High-Dimensional SQKD

Hasan Iqbal, Walter Krawec

CSE, UCONN

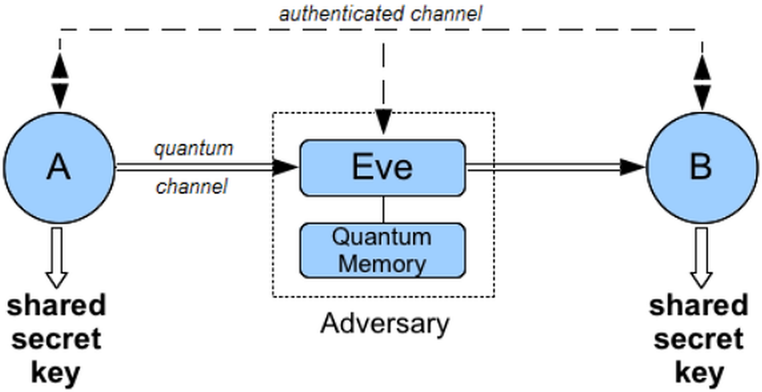
November 11, 2020

New high-dimensional semi-quantum key distribution protocol [1]

Simpler method for security analysis

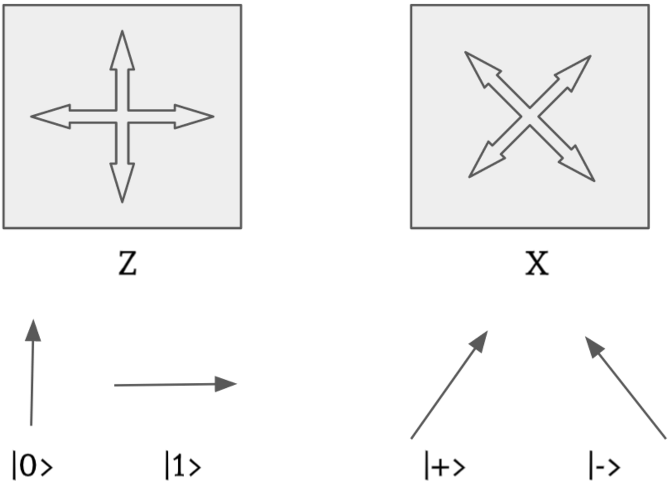
Proof of information theoretic security

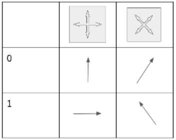
[1] https://arxiv.org/abs/1907.11340



Quantum Key Distribution(QKD)

A Concrete Example

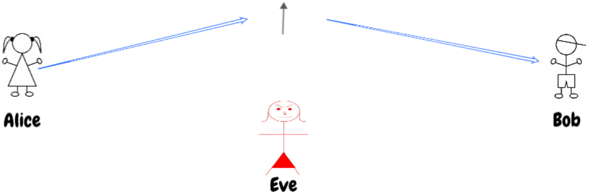

Z
X
|0>
|1>
|+>
|->



Alice's Choices

Alice's secret key: 0101

Alice's random gates: ZXXZ



Alice's Bit	Alice's gate	Result	Eve's Gate	Result	Bob's Gate	Result	Bob's Bit
0		↑		↑		↑	0

QKD: All parties have advanced quantum capabilities.
What if Bob can't measure in the X basis?

Semi-Quantum Key Distribution (Boyer et al., 2007)

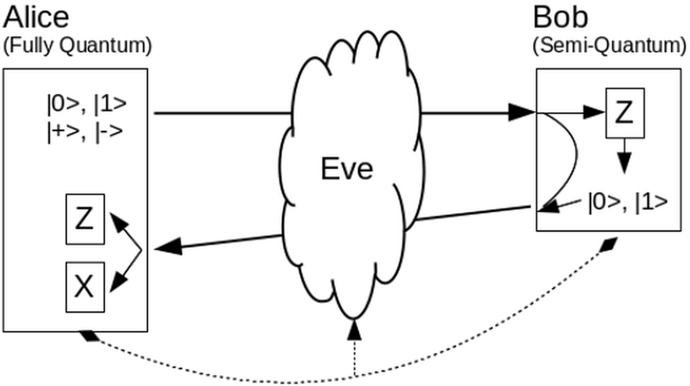
Bridge the gap between Classical and Quantum realms

Use less expensive hardware

Fallback option for fully fledged QKD

But It's Too...

A Concrete Example



SQKD

QKD with High-dimensional(HD) systems

Naturally carries more information

More robust against quantum cloning

More noise resistant

Earlier works on HD-QKD :

High-dimensional quantum key distribution based on mutually partially unbiased bases (Wang et al., 2020)

Provably secure and high-rate quantum key distribution with time-bin qudits (Islam et al., 2017)

Security proof for quantum key distribution using qudit systems (Sheridan et al., 2010)

Can we use HD-systems in SQKD scenario and still prove information theoretic security?

A key is secure if Alice's and Bob's keys are the same and Eve has no knowledge about it.

Let a joint state among Alice, Bob and Eve be:

$$\rho_{XYE}^{real} = \sum_{k_A, k_B \in \{0,1\}^l} Pr(k_A, k_B) \, |k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \rho_E^{(k_A,k_B)},$$

and another desired state be:

$$\rho_{XYE}^{ideal} = \frac{1}{2^l} \sum_{k \in \{0,1\}^m} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \rho_E.$$

Then the final key k is said to be ϵ-secure if (Renner 2005)

$$\frac{1}{2} ||\rho_{XYE}^{real} - \rho_{XYE}^{ideal}||_1 \leq \epsilon,$$

where $||A||_1 := \mathrm{Tr}\left(\sqrt{A^\dagger A}\right)$ is the trace norm of A.

$\epsilon = \epsilon' + \epsilon''$-security also implies that it is:

$$\epsilon'\text{-correct} := \Pr(k_A \neq k_B) \leq \epsilon',$$

and if C is communication transcript in IR,

$$\epsilon''\text{-secret} := \frac{1}{2}||\rho_{XCE}^{real} - \rho_{XCE}^{ideal}||_1 \leq \epsilon''$$

Renner (2005) proved that:

$$||\rho_{XCE}^{real} - \rho_{XCE}^{ideal}||_1 \leq 2^{-\frac{1}{2}(H_{min}(X|CE)-l)},$$

where l is the final length of the key. We want the r.h.s to be at most $2\epsilon''$.

Solving for l, we get:

$$l \leq H_{min}(X|CE) + 2\log\bigl(2\epsilon''\bigr)$$

Let's take the equality to get the maximum length:

$$\begin{aligned} l &= H_{min}(X|CE) + 2\log\bigl(2\epsilon''\bigr) \\ &\geq H_{min}(XC|E) - H_{max}(C) + 2\log\bigl(2\epsilon''\bigr) \text{ [Chain rule]} \\ &\geq H_{min}(X|E) + H_{min}(C|X) - H_{max}(C) + 2\log\bigl(2\epsilon''\bigr) \\ &\geq H_{min}(X|E) - (H_{max}(C) - H_{min}(C|X)) + 2\log\bigl(2\epsilon''\bigr) \end{aligned}$$

Now, as we are interested in the asymptotic scenario, where:

$$\frac{1}{n}H_{min}(X|E) = H(X|E), \text{ and } \frac{1}{n}(H_{max}(C) - H_{min}(C|X)) = H(X|Y).$$

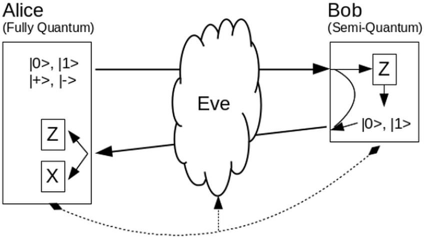
So, finally:

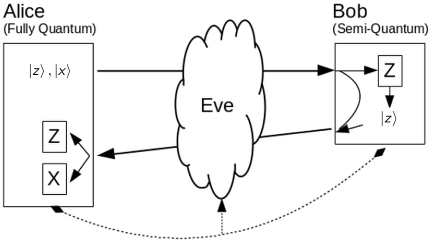
$$l \geq H(X|E) - H(X|Y) + 2\log\bigl(2\epsilon''\bigr)$$

Finally, if ρ is one key-iteration of a protocol,the key-rate is defined as:

$$\text{key-rate} := \frac{l}{n} = min(H(X|E)_\rho - H(X|Y)_\rho)$$

The Protocol

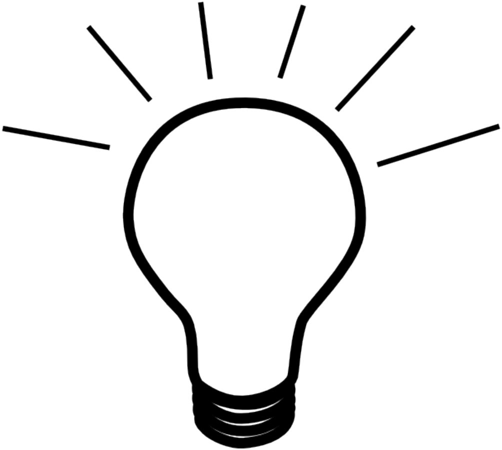




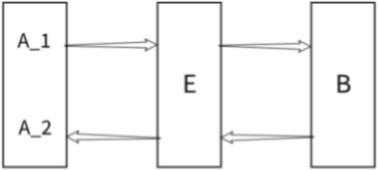
SQKD: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ are two dimensional.

HD-SQKD: $|z\rangle \in \{|0\rangle, |1\rangle \dots |N-1\rangle\}$, $|x\rangle \in \mathcal{F}\{|0\rangle, |1\rangle \dots |N-1\rangle\}$ where $\mathcal{F}$ is Quantum Fourier transformation.

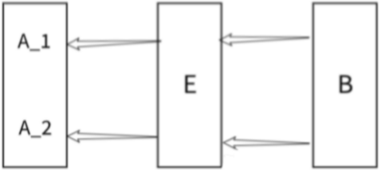
Problem: Two-way SQKD analysis and density matrix computation is too complex



Solution: Reduction to One Way Protocol



Two-Way SQKD



One-Way SQKD

Theorem

Let (U_F, U_R) *be a collective attack against HD-SQKD. Then, there is an attack against the OW-SQKD protocol such that, Eve gets no advantage in either scenario.*

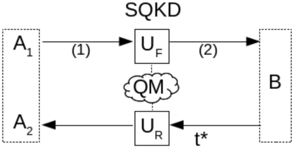
HD-SQKD	**OW-SQKD**
1. A prepares $\|z\rangle$ or $\|x\rangle$, sends to Bob	1. Bob prepares and sends $\|\phi_R\rangle$ or $\|\phi_{MR}\rangle$ if he wants to reflect or measure respectively
2. Eve attacks with U_F	2. Eve attacks with U
3. Bob measures or resends in $\mathcal{Z}$ basis	3. Alice measures A_1 and A_2 registers in $\mathcal{Z}$ or $\mathcal{X}$ basis
4. Eve attacks with U_R	
5. Alice measures the returning n qubits in the preparation basis	

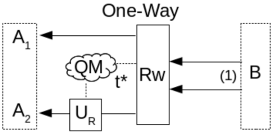
$$|z\rangle \in \{|0\rangle, |1\rangle, \ldots.., |N-1\rangle\}, |x\rangle = \mathcal{F}|z\rangle \tag{1}$$

$$|\phi_R\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)}\, |b, b\rangle_{A_1 A_2} \otimes |0\rangle_B \tag{2}$$

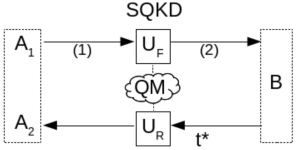
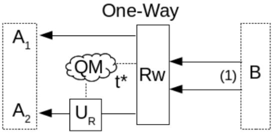
$$|\phi_{MR}\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)}\, |b, b, b\rangle_{A_1 A_2 B} \tag{3}$$

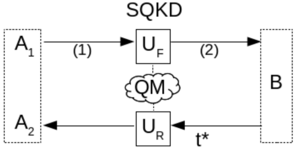
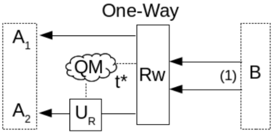
Proof

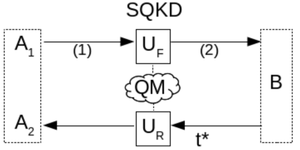
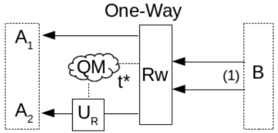
<table>
<tr><th>HD-SQKD</th><th>OW-SQKD</th></tr>
<tr><td>


</td><td>


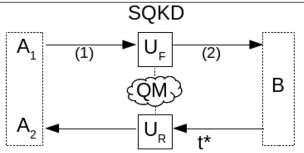
</td></tr>
</table>

<table>
<tr><th>HD-SQKD</th><th>OW-SQKD</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_a |a, a\rangle$$</td><td>$$|\phi\rangle = \sum_{b=0}^{N-1} \sqrt{p(b)}\, |b, b, b\rangle_{A_1 A_2 B}$$</td></tr>
</table>

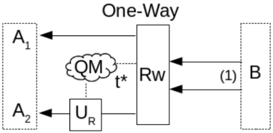
HD-SQKD	OW-SQKD
 	
$\|\psi\rangle = \frac{1}{\sqrt{N}} \sum_a \|a, a\rangle$ $U_F \|a\rangle \otimes \|\chi\rangle = \sum_b \|b, e_{ab}\rangle$	$\|\phi\rangle = \sum_{b=0}^{N-1} \sqrt{p(b)}\, \|b, b, b\rangle_{A_1 A_2 B}$ $R_w \|b, b\rangle_{A_1 A_2} = \frac{\sum_a \|a, b, e_{ab}\rangle}{\sqrt{N.p(b)}}$

HD-SQKD	OW-SQKD
	
$\vert\psi\rangle = \frac{1}{\sqrt{N}} \sum_a \vert a, a\rangle$ $U_F \vert a\rangle \otimes \vert\chi\rangle = \sum_b \vert b, e_{ab}\rangle$	$\vert\phi\rangle = \sum_{b=0}^{N-1} \sqrt{p(b)}\, \vert b, b, b\rangle_{A_1 A_2 B}$ $R_w \vert b, b\rangle_{A_1 A_2} = \frac{\sum_a \vert a, b, e_{ab}\rangle}{\sqrt{N.p(b)}}$
$U_F \vert\psi\rangle = \frac{1}{\sqrt{N}} \sum_a \vert a\rangle \sum_b \vert b, e_{ab}, b\rangle_{TEB}$	$R_w \vert\phi\rangle = \sum_b \sqrt{p(b)} \Big(\frac{\sum_a \vert a, b, e_{ab}\rangle}{\sqrt{N.p(b)}} \Big) \otimes \vert b\rangle_B$

<table>
<tr><th>HD-SQKD</th><th>OW-SQKD</th></tr>
<tr><td>



</td><td>



</td></tr>
<tr><td>

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_a |a, a\rangle$$
$$U_F\,|a\rangle \otimes |\chi\rangle = \sum_b |b, e_{ab}\rangle$$

</td><td>

$$|\phi\rangle = \sum_{b=0}^{N-1} \sqrt{p(b)}\,|b, b, b\rangle_{A_1 A_2 B}$$
$$R_w\,|b, b\rangle_{A_1 A_2} = \frac{\sum_a |a, b, e_{ab}\rangle}{\sqrt{N.p(b)}}$$

</td></tr>
<tr><td>

$$U_F\,|\psi\rangle = \frac{1}{\sqrt{N}} \sum_a |a\rangle \sum_b |b, e_{ab}, b\rangle_{TEB}$$

</td><td>

$$R_w\,|\phi\rangle = \sum_b \sqrt{p(b)} \left(\frac{\sum_a |a, b, e_{ab}\rangle}{\sqrt{N.p(b)}} \right) \otimes |b\rangle_B$$
$$= \frac{1}{\sqrt{N}} \sum_a |a\rangle_{A_1} \sum_b |b, e_{ab}, b\rangle_{A_2 E B}$$

</td></tr>
</table>

In two-way case, let Alice's choices are $|0\rangle, |1\rangle, |2\rangle, |3\rangle$ and she chooses $|1\rangle$ to send to Bob. Eve attacks then:

$$U_F |1\rangle = |0, e_{10}\rangle + |1, e_{11}\rangle + |2, e_{12}\rangle + |3, e_{13}\rangle$$

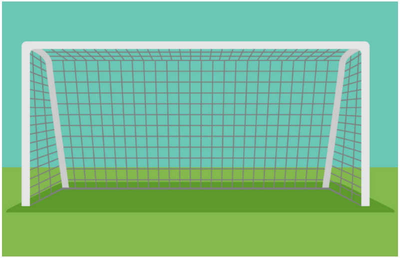
Bob measures and finds a $|2\rangle$ with probability $\langle e_{12}|e_{12}\rangle$. Then, one-way case, R_w must recreate all the scenarios where Bob could measure a $|2\rangle$. Specifically,

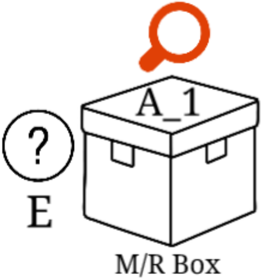
$$\begin{aligned}
|0\rangle &\to |2\rangle\,, \text{ with probability } \langle e_{02}|e_{02}\rangle \\
|1\rangle &\to |2\rangle\,, \text{ with probability } \langle e_{12}|e_{12}\rangle \\
|2\rangle &\to |2\rangle\,, \text{ with probability } \langle e_{22}|e_{22}\rangle \\
|3\rangle &\to |2\rangle\,, \text{ with probability } \langle e_{32}|e_{32}\rangle
\end{aligned}$$

So,

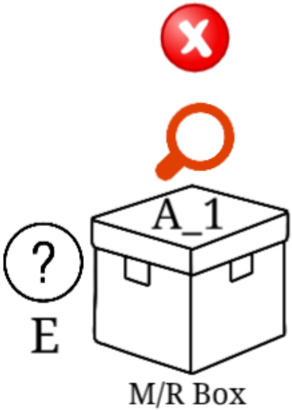
$$R_w |2, 2\rangle = \frac{|0, 2, e_{02}\rangle + |1, 2, e_{12}\rangle + |2, 2, e_{22}\rangle + |3, 2, e_{32}\rangle}{\sqrt{4 \cdot p(2)}}$$

Key-rate Computation

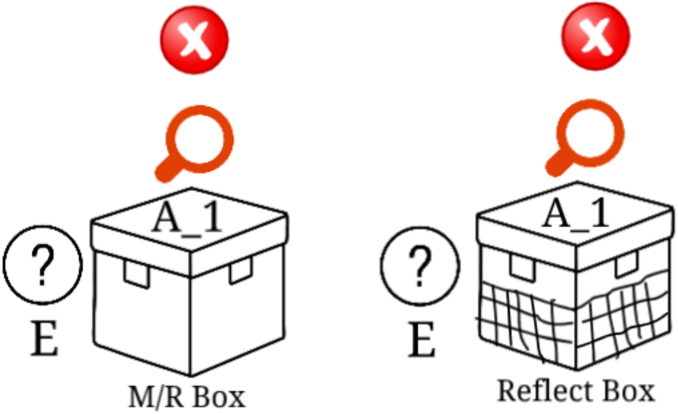




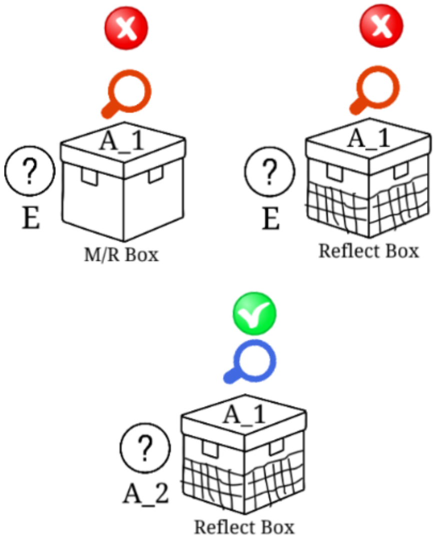
Only Measure/Resend (M/R) rounds are key-generating-rounds. Reflect rounds are used for noise estimation. So the goal is to upper bound Eve's uncertainty about Alice's register in M/R case.



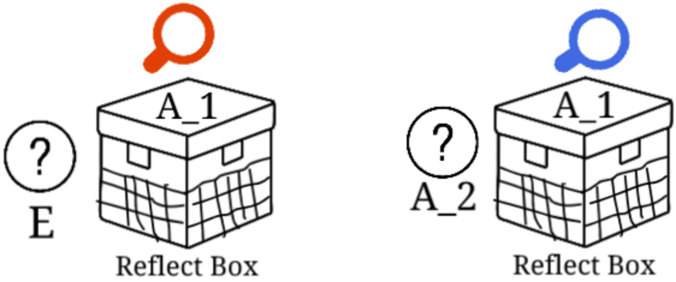
But it's not observable!



Eve’s uncertainty about the reflect case is not observable either.

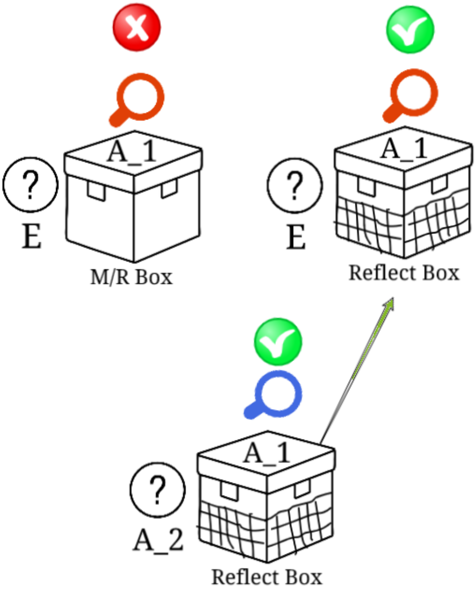


But Alice can measure the uncertainty in the reflect case!

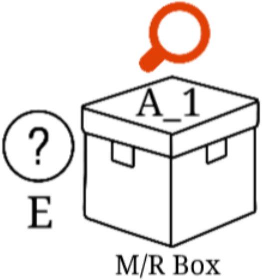


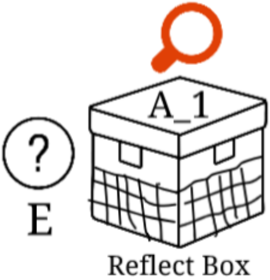
Entropic uncertainty relation (Berta et al., 2009): For any density operator $\rho_{A_1 A_2 E}$ and two measurements $\mathcal{Z}$ and $\mathcal{F}$,

$$H(A_1^Z|E) + H(A_1^F|A_2) \geq n$$



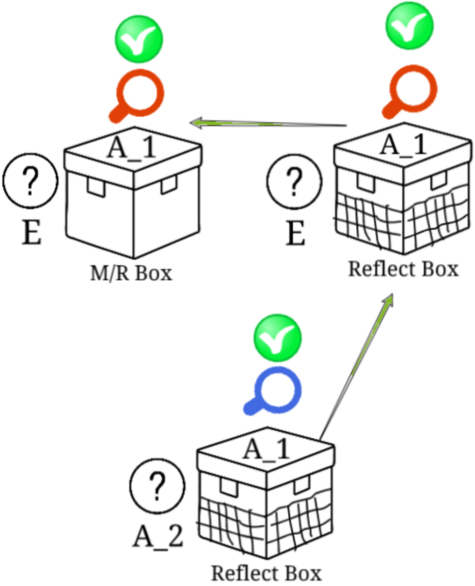
We can bound Eve's uncertainty in Reflect case



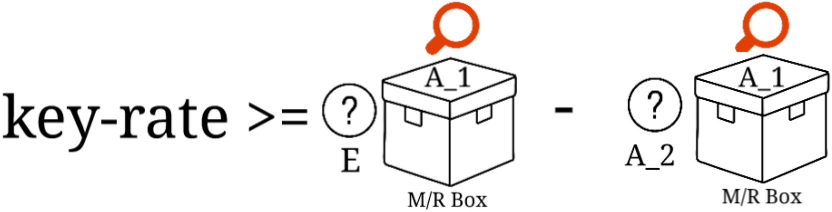


Continuity bound(Winter, 2015): For states ρ and μ on a Hilbert space $A \otimes E$, if $\frac{1}{2}||\rho - \sigma|| \leq \delta \leq 1$ then

$$|H(A_1^Z|E)_\rho - H(A_1^Z|E)_\mu| \leq 2\delta log|A_1^Z| + (1+\delta)h(\frac{\delta}{1+\delta})$$



We can bound Eve's uncertainty in M/R case



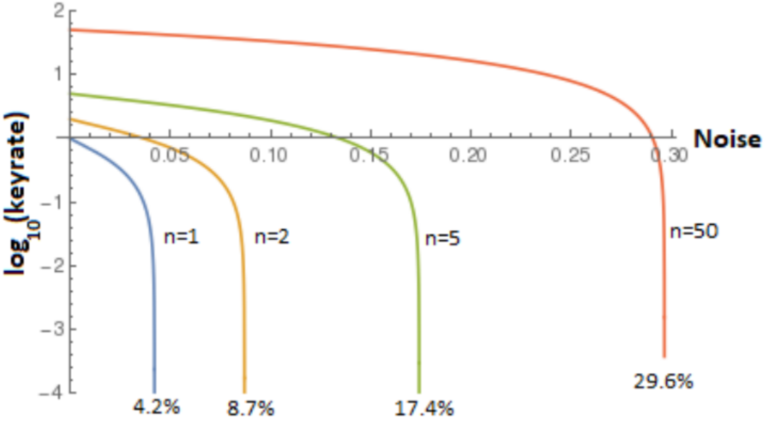
In our case, δ is linear function.

$$\delta = f(\text{noise, eigenvalues, dimension}),$$

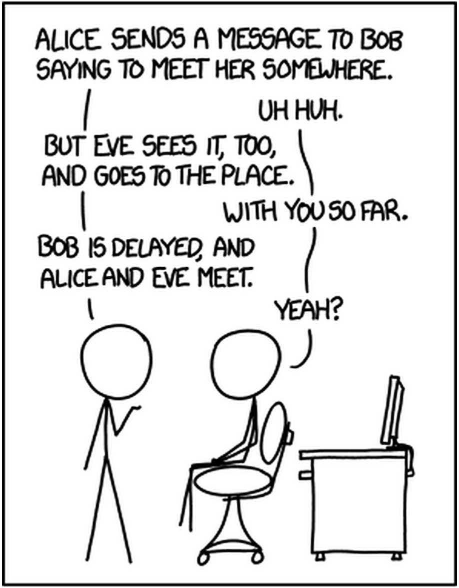
and key-rate r is:

$$r \geq n(1-\delta) - (1+\delta)H(\frac{\delta}{1+\delta}) - 2Q\log_2(2^n - 1) - 2H(Q),$$

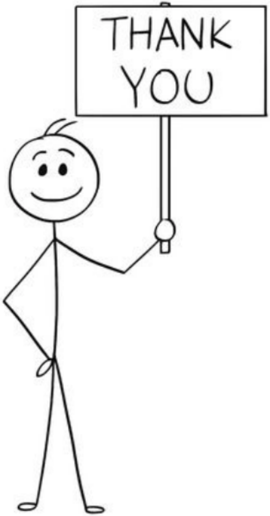
where, n is the number of qubits sent, δ is the trace distance, Q is the noise parameter.



Key-rate of our HD-SQKD protocol



I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.


THANK YOU