Horizontal Collision Correlation Attack on Elliptic Curves

A. Bauer E. Jaulmes E. Prouff J. Wild

Talk by J.-R. Reinhard

ANSSI (French Network and Information Security Agency)

Selected Areas in Cryptography 2013
Burnaby, Canada – August 16, 2013

Elliptic Curve Cryptography

- Introduced by Koblitz and Miller in mid 80s
- Use the group of $\mathbb{F}_p$-rational points of an Elliptic Curve to build cryptosystems
- Security based on the hardness of DL in this group
- Many advantages
  - DL believed to be more difficult on $E(\mathbb{F}_p)$ than on $(\mathbb{F}_p^*, \times)$
  - Thus, smaller parameter sizes can be chosen
  - Faster computations, more compact implementations
- Use of ECC (mainly ECDSA, ECDH) is spreading
  - Introduction in SSL/TLS, openssl, `https://www.google.com`
  - Smart cards, E-passport, ...

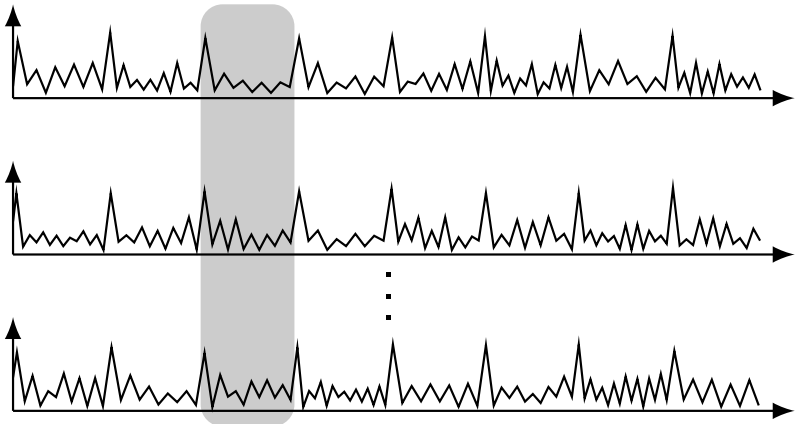
Side Channel Attacks

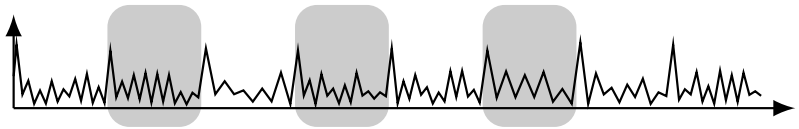
- Introduced by Kocher et al. in mid 90s
- Cryptographic computations are performed stepwise by processors
- Sequence of performed operations and/or intermediate values may leak partially through observable physical side channels
  - Power consumption
  - Electromagnetic emanation
- Simple SC Analysis
  - Sensitive targeted operations need to be observed only for fixed inputs
  - e.g., SPA
- Advanced SC Analysis
  - Sensitive targeted operations need to be observed for several different inputs
  - A statistical post-processing is applied to aggregate observations relative to a same secret data (e.g., key bit)
  - e.g., CPA

Variations on Advanced SCA

Vertical vs Horizontal Attacks [CFGRV10]

- Differ by the origin of aggregated observations:
- Vertical: N executions
- Horizontal: N sub-parts of a single execution





Correlation [BCO04] vs Collision Attacks [SWP03]

- Differ by what the statistical post-processing correlates:
- Observations and hypotheses stemming from a model
- Several observations

ECC Implementation

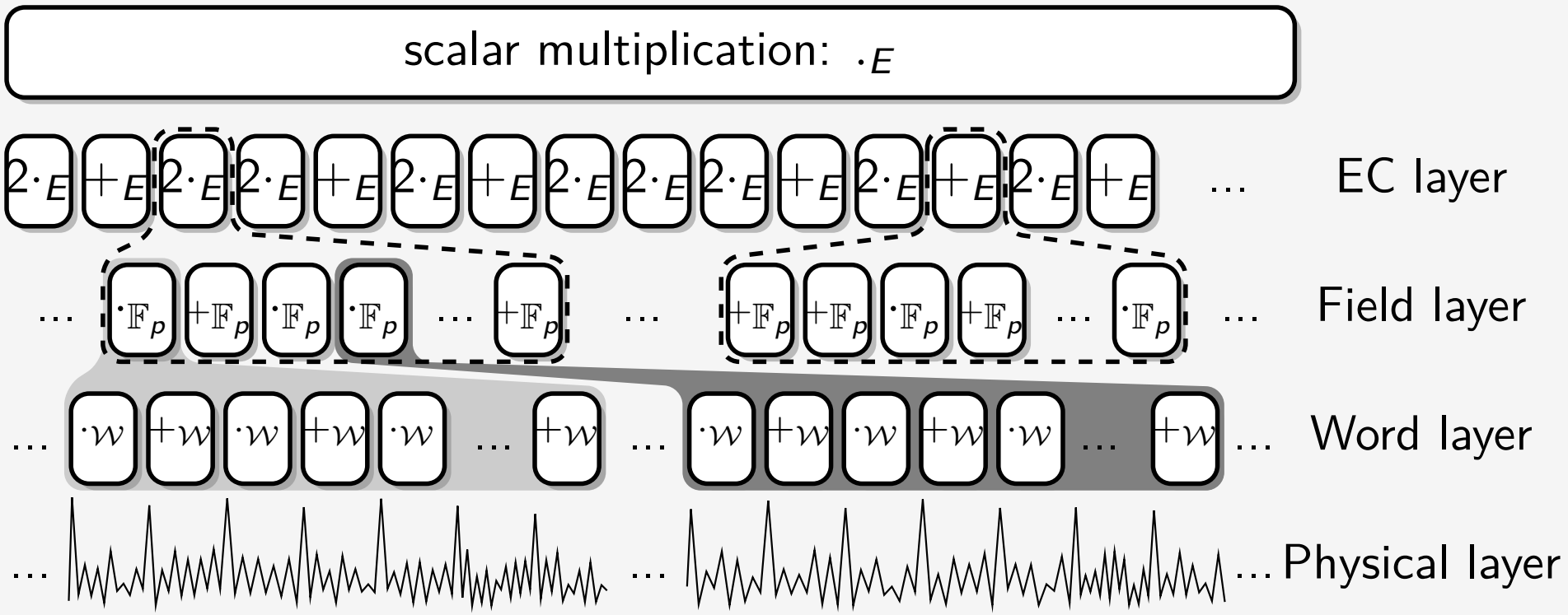
Point Representation

- $P \sim$ a triplet of $\mathbb{F}_p$ values: $(X : Y : Z)$
- e.g., *Projective coordinates*
- Point addition and doubling formulas express coordinates of $P + Q$, $2P$ explicitely from the coordinates of P and Q

Computations

- scalar multiplication: $Q = sP$
- $\leftrightarrow$ sequence of elliptic curve operations (E-operations)
- each of these E-operations: $\leftrightarrow$ sequence of field operations ($\mathbb{F}_p$-operations)
- each of these $\mathbb{F}_p$-operations: $\leftrightarrow$ sequence of word multi-precision operations ($\mathcal{W}$-operations), manageable by the processor

ECC Implementation: Logical Layers



ECC & SCA

Specificities of EC regarding SCA

- Usually, s is ephemeral: ECDH, ECDSA
  - For each s, only one trace is available
- The sequence of operations in the EC layer is correlated to s

SCA Protection

- Use *regular* algorithms: the sequence of operation types is independent of s
  - Double & Add always, unified formulas: regular EC layer
  - Atomicity: regular Field layer
- Correlation to s is moved to operations I/O routing

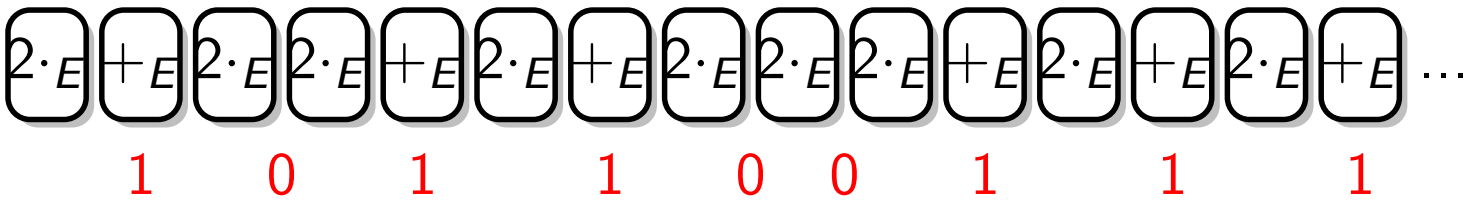
ECC & SCA

Specificities of EC regarding SCA

SC

Double & Add: SPA

1: $\pi \leftarrow 0$
2: **for** $i := 0$ **to** $\lceil \log_2(q) \rceil - 1$ **do**
3: $\quad \pi \leftarrow 2 \cdot \pi$
4: $\quad$ **if** $s_i = 1$ **then**
5: $\quad\quad \pi \leftarrow \pi + P$
6: $\quad$ **end if**
7: **end for**



ECC & SCA

Specificities of EC regarding SCA

- Usually, s is ephemeral: ECDH, ECDSA
  - For each s, only one trace is available
- The sequence of operations in the EC layer is correlated to s

SCA Protection

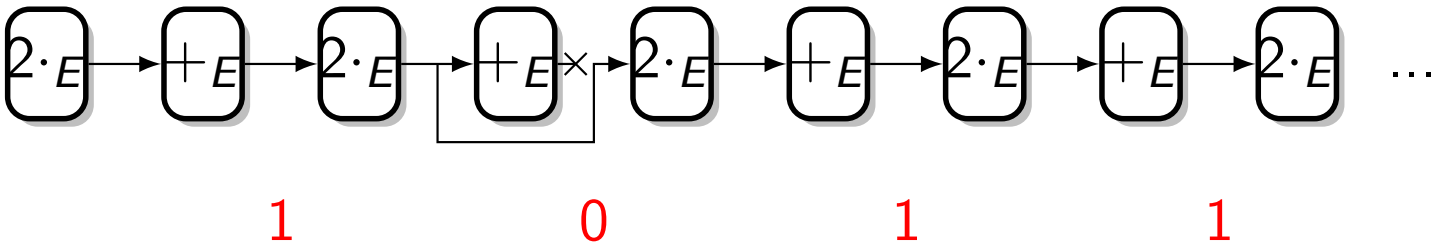
- Use *regular* algorithms: the sequence of operation types is independent of s
  - Double & Add always, unified formulas: regular EC layer
  - Atomicity: regular Field layer
- Correlation to s is moved to operations I/O routing

ECC & SCA

Specificities of EC regarding SCA

Double & Add Always

1: $\pi \leftarrow 0$
2: **for** $i := 0$ **to** $\lceil \log_2(q) \rceil - 1$ **do**
3: $\quad \pi_0 \leftarrow 2 \cdot \pi$
4: $\quad \pi_1 \leftarrow \pi_0 + P$
5: $\quad \pi \leftarrow \pi_{s_i}$
6: **end for**



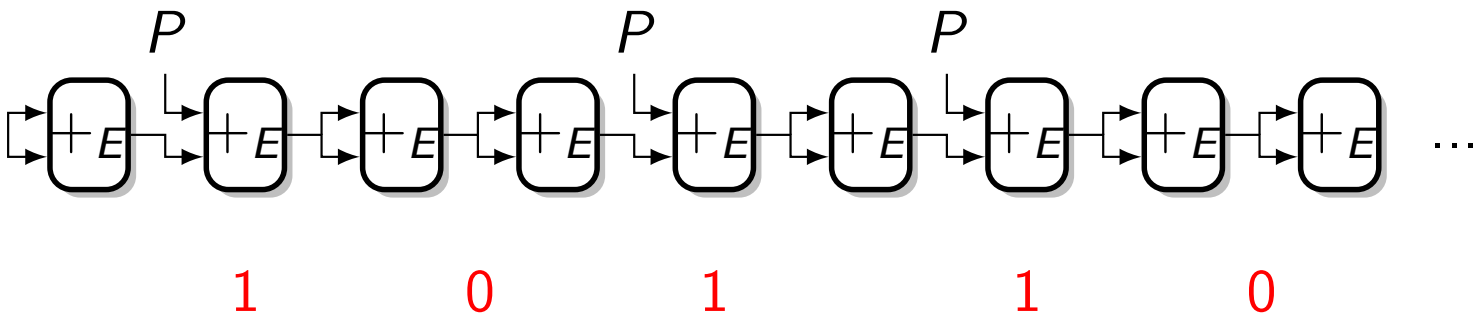
ECC & SCA

Specificities of EC regarding SCA

- Usually, s is ephemeral: ECDH, ECDSA

Unified Formulas

- Basic double & add algorithm, but using the same operator for both $+_E$ and $2\cdot_E$



ECC & SCA

Specificities of EC regarding SCA

- Usually, s is ephemeral: ECDH, ECDSA
  - For each s, only one trace is available
- The sequence of operations in the EC layer is correlated to s

SCA Protection

- Use *regular* algorithms: the sequence of operation types is independent of s
  - Double & Add always, unified formulas: regular EC layer
  - Atomicity: regular Field layer
- Correlation to s is moved to operations I/O routing

Contribution

- Establish a *shared factor* distinguisher by analyzing the word layer
- Use this distinguisher to build secret scalar recovery attacks
- Explore the wide applicability of these *Horizontal Collision Correlation attacks*

Core Ideas

- Field multiplications are not atomic but built on word multiplications
- By combining information leaked by word multiplications corresponding to two field multiplications, one can identify factor reuse
- Identifying factor reuse enables to distinguish point addition from point doubling in classical regular algorithms, even in presence of classical blindings, using a single trace

Multiplication over $\mathbb{F}_p$: Implementation and Modeling

Implementation

- Each element $X \in \mathbb{F}_p$ is represented by an array of t words, $X[i] \in \mathcal{W}$
- $\cdot_{\mathbb{F}_p}$ interleaves word additions, multiplications and reductions
- $X \cdot_{\mathbb{F}_p} Y$ involves computations of N word multiplications $x \cdot_{\mathcal{W}} y$

Multiplication example

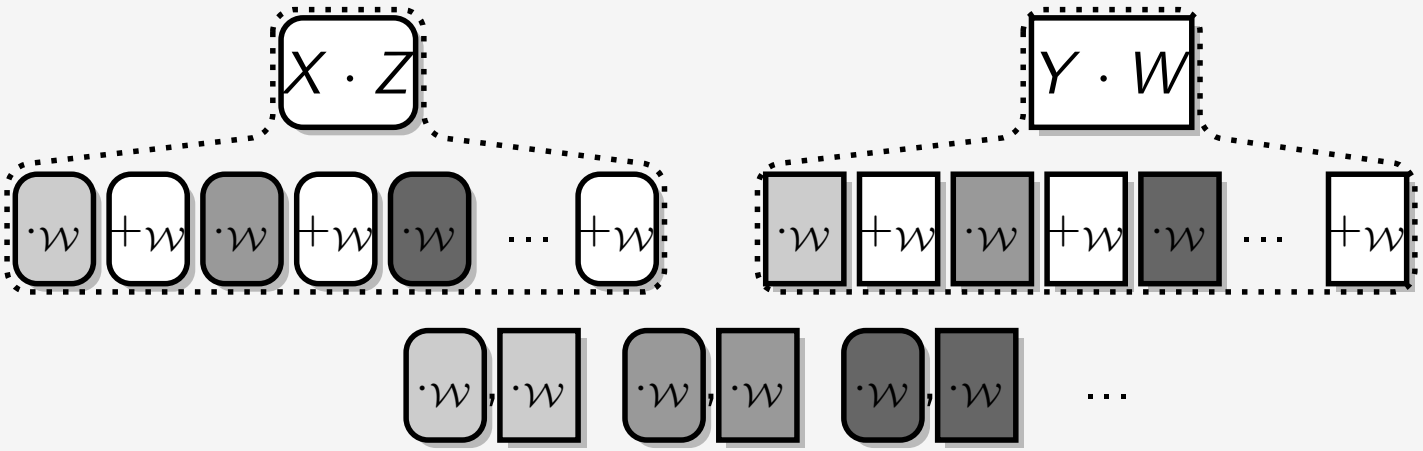
- LIM: $X[i] \cdot_{\mathcal{W}} Y[j], N = t^2$

Modeling

- Heuristically: words x are independent and follow $\mathcal{U}(\mathcal{W})$
- Distribution of word multiplication results can be deduced
- Per field multiplication, we get N noisy samples of a random variable following this distribution

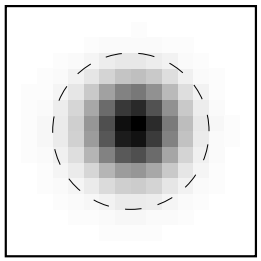
Shared Factor Bias

- Let us consider jointly two $\mathbb{F}_p$ multiplications $(X.Z, Y.W)$



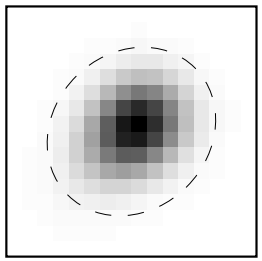
No Factor Repetition

- No correlation between the word multiplication results



$Z = W$

- Correlation due to the reuse of Z (*Collision*)



- N word multiplication pairs available (*Horizontal*)

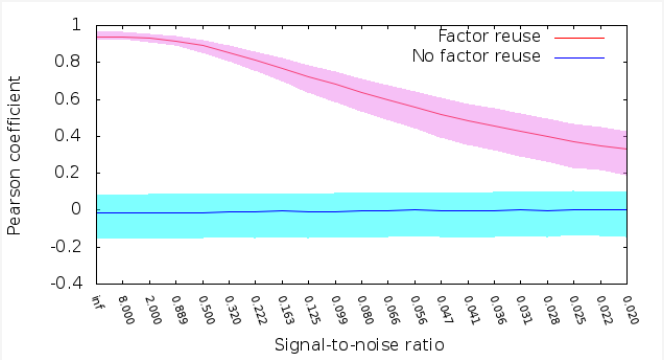
A Distinguisher

Algorithm

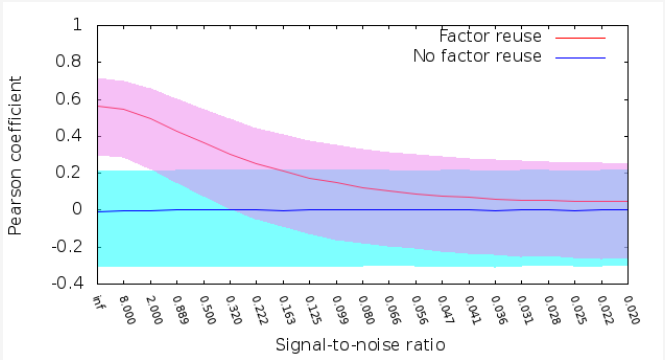
1: Get observations $\left(l_i^{X \cdot Z}\right)$, $\left(l_i^{Y \cdot W}\right)$ of the word multiplications
2: Compute the Pearson coefficient $\rho = \hat{\rho}(l^{X \cdot Z}, l^{Y \cdot W})$
3: **if** $\rho > \rho_{\text{limit}}$ **then return** "shared factor"
4: **else return** "no shared factor"

Simulation

- LIM multiplication (optimized distinguisher)
- Leakage model: $l_{i,j}^{U \cdot V} = \mathrm{HW}(U[i] \cdot V[j]) + B_{i,j}^{U \cdot V}, B \sim \mathcal{N}(0, \sigma^2)$



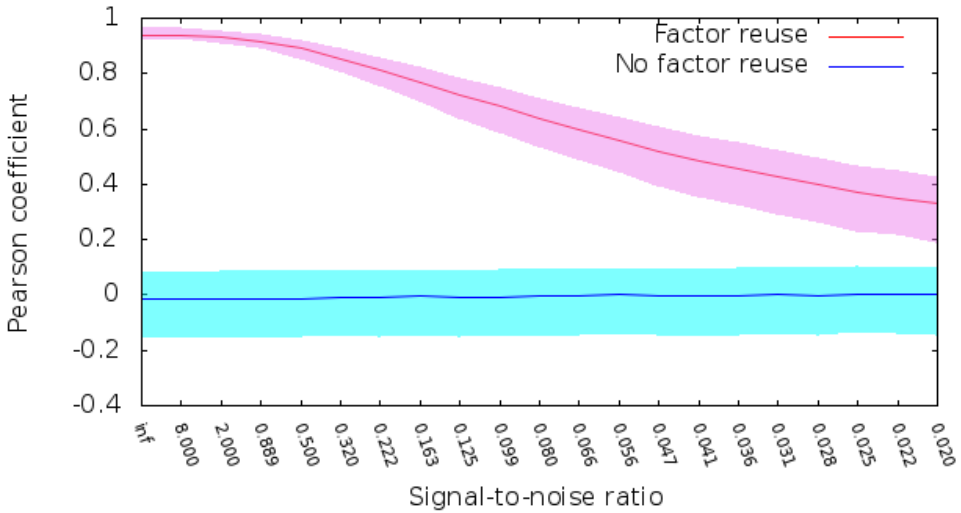
Correlation as a function of SNR (8-bit proc., 384-bit curves)



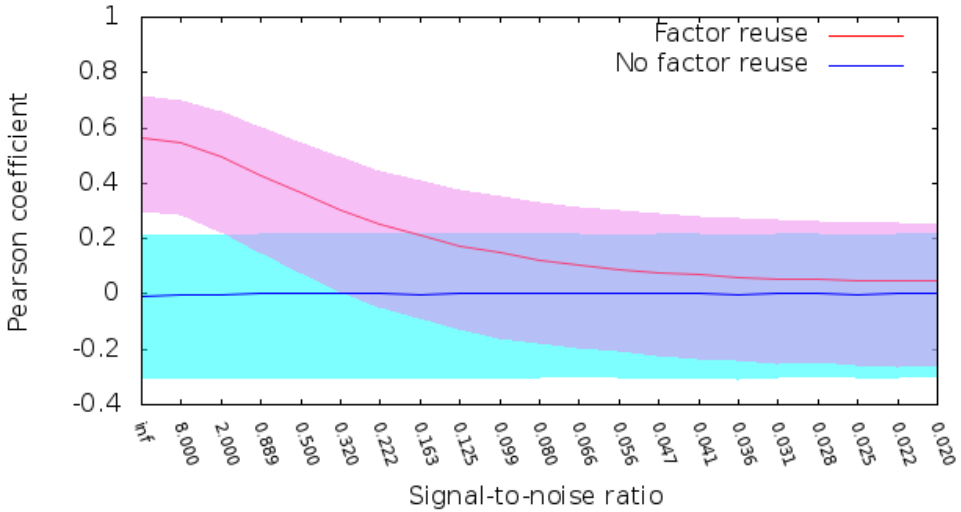
Correlation as a function of SNR (32-bit proc., 384-bit curves)

A Distinguisher

Pearson Coefficient: Simulation



Correlation as a function of SNR (8-bit proc., 384-bit curves)



Correlation as a function of SNR (32-bit proc., 384-bit curves)

Correlation as a function of SNR (8-bit proc., 384-bit curves) Correlation as a function of SNR (32-bit proc., 384-bit curves)

From Distinguisher to Secret Recovery Attacks

Definition: Characteristic Multiplication Pair

A pair of field multiplications is said to be *characteristic* for bit b if there is a factor reuse in this pair according to b

Outline

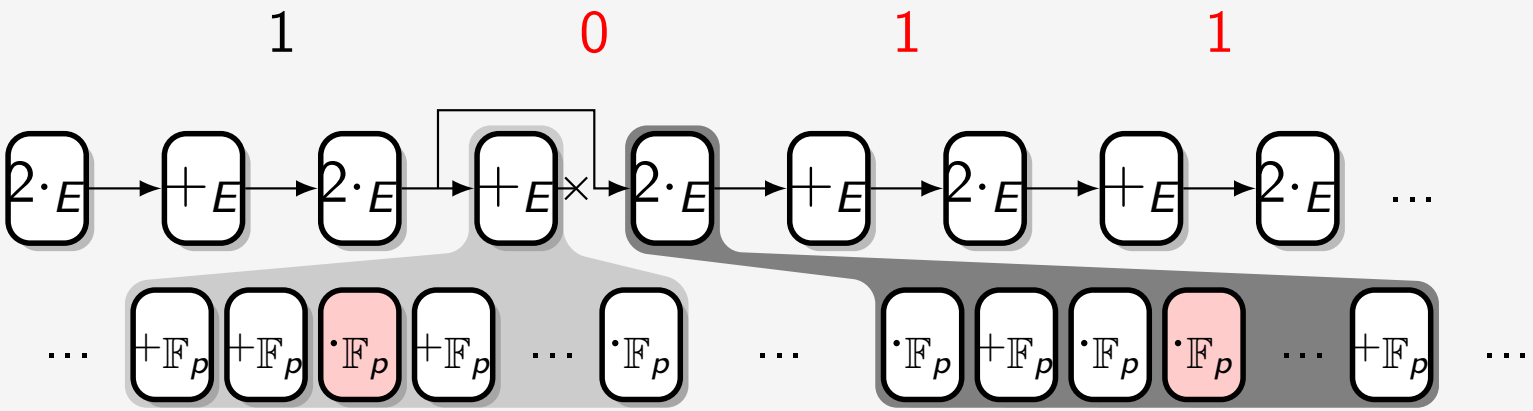
1: **while** there is an unknown bit in s **do**
2: Identify a characteristic multiplication pair for an unknown bit b
3: Apply the shared factor distinguisher to this pair
4: Recover b from the result
5: **end while**

- Characteristic pairs identification depends on the field logical layer
- We detail 3 examples to expose the generality of the technique

Double & Add Always

Characteristic Pair

- Each scalar bit b determines what happens after an addition
  - $b = 0$: the result is discarded, and an input of the addition is reused in next step
  - $b = 1$: the result is kept, and replaces the input of the addition
- One can identify two field multiplications, one for a $+_E$, one for the following $2\cdot_E$, which share an input iff $b = 0$



Unified formulas

Edwards Curves Formulas

$P = (X_1:Y_1:Z_1)$, $Q = (X_2:Y_2:Z_2)$, $P + Q = (X_3:Y_3:Z_3)$
c: a parameter of the curve

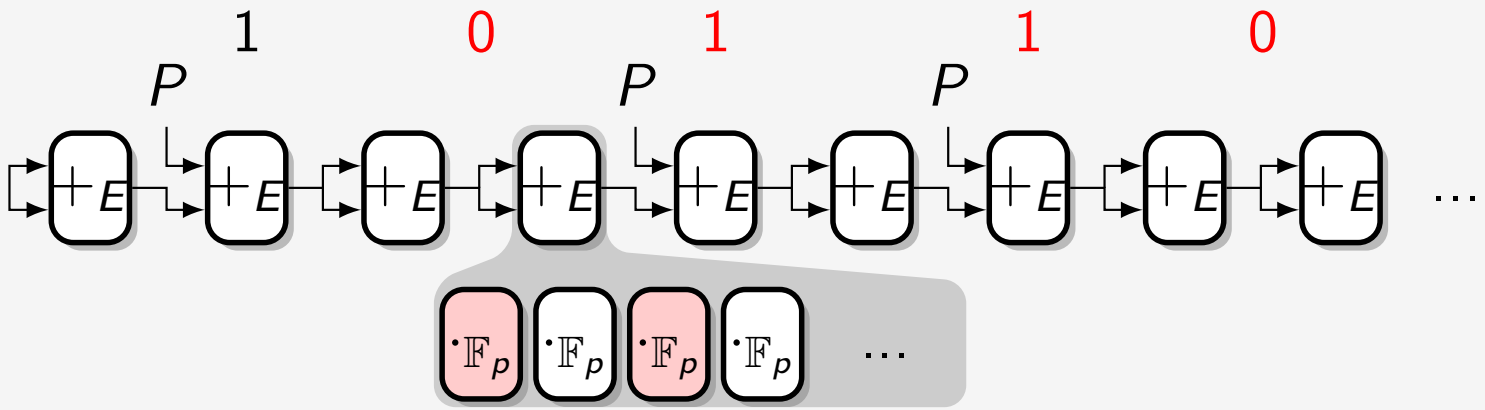
$$\begin{cases} X_3 &= Z_1 Z_2 (X_1 Y_2 - Y_1 X_2)(X_1 Y_1 Z_2^2 + X_2 Y_2 Z_1^2) \\ Y_3 &= Z_1 Z_2 (X_1 X_2 + Y_1 Y_2)(X_1 Y_1 Z_2^2 - X_2 Y_2 Z_1^2) \\ Z_3 &= \frac{1}{c} Z_1^2 Z_2^2 (X_1 X_2 + Y_1 Y_2)(X_1 Y_2 - Y_1 X_2) \end{cases}$$

Field Operations Sequence

Addition	Doubling
1. $R_1 \leftarrow X_1 Z_2$	1. $R_1 \leftarrow \mathbf{X_1 Z_1}$
2. $R_2 \leftarrow Y_1 Z_2$	2. $R_2 \leftarrow Y_1 Z_1$
3. $R_3 \leftarrow Z_1 X_2$	3. $R_3 \leftarrow \mathbf{Z_1 X_1}$
4. $R_4 \leftarrow Z_1 Y_2$	4. $R_4 \leftarrow Z_1 Y_1$
⋮	⋮

Characteristic Pair

- Use the multiplication pair in the first undetermined EC operation



Atomic Schemes

Principle

- A fixed pattern of field operations repeated several times
- Act on a set of registers initialized with input or random values
- Appropriate I/O routing ensures computation of addition or doubling

Chevallier-Mames et al.'s Scheme

Addition

$R_1 \leftarrow X_1,\ R_2 \leftarrow Y_1,\ R_3 \leftarrow Z_1,$
$R_7 \leftarrow X_2,\ R_8 \leftarrow Y_2,\ R_9 \leftarrow Z_2$

1. $R_4 \leftarrow R_9 \cdot R_9 \quad (= Z_2 \cdot \boldsymbol{Z_2})$
   $\star$
   $\star$
   $\star$
2. $R_1 \leftarrow R_1 \cdot R_4$
   $\star$
   $\star$
   $\star$
3. $R_4 \leftarrow R_4 \cdot R_9 \quad (= Z_2^2 \cdot \boldsymbol{Z_2})$
   $\star$
   $\star$
   $\star$

...

Doubling

$R_0 \leftarrow a,\ R_1 \leftarrow X_1,\ R_2 \leftarrow Y_1,\ R_3 \leftarrow Z_1$

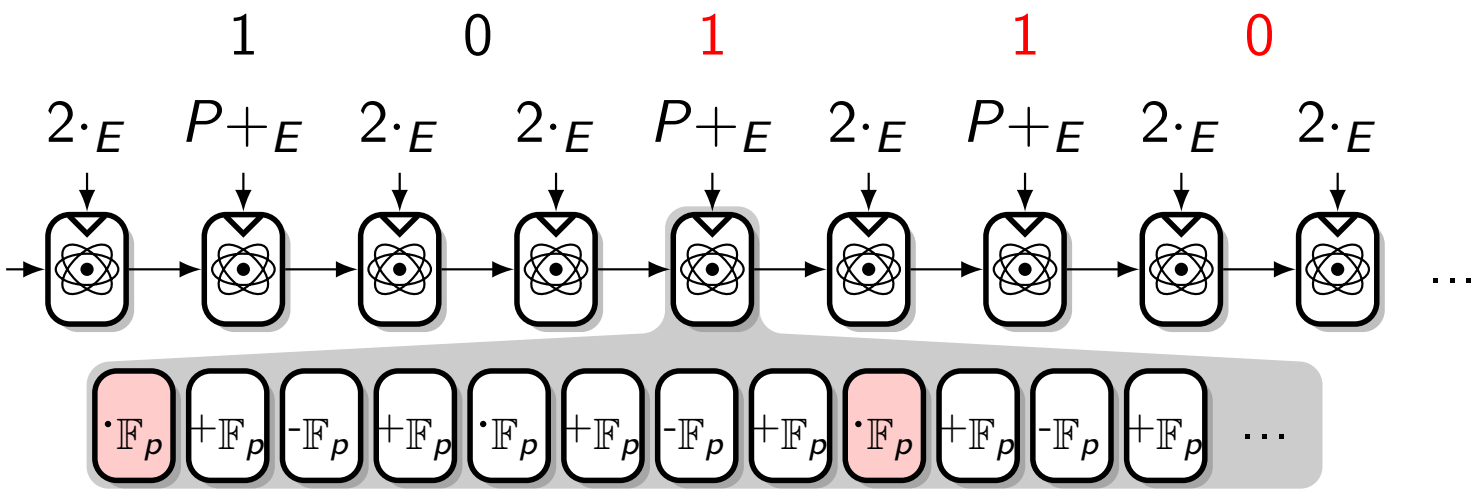
1. $R_4 \leftarrow R_1 \cdot R_1 \quad (= X_1 \cdot X_1)$
   $R_5 \leftarrow R_4 + R_4$
   $\star$
   $R_4 \leftarrow R_4 + R_5$
2. $R_5 \leftarrow R_3 \cdot R_3$
   $R_1 \leftarrow R_1 + R_1$
   $\star$
   $\star$
3. $R_5 \leftarrow R_5 \cdot R_5 \quad (= Z_1^2 \cdot Z_1^2)$
   $\star$
   $\star$
   $\star$

Atomic Schemes

Principle

Characteristic Pair

- Use the multiplication pair in the first undetermined EC operation

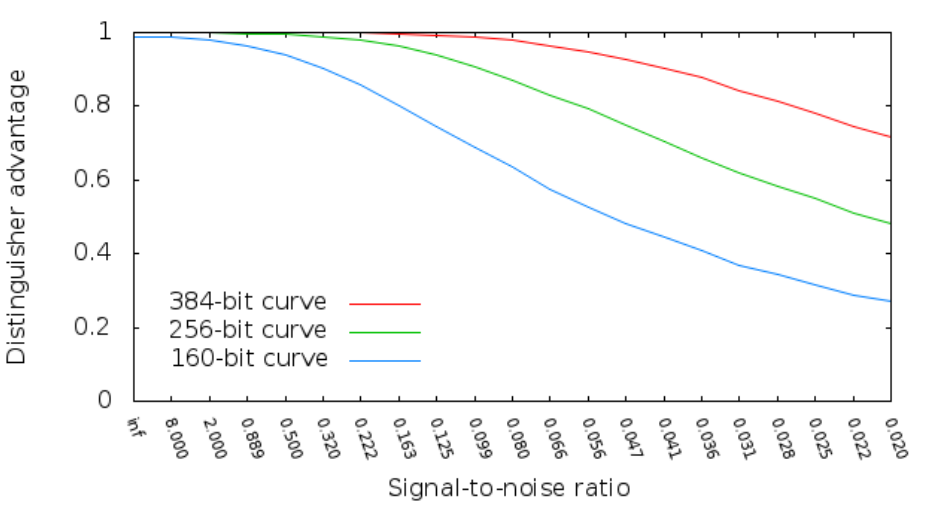


Simulation

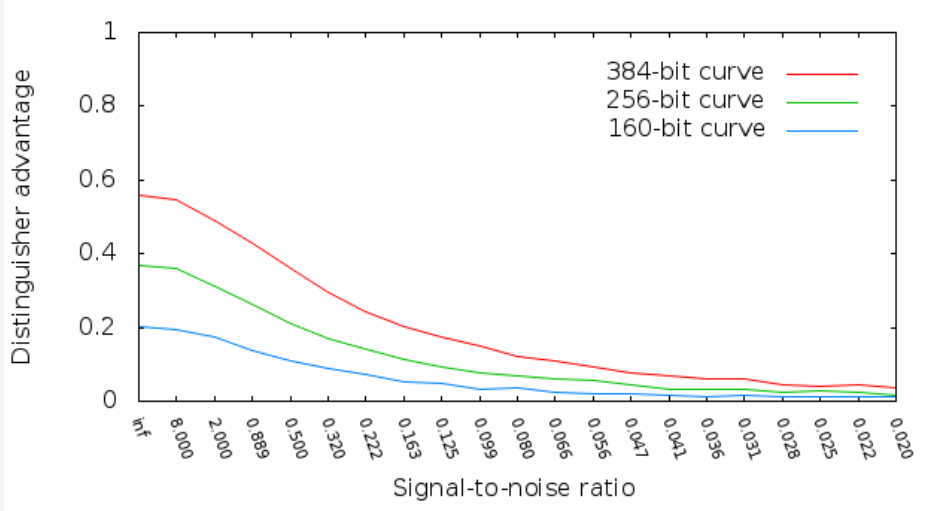
- Simulation performed to assess attack success probability

Simulation setup

- LIM multiplication (use of optimized distinguisher)
- Leakage model: noisy Hamming weight with Gaussian noise
- Chevallier-Mames et al.'s atomic scheme
- Perform attack on simulated traces for classical curve sizes
- Attacker's goal: recover 1 bit of secret scalar



Distinguisher advantage as a function of SNR (8-bit processor)



Distinguisher advantage as a function of SNR (32-bit processor)

Practicality of the attacks

- Presented attacks are theoretical, supported by simulations

Obstacles to Practical Application

- Identification of the multiplication algorithm
- Identification of the anti-SPA technique
- Resynchronization

However...

- Simulation indicates applicability even in presence of significant noise
- A single power trace is enough

Practicality of the attacks

- Presented attacks are theoretical, supported by simulations

Obstacles to Practical Application

- Identification of the multiplication algorithm
- Identification of the anti-SPA technique
- Resynchronization

However...

- Simulation indicates applicability even in presence of significant noise
- A single power trace is enough

Further (applied) work is needed!

Countermeasures

Ineffective Classical Countermeasures

- Input (s, P) randomization: attack independent of s and P values
- Point representation randomization
  - Single EC operation targeted
  - Multiplicative randomization

Countermeasures to Investigate

- Field multiplication generic protection
  - Randomization of the order of word operations in field multiplications
  - Operands blinding

Countermeasures

Ineffective Classical Countermeasures

- Input (s, P) randomization: attack independent of s and P values
- Point representation randomization
  - Single EC operation targeted
  - Multiplicative randomization

Countermeasures to Investigate

- Field multiplication generic protection
  - Randomization of the order of word operations in field multiplications
  - Operands blinding

Further work needed to determine the most efficient solutions

Conclusion

Identification of a new SC attack principle against ECC

- Combining *Horizontal* and *Collision* attack principles
- Only one trace needed
- Based on a shared factor distinguisher
- Theoretically applicable against a lot of implementations
  - Various $\mathbb{F}_p$ multiplication algorithms
  - Various EC arithmetics
- Even in presence of classical blindings

Open questions

- Practicality of the attack?
- Efficient countermeasures?

Thank you for your attention