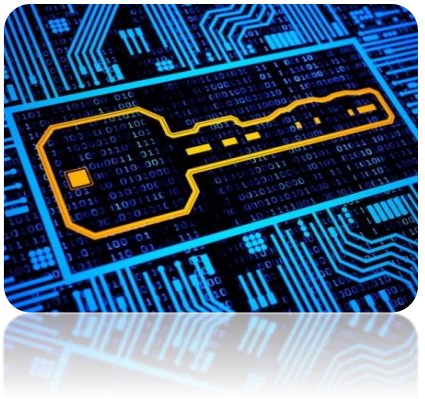
WRIGHT STATE UNIVERSITY

Evaluating Obfuscation Performance of Novel Algorithm-to-Architecture Mapping Techniques in Systolic-Array-based Circuits

Jiafeng Xie (Wright State Univ.) and Xiaojun Zhou (Central South Univ.)

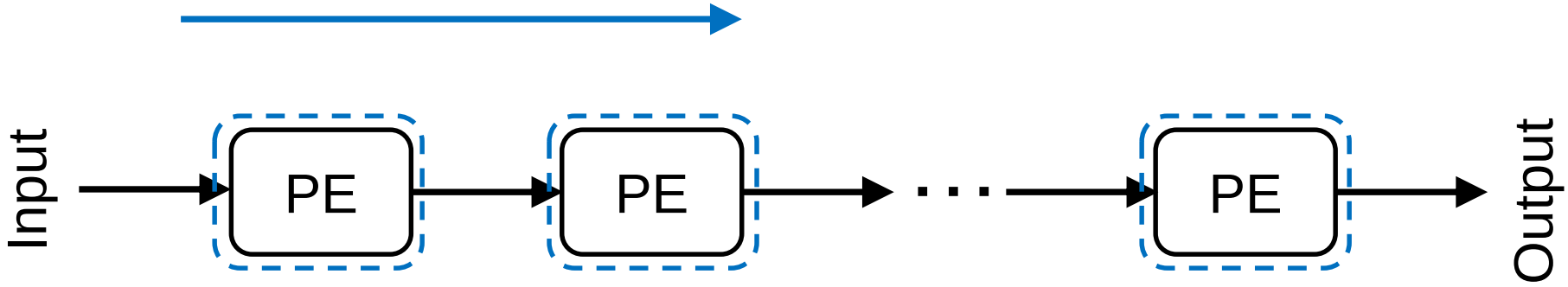
Date: Oct 20, 2017

Contents



- Background and security analysis
- Proposed strategy
- Conclusion and discussion
- References

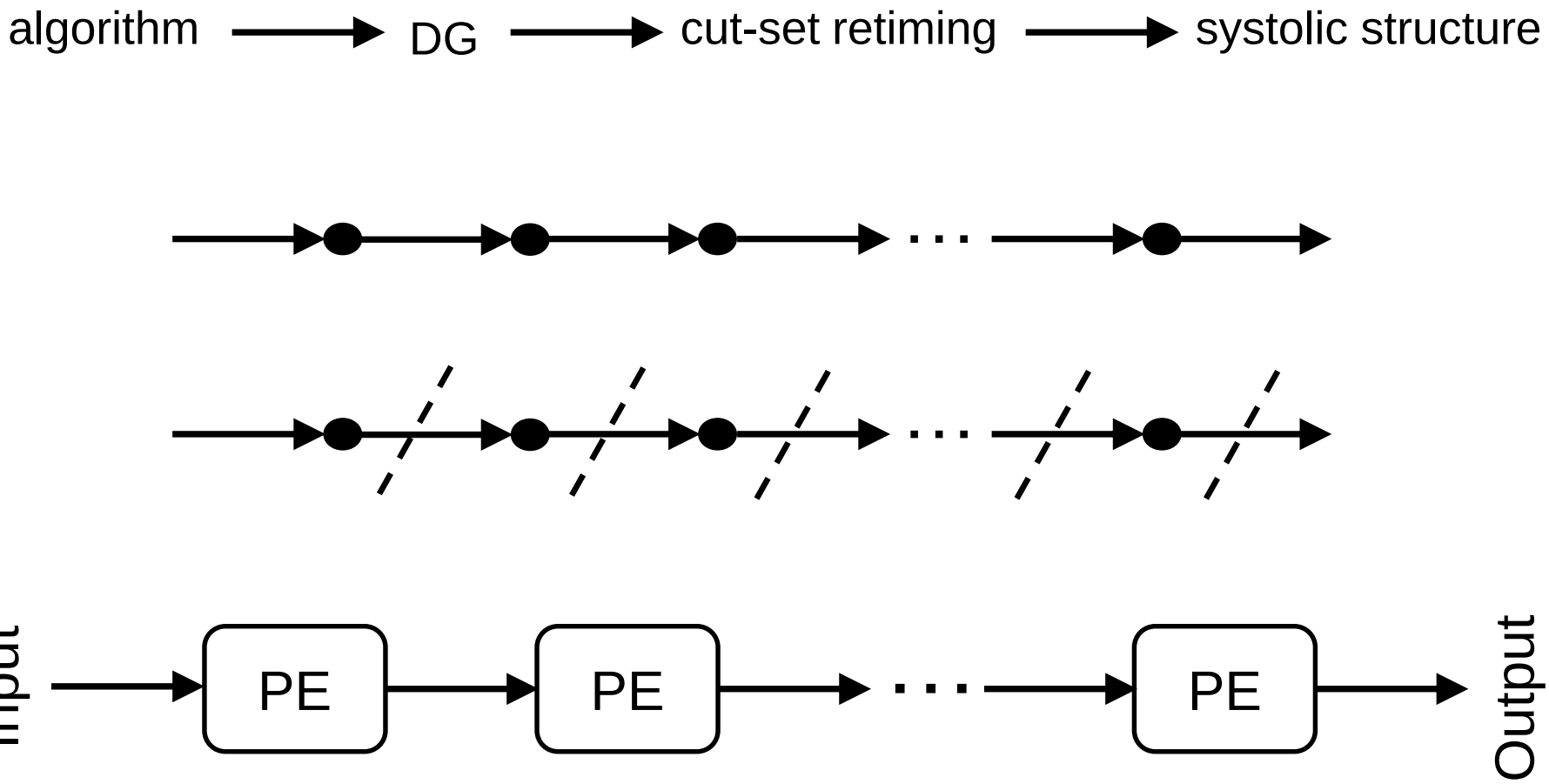
Background



A typical 1-D systolic structure

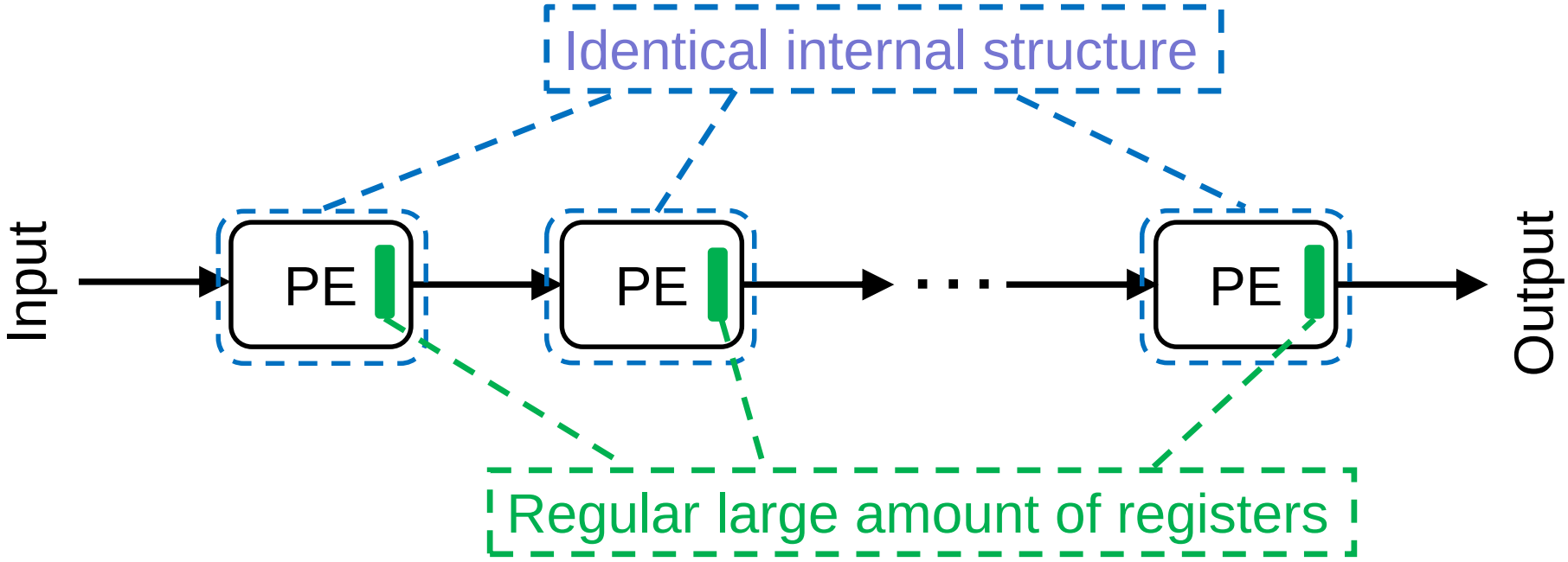
Widely used in many high-performance applications such as signal processing, image processing, artificial intelligence, pattern recognition, computer vision, and cryptosystem.

Background



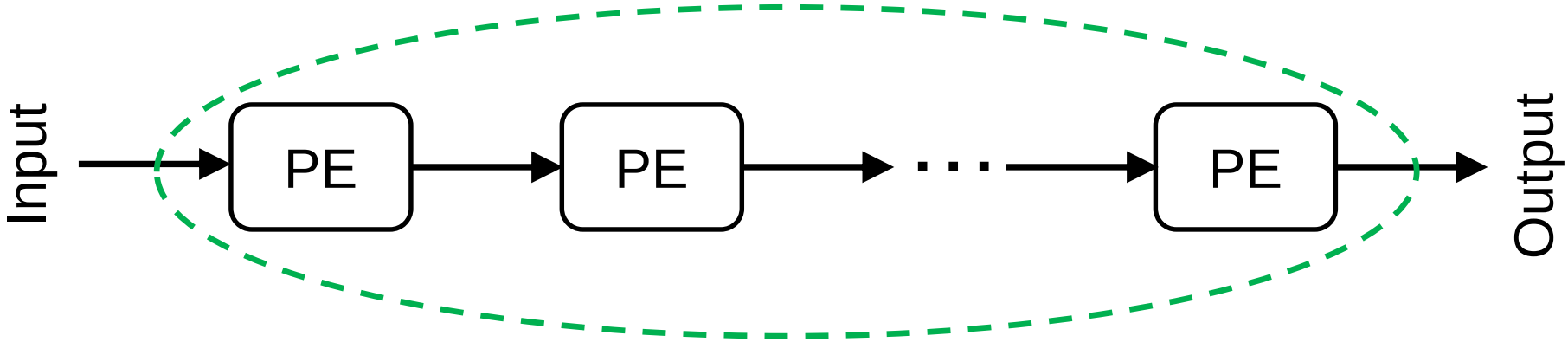
A typical 1-D systolic structure design process

Background



Two unique properties of systolic structure

Security concerns



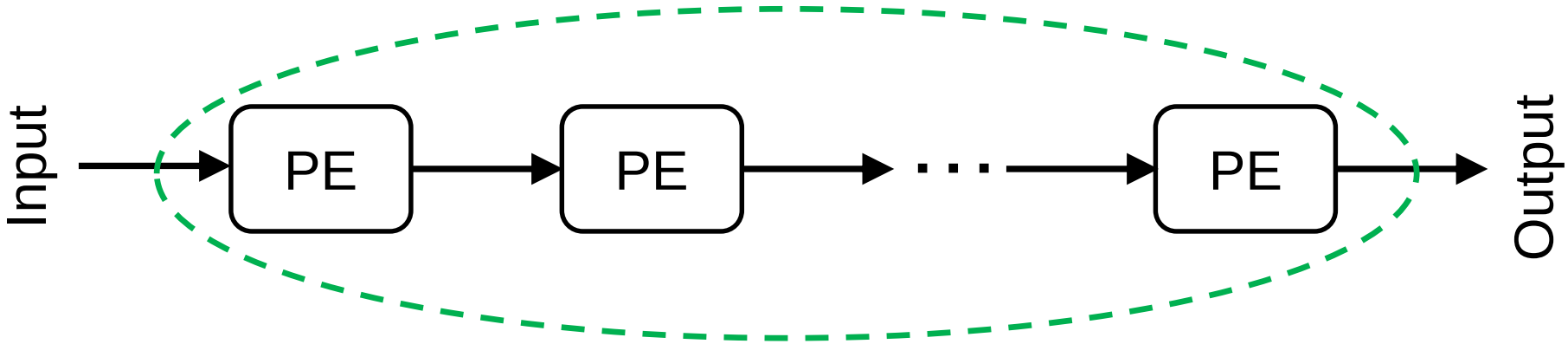
Challenge: how to obfuscate it?

Type-I: all PEs are obfuscated with the same obfuscation technique with the same complexity overhead

Type-II: each PE is obfuscated with different obfuscation techniques

Security issue-I: identicality of PEs

Security concerns



Challenge: how to obfuscate it?

Type-I: all PEs are obfuscated with the same obfuscation technique with the same complexity overhead

Each PE can be easily isolated and be attacked individually

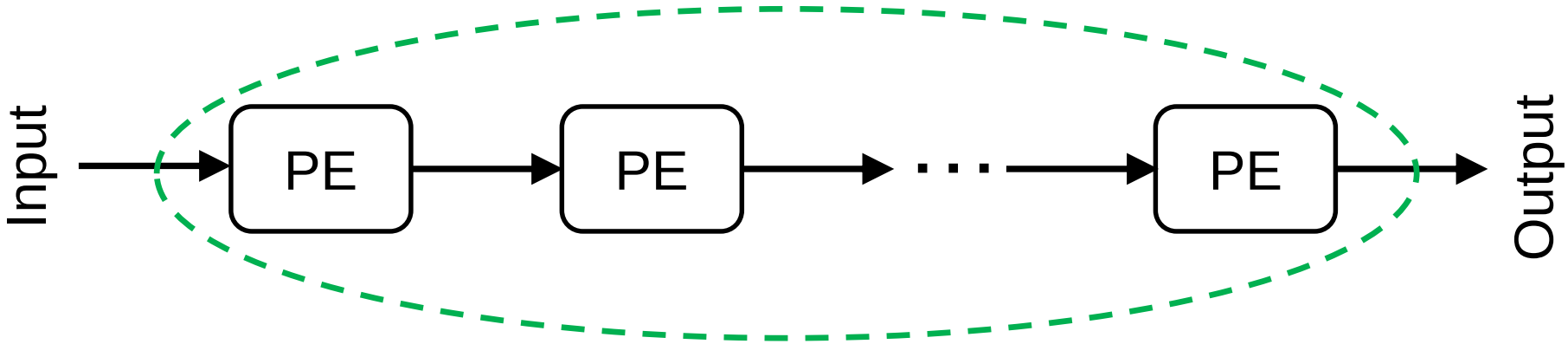
Type-II: each PE is obfuscated with different obfuscation techniques

(a) it is very hard to keep all obfuscated PE's performance in the same level

(b) large number of PEs, quite burdensome

Security issue-I: identicality of PEs

Security concerns

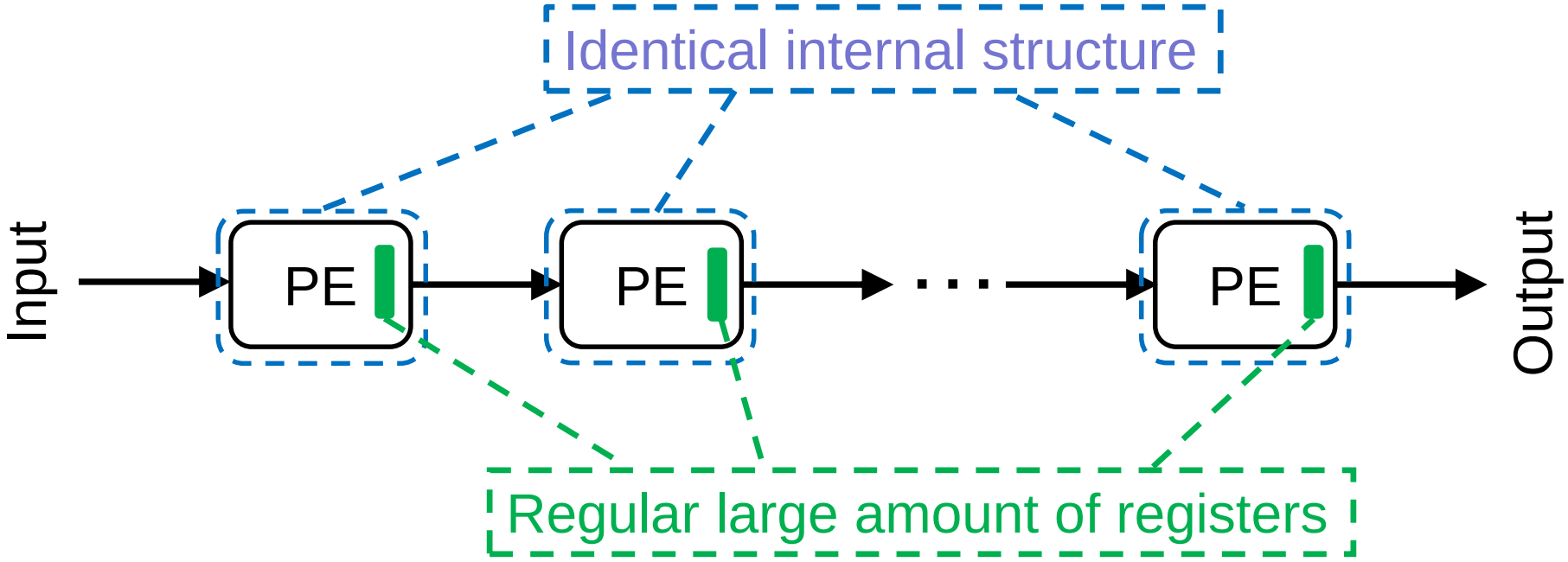


Challenge: how to obfuscate it?

Because of the regular arrangement of these registers (high density) within PEs of systolic circuits. It will be easy for the attacker to isolate all the PEs individually one by one.

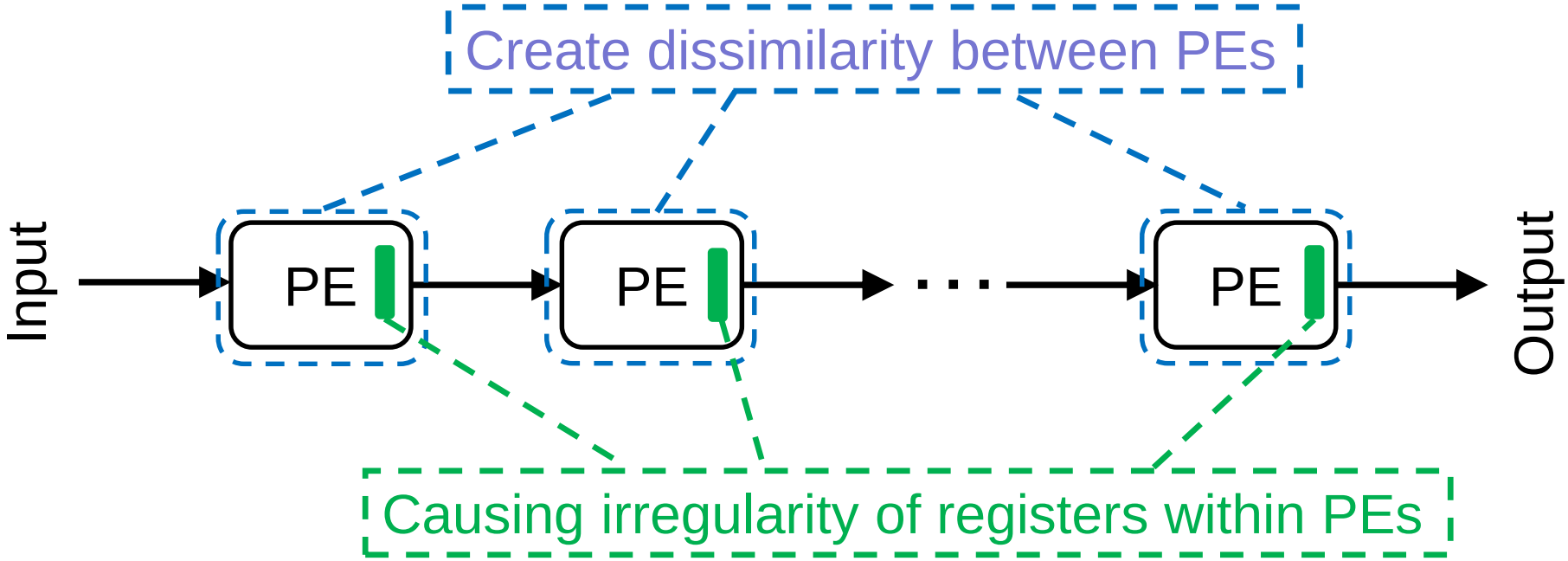
Security issue-II: regularity of registers in PEs

Security concerns



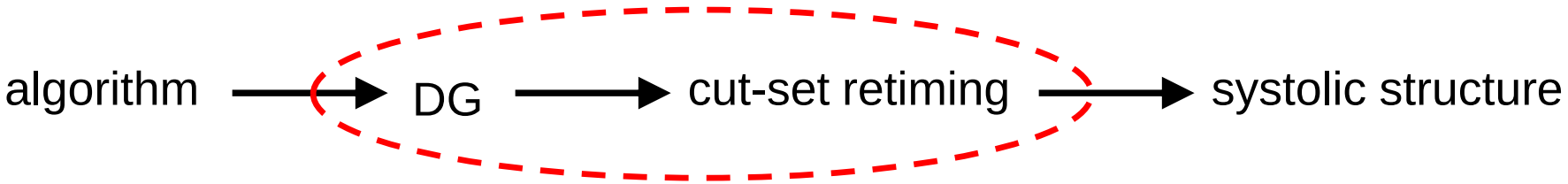
Identical internal structures of PEs and registers can deteriorate the overall obfuscation performance

Security concerns



Two potential ideas

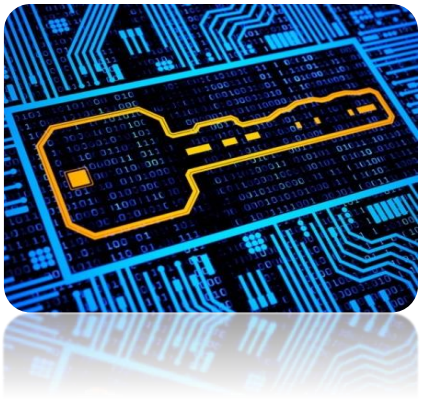
Security concerns



Proposal: novel algorithm-to-architecture mapping techniques to solve or eliminate the negative impacts brought by these two fundamental issues for further employing the obfuscation techniques

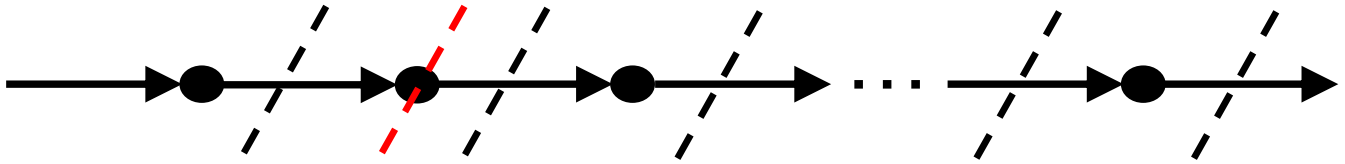
Begin with fundamental design strategy aspect

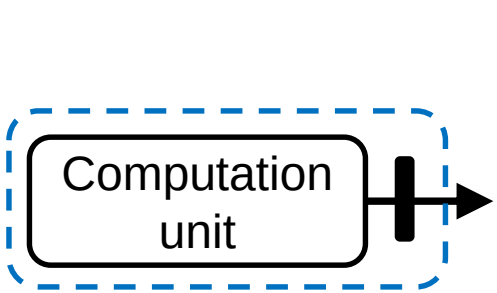
Contents

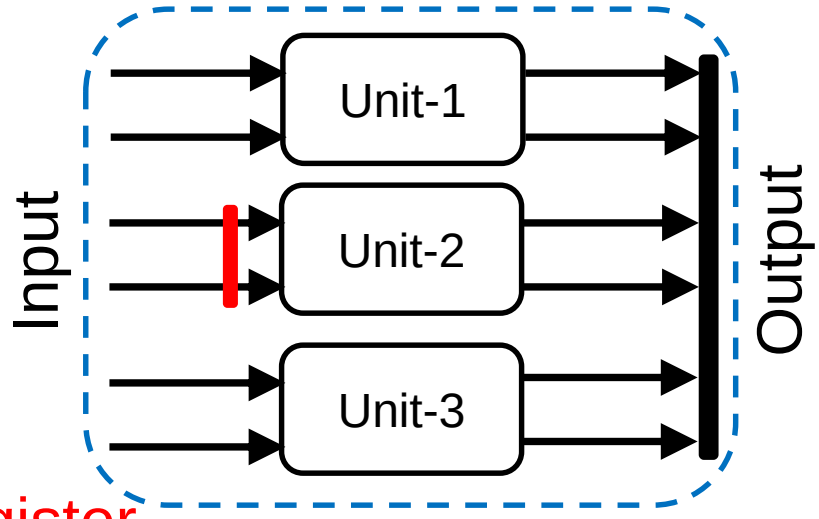


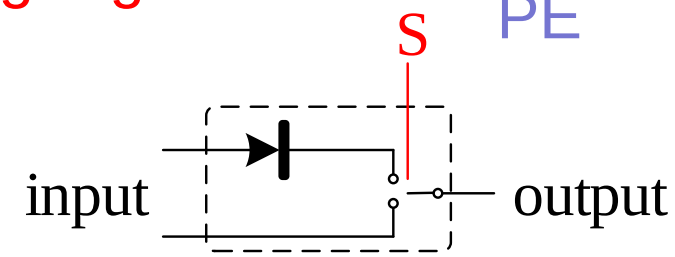
- Background and security analysis
- Proposed strategy
- Conclusion and discussion
- References

I: Irregular cut-set retiming





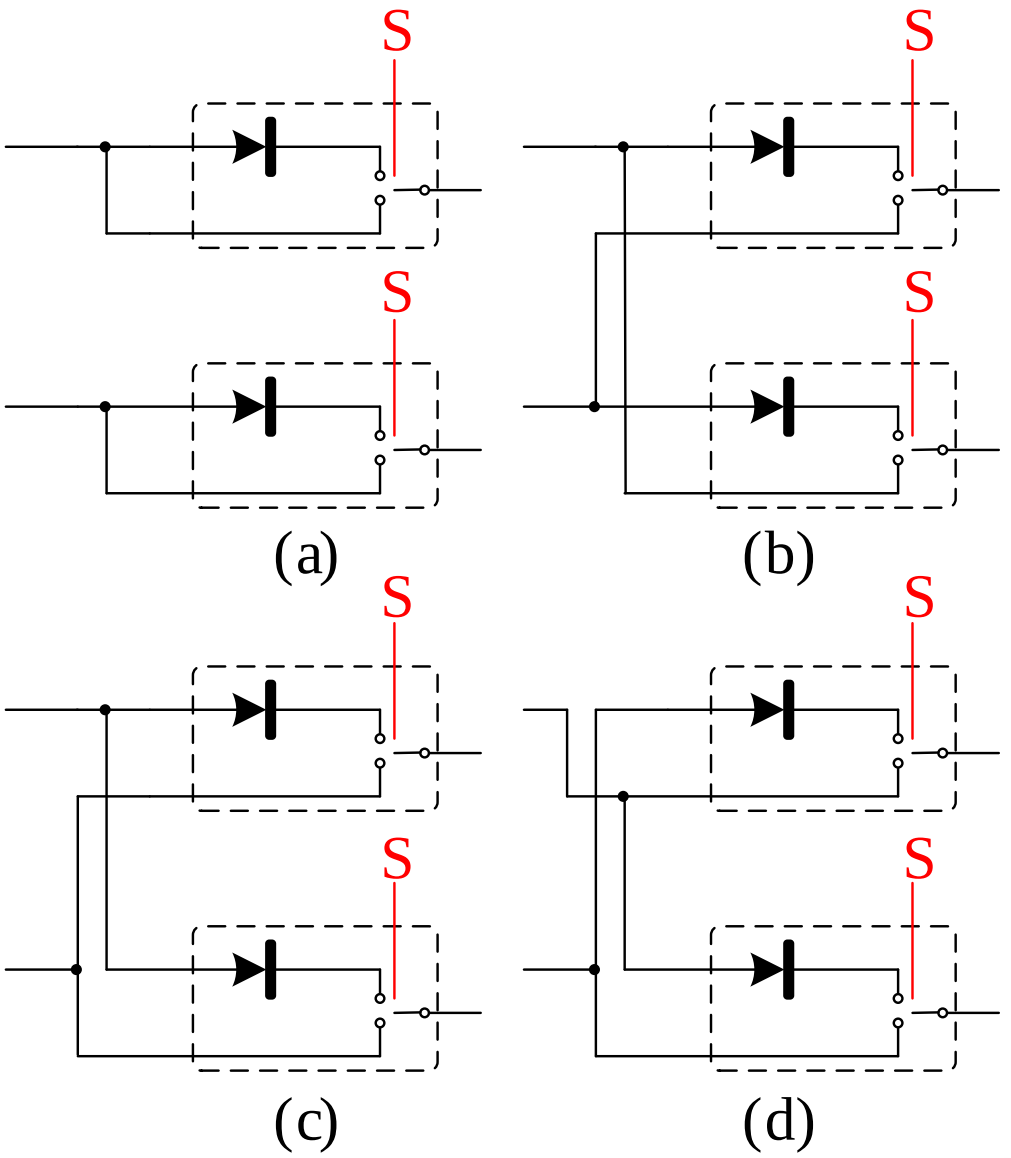




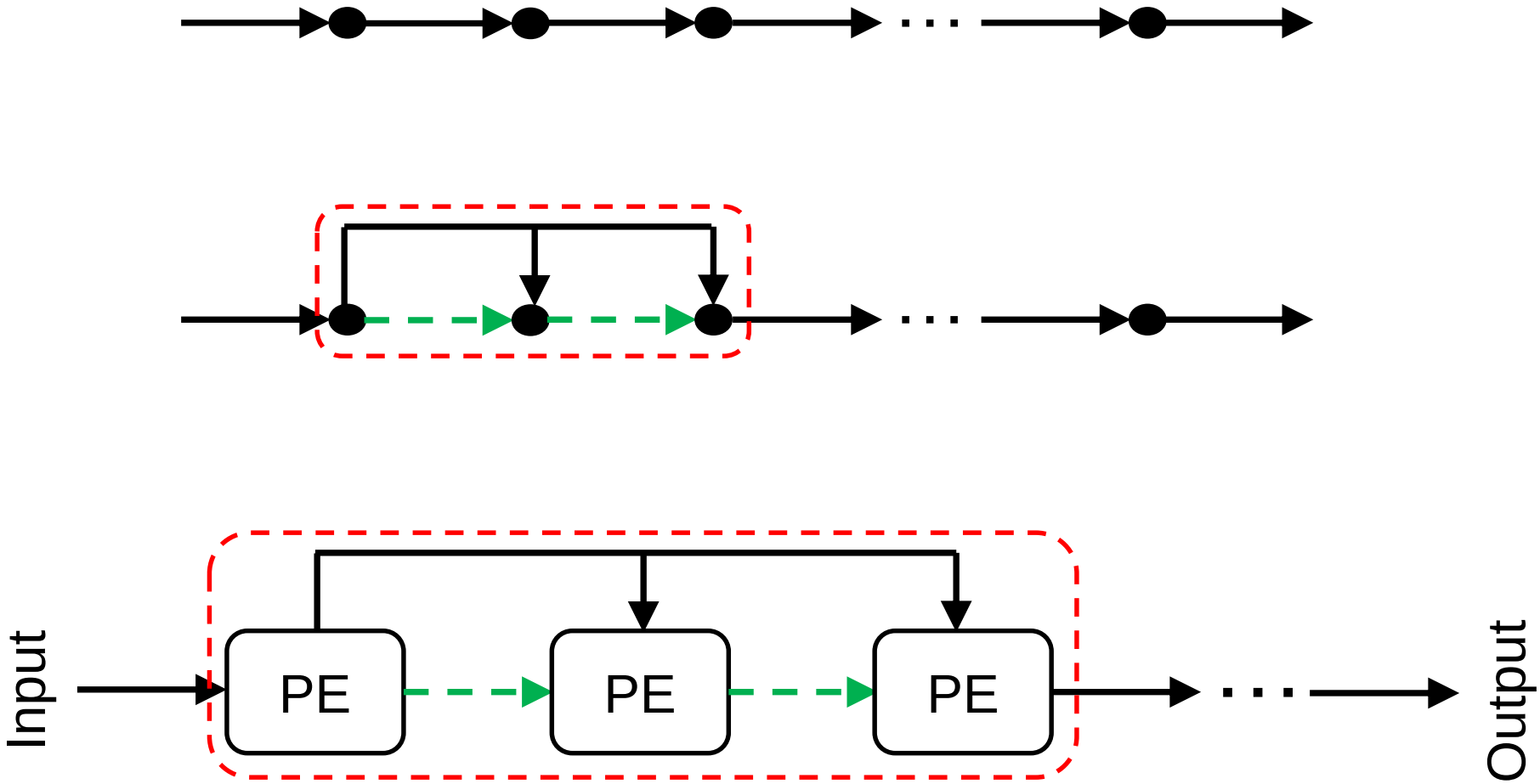
Mapping Technique-I

Examples of inputs connecting with switching register

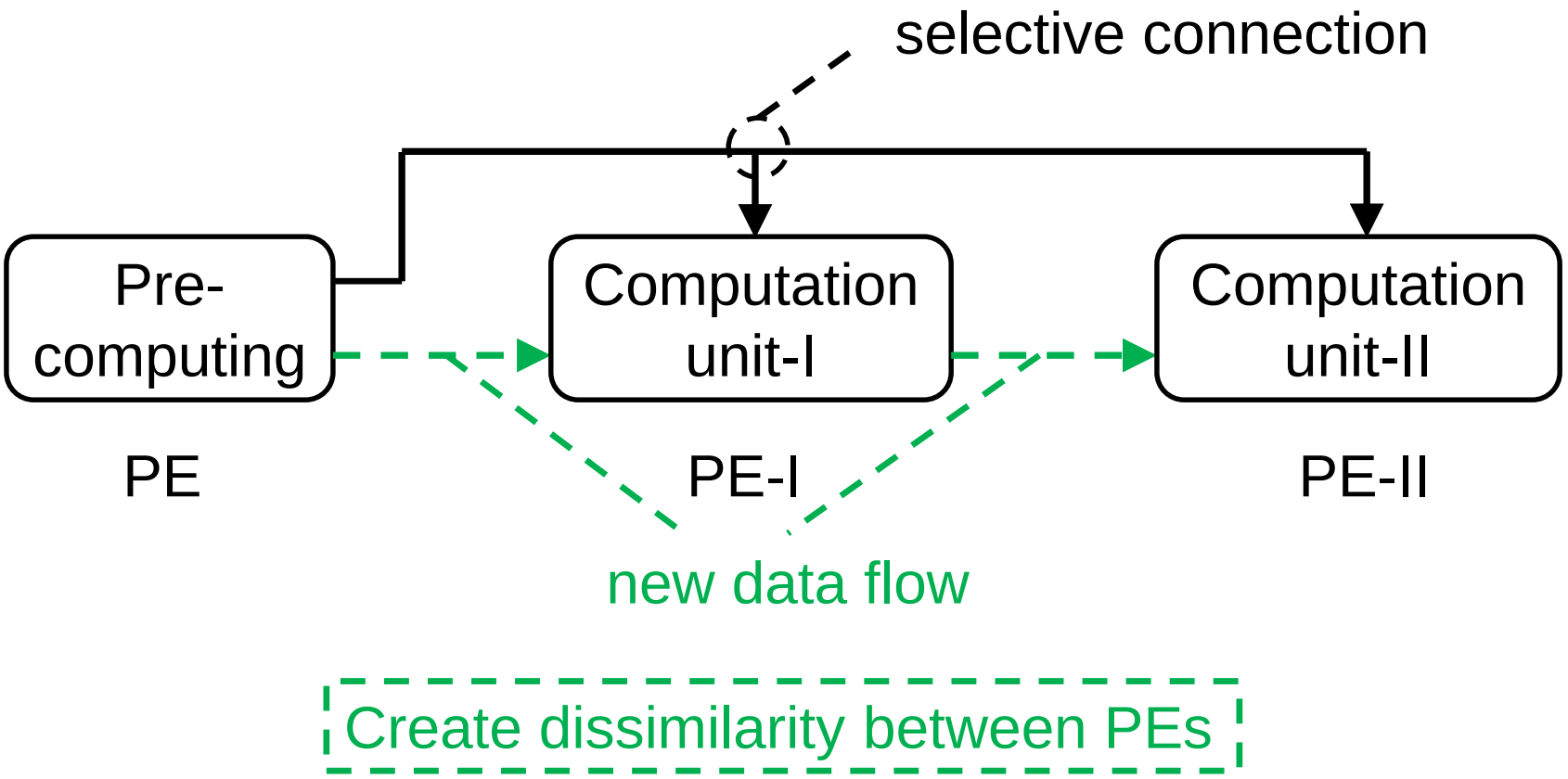
Causing irregularity of registers within PEs



II: Partial broadcasting



II: Partial broadcasting



Further discussion

The proposed techniques, however, when applying to various kinds of systolic-based structures, may vary a little on the detailed internal structures while still follow the same principle, strategy, and concept proposed here.

Evaluation

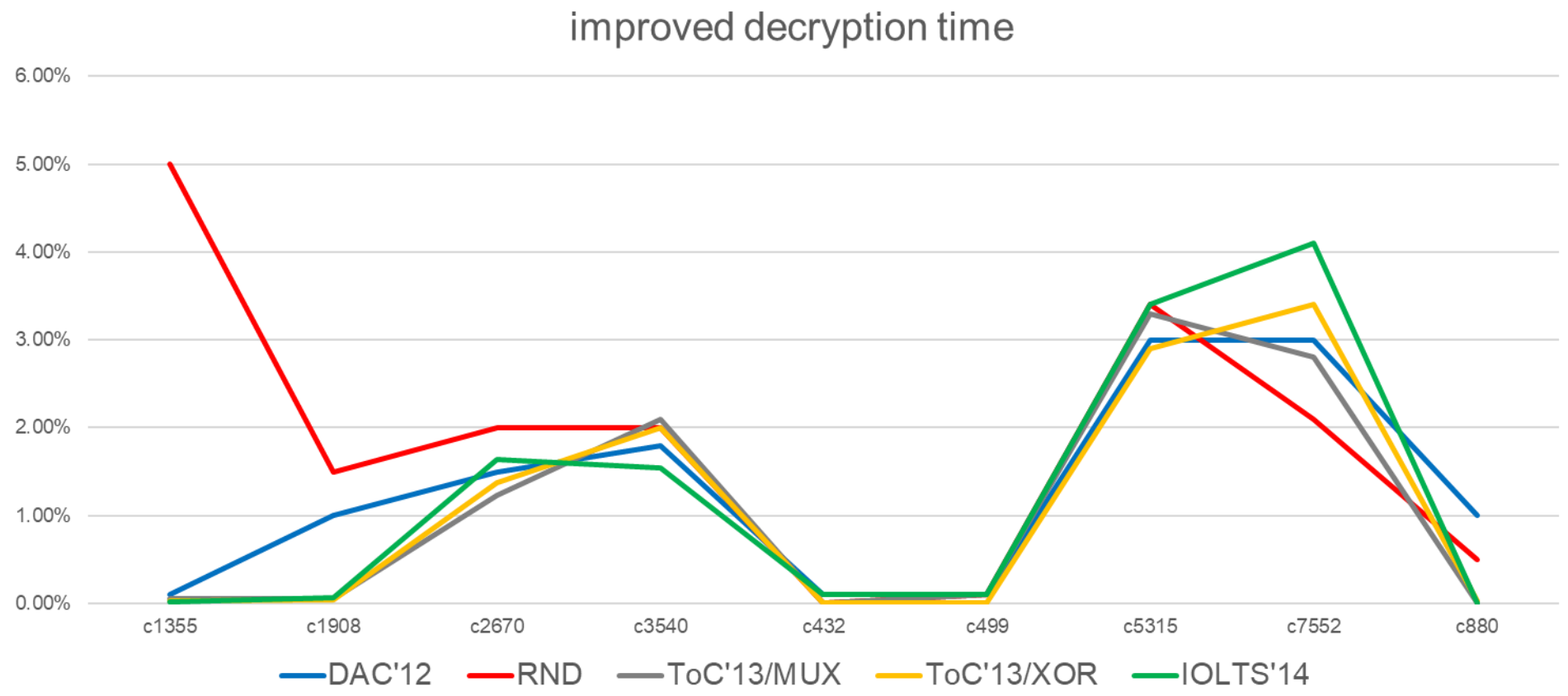
No standard test-systolic-structure exist. Thus,

Irregular cut-set retiming setup. In this step, employ standard ISCAS’85 benchmark circuits (in total 9 circuits, excluding c17 and c6288)

SAT solver from [12]

[12] S. Pramod, S. Ray, and S. Malik, “Evaluating the security of logic encryption algorithms,” Hardware Oriented Security and Trust (HOST), 2015 IEEE Inter. Symposium on. IEEE, 2015.

Evaluation



Results of improved decryption time (based on the irregular cut-set retiming) over the conventional obfuscated PE

Evaluation

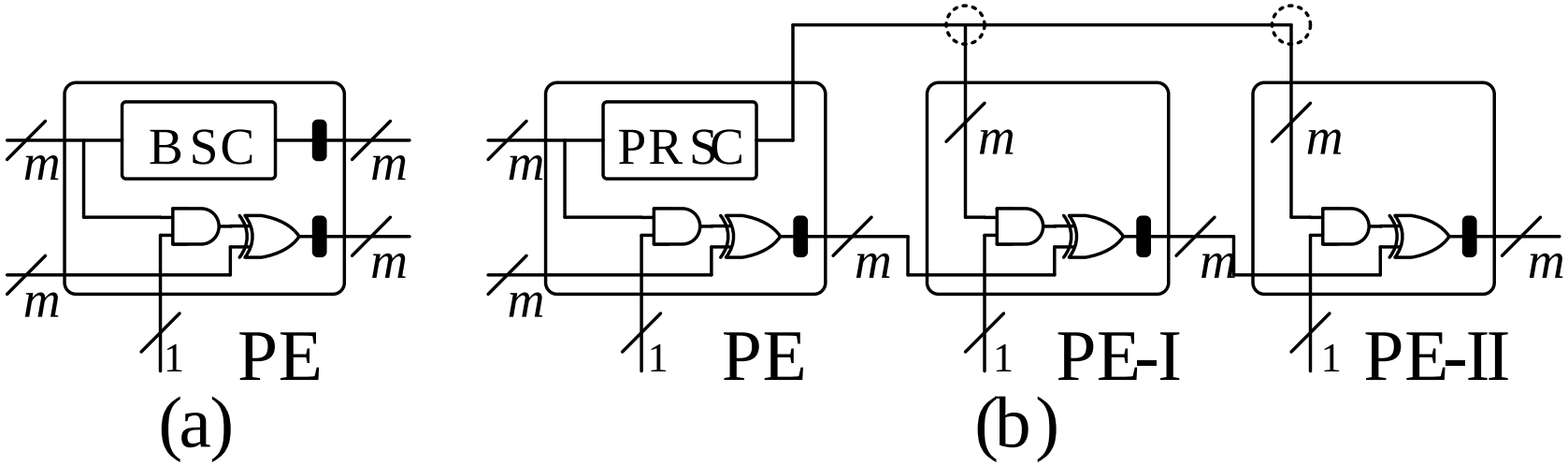
WRIGHT STATE UNIVERSITY

No standard test-systolic-structure exist. Thus,

Partial broadcasting setup. Since all the benchmark circuits of ISCAS’85 have different input and output pin numbers, they cannot simply be embedded in all the PEs to be connected to form a practical systolic-structure (for systolic structure, usually the output of a PE should match the input of next PE followed). We propose to use a systolic structure of finite field multiplier over GF(2m) based on all-one-polynomials (AOP)

SAT solver from [12]

Evaluation

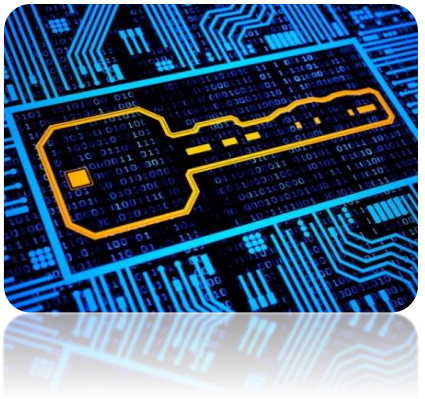


Evaluation

OT[1]	AO[1]	AO[2]	AO[3]	IDT[4]
“RND”	5%	-33%	5%	30%
“DAC 12”	5%	-33%	5%	31%
“ToC” 13/XOR	5%	-33%	5%	35%
“TOC” 13/MUX	5%	-33%	5%	28%
“IOLTS” 14	5%	-33%	5%	27%

OT[1]: Obfuscation techniques being applied.
AO[1]: Area overhead, refers to the area overhead of the PEs compared with the original one, based on the existing obfuscation strategy.
AO[2]: Refers to the area (register) overhead of the PEs compared with the original one, based on the partial broadcasting strategy.
AO[3]: Refers to the area overhead of the PEs compared with the original one, based on the partial broadcasting strategy and the existing obfuscation strategy.
IDT[4]: Improved decryption time.

Contents



- Background and security analysis
- Proposed strategy
- Conclusion and discussion
- References

Conclusion and discussion

WRIGHT STATE UNIVERSITY

The work proposed improves the obfuscation performance for systolic-based circuits.

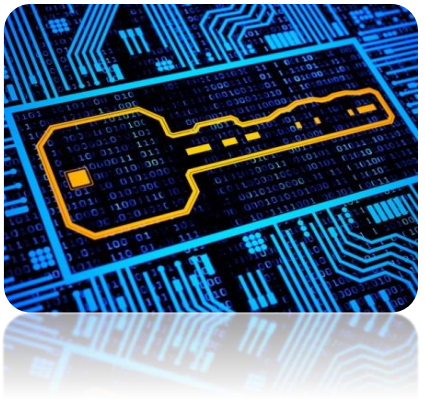
Future development directions:

(i) Further propose novel algorithm-to-architecture mapping techniques

(ii) Develop a test-structure and specific attack algorithm for systolic-based circuits

(iii) Explore novel obfuscation techniques to holistically obfuscate the whole systolic array-based circuits rather than the single PE.

Contents



- Background and security analysis
- Proposed strategy
- Conclusion and discussion
- References

References

RND: J. A. Roy, F. Koushanfar, and I. L. Markov, “EPIC: Ending piracy of integrated circuits,” In Proceedings of Design, Automation and Test in Europe, 2008.

DAC 12: J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, “Security analysis of logic obfuscation,” In Proceedings of the Design Automation Conference, 2012.

ToC 13/XOR & ToC 13/MUX: J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, “Fault analysis-based logic encryption,” IEEE Transactions on Computers, 64(2), Feb 2015.

ILOTS 14: S. Dupuis, P.-S. Ba, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, “A novel hardware logic encryption techniquefor thwarting illegal overproduction and hardware trojans,” In IEEE Inter. On-Line Test. Symp., 2014.


Thank you