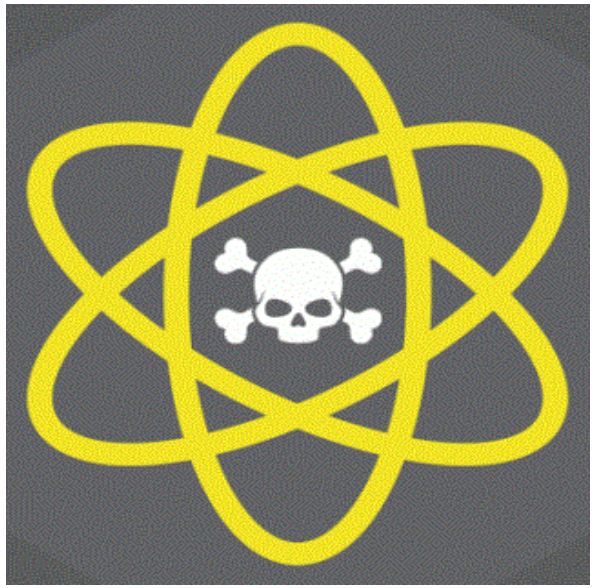
Quantum Physical Unclonable Functions: Possibilities and Impossibilities

Myrto Arapinis, Mahshid Delavar,
Mina Doosti and Elham Kashefi

QCRYPT2019
https://eprint.iacr.org/2019/1181

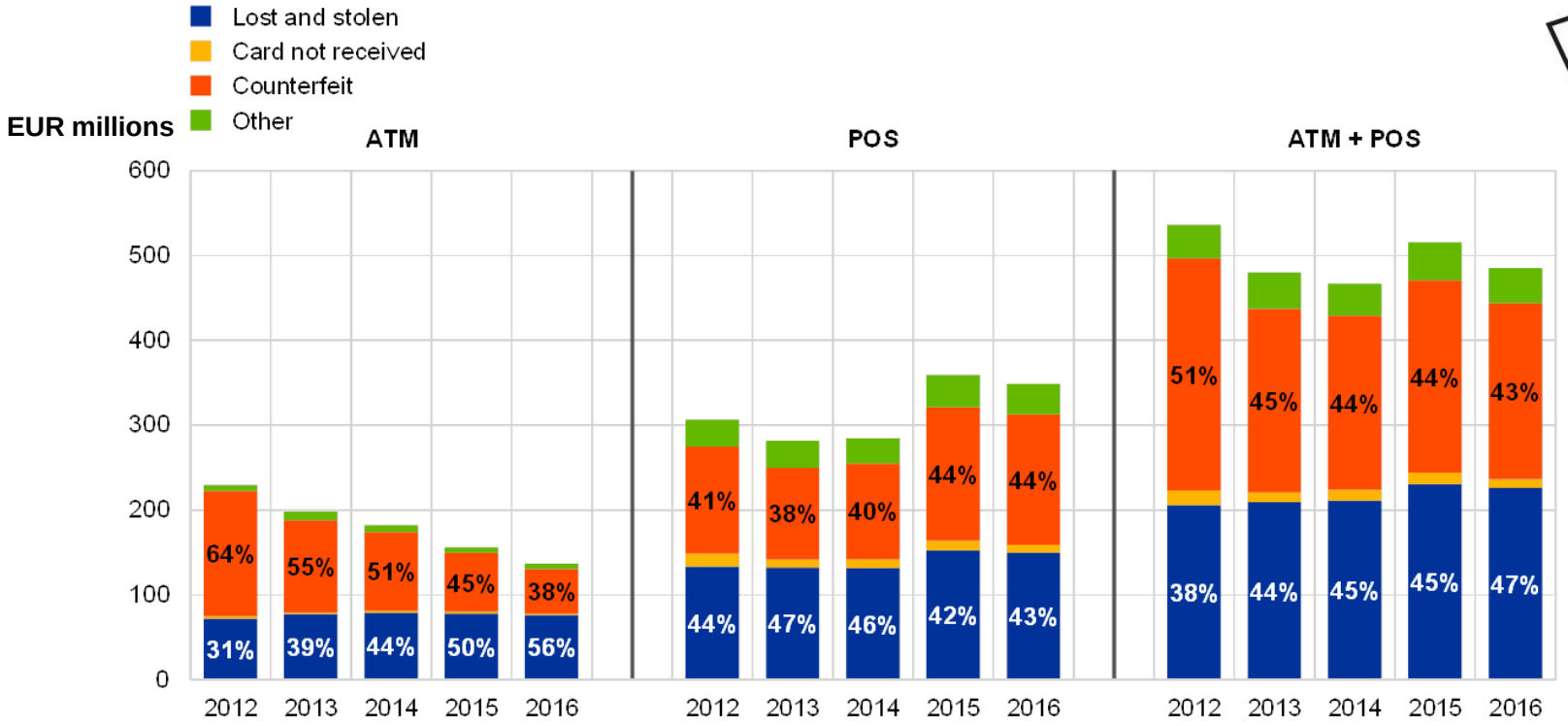



SOCIETE GENERALE
MARC DEMONCEAU
PRESENTER LA CARTE


Transport

International losses due to card skimming have *raised from €87* ***million*** *in 2018 to €100* ***million*** *in 2019*

European ATM Security Team (EAST)
https://www.association-secure-transactions.eu/tag/card-skimming/



European Central Bank, Fifth report on card fraud, September 2018
https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html#toc1

The Problem

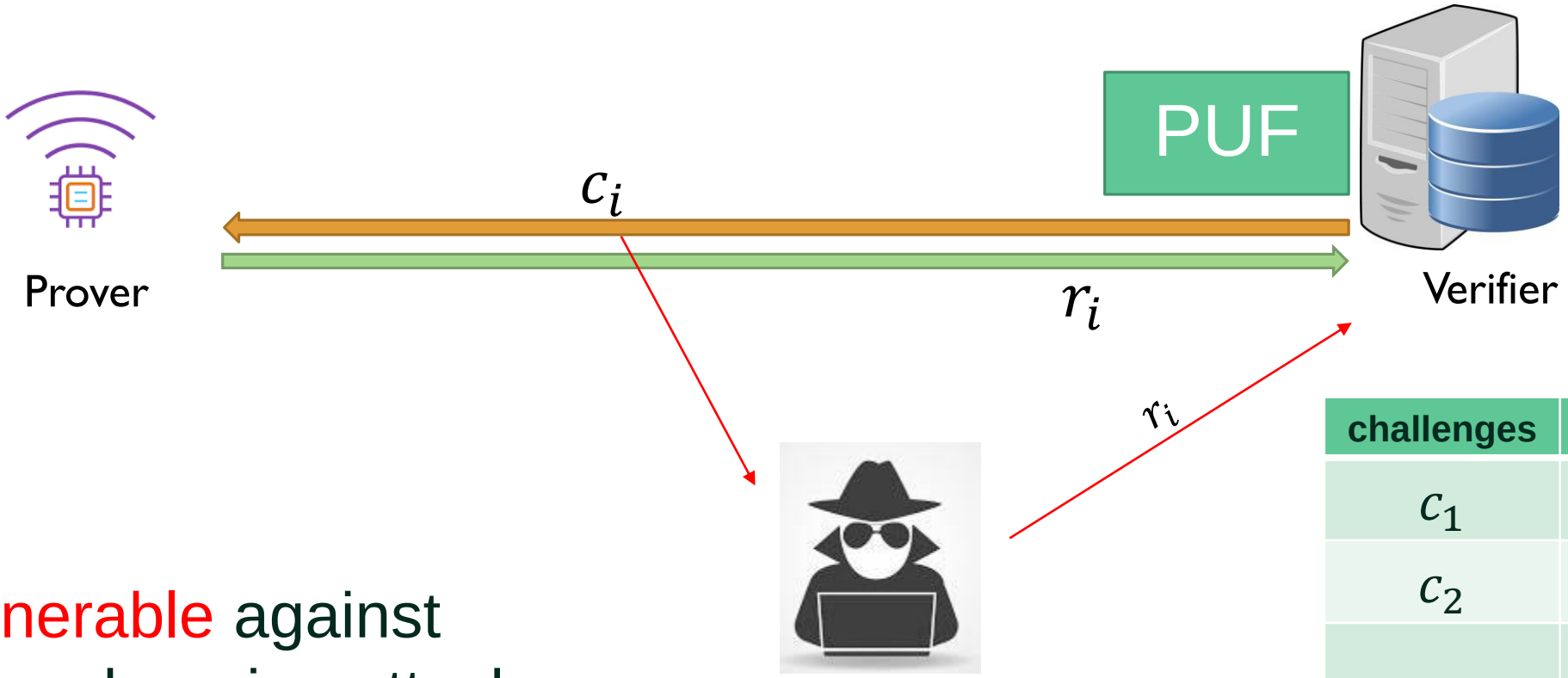
Storing the sensitive data in the non-volatile memories

The Solution

Physical Unclonable Functions (PUFs)

Unique Features ≡ Set of Challenge-Response Pairs (CRPs)

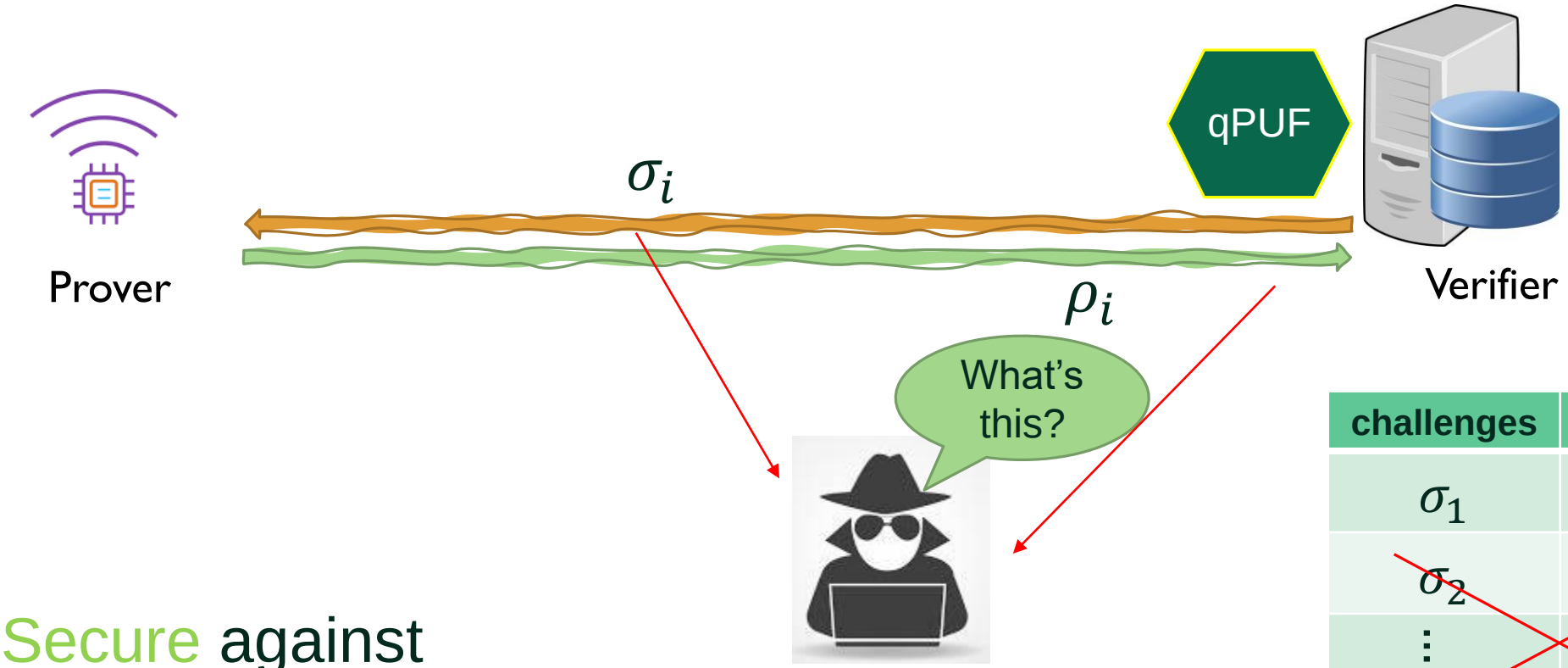
PUF-based Identification Protocol



challenges	responses
c_1	r_1
c_2	r_2
...	...
c_k	r_k

Vulnerable against eavesdropping attack

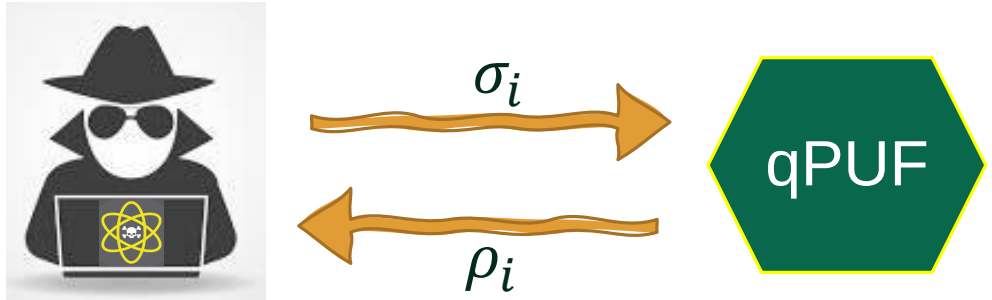
qPUF-based Identification Protocol



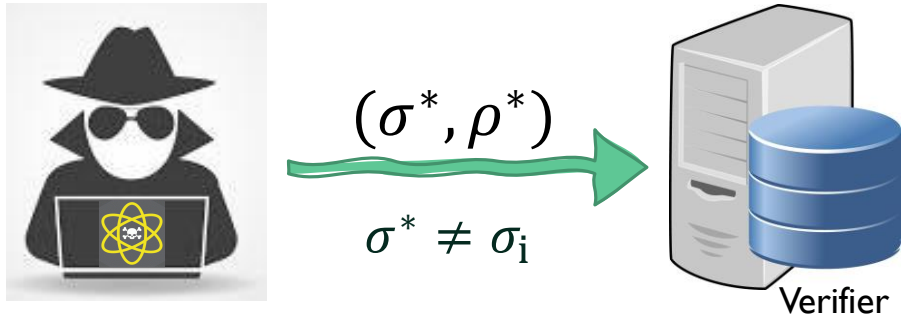
challenges	responses
σ_1	ρ_1
~~σ_2~~	~~ρ_2~~
⋮	⋮
~~σ_k~~	~~ρ_k~~

Secure against eavesdropping attack

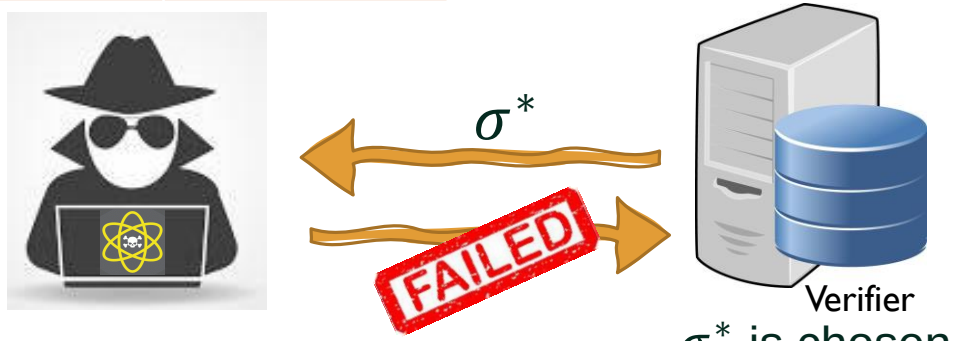
But how about security against a Quantum Polynomial-Time (QPT) adversary who has access to the qPUF and can query it polynomial number of times?



challenges	responses
σ_1	ρ_1
σ_2	ρ_2
⋮	⋮
σ_k	ρ_k



challenges	responses
σ_1	ρ_1
σ_2	ρ_2
⋮	⋮
σ_k	ρ_k



σ^* is chosen uniformly at random from the whole challenge space

Conclusion

qPUFs are quantum secure (unforgeable) hardware cryptographic primitives and can be used in different applications.

Future Work

- Analysing the quantum security of classical PUFs
- Design of provable secure qPUF-based protocols

Email: Mdelavar@ed.ac.uk
Mahshid.Delavar@gmail.com