KU LEUVEN

SPACE 2012, Chennai, India, November 2-3

Performance and Security Evaluation of AES S-Box-based Glitch PUFs on FPGAs

Dai Yamamoto
Fujitsu Laboratories Ltd., Japan
KU Leuven, Belgium

Collaborators:
Gabriel Hospodar, Roel Maes,
Ingrid Verbauwhede
(KU Leuven, Belgium)

Introduction

- Semiconductor counterfeiting has recently boomed
- Huge threat for companies
  - Technologically
  - Financially
- Call for solutions

BBC NEWS TECHNOLOGY
Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Edu
Entertainment & Arts

10 April 2012 Last updated at 15:12

Share

Fake semiconductors 'could cause tragedy'

The number of fake memory chips and processors in use has tripled since 2009, suggests a report.

The report, compiled by semiconductor analyst IHS iSuppli, said fakes were found in phones, computers, military hardware, cars and hospital equipment.

The analyst said the fakes were turning up in so many places that they might soon put lives at risk.

Fakes are turning up in more and more gadgets, warns iSuppli

The military and aerospace firms were the most likely to be using fakes, it said.

Chip police

More than 1,363 fakes were reported in 2011, said the report, and threatened to dent a market worth more than $169bn (£109bn) a year.

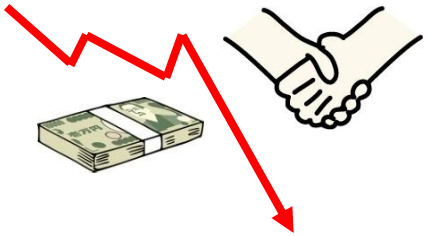
The five most widely counterfeited chips included memory chips

BBC NEWS TECHNOLOGY
http://www.bbc.co.uk/news/technology-17665527

KU LEUVEN

Why is Counterfeiting Serious?

- Monetary damage for honest manufacturers
  - Customers buy counterfeits → drop in sales → drop in revenues
  - Costs increase due to extra security analyses



- Losing the trust of customers
  - Mistaking the fake with the original
  - Counterfeit often has poorer quality

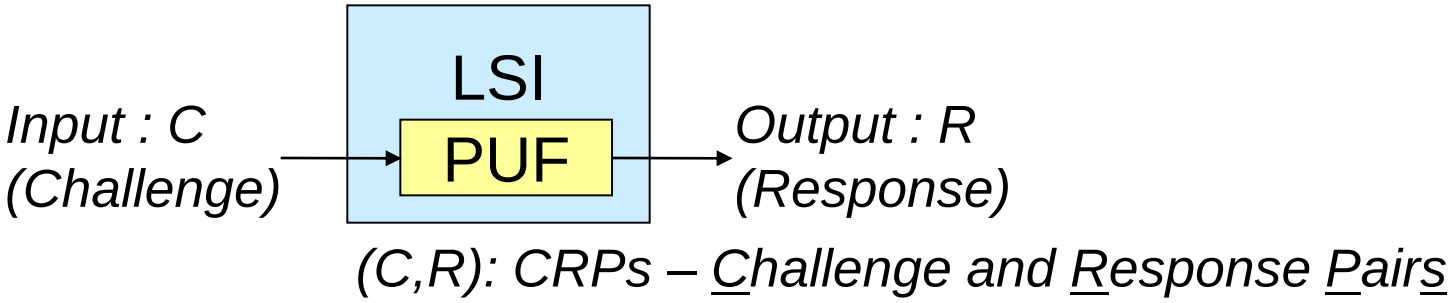
- Increase risks of life-threatening accidents
  - Electric vehicles, medical devices, smart grid, etc.

- Anti-counterfeiting technologies are specifically required
  - PUF (Physically Unclonable Function)

KU LEUVEN

PUF: Physically Unclonable Function

- Focus on PUFs on LSIs: Silicon PUFs



- Outputs depend on process variations of each individual LSIs
  - Slight differences of wire/gate delays, drive capability, etc.
  - Responses ideally NOT predictable

- Counterfeiting and modeling PUFs is quite difficult
  - Encryption keys can be derived from PUF responses

KU LEUVEN

Motivation (1/2)

- Two types of PUFs:
  - Memory-based PUFs
    - SRAM-PUFs, Latch PUFs, Butterfly PUFs, Flip-flop (FF) PUFs, etc.
  - Delay-based PUFs
    - Ring-oscillator PUFs, Arbiter PUFs, **Glitch PUFs**, etc.

- Developers' self-evaluation is valuable, but they may…
  - Overstate good results
  - Understate undesirable results

- Third-party evaluation is very important
  - Independent verification of claims about proposed PUFs
  - Results contribute for practical usability assessment of new PUFs

KU LEUVEN

Motivation (2/2)

- Third party evaluation of AES S-Box-based Glitch PUFs
  - Suzuki et al. at CHES 2010 (“developers”)

- AES S-Box-based Glitch PUFs (GPUFs)
  - One of the most feasible and secure delay-based PUFs
  - Resistance against machine learning attacks
  - Not evaluated by the community yet

KU LEUVEN

Overview

- Performance and Security evaluation of GPUFs
  - Performance: **Reliability** and Uniqueness
  - Security: How difficult is GPUF response prediction?

- Contributions

  [1] # CRPs = 2^{19} (not 2^{11})

  [2] Low robustness against voltage variation
    - Reliability (response error rate: RER)
      - Ours ≈ 35%, Developers' ≈ 10%

  [3] Weak challenges → easily predictable responses
    - Potential vulnerability against machine learning attacks

- Conclusion
  - GPUFs present almost no PUF-behavior

KU LEUVEN

Table of Contents

- Background
  - PUF performance: Reliability
  - GPUF

- Contributions

  [1] Number of CRPs is 2^{19}, instead of 2^{11}

  [2] Performance: Low robustness against voltage variation

  [3] Weak challenges leading to more easily predictable responses

- Summary / Future work

KU LEUVEN

Table of Contents

- Background
  - PUF performance: Reliability
  - GPUF

- Contributions

  [1] Number of CRPs is 2^{19}, instead of 2^{11}

  [2] Performance: Low robustness against voltage variation

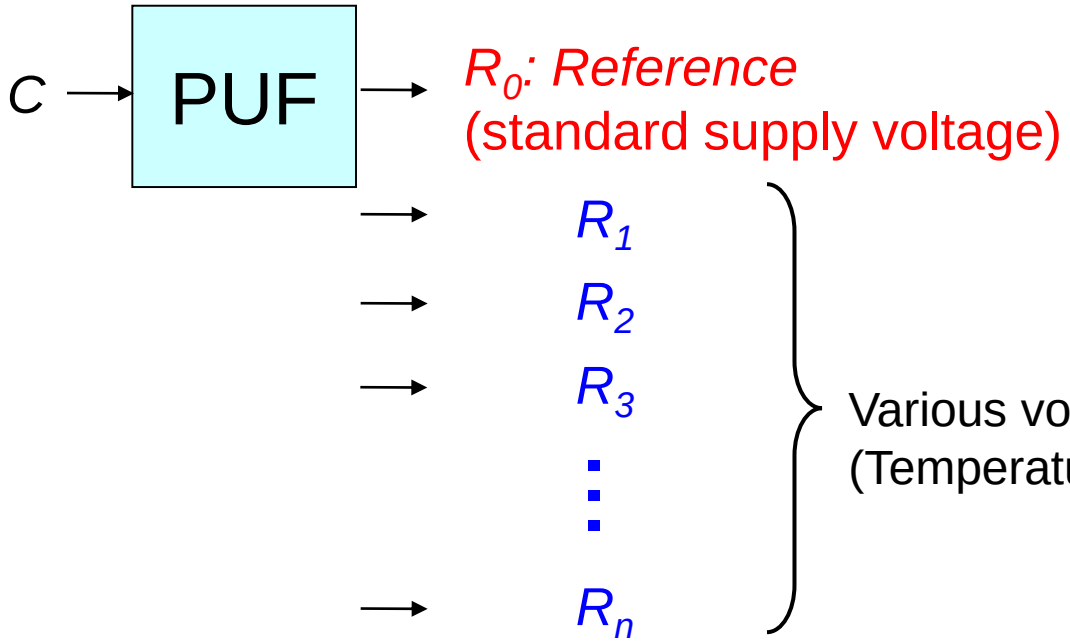
  [3] Weak challenges leading to more easily predictable responses

- Summary / Future work

KU LEUVEN

Reliability (Response Error Rate)

- Consistency of responses generated by the same challenges
  - Mean of Hamming distances (HDs) between a reference and n-times measurements



Response Error Rate

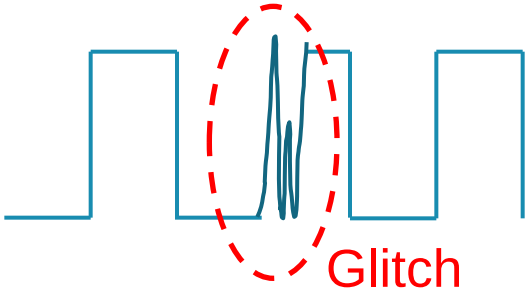
$$= \frac{1}{n}\sum_{i=1}^{n} \mathrm{HD}(R_0, R_i)$$

- **High reliability = low RER (ideally HD=0)**
- Important to keep high reliability in various conditions

KU LEUVEN

GPUF

- Glitch: A pulse of short duration
  - Occurring before the signal settles to a value



- GPUF
  - Using an AES S-Box as a glitch generator
    - Based on composite Galois Field
  - A toggle FF (TFF) outputs “1” if the parity of the # of glitches is odd
  - Challenge: 11 bits, Response: 1 bit

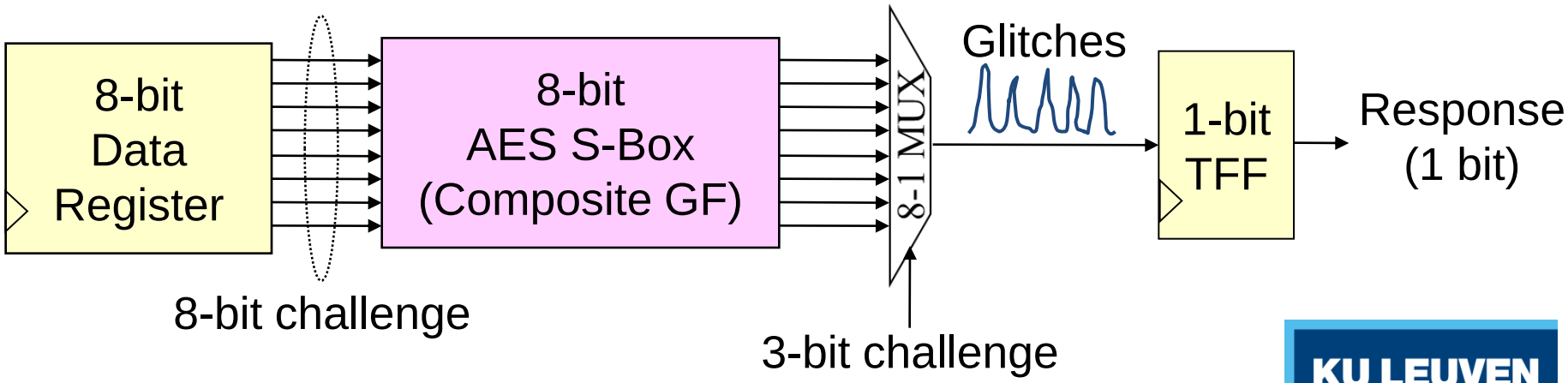


Table of Contents

- Background
  - PUF performance: Reliability
  - GPUF

- Contributions

  [1] Number of CRPs is 2^{19}, instead of 2^{11}

  [2] Performance: Low robustness against voltage variation

  [3] Weak challenges leading to more easily predictable responses

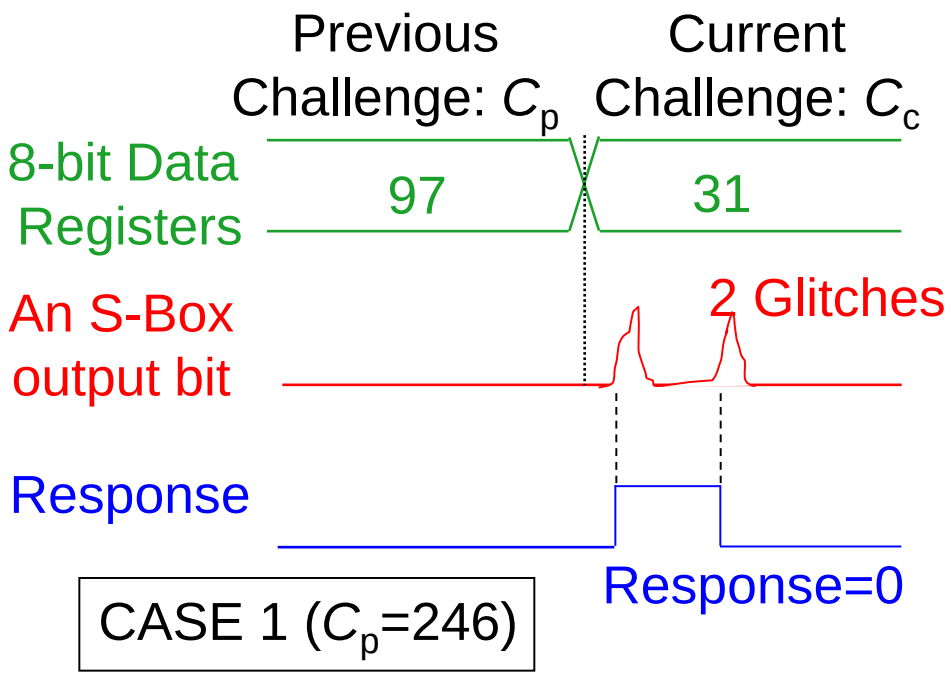
- Summary / Future work

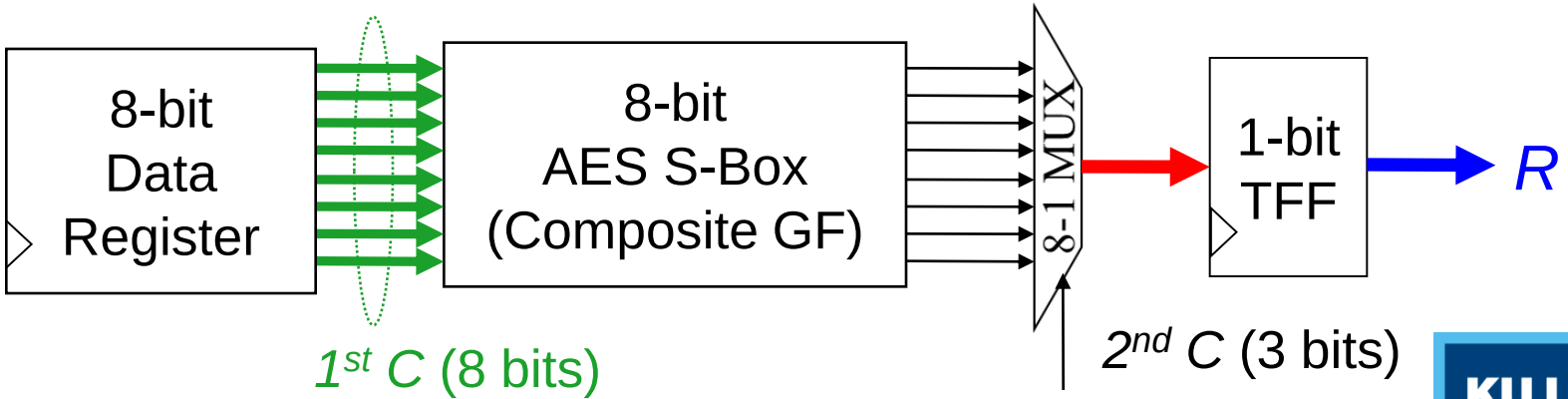
KU LEUVEN

A General Method to Generate Responses

1st Contribution
2nd Contribution
3rd Contribution

- **GPUF has 2^{19} CRPs**
  - Developers evaluated 2^{11} CRPs
  - No reason in their paper
- Glitches: 8-bit challenge changes from C_p to C_c
  - C_p affects glitches
- Challenge is 19 bits
  - 8-bit C_p, 8-bit C_c, 3-bit *2nd C*



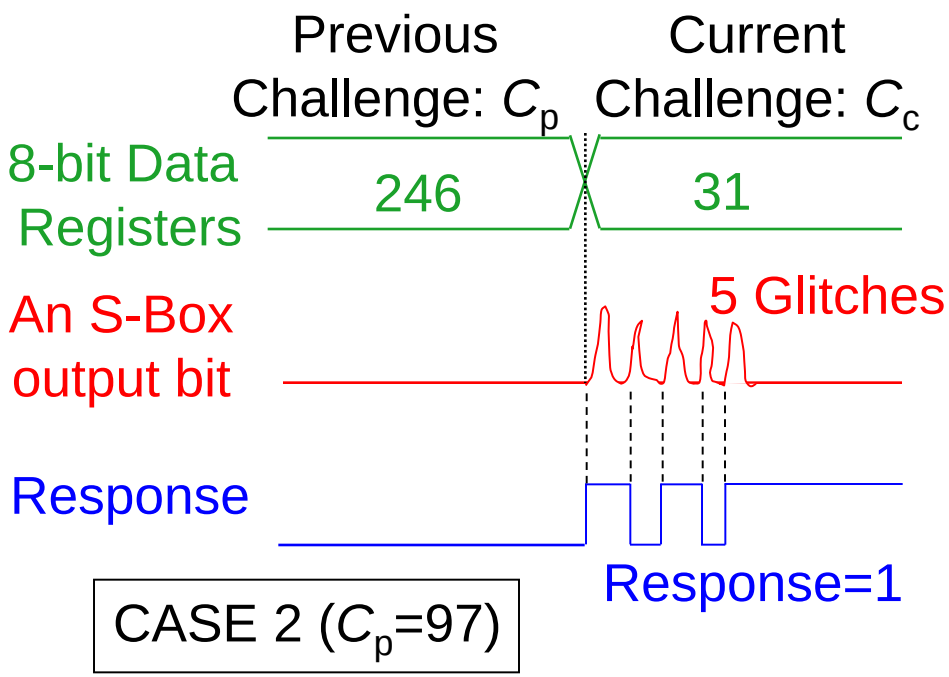


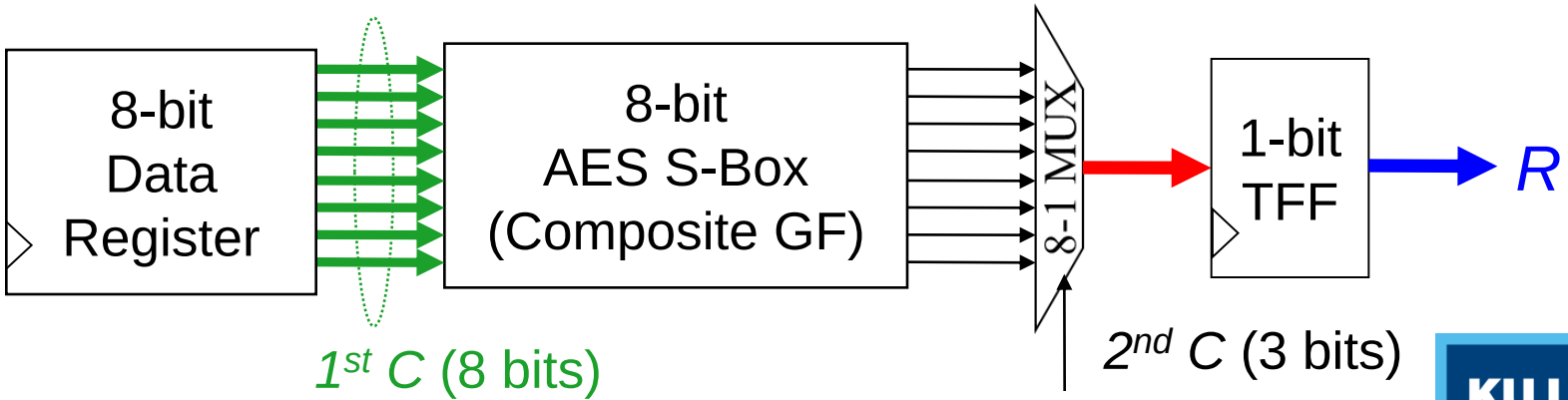
KU LEUVEN

A General Method to Generate Responses

1st Contribution
2nd Contribution
3rd Contribution

- **GPUF has 2^{19} CRPs**
  - Developers evaluated 2^{11} CRPs
  - No reason in their paper
- Glitches: 8-bit challenge changes from C_p to C_c
  - C_p affects glitches
- Challenge is 19 bits
  - 8-bit C_p, 8-bit C_c, 3-bit *2nd C*





KU LEUVEN

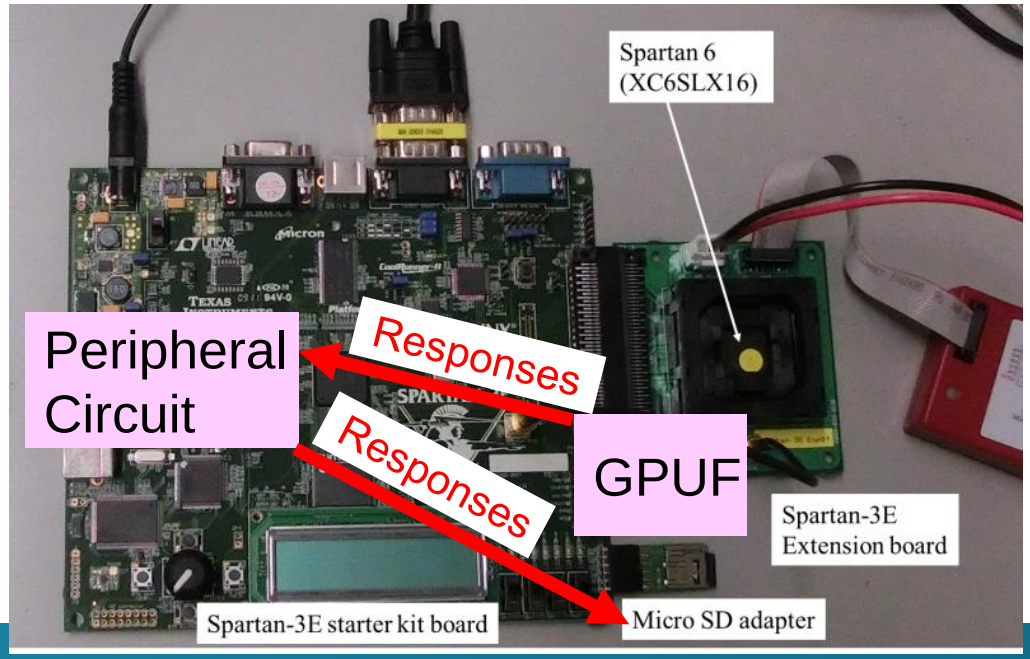
Performance Evaluation of GPUFs

1st Contribution
2nd Contribution
3rd Contribution

- Original performance results are insufficient
  - Developers evaluated only a subset (2^{11}) of all CRPs (2^{19})

- Evaluating performance of GPUFs using all CRPs (2^{19})
  - Reliability in various voltage conditions
  - Relation between reliability and challenges: HD(C_p, C_c)

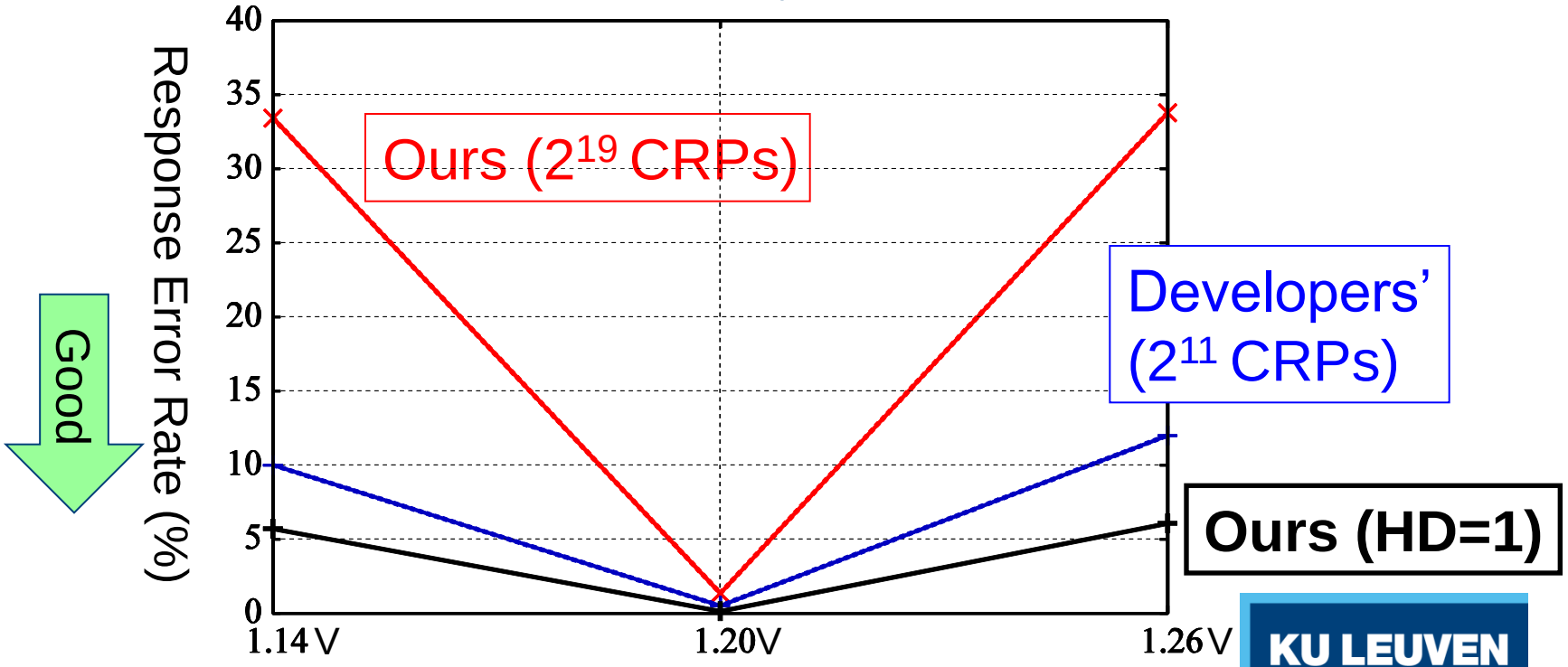
- FPGA-based evaluation
  - Custom-made FPGA board
    - GPUF on FPGAs
    - Varying core voltages
    - 20 replaceable FPGAs



Robustness in Various Voltages

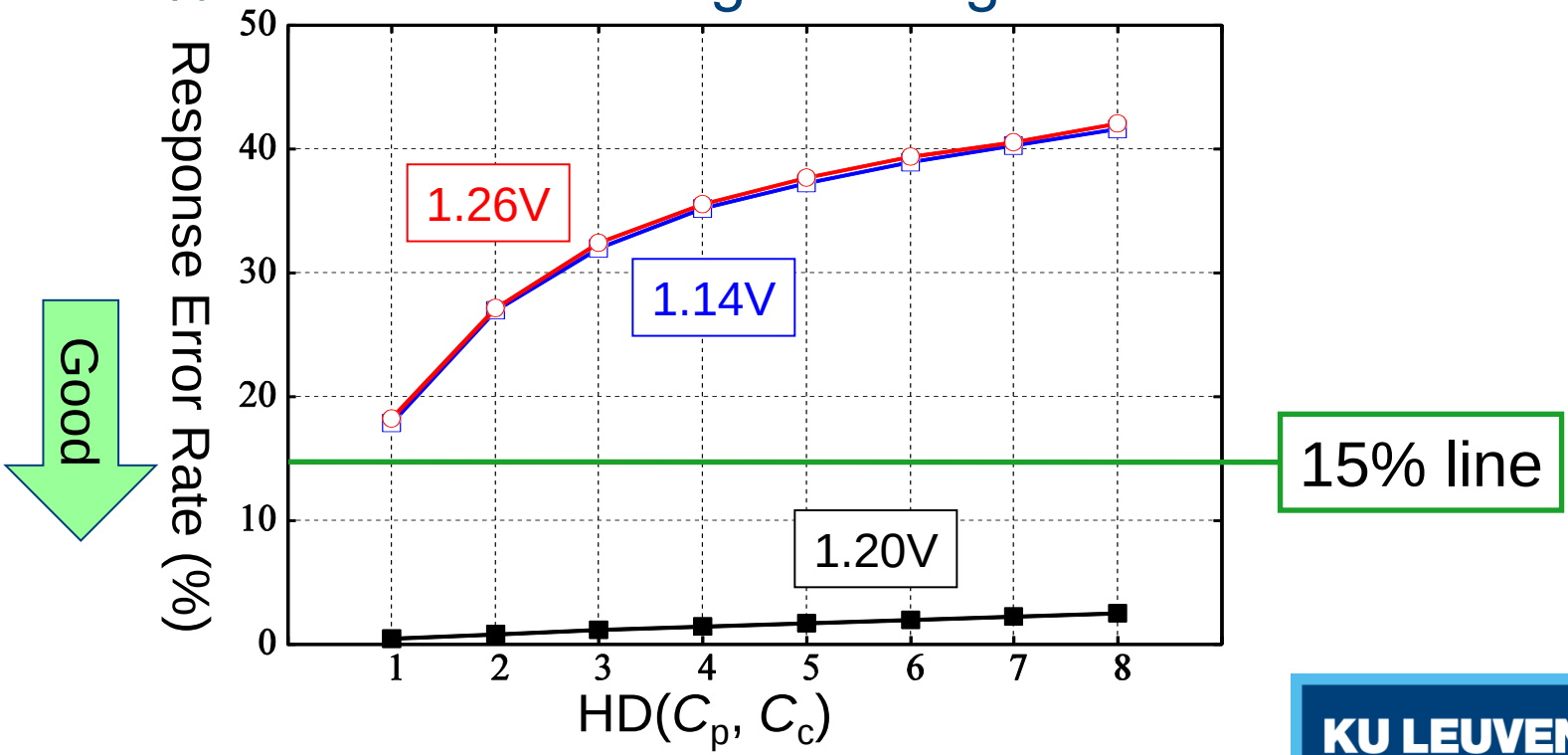
1st Contribution
2nd Contribution
3rd Contribution

- RER in 1.14V, 1.20V, and 1.26V
- Our RER is much higher than the developers'
  - Ours ≈ 35% (Low robustness!!), Developers' ≈ 10%
- Reason: Number of evaluated CRPs
  - Result of 2^{11} CRPs satisfying HD(C_p, C_c) = 1, LSB is different bit



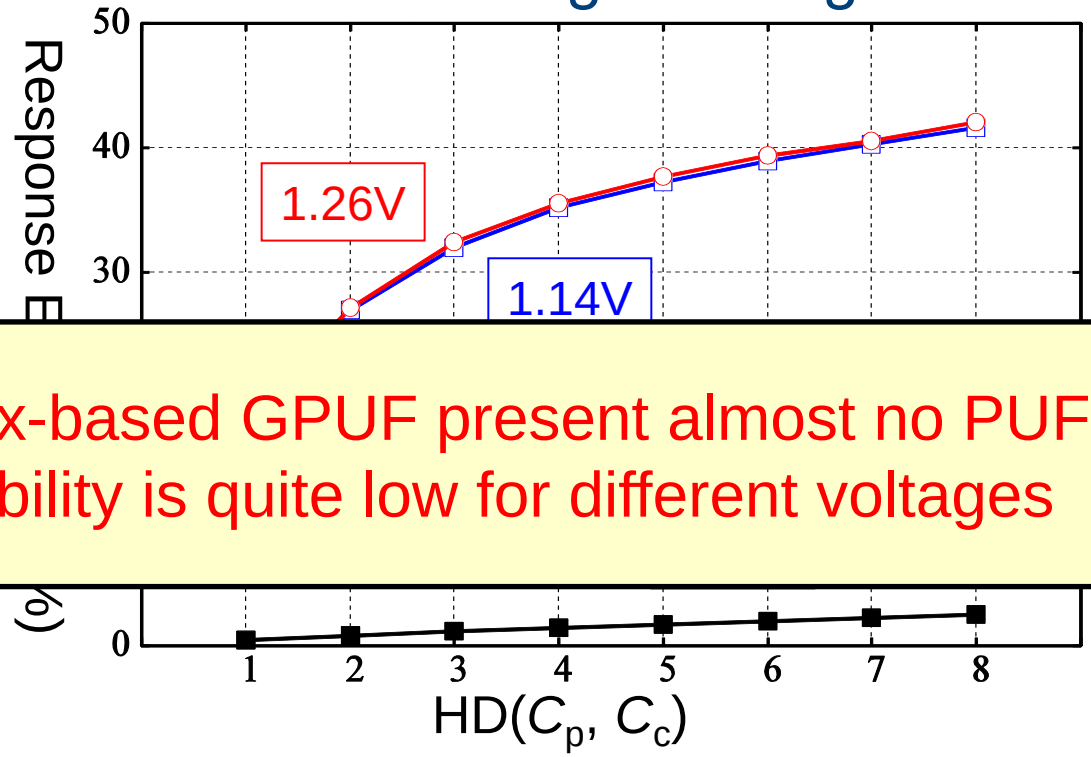
RER vs HD(C_p, C_c)

- RER strongly depends on HD(C_p, C_c)
  - Small HD(C_p, C_c) → low RER
  - Small number of challenge-bit transitions → little influence on glitches
- Appropriate CRPs selection needed→ higher design cost
- RER > 15% → error correcting with large redundant data



RER vs HD(C_p, C_c)

- RER strongly depends on HD(C_p, C_c)
  - Small HD(C_p, C_c) → low RER
  - Small number of challenge-bit transitions → little influence on glitches
- Appropriate CRPs selection needed→ higher design cost
- RER > 15% → error correcting with large redundant data

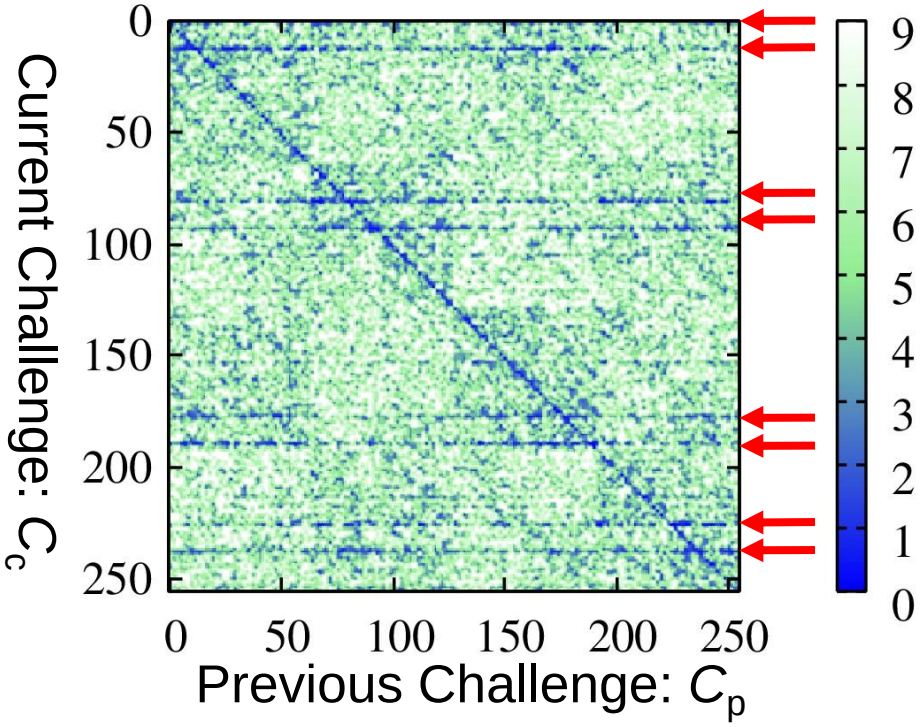


AES S-Box-based GPUF present almost no PUF-behavior since reliability is quite low for different voltages

Security Evaluation of GPUFs

1st Contribution
2nd Contribution
3rd Contribution

- # glitches from 6th S-Box bit
- Horizontal lines (= 16 Weak challenges)
  - 16 C_c leading to almost no glitches regardless of C_p
  - Attackers can predict such responses more easily than other ones
  - Machine learning attacker could benefit from these correlations

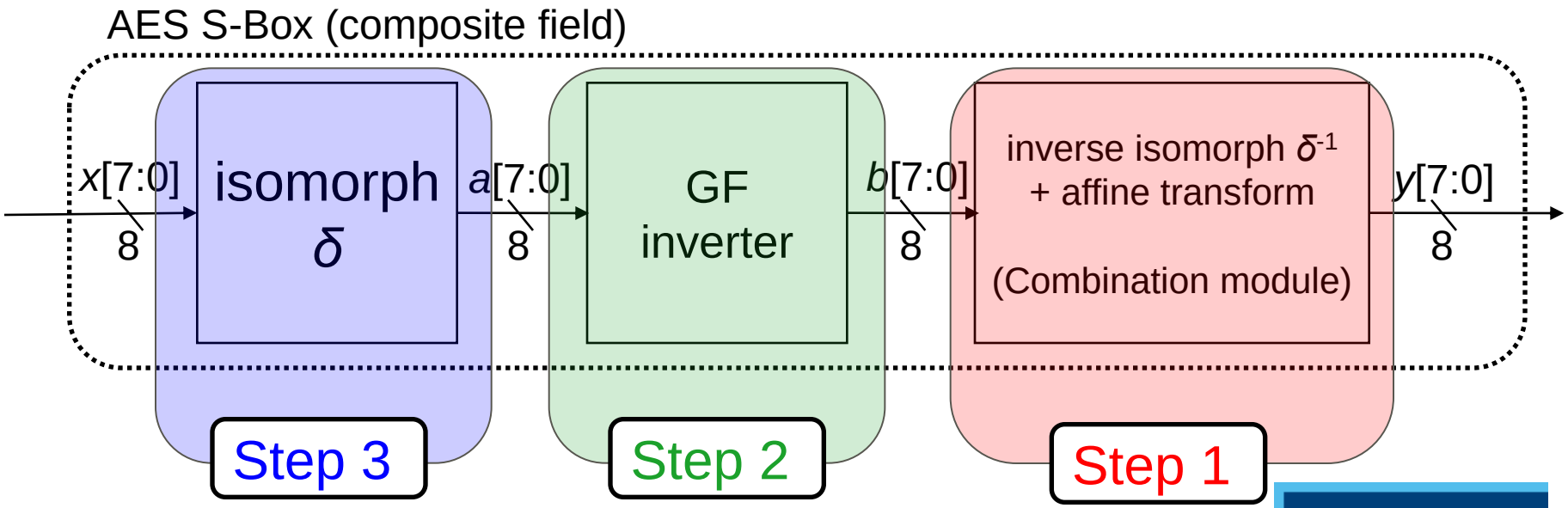


KU LEUVEN

Why such weak challenges exist?

1st Contribution
2nd Contribution
3rd Contribution

- AES S-Box (composite field) consists of 3 sub-modules
  - Input / output of S-Box: *x* and *y*
  - Input / output of GF inverter: *a* and *b*
- Our Goal
  - To find special values of *x* yielding *y*[6] = zero

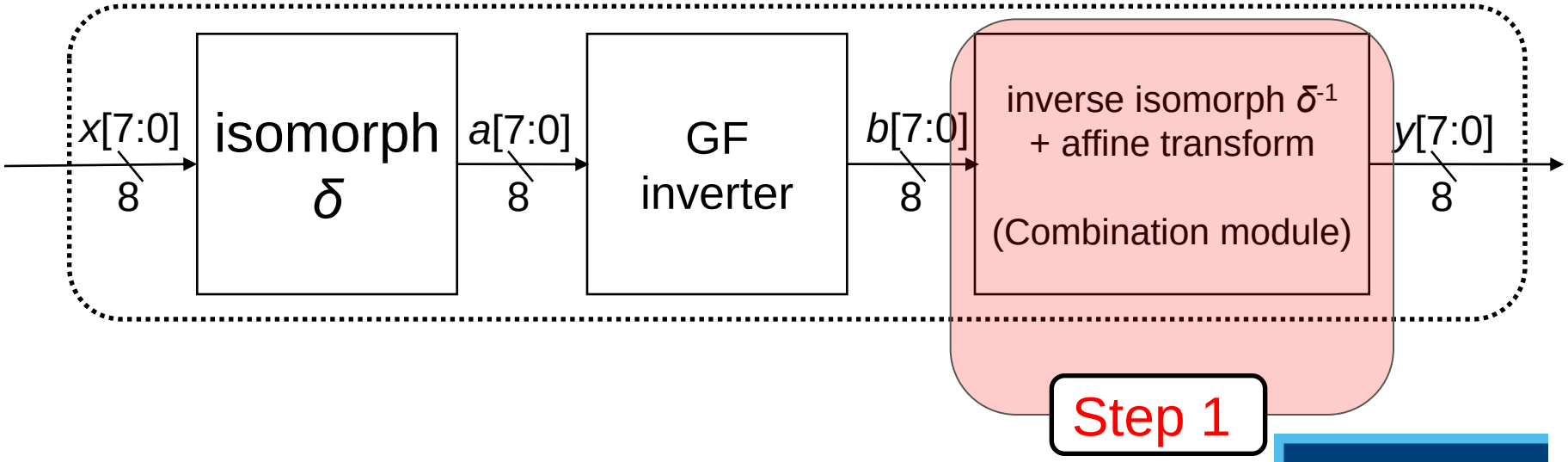


KU LEUVEN

Step1: Combination module

1st Contribution
2nd Contribution
3rd Contribution

- $y[6] = \sim b[4] \oplus b[5] \oplus b[6] \oplus b[7]$
  - $y[6]$ depends only on the upper 4 bits of b

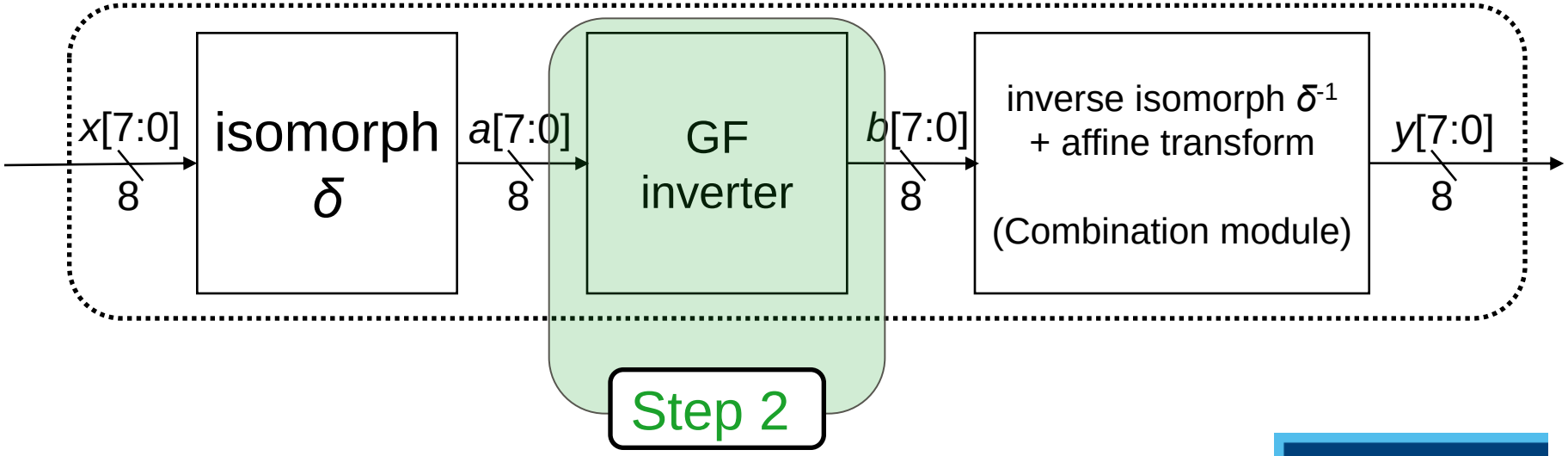


KU LEUVEN

Step2: GF inverter (1/2)

1st Contribution
2nd Contribution
3rd Contribution

- The upper 4 bits of b satisfy:
  - $b[7] = tn[0] \oplus tn[1] \oplus tn[3] \oplus tn[4]$
  - $b[6] = tn[0] \oplus tn[2] \oplus tn[3] \oplus tn[5]$
  - $b[5] = tn[0] \oplus tn[1] \oplus tn[7] \oplus tn[8]$
  - $b[4] = tn[0] \oplus tn[2] \oplus tn[6] \oplus tn[7]$
- *tn* is a 9-bit internal variable in the GF inverter



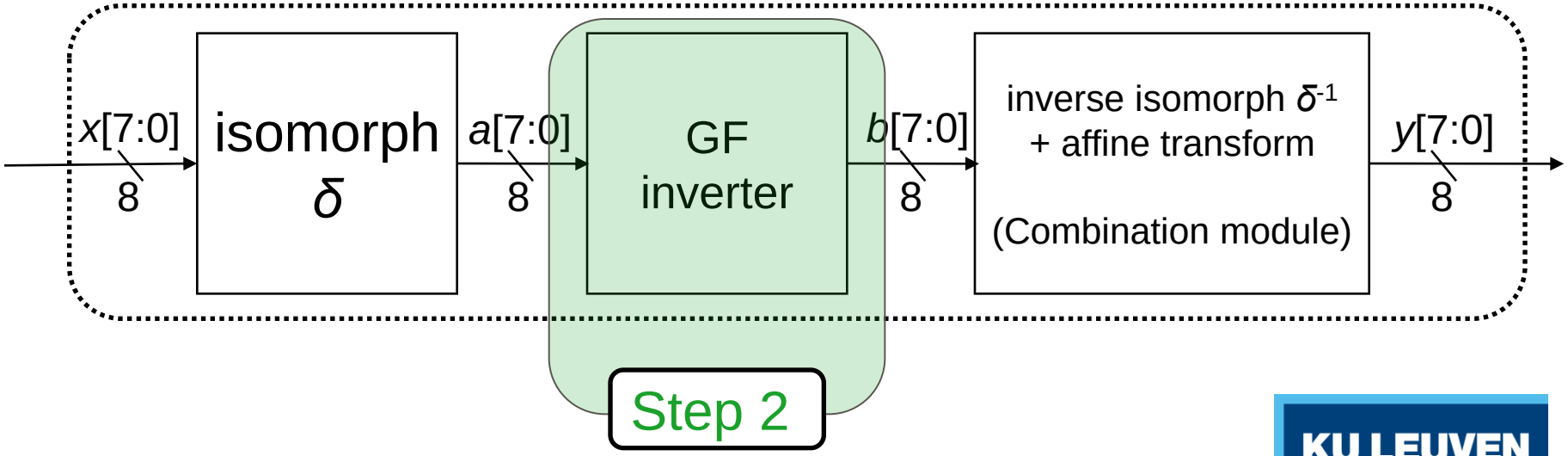
Step2: GF inverter (2/2)

1st Contribution
2nd Contribution
3rd Contribution

- *tn* satisfies:

$$
\begin{aligned}
tn[8] &= (v[3]) && \& (a[7]) \\
tn[7] &= (v[2] \oplus v[3]) && \& (a[6] \oplus a[7]) \\
tn[6] &= (v[2]) && \& (a[6]) \\
tn[5] &= (v[1] \oplus v[3]) && \& (a[5] \oplus a[7]) \\
tn[4] &= (v[0] \oplus v[1] \oplus v[2] \oplus v[3]) && \& (a[4] \oplus a[5] \oplus a[6] \oplus a[7]) \\
tn[3] &= (v[0] \oplus v[2]) && \& (a[4] \oplus a[6]) \\
tn[2] &= (v[1]) && \& (a[5]) \\
tn[1] &= (v[0] \oplus v[1]) && \& (a[4] \oplus a[5]) \\
tn[0] &= (v[0]) && \& (a[4])
\end{aligned}
$$

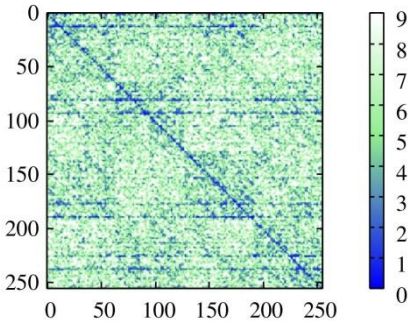
- If ***a*[7:4] are zero**, then no glitch is expected in *y*[6]



Step3: isomorph δ

1st Contribution
2nd Contribution
3rd Contribution

- Our goal
  - To find special values of x yielding $a[7:4]$ = zero
- 16 patterns of x (weak challenges C_c regardless of C_p)...
  - 0,1,80,81,12,13,92,93, 224,225,176,177, 236,237,188,189
- ...matching the 16 horizontal lines
  - Easily predictable responses due to almost no glitches



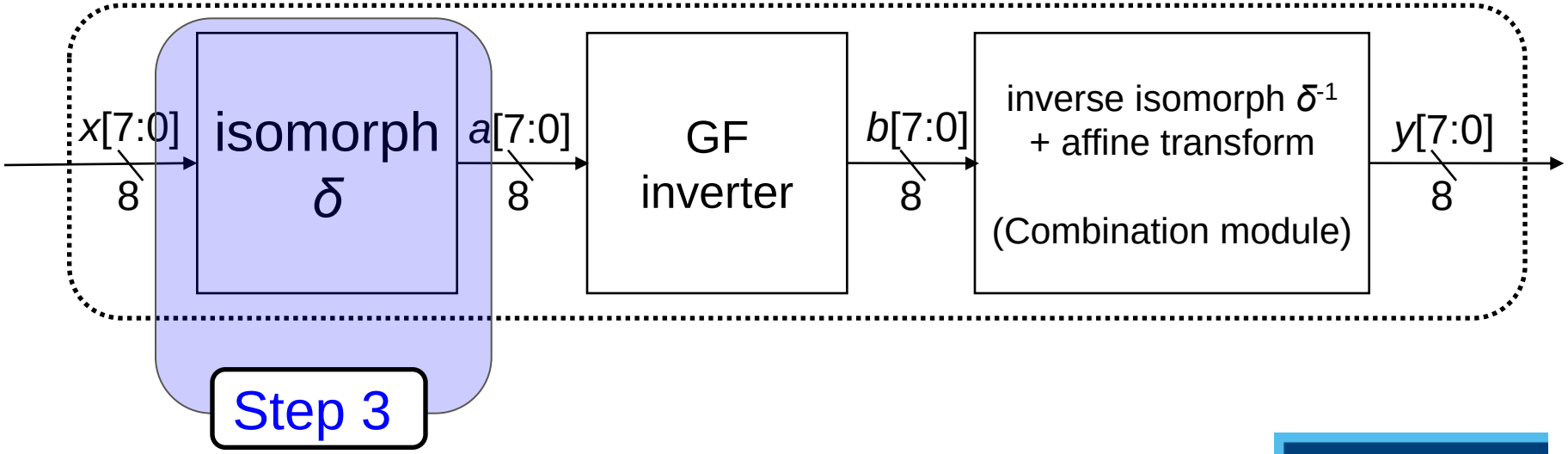


Table of Contents

- Background
  - PUF performance: Reliability
  - GPUF

- Contributions

  [1] Number of CRPs is 2^{19}, instead of 2^{11}

  [2] Performance: Low robustness against voltage variation

  [3] Weak challenges leading to more easily predictable responses

- Summary / Future work

KU LEUVEN

Summary

- Goal
  - Performance and Security evaluation of GPUFs
- Contributions
  - Number of CRPs is not 2^{11} but 2^{19}
  - Clarify Reliability of GPUFs
    - Low robustness against voltage variation
    - Reliability strongly depends on HD(C_p, C_c)
  - 16 weak challenges leading to more easily predictable responses
- Conclusion
  - GPUFs should not use AES S-Box as a glitch generator
- Future work
  - ASIC Evaluation of GPUFs
  - Proposing an alternative glitch generator for GPUFs

KU LEUVEN

Questions?

Thank you very much

KU LEUVEN