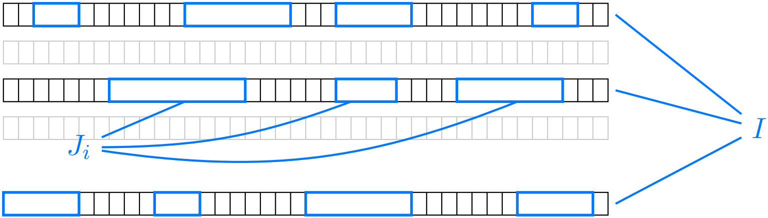
$$\hat{a}_{i,j} = \operatorname*{argmax}_{b \in \{0,1\}} \Pr[a_{i,j} = b]$$

- Good-guess probability

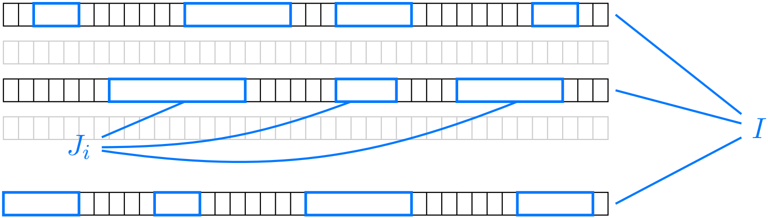
$$p_{i,j} := \Pr[a_{i,j} = \hat{a}_{i,j}] = \max_{b \in \{0,1\}} \Pr[a_{i,j} = b]$$

- Select some guess bits to construct the lattice


I



J_i
I



- Goal: select I and $(J_i)_{i \in I}$ to maximize

$$\text{success proba} = \prod_{i \in I} \prod_{j \in J_i} p_{i,j}$$

such that

$$\underbrace{\sum_{i \in I} (|J_i| - \lambda - c_1 \cdot N_i) \geq \ell}_{\text{CVP constraint}} \quad \text{and} \quad \underbrace{\sum_{i \in I} N_i \leq \Delta_{max}}_{\text{lattice dimension}}$$

- For each selected set J_i

  CVP constraint **+=** $|J_i| - \lambda - c_1 \cdot N_i$ (must reach ℓ)

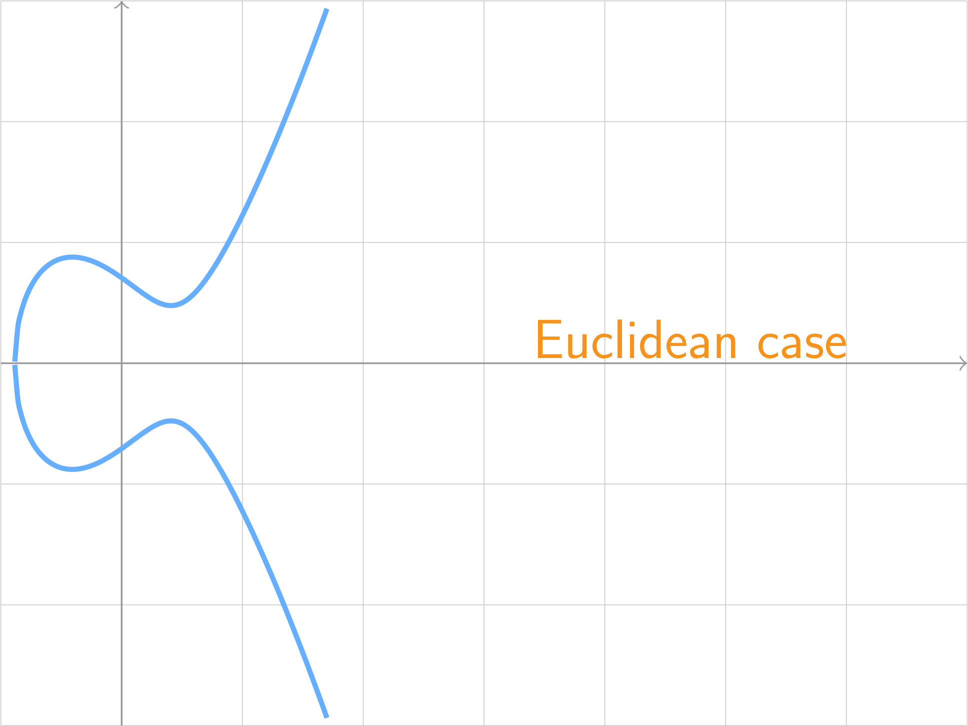
  $\dim(\mathcal{L})$ **+=** N_i (must not exceed Δ_{max})

  success proba $\times$**=** $\prod_{j \in J_i} p_{i,j}$

- Select J_i to maximize

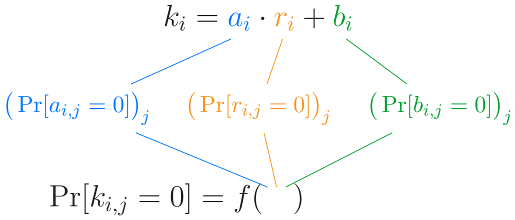
$$\gamma_i = \Big(\prod_{j \in J_i} p_{i,j} \Big)^{\frac{1}{|J_i| - \lambda - c_1 N_i}}$$

- Efficient algorithm based on dynamic programming


Euclidean case

$$k_i = a_i \cdot r_i + b_i$$

$$\big(\Pr[a_{i,j} = 0]\big)_j \qquad \big(\Pr[r_{i,j} = 0]\big)_j \qquad \big(\Pr[b_{i,j} = 0]\big)_j$$

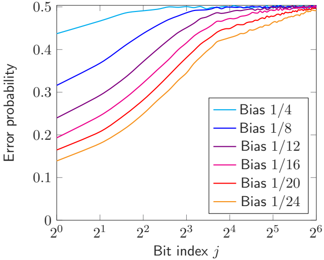

$k_i = a_i \cdot r_i + b_i$
$\left(\Pr[a_{i,j} = 0]\right)_j$
$\left(\Pr[r_{i,j} = 0]\right)_j$
$\left(\Pr[b_{i,j} = 0]\right)_j$
$\Pr[k_{i,j} = 0] = f(\quad)$

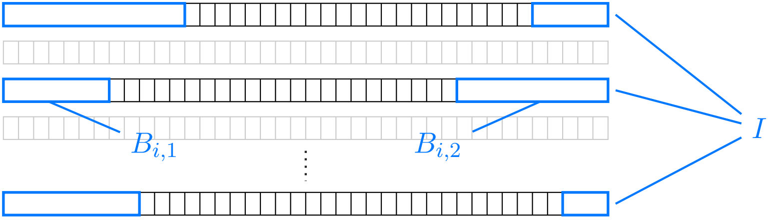
$$k_i = a_i \cdot r_i + b_i$$

$$\big(\Pr[a_{i,j} = 0]\big)_j \quad \big(\Pr[r_{i,j} = 0]\big)_j \quad \big(\Pr[b_{i,j} = 0]\big)_j$$

$$\Pr[k_{i,j} = 0] = f(\quad)$$

- Bias decreases exponentially as $j \to \frac{\ell}{2}$





$$\Rightarrow \quad |J_i| = |B_{i,1}| + |B_{i,2}| \qquad N_i = 1 \qquad \lambda = 0$$

$$\sum_{i \in I} (|J_i| - \lambda - c_1 \cdot N_i) \geq \ell \qquad \sum_{i \in I} N_i \leq \Delta_{max}$$

$$\Rightarrow \sum_{i \in I} (|B_{1,i}| + |B_{2,i}| - c_1) \geq \ell \qquad \Rightarrow |I| \leq \Delta_{max}$$

- Block probabilities

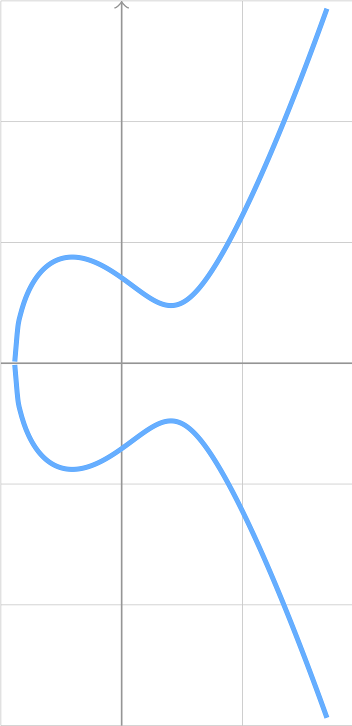
$$\begin{aligned}&\Pr[B_{i,j} = x] \\ &\quad = f\Big(\big(\Pr[a_{i,j} = 0]\big)_j ; \big(\Pr[r_{i,j} = 0]\big)_j ; \big(\Pr[b_{i,j} = 0]\big)_j ; x\Big)\end{aligned}$$

- Block guesses

$$\begin{aligned}\hat{B}_{i,j} &= \operatorname*{argmax}_x \Pr[B_{i,j} = x] \\ \Pr[B_{i,j} = \hat{B}_{i,j}] &= \max_x \Pr[B_{i,j} = x]\end{aligned}$$

- Select blocks maximizing

$$\gamma_i = \Big(\Pr[\hat{B}_{i,1} = B_{i,1}] \cdot \Pr[\hat{B}_{i,2} = B_{i,2}]\Big)^{\frac{1}{|B_{1,i}|+|B_{2,i}|-c_1}}$$



Experimental results

Experimental setting

- ANSSI 256-bit elliptic curve (*i.e.* $\ell = 256$)
- Three different random sizes $\lambda \in \{16, 32, 64\}$
- Probability scores simulated using $\mathcal{D}_\theta(\cdot)$ with

$$\theta = \alpha \cdot (0.5, 1, 2)$$

  with $\alpha \in \{1.5,\ 2\}$
- Attack parameters
  - n_{sig} signatures (with leaking blinded nonces)
  - n_{tr} trials for the subset I

$$(n_{sig}, n_{tr}) \in \{(10,1),(20,5),(20,10),(100,10),(100,50),(100,100)\}$$

  - Linear factor c_1 set to 4

Experimental results

(n_{sig}, n_{tr})		(10,1)	(20, 5)	(20, 10)	(100, 10)	(100, 50)	(100, 100)
Classic blinding							
$\alpha = 1.5$	$\lambda = 16$	13.5 %	38.3 %	54.0 %	70.1 %	99.0 %	99.9 %
	$\lambda = 32$	3.5 %	13.6 %	22.7 %	27.8 %	73.9 %	91.9 %
	$\lambda = 64$	0.2 %	0.6 %	1.2 %	1.5 %	6.2 %	11.7 %
$\alpha = 2$	$\lambda = 16$	91.2 %	99.9 %	100 %	100 %	100 %	100 %
	$\lambda = 32$	90.5 %	99.5 %				
	$\lambda = 64$	85.7 %	99.3 %				
Euclidean blinding							
$\alpha = 1.5$	$\lambda = 16$	0 %	0 %	0 %	0 %	0 %	0 %
	$\lambda = 32$						
	$\lambda = 64$						
$\alpha = 2$	$\lambda = 16$	0.7 %	3.1 %	5.8 %	42.8 %	76.8 %	83.3 %
	$\lambda = 32$	0.1 %	0.4 %	0.8 %	41.1 %	74.9 %	82.6 %
	$\lambda = 64$	0.1 %	0.4 %	1.0 %	40.2 %	75.0 %	82.8 %

- Lattice reduction (almost) always works (for correct guesses)
  $\Rightarrow$ sound choice for c_1
- λ has small impact for Euclidean blinding
- Classic blinding more sensitive to our attack than Euclidean blinding