

# Horizontal address-bit SCA attacks and countermeasures



Ievgen Kabin

Sensitive applications require algorithms resistant to side-channel analysis (SCA) attacks, especially when attackers have physical access to cryptographic devices. Highly regular Montgomery  $kP$  algorithm as well as  $kP$  algorithms based on the atomicity principle are in the literature reported as resistant against simple SCA attacks.

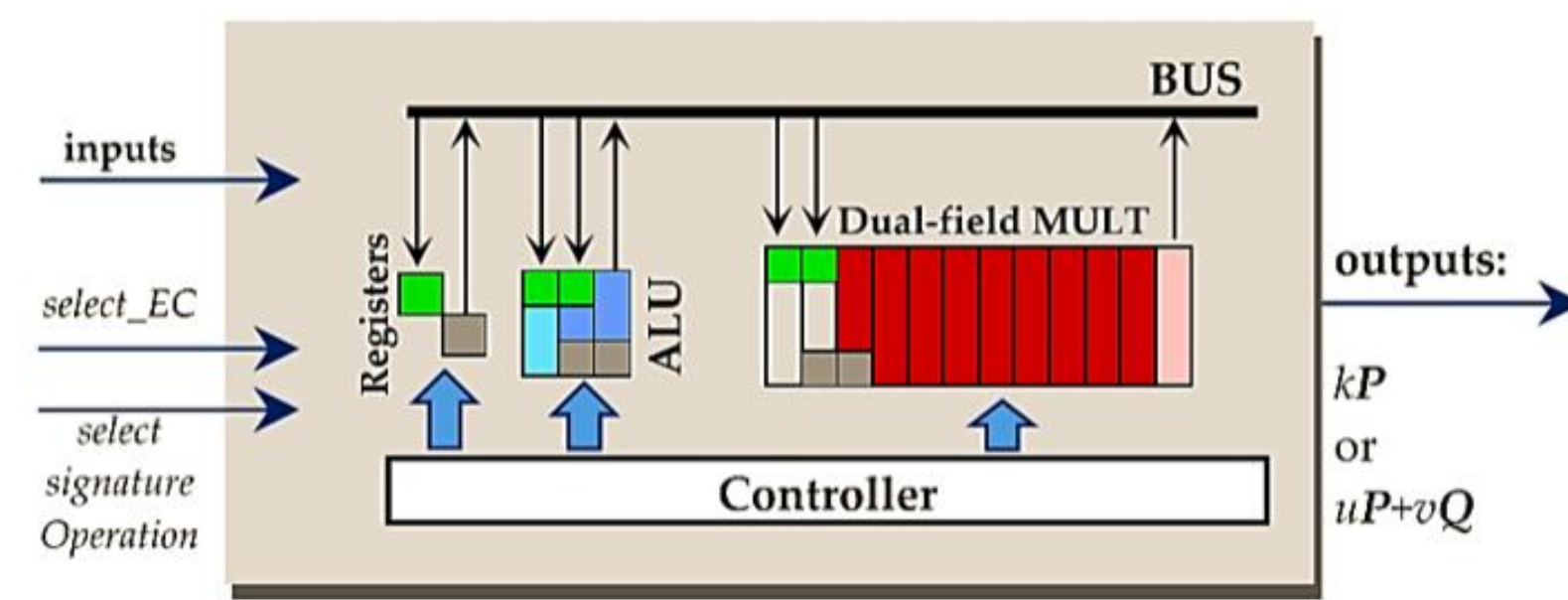
- “Provided that the writing in registers R0 and R1 (resp. that the squaring of registers R0 and R1) can-not be distinguished from a single side-channel measurement, the Montgomery ladder can be implemented to prevent a given [simple] side-channel attack.” M. Joye and S.-M. Yen, “The Montgomery Powering Ladder,” in *Cryptographic Hardware and Embedded Systems - CHES 2002*, Aug. 2002, pp. 291–302.
- “Implementations based on the Montgomery ladder [12]–[14], shown as Alg. 3, are protected against timing attacks and simple SCA since the execution time of the scalar multiplication is inherently unrelated to the Hamming weight of the secret scalar.” J. Fan, X. Guo, E. De Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, “State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures,” in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Jun. 2010, pp. 76–87.

## Montgomery $kP$ using projective Lopez-Dahab coordinates

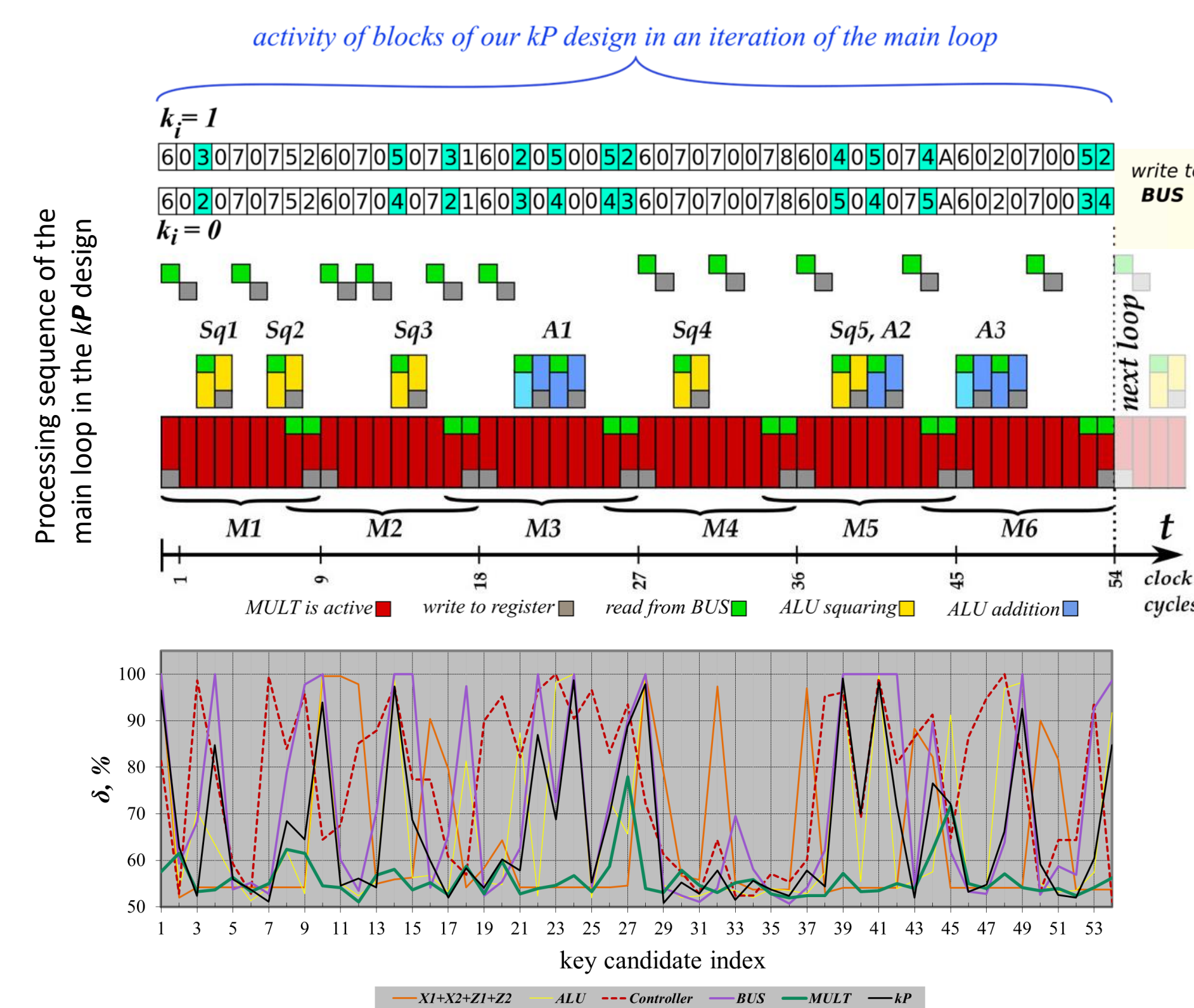
Input:  $k = (k_{l-1} \dots k_1 k_0)_2$  with  $k_{l-1} = 1$ ,  $P=(x,y)$  is a point of EC over  $GF(2^n)$

Output:  $kP = (x_1, y_1)$

- $X_1 \leftarrow x, Z_1 \leftarrow 1, X_2 \leftarrow x^4 + b, Z_2 \leftarrow x^2$
- for**  $i=l-2$  **down to** 0 **do**
- if**  $k_i=1$
- $T \leftarrow Z_1, Z_1 \leftarrow (X_1 Z_2 + X_2 T)^2, X_1 \leftarrow x Z_1 + X_1 X_2 T Z_2$
- $T \leftarrow X_2, X_2 \leftarrow T^4 + b Z_2^4, Z_2 \leftarrow T^2 Z_2^2$
- else**
- $T \leftarrow Z_2, Z_2 \leftarrow (X_2 Z_1 + X_1 T)^2, X_2 \leftarrow x Z_2 + X_1 X_2 T Z_1$
- $T \leftarrow X_1, X_1 \leftarrow T^4 + b Z_1^4, Z_1 \leftarrow T^2 Z_1^2$
- end if**
- end for**
- $x_1 \leftarrow X_1 / Z_1$
- $y_1 \leftarrow y + (x + x_1)[(X_1 + x Z_1)(X_2 + x Z_2) + (x^2 + y)(Z_1 Z_2)] / (x Z_1 Z_2)$
- return**  $(x_1, y_1)$



Structure of the investigated  $kP$  design



Horizontal attack using the comparison to the mean method: results of the analysis for the IHP basic  $kP$  design and its components synthesised for the IHP 250 nm technology.

## Key-dependent addressing of the registers and other design blocks is an inherent feature of binary $kP$ algorithms.

- This dependency was successfully exploited in the past by Itoh et al. in a vertical address-bit differential power analysis attack against Montgomery ladder.
- [The vulnerability of the Montgomery ladder against horizontal address-bit attacks was detected and demonstrated during our investigations.](#)

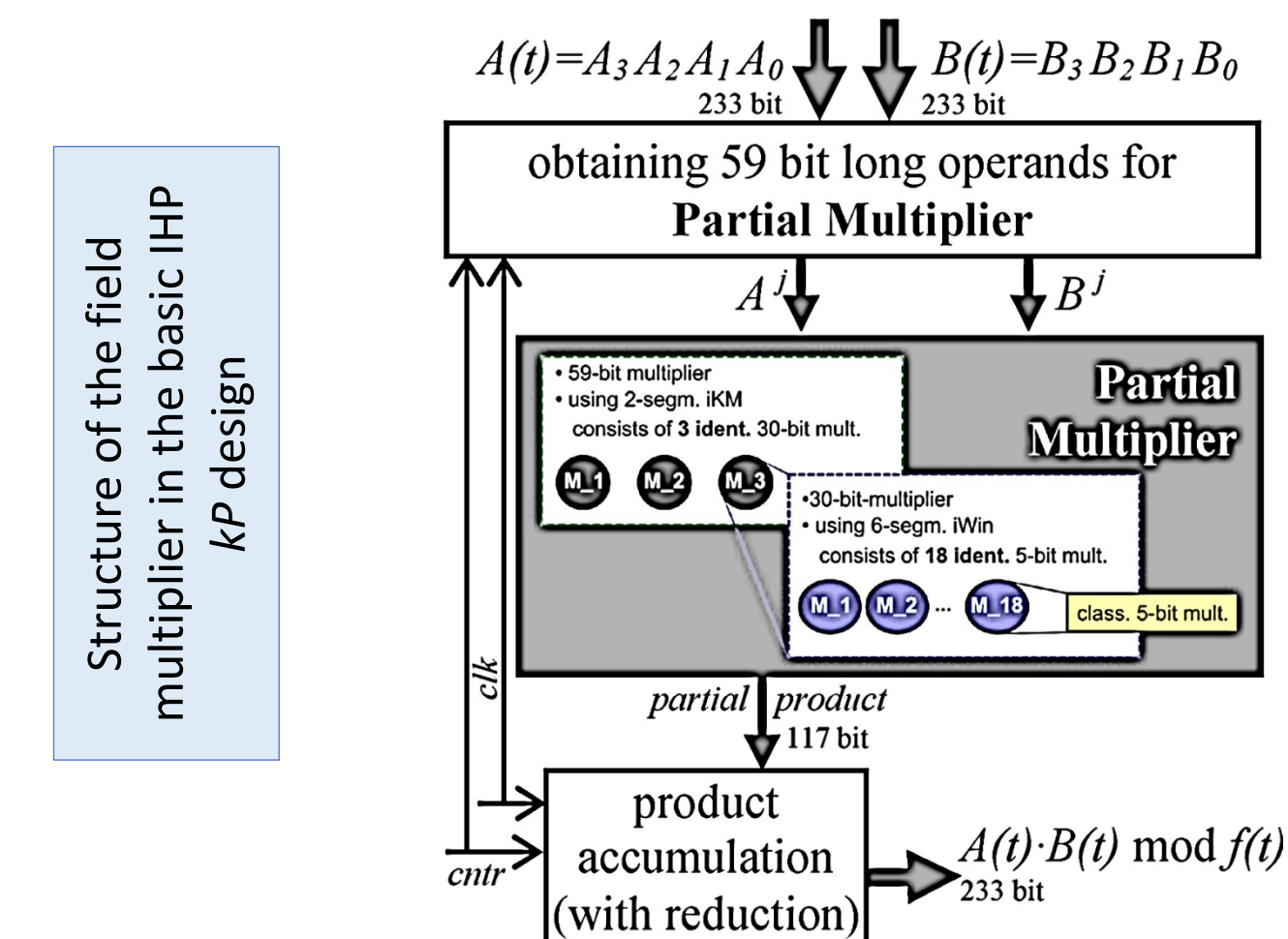
## State-of-the-art countermeasures are not effective against single-trace attacks, i.e. horizontal address-bit attacks:

- Well-known Coron’s countermeasures against vertical attacks – the EC point blinding, the randomization of the projective coordinates of the EC point and the randomisation of the scalar  $k$
- Randomization of the execution order of the operations in the main loop of the  $kP$  algorithm.
- GALS- design (Globally asynchronous locally synchronous)

## Proposed countermeasures

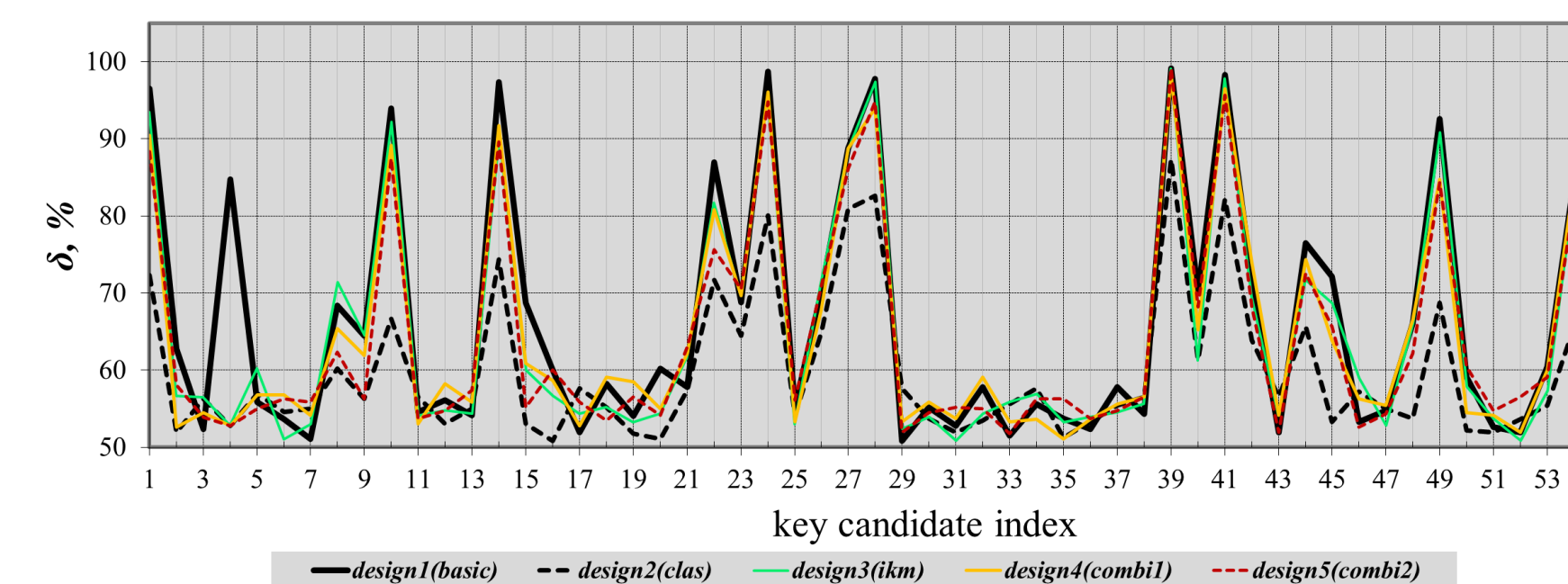
- Field Multiplier** activity as a means for hiding SCA leakages
  - the implemented formula for partial multiplication has a significant impact on the resistance of the  $kP$  design against horizontal attacks.
  - randomized sequence of partial multiplications
- Regular scheduling** for the addressing of the blocks of the design.

and their combination



## Implementation of the partial multiplier block of the $kP$ design:

- design1(basic)** - a combination of the 2-segment Karatsuba multiplication (IKM) formula, the 6-segment iterative Winograd MM and the classical MM for 5-bit long operands.
- design2(clas)** - using only the classical multiplication formula
- design3(ikm)** - 4-segment IKM formula applied for 60-bit long multiplicands + 4-segment IKM formula applied for 15-bit long multiplicands + 4-bit multipliers implemented using the classical multiplication formula
- design4(combi1)** - different combinations of the 3-segment iterative Winograd MM, the 4-segment iterative Karatsuba MM and the classical MM.
- design5(combi2)** - different combinations of the 3-segment iterative Winograd MM, the 4-segment iterative Karatsuba MM and the classical MM.



Iterative 4-segment Karatsuba Multiplication formula

$$A(t) \cdot B(t) = A_3 A_2 A_1 A_0 \cdot B_3 B_2 B_1 B_0 =$$

$$= A_0 B_0 \cdot 2^0 + (A_0 B_0 \oplus A_1 B_1 \oplus (A_0 \oplus A_1)(B_0 \oplus B_1)) \cdot 2^1 +$$

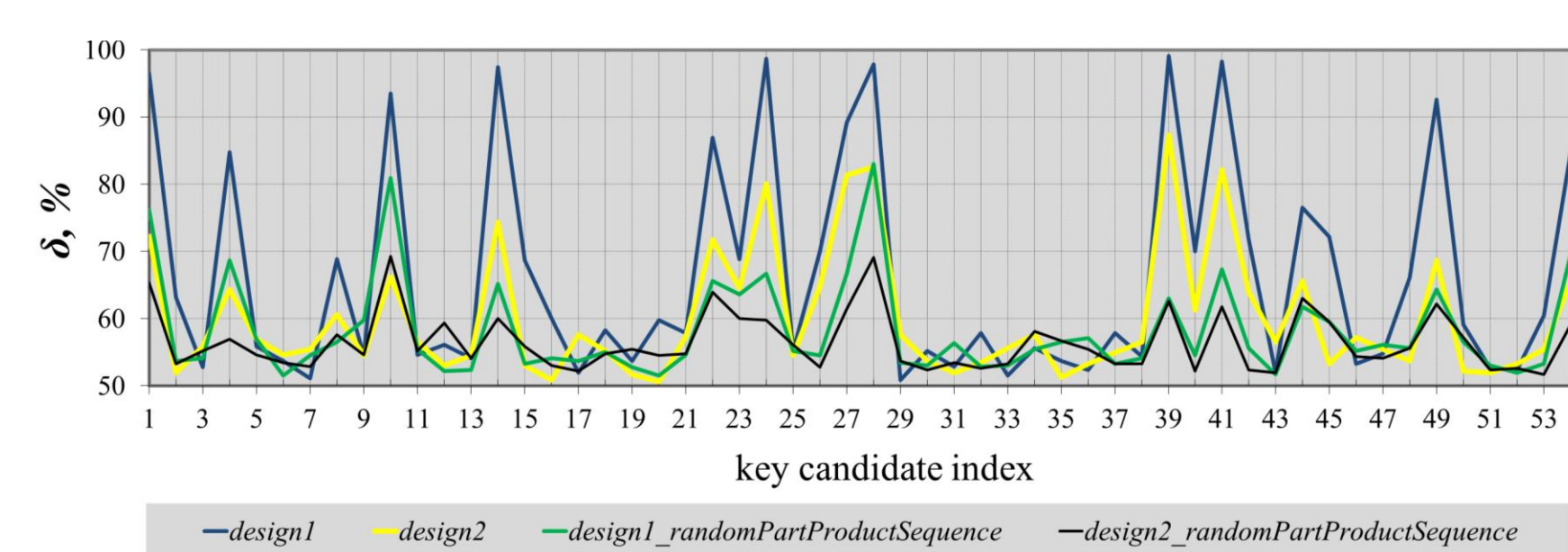
$$\oplus (A_0 B_0 \oplus A_1 B_1 \oplus A_2 B_2 \oplus (A_0 \oplus A_2)(B_0 \oplus B_2)) \cdot 2^2 +$$

$$\oplus (A_0 \oplus A_1 \oplus A_2 \oplus A_3)(B_0 \oplus B_1 \oplus B_2 \oplus B_3) \cdot 2^3 +$$

$$\oplus (A_1 B_1 \oplus A_2 B_2 \oplus A_3 B_3 \oplus (A_1 \oplus A_2)(B_1 \oplus B_2)) \cdot 2^4 +$$

$$\oplus (A_2 B_2 \oplus A_3 B_3 \oplus (A_2 \oplus A_3)(B_2 \oplus B_3)) \cdot 2^5 + A_3 B_3 \cdot 2^6$$

- clock cycle 1:  $PP\_1 = A_0 B_0$   
 clock cycle 2:  $PP\_2 = A_1 B_1$   
 clock cycle 3:  $PP\_3 = A_2 B_2$   
 clock cycle 4:  $PP\_4 = A_3 B_3$   
 clock cycle 5:  $PP\_5 = (A_0 \oplus A_1)(B_0 \oplus B_1)$   
 clock cycle 6:  $PP\_6 = (A_0 \oplus A_2)(B_0 \oplus B_2)$   
 clock cycle 7:  $PP\_7 = (A_1 \oplus A_2)(B_1 \oplus B_2)$   
 clock cycle 8:  $PP\_8 = (A_2 \oplus A_3)(B_2 \oplus B_3)$   
 clock cycle 9:  $PP\_9 = (A_0 \oplus A_1 \oplus A_2 \oplus A_3)(B_0 \oplus B_1 \oplus B_2 \oplus B_3)$
- 9! permutations

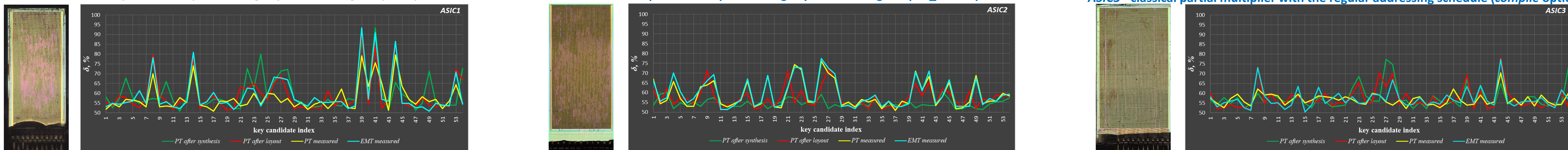


With the goal to evaluate the efficiency of the proposed countermeasures practically, i.e. analysing measured traces, some designs were selected for manufacturing in the IHP 250 nm technology.

ASIC1 - classical partial multiplier + design synthesis using compile option

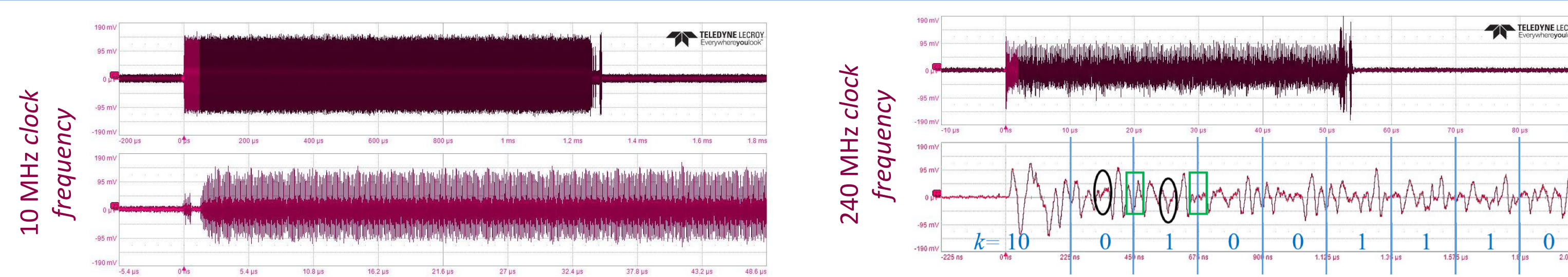
ASIC2 - classical partial multiplier + design synthesis using compile\_ultra option

ASIC3 - classical partial multiplier with the regular addressing schedule (compile option)



Results of the comparison to the mean attack applied to the simulated compressed power traces after the synthesis, after layout, as well as to the compressed measured power trace and electromagnetic trace

- The resistance of the same implementation, i.e. the same VHDL code, depends significantly on the operating frequency for each investigated target platform. This means that designers have to evaluate the resistance of their implementations for each target frequency and implement mechanisms that prevent attackers from running the designs at any other frequency.
- The resistance of the same implementation, i.e. the same VHDL code, depends significantly on the applied synthesis options



Screenshots of the captured traces of the  $kP$  execution on an FPGA

- The key-dependent addressing of the registers or other design blocks is an intrinsic feature, not only of the Montgomery ladder, but also of binary  $kP$  algorithms based on the atomicity principle.
- We showed that the application of the Montgomery ladder as well as atomic patterns not sufficient to prevent simple SCA attacks. The source of the leakage is related to the key-dependent addressing of design blocks/registers, i.e. the assumption about the indistinguishability of the addressing of the design blocks/registers has to be revised (for hardware implementations).
- The noise produced by the activity of the field multiplier can reduce the success of applied attacks and therefore increase the inherent resistance of the whole design.
- We proposed regular scheduling for the addressing of the blocks of the design. This approach is an effective strategy for reducing the success of horizontal attacks in all clock cycles in which it is applicable. Combining this approach with hiding features of the field multipliers can increase the resistance of the design significantly.
- Usage of the same RTL code synthesized for different cell libraries leads to completely different outcomes from the design’s side-channel resistance perspective, even for the same technology node.
- Proposed analysis methods such as the comparison to the mean, an automated simple SCA analysis and statistical analysis in the frequency domain can be very effective means for attackers. Designers can benefit from these approaches as well since they can be successfully applied to determine SCA leakage sources in early design phases.

