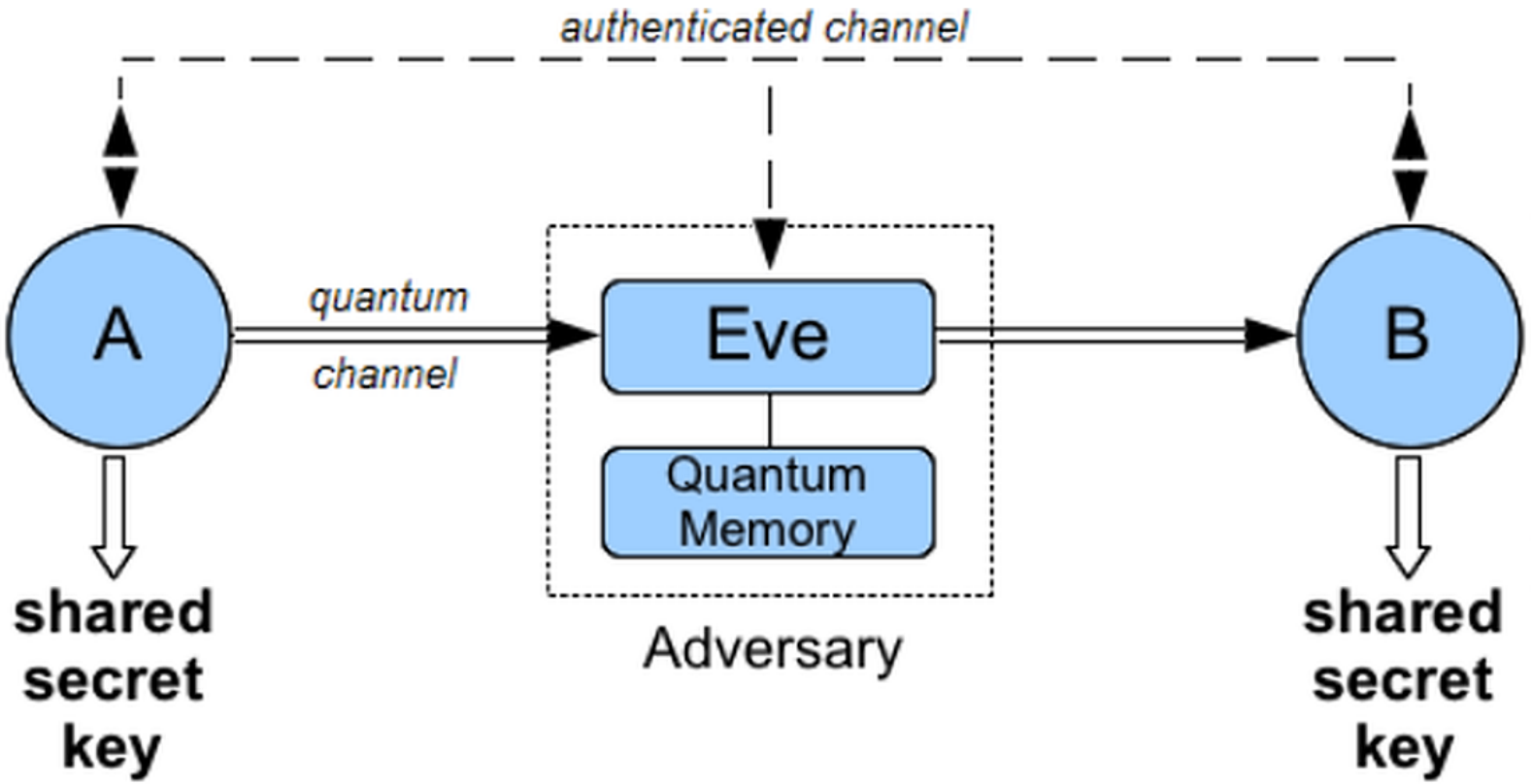
High-Dimensional SQKD

Hasan Iqbal, Walter Krawec

CSE, UCONN

October 27, 2020

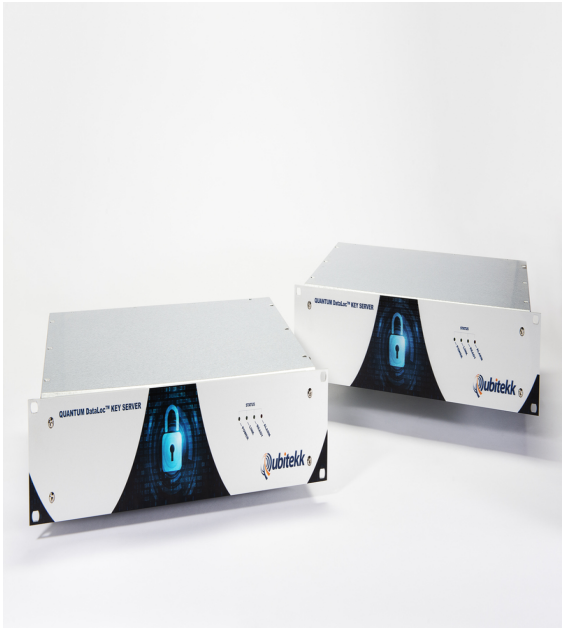
- Proposed a high-dimensional semi-quantum key distribution protocol
- Showed how to convert a two-way SQKD protocol to one-way
- Proved information theoretic security of our protocol



Quantum Key Distribution(QKD)

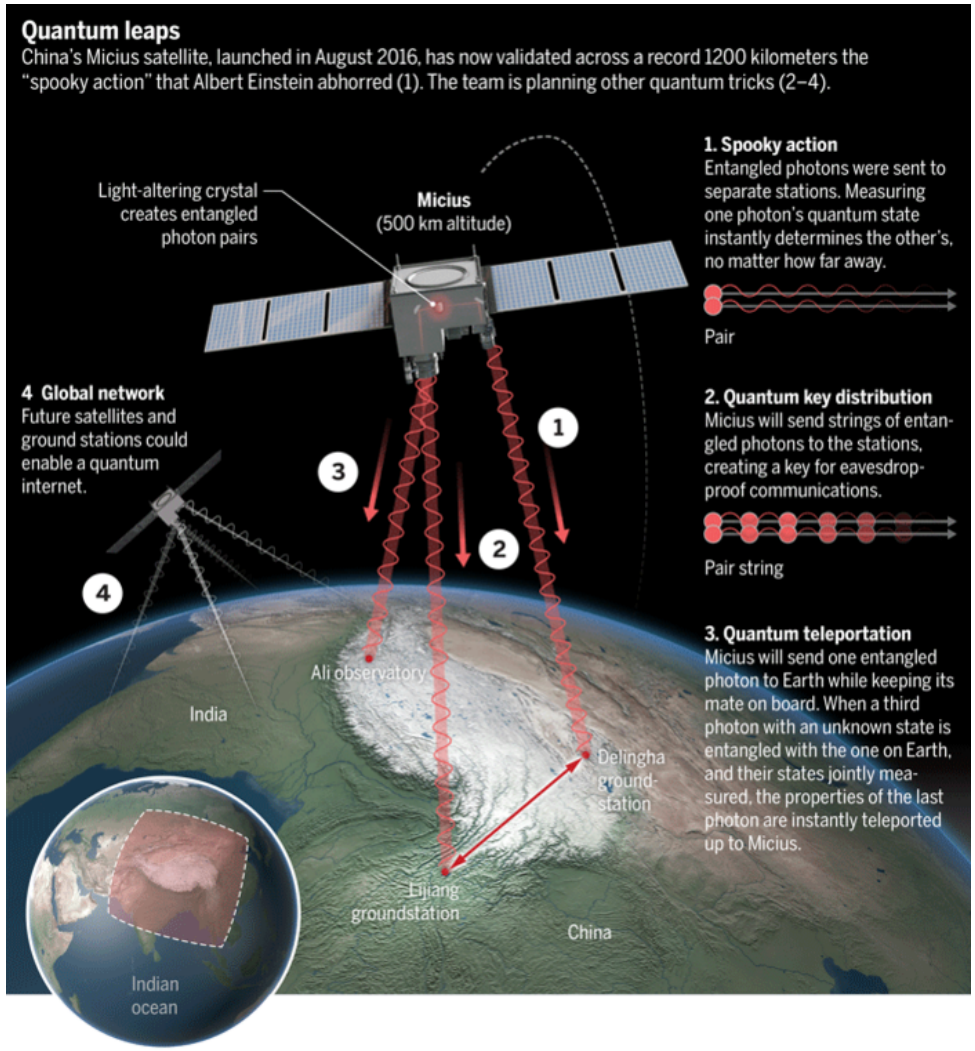
IDQuantique, Switzerland

Toshiba, Japan



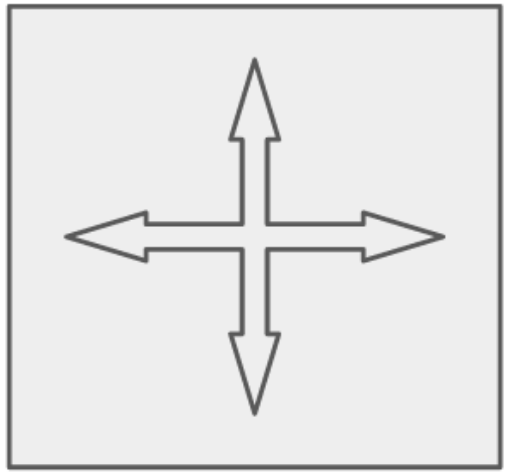
Qubittek, USA

QKD in Practice

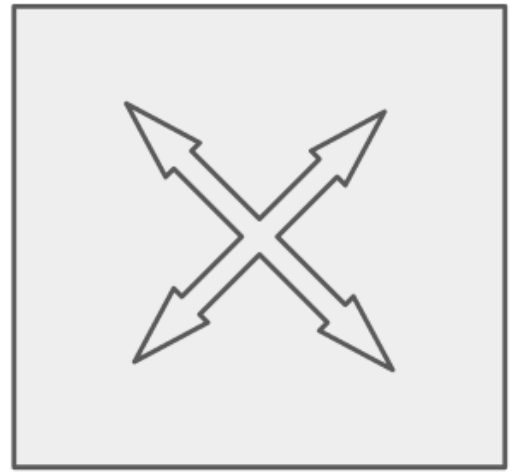


Free Space QKD and Teleportation

A Concrete Example



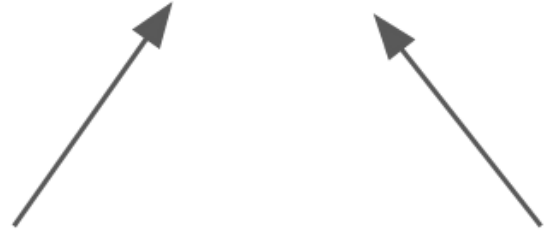
Z



X

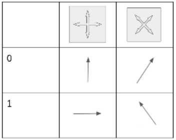
|0>

|1>



|+>

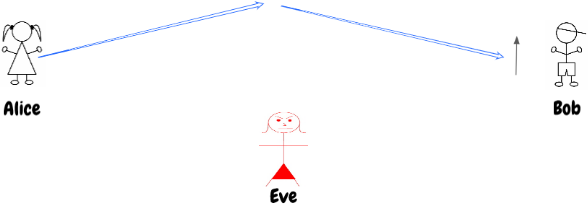
|->



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
1							N/A

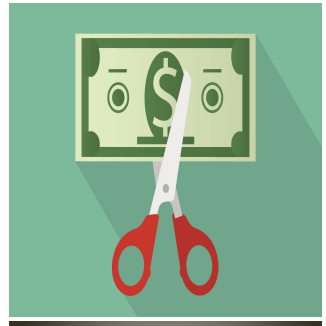
QKD: All parties have advanced quantum capabilities.
What if Bob can't measure in the X basis?

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

Bridge the gap between Classical and Quantum realms

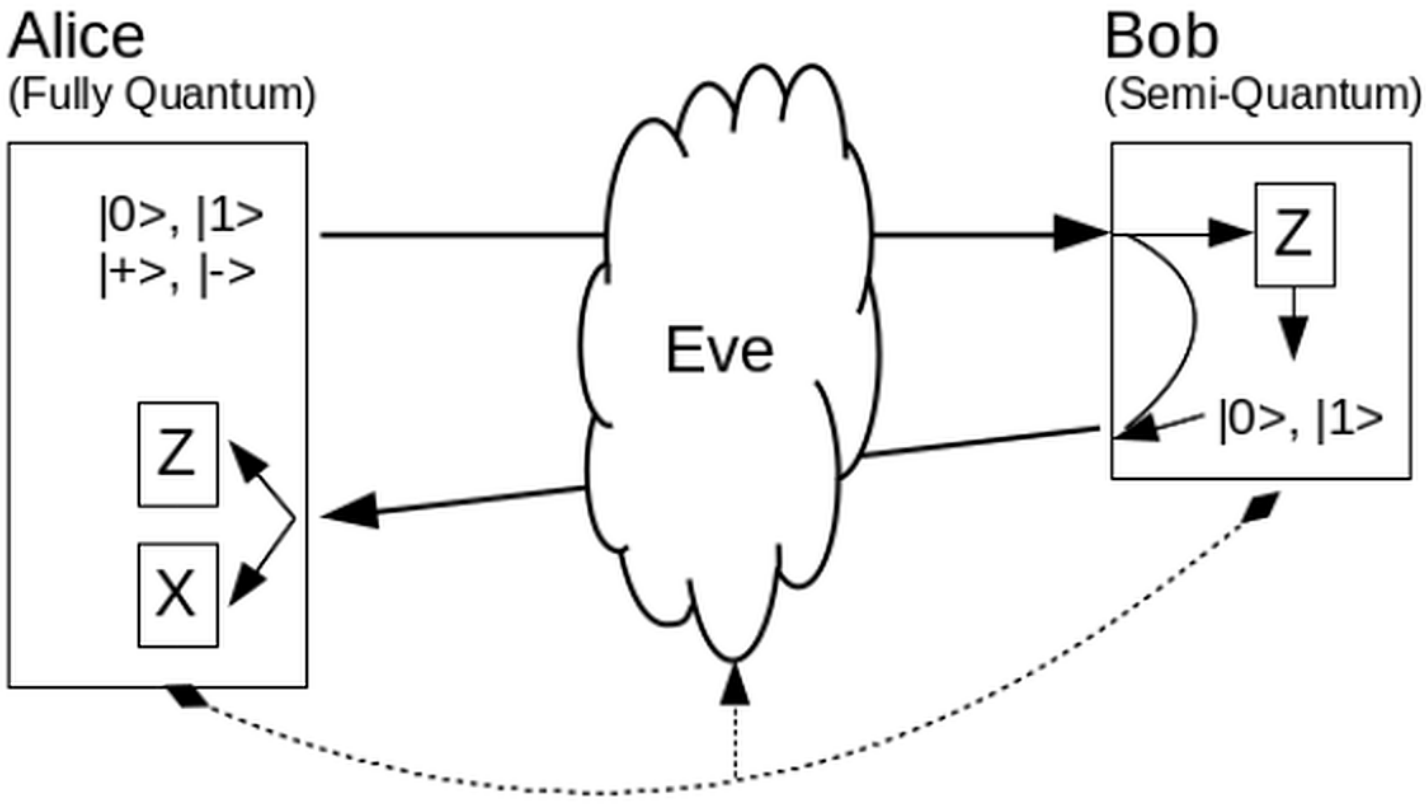
Use less expensive hardware

Fallback option for fully fledged QKD



But It's Too...

A Concrete Example



SQKD

QKD with High-dimensional(HD) systems

Naturally carries more information

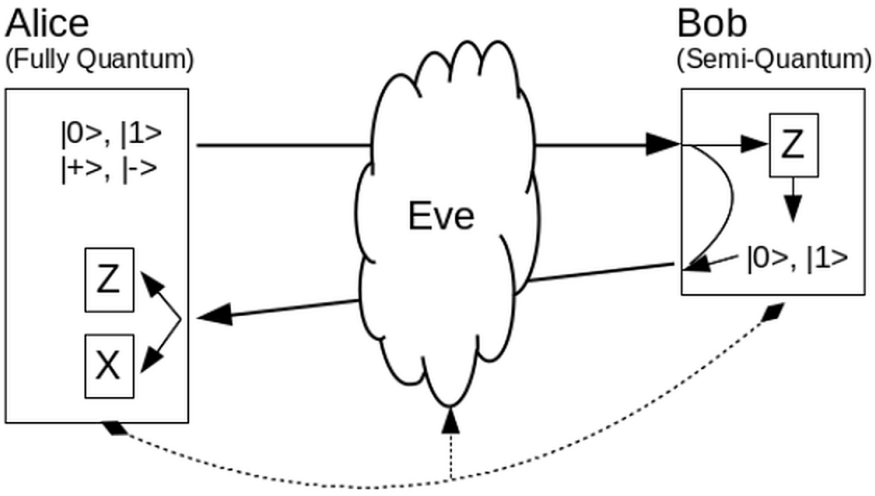
More Robust against quantum cloning

More noise resistant

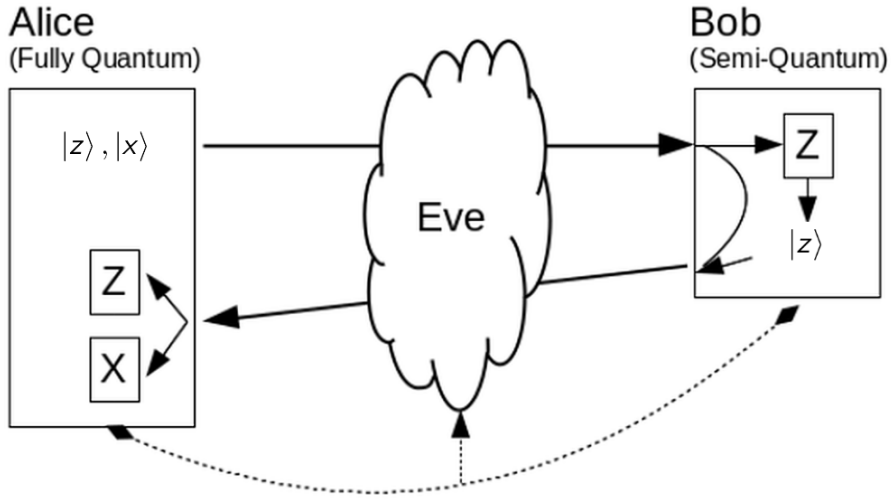
Earlier works on HD-QKD include:

- 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?



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



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

,

Is It Secure?

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:

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

and another desired state be:

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

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

$$\min_{\rho_E} \frac{1}{2}(1 - p_{abort}) ||\rho_{ABE}^{real} - \rho_{ABE}^{ideal}||_1 \leq \epsilon,$$

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

By monotonicity of trace distance, this implies (hiding some factors):

$$\delta := ||\rho_{AE}^{real} - \rho_{AE}^{ideal}||_1 \leq \epsilon$$

Renner (2005) proved the following about the distance :

$$\delta \leq 2^{-\frac{1}{2}(H_{min}(\rho_{AE}|E)-l)},$$

where l is the final length of the key.

He also proved that if $H(\cdot)$ is the Von Neumann entropy, A, B, E are the memory registers of Alice, Bob and Eve respectively, then if:

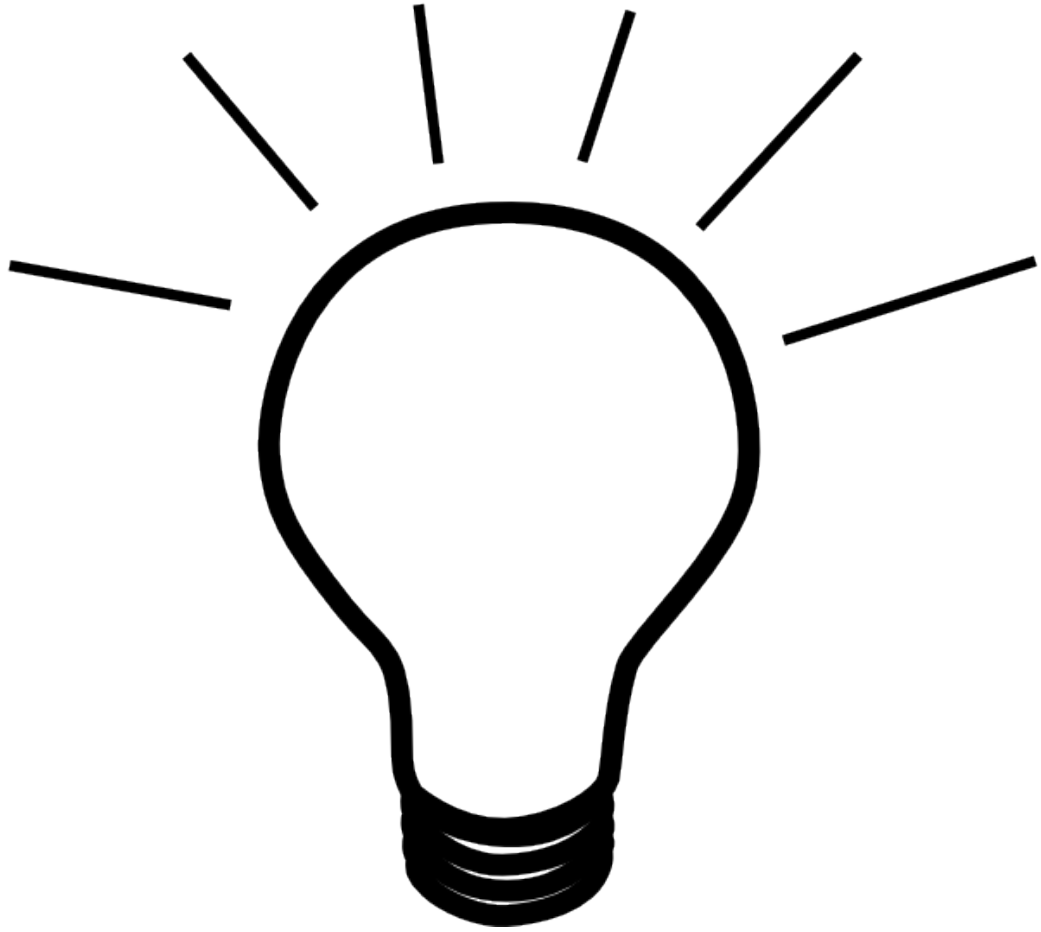
$$I \lessapprox n\big(\min_{\sigma_{AB}\in\Gamma} H(A|E) - H(A|B)\big),$$

where Γ is the set of bipartite density operators for which the protocol does not abort, then the protocol is ϵ'-secure.

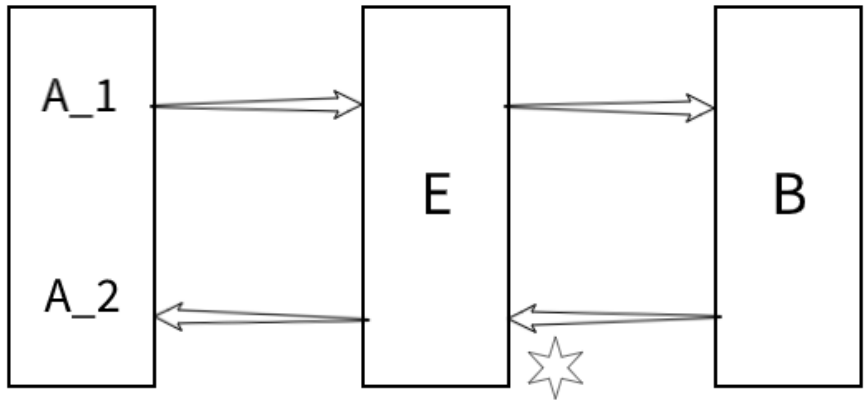
The key-rate of a protocol is defined as:

$$\text{key-rate} := \frac{I}{n} = \min_{\sigma_{AB} \in \Gamma} H(X|E) - H(X|Y)$$

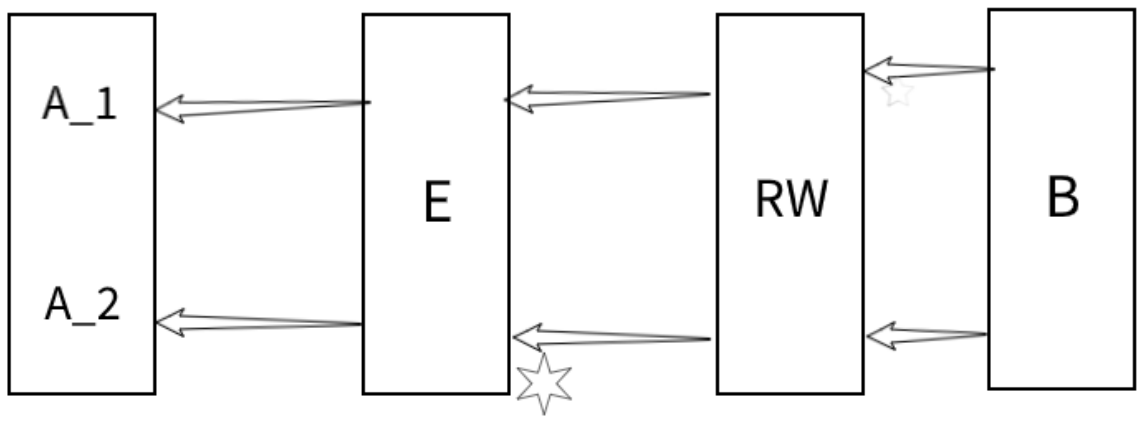
Problem: Two-way SQKD analysis and density matrix computation is too complex



Solution: Reduction to One Way Protocol



Two-Way SQKD



One-Way SQKD

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	

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

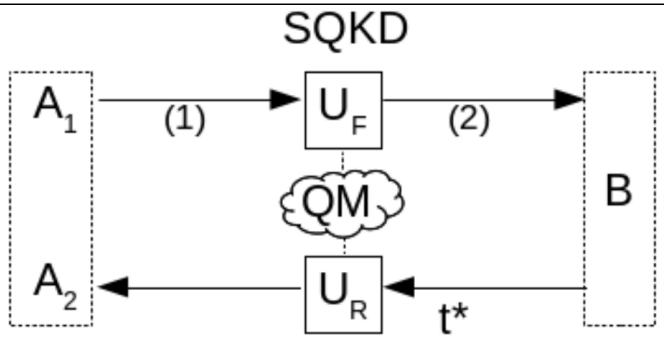
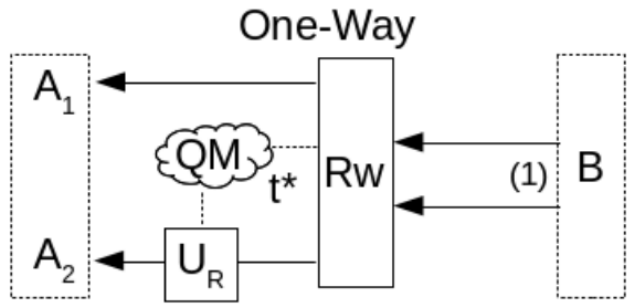
$$|\phi_R\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)}\, |b,b\rangle_{A_1A_2} \otimes |0\rangle_B \tag{2}$$

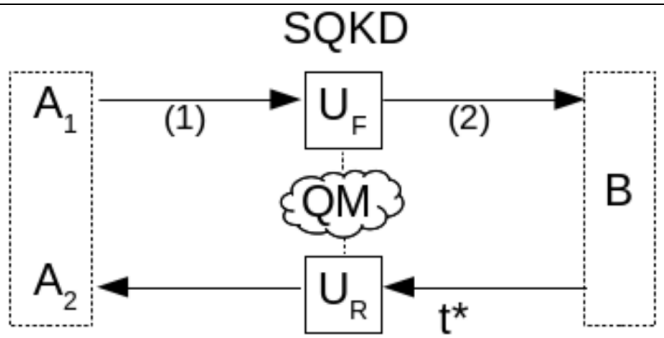
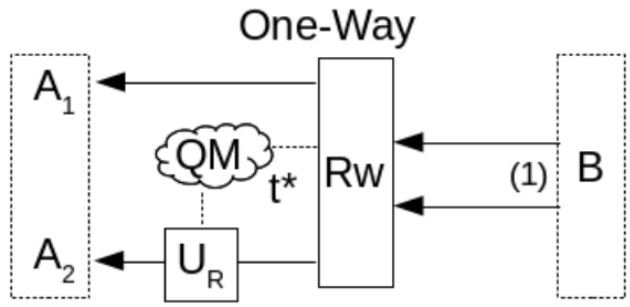
$$|\phi_{MR}\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)}\, |b,b,b\rangle_{A_1A_2B} \tag{3}$$

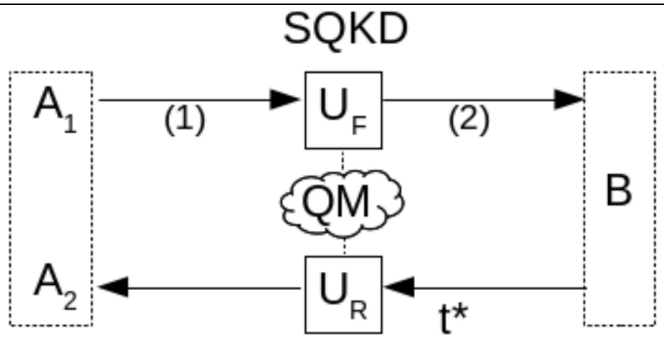
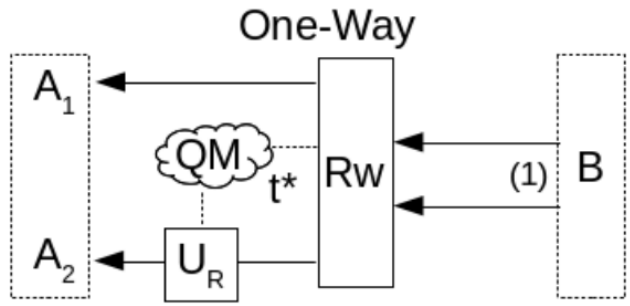
Theorem

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.

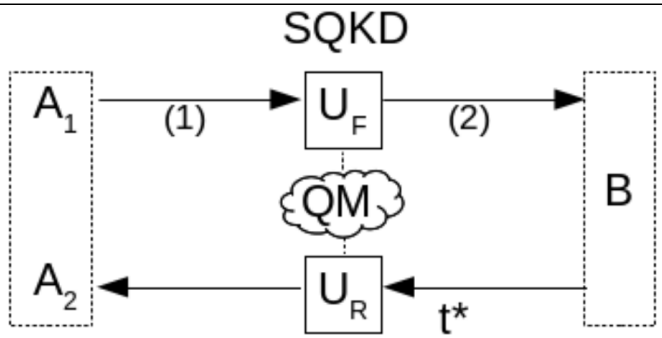
Proof

HD-SQKD	OW-SQKD
	

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

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

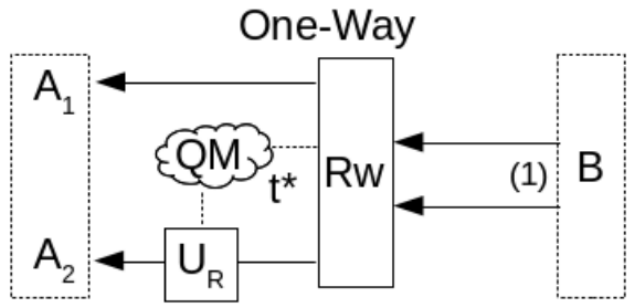


$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_a |a, a\rangle$$

$$U_F |a\rangle \otimes |\chi\rangle = \sum_b |b, e_{ab}\rangle$$

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

OW-SQKD

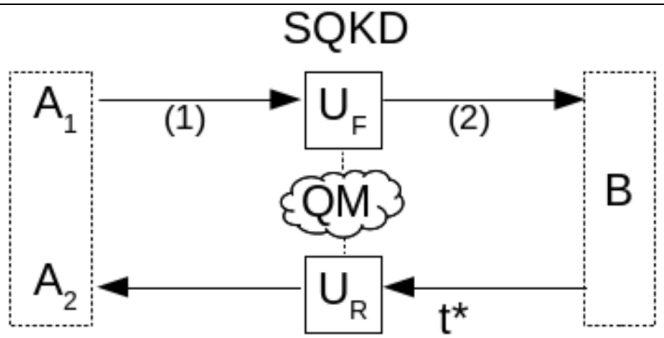


$$|\phi\rangle = \sum_{b=0}^{N-1} \sqrt{p(b)}\, |b, b, b\rangle_{A_1 A_2 B}$$

$$R_w |b, b\rangle_{A_1 A_2} = \frac{\sum_a |a, b, e_{ab}\rangle}{\sqrt{N.p(b)}}$$

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

HD-SQKD

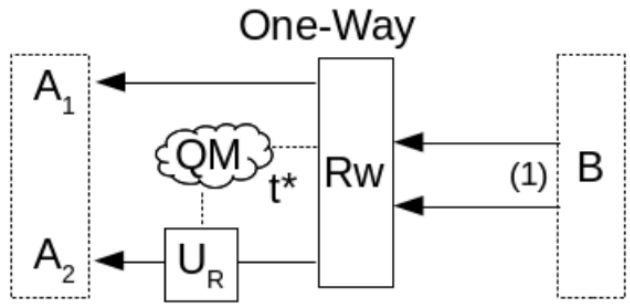


$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_a |a, a\rangle$$

$$U_F |a\rangle \otimes |\chi\rangle = \sum_b |b, e_{ab}\rangle$$

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

OW-SQKD



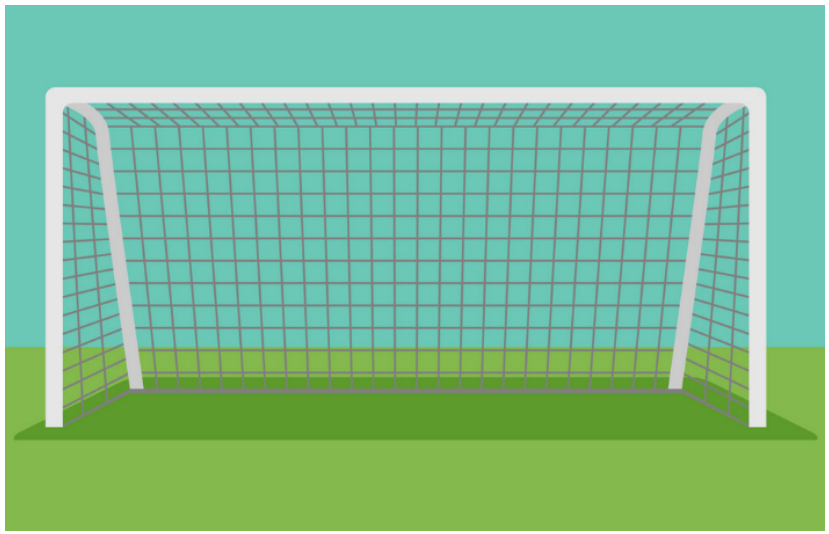
$$|\phi\rangle = \sum_{b=0}^{N-1} \sqrt{p(b)}\, |b, b, b\rangle_{A_1 A_2 B}$$

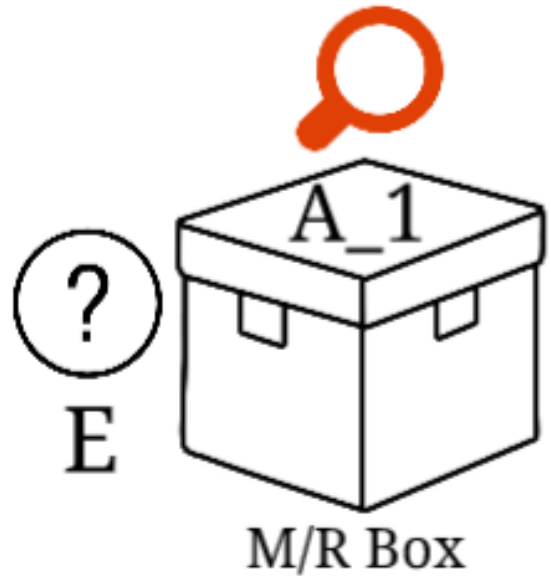
$$R_w |b, b\rangle_{A_1 A_2} = \frac{\sum_a |a, b, e_{ab}\rangle}{\sqrt{N.p(b)}}$$

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

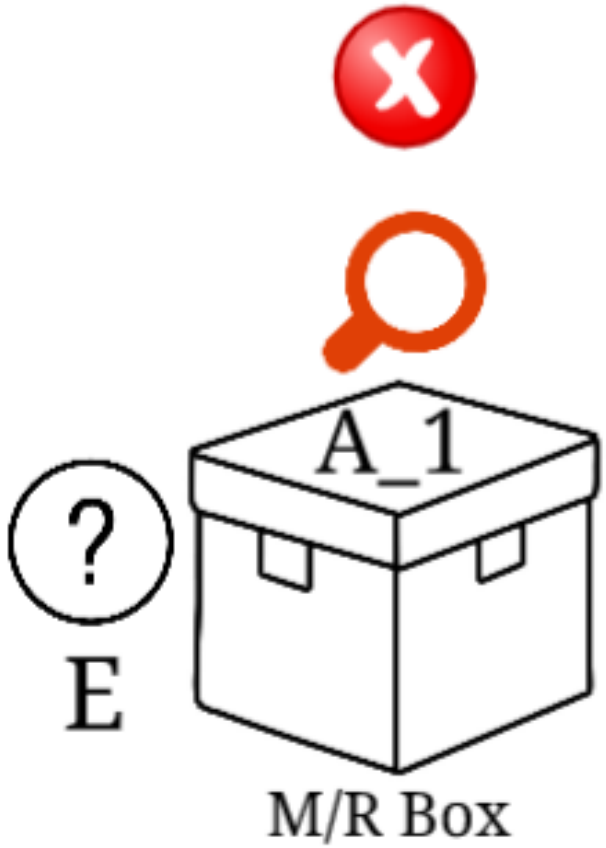
$$= \frac{1}{\sqrt{N}} \sum_a |a\rangle_{A_1} \sum_b |b, e_{ab}, b\rangle_{A_2 EB}$$

Key-rate Computation

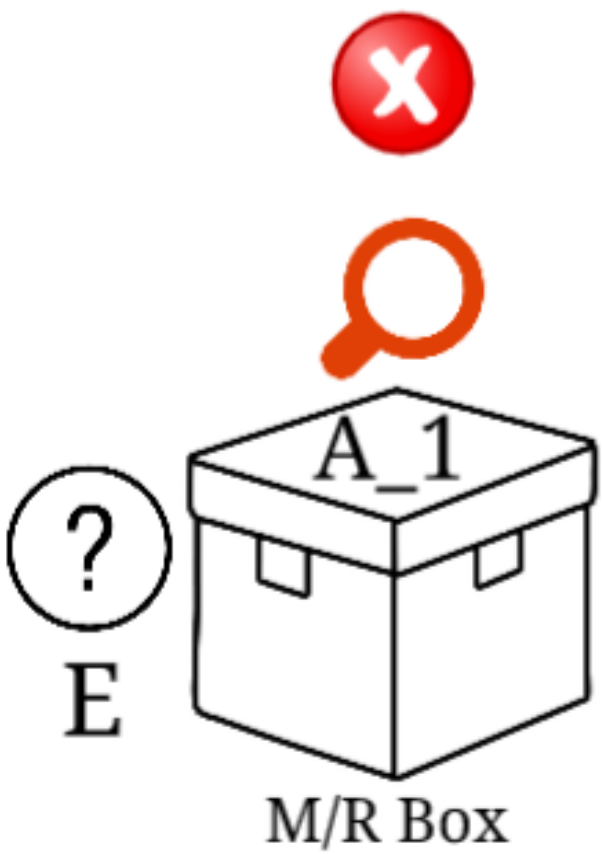


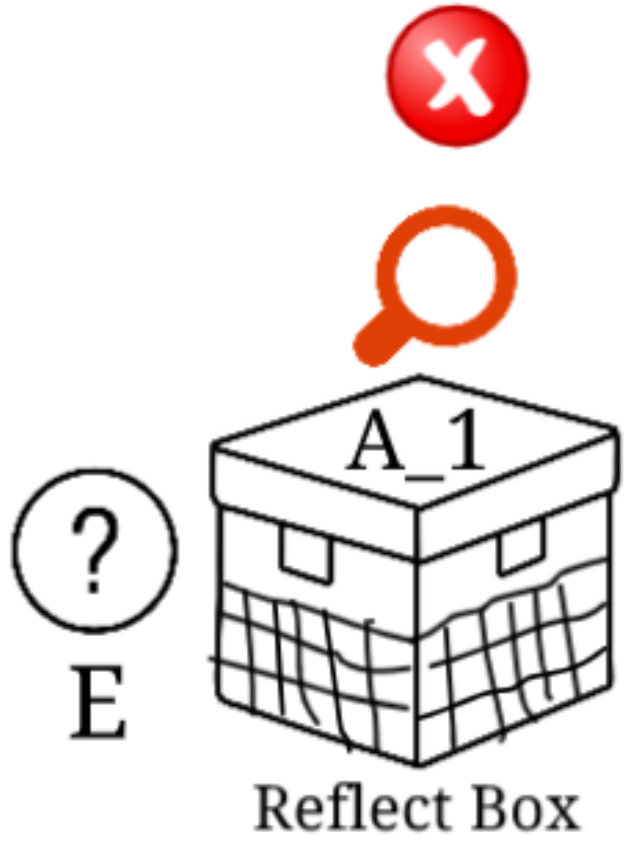


Our goal is to upper bound Eve's uncertainty about Alice's register in measure/resend (M/R) case.

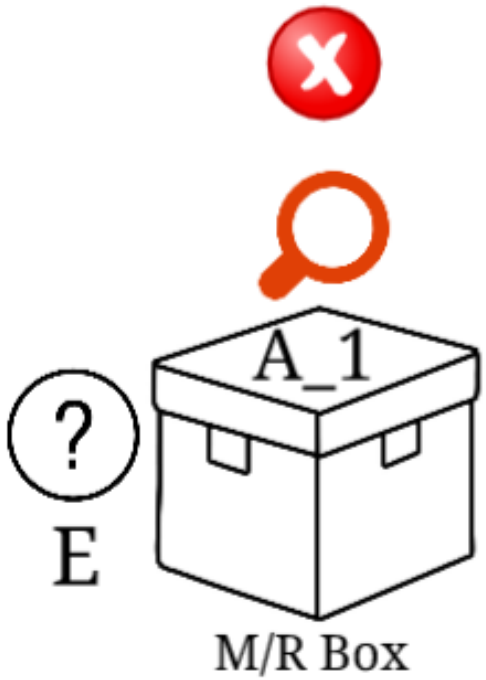


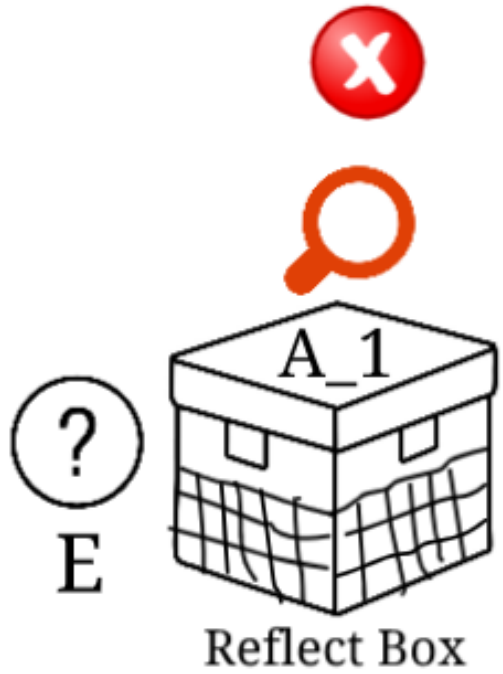
But it's not observable!

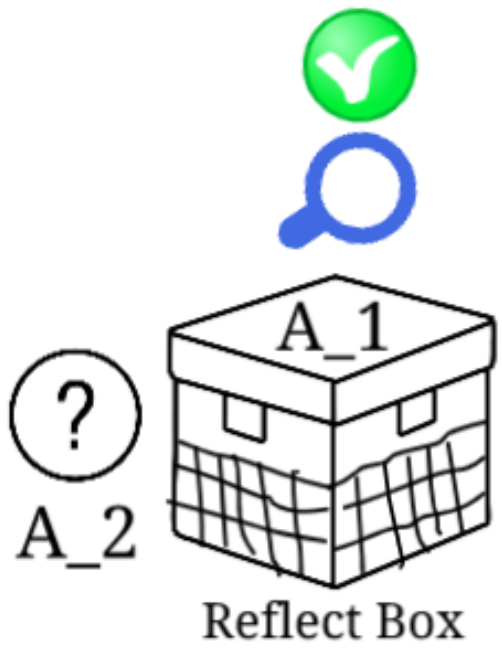


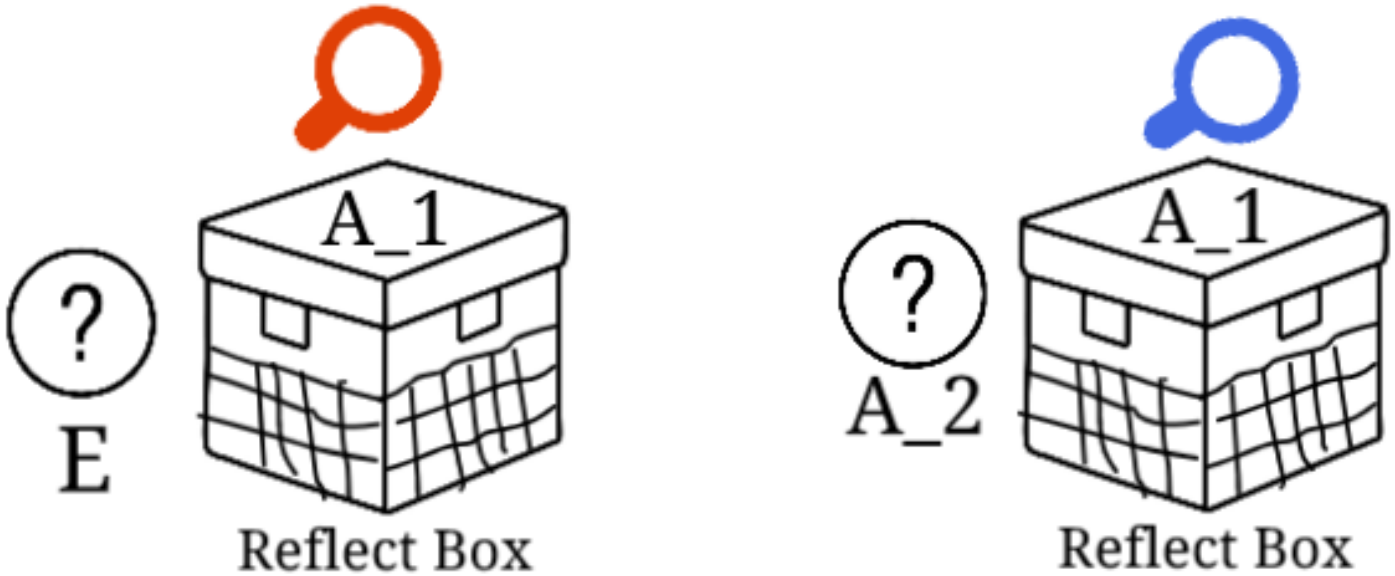


It doesn’t get easier.


A_1
?
E
M/R Box


A_1
?
E
Reflect Box

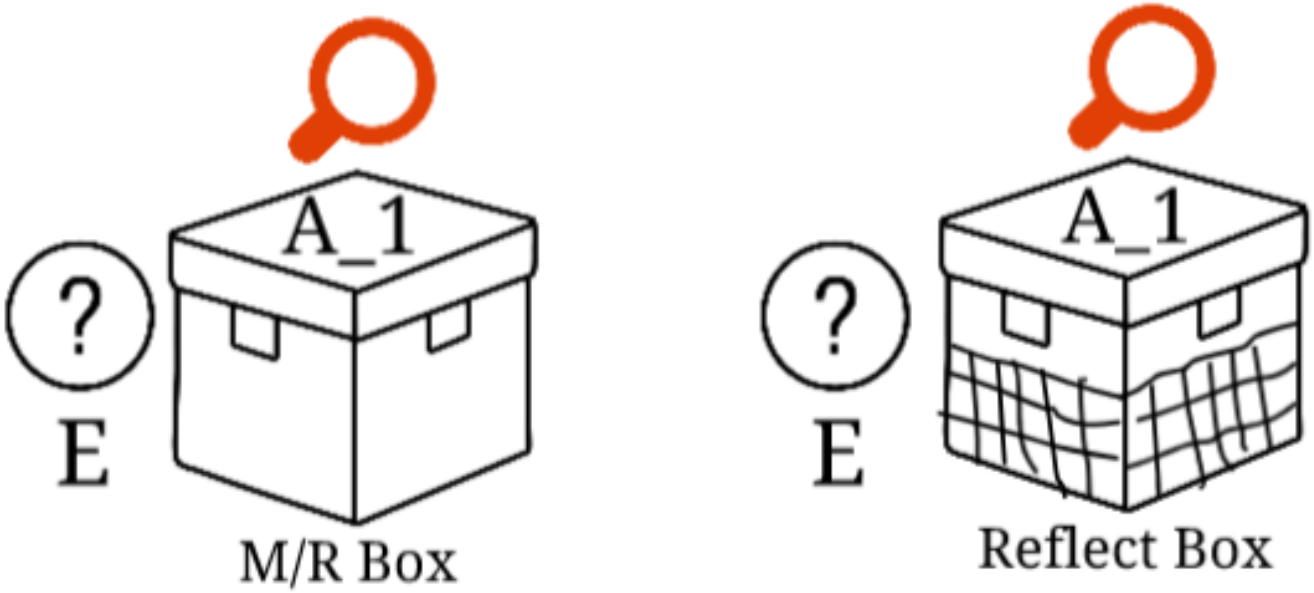

A_1
?
A_2
Reflect Box



Eve and A_2's uncertainty about A_1 has a lower bound (Berta et al. (2009)

Formally, for any density operator $\rho_{A_1 A_2 E}$ and two measurements Z and F,

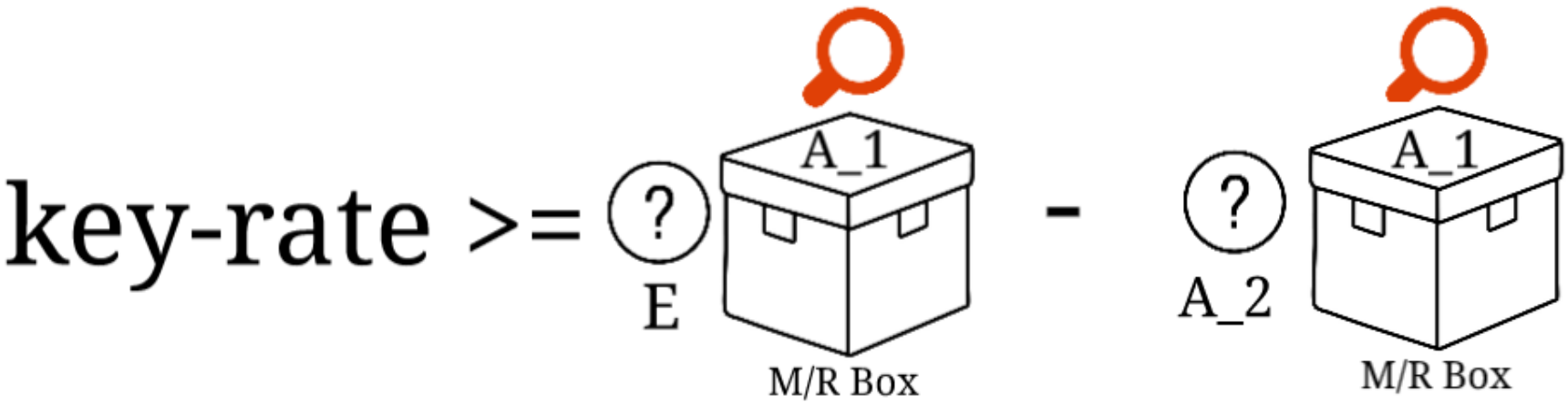
$$H(A_1^Z|E) + H(A_1^F|A_2) \geq \log_2 \frac{1}{c}$$



Eve's uncertainty about Alice's same measurement about both of the boxes is lower bounded by how different the boxes are. (Winter, 2005)

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

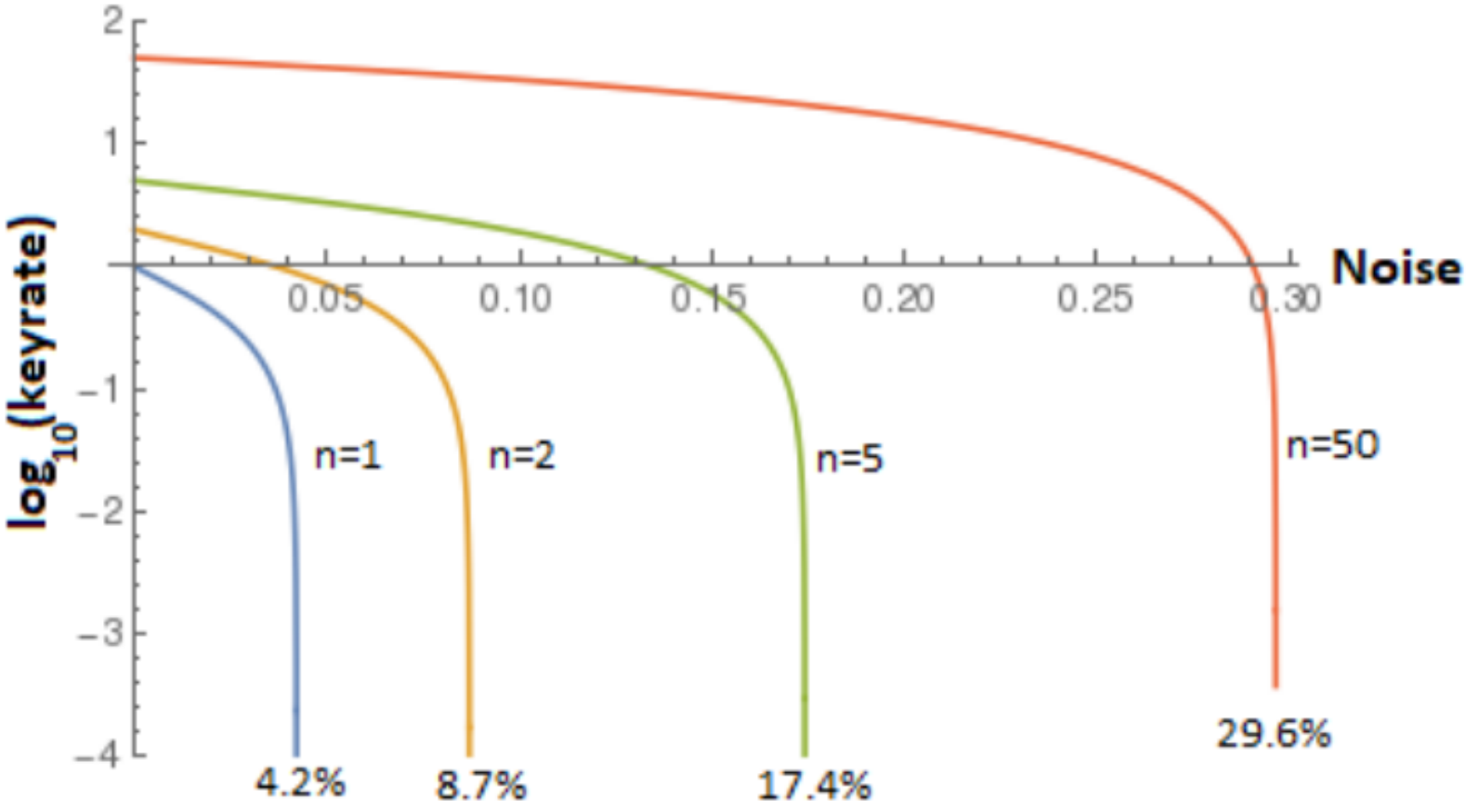
$$|H(A_1^Z|E)_\rho - H(A_1^Z|E)_\mu| \leq 2\delta log|A_1^Z| + (1+\delta)h(\frac{\delta}{1+\delta})$$



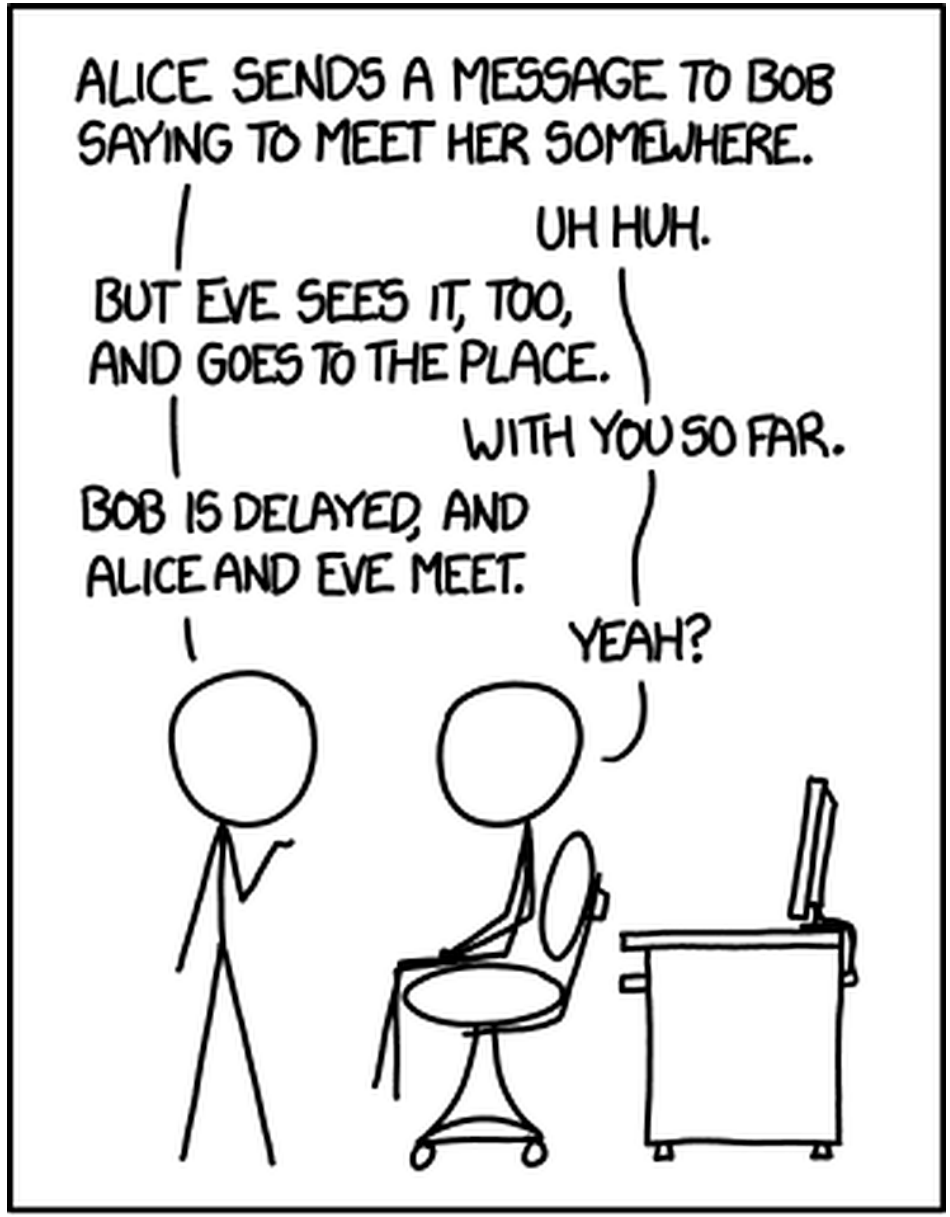
In our case, this is:

$$\text{key-rate} \geq f(n, \delta, Q, Q_F),$$

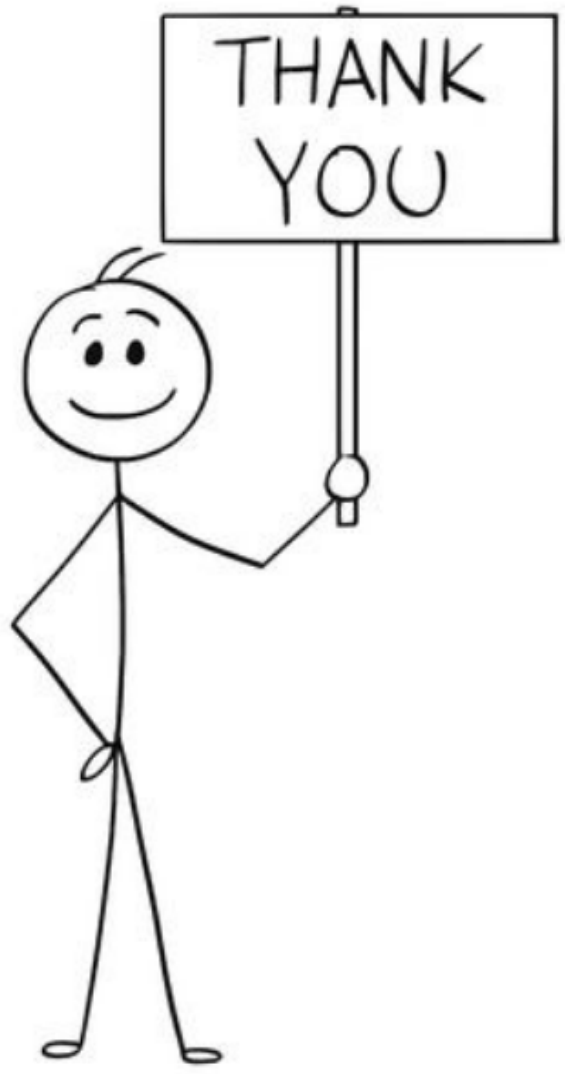
where, n is the number of qubits sent, δ is the trace distance, Q and Q_F are noise in both direction and noise in the forward direction only.



Key-rate of our HD-SQKD protocol



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


THANK
YOU