Analyzing Side-Channel Leakage of RFID-Suitable Lightweight ECC Hardware

Erich.Wenger@iaik.tugraz.at
Thomas.Korak@iaik.tugraz.at
Mario.Kirschbaum@iaik.tugraz.at

Outline

- RFID?
- ECC Hardware (DUT)
- Power Analysis Attacks
  - Difference-of-Means
  - Correlation Attack
  - Revealing Intermediates
- Conclusion

What is RFID?


10:42
New tag collected
http://www.iaik.tugraz.at
Browser
http://www.tugraz.at
Browser
Done
Delete

What are the requirements?

- Analog interface
- Data transmission protocol
  - ISO14443A
  - ISO15693
  - NFC
- Top-level application
  - Authentication
  - Privacy
  - Cryptographic primitives

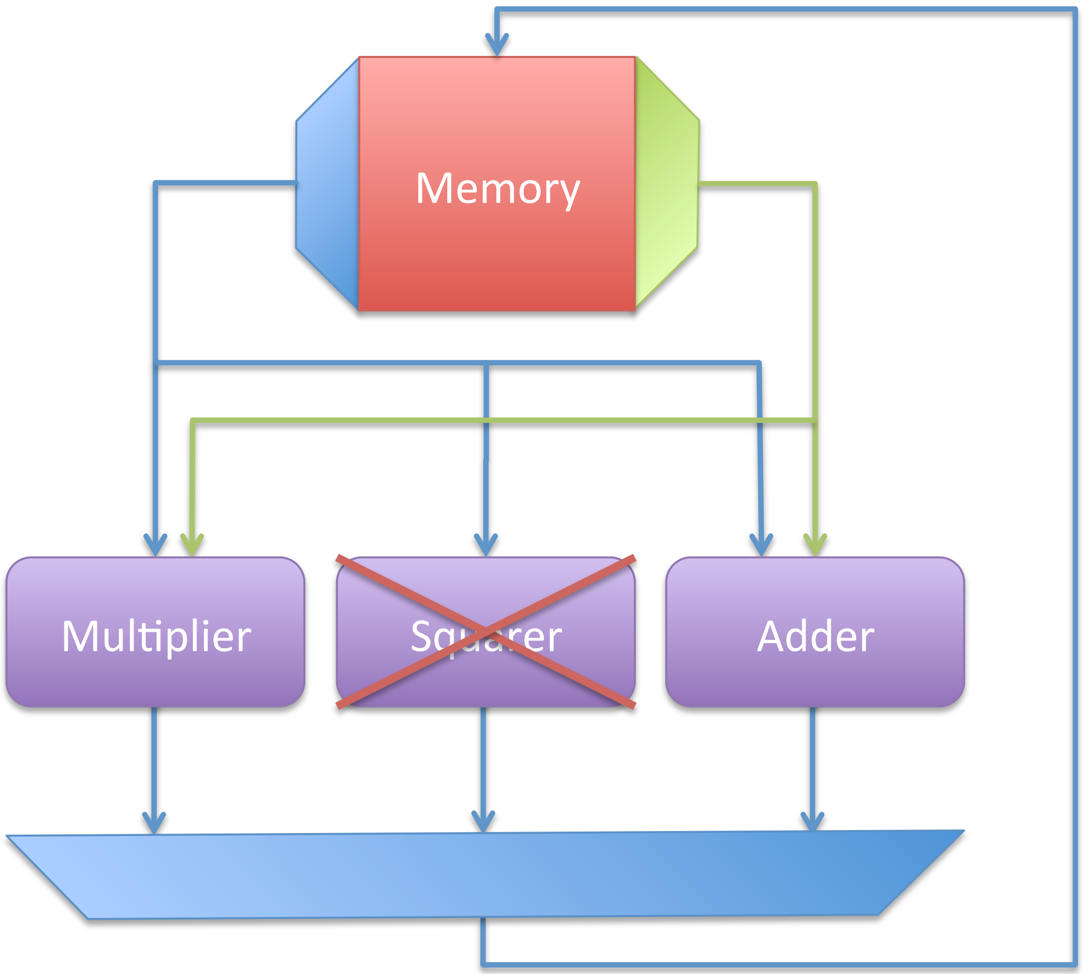
Elliptic Curve Cryptography

- Why?
  - e.g. for privacy preserving protocols
- Standardized (SECG, NIST)
  - For best interoperability
  - Already used for TLS, IPSec, and SSH
- Implemented elliptic curve
  - sect163r1 (NIST B-163)

Algorithms

- Left-to-right Montgomery Ladder by López and Dahab
- Randomized Projective Coordinates
- Use the Private Scalar only Once

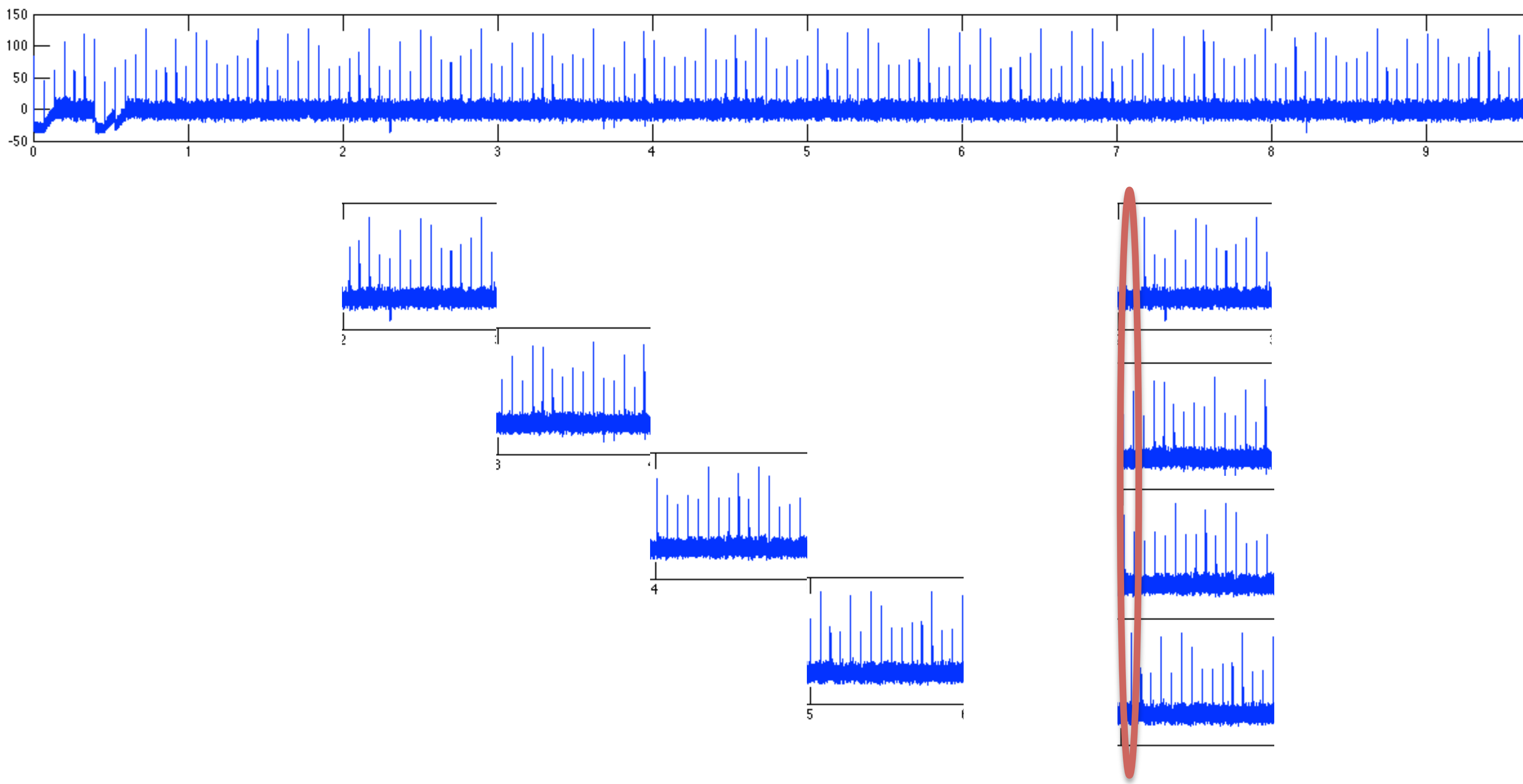
Architecture



Measurement Setup

- ASIC
  - Placed and Routed Design
  - VCD-based Toggle Count
- FPGA
  - SASEBO
  - Resolution Based on Input Buffer of Oscilloscope
  - Exact Clock Source Required

Measurement Methodology



Assuring Side-Channel Resistance

K162=1

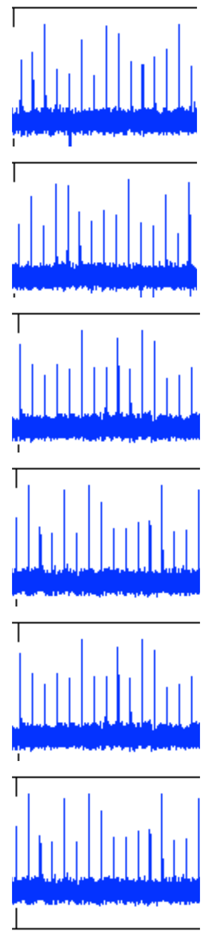
K161=0

K160=0

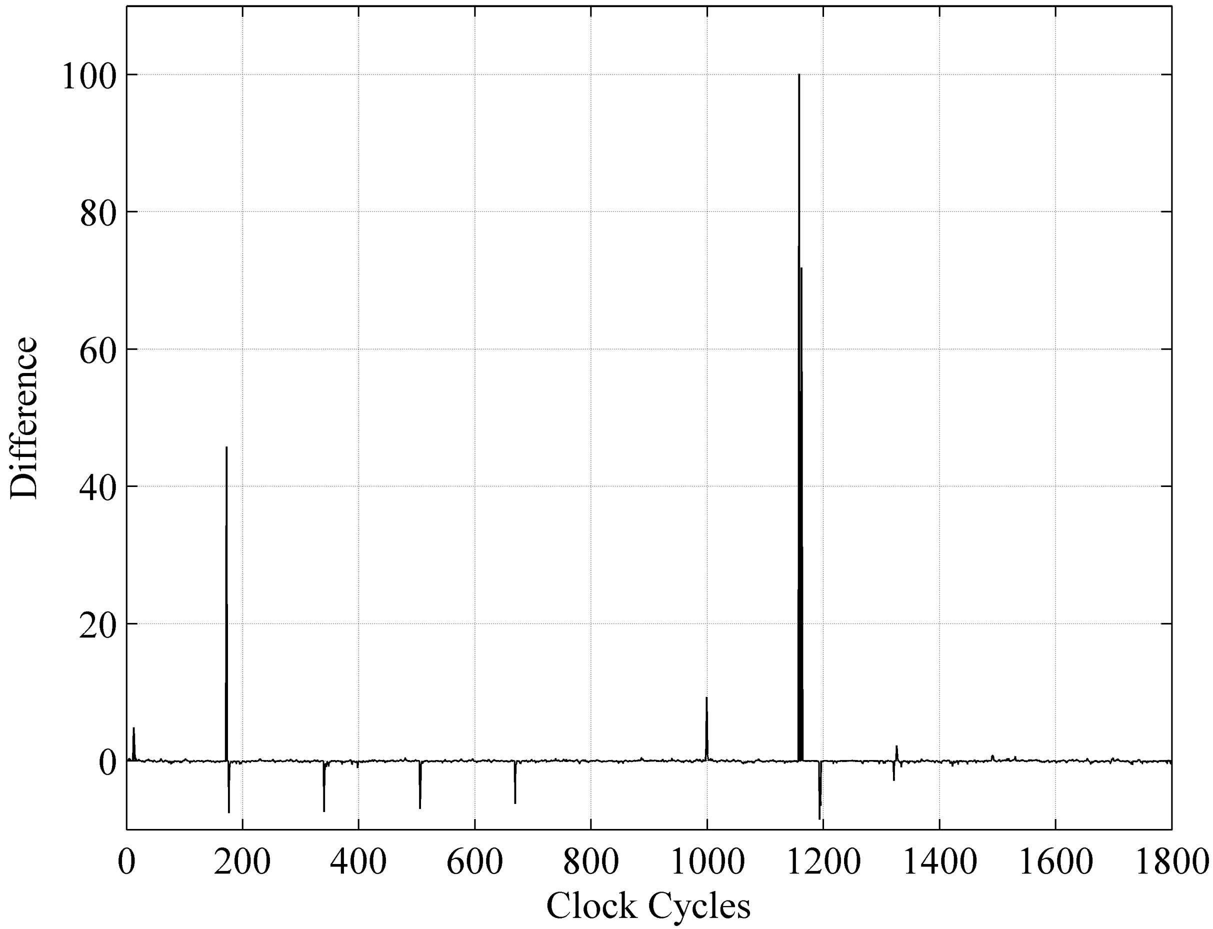
K159=1

K158=1

K157=0

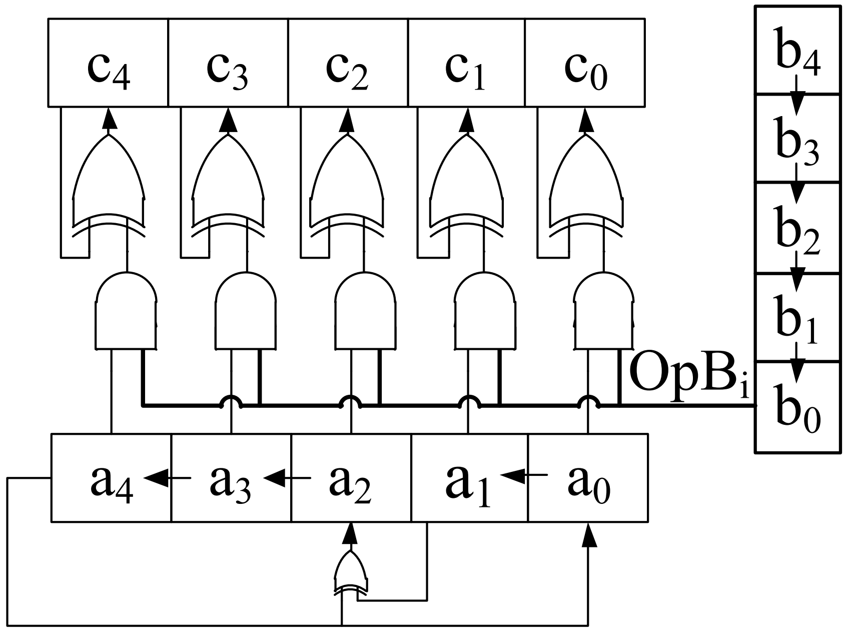


Assuring Side-Channel Resistance

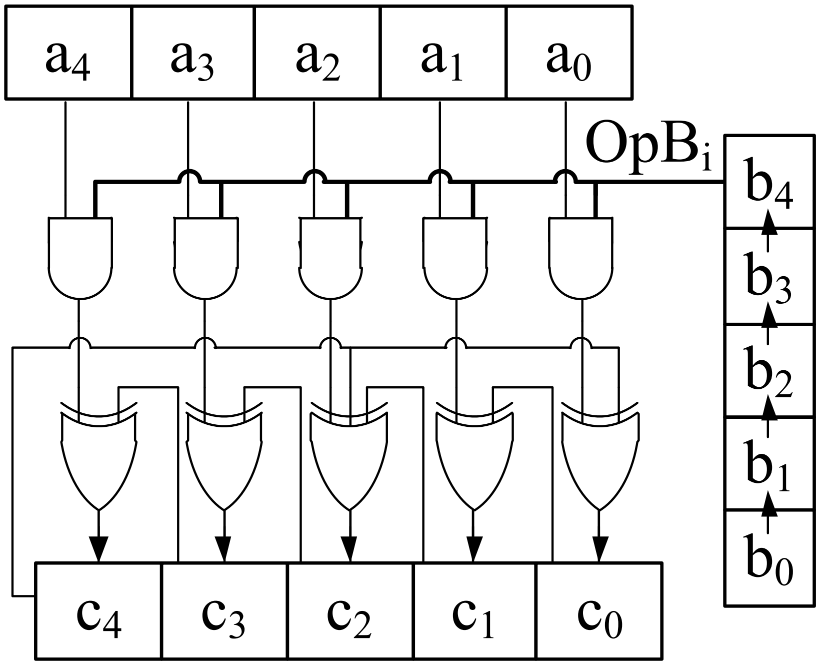


Finite Field Multiplier

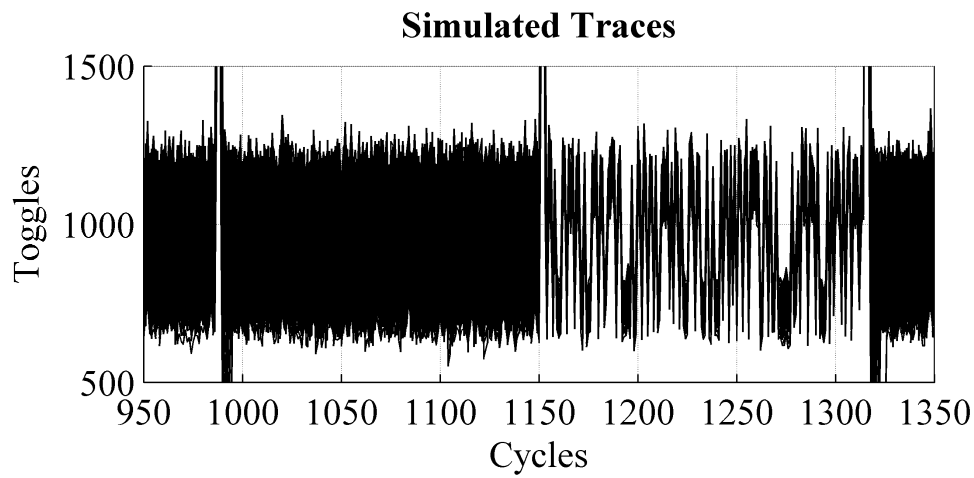
LSB First Multiplier

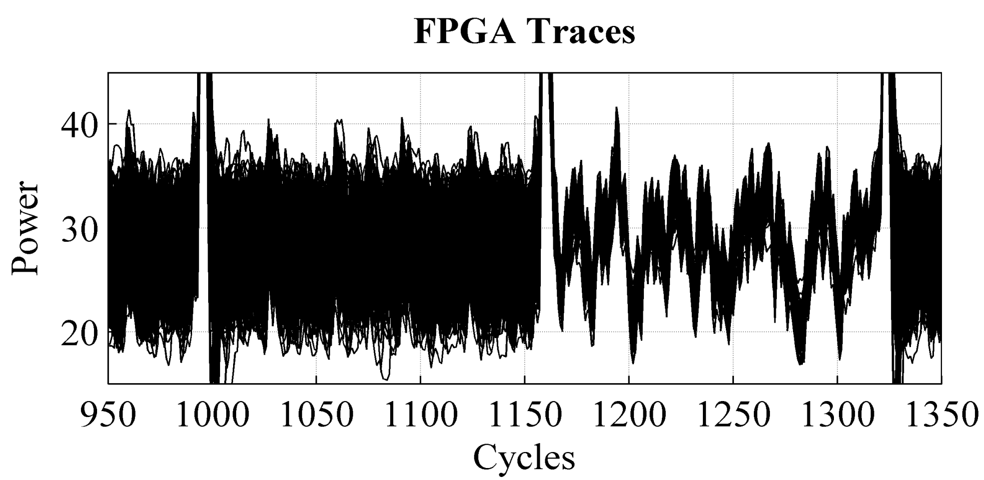


MSB First Multiplier

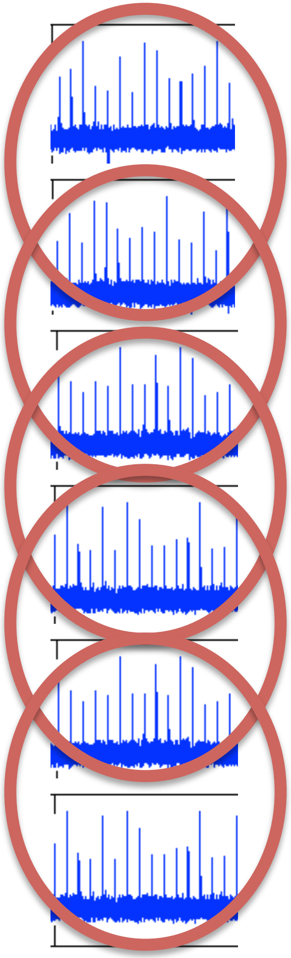


Leakage of Digit-Serial Multiplier

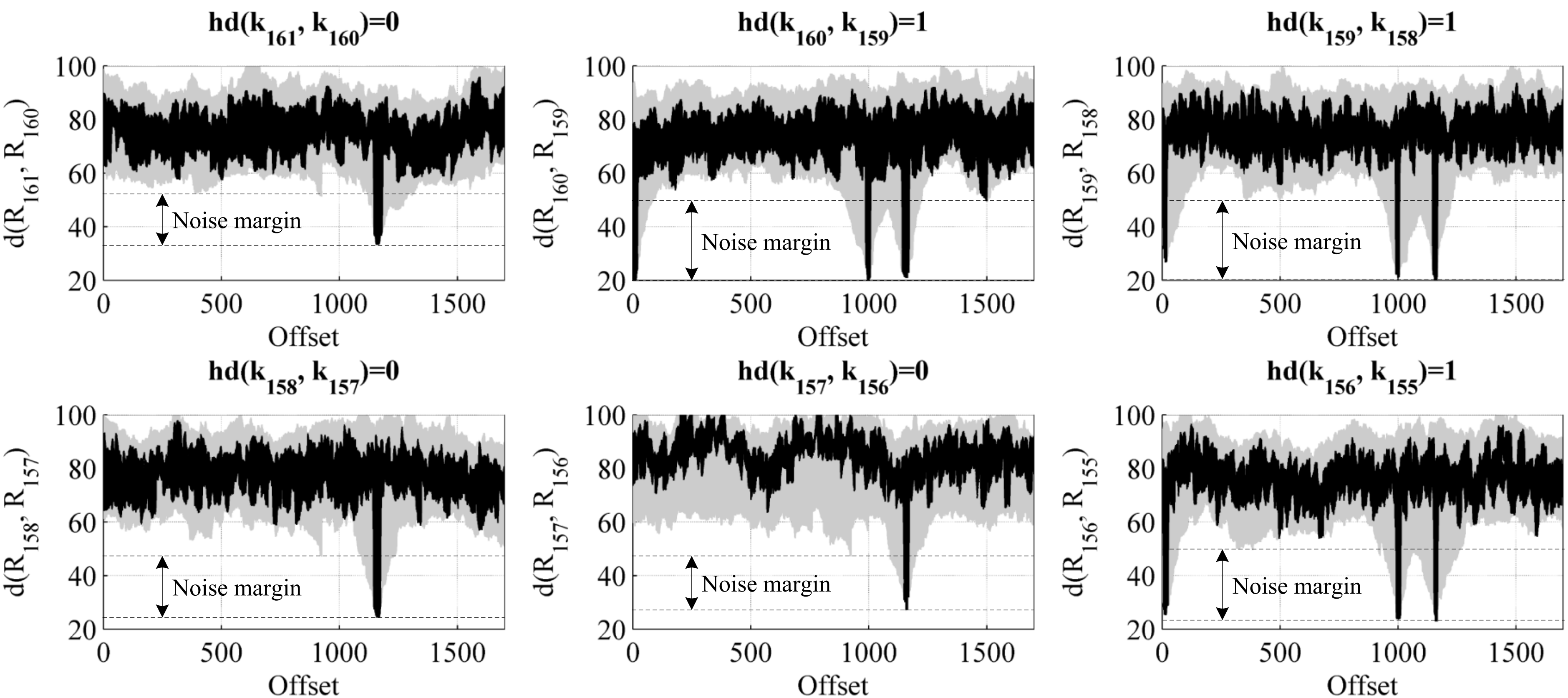




Correlation of Consecutive Rounds



Correlation of Consecutive Rounds



Correlation of Consecutive Rounds

Algorithm 1 López and Dahab round operations with key bits (0-0-1).

Ensure: $P_1' \leftarrow P_1 + P_2$.
Ensure: $P_2' \leftarrow 2 \cdot P_2$.

Point Addition

$X_1 \leftarrow X_1 \cdot Z_2$
$Z_1 \leftarrow Z_1 \cdot X_2$
$T_1 \leftarrow X_1 \cdot Z_1$
$Z_1 \leftarrow Z_1 + X_1$
$Z_1 \leftarrow Z_1 \cdot Z_1$
$X_1 \leftarrow x \cdot Z_1$
$X_1 \leftarrow X_1 + T_1$

Point Doubling

$X_2 \leftarrow X_2 \cdot X_2$
$Z_2 \leftarrow Z_2 \cdot Z_2$
$T_1 \leftarrow Z_2 \cdot c$
$Z_2 \leftarrow Z_2 \cdot X_2$
$T_1 \leftarrow T_1 \cdot T_1$
$X_2 \leftarrow X_2 \cdot X_2$
$X_2 \leftarrow X_2 + T_1$

Ensure: $P_1' \leftarrow P_1 + P_2$.
Ensure: $P_2' \leftarrow 2 \cdot P_2$.

Point Addition

$X_1 \leftarrow X_1 \cdot Z_2$
$Z_1 \leftarrow Z_1 \cdot X_2$
$T_1 \leftarrow X_1 \cdot Z_1$
$Z_1 \leftarrow Z_1 + X_1$
$Z_1 \leftarrow Z_1 \cdot Z_1$
$X_1 \leftarrow x \cdot Z_1$
$X_1 \leftarrow X_1 + T_1$

Point Doubling

$X_2 \leftarrow X_2 \cdot X_2$
$Z_2 \leftarrow Z_2 \cdot Z_2$
$T_1 \leftarrow Z_2 \cdot c$
$Z_2 \leftarrow Z_2 \cdot X_2$
$T_1 \leftarrow T_1 \cdot T_1$
$X_2 \leftarrow X_2 \cdot X_2$
$X_2 \leftarrow X_2 + T_1$

Ensure: $P_2' \leftarrow P_2 + P_1$.
Ensure: $P_1' \leftarrow 2 \cdot P_1$.

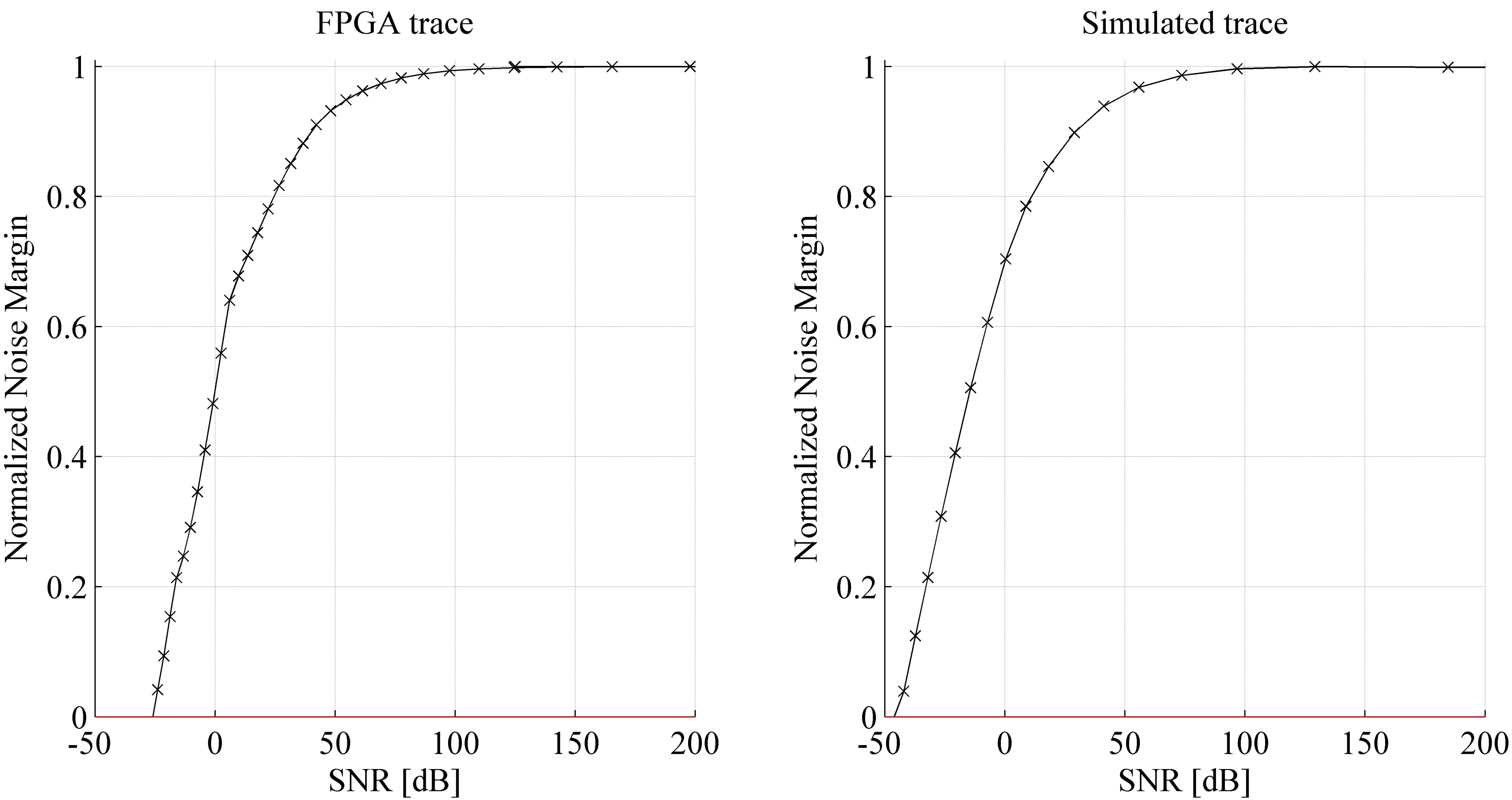
Point Addition

$X_2 \leftarrow X_2 \cdot Z_1$
$Z_2 \leftarrow Z_2 \cdot X_1$
$T_1 \leftarrow X_2 \cdot Z_2$
$Z_2 \leftarrow Z_2 + X_2$
$Z_2 \leftarrow Z_2 \cdot Z_2$
$X_2 \leftarrow x \cdot Z_2$
$X_2 \leftarrow X_2 + T_1$

Point Doubling

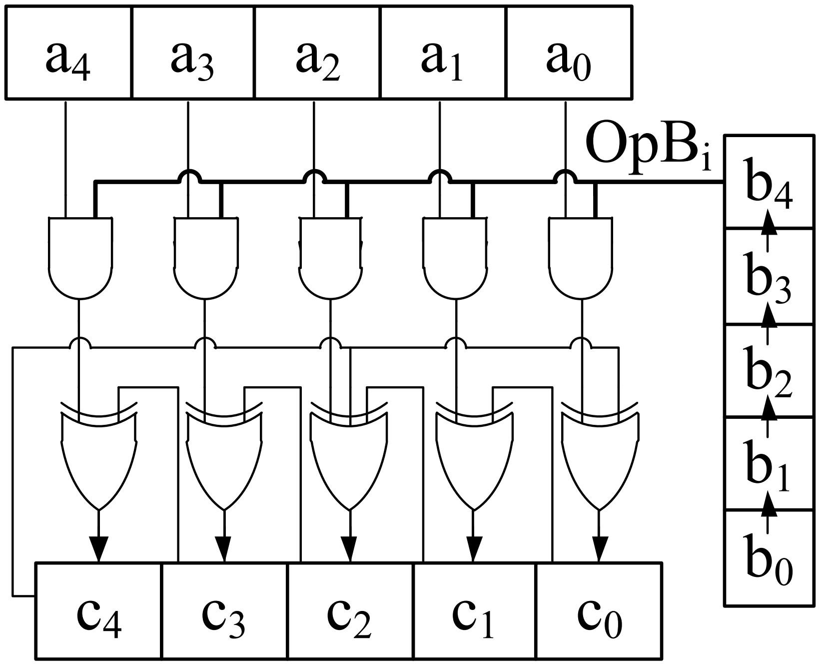
$X_1 \leftarrow X_1 \cdot X_1$
$Z_1 \leftarrow Z_1 \cdot Z_1$
$T_1 \leftarrow Z_1 \cdot c$
$Z_1 \leftarrow Z_1 \cdot X_1$
$T_1 \leftarrow T_1 \cdot T_1$
$X_1 \leftarrow X_1 \cdot X_1$
$X_1 \leftarrow X_1 + T_1$

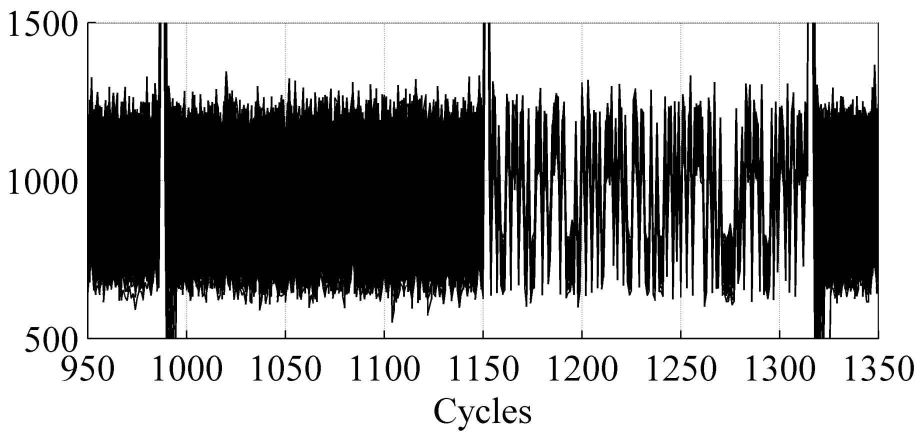
Correlation of Consecutive Rounds



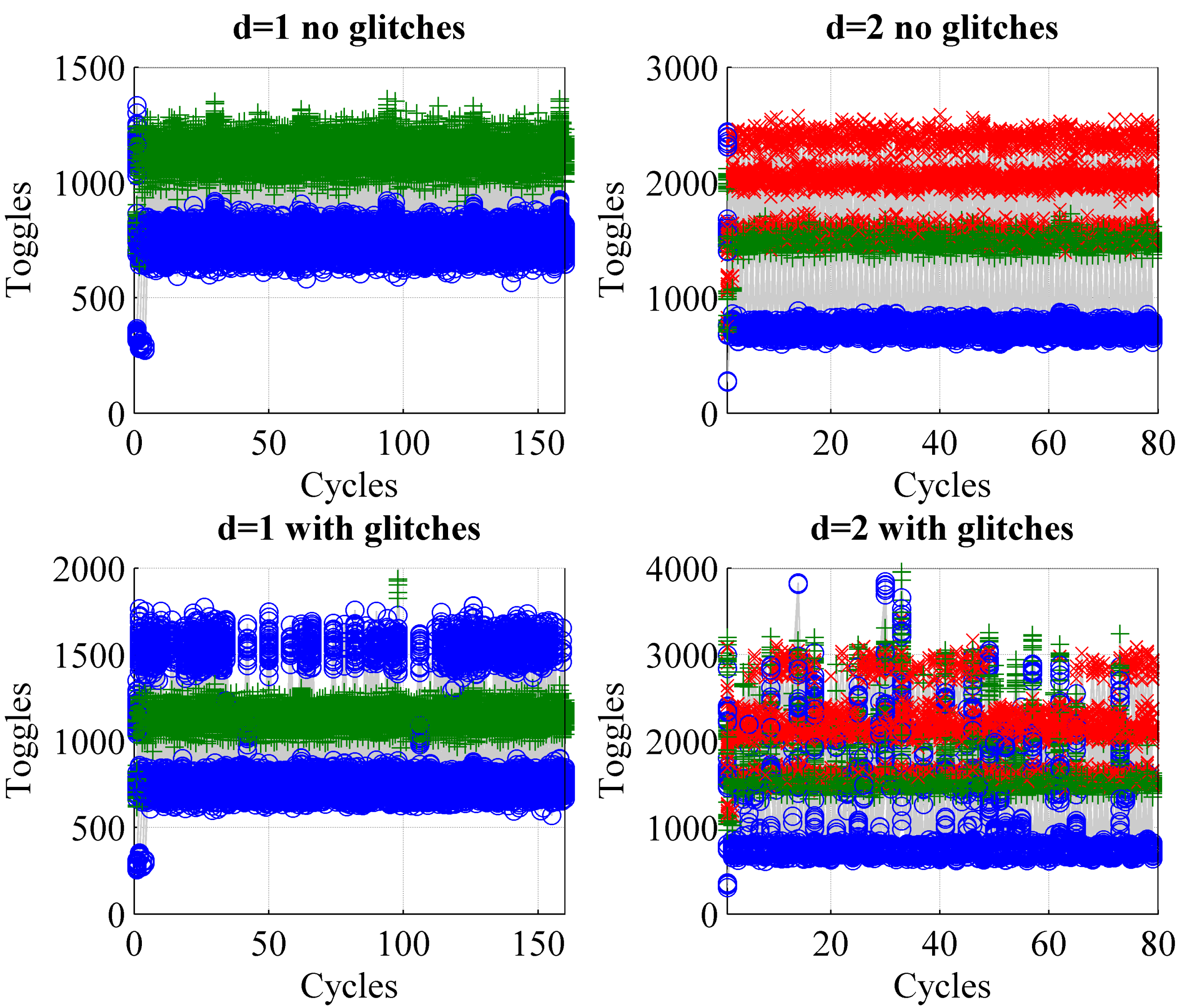
Revealing Intermediate Operands

MSB First Multiplier





Revealing Intermediate Operands



	0	1	2	3
0	0	1	1	2
1	1	0	2	1
2	1	2	0	1
3	2	1	1	0

Revealing Intermediate Operands

$$N_{solutions} = 2^d \cdot \left(\prod_{h=0}^{d} \#(hd = h)^{p(hd=h)} \right)^{\lceil \frac{N}{d} \rceil - 1}$$

Parameter	**N = 163**	**N = 256**
$d = 1$	$2^1 = 2^1$	$2^1 = 2^1$
$d = 2$	$2^2 2^{0.5\times 81} = 2^{42.5}$	$2^2 2^{0.5\times 127} = 2^{65.5}$
$d = 3$	$2^3 3^{0.75\times 54} = 2^{67.2}$	$2^3 3^{0.75\times 85} = 2^{104}$
$d = 4$	$2^4 4^{0.5\times 40} 6^{0.375\times 40} = 2^{82.8}$	$2^4 4^{0.5\times 63} 6^{0.375\times 63} = 2^{128.1}$

Revealing Intermediate Operands

- Correlate with an Arithmetic Combination of Intermediates $F = f(OpB^1, OpB^2, \ldots)$
- Attack Several Intermediates Simultaneously $F = f(OpB^1, OpB^2, \ldots)$
- Find the x-Coordinate
  $$x_i = X_r \cdot Z_r^{-1} = (\lambda X_i) \cdot (\lambda Z_i)^{-1} = X \cdot Z^{-1}$$
- Undo the Projective Coordinate Randomization $X_r = X \cdot \lambda$

Conclusion

- Investigated RFID-suitable ECC Hardware with
  - Montgomery Ladder
  - Randomized Projective Coordinates
  - Ephemeral Scalars
- Several Practical Attack Scenarios were Investigated
- **We do not recommend to use a bit-serial multiplier (d=1) for security-critical applications!**

Thank you...