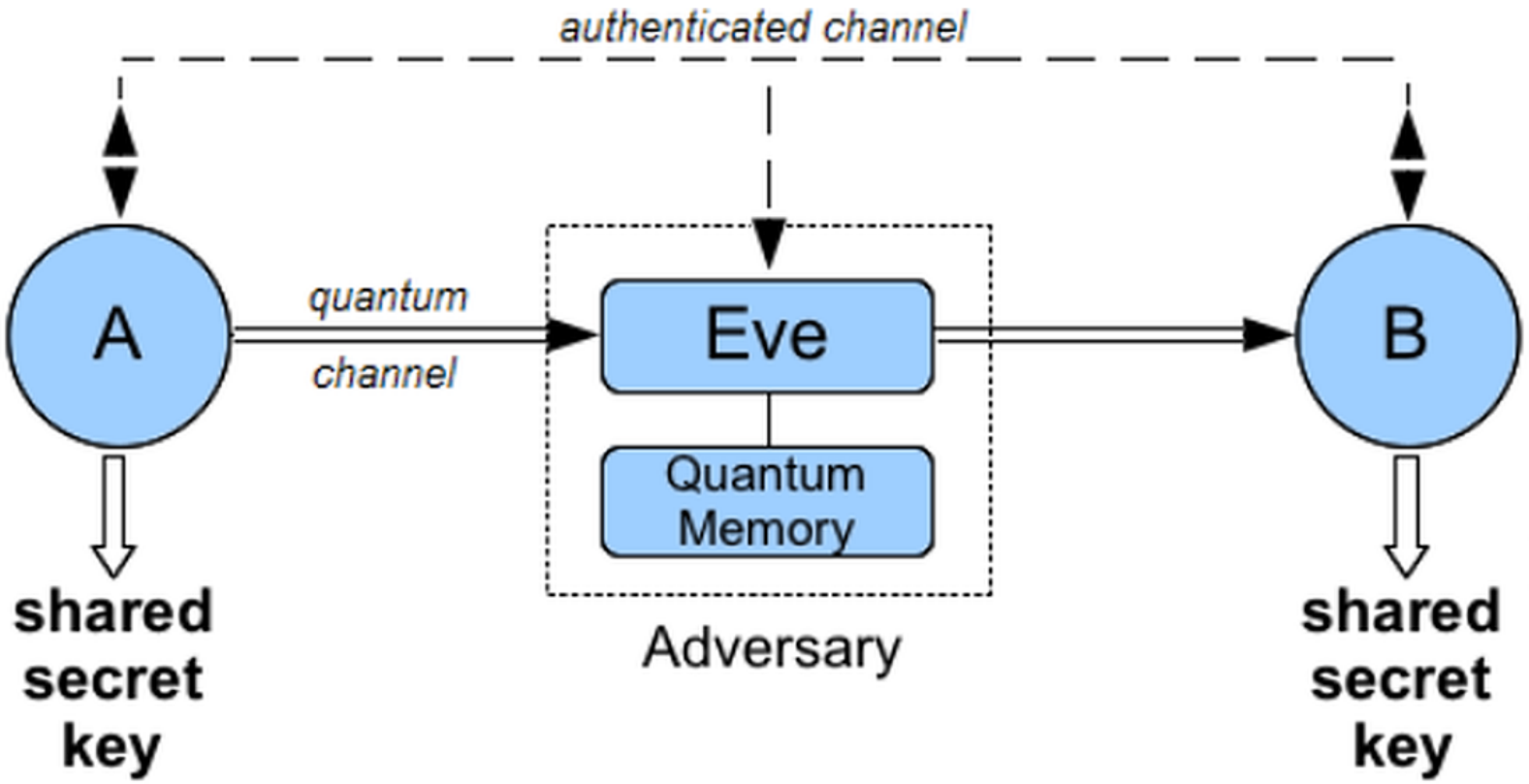
High-Dimensional SQKD

Hasan Iqbal, Walter Krawec

CSE, UCONN

July 10, 2020

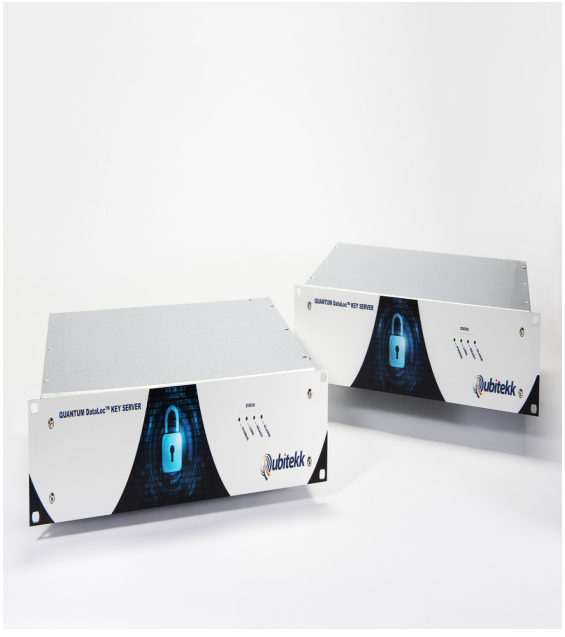
What is Quantum Key Distribution(QKD)



QKD in Practice

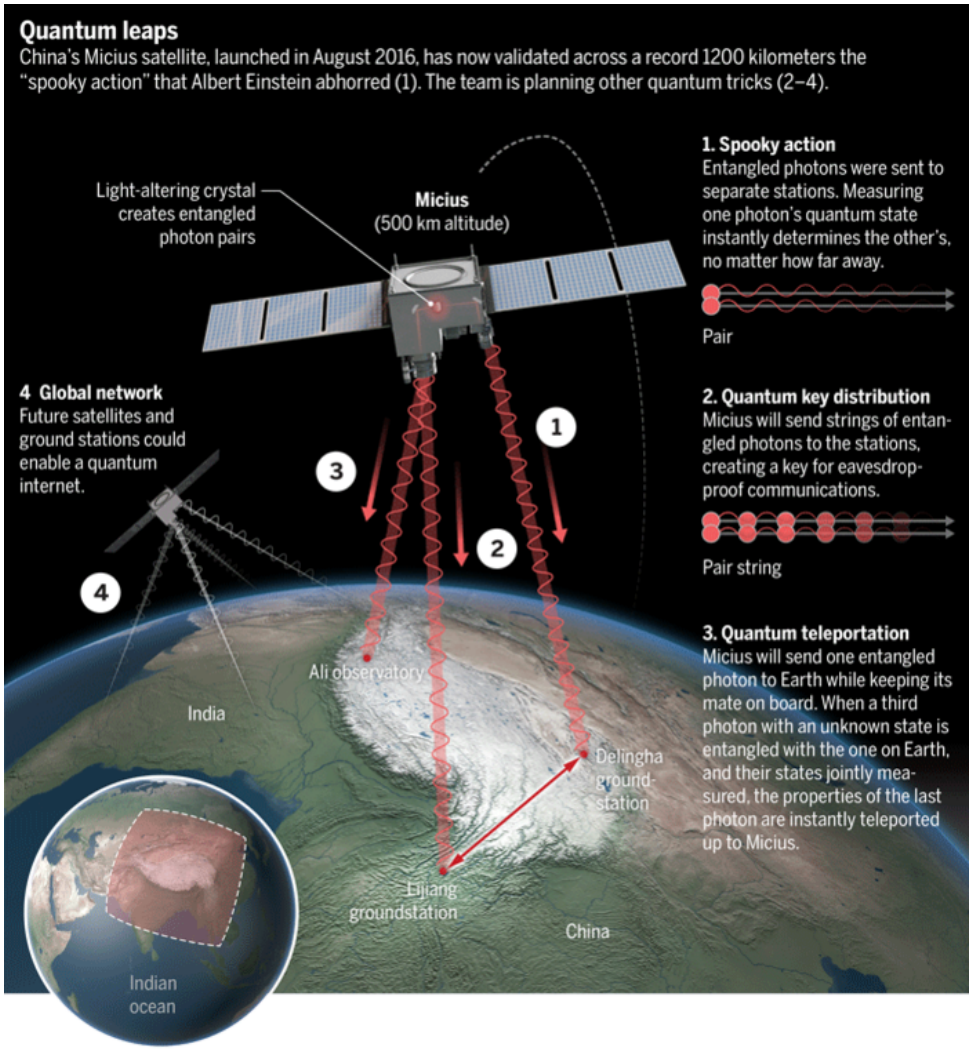
IDQuantique, Switzerland

Toshiba, Japan



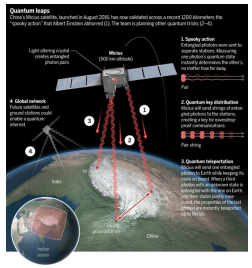
Qubittek, USA

In The Space! (Liao et al., 2017)



Free Space QKD and Teleportation

In The Space! (Liao et al., 2017)



Free Space QKD and Teleportation

1. micius launched in 2016. 2. uses decoy state qkd to establish k1, k2 with two ground stations, xors them, sends them to one of the grounds, that base can do xor to get shared key. 3. AES could be used to do further communication

Wait a Minute...

QKD: All parties have advanced quantum capabilities.

What if one of them doesn't?

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

Bridge the gap between Classical and Quantum realms

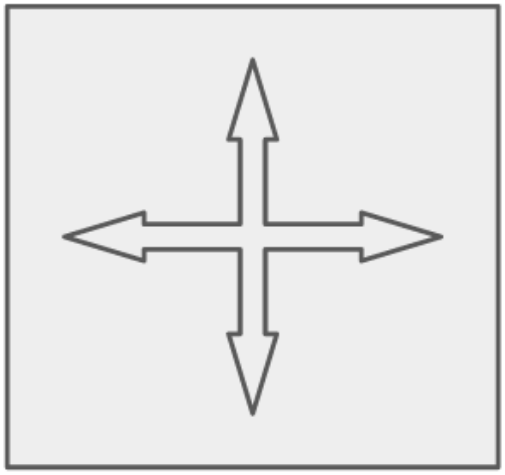
Use less expensive hardware

Fallback option for fully fledged QKD

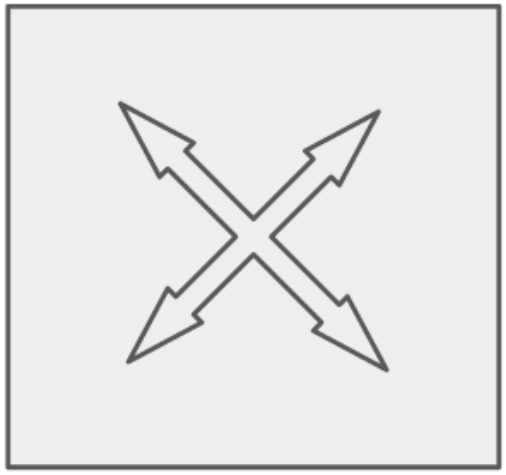
But It's Too...

A Concrete Example

(Qu)Bit of Background (1/4)



Z



X

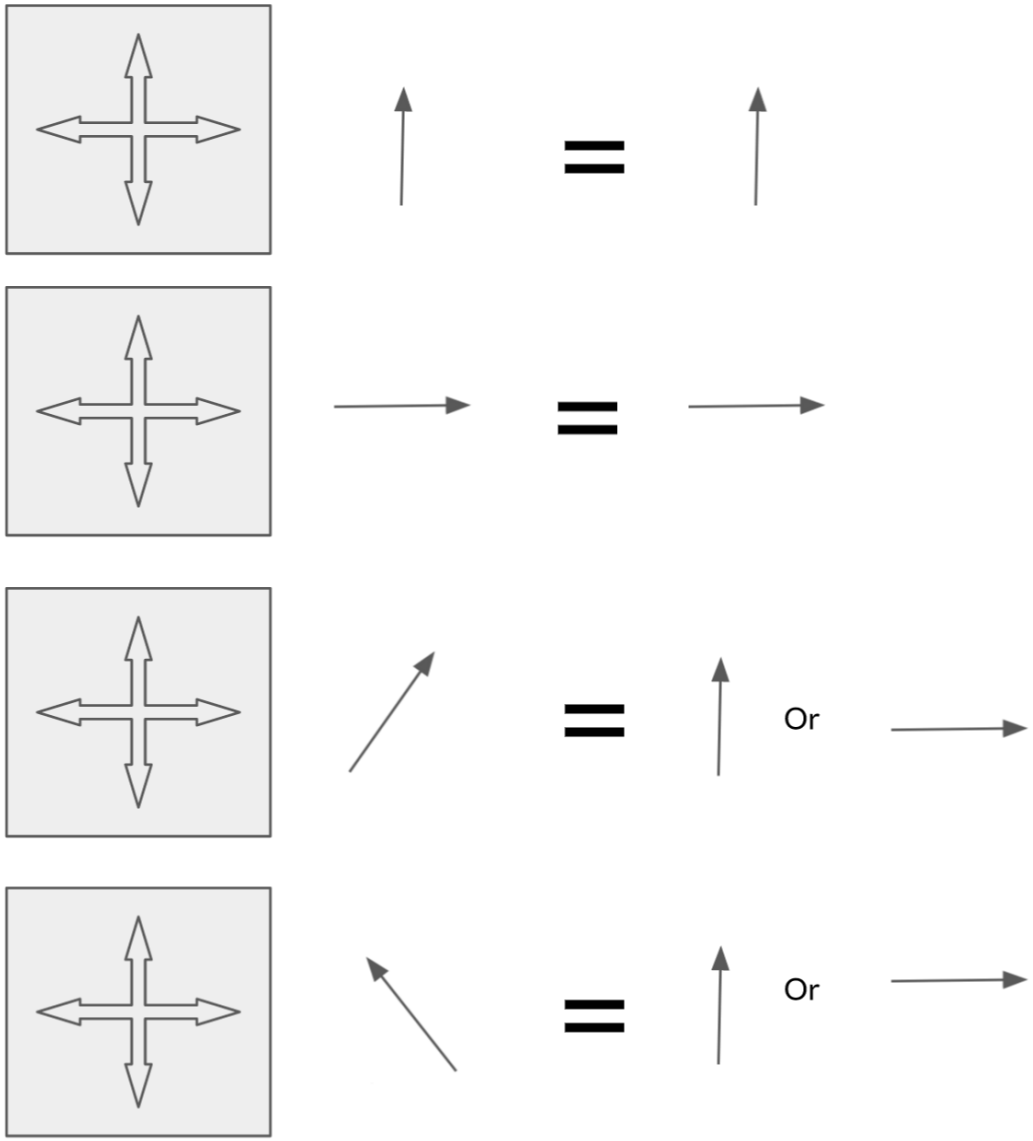
|0>

|1>

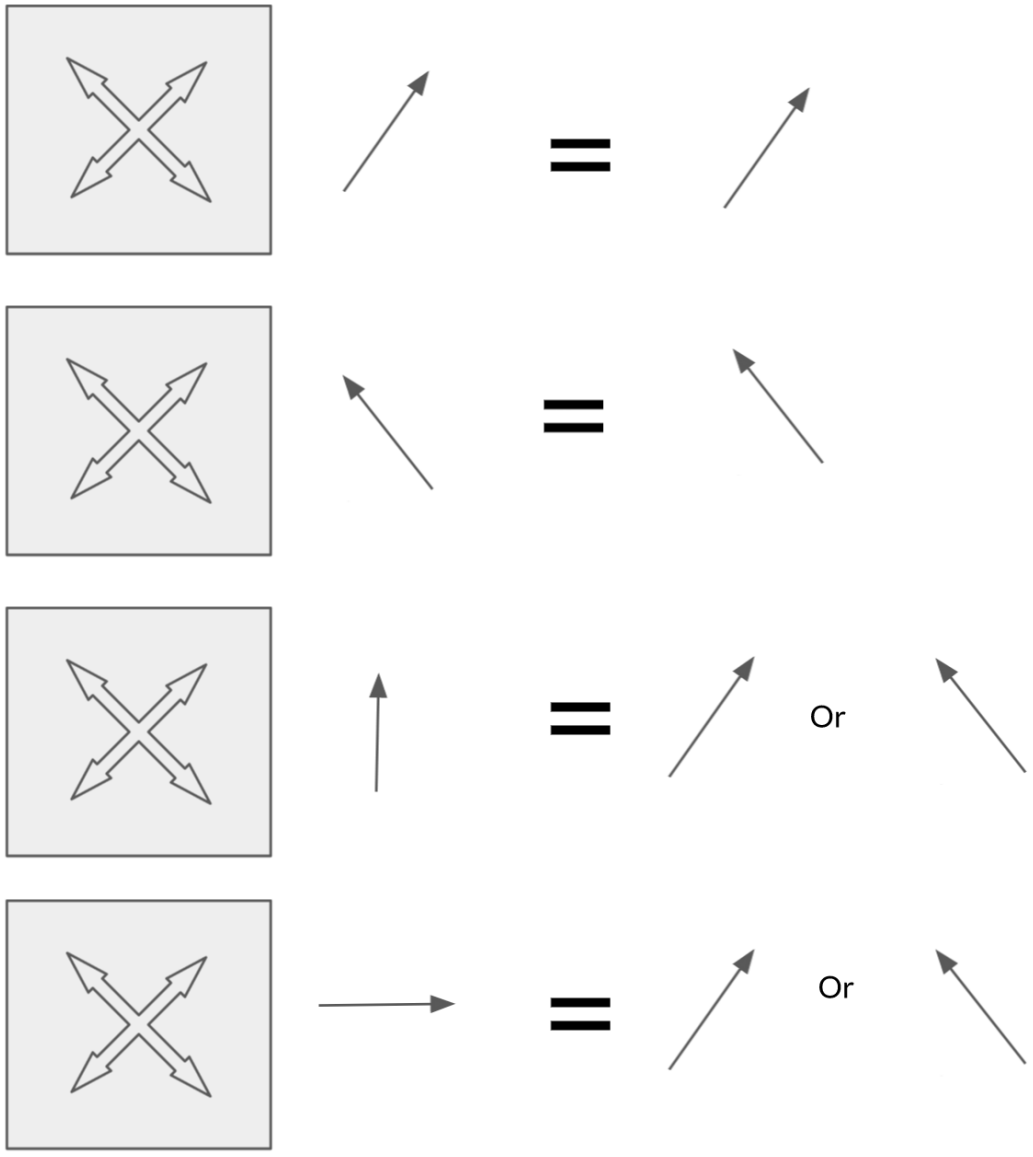
|+>

|->

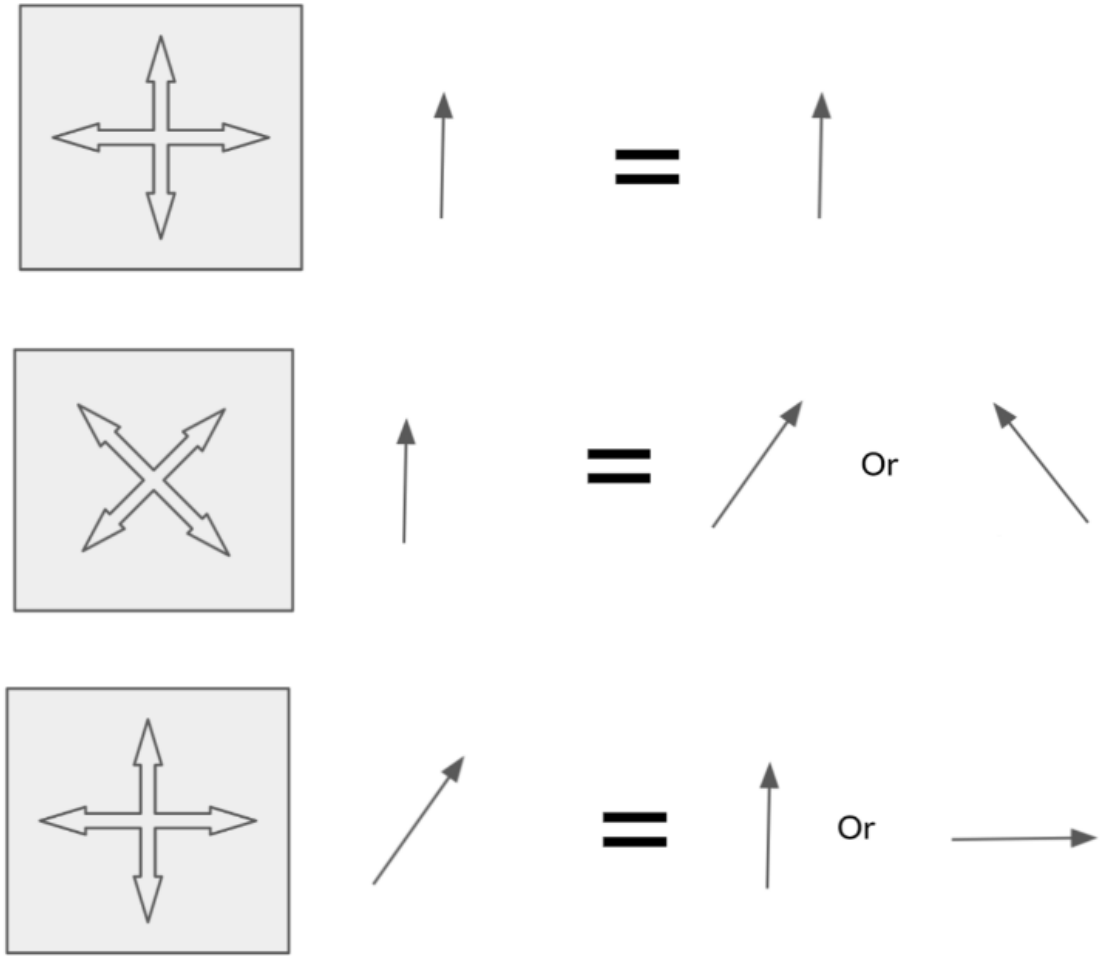
(Qu)Bit of Background (2/4)



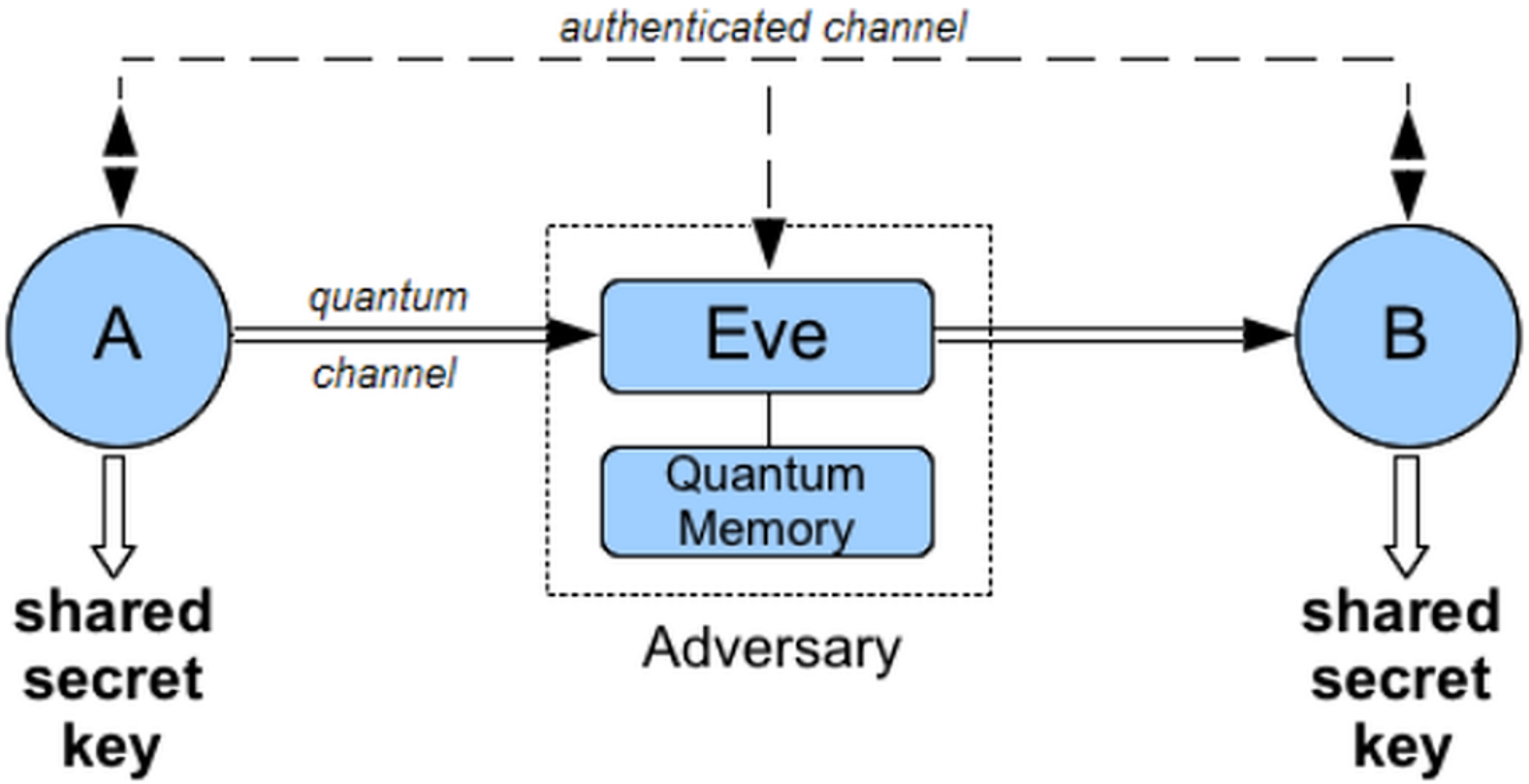
(Qu)Bit of Background (3/4)



(Qu)Bit of Background (4/4)

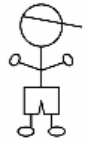


Remember...QKD?

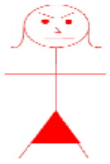


BB84 (Bennett & Brassard, 1984)

Alice



Bob



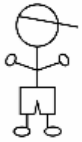
Eve

BB84 (Bennett & Brassard, 1984)

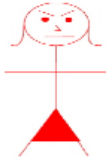
		
0		
1		

Alice's Choices

Alice

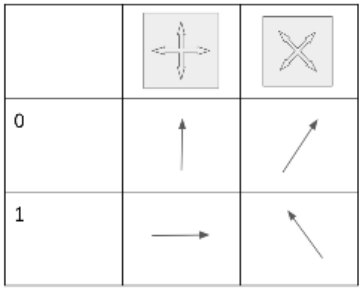


Bob



Eve

BB84 (Bennett & Brassard, 1984)

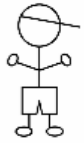


Alice's Choices

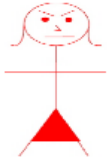
Alice's secret key: 0101

Alice's random gates: ZXXZ

Alice

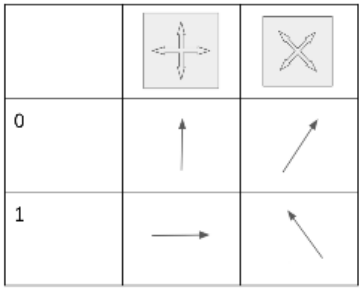


Bob



Eve

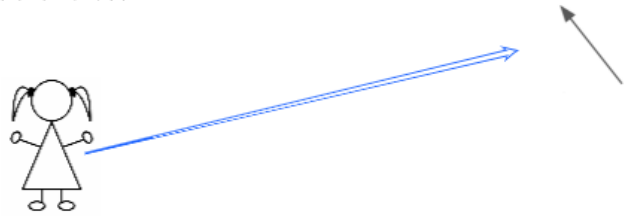
BB84 (Bennett & Brassard, 1984)



Alice's Choices

Alice's secret key: 0101

Alice's random gates: ZXXZ



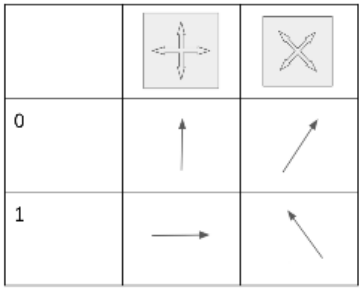
Alice

Eve

Bob

Alice's Bit	Alice's gate	Result	Eve's Gate	Result	Bob's Gate	Result	Bob's Bit
1							

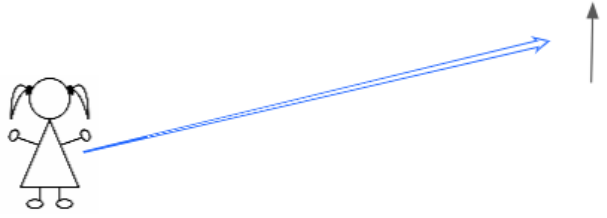
BB84 (Bennett & Brassard, 1984)

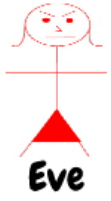


Alice's Choices

Alice's secret key: 0101

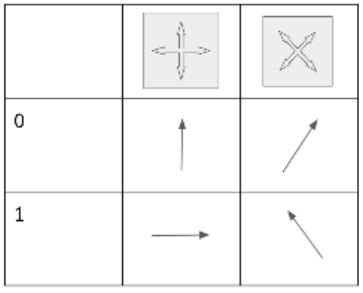
Alice's random gates: ZXXZ





Alice's Bit	Alice's gate	Result	Eve's Gate	Result	Bob's Gate	Result	Bob's Bit
1							

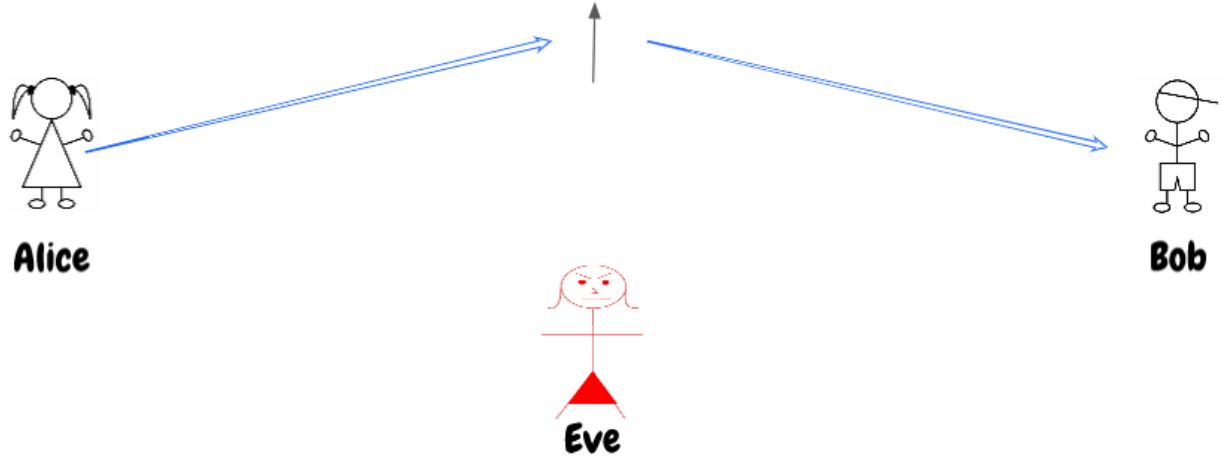
BB84 (Bennett & Brassard, 1984)



Alice's Choices

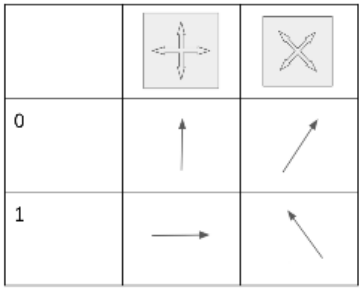
Alice's secret key: 0101

Alice's random gates: ZXXZ



Alice's Bit	Alice's gate	Result	Eve's Gate	Result	Bob's Gate	Result	Bob's Bit
1							

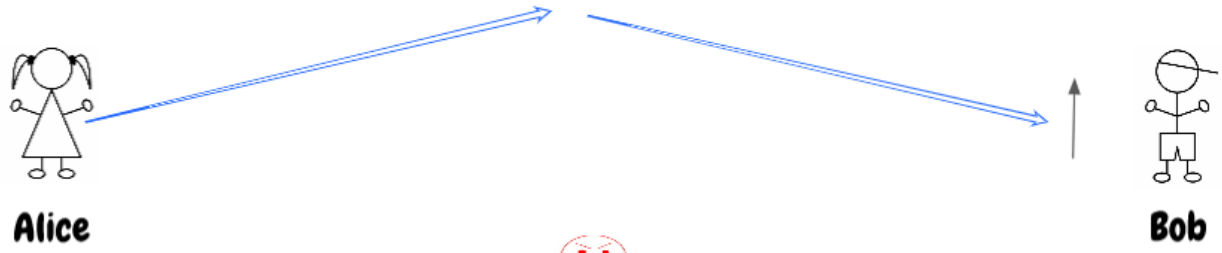
BB84 (Bennett & Brassard, 1984)

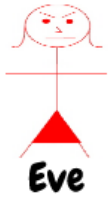


Alice's Choices

Alice's secret key: 0101

Alice's random gates: ZXXZ



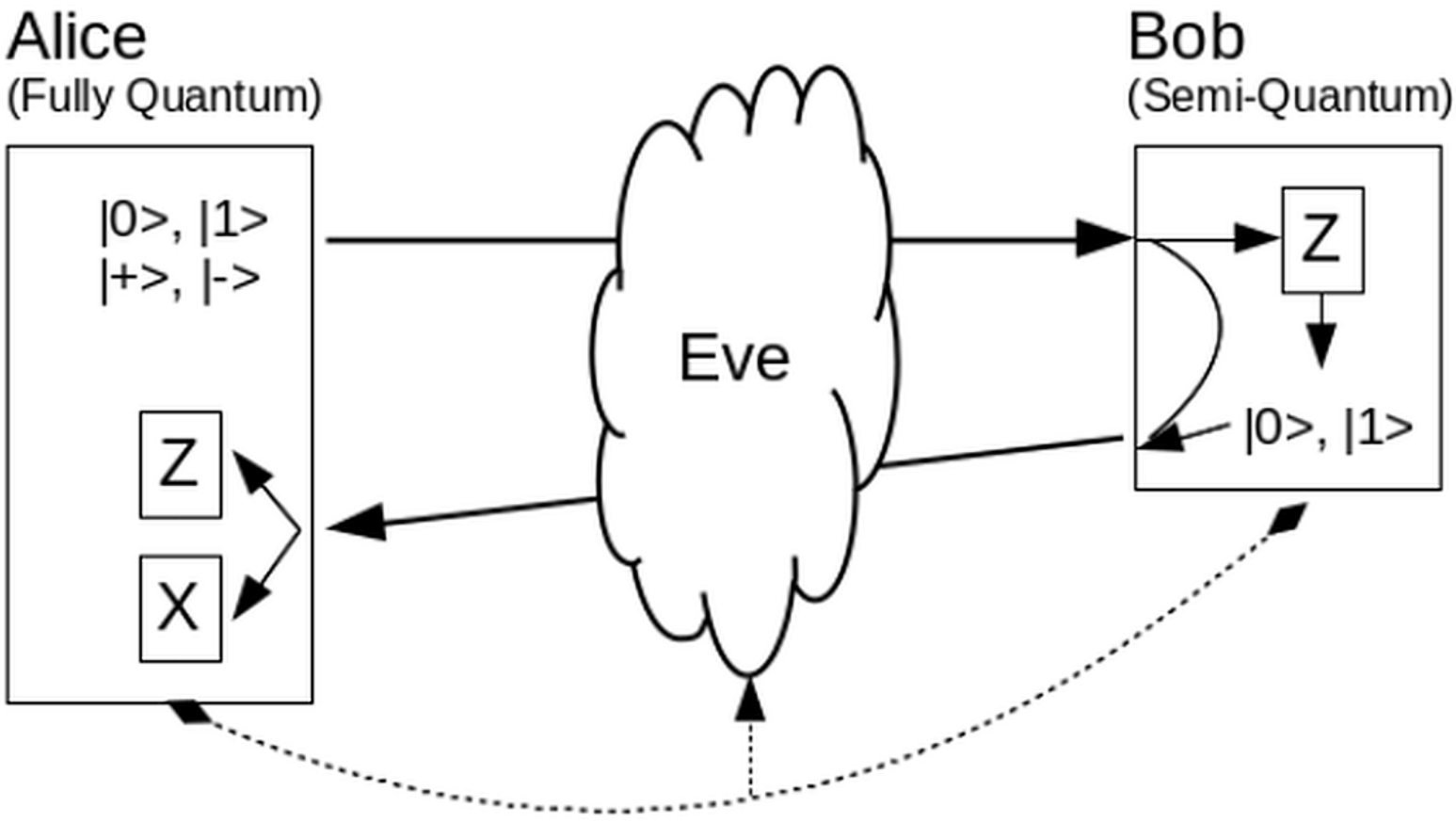


Alice's Bit	Alice's gate	Result	Eve's Gate	Result	Bob's Gate	Result	Bob's Bit
1							N/A

Ok, But...

Where is the middle ground?

SQKD



Motivations for High-Dimensional SQKD (Bourennane et al., 2001)

Naturally carries more information

More Robust against quantum cloning(less fidelity as dimension increases)

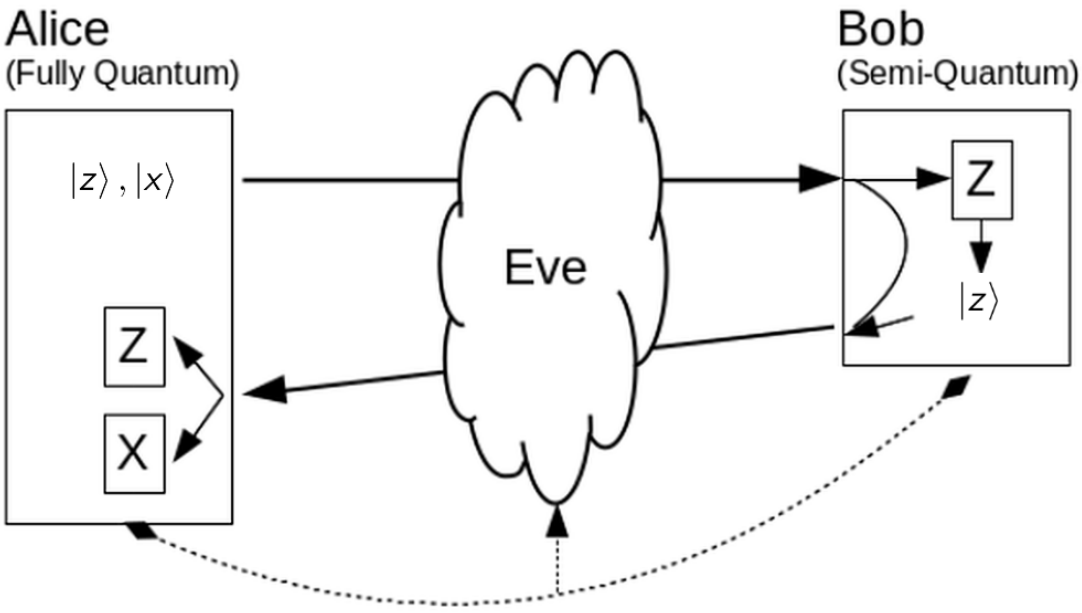
More noise resistant, more efficient

Prior Works on High-Dimensional QKD

- Cerf et al., 2002, Unconditional Security of Bourennane et al.'s result
- Sheridan et al., 2010, Security proof for quantum key distribution using qudit systems
- Mafu et al., 2013, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases
- Cui et al. 2019, Measurement-device-independent quantum key distribution with hyper-encoding

Really? Give Me a Protocol Then...

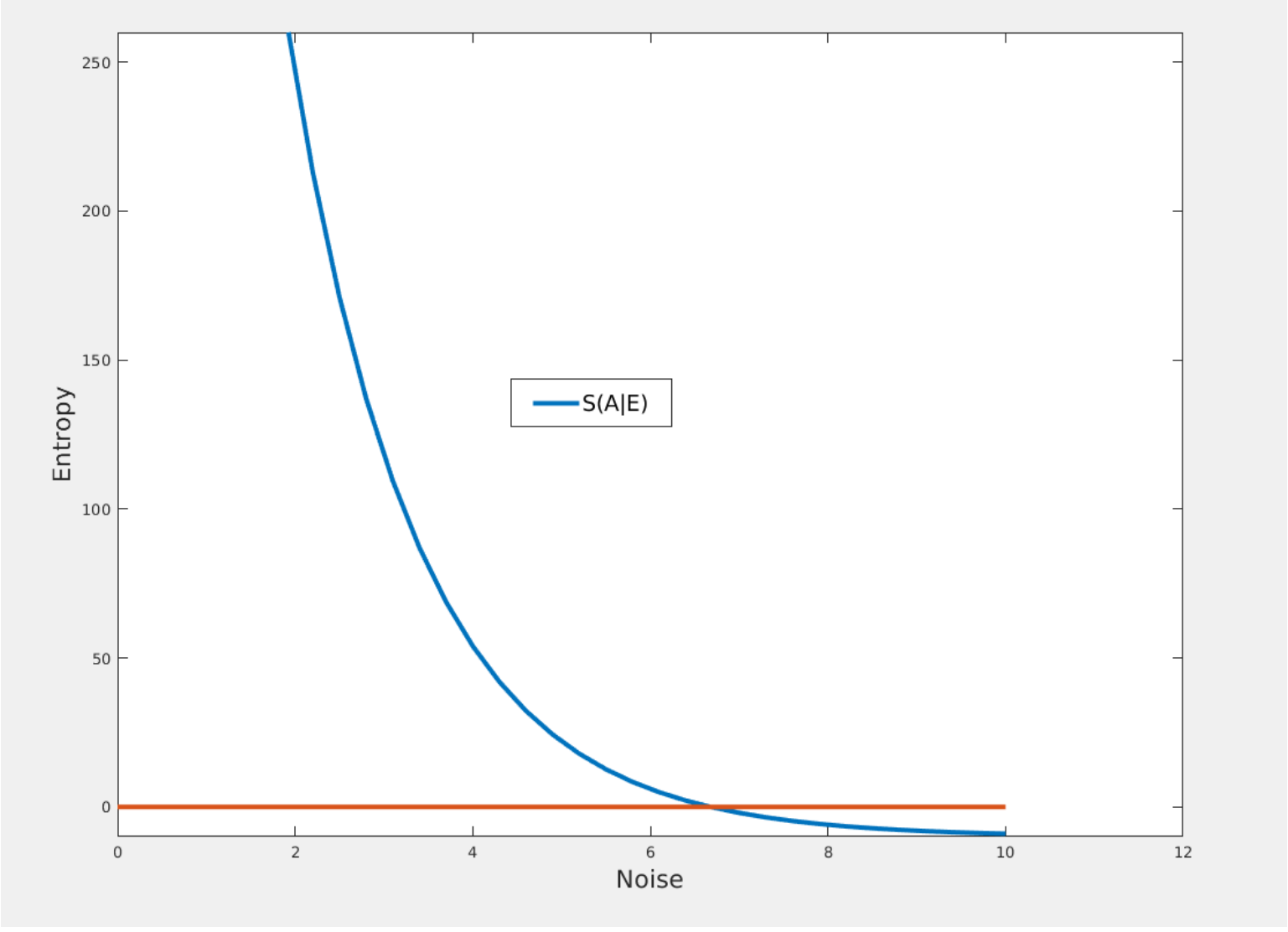
Great news! We already know it...



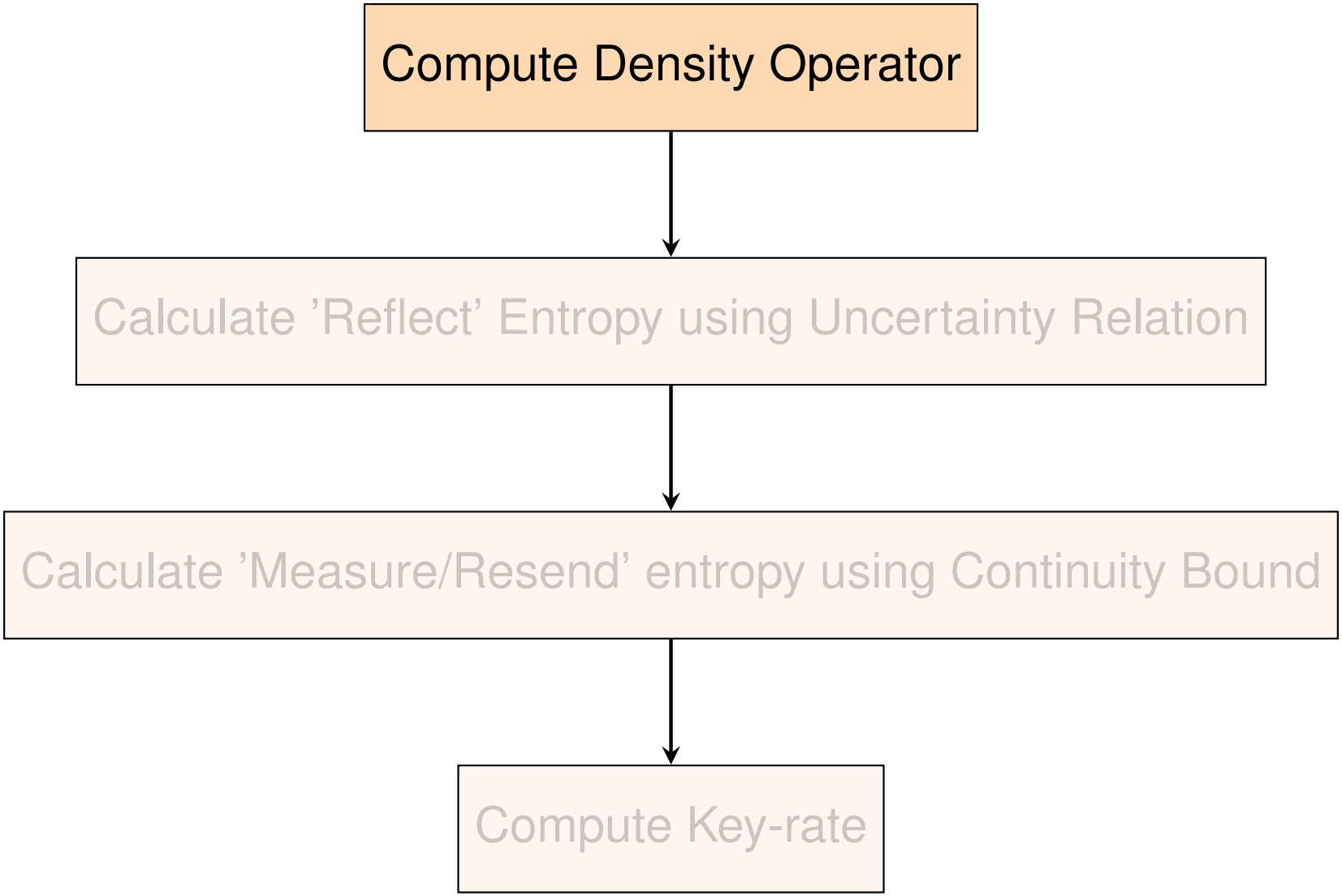
$$|z\rangle \in \{|0\rangle, |1\rangle, ..., |N-1\rangle\}$$
$$|x\rangle \in \mathcal{F}\,|z\rangle$$

But Is It Secure?

What is ’Secure’?



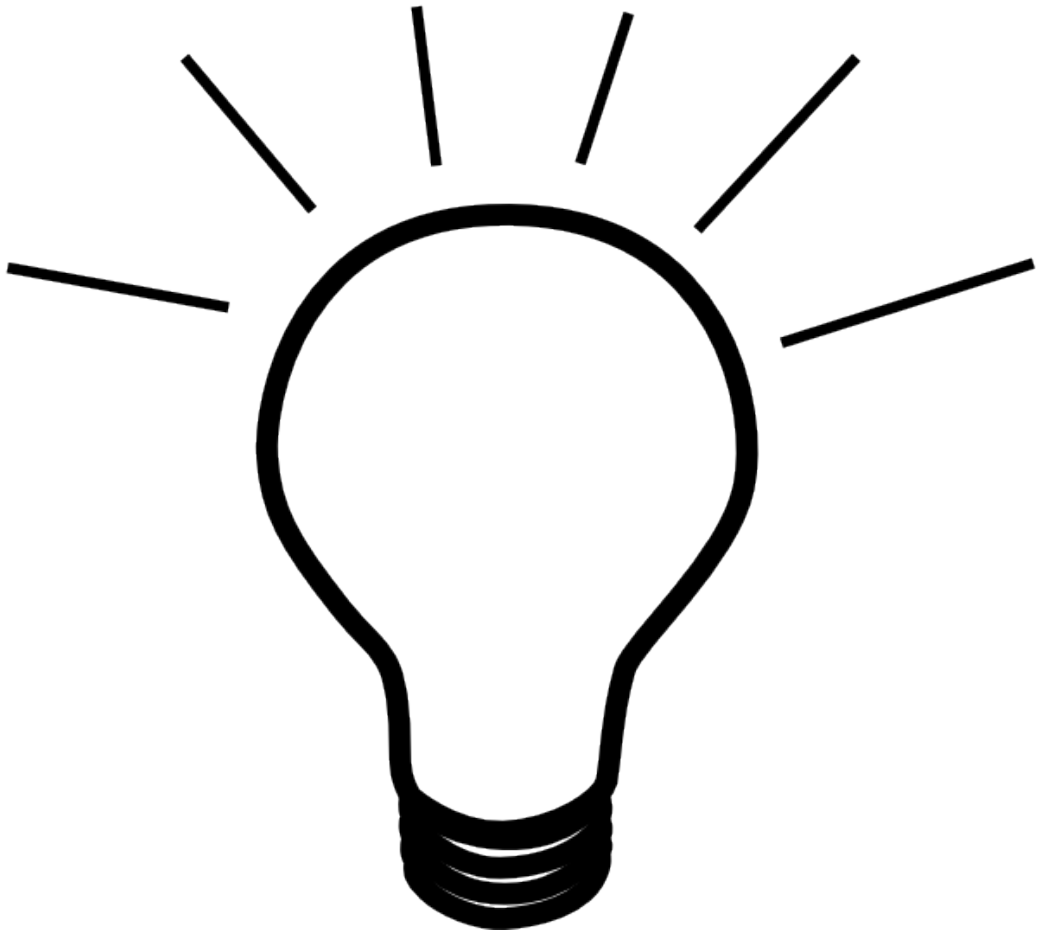
Proof Sketch



High-Dimensional SQKD (cont.)

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

Solution?



Reduction to One Way Protocol

SQKD Protocol

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	

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

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

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

SQKD Protocol

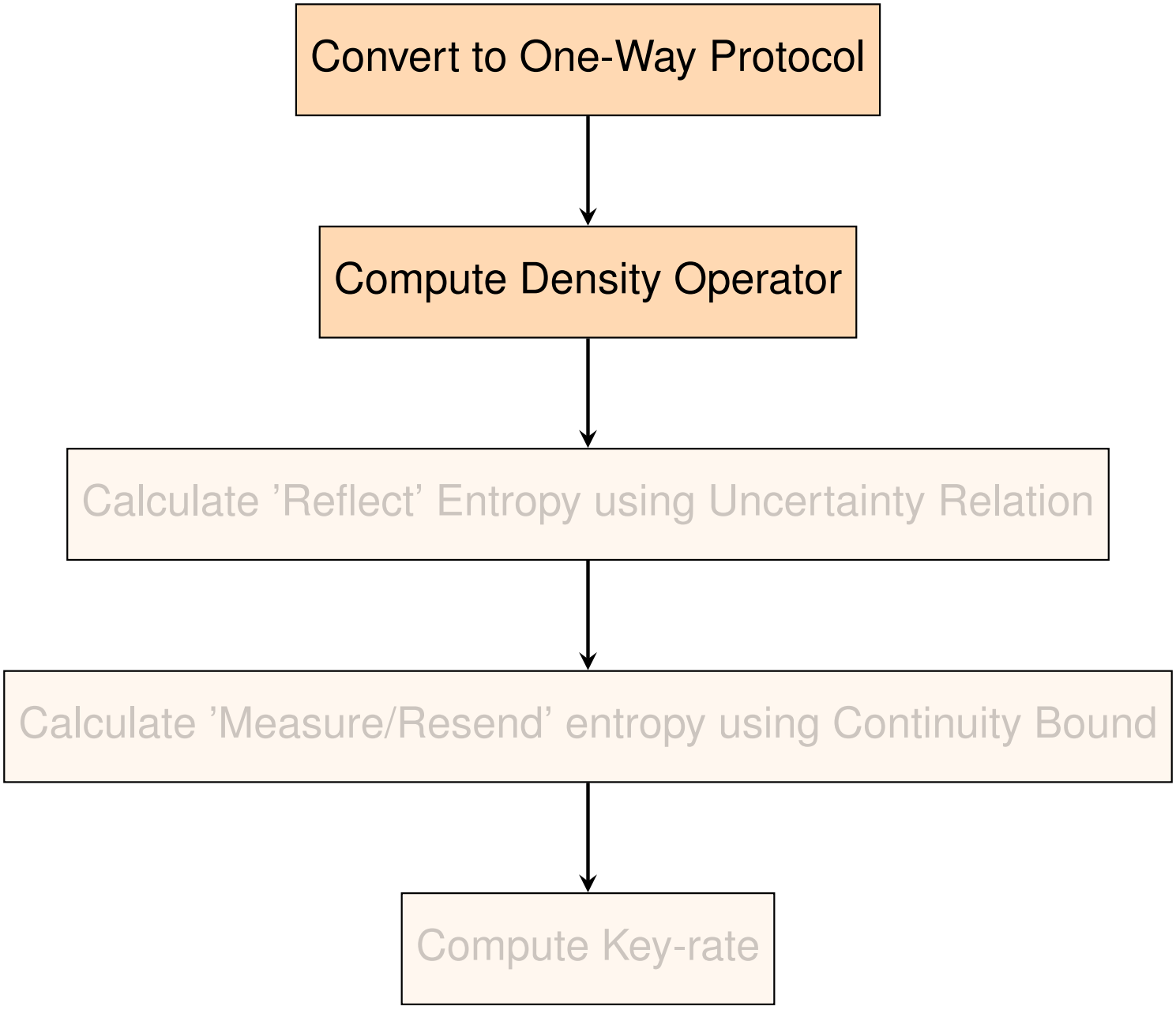
HD-SQKD	**OW-SQKD**
1. A prepares $\|z\rangle$ or $\|x\rangle$, sends to Bob	1. Bob prepares and sends $\|\phi_R\rangle$ or $\|\phi_{MR}\rangle$ if he wants to reflect or measure respectively
2. Eve attacks with U_F	2. Eve attacks with U
3. Bob measures or resends in $\mathcal{Z}$ basis	3. Alice measures 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	

$$|z\rangle \in \{|0\rangle, |1\rangle, ..., |N-1\rangle\}, |x\rangle = \mathcal{F}|z\rangle \tag{4}$$

$$|\phi_R\rangle = \sum_{b=0}^{2^n-1} \boxed{\sqrt{p(b)}} |b,b\rangle_{A_1A_2} \otimes |0\rangle_B \tag{5}$$

$$|\phi_{MR}\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)} |b,b,b\rangle_{A_1A_2B} \tag{6}$$

Now, The Sketch...



SQKD & One-Way SQKD

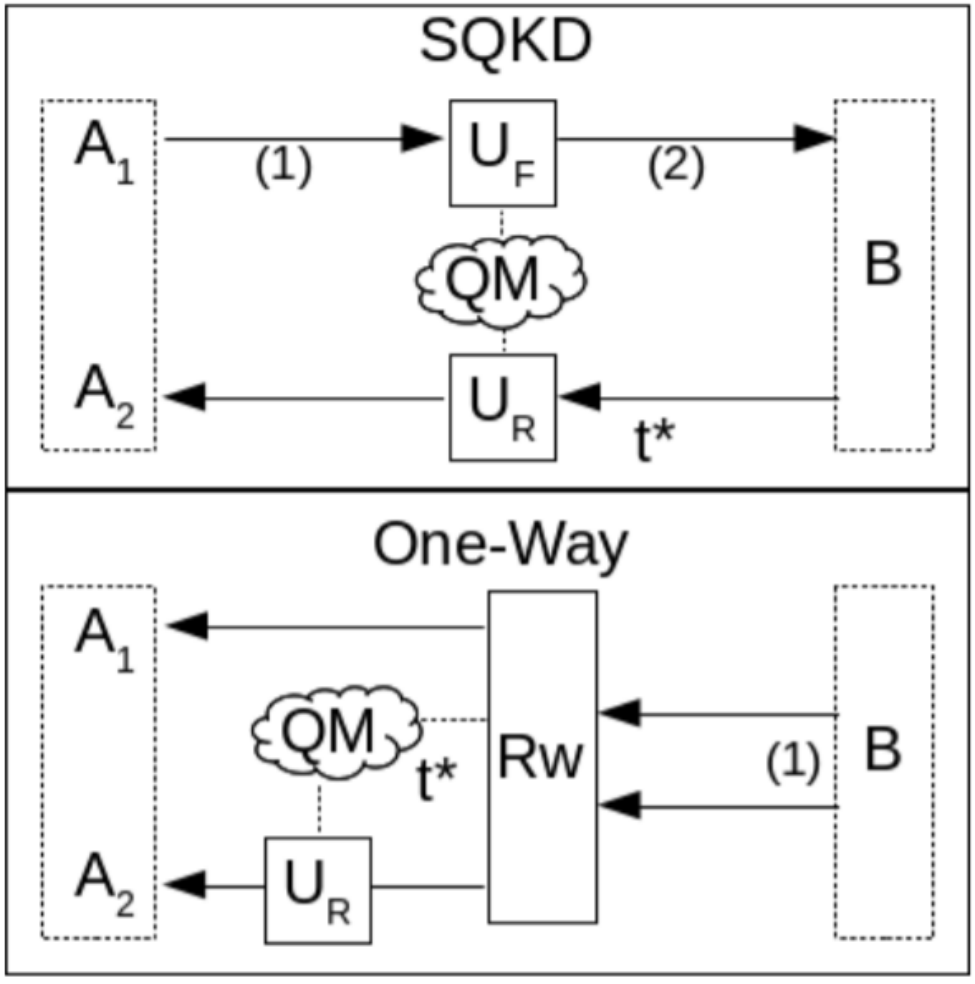


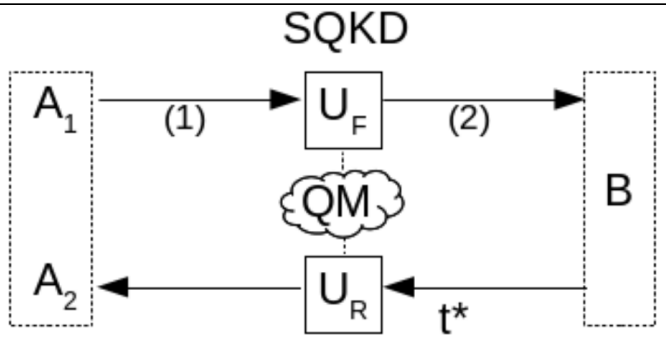
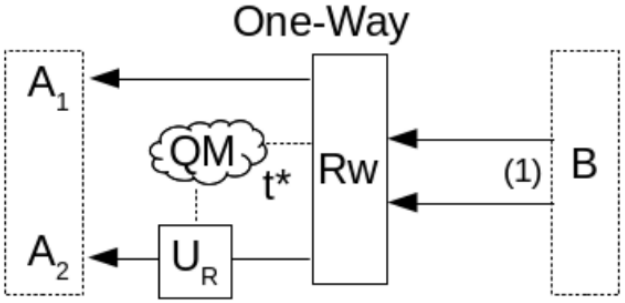
Figure 1: Two-way SQKD to One-way SQKD

The Theorem...

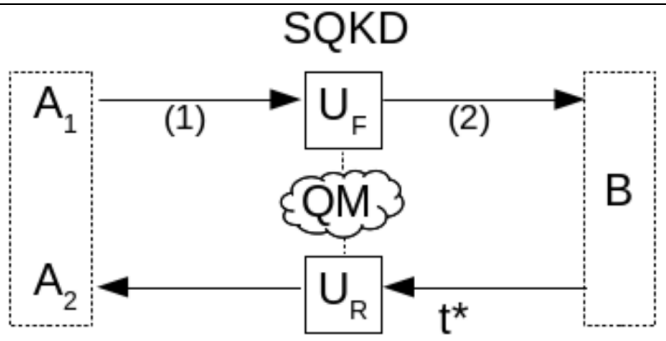
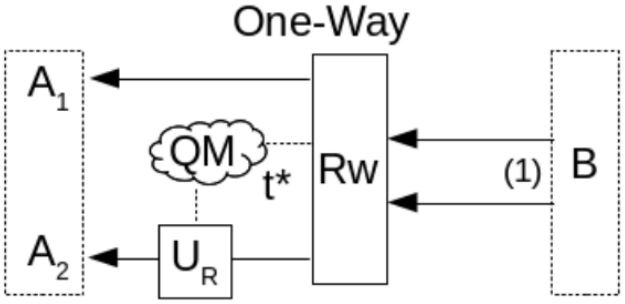
Theorem

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.

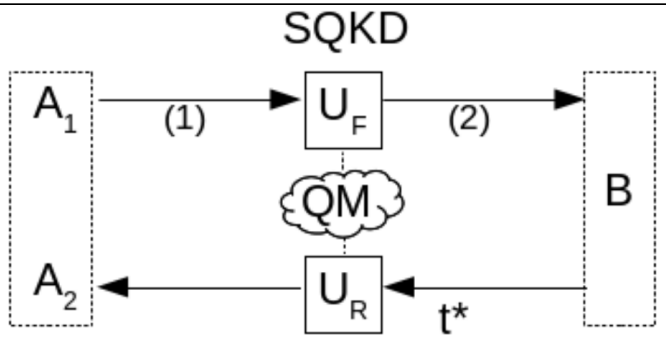
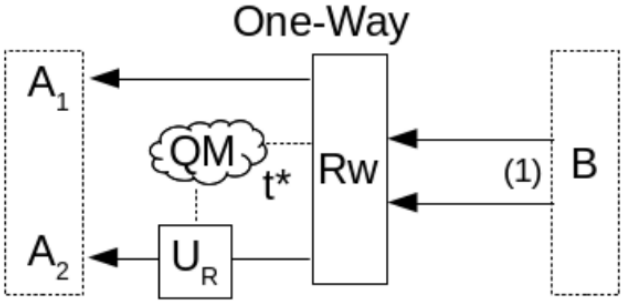
proof with table

HD-SQKD	OW-SQKD
	

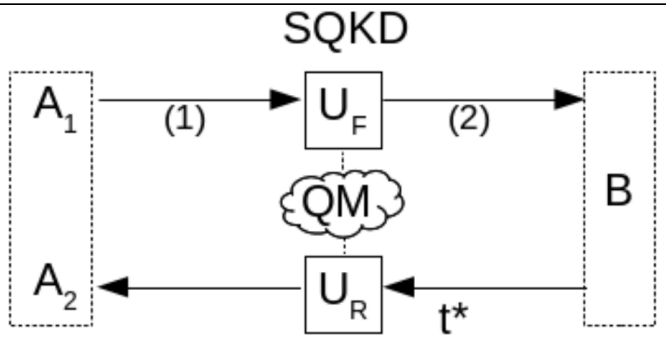
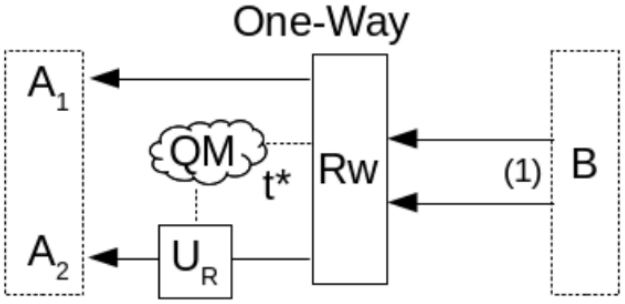
proof with table

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

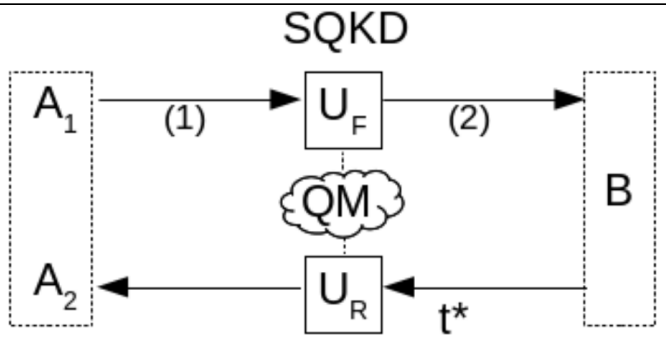
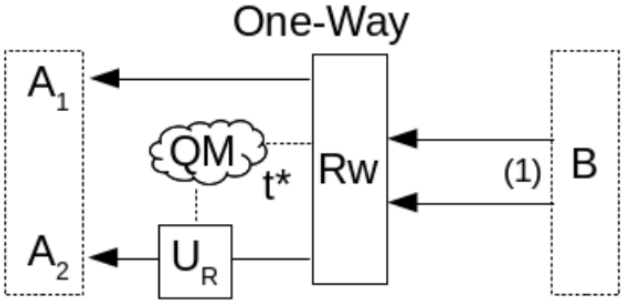
proof with table

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

proof with table

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

proof with table

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

Here Comes The...

Devetak-Winter Key Rate Equation

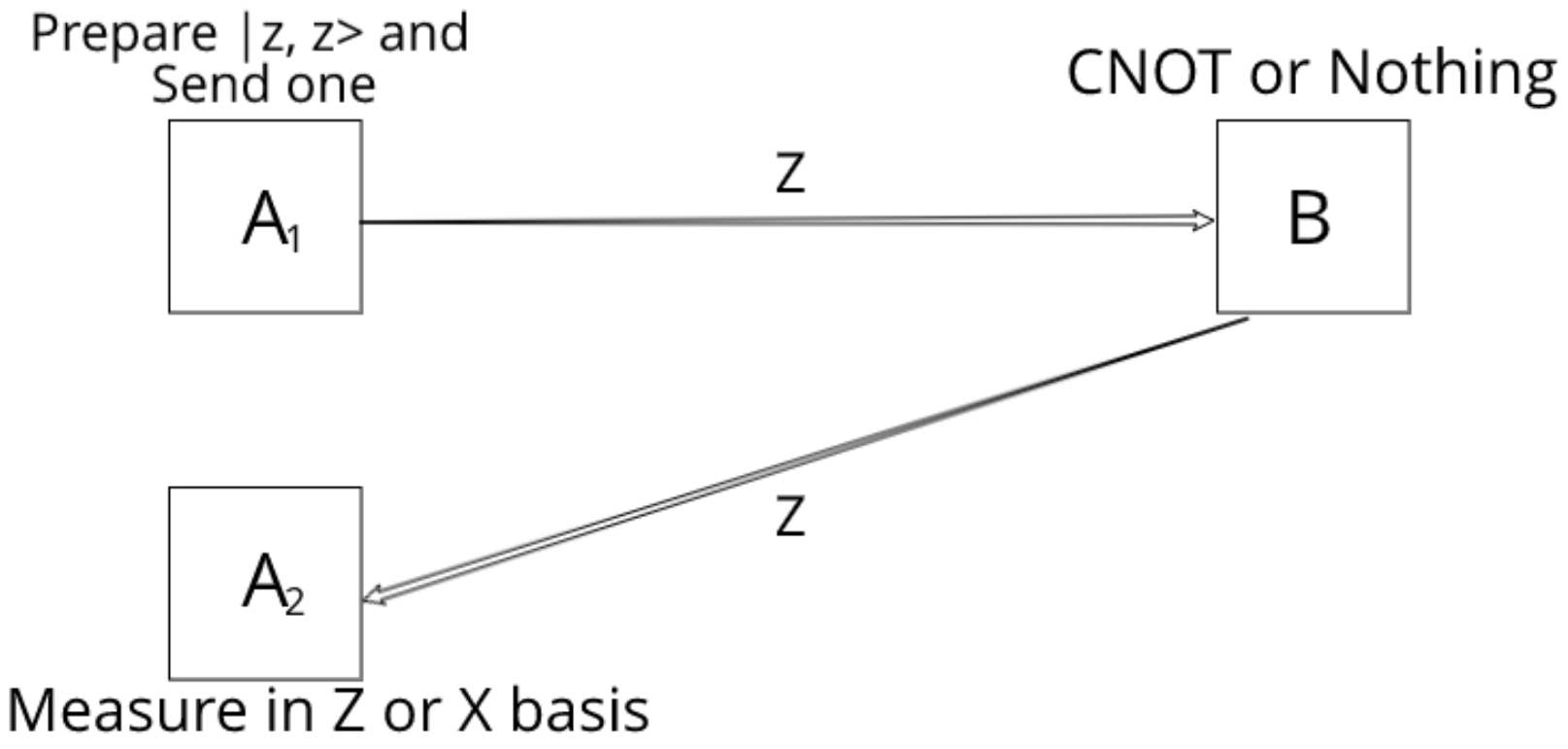
High-Dimensional SQKD (cont.)

Informal

The more Eve knows about Alice than Bob does, the less amount of key is generated.

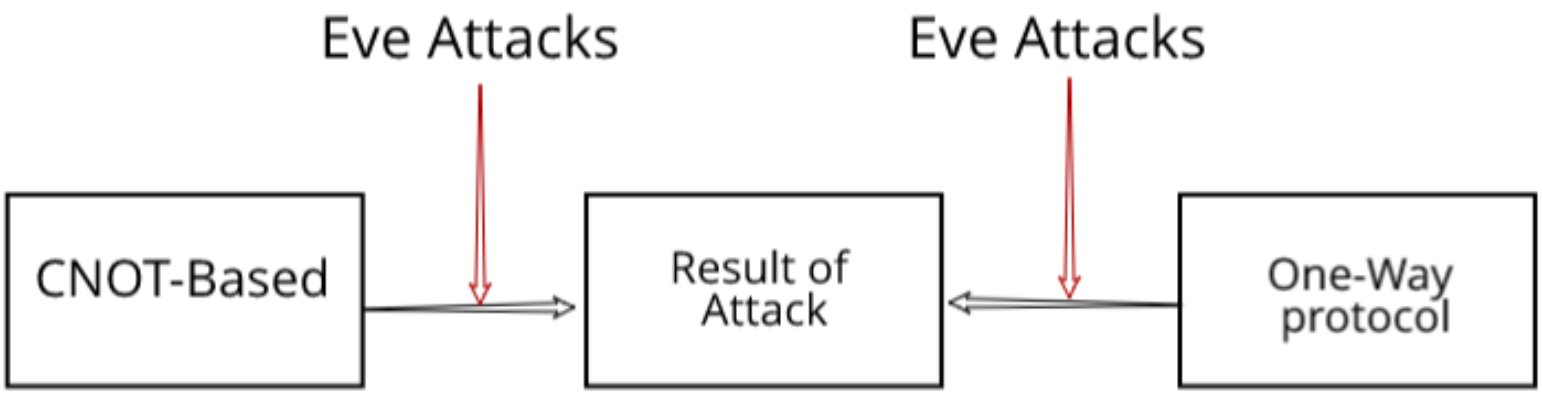
$$\text{Key Rate} = inf(H(A|E)_\rho - H(A|B)_\rho) \tag{7}$$

CNOT-Based SQKD



Reduction Sketch

SQKD = CNOT-Based

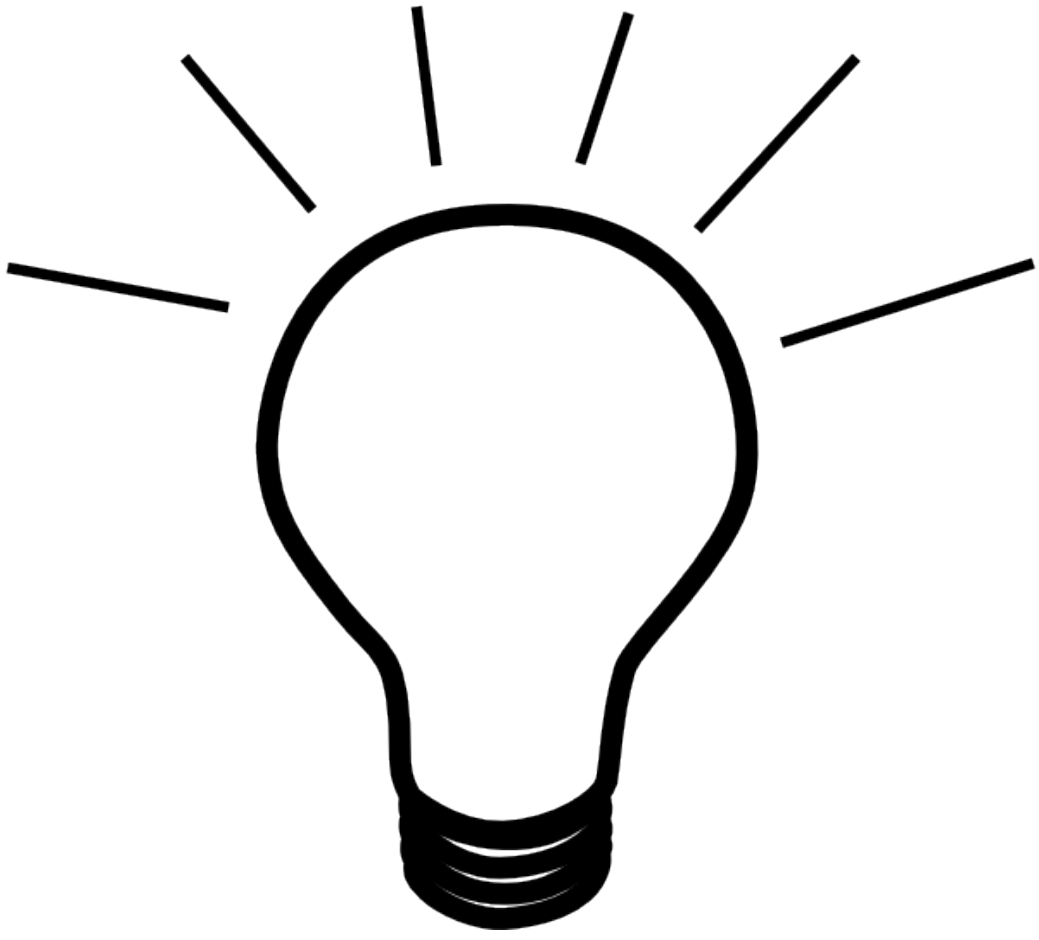


Compute Key Rate

High-Dimensional SQKD (cont.)

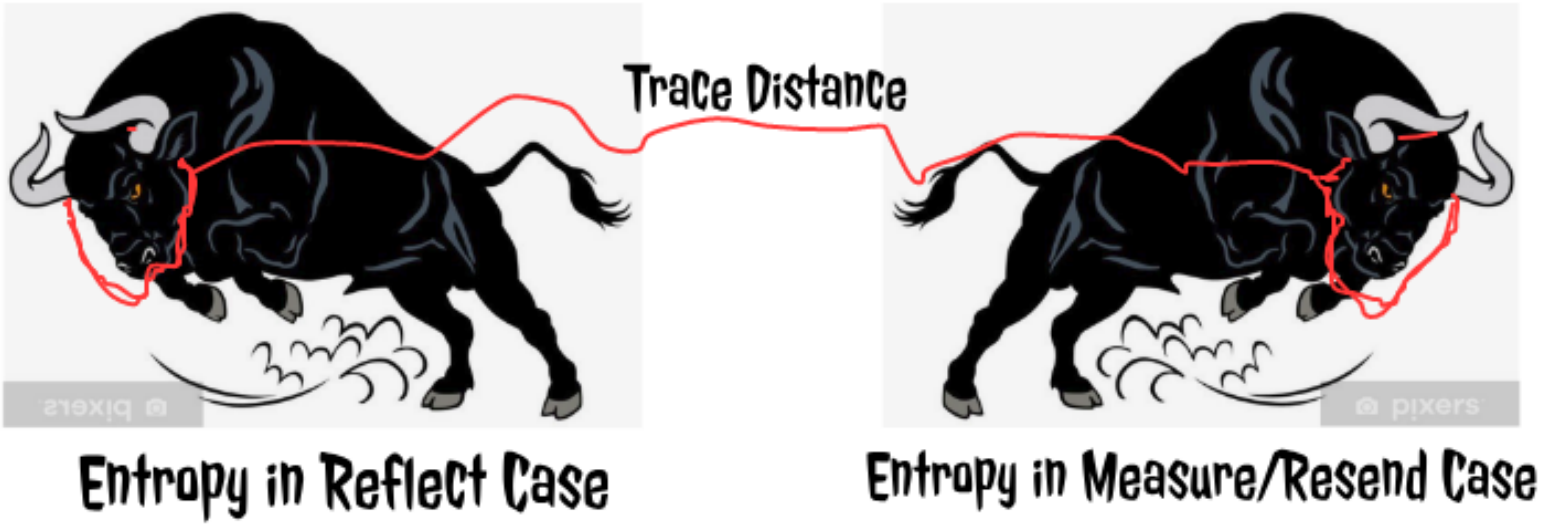
Problem: Eve doesn't tell what she knows about Alice in the Measure/Resend Case

Solution?



Winter's Continuity Bound

Winter's Continuity Bound



Winter's Continuity Bound

Informal

If two density operators are bounded by some trace distance, then the absolute difference in their conditional entropy has an upper bound.

Formal

$$|S(A|B)_\rho - S(A|B)_\sigma| \leq \epsilon \log |A| + (1+\epsilon) h(\frac{\epsilon}{1+\epsilon}) \tag{8}$$

Where,

$$\rho_{AB} = \sum_x p_x \, |x\rangle\langle x|^A \otimes \rho_x^B \tag{9}$$

and

$$\sigma_{AB} = \sum_x q_x \, |x\rangle\langle x|^A \otimes \sigma_x^B \tag{10}$$

and

$$\frac{1}{2}\|\rho - \sigma\| \leq \epsilon \tag{11}$$

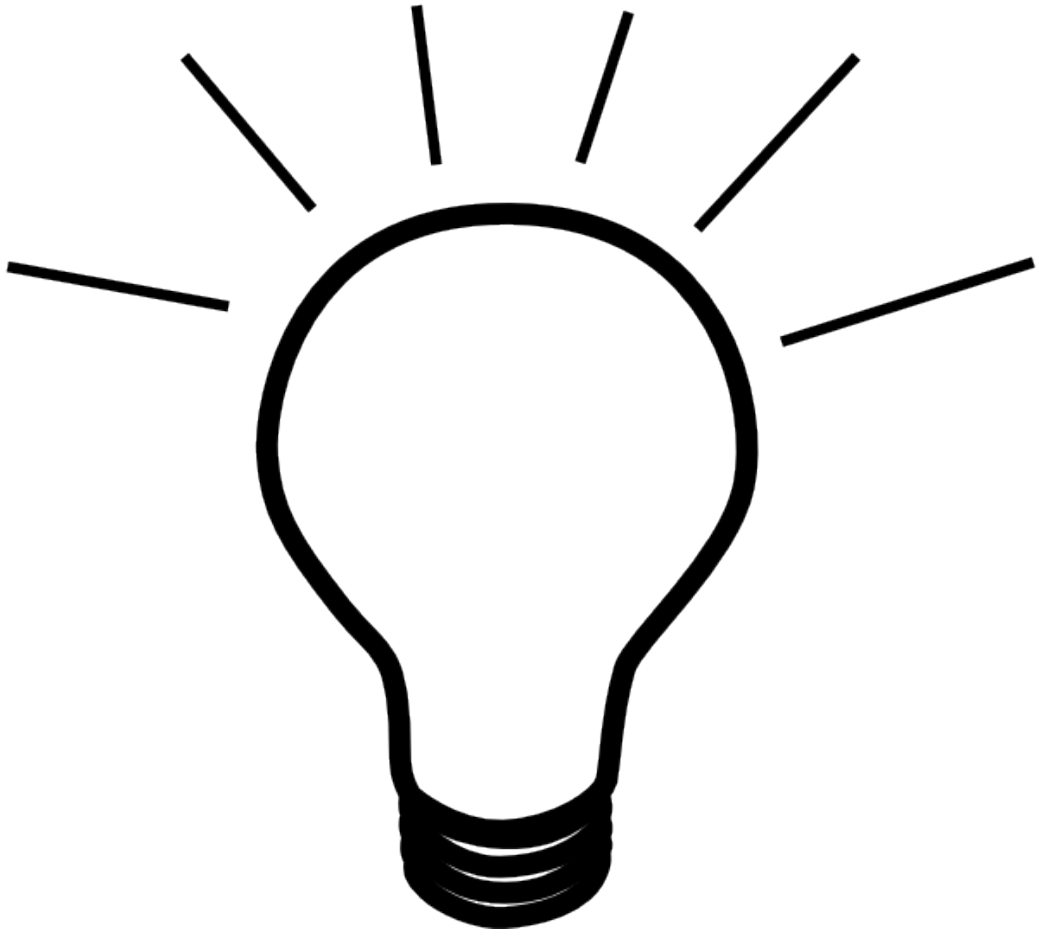
Continuity Bound in Our Case

Just apply it to bound entropy in the measure/resend case?

Continuity Bound in Our Case

Problem: Eve gives no info in Reflect case either.

Solution?



Berta’s Theorem

Berta's Theorem

Summation of the outcomes of two different measurements in a system shared by 3 people having quantum and classical memory has a lower bound

Summation of the outcomes of two different measurements in a system shared by 3 people having quantum and classical memory has a lower bound

For any density operator on a tripartite Hilbert space $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{E}}$,

$$H(R|E) + H(S|B) \geq \log_2 \frac{1}{c} \tag{12}$$

Where, R and S are two measurements, B and E are registers. c is the maximum overlap between R and S.

Is, bob's memory classical? or quantum? the original proof is for quantum memories.

Our case

$$H(R|E) + H(S|B) \geq \log_2 \frac{1}{c} \tag{13}$$

Uncertainty about the outcome of measurement R given some memory E + Uncertainty about the outcome of measurement S given quantum memory $B \geq$ c.

$$H(A_1^Z|E)_\rho + H(A_1^F|A_2)_\rho \geq n \tag{14}$$

Conditional entropy in A_1 in standard basis given Eve's memory + Conditional entropy in A_1 in Fourier basis given $A_2 \geq$ n.

Linking Seen and Unseen

Density Matrix for Reflect Case

$$\mu_{A_1^Z A_2^Z BE} = \frac{1}{N} \sum_a |a\rangle \langle a|_{A_1} \otimes \sum_c |c\rangle \langle c|_{A_2} \otimes \sum_b |b\rangle \langle b|_B \otimes |e_{a,b,c}\rangle \langle e_{a,b,c}|$$

Here,

$$p(a, b, c) = \langle e_{a,b,c} | e_{a,b,c} \rangle / N \tag{15}$$

According to the noise model we used,

$$p(a, b, c) = \frac{1}{N}(1 - Q)^2 \tag{16}$$

If $a = b = c$.

Result

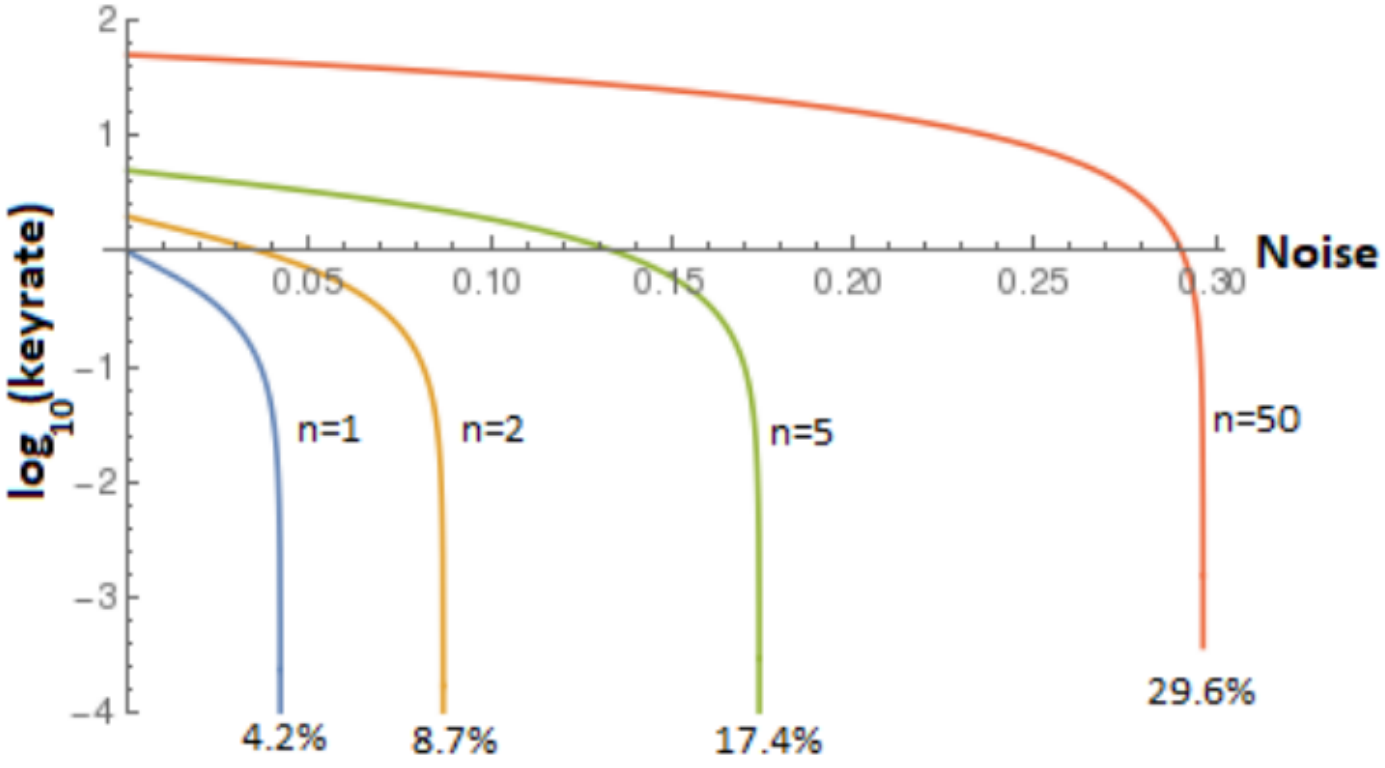
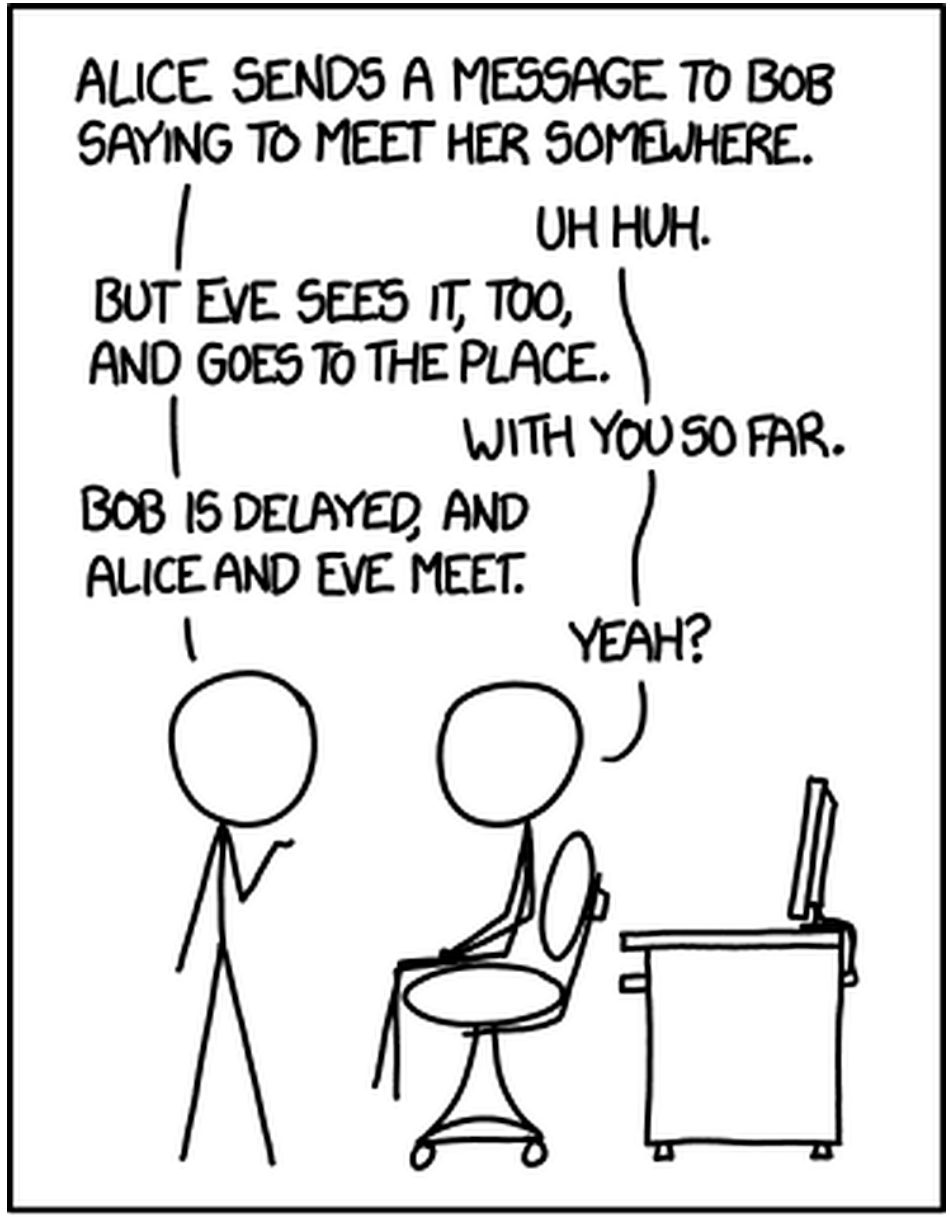
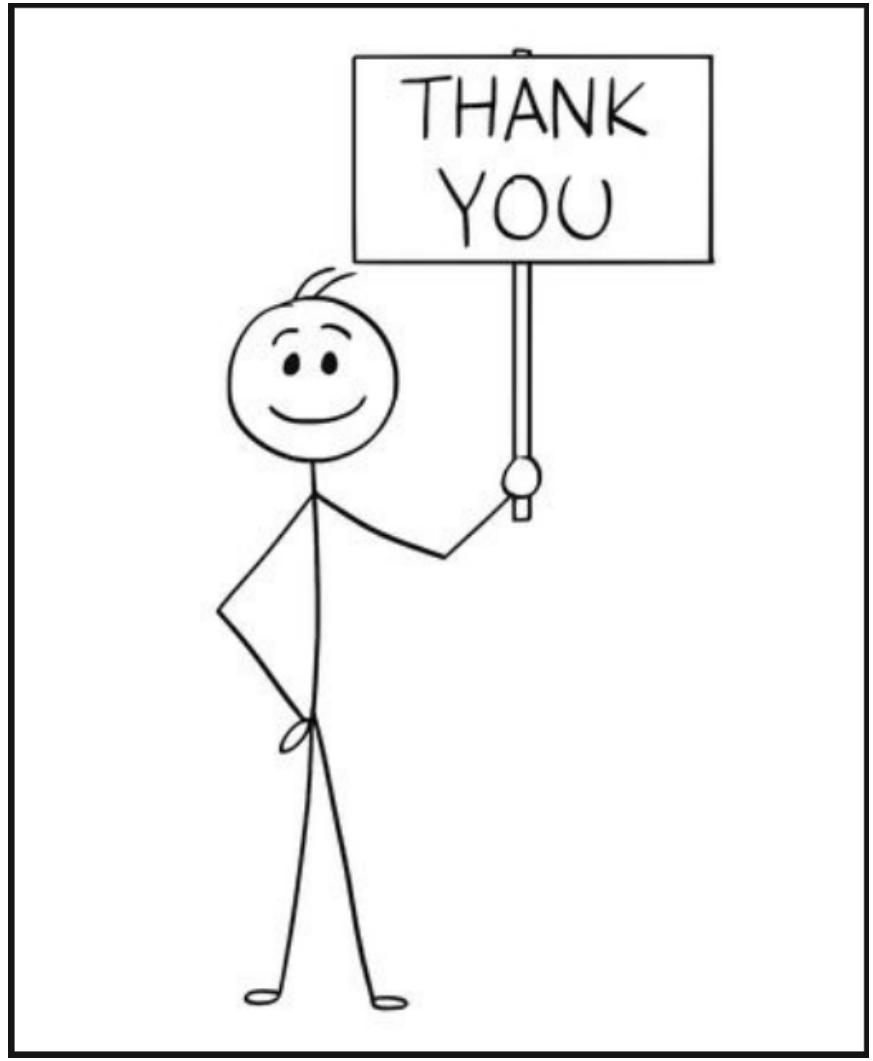


Figure 2: Key-rate of our protocol



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


THANK
YOU