SaTC: CORE: Medium: Collaborative: Countermeasures Against Side-Channel Attacks Targeting Hardware and Embedded System Implementations of Post-Quantum Cryptographic Algorithms

Mehran Mozaffari Kermani, University of South Florida

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1801488

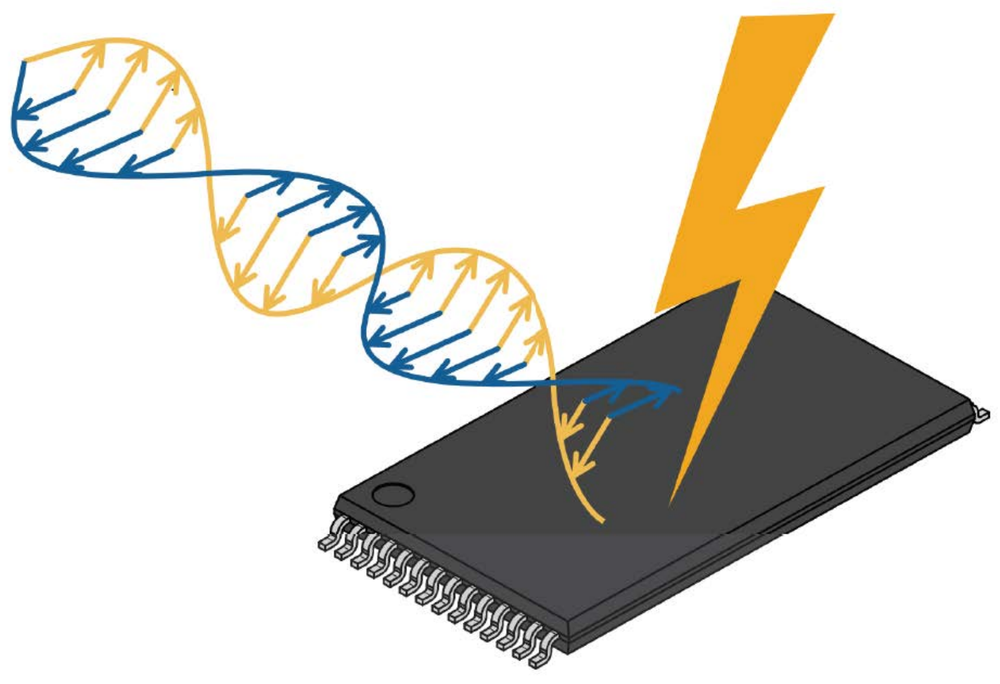
Motivation:

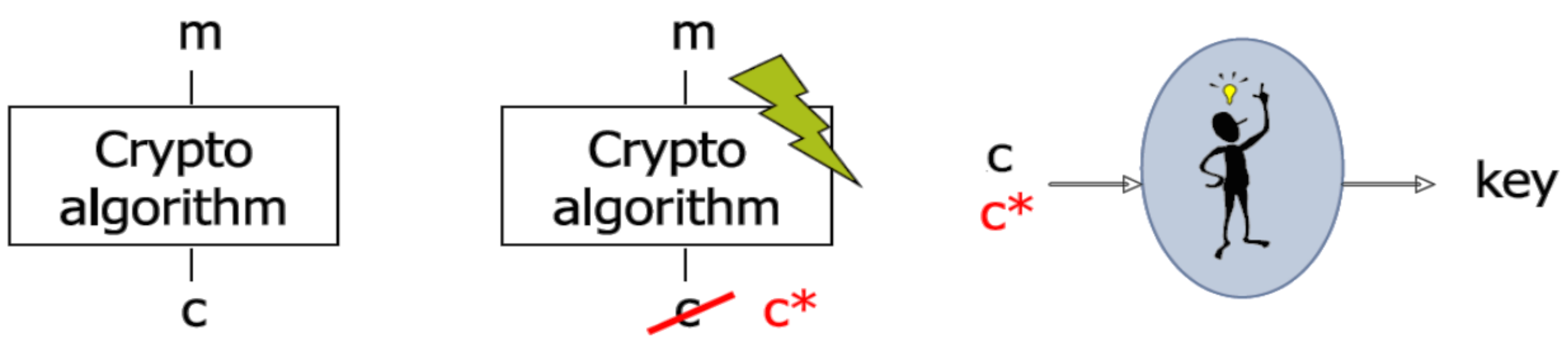
Post-Quantum Cryptography (PQC) is devoted to the design and analysis of cryptographic algorithms resistant against attacks using quantum computers. Investigating side-channel analysis attacks for PQC needs to be explored to reach innovative solutions.

- NIST PQC standardization does not directly include side-channel analysis to scrutinize the candidates or assess the countermeasures.
- Fair assessment for side-channel attack analysis security and cost is challenging but essential.
- Combined side-channel attacks and countermeasures, e.g., fault/power analysis assessment is critical for PQC.

Example:

Fault attacks and countermeasures on PQC





McEliece Operations and Corresponding Processes

Operation	Process
Goppa Division	Key Generation, Decryption
Goppa Multiplication/Addition	Key Generation, Encryption, Decryption
Goppa Squaring	Key Generation
Goppa Square Root	Decryption
Goppa GDC, Goppa Inversion, and Goppa Polynomial Decomposition	Key Generation, Decryption
Goppa Polynomial Evaluation	Key Generation, Decryption

	Signatures		KEM/ Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

Architecture	Area (occupied slices)	Delay (ns)	Power (mW) @50 MHz	Throughput (Gbps)	Error Coverage Percentage	Xilinx FPGA family and device
GPE	1370	4.205	0.205	3.09	Not Applicable	Kintex-7 (xc7k70tfbv676-1)
GPE with Normal Sign.	1447 (5.62%)	4.494 (6.87%)	0.213 (3.90%)	3.12 (0.97%)	$100 \cdot (1-(\frac{1}{2})^{6\cdot10^3})\%$	
GPE with Two-Part Sign.	1484 (8.32%)	4.415 (4.99%)	0.213 (3.90%)	3.17 (2.59%)	$100 \cdot (1-(\frac{1}{2})^{1.2\cdot10^4})\%$	
GPE with Three-Part Sign.	1487 (8.54%)	4.402 (4.68%)	0.213 (3.90%)	3.18 (2.91%)	$100 \cdot (1-(\frac{1}{2})^{1.8\cdot10^4})\%$	
GPE	1339	5.386	0.219	2.41	Not Applicable	Spartan-7 (xc7s100fgga676-1)
GPE with Normal Sign.	1470 (9.78%)	5.461 (1.39%)	0.225 (2.74%)	2.56 (6.22%)	$100 \cdot (1-(\frac{1}{2})^{6\cdot10^3})\%$	
GPE with Two-Part Sign.	1491 (11.35%)	5.431 (0.84%)	0.225 (2.74%)	2.58 (7.05%)	$100 \cdot (1-(\frac{1}{2})^{1.2\cdot10^4})\%$	
GPE with Three-Part Sign.	1467 (9.57%)	5.440 (1.00%)	0.225 (2.74%)	2.57 (6.64%)	$100 \cdot (1-(\frac{1}{2})^{1.8\cdot10^4})\%$	

Broader Impacts:

Through publications in prestigious venues (IEEE/ACM Transactions for example), project deliverables have been made available to researchers and educators in the non-profit sector, such as universities, research institutions, and government laboratories. We have developed dedicated courses, disseminated the results, hired NSF-funded REUs, employed women/minority graduate researchers, and utilized schemes for broadening participation in computing.

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting)
June 1-2, 2022 | Arlington, Virginia