

HIGH-DIMENSIONAL B92 PROTOCOL

Hasan Iqbal, Walter O. Krawec

Department of Computer Science, University of Connecticut

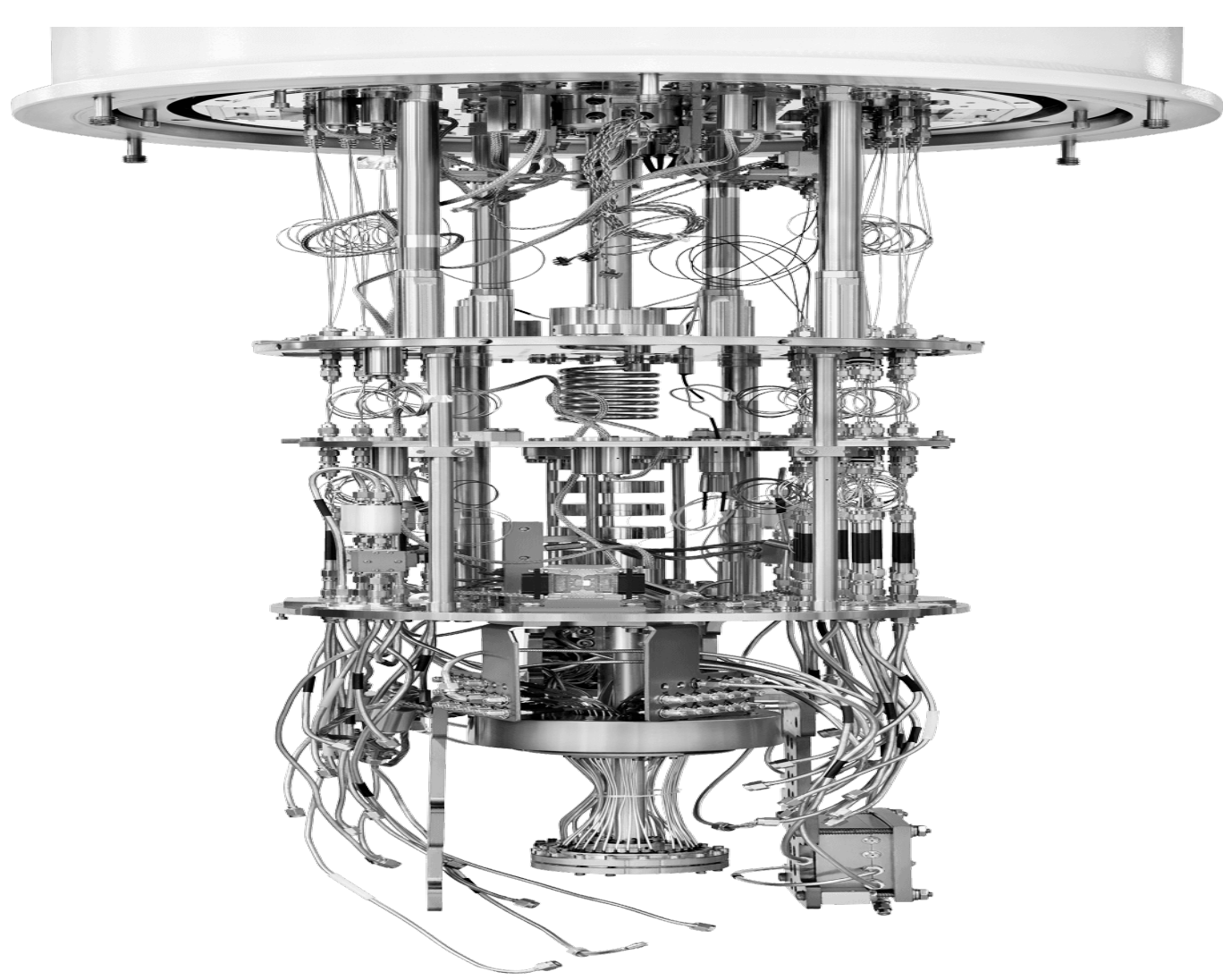


The Situation Now



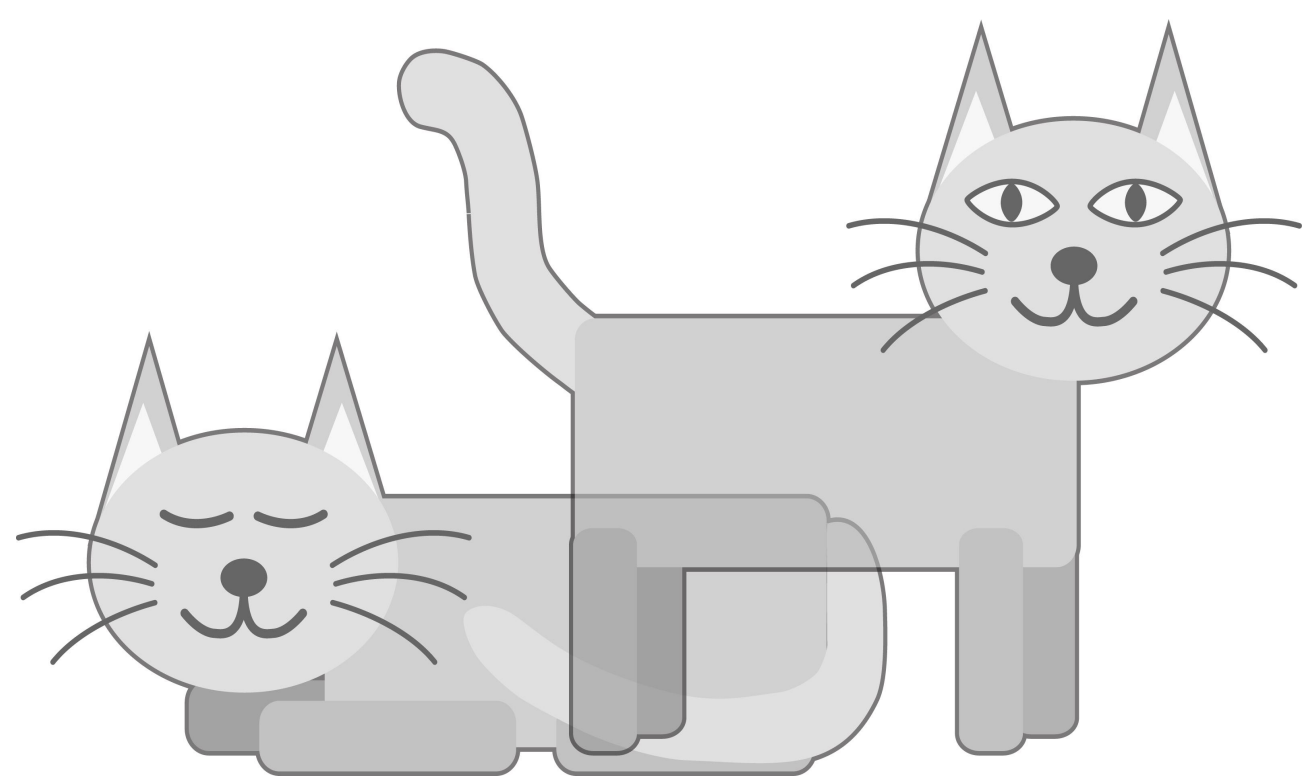
- We think that our messages, password, healthcare data are securely encrypted.
- But this is based on unproven mathematical assumptions.

The Looming Threat



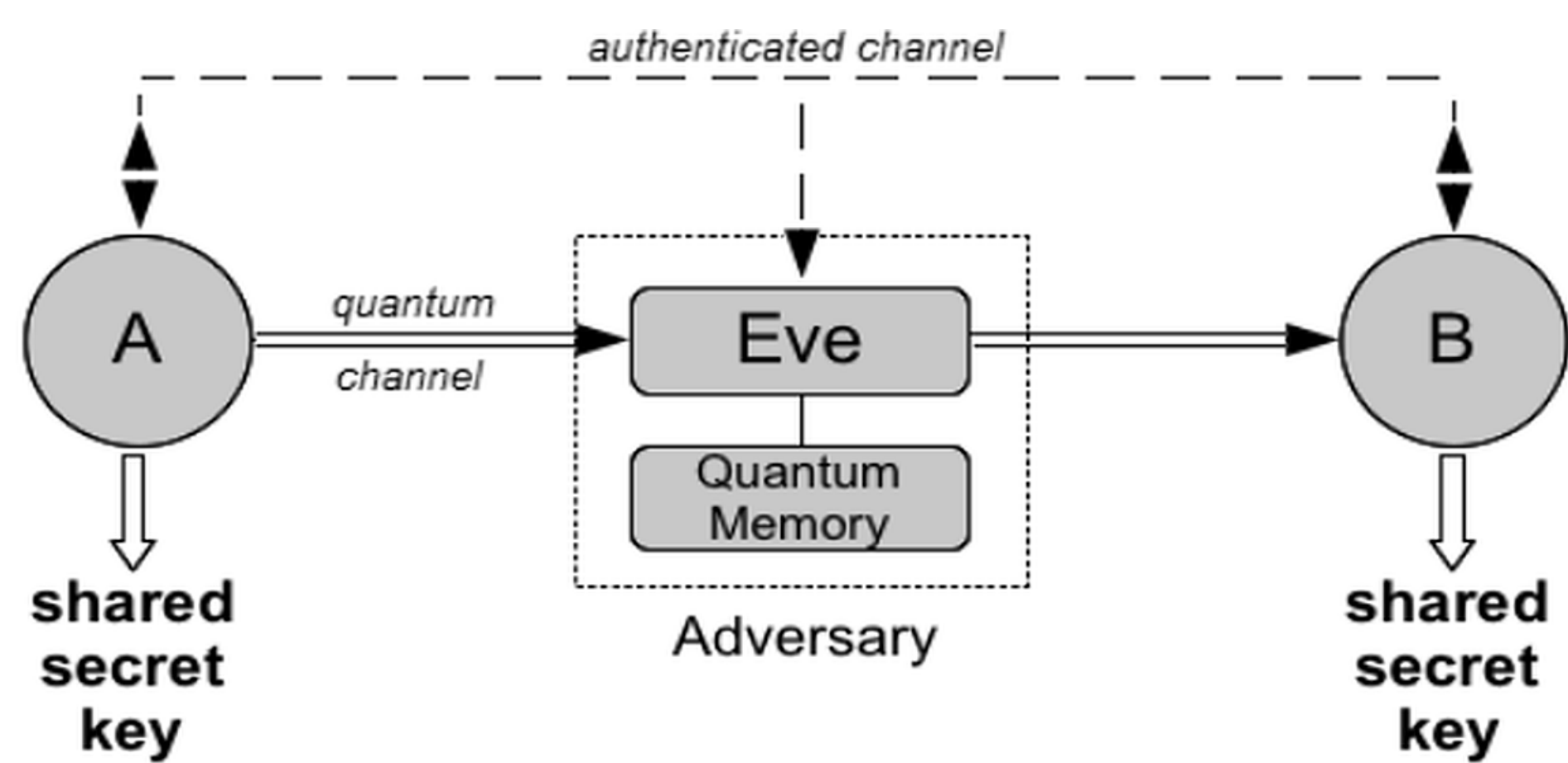
- Quantum Computers can break our modern security infrastructure.
- Much stronger encryption system is needed.

The Solution: Quantum Key Distribution



- Really small particles exhibit quantum mechanical properties like superposition and wave function collapse.
- Quantum key distribution (QKD) exploits these properties to design secret-key generation and distribution protocols.

Sturcture of a QKD protocol



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

B92



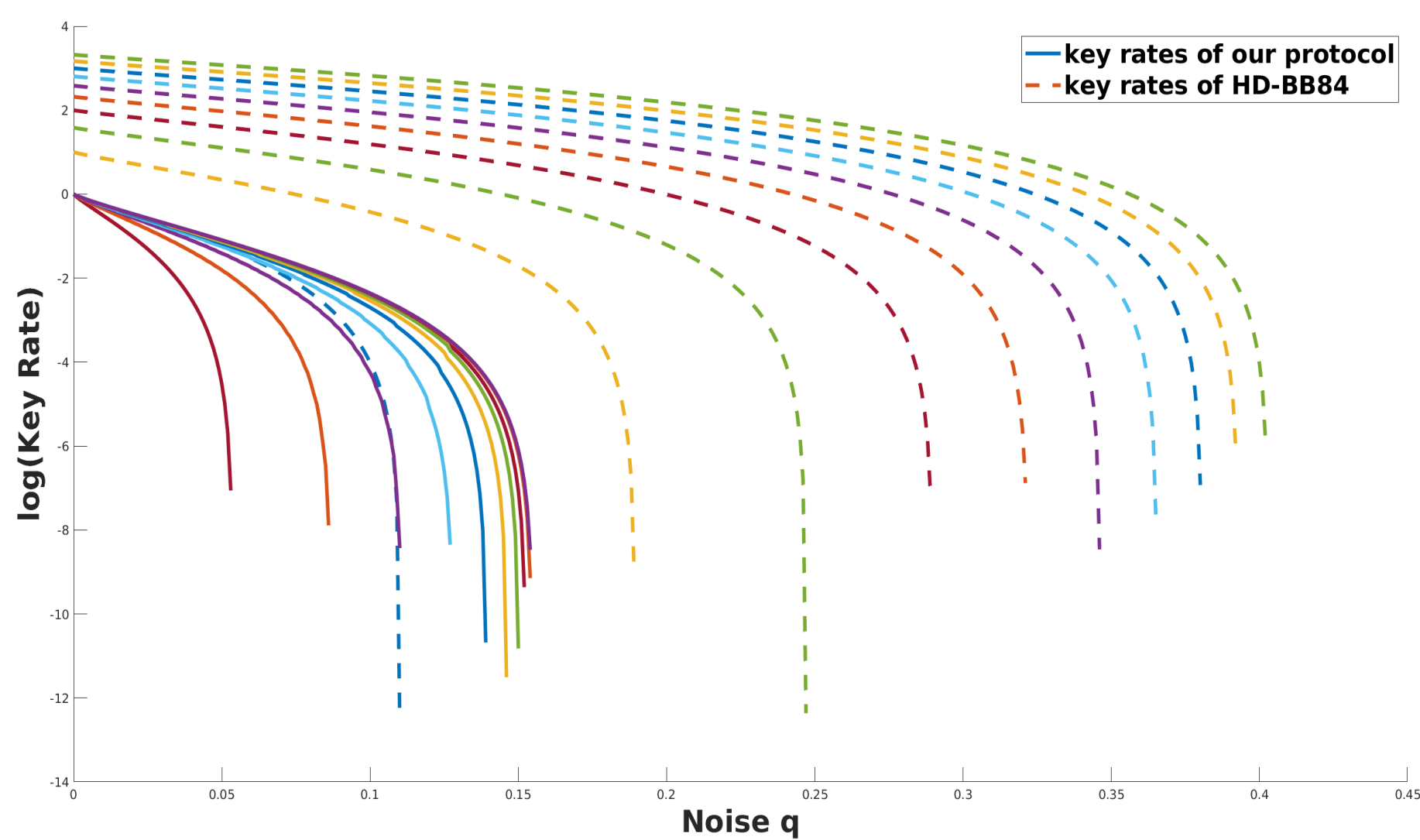
- B92 QKD protocol, one of the simplest and easiest to implement, is quite susceptible to environmental noise.
- I propose a solution to this noise sensitivity.

High-Dimensional B92

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

- Qubits are described by two complex numbers but high-dimensional systems (qudits) need n.
- Qudits are seeing increasing interest in the community.
- I propose using qudits in a B92-variant to increase noise sensitivity and prove its unconditional security.

Result in Depolarizing Channel



- Depolarizing channel models the ‘worst’ that can happen to a qudit.
- My result (solid lines) shows *higher noise-tolerance than any other B92 protocol to date*.
- I also compare it with HD-BB84 protocol, 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

- Another very important quantum channel, models spontaneous emission of energy.
- This table shows that in a variant of this channel, choices of basis states affect the protocols performance.

Contact

Email: hasan.iqbal@uconn.edu