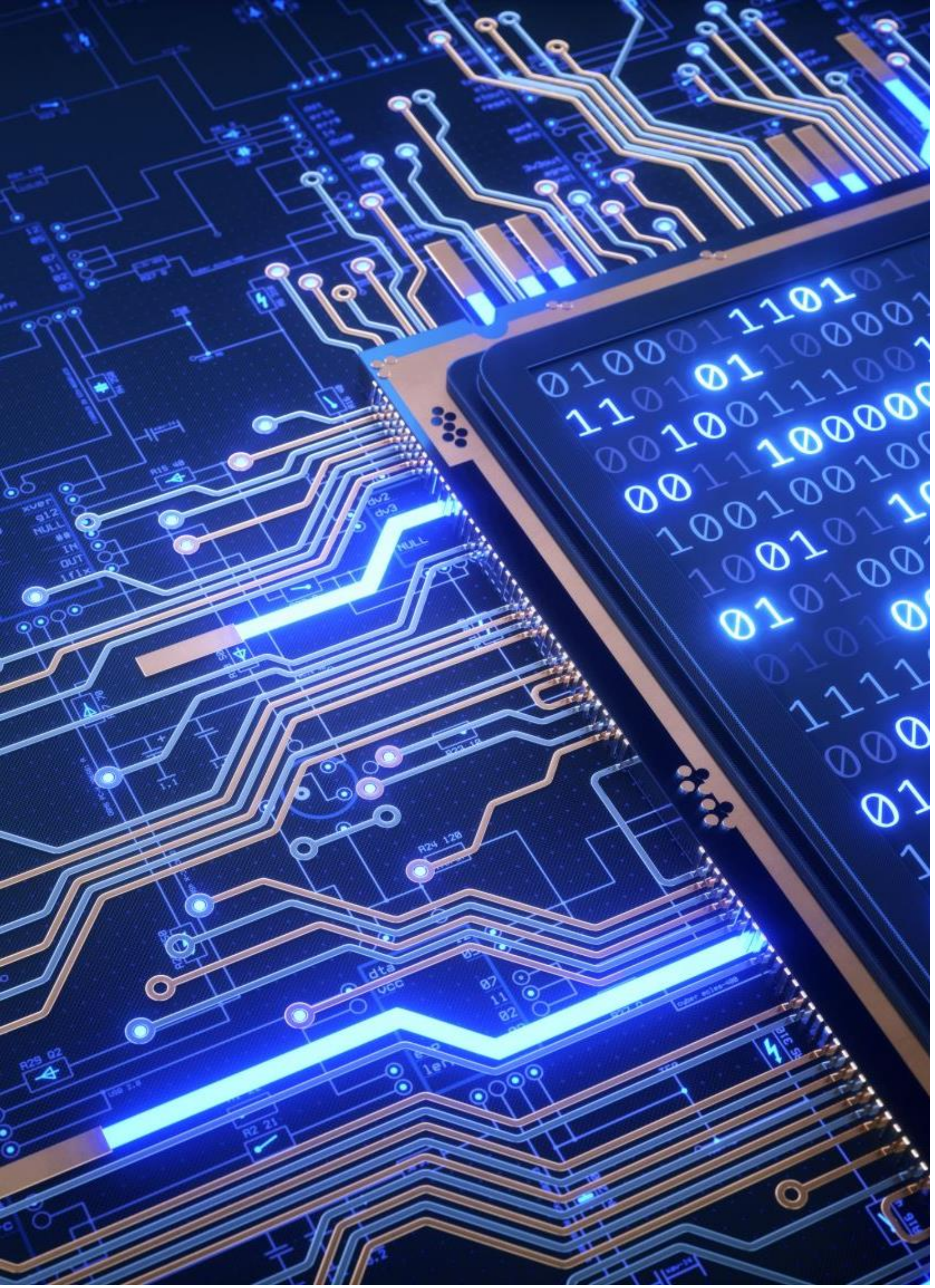


Experimental QKD secure against malicious devices

Víctor Zapatero[1,], Wei Li[2,3,4,*], Feihu Xu[2,3,4] and Marcos Curty[1]*

[1] EI Telecomunicación, Departamento de Teoría de la Señal y Comunicaciones, Universidad de Vigo, Vigo E-36310, España
[2] Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China
[3] Shanghai Branch, CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China
[4] Shanghai Research Center for Quantum Sciences, Shanghai 201315, China

UNIVERSIDADE DE VIGO

arXiv:2006.12863
arXiv:2006.14337

Why bother considering malicious devices in QKD?

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

The Hunt for the Kill Switch

Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out

By **Sally Adee**

The Athens Affair

How some extremely smart hackers pulled off the most audacious cell-network break-in ever

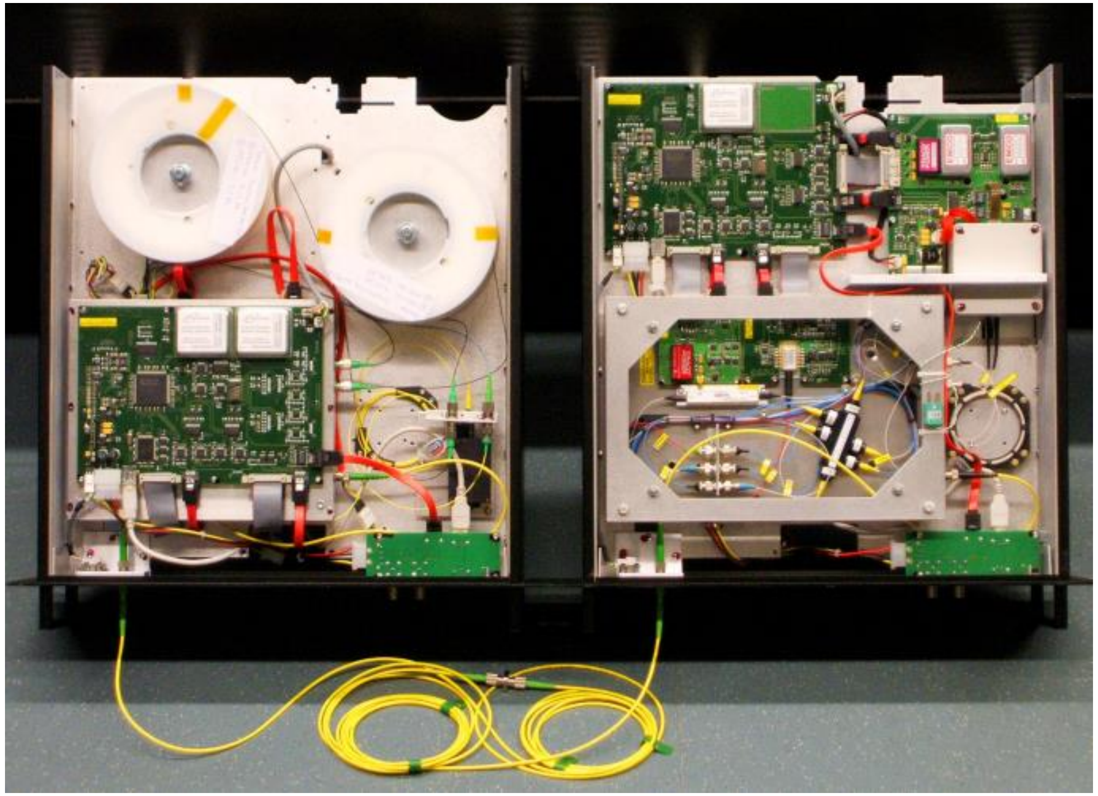
By **Vassilis Prevelakis and Diomidis Spinellis**

What about device-independent QKD? It is not a solution.

Memory Attacks on Device-Independent Quantum Cryptography

Jonathan Barrett, Roger Colbeck, and Adrian Kent
Phys. Rev. Lett. **110**, 010503 – Published 2 January 2013

What about post-fabrication tests?
Ideal but time-consuming and
easily evaded in practice.



The main idea: use redundant QKD equipment

npj Quantum Information

www.nature.com/npjqi

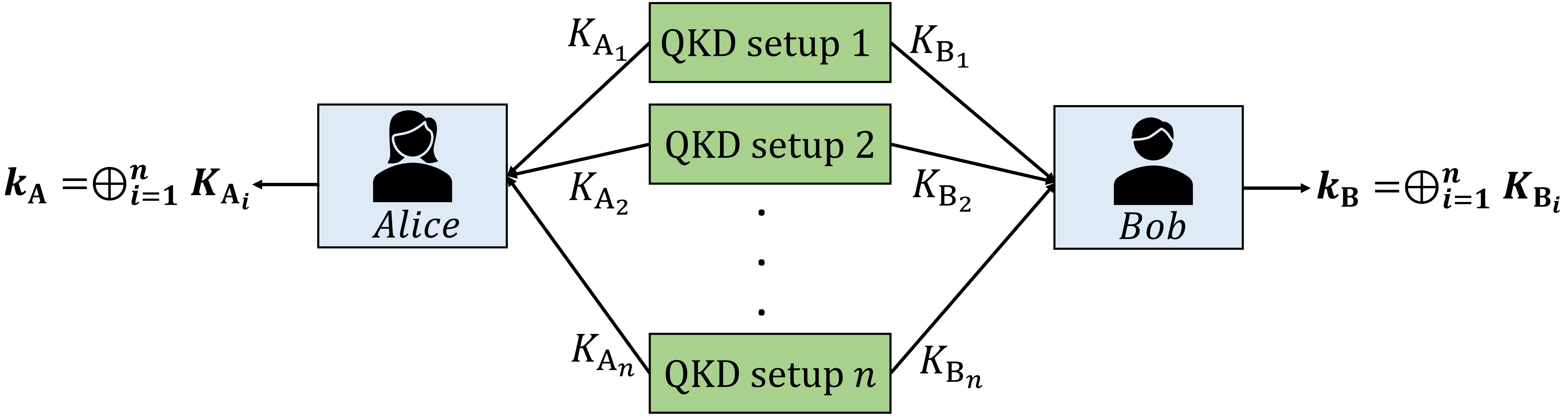
ARTICLE OPEN

Foiling covert channels and malicious classical post-processing units in quantum key distribution

Marcos Curty[1] and Hoi-Kwong Lo[2]

The parties should use a redundant number of QKD devices and assume that a limited number of them is corrupted. In this scenario, security can be restored by combining two well-known techniques: **verifiable secret sharing (VSS)** and **privacy amplification (PA)**.

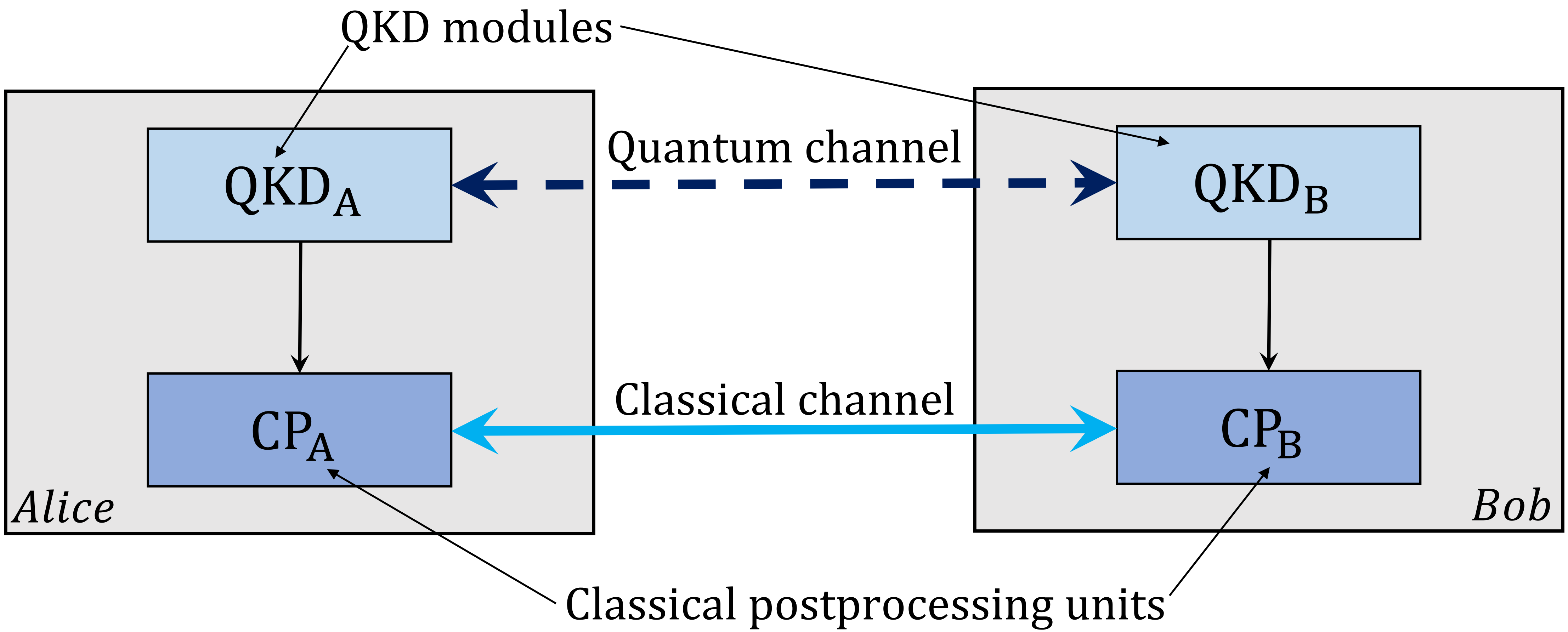
The XOR approach



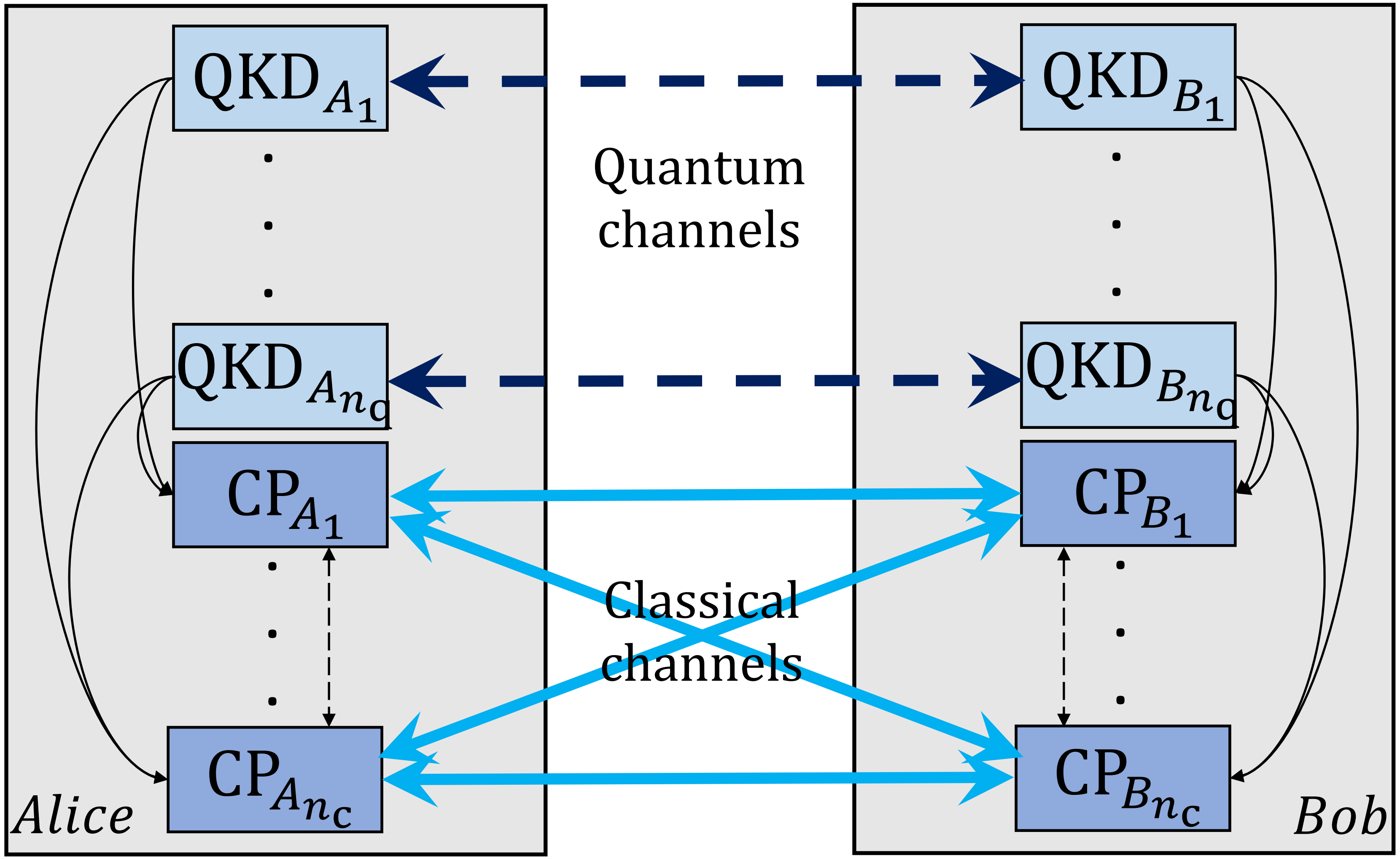
MAJOR PROBLEMS (among others)

(1) Correctness of the final keys is not guaranteed in the presence of actively misbehaving devices.
(2) The approach requires more devices than actually necessary to establish security.

Standard QKD setup with trusted devices



Alternative QKD setup with untrusted devices

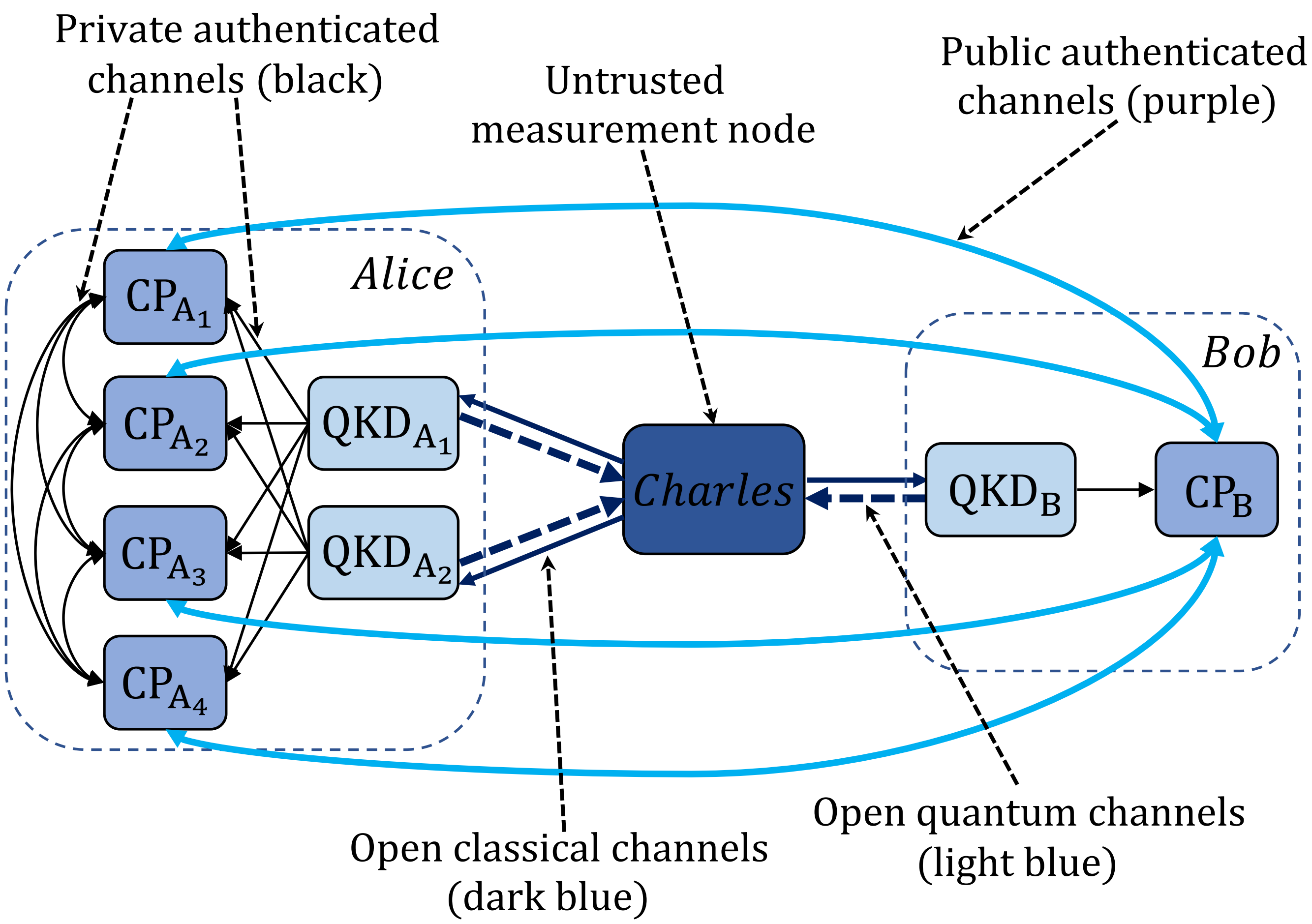


ASSUMPTIONS

1. At least one QKD pair is not corrupted.
2. Less than one third of the CP units are corrupted in each lab.
3. Eve fully controls all the corrupted devices.

Under these assumptions, secure QKD is possible by combining PA with VSS. For alternative models of the corrupted devices, see *V. Zapatero & M. Curty, arXiv:2006.14337 (2020).*

Combining VSS and PA: our setup



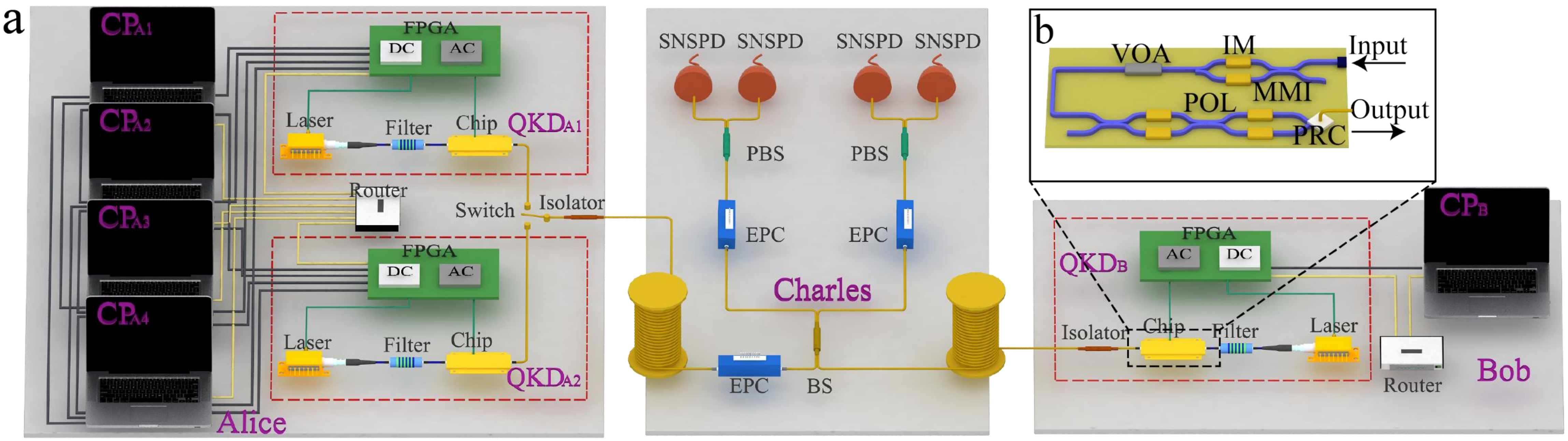
RATIONALE

1. **Multiple QKD sessions**: each QKD pair implements a MDI-QKD session.

2. **VSS**: the post-processing of each key is performed redundantly by Alice's units to assure correctness, and the key material is divided into random shares to be kept private through the process. The linearity of the post-processing operations makes them very easy to implement in the multiparty setting.

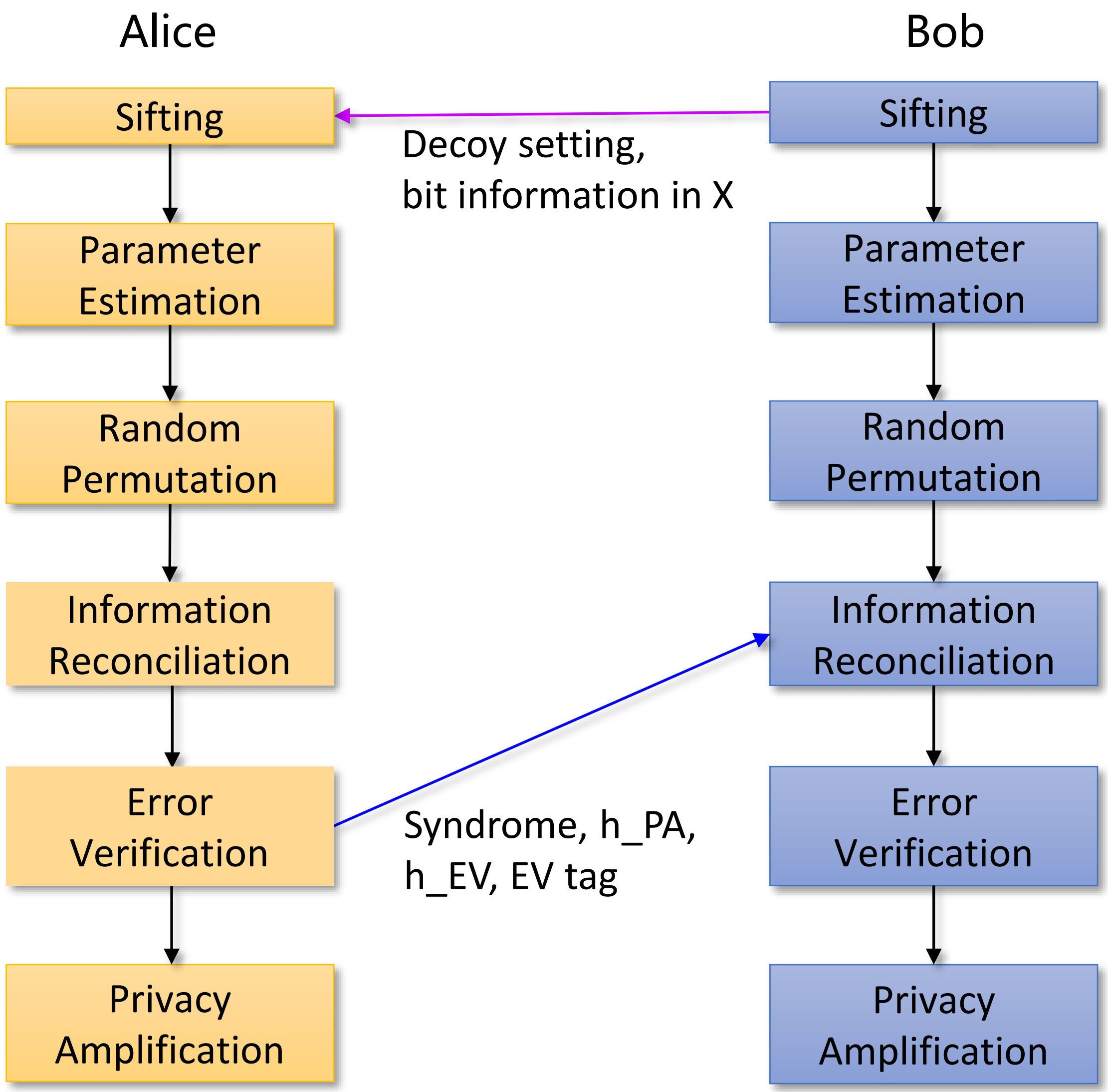
3. **PA**: At the end of the post-processing, PA is applied (also redundantly and share-wise) to remove not only the information Eve learns from the quantum channel, but also the key material coming from the corrupted QKD pair.

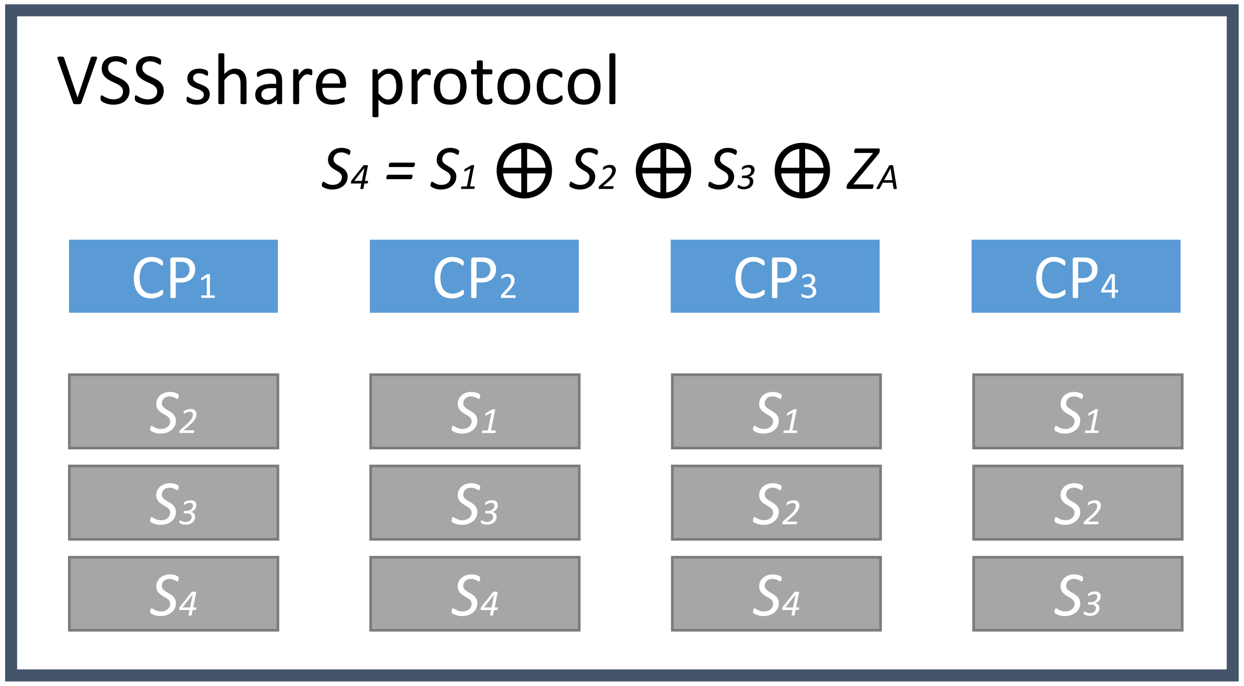
Experimental setup



- 1.25 GHz chip-based MDI-QKD with random modulations
- Silicon chip integrates all the encoding components of the transmitter
- Alice's QKD modules are selected by a switch
- Alice's CP units are connected to each other via dedicated cables

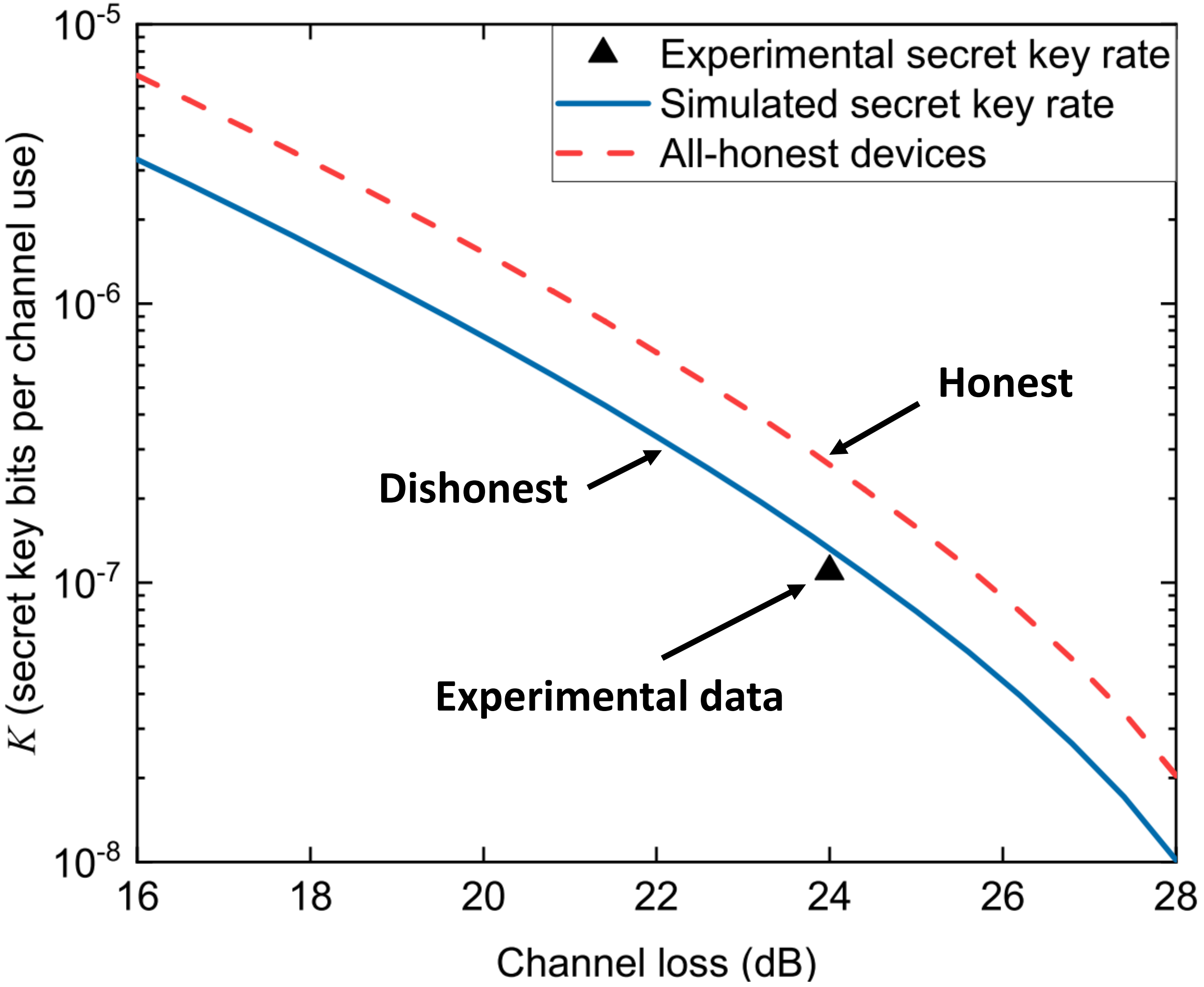
Post-processing with VSS



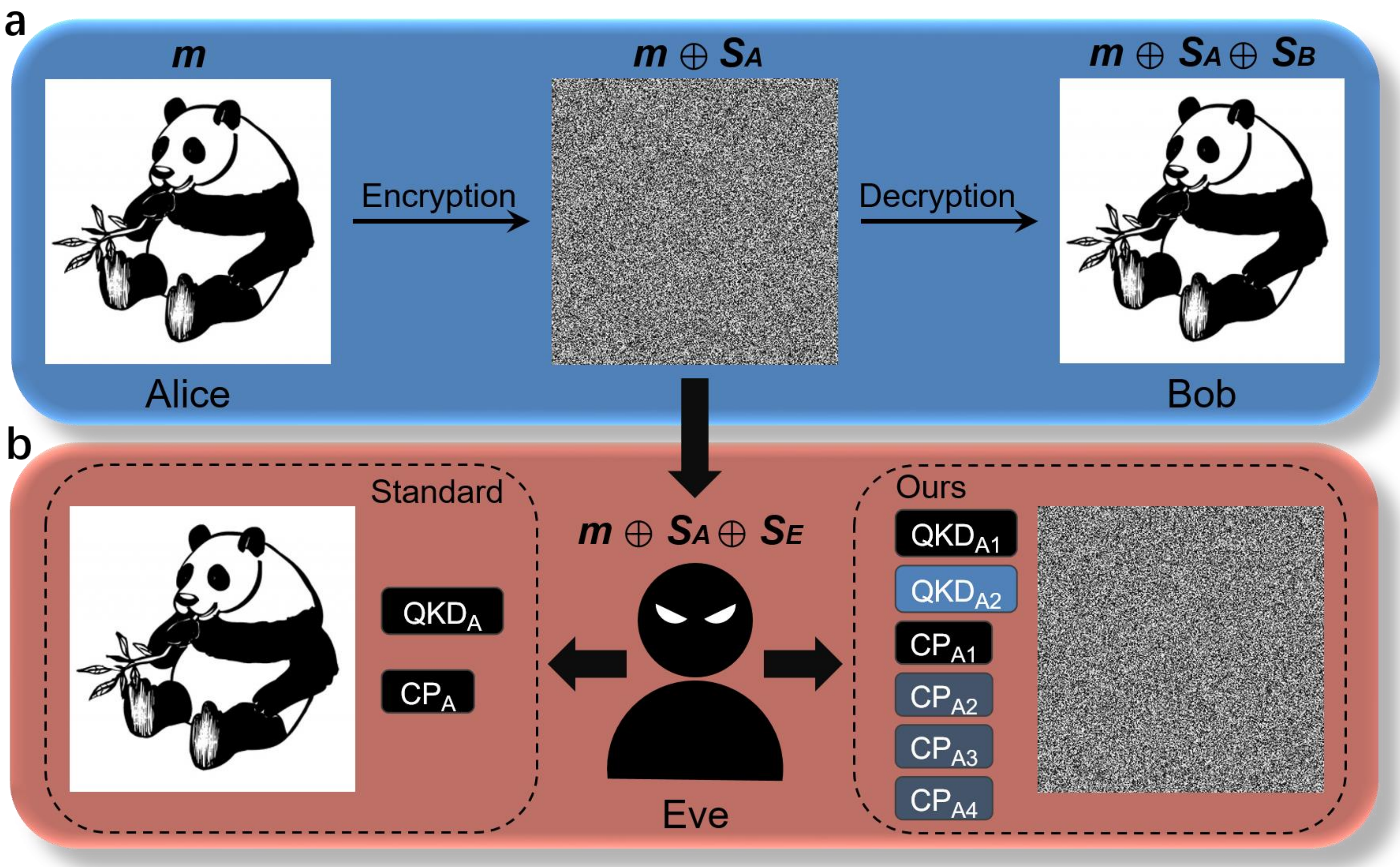


Experimental result

Parameter	Result
Channel loss	24 dB
η_{det}	49.5%
f_{EC}	1.14
N	2e13
Total secret key	4386592 bits
Authentication cost	960 bits



Secure against malicious devices



Eve's failed attempt to decrypt the encrypted picture in the redundant setup