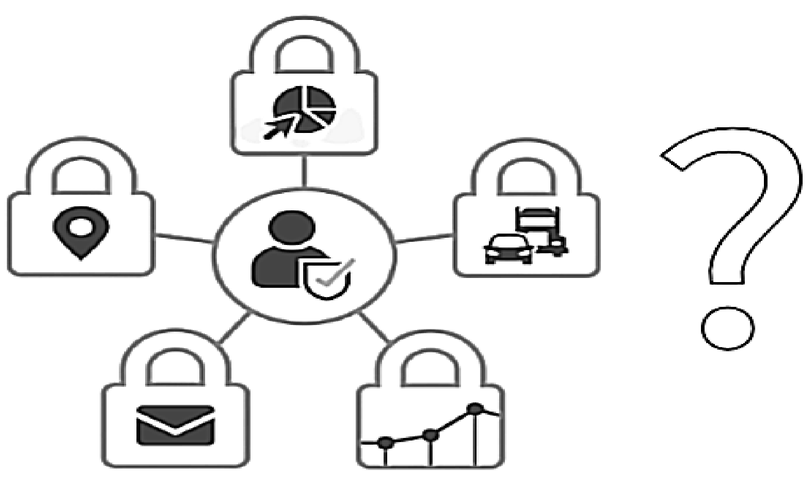
High-Dimensional B92 Protocol

Hasan Iqbal, Walter O. Krawec

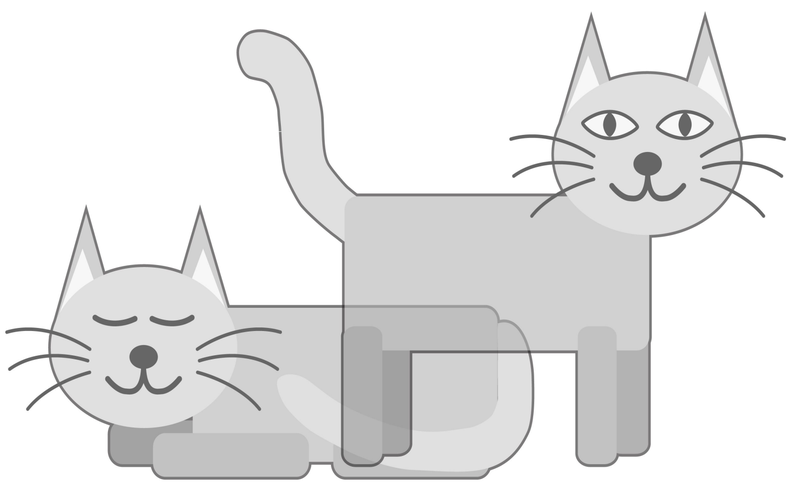
Department of Computer Science, University of Connecticut

The Looming Threat



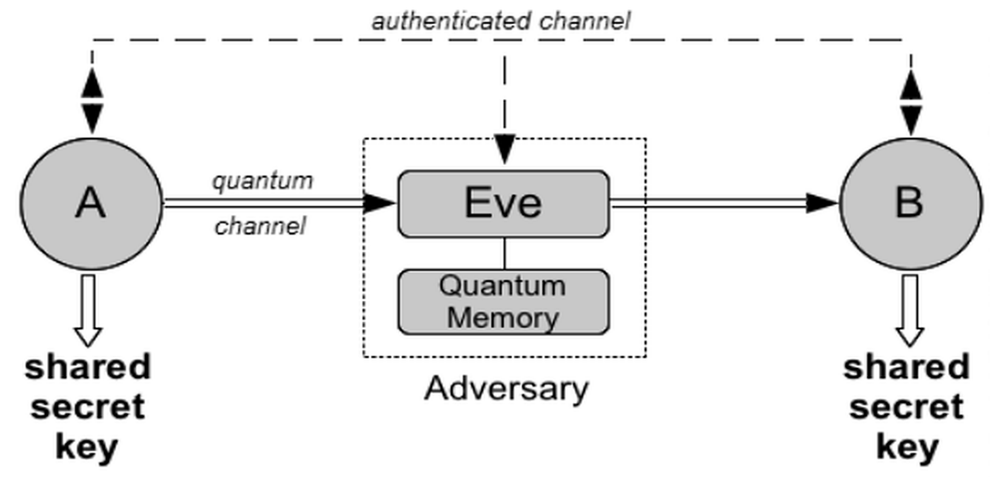
- We think that our messages, password, healthcare data are securely encrypted.
- But this is based on unproven mathematical assumptions.
- Quantum computers can undermine them and severely disrupt our modern security infrastructure.

The Solution: Quantum Key Distribution



- Really small particles exhibit some quantum mechanical properties like superposition and entanglement.
- Quantum key distribution (QKD) is about using these properties to create quantum-proof encryptions and guarantee unconditional security.

How does it work?



- Alice(A) and Bob(B), prepare, send and measure quantum bits (qubits) through the quantum channel.
- The adversary, Eve, attacks these qubits.
- A and B can use the classical channel to detect Eve and finalize their key.

Example: B92 QKD Protocol

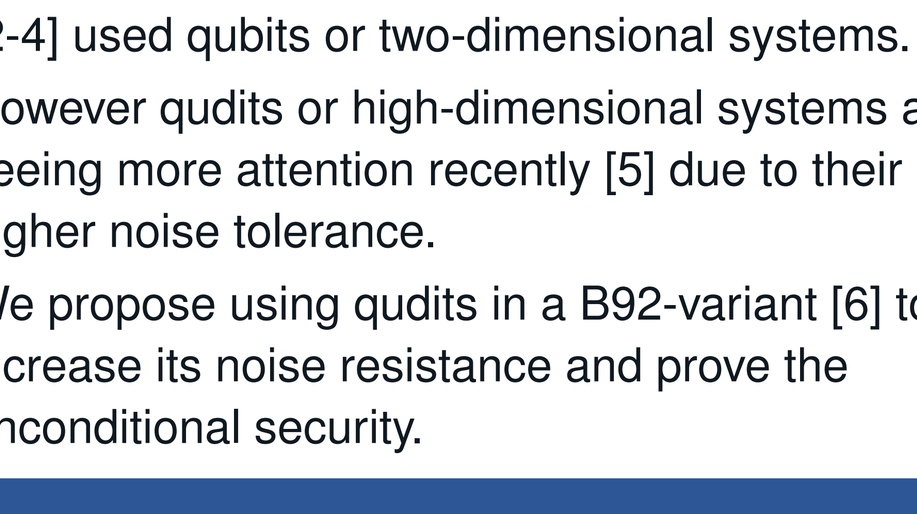
- B92 QKD protocol [1] is one of the simplest and easiest to implement.
- However it is very sensitive to environmental noise and there have been attempts to improve it.

Our solution: High-Dimensional B92

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \quad vs \quad \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix}$$

- Previous attempts to improve noise-tolerance B92 [2-4] used qubits or two-dimensional systems.
- However qudits or high-dimensional systems are seeing more attention recently [5] due to their higher noise tolerance.
- We propose using qudits in a B92-variant [6] to increase its noise resistance and prove the unconditional security.

Result in Depolarizing Channel



- Depolarization is the 'worst' that can happen to a qudit.
- Our result (solid lines) shows the ***highest noise-tolerance in a B92 protocol to date***.
- We also compare it with HD-BB84 protocol [7], which uses twice as much resources.

Result in Amplitude Damping Channel

$\|\phi\rangle = \frac{1}{\sqrt{2}}(\|i\rangle + \|j\rangle)$	key-rate
$\|i\rangle = \|0\rangle, \|j\rangle = \|1\rangle$	.9158
$\|i\rangle = \|0\rangle, \|j\rangle = \|2\rangle$	.5184
$\|i\rangle = \|1\rangle, \|j\rangle = \|3\rangle$	-.2844
$\|i\rangle = \|2\rangle, \|j\rangle = \|3\rangle$	-.4366

- This widely used channel models spontaneous emission of energy.
- The table confirms our guess that in a variant of this channel that we formulate, choice of parameters would affect the protocol's performance.

References

[1] Bennett, C. H. (1992). Phys. Rev. Lett., 68(21), 3121.
[2] Tamaki, K. et al. (2003) Phys. Rev. Lett., 90(16), 167904.
[3] Lucamarini, M. et al. (2009) Phys. Rev. A, 80(3), 032327.
[4] Matsumoto, R. (2013) IEEE ISIT, pp. 351-353.
[5] Cozzolino, D. et al. (2019) Adv. Quant. Tech., 2(12), 1900038.
[6] Amer, O. et al. (2020) IEEE ISIT, pp. 1944-1948.
[7] Cerf, N. J. et al. (2002), Phys. Rev. Lett., 88(12), 127902.