Client-Server Identification Protocols with Quantum PUF

Mina Doosti[1] , Niraj Kumar[1], Mahshid Delavar[1], and Elham Kashefi[1,2]

[1] LFCS, University of Edinburgh, United Kingdom [2] CNRS, LIP6, Sorbonne Université, Paris, France

QCRYPT 2020

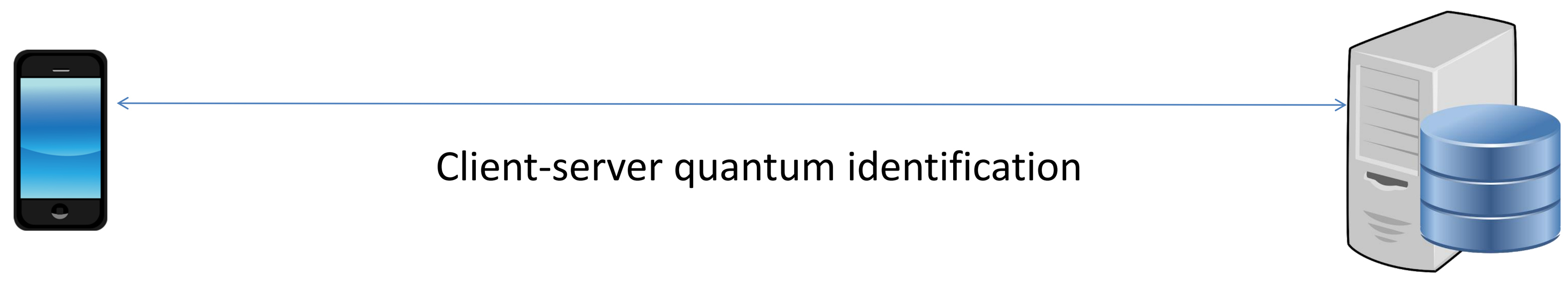
Abstract

The rise of quantum internet has enabled a broad range of applications that would be out of reach for classical internet. Most of these applications such as delegated quantum computation require running a secure identification protocol between a low-resource and a high-resource party. *Physical Unclonable Functions* (PUFs) have been shown as resource-efficient hardware solutions for providing secure identification schemes in both classical and quantum settings. In this work, we propose two identification protocols based on quantum PUFs (qPUFs).

Work highlights:

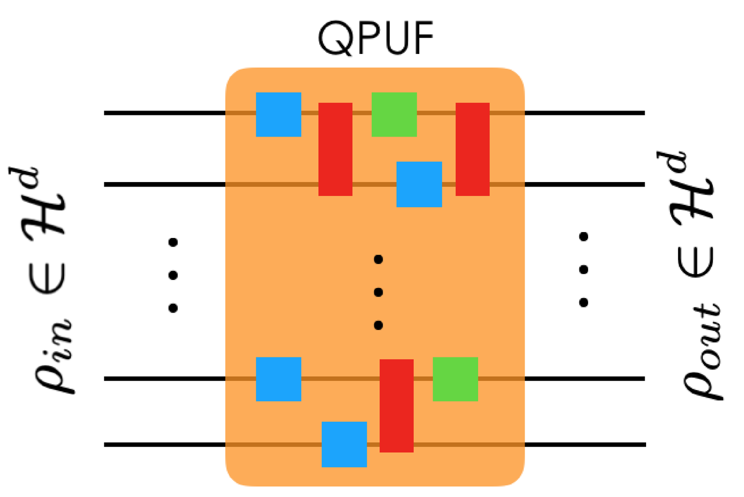
- In the first protocol, the low-resource party wishes to prove its identity to the high-resource party and in the second protocol, it is vice versa.
- Unlike existing identification protocols based on Quantum Read-out PUFs which rely on the security against a specific family of attacks, our protocols provide provable exponential security against any Quantum Polynomial-Time adversary with resource-efficient parties.
- We provide a comprehensive comparison between the two proposed protocols in terms of resources such as quantum memory and computing ability required in both parties as well as the communication overhead.
- A stand-out feature of our second protocol is secure identification of a high-resource party by running a purely classical verification algorithm. This is achieved by delegating quantum operations to the high-resource party and utilizing the resulting classical outcomes for identification.

Mutual quantum identification between client and server



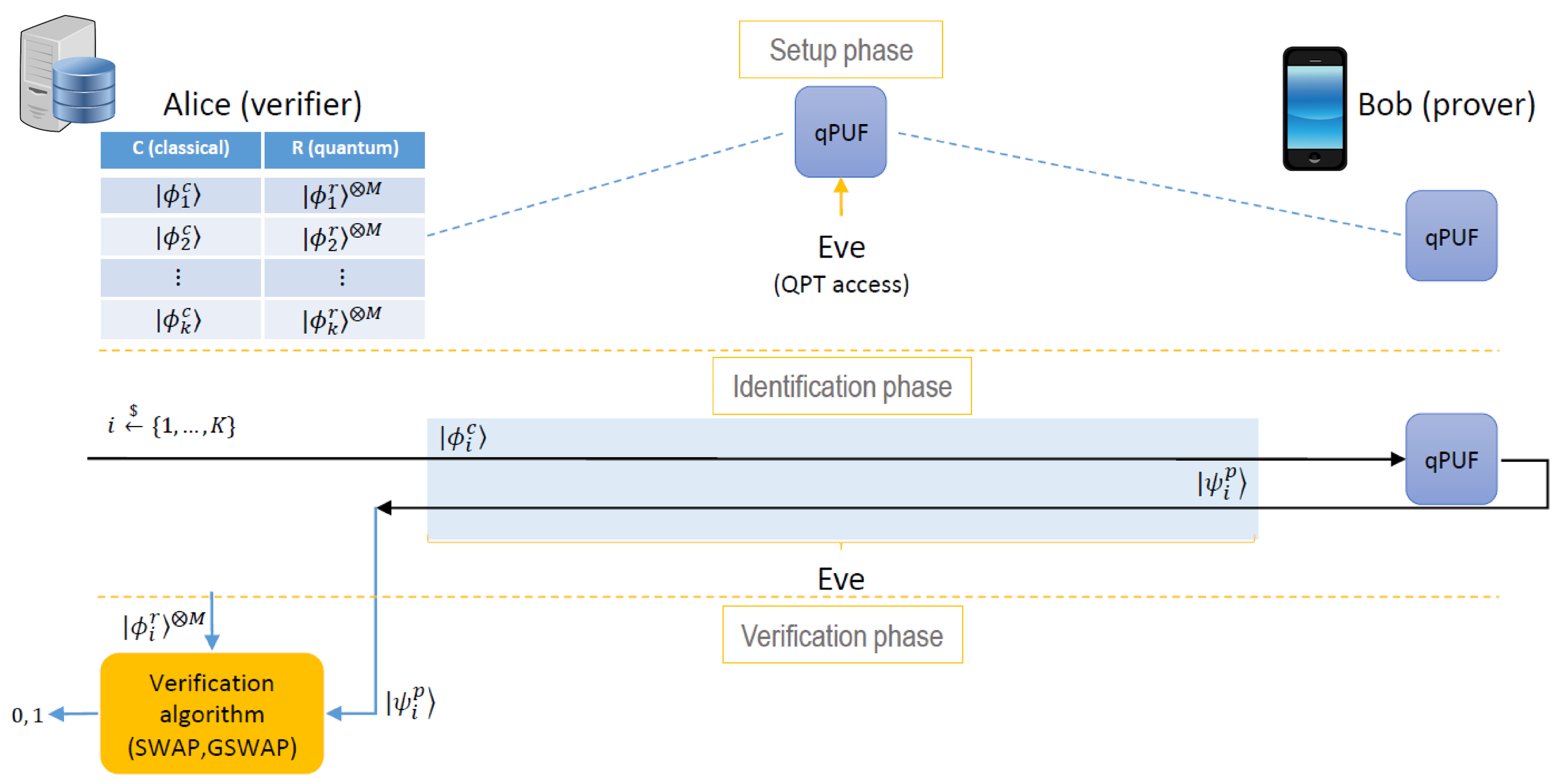
- First scenario: A quantum high-resource party wants to securely identify a low resource, mobile-like client.
- Second Scenario: A low-resource party wants to securely identify a server

Quantum Physical Unclonable Functions (qPUF)



- Cost-efficient hardware tokens
- Unique and unclonable
- Proven unforgeable against QPT adversaries[1]

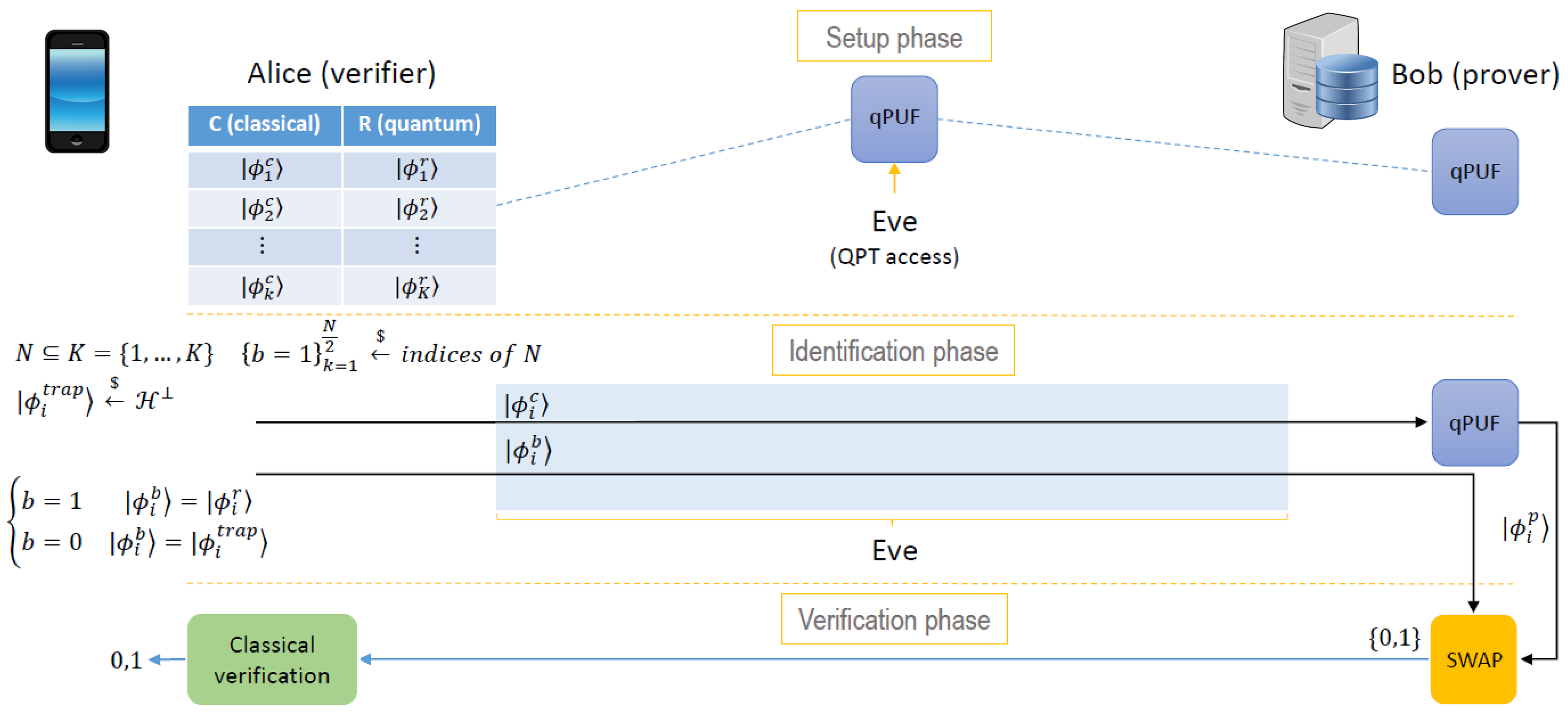
High-resource Verifier Protocol



Features:

- Almost-classical prover (no quantum computing ability required)
- Flexible quantum verification (Using SWAP or GSWAP)
- Exponential security against collective and coherent attacks
- Two-way quantum communication

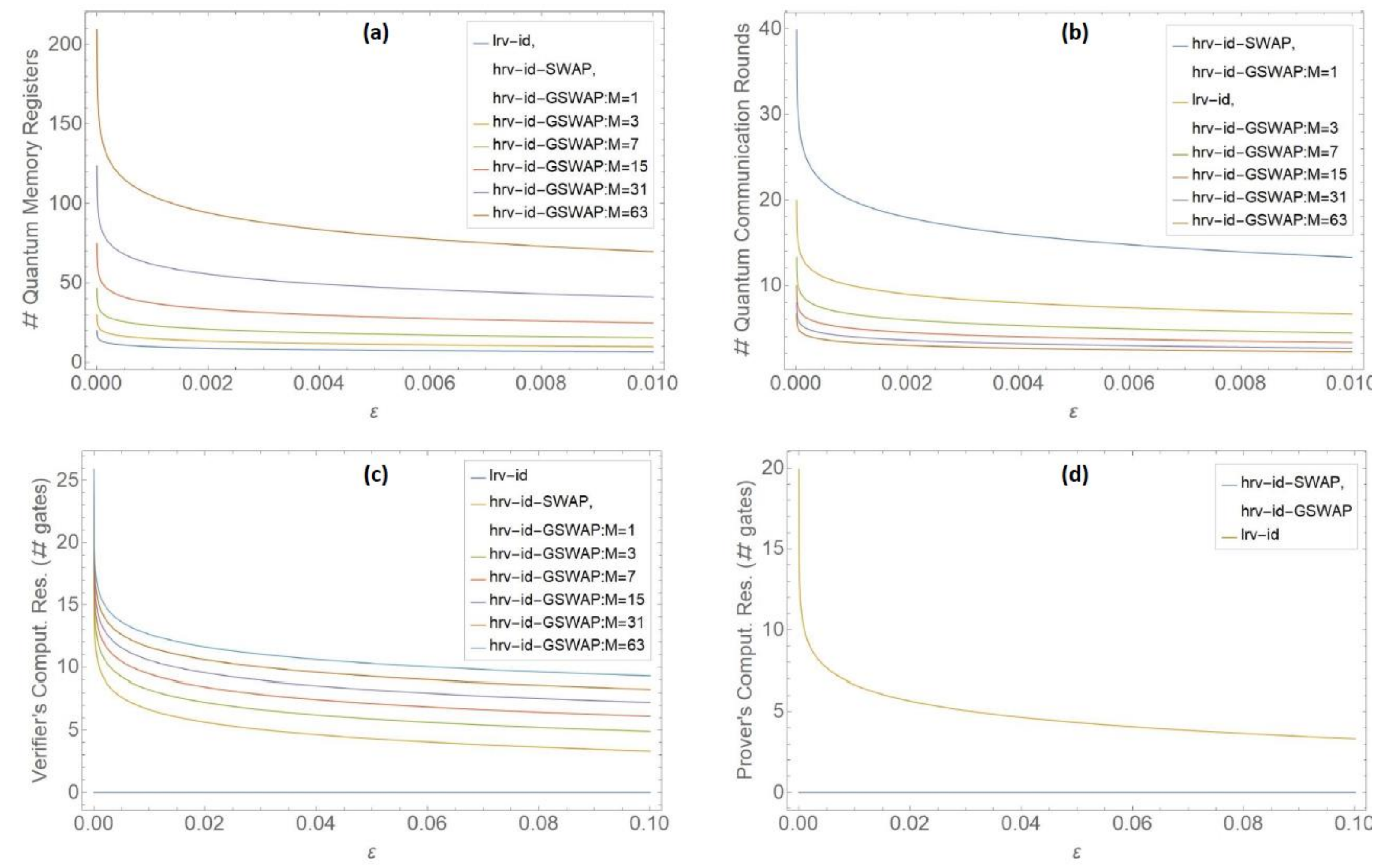
Low-resource Verifier Protocol



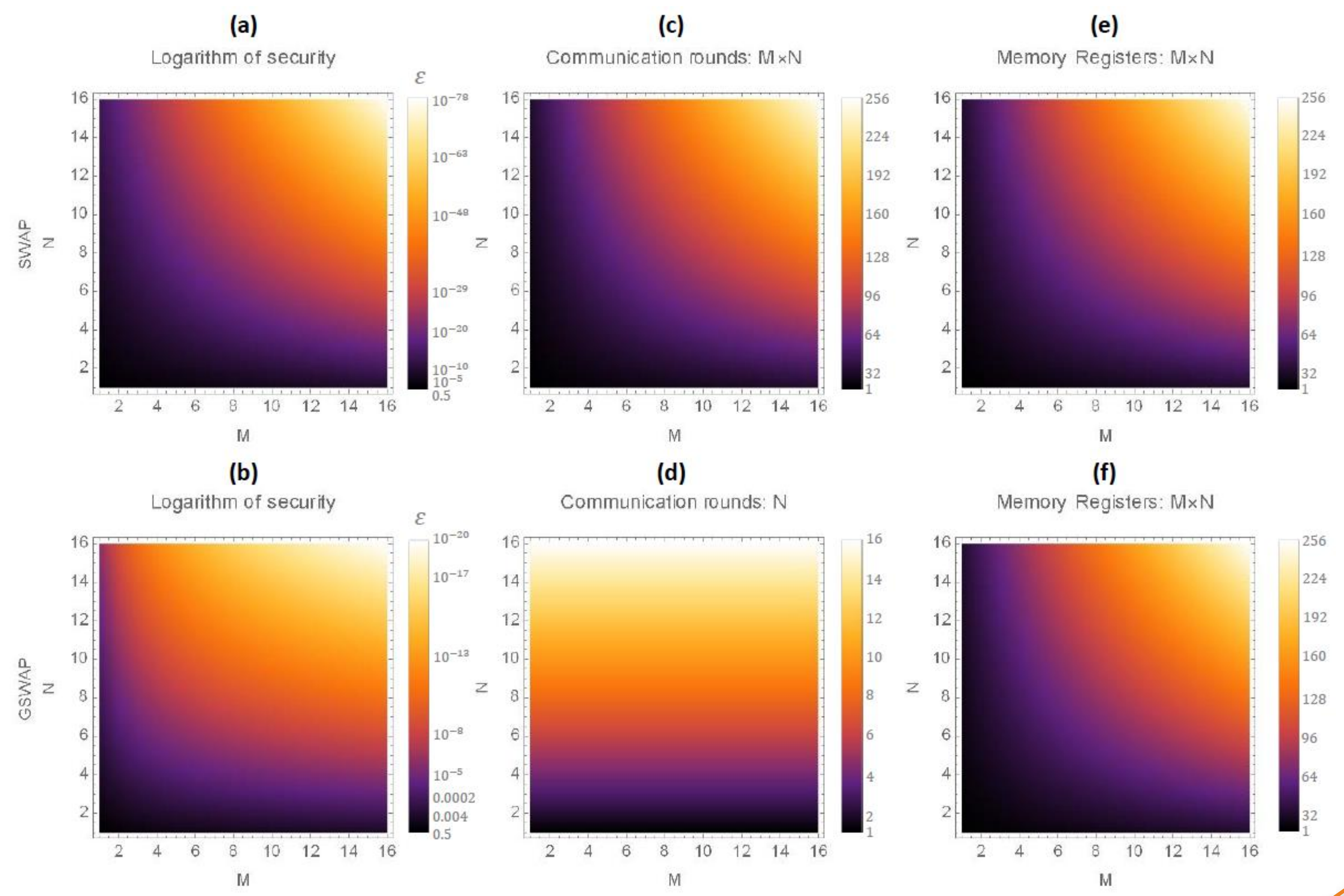
Features:

- Almost classical verifier (no quantum computation ability is required)
- Classical verification algorithm
- Exponential security against collective and coherent attacks
- One-way quantum communication
- The quantum memory requirement can be reduced
- Can be generalized to arbitrary distribution of traps within some valid bounds

Comparison and simulation



Protocol	Security		Quantum Memory		Computing ability		Communication round	
			Verifier	Prover	Verifier	Prover	Quantum	Classical
hrv-id-SWAP	ϵ	$= 2^{-MN}$	$\log 1/\epsilon$	0	$poly \log D$	0	$\log 1/\epsilon$	0
hrv-id-GSWAP		$= (M+1)^{-N}$	$\frac{M}{\log M+1} \log 1/\epsilon$	0	$poly \log MD$	0	$\frac{1}{\log M+1} \log 1/\epsilon$	0
lrv-id		$= 2^{-N}$	$\log 1/\epsilon$	0	0	$poly \log D$	$\log 1/\epsilon$	1



Comparison of SWAP and GSWAP verification

Boris˘Skorĭ c. Quantum readout of physical unclonable functions. InProceedings of InternationalConference on Cryptology in Africa, pages 369–386. Springer, 2010.
Myrto Arapinis, Mahshid Delavar, Mina Doosti, and Elham Kashefi. Quantum physical un-clonable functions: Possibilities and impossibilities.arXiv preprint arXiv:1910.02126, 2019
Ulysse Chabaud, Eleni Diamanti, Damian Markham, Elham Kashefi, and Antoine Joux. Optimal quantum-programmable projective measurement with linear optics.Physical Review A,98(6):062318, 2018

THE UNIVERSITY of EDINBURGH informatics

LIP6

SORBONNE UNIVERSITÉ