Revisiting the Security of LPN based RFID Authentication Protocol and Potential Exploits in Hardware Implementations

Krishna Bagadia, **Urbi Chatterjee**, Debapriya Basu Roy, Debdeep Mukhopadhyay, and Rajat Subhra Chakraborty

Secure Embedded Architecture Laboratory (SEAL)
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur, India

Motivation

- RFID Authentication Protocols

Motivation

- RFID Authentication Protocols
- Hopper and Blum (HB): Learning Parity with Noise (LPN) problem

Motivation

- RFID Authentication Protocols
- Hopper and Blum (HB): Learning Parity with Noise (LPN) problem
- HB^{+}, HB^{++}, $HB^{\#}$, HB-MP, $HB\text{-}MP^{+}$, HB-MAC, PUF-HB, HB+PUF, Tree-LSHB++, Trusted-HB, $GHB^{\#}$, LAPIN

Motivation

- RFID Authentication Protocols
- Hopper and Blum (HB): Learning Parity with Noise (LPN) problem
- HB^{+}, HB^{++}, $HB^{\#}$, HB-MP, $HB\text{-}MP^{+}$, HB-MAC, PUF-HB, HB+PUF, Tree-LSHB++, Trusted-HB, $GHB^{\#}$, LAPIN
- Cryptanalysis techniques, Man-in-the-middle and side-channel analysis (SCA) to deploy cogent attacks

Motivation

- RFID Authentication Protocols
- Hopper and Blum (HB): Learning Parity with Noise (LPN) problem
- HB^{+}, HB^{++}, $HB^{\#}$, HB-MP, $HB\text{-}MP^{+}$, HB-MAC, PUF-HB, HB+PUF, Tree-LSHB++, Trusted-HB, $GHB^{\#}$, LAPIN
- Cryptanalysis techniques, Man-in-the-middle and side-channel analysis (SCA) to deploy cogent attacks
- LCMQ[1]: consolidation of LPN, Circulant Matrix and Multivariate Quadratic (MQ) problem

[1] Z. Li, G. Gong, and Z. Qin, "Secure and Efficient LCMQ Entity Authentication Protocol," IEEE Trans. Information Theory, vol. 59, no. 6, pp. 40424054, 2013.

Motivation

- Security analysis of LPN based implementations against fault attacks is hard: inherently possess an algebraic structure, resist against such attacks.

Motivation

- Security analysis of LPN based implementations against fault attacks is hard: inherently possess an algebraic structure, resist against such attacks.
- Flipping of intermediate variable does not provide any information leakage, key retrieval is hard

Motivation

- Security analysis of LPN based implementations against fault attacks is hard: inherently possess an algebraic structure, resist against such attacks.
- Flipping of intermediate variable does not provide any information leakage, key retrieval is hard
- Hardware Trojan Horse: accurate fault injection in the circuit or for side channel

Objectives

- Security Evaluation of LCMQ: **although the authentication uses two keys, knowledge of only one key is sufficient to impersonate as a legitimate tag**

Objectives

- Security Evaluation of LCMQ: **although the authentication uses two keys, knowledge of only one key is sufficient to impersonate as a legitimate tag**
- Demonstration of Security Evaluations:
  - Lightweight hardware architecture of LCMQ authentication protocol on an FPGA platform

Objectives

- Security Evaluation of LCMQ: **although the authentication uses two keys, knowledge of only one key is sufficient to impersonate as a legitimate tag**
- Demonstration of Security Evaluations:
  - Lightweight hardware architecture of LCMQ authentication protocol on an FPGA platform
  - HTH based fault attack methodology which leaks one of the authentication keys

Objectives

- Security Evaluation of LCMQ: **although the authentication uses two keys, knowledge of only one key is sufficient to impersonate as a legitimate tag**
- Demonstration of Security Evaluations:
  - Lightweight hardware architecture of LCMQ authentication protocol on an FPGA platform
  - HTH based fault attack methodology which leaks one of the authentication keys
  - Demonstrate the use of HTH to induce precise fault attack.

Objectives

- Security Evaluation of LCMQ: **although the authentication uses two keys, knowledge of only one key is sufficient to impersonate as a legitimate tag**
- Demonstration of Security Evaluations:
  - Lightweight hardware architecture of LCMQ authentication protocol on an FPGA platform
  - HTH based fault attack methodology which leaks one of the authentication keys
  - Demonstrate the use of HTH to induce precise fault attack.
  - Less than 2^8 rounds of protocol run to guess the key and forge the authentication

LPN Problem

- Let A be a random $(l \times m)$-binary matrix
- $\mathcal{K}$ be a random m-bit vector
- $\epsilon \in (0, \frac{1}{2})$ be a noise parameter
- $\mathcal{V}$ be a random l-bit vector such that $\mathrm{Hwt}(\mathcal{V}) \leq \epsilon \times l$.

LPN Problem

- Let A be a random $(l \times m)$-binary matrix
- $\mathcal{K}$ be a random m-bit vector
- $\epsilon \in (0, \frac{1}{2})$ be a noise parameter
- $\mathcal{V}$ be a random l-bit vector such that $\text{Hwt}(\mathcal{V}) \leq \epsilon \times l$.
- **LPN Problem:** Given A, ϵ, and $\mathbf{z} = < A \cdot \mathcal{K}^t > \oplus \mathcal{V}^t$, find a k-bit vector $\mathbf{y^t}$ such that $\text{Hwt}(< A \cdot \mathbf{y^t} > \oplus \mathbf{z}) \leq \epsilon \times l$.

LPN Problem

- Let A be a random $(l \times m)$-binary matrix
- $\mathcal{K}$ be a random m-bit vector
- $\epsilon \in (0, \frac{1}{2})$ be a noise parameter
- $\mathcal{V}$ be a random l-bit vector such that $\text{Hwt}(\mathcal{V}) \leq \epsilon \times l$.
- **LPN Problem:** Given A, ϵ, and $\mathbf{z} = < A \cdot \mathcal{K}^t > \oplus \mathcal{V}^t$, find a k-bit vector $\mathbf{y^t}$ such that $\text{Hwt}(< A \cdot \mathbf{y^t} > \oplus \mathbf{z}) \leq \epsilon \times l$.
- This problem is proven to be NP-Hard and the key length m and the noise level ϵ decides the security of the problem instances.

LPN Problem

- Let A be a random $(l \times m)$-binary matrix
- $\mathcal{K}$ be a random m-bit vector
- $\epsilon \in (0, \frac{1}{2})$ be a noise parameter
- $\mathcal{V}$ be a random l-bit vector such that $\text{Hwt}(\mathcal{V}) \leq \epsilon \times l$.
- **LPN Problem:** Given A, ϵ, and $\mathbf{z} =< A \cdot \mathcal{K}^t > \oplus \mathcal{V}^t$, find a k-bit vector $\mathbf{y^t}$ such that $\text{Hwt}(< A \cdot \mathbf{y^t} > \oplus \mathbf{z}) \leq \epsilon \times l$.
- This problem is proven to be NP-Hard and the key length m and the noise level ϵ decides the security of the problem instances.
- For 80-bit security, m and ϵ are set to 512 and 0.25.

Circulant-P2 Matrix

Given $n < m$, a circulant-P2 matrix is an $(m \times m)$ square circulant matrix, or an $(n \times m)$ landscape circulant matrix, or an $(m \times n)$ portrait circulant matrix, satisfying the below criteria.

1. It must be a binary matrix.
2. m is a prime number such that 2 is a primitive element of the finite field $\mathbb{F}_m$. Here, m is defined as a *P2 number*.
3. No row vector and column vector of a Circulant-P2 matrix can be all zeroes or all ones.

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & $\mathrm{Hwt}(\mathbf{a})$ is even$\}$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$
5. **LCMQ Problem**:

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$
5. **LCMQ Problem**:
   - Given l pairs of $(\mathbf{b_i}, \mathbf{z_i} = (((\mathbf{b_i} \cdot C_{\mathbf{K_1}}^{[m \times n]}) \oplus \mathbf{v_i}) || \mathbf{r_i}) \cdot C_{\mathbf{K_2}}^{[(m-1) \times m]}), \forall i \in \{0, \cdots, l-1\}$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$
5. **LCMQ Problem**:
   - Given l pairs of $(\mathbf{b_i}, \mathbf{z_i} = (((\mathbf{b_i} \cdot C_{\mathbf{K_1}}^{[m \times n]}) \oplus \mathbf{v_i}) || \mathbf{r_i}) \cdot C_{\mathbf{K_2}}^{[(m-1) \times m]}), \forall i \in \{0, \cdots, l-1\}$
   - where $\mathbf{b_i} \in_R \{0,1\}^m$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$
5. **LCMQ Problem**:
   - Given l pairs of $(\mathbf{b_i}, \mathbf{z_i} = (((\mathbf{b_i} \cdot C_{\mathbf{K_1}}^{[m \times n]}) \oplus \mathbf{v_i}) || \mathbf{r_i}) \cdot C_{\mathbf{K_2}}^{[(m-1) \times m]}), \forall i \in \{0, \cdots, l-1\}$
   - where $\mathbf{b_i} \in_R \{0,1\}^m$
   - $\Pr[\mathbf{v_i}[j] = 1] = \epsilon$, $\Pr[\mathbf{v_i}[j] = 0] = (1 - \epsilon)$ $\forall 0 \leq j \leq n-1$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$
5. **LCMQ Problem**:
   - Given l pairs of $(\mathbf{b_i}, \mathbf{z_i} = (((\mathbf{b_i} \cdot C_{\mathbf{K_1}}^{[m \times n]}) \oplus \mathbf{v_i}) || \mathbf{r_i}) \cdot C_{\mathbf{K_2}}^{[(m-1) \times m]}), \forall i \in \{0, \cdots, l-1\}$
   - where $\mathbf{b_i} \in_R \{0,1\}^m$
   - $\Pr[\mathbf{v_i}[j] = 1] = \epsilon$, $\Pr[\mathbf{v_i}[j] = 0] = (1-\epsilon)$ $\forall 0 \leq j \leq n-1$
   - $\mathbf{r_i} \in_R \{0,1\}^{m-n-1}$

LCMQ Problem

1. $\mathcal{E} = \{\mathbf{a} | \mathbf{a} \in \{\{0,1\}^m \setminus \{\{0\}^m,\ \{1\}^m\}\}$ & Hwt($\mathbf{a}$) is even$\}$
2. For m-bit binary vector α, $C_\alpha$is a square circulant matrix of order $m \times m$ with first row as α
3. m be a P2 number, $\epsilon \in (0, \frac{1}{2})$
4. $\mathbf{K_1} \in_R \{0,1\}^m$, parity of Hwt of $\mathbf{K_1}$ is publicly known, $\mathbf{K_2} \in_R \mathcal{E}$
5. **LCMQ Problem**:
   - Given l pairs of $(\mathbf{b_i}, \mathbf{z_i} = (((\mathbf{b_i} \cdot C_{\mathbf{K_1}}^{[m \times n]}) \oplus \mathbf{v_i}) || \mathbf{r_i}) \cdot C_{\mathbf{K_2}}^{[(m-1) \times m]}), \forall i \in \{0, \cdots, l-1\}$
   - where $\mathbf{b_i} \in_R \{0,1\}^m$
   - $\Pr[\mathbf{v_i}[j] = 1] = \epsilon$, $\Pr[\mathbf{v_i}[j] = 0] = (1-\epsilon)$ $\forall 0 \leq j \leq n-1$
   - $\mathbf{r_i} \in_R \{0,1\}^{m-n-1}$
   - determine $\mathbf{K_1}$ and $\mathbf{K_2}$

Mapping to Multivariate Quadratic (MQ) Problem

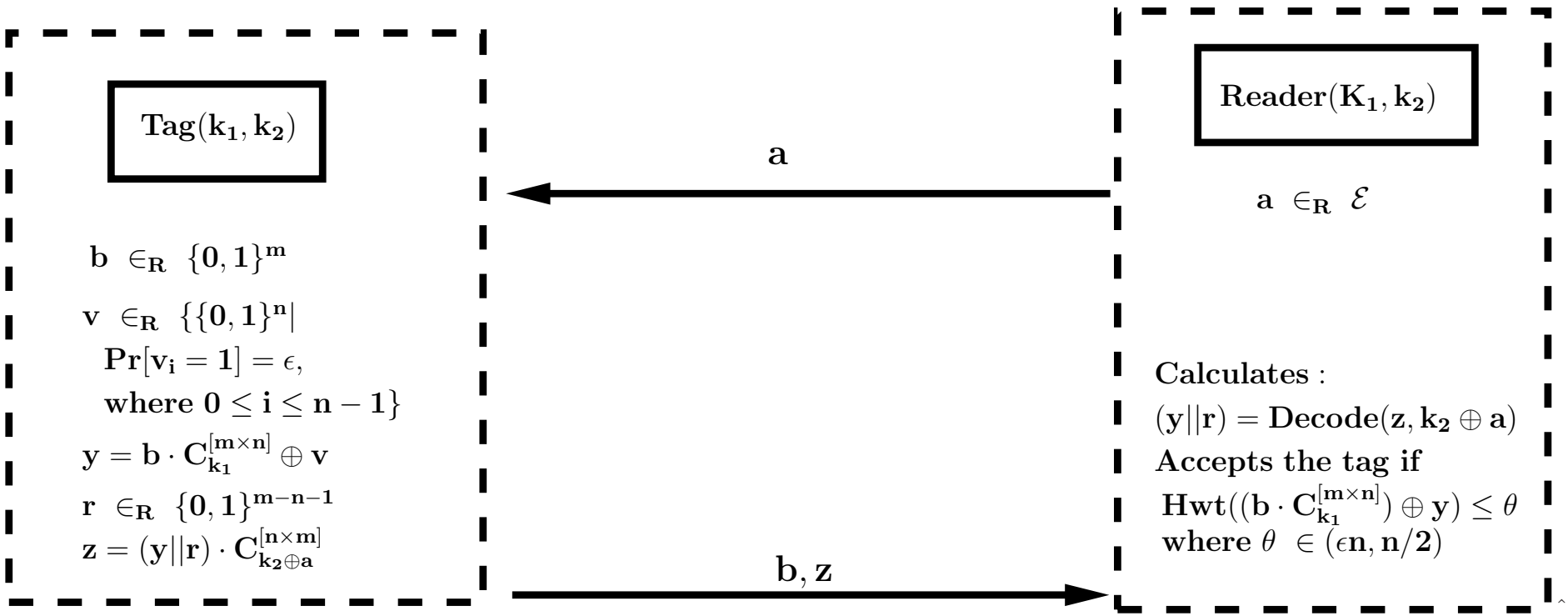
If $n = m - 1$ and there is no noise, the problem reduces to finding K_1 and K_2 such that:

$$(\mathbf{b_i} \in_R \{0,1\}^m, \mathbf{z'_i} = (\mathbf{b_i} \cdot C_{\mathbf{K_1}}^{[m \times n]}) \cdot C_{\mathbf{K_2}}^{[(m-1) \times m]})$$

This problem is an instance of MQ problem in $2(m-1)$ variants, known to be NP-complete.

MQ Problem: Given a system of d multivariate quadratic equations in t variables over a finite field, find a valid solution satisfying all equations.

The LCMQ Protocol



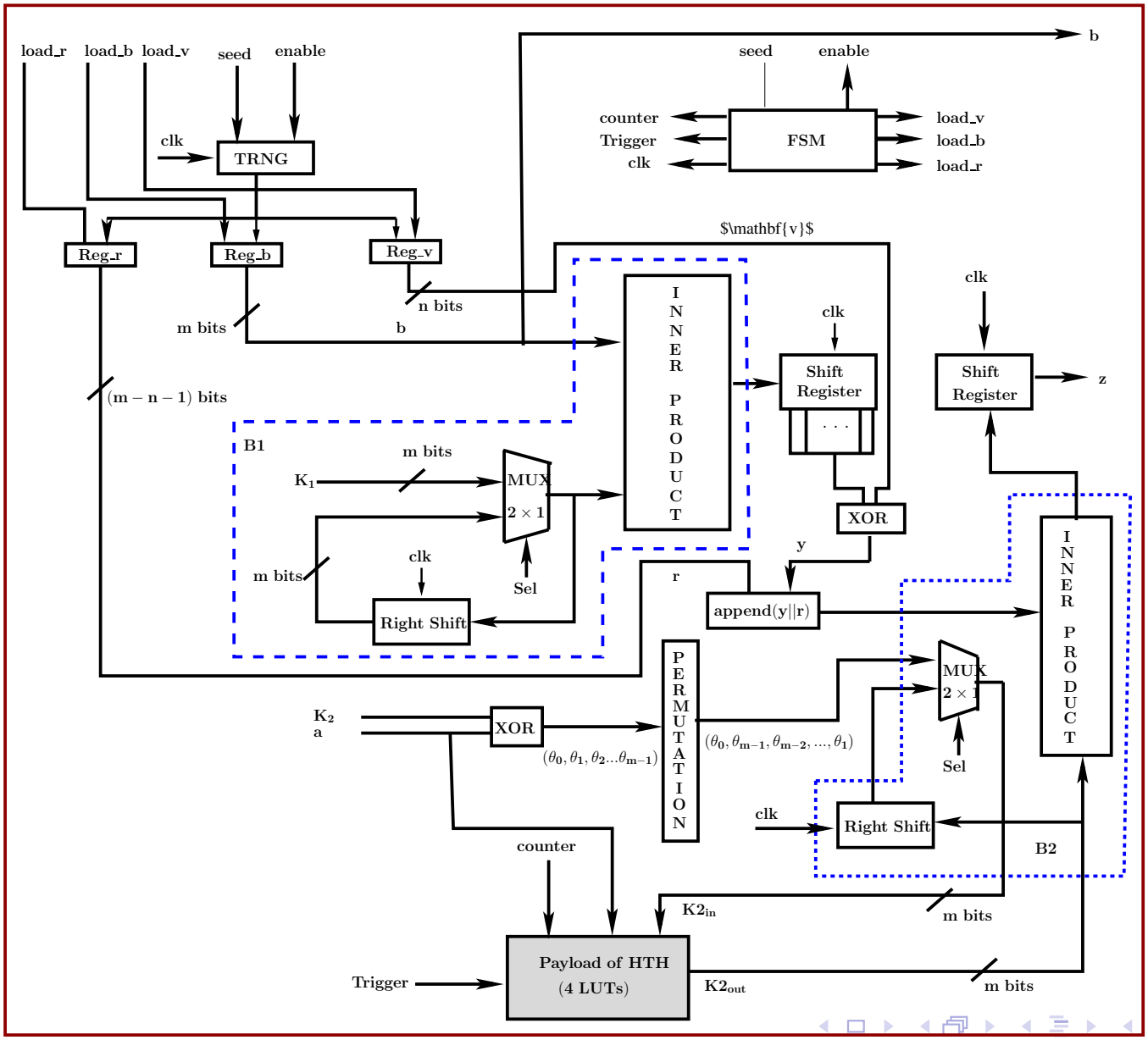
$\theta \in (\epsilon \times n, \frac{n}{2})$ be a threshold value and for 80-bit security, m is 163 bits

Tag Impersonation Attack

- The adversary eavesdrops to obtain a triplet $\mathbf{a_c}, \mathbf{b_c}, \mathbf{z_c}$.
- $\mathbf{K_2}$ is also known.
- $\mathbf{y_c} = \text{Decode}(\mathbf{z_c}, \mathbf{K_2} \oplus \mathbf{a_c})$
- The reader sends $\mathbf{a_w}$.
- Adversary reuses $\mathbf{y_c}$ and calculates $\mathbf{z_w} = \mathbf{y_c} \cdot C_{\mathbf{K_2} \oplus \mathbf{a_w}}$ and sends $\mathbf{z_w}, \mathbf{b_c}$.
- The reader executes decode algorithm with $\mathbf{z_w}$ and $\mathbf{K_2} \oplus \mathbf{a_w}$ and obtains $\mathbf{y_c}$ which was already authenticated by the reader for $\mathbf{b_c}$.

If the adversary obtains the key $\mathbf{K_2}$, it can impersonate as a valid tag, without even having the knowledge of key $\mathbf{K_1}$.

Architecture of LCMQ - Tag



HTH Induced Safe Error Attack

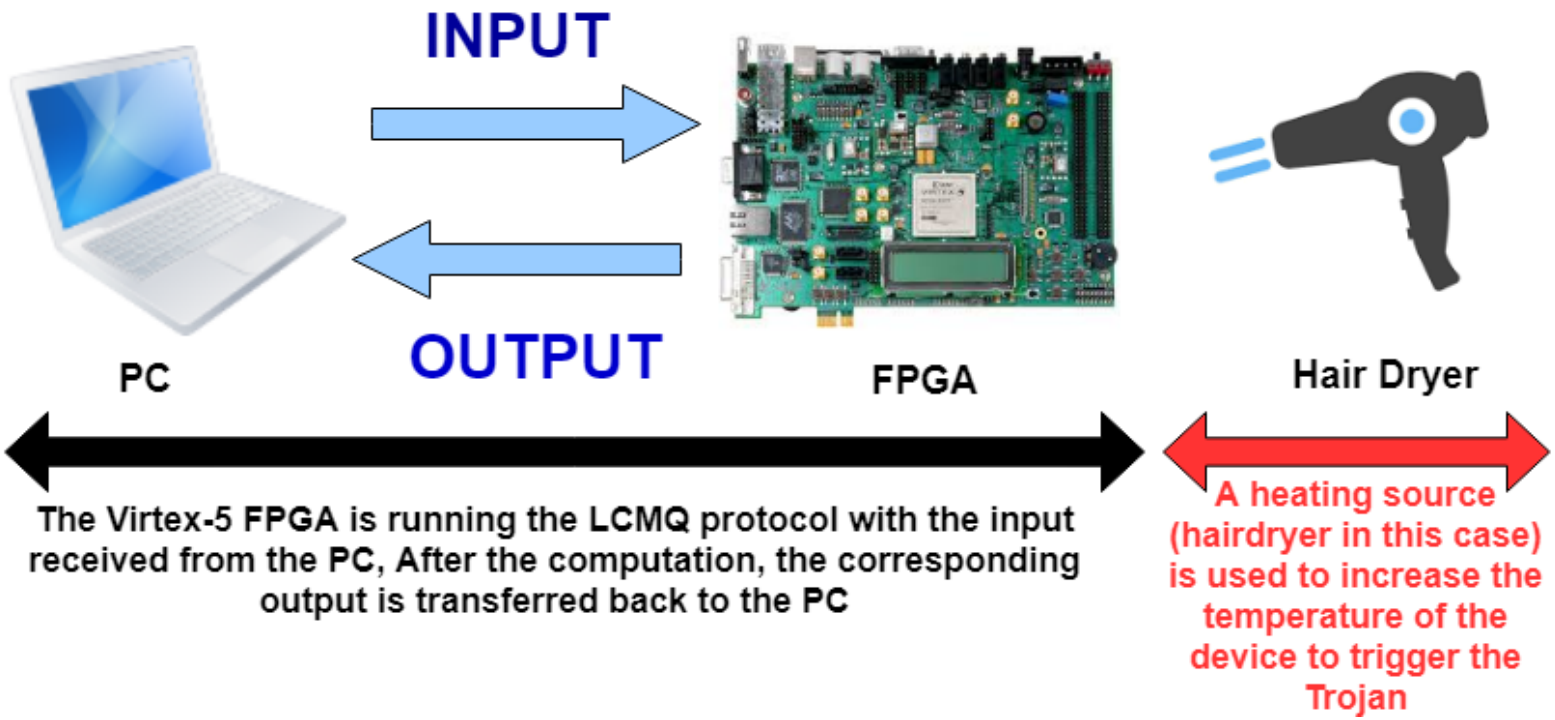
Adversarial Model:

- The designer is malicious and has a nexus with a personnel at a fabrication facility.
- The personnel in the fabrication facility injects the HTH.
- One must ensure that gate count difference between actual design and infected design should not be very high.
- The HTH is implemented using the LUTs on the FPGAs directly, with almost negligible overhead in power and hardware.

HTH Induced Safe Error Attack

Activation:

- External Triggering
- Internal triggering



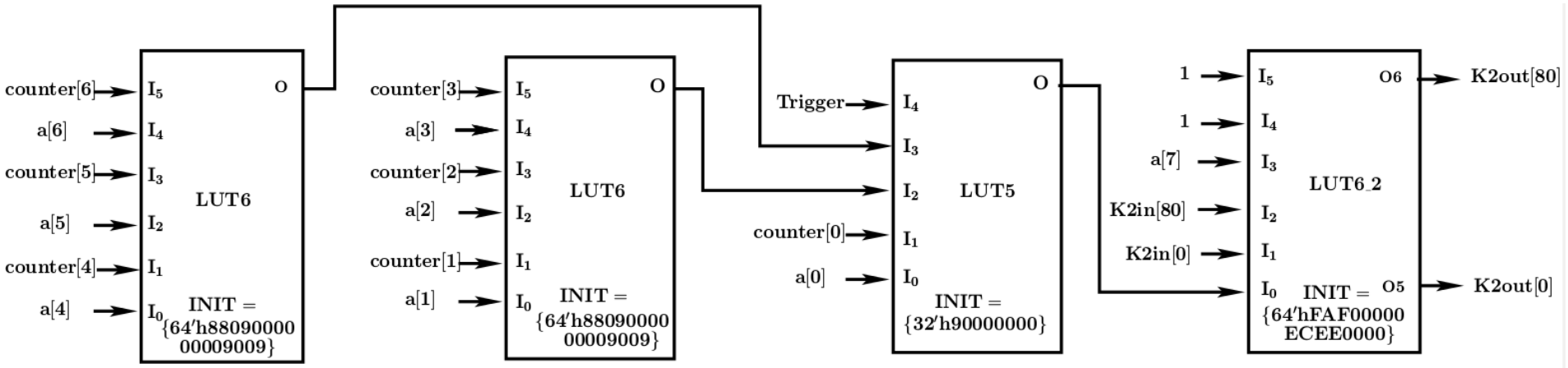
HTH Induced Safe Error Attack

Payload:

- We present an ultra-low hardware footprint HTH which occupies only 4 LUTs.
- To obtain $\mathbf{K_2}$, we need to inject a fault in all m bits.
- Exploits the property of circulant matrix to reduce the linear increase in the overhead.

The input key is right shifted at each clock cycle. A stuck at 1 fault induced in the $\mathbf{1^{st}}$ bit of right shift register in $\mathbf{t}$-th clock cycle is equivalent in inducing a stuck at 1 fault in $\mathbf{t}$-th bit of initial input key.

HTH Induced Safe Error Attack



1. **a[6:0] equals counter value and a[7]=0**: $K_2[0]$ gets injected by the stuck at 1 fault at $a[6:0]^{th}$ clock cycle. It is equivalent to injecting stuck at one fault at $a[6:0]^{th}$ bit of K_2.
2. **a[6:0] equals counter value and a[7]=1**: $K_2[80]$ gets injected by the stuck at 1 fault at $a[6:0]^{th}$ clock cycle. This injects stuck at one fault at $(a[6:0]+80)^{th}$ bit of K_2.

HTH Induced Safe Error Attack

Advantage of targeting either $K_2[0]$ or $K_2[80]$:

- To inject fault at 114^{th} bit position, we need to wait 114 cycle.
- If the value of a is $162 = 8'b10100100$, $K_2[80]$ can be set as 1 in 34^{th} cycle.
- After inducing the stuck at 1 fault, if the authentication succeeds then the adversary infers that the corresponding bit was 1, otherwise that corresponding bit 0.

Experimental Setup and Implementation Results

- The hardware designs for both the hardware implementation of the LCMQ protocol and the proposed HTH were performed using *Verilog HDL* and executed on Virtex-5 FPGA board.
- For 80-bit security, the parameter values are: $m = 163, n = 162, \theta = 18, \eta = 0.08$.
- The designs were synthesized and implemented using *Xilinx ISE 14.5*, and simulated using *Xilinx Isim*.
- The power estimation of the circuit was carried out using *Xilinx XPower Analyzer* and delay estimation using *Xilinx Timing Analyzer*.

Experimental Setup and Implementation Results

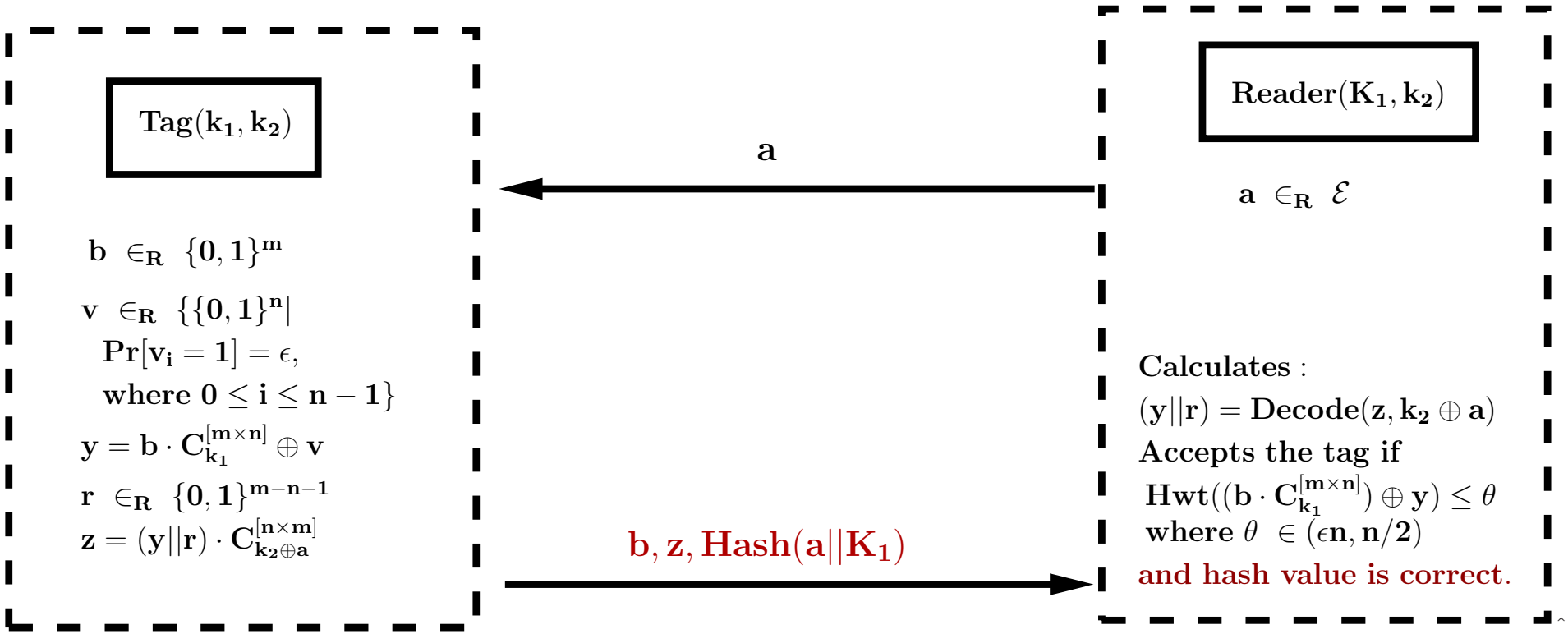
Table: Power and Execution Time Overhead

Overhead	Original Design	Design with HTH	Increase in Number
Power	0.539 W	0.539 W	0
Timing	3.789 ns	3.794 ns	0.13

Table: Hardware Overhead

Components	Original Design	Design with HTH	Increase in Number
LUT	714	717	0.4
SliceRegs	1507	1507	0
Slices	589	589	0.0

Countermeasure



Conclusions

- We made an key observation that in an LCMQ protocol an attacker can impersonate without the knowledge of key $\mathbf{K_1}$, thus motivating a HTH designer to just target key $\mathbf{K_2}$.
- We gave an effective and efficient architecture of tag part of the LCMQ problem.
- We provided an ultra-lightweight HTH design which can induce safe errors surreptitiously to leak $\mathbf{K_2}$ potentially.

Thank You