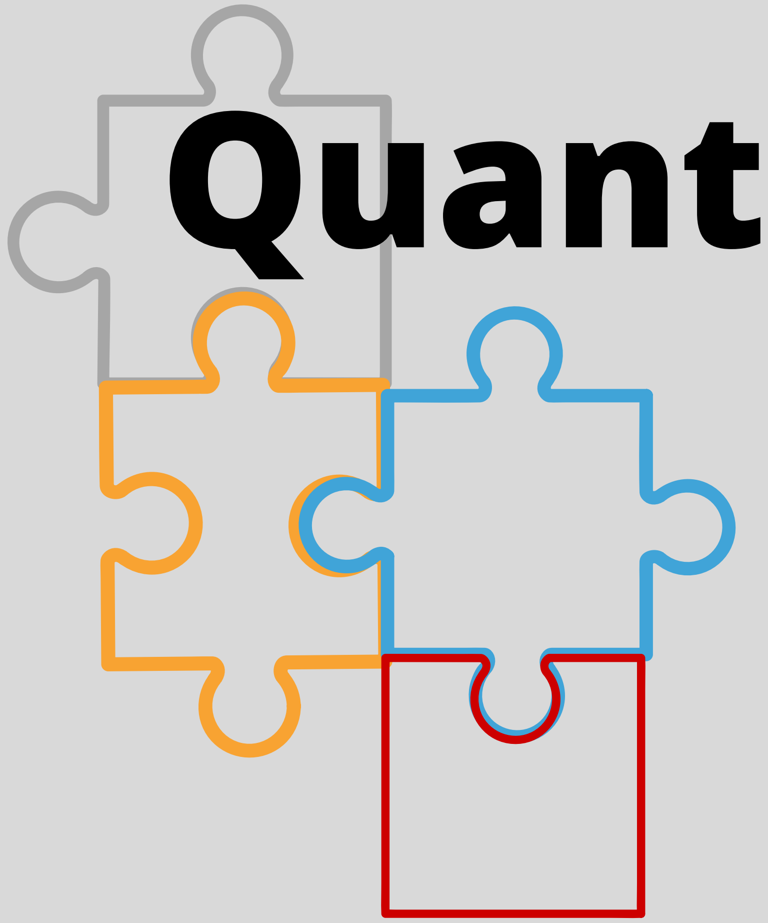
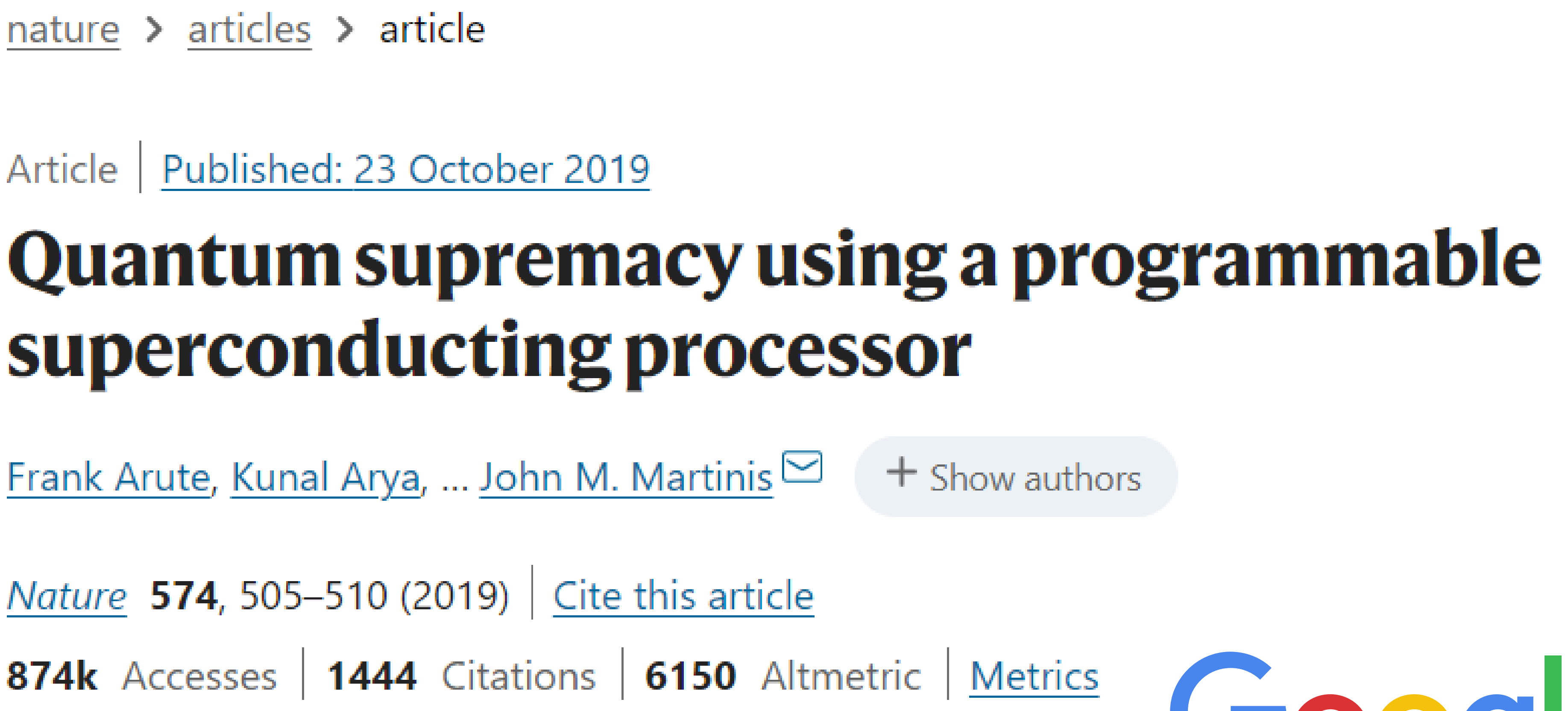
Quantum Key Distribution



Team: One-Zero

Problem

HTTPS://DOI.ORG/10.1038/S41586-019-1666-5



nature > articles > article

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

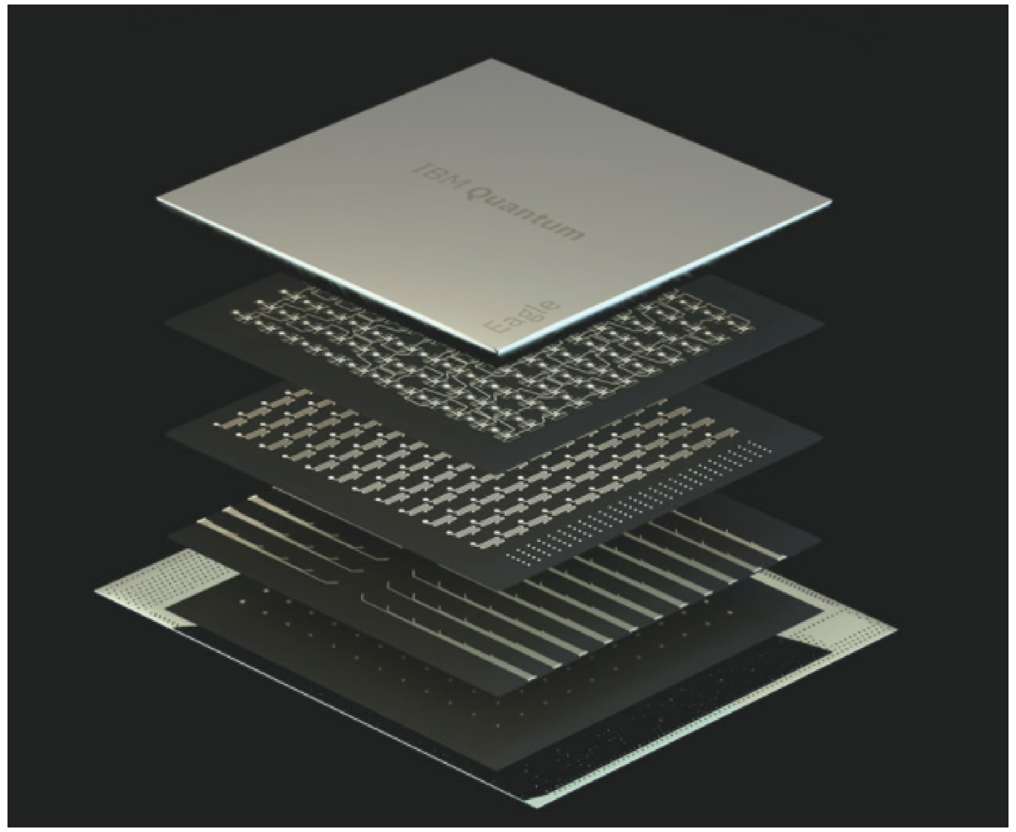
Frank Arute, Kunal Arya, ... John M. Martinis + Show authors

Nature **574**, 505–510 (2019) | Cite this article

874k Accesses | **1444** Citations | **6150** Altmetric | Metrics

Google

ARMONK, N.Y., NOV. 16, 2021 /PRNEWSWIRE/ -- IBM (NYSE: IBM)



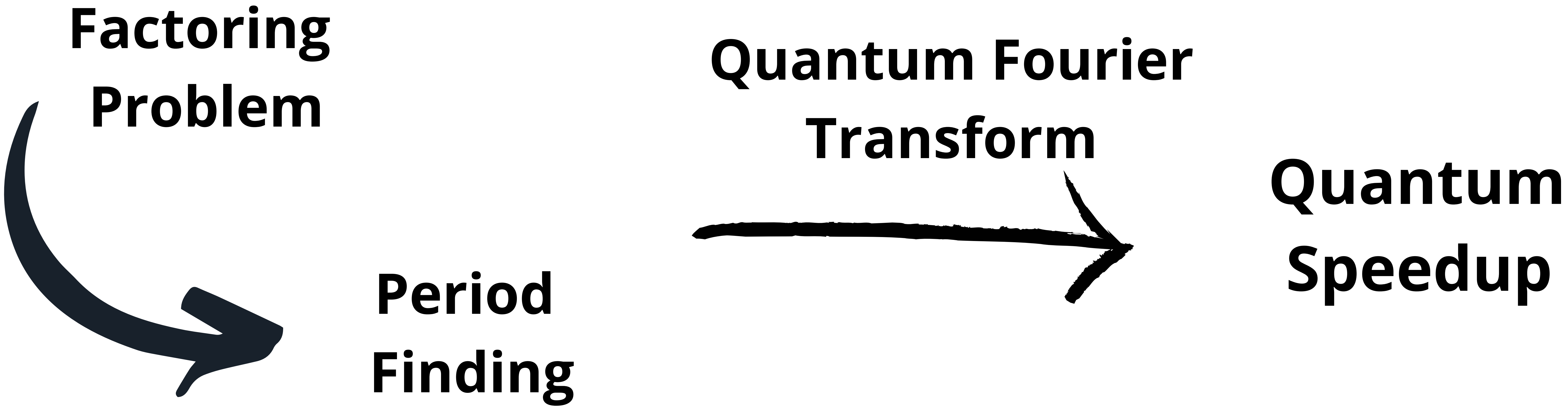
"IBM Unveils Breakthrough 127-Qubit Quantum Processor"

Advances in Quantum Computation may break into your private security. Classicaly any RSA type protocol shall be broken quantically

Rivest–Shamir–Adleman (RSA) type protocols

Why does it influence our current RSA protocols?

Public key consists of: Prime 1 **X** Prime 2



Factoring Problem

Period Finding

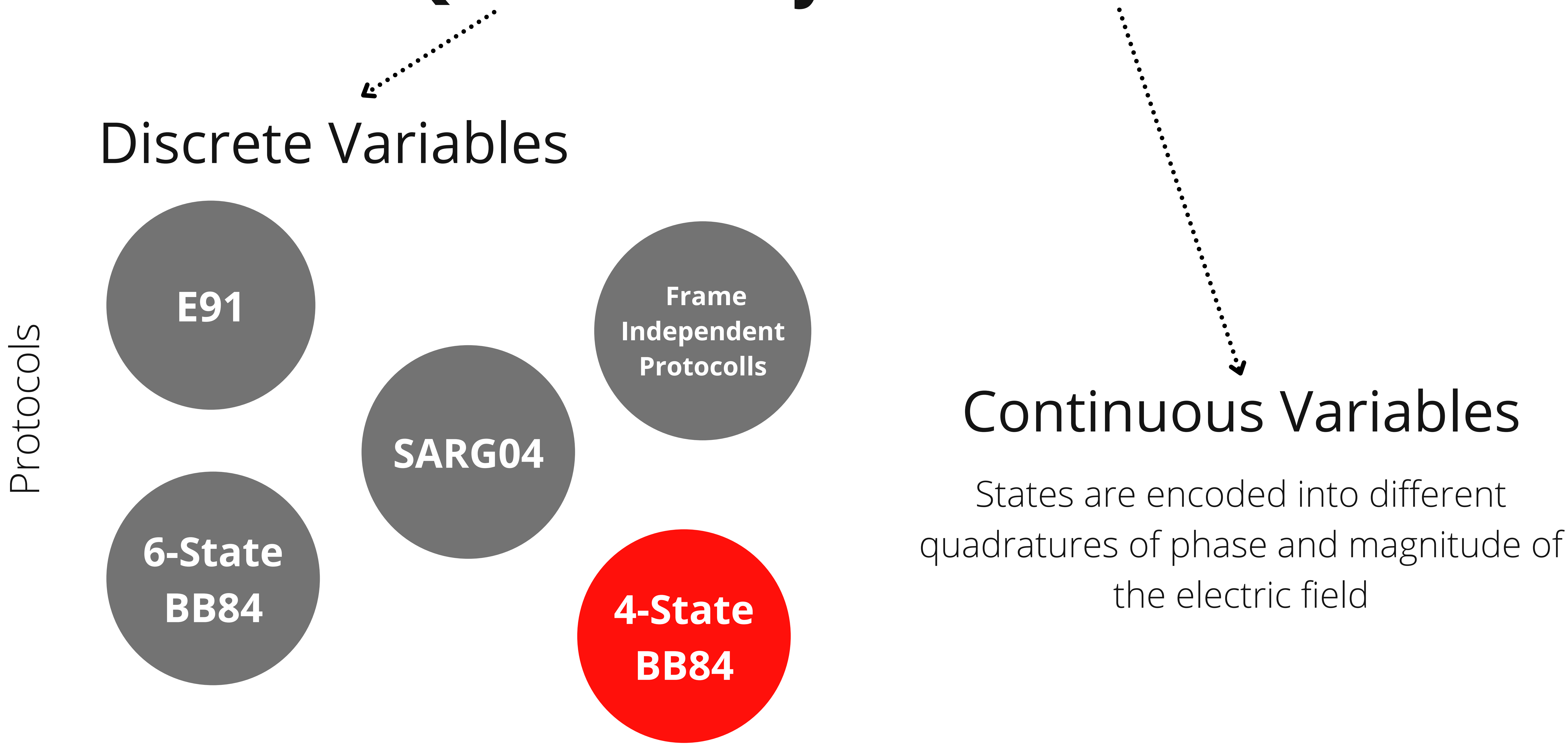
Quantum Fourier Transform

Quantum Speedup

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs

Quantum Key Distribution



Discrete Variables

Protocols

E91

SARG04

Frame Independent Protocolls

6-State BB84

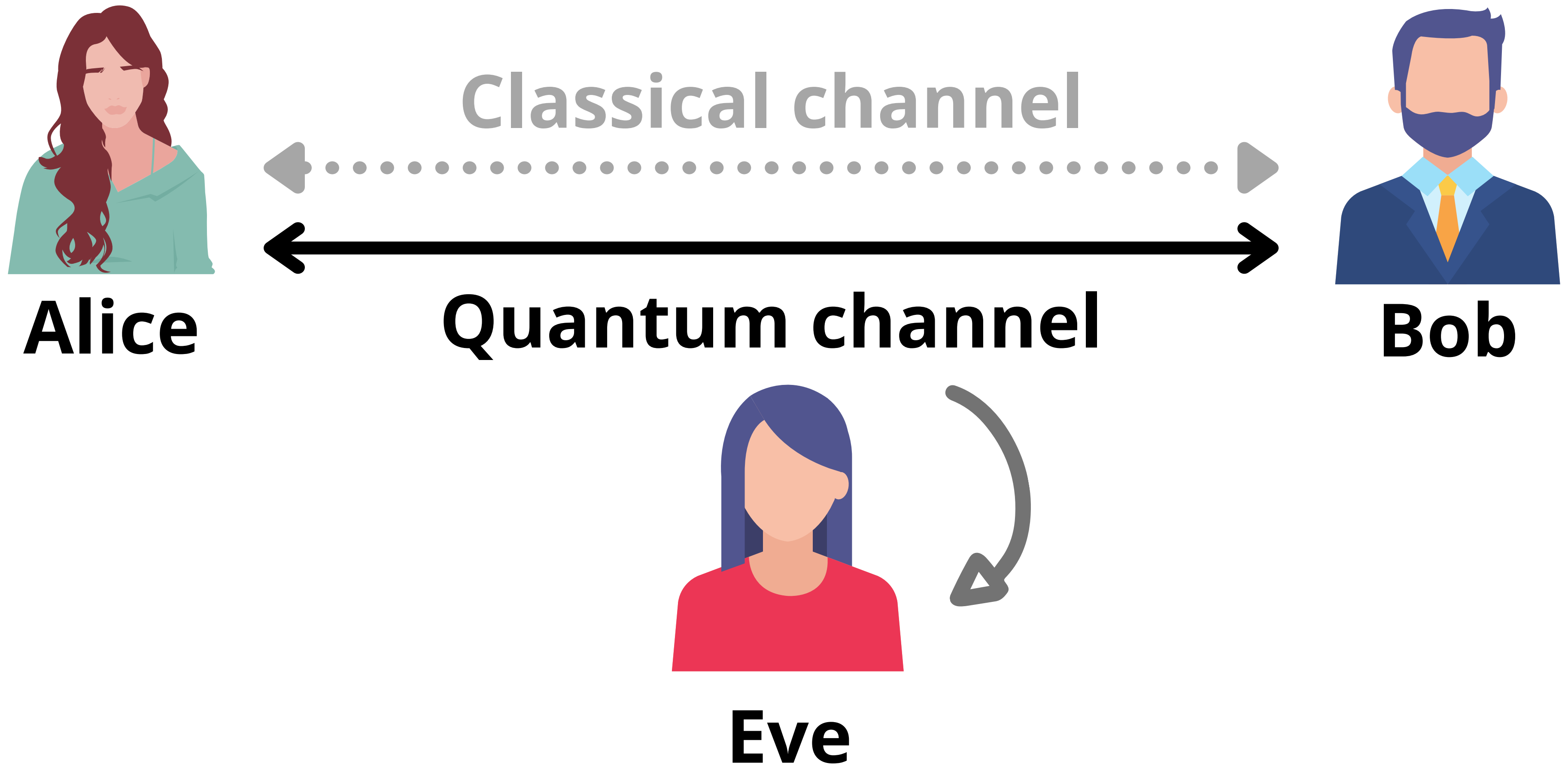
4-State BB84

Continuous Variables

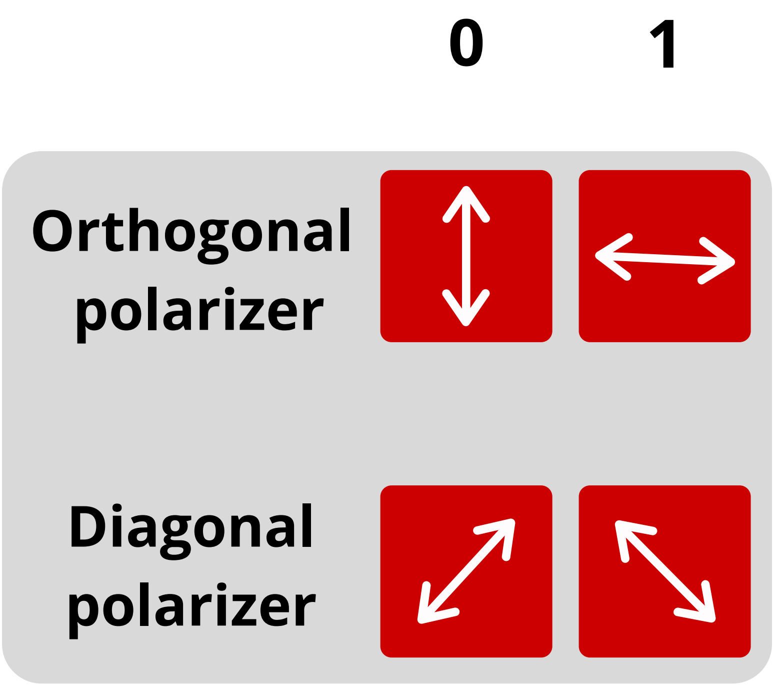
States are encoded into different quadratures of phase and magnitude of the electric field

BB84 - The Process

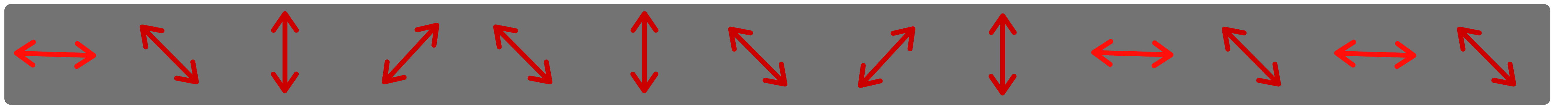
- Alice generates a random key from an X or Z basis and sends it to Bob.
- Bob reads on a random basis the information received.
- Key sifting occurs - Via the classical channel Alice and Bob compare the basis and the key is shortened and identical.
- Secret key distillation with privacy amplification occurs to account for Eve resulting in a final key.



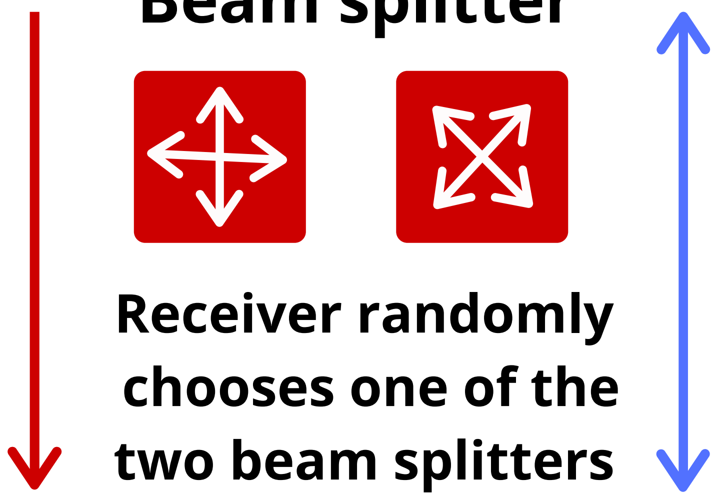
Example for BB84



Alice

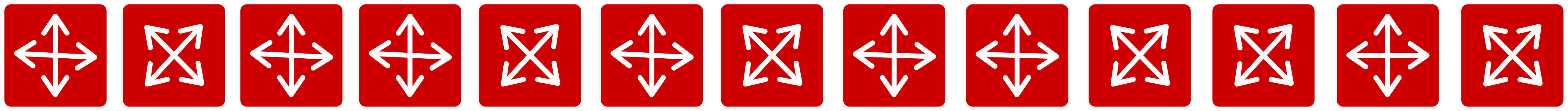


1	1	0	0	1	0	1	0	0	1	1	1	1



Receiver randomly chooses one of the two beam splitters

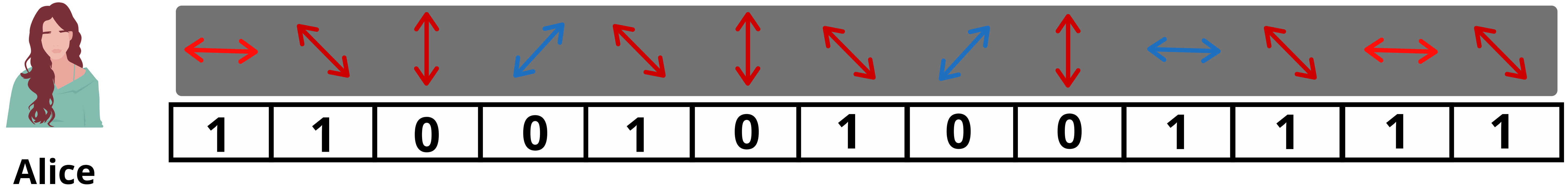
Information is decoded and a sifting key is created



1	1	0	0	1	1	1	1	0	0	1	1	1

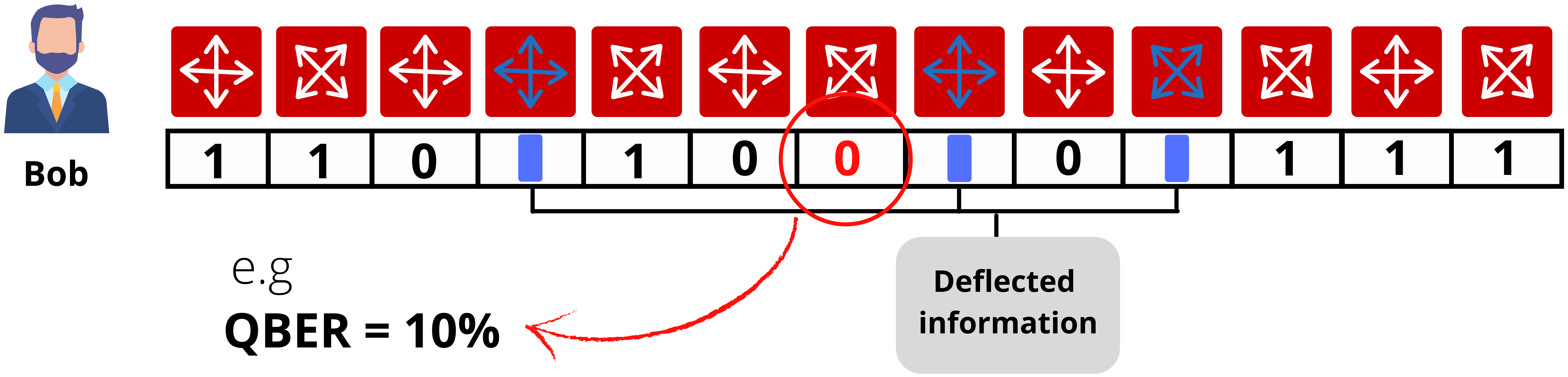
Bob

Quantum Bit Error Rate (QBER) and sifted key rate



1	1	0	0	1	0	1	0	0	1	1	1	1

The Quantum Bit Error Rate (QBER) is the ratio of an error rate to the key rate



1	1	0	▮	1	0	0	▮	0	▮	1	1	1

Deflected information

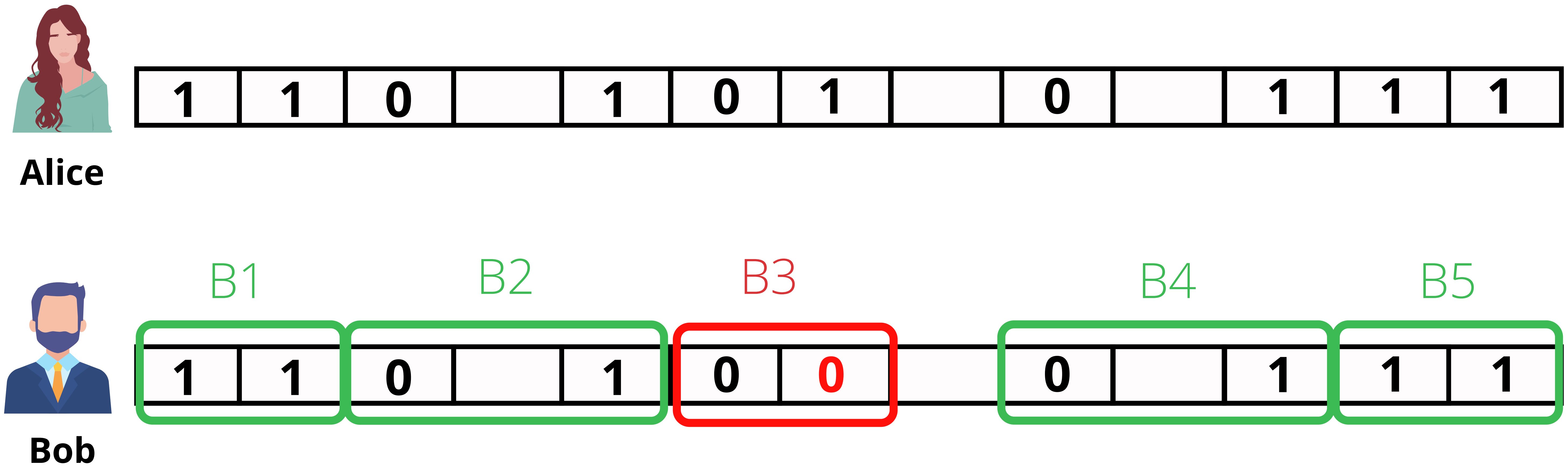
e.g

QBER = 10%

Same basis between both, but state is **different**. Background or Eve are present, shifting the state.

Distillation and privacy amplification

1. Even with key sifting, the keys are not the same, due to noise or/and evesdropping. If Eve's is found (QBER above the treshhold limit): Protocol is aborted.
2. Otherwise, parity checks are performed:
   - Distribute the key into different blocks, and perform sequential parity checks, until descrepancy is found.



Alice	1	1	0		1	0	1		0		1	1	1
	B1		B2			B3			B4			B5	
Bob	1	1	0		1	0	0		0		1	1	1

And now that the basics are explained -
Do you have any questions?