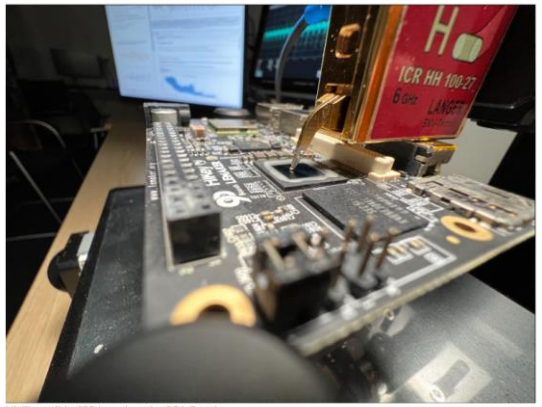
Balancing Performance and Side-Channel Resilience in a Lightweight ECC Cryptosystem

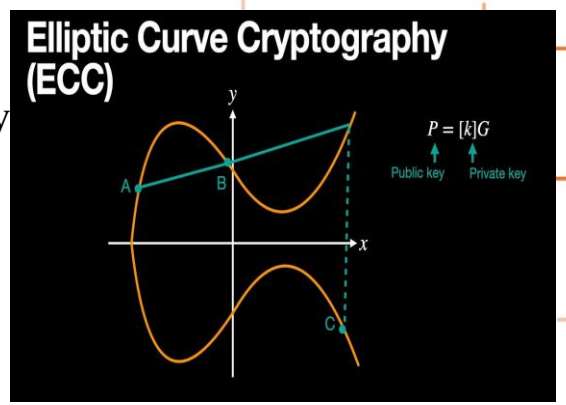
Harikrishnan Balagopal, Lang Lin, Norman Chang, Ansys Inc.
Mitra Mirhassani, Seyedeh Nejati University of Windsor

SPONSORED BY CEDA IEEE Council on Electronic Design Automation sigda acm

Motivation:

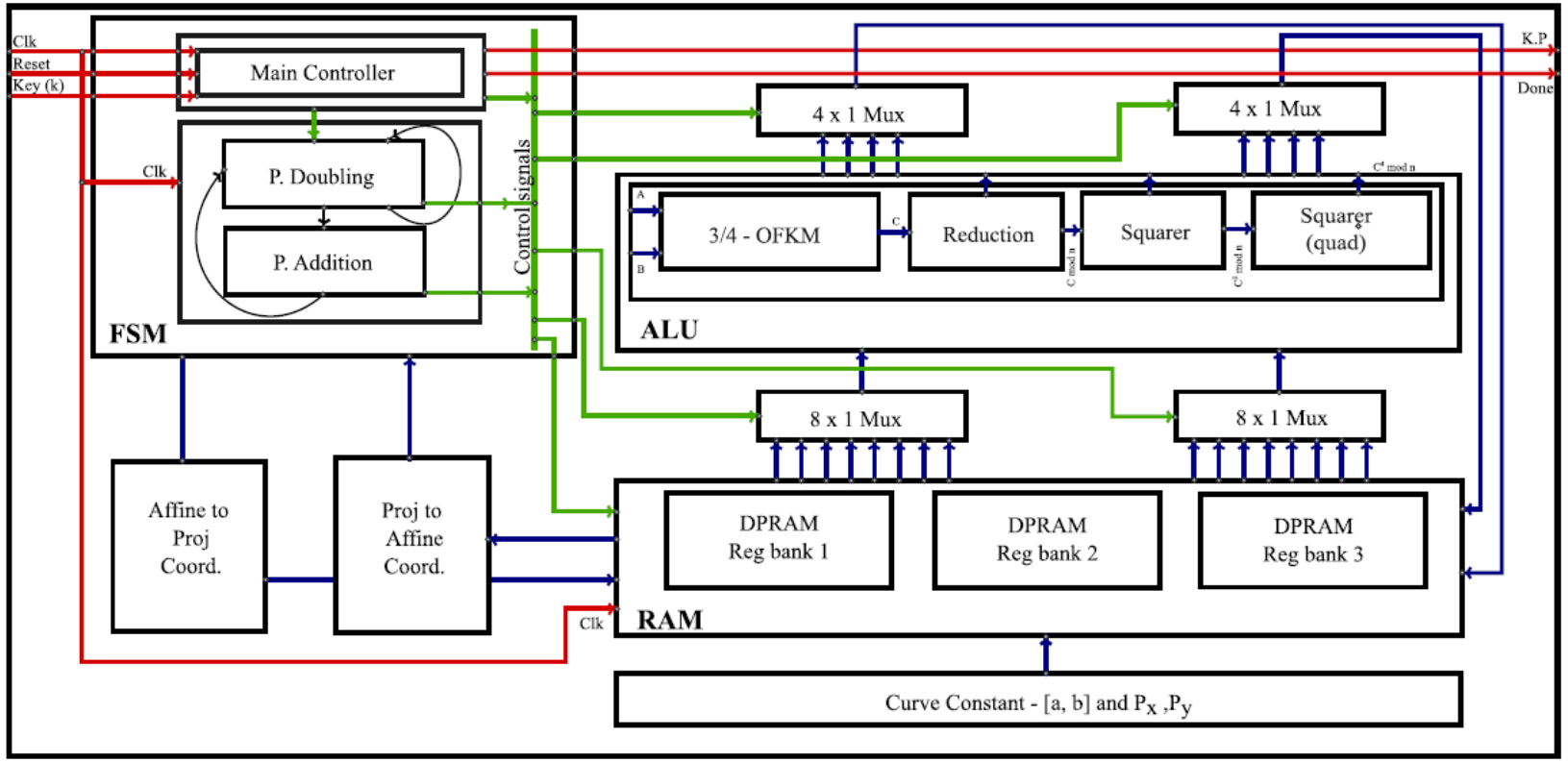
- Elliptic Curve Cryptography (ECC) is a lightweight and secure encryption method well-suited for IoT devices, offering effective data protection.
- Custom digital ECC implementations on FPGAs or ASICs provide superior performance compared to general-purpose architectures, leveraging optimized algorithms for primitive operations.
- This study introduces advanced binary polynomial multipliers using an enhanced four-term overlap-free Karatsuba algorithm, improving ECC processor efficiency for lightweight cryptosystems.
- The implementation of the proposed ECC has been fully validated by power side-channel leakage analysis to root-cause design weakness and improve the security at the early RTL design stage


Hisilicon Kirin 620 board on the SCA Bench



Main Idea: ECC Scalar Multiplication Unit Design

- We developed and tested improved digit-parallel recursive multipliers using an optimized Karatsuba recurrence approach.
- To reduce the subquadratic complexity, eliminate the unnecessary zero padding for the proposed four-term OFKM recurrence; an effective implementation technique was used by employing the four-term Karatsuba multipliers (KM) on the final recurrence.
- We conducted an experimental evaluation of the constructed ECC processor using Xilinx FPGAs for elliptic curves recommended by standards, such as B-163 and B-233.

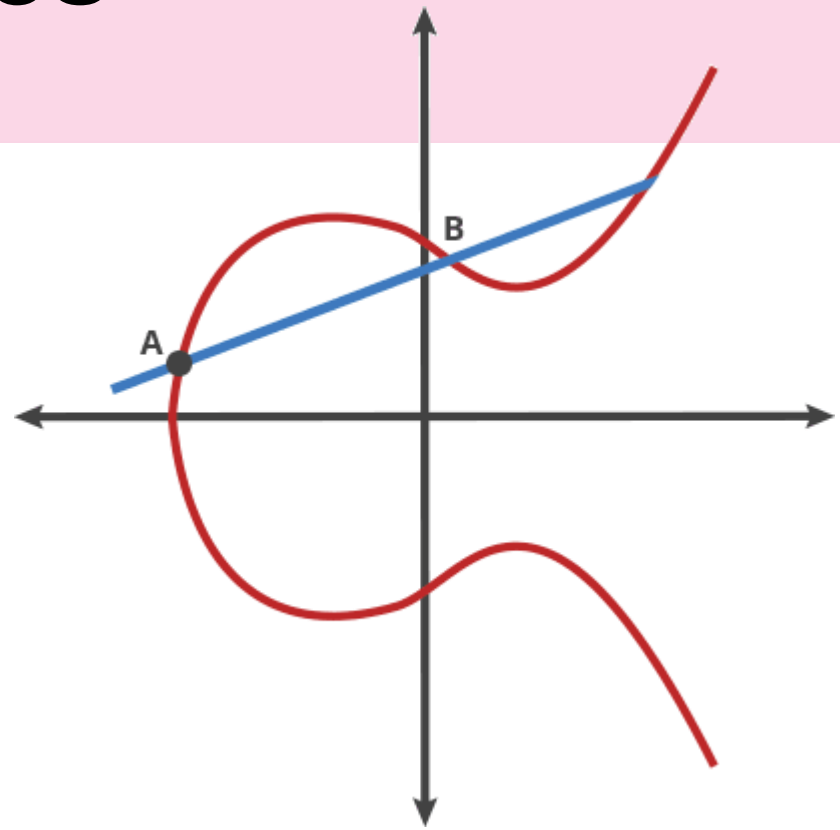


Elliptic Curve Crypto Basics

Find k from: $2 = 2^k$

$2 = 2^k \bmod 234$

- Public key crypto based on difficulty to solve discrete logarithm problem
  - Given a starting point P on an EC known to all
  - Use a private key k to get public key Q=k P=(P dot P) dot P..
  - Trapdoor function: easy to get Q from k and P, but computationally impossible to get k from Q and P
  - Public key to encrypt, and private key to decrypt

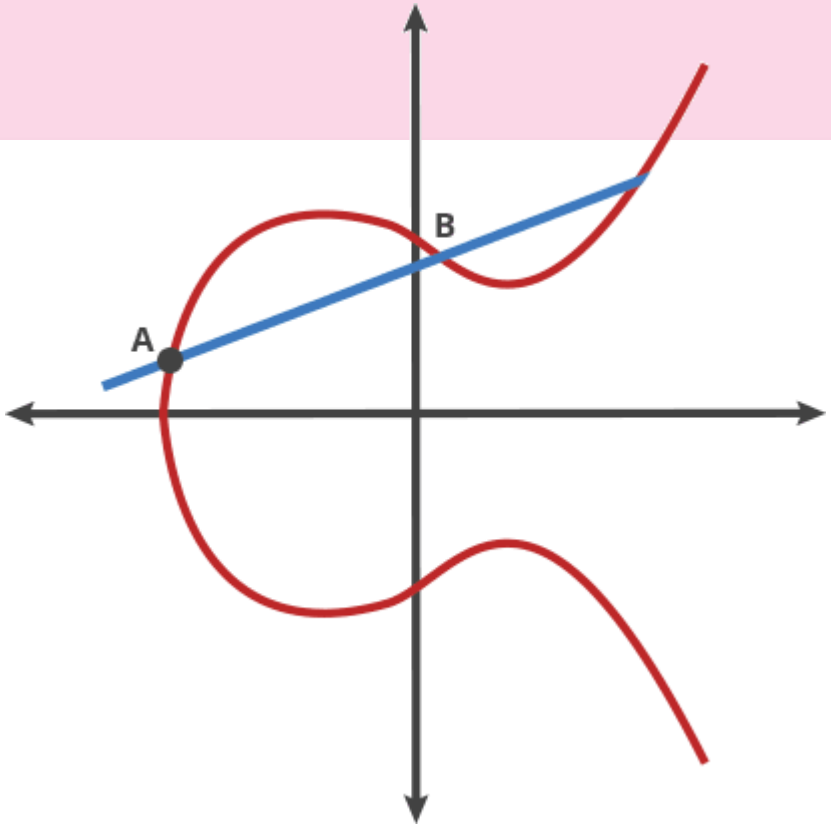


Example of EC: $y^2 = x^3 + ax + b \pmod p$ where p is a large prime number

Elliptic Curve Crypto Basics

ECC implementation on silicon is challenging

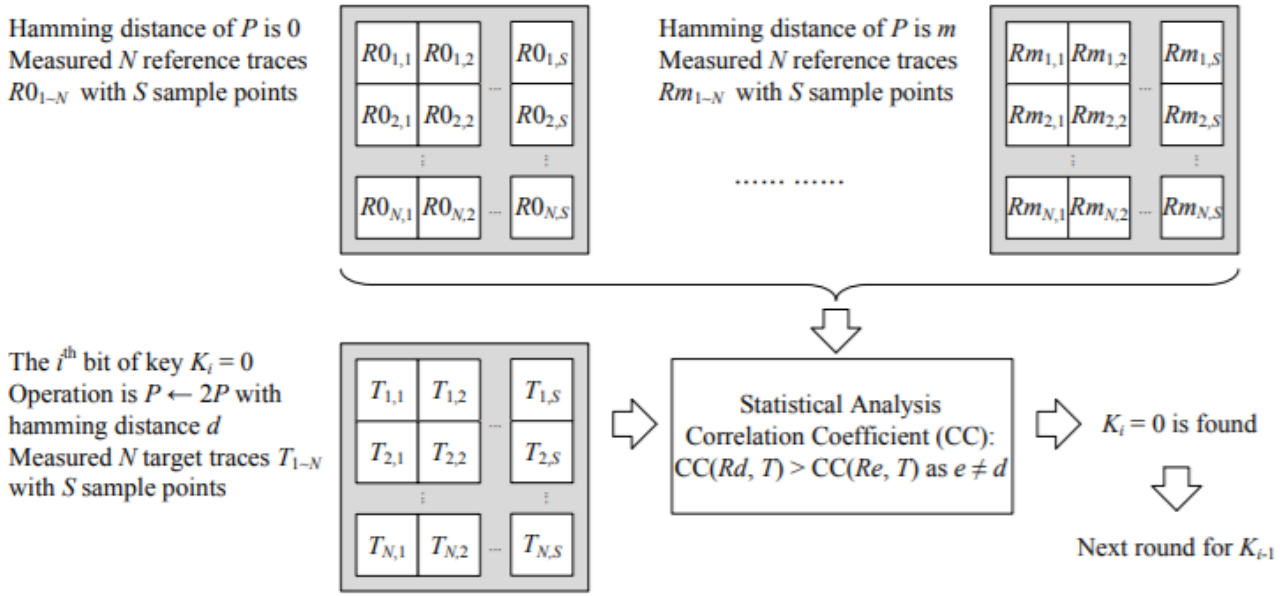
- Longer key is more secure, but with implementation costs!
- “Side-Channel” of ECC implementation:
  - point-addition and point-double shows different timing/power signatures during k dot P operation
  - For all bits in k, point-add will be executed only if the bit is one.
  - Example for private key 1001: PA+PD -> PD -> PD -> PA+PD
- Countermeasures: random coordinates, constant time arithmetic, random curve isomorphism, point blinding, side-channel atomicity…



Example of EC: $y^2 = x^3 + ax + b \pmod p$ where p is a large prime number

Countermeasure Example against CPA

- Add-and-double would disclose the key value of 0/1 bit-by-bit with correlation power analysis
- Montgomery ladder ECSM algorithm: ALWAYS add and double
- Advanced algorithms with randomization operations proposed later



Algorithm 1 Montgomery ladder ECSM algorithm

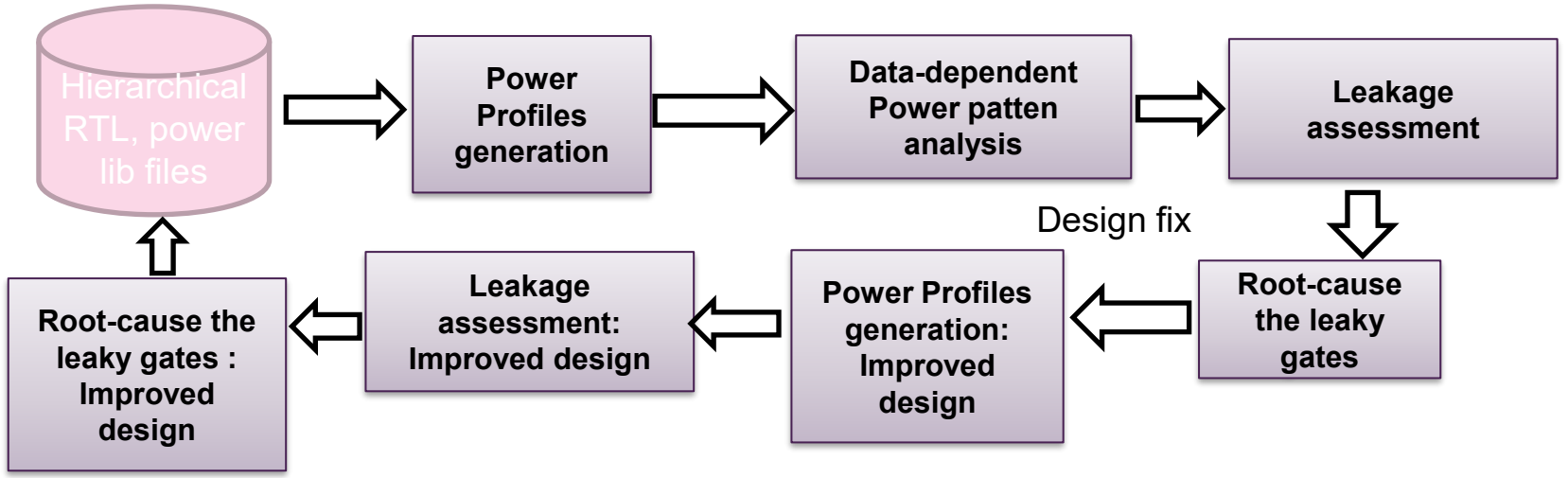
Input: K and P
Output: KP
1. Let $P_1 \leftarrow P$, $P_2 \leftarrow 2P$
2. **For** i from $m-2$ to 0 **do**
3. **If** $K_i = 1$ **then** $P_1 \leftarrow P_1 + P_2, P_2 \leftarrow 2P_2$
4. **else** $P_2 \leftarrow P_1 + P_2, P_1 \leftarrow 2P_1$
5. **Return** P_1

"An Efficient Countermeasure against Correlation Power-Analysis Attacks with Randomized Montgomery Operations for DF-ECC Processor", CHES 2012.

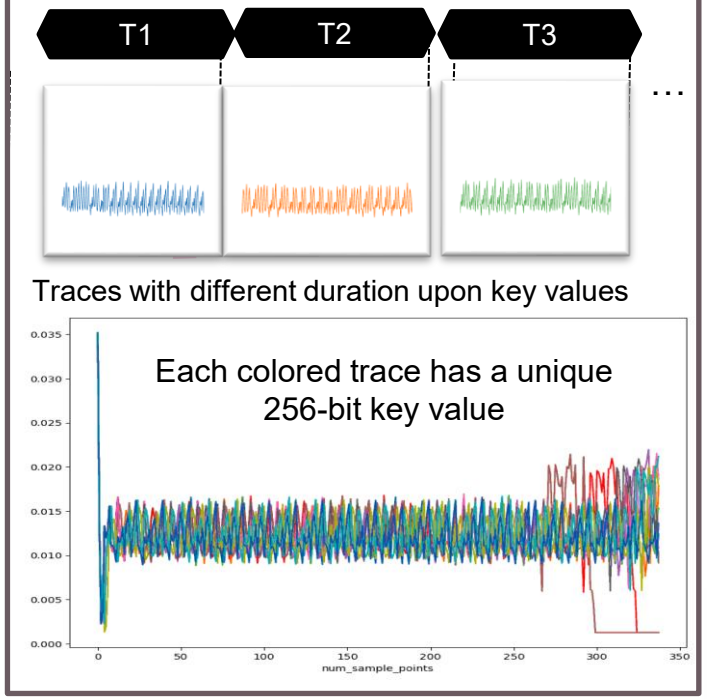
Main Idea: Security Verification for ECC Crypto

Different implementations of the proposed ECC multiplier can imply different security vulnerabilities. We propose a fast and comprehensive RTL power side-channel analysis flow to assess the design resistance to side-channel leakage

1. Power Profile Generation: Cycle-accurate RTL/gate power profiling to get power side-channel traces with different ECC key and input values.
2. Data-dependent power pattern analysis: This is to align the starting time of each transaction with the same operating cycle and identify any cycle with observable power patterns
3. Leakage Assessment: Apply side channel leakage model to assess potential key leakage such as T-Score
4. Root-cause analysis: Given the time and power value, find critical RTL gates to be fixed for enhanced security
5. Design Fix: Enhanced design is undergone the same procedure to analyses the T-score.

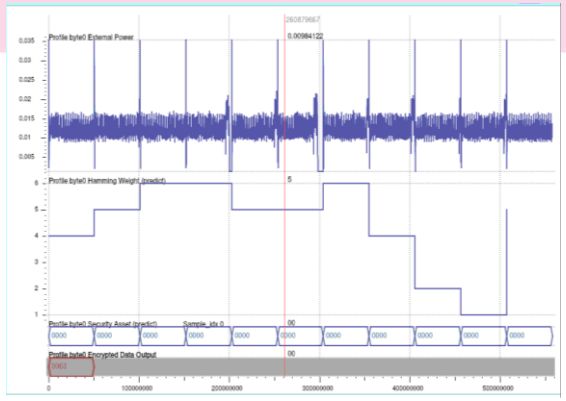


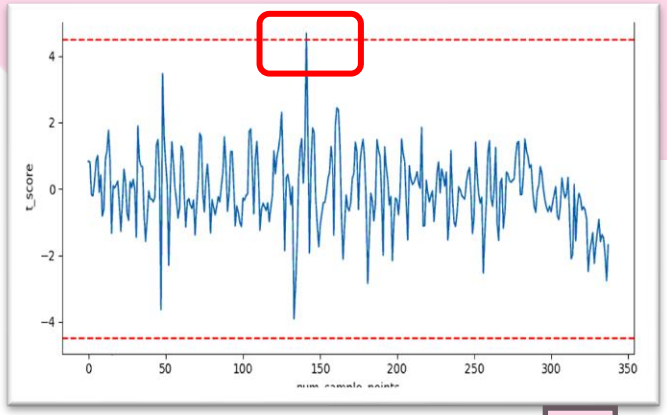
Evidence: Key disclosure, T-score and Root-cause



Traces with different duration upon key values

Key-dependent pattern identified after alignment



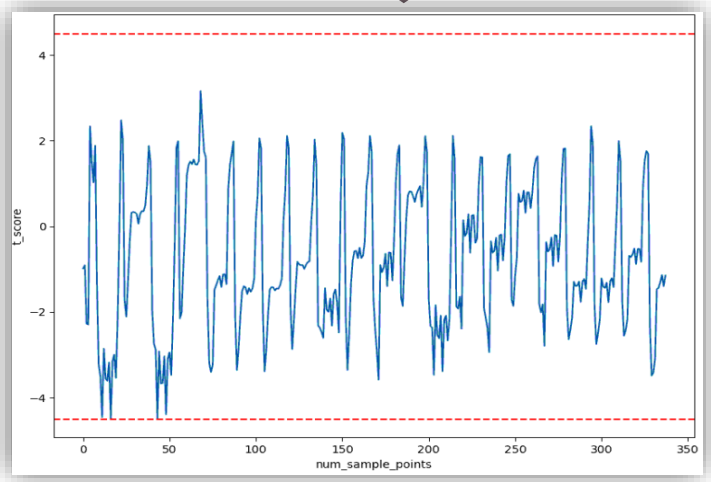


The leakage model to analyze the ECC Multiplier was able to solve T-score with 338 traces to find leakage time

```
always @(state) begin
        case(state)
        6'd0: begin
                cwl <= 10'h000;
                cwh <= 23'h4x8484;
        end
        6'd1: begin
                cwl <= 10'h000;
                cwh <= 23'h4x808D;
        end
```

Root-cause the FSM with case conditions to be leaky, with power consumed by cwh flops

- **Implemented time equalization logic** by inserting dummy, make execution time independent of key bit patterns.
- **Redesigned FSM transitions and aligned computation steps** to ensure uniform control flow.



The leakage model to analyze the ECC Multiplier was able to solve T-score with 338 traces.

Summary

- Pre-silicon security verification flow is essential for semiconductor industry, particularly for crypto design implementation like ECC.
- A Proposal of EDA flow for side-channel trace generation, leakage assessment and root-cause analysis for ECC Multiplier design, with scalable performance and comprehensive coverage of leakage to mitigate power side-channel vulnerabilities.
- A demonstration of the security verification flow can identify the leakage source from the RTL code of the Finite State Machine (FSM), which needs design countermeasures.
- A countermeasure was introduced as an improved version of the design which proved an enhanced performance while analyzing T-score.
- Our future work includes the design PPA and security trade-off study of several optimization versions of the ECC cryptosystem.

AI

Security

Systems

EDA

Design

62 THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation

sigda acm