MUNI
FI

CROCS
Centre for Research on
Cryptography and Security

Jan Jancar
Vladimir Sedlacek
Petr Svenda
Marek Sys

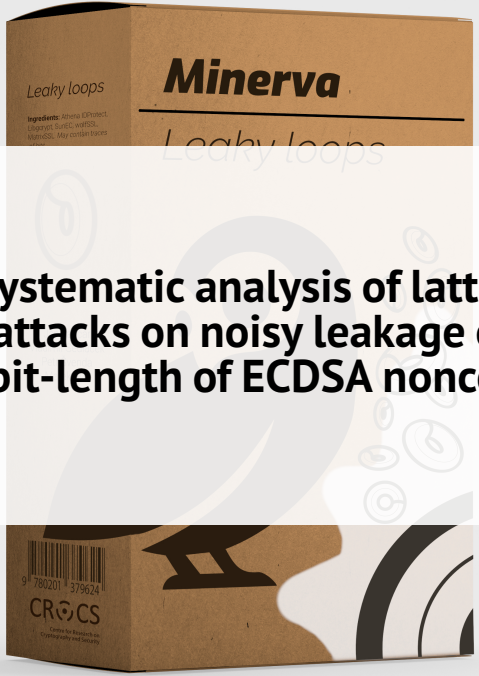
CHES
2020

MUNI FI

CROCS
Centre for Research on Cryptography and Security

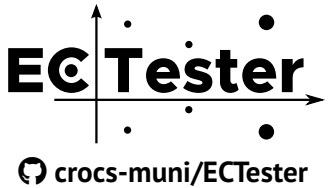
Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces

Jan Jancar
Vladimir Sedlacek
Petr Svenda
Marek Sys



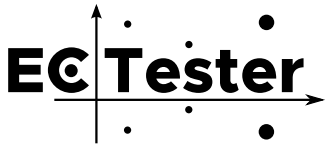
CHES 2020

Discovery



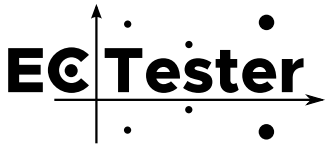
- Tool for testing black-box ECC implementations
  - JavaCards
  - Software libraries (15 supported)

Discovery



- Tool for testing black-box ECC implementations
  - JavaCards
  - Software libraries (15 supported)
- 12 test suites (invalid curve attacks, …)

Discovery



- Tool for testing black-box ECC implementations
  - JavaCards
  - Software libraries (15 supported)
- 12 test suites (invalid curve attacks, …)
- Decided to test timing of **ECDH** and **ECDSA**!

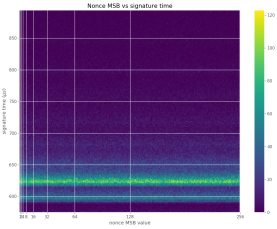
ECDSA

Sign(message m, private key x)

1. $k \xleftarrow{\$} \mathbb{Z}_n$ (nonce)
2. $r \equiv ([k]G)_x \mod n$
3. $s \equiv k^{-1}(H(m) + rx) \mod n$
4. Output (r, s)

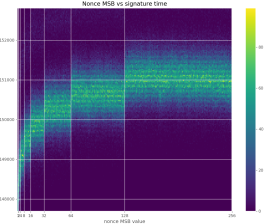
Leakage

t

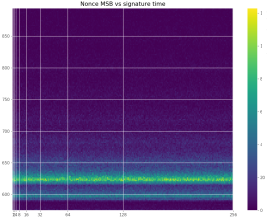

Nonce MSB vs signature time
signature time (µs)
nonce MSB value
MSB(k)

Leakage

Athena IDProtect



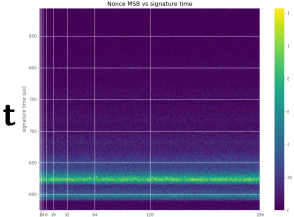
t



MSB(k)

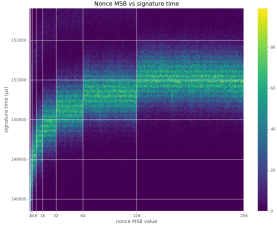
Leakage

Athena IDProtect

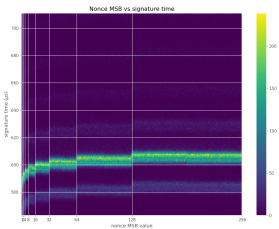


t

MSB(k)

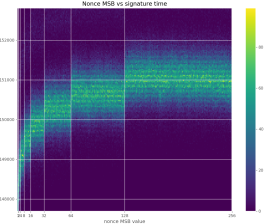


SunEC/Java

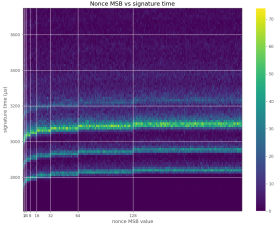


Leakage

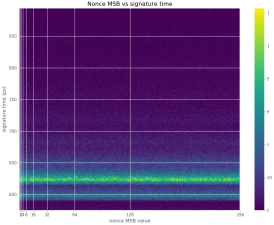
Athena IDProtect



libgcrypt

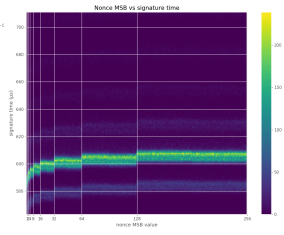


t



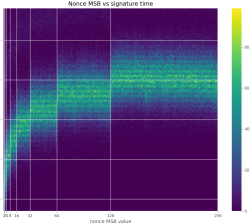
MSB(k)

SunEC/Java

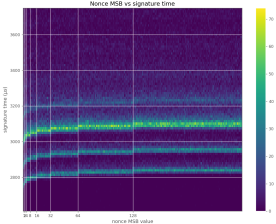


Leakage

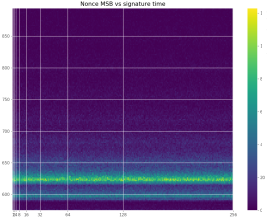
Athena IDProtect



libgcrypt

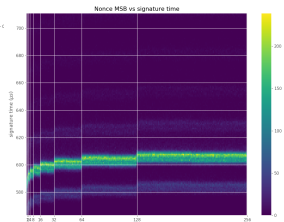


t

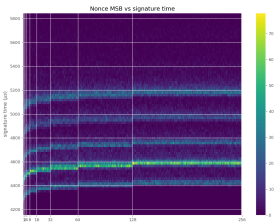


MSB(k)

SunEC/Java

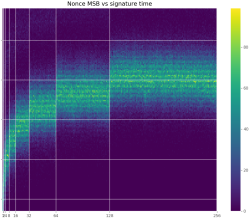


MatrixSSL

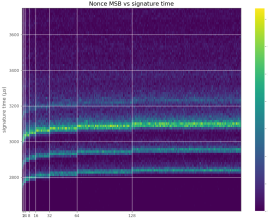


Leakage

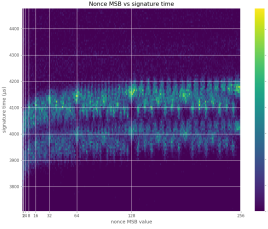
Athena IDProtect



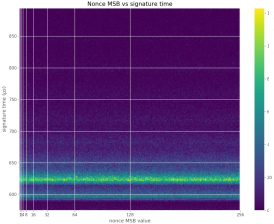
libgcrypt



Crypto++

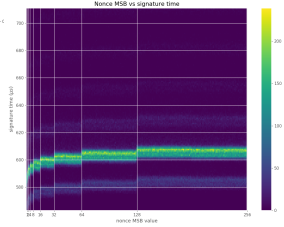


t

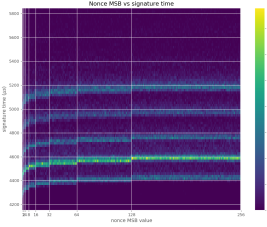


MSB(k)

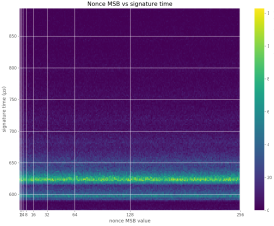
SunEC/Java



MatrixSSL



Leakage



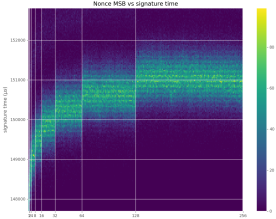
t

MSB(k)

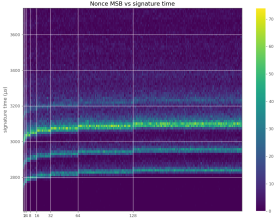
FIPS VALIDATED 140-2 ™

Common Criteria

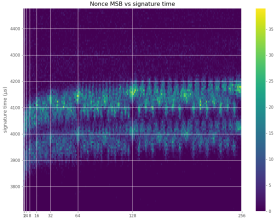
Athena IDProtect



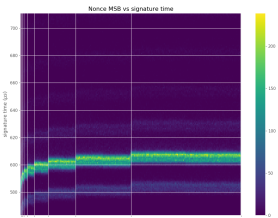
libgcrypt



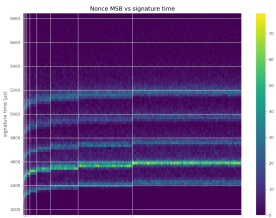
Crypto++



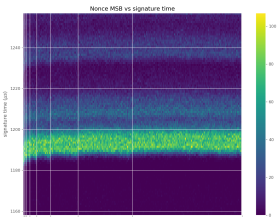
SunEC/Java



MatrixSSL

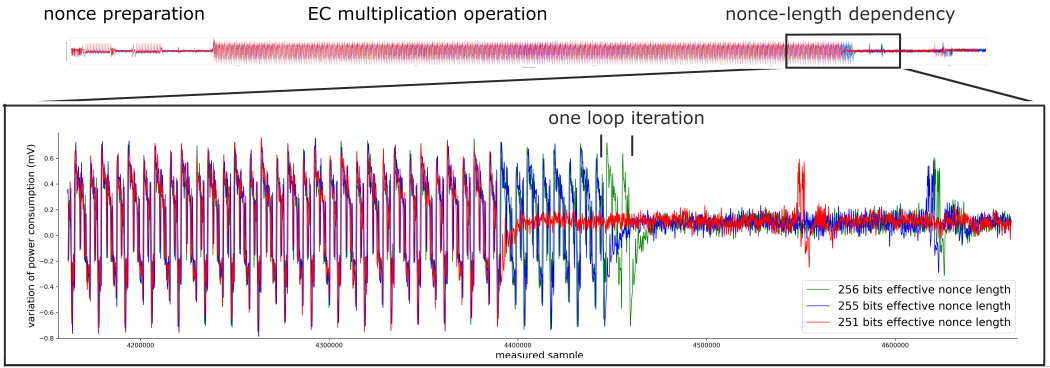


WolfSSL



Leakage

[k]G


nonce preparation
EC multiplication operation
nonce-length dependency
one loop iteration
variation of power consumption (mV)
measured sample
256 bits effective nonce length
255 bits effective nonce length
251 bits effective nonce length

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP
- Get the key!

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i **How?**
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP
- Get the key!

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i **How?**
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP **Which?**
- Get the key!

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i **How?**
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP **Which?**
- Get the key!

Recentering?

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i **How?**
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP **Which?**
- Get the key!

Recentering?

Nonce differences?

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i **How?**
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP **Which?**
- Get the key!

Recentering?

Nonce differences?

Random subsets?

Exploitation

Noisy bit-length of $k \rightarrow$ HNP [1] $\rightarrow$ CVP or SVP $\rightarrow$ private key

- Collect N signatures, take d fastest
- Assume bounds l_i **How?**
- Form inequalities $|k_i| = |t_i x - u_i| < n/2^{l_i}$
- Construct HNP lattice and target vector
- Solve via CVP/SVP **Which?**
- Get the key!

Recentering?

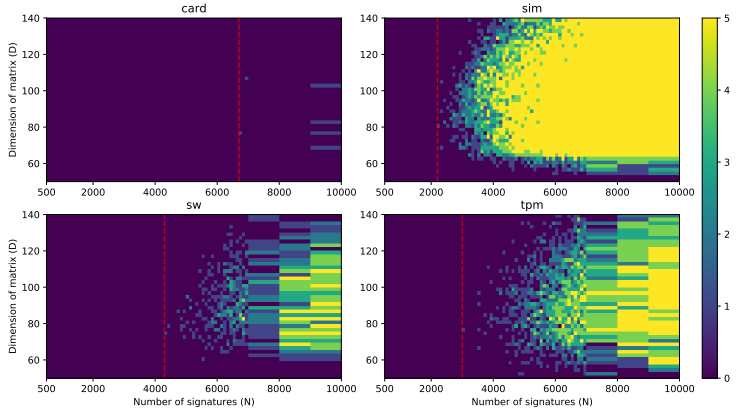
Nonce differences?

Random subsets?

u-bitflips?

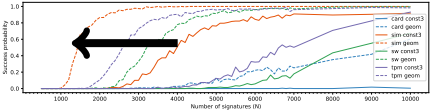
Analysis

- 4 datasets of signatures, varying noise, `secp256r1` curve
- Run attack 5 times for grid of (N, d)



#Successes
(out of 5)

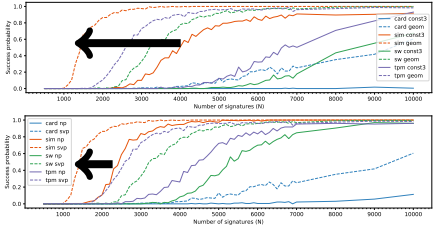
Analysis



- **Bounds** l_i
  - Constant or geometric (✸ **new**)

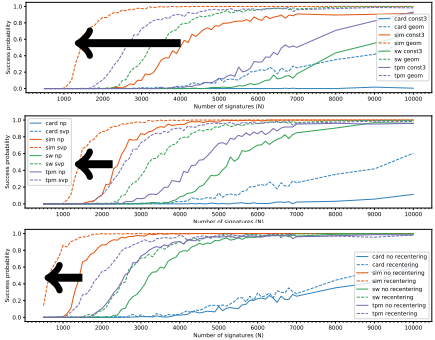
Analysis

- **Bounds** l_i
  - Constant or geometric (✸ **new**)
- **CVP/SVP**
  - CVP via Babai or embedding into SVP



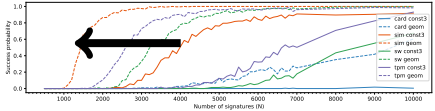
Analysis

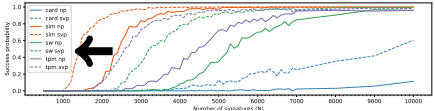
- **Bounds** l_i
  - Constant or geometric (✸ **new**)
- **CVP/SVP**
  - CVP via Babai or embedding into SVP
- **Recentering**
  - $|k_i - n/2^{l_i+1}| < n/2^{l_i+1}$

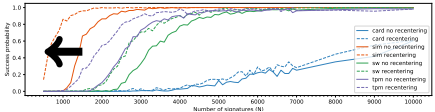


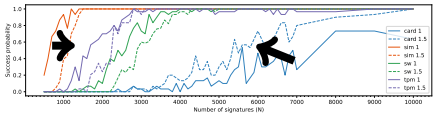
Analysis

- **Bounds** l_i
  - Constant or geometric (✸ **new**)
- **CVP/SVP**
  - CVP via Babai or embedding into SVP
- **Recentering**
  - $|k_i - n/2^{l_i+1}| < n/2^{l_i+1}$, yes
- **Random subsets**
  - random d out of $1.5d$ fastest



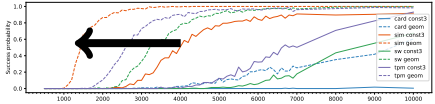


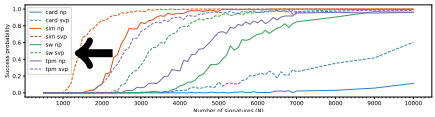


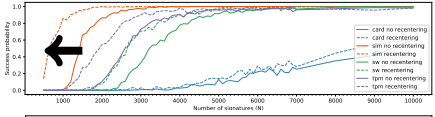


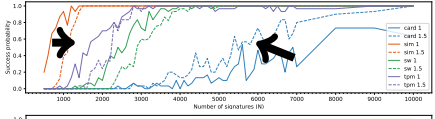
Analysis

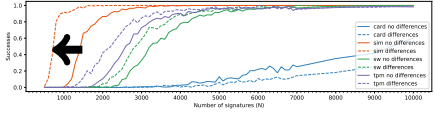
- **Bounds l_i**
  - Constant or geometric (✹ **new**)
- **CVP/SVP**
  - CVP via Babai or embedding into SVP
- **Recentering**
  - $|k_i - n/2^{l_i+1}| < n/2^{l_i+1}$, yes
- **Random subsets**
  - random d out of $1.5d$ fastest, yes, if ↑ errors
- **Nonce differences**
  - $|k_i - k_j| < n/2^{min(l_i,l_j)}$





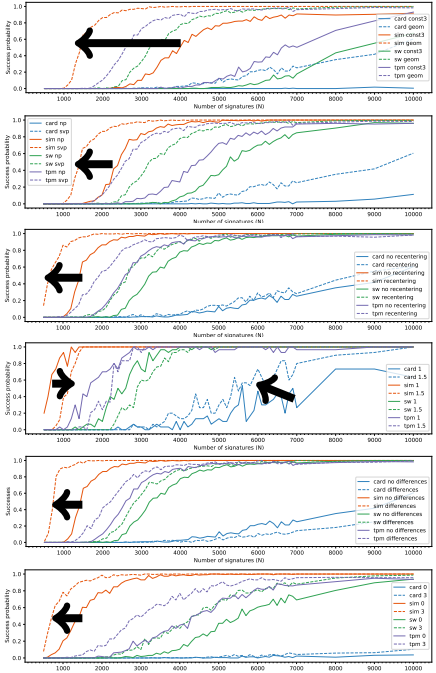






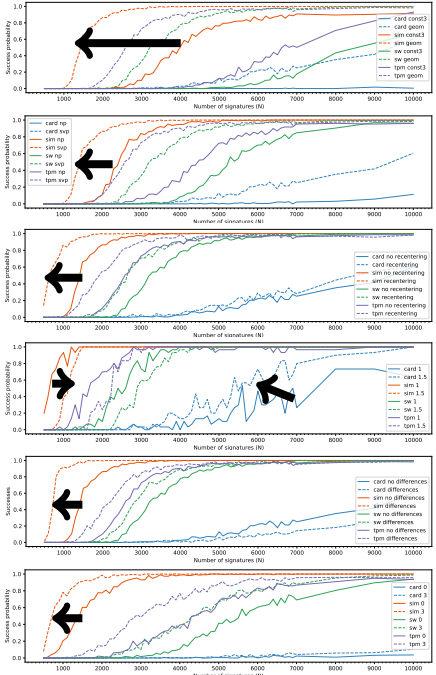
Analysis

- **Bounds l_i**
  - Constant or geometric (✹ **new**)
- **CVP/SVP**
  - CVP via Babai or embedding into SVP
- **Recentering**
  - $|k_i - n/2^{l_i+1}| < n/2^{l_i+1}$, yes
- **Random subsets**
  - random d out of $1.5d$ fastest, yes, if ↑ errors
- **Nonce differences**
  - $|k_i - k_j| < n/2^{min(l_i,l_j)}$, like recentering
- **u-bitflips with CVP** (✹ **new**)
  - Brute-force and CVP solve



Analysis

- **Bounds l_i**
  - Constant or geometric (✹ **new**)
- **CVP/SVP**
  - CVP via Babai or embedding into SVP
- **Recentering**
  - $|k_i - n/2^{l_i+1}| < n/2^{l_i+1}$, yes
- **Random subsets**
  - random d out of $1.5d$ fastest, yes, if ↑ errors
- **Nonce differences**
  - $|k_i - k_j| < n/2^{min(l_i,l_j)}$, like recentering
- **u-bitflips with CVP** (✹ **new**)
  - Brute-force and CVP solve, like recentering



Conclusions

- Private key extraction in ECDSA
  - CC EAL4+ smartcard, 5 libraries
- Two new methods
  - Geometric bounds
  - *u*-bitflips
- Systematic analysis of lattice attacks on bit-length leakage
- Attack on data from the TPM-FAIL paper [3], with only 900 signatures, instead of 40 000

Thanks!

jan@neuromancer.sk

The paper: minerva.crocs.fi.muni.cz

Icons from Noun Project & Font Awesome

Photos from Unsplash

References

1. Dan Boneh, Ramarathnam Venkatesan; **Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes**
2. Billy Bob Brumley, Nicola Tuveri; **Remote Timing Attacks are Still Practical**
3. Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, Nadia Heninger; **TPM-FAIL: TPM meets Timing and Lattice Attacks**
4. Sohaib ul Hassan, Iaroslav Gridin, Ignacio M. Delgado-Lozano, Cesar Pereida García, Jesús-Javier Chi-Domínguez, Alejandro Cabrera Aldaya, Billy Bob Brumley; **Déjà Vu: Side-Channel Analysis of Mozilla's NSS**
5. Joachim Breitner, Nadia Heninger; **Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies**
6. Jean-Charles Faugere, Christopher Goyet, Guénaël Renault; **Attacking (EC)DSA given only an implicit hint**