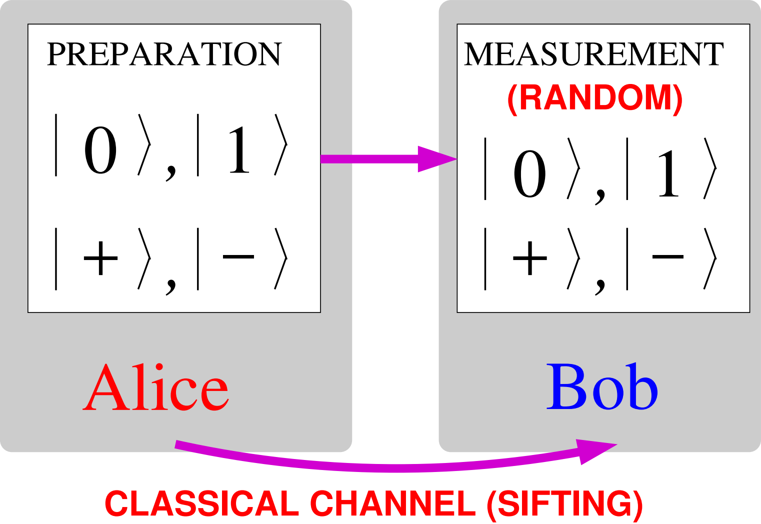
Two-Way Deterministic Communication Is Like Sending Plain Text under Quantum Protection

Mladen Pavičić
PQO, Center of Excellence CEMS, Ruđer Bošković Institute, Zagreb

NanoGroup, HU-Berlin, 7.10.16

One-Way Quantum Key Distribution: BB84

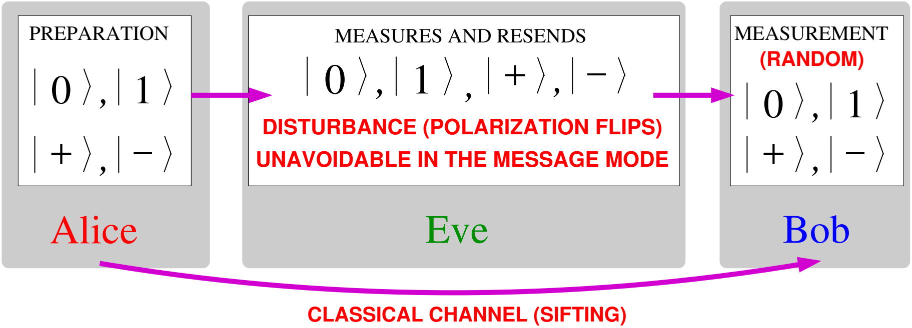


One-Way Protocol: BB84; The protocol is probabilistic.

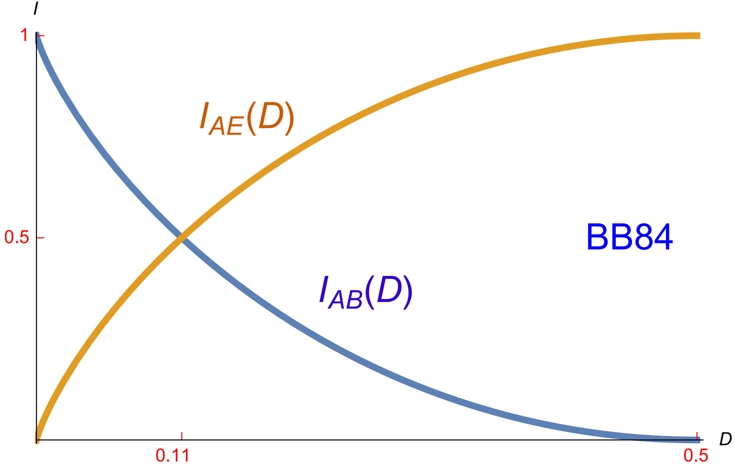
1	1	0	0	1	0	0	1	1	0	1	0	0	1	1	0
2	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxplus$	$\boxplus$	$\boxplus$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxtimes$	$\boxplus$
3		$\updownarrow$		$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$			$\updownarrow$				$\updownarrow$
4	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxtimes$	$\boxtimes$	$\boxplus$
5					$\updownarrow$			$\leftrightarrow$		$\updownarrow$	$\updownarrow$				$\updownarrow$
6	$\boxplus$		$\boxtimes$		$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxplus$		$\boxplus$	$\boxtimes$	$\boxtimes$		$\boxtimes$	$\boxplus$
7			✓		✓			✓				✓		✓	✓
8					$\updownarrow$										
9					✓									✓	
10			0					1				0			0

Table: An example of the BB84 protocol.

Attack on One-Way Protocol: BB84



Mutual Information: BB84



$$
\begin{aligned}
I_{AB} &= 1 + x\log_2 x + (1-x)\log_2(1-x), \\
I_{AE} &= -x\log_2 x - (1-x)\log_2(1-x)
\end{aligned}
$$

Two-Way Entangled Photon Protocols—Bell States
Deterministic Protocols

Bell states:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle \pm |V\rangle|H\rangle), \quad |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle),$$

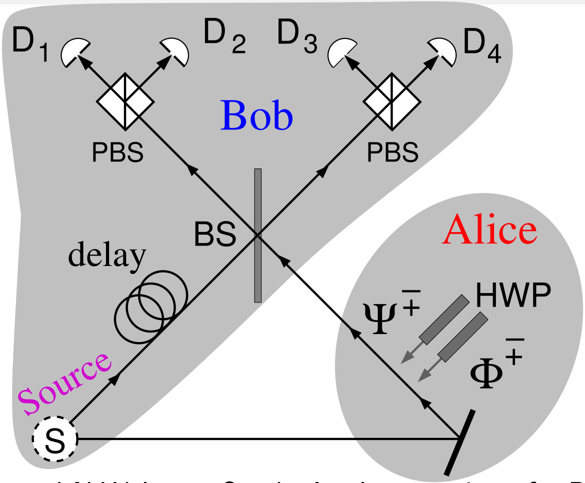
Two Bell states, $|\Psi^{\pm}\rangle$—*ping-pong protocol*.

Kim Boström and Timo Felbinger,
Deterministic Secure Direct Communication Using Entanglement,
Phys. Rev. Lett., **89**, 187902 (2002).
On the Security of the Ping-Pong Protocol, *Phys. Lett. A*, **372**, 3953 (2008).

All four Bell States:

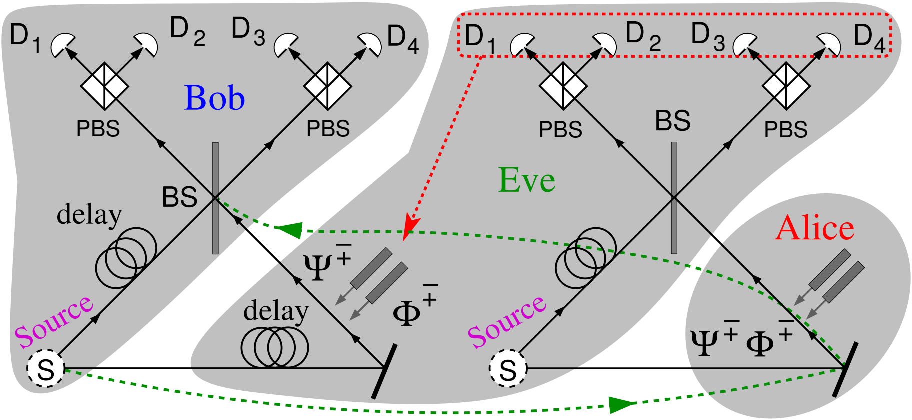
Quing-yu Cai and Ban-wen Li,
Improving the Capacity of the Boström–Felbinger Protocol,
Phys. Rev. A, **69**, 054301 (2004).

Bell State Deterministic Direct Communication Protocol



M.Ostermeyer and N.Walenta, On the Implementation of a Deterministic Secure Coding Protocol Using Polarization Entangled Photons, *Opt. Commun.*, **281**, 4540 (2008).

Attack on a Bell State Protocol



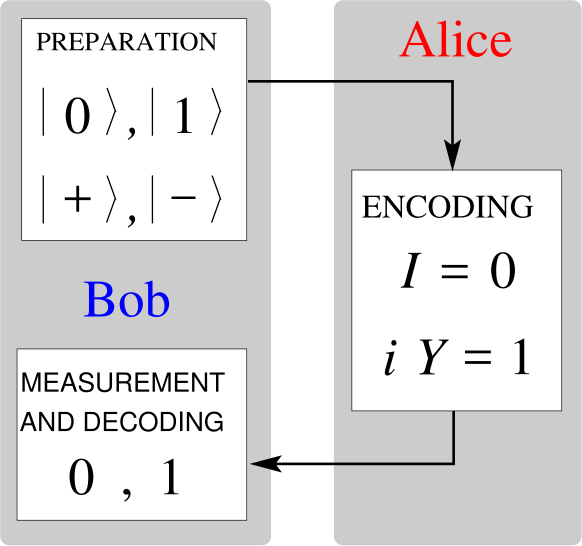
Attack on One Photon Deterministic Two-Way Protocol

Marco Lucamarini and Stefano Mancini,
Secure Deterministic Communication without Entanglement,
Phys. Rev. Lett., **94**, 140501 (2005).

A. Cerè, M. Lucamarini, G. Di Giuseppe and P. Tombesi,
Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise,
Phys. Rev. Lett., **96**, 200501 (2006).

R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini and P. Tombesi,
Two-Way Quantum Key Distribution at Telecommunication Wavelength,
Phys. Rev. A, **77**, 022304 (2008).

One Photon Deterministic Direct Communication Protocol

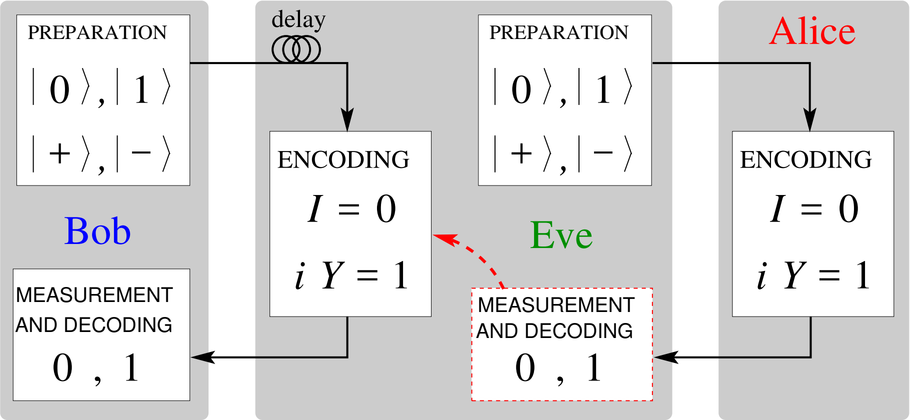


$\boldsymbol{I}$ leaves the qubit unchanged; encodes $\mathbf{0}$;

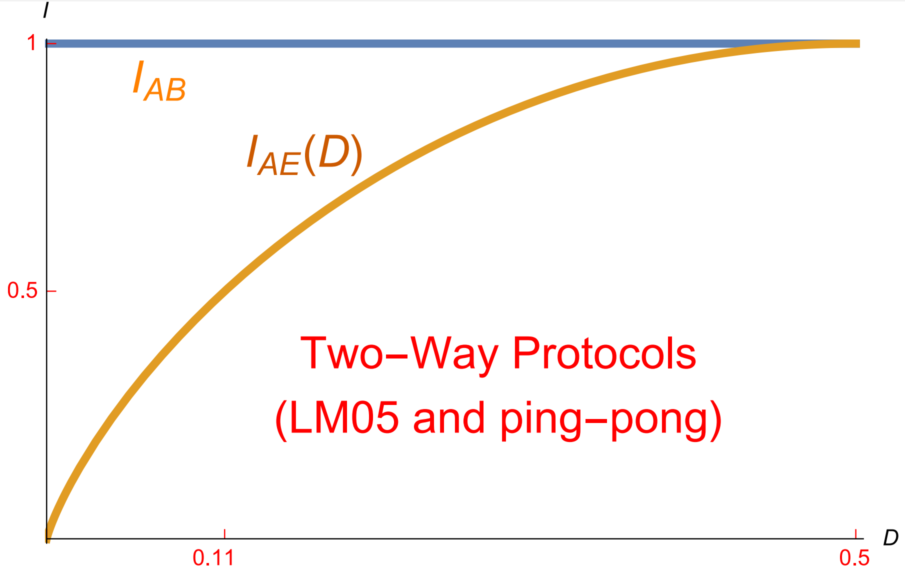
$i\boldsymbol{Y} = \boldsymbol{ZX}$ (Pauli operators), flips the qubit state; encodes $\mathbf{1}$:

$i\boldsymbol{Y}|0\rangle = -|1\rangle$,
$i\boldsymbol{Y}|1\rangle = |0\rangle$,
$i\boldsymbol{Y}|+\rangle = |-\rangle$,
$i\boldsymbol{Y}|-\rangle = -|+\rangle$.

Attack on One Photon Deterministic Two-Way Protocol



2-Way Deterministic Protocols: Like Sending Plain Text



Is LM05 Secure?

BB84: security of the protocol and critical disturbance (D, QBER) via secret fraction

$$r = \lim_{N\to\infty} \frac{l}{n} = I_{AB} - I_{AE}$$

l—length of the final key; n—length of the raw key

H. Lu, C.-H. F. Fung, X. Ma and Q.-y. Cai,
Unconditional Security Proof of a Deterministic Quantum Key Distribution with a Two-Way Quantum Channel,
Phys. Rev. A, **84**, 042344 (2011).

Quantum protection of plain text sending: Control Mode. Does it work?

Proof of Unconditional Security Does not Work

"Eve's most general attack in the Bob-Alice channel:

$$\begin{aligned} U_{BE}|0\rangle_B|E\rangle &= c_{00}|0\rangle_B|E_{00}\rangle + c_{01}|1\rangle_B|E_{01}\rangle, \ldots \\ U_{BE}|+\rangle_B|E\rangle &= c_{++}|+\rangle_B|E_{++}\rangle + c_{+-}|-\rangle_B|E_{+-}\rangle, \ldots \text{"} \end{aligned}$$

"After verifying $c_{++}^2 - c_{01}^2 \geq 1/2$, Alice and Bob get the [secret fraction] against collective attacks,

$$r = 1 - h(\xi),$$

where $\xi = c_{++}^2 - c_{01}^2$ and $h(\xi) = -\xi \log_2 \xi - (1-\xi)\log_2(1-\xi)$ is the binary Shannon entropy."

However, with our attack, we have $c_{++} = 1$ and $c_{01} = 0$. This yields: $\xi = 1$ and $r = 1$. There is no critical disturbance: $I_{AE} \leq I_{AB}$.

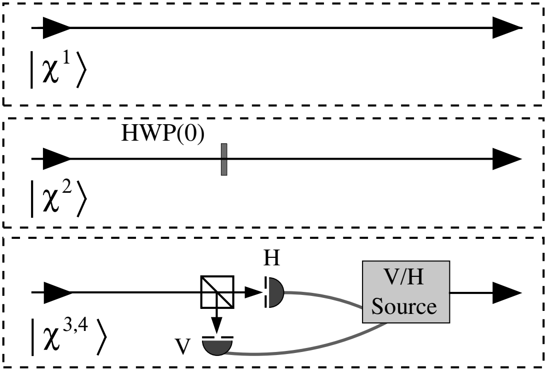
List of Two-Way Deterministic Protocol Properties

	BB84	pp	LM05
type	probabilistic	deterministic	deterministic
mode(s)	message (MM)	message (MM) + control (CM)	message (MM) + control (CM)
security	QBER of MM	QBER of CM	QBER of CM
secure	for QBER $< 11\%$	no/unknown	no/unknown
disturbance	$0 \leq D \leq 0.5$ in MM	$D = 0$ in MM, $0 \leq D \leq 0.5$ in CM	$D = 0$ in MM, $0 \leq D \leq 0.5$ in CM
critical disturbance	$D = 0.11$	indeterminable — dependent on inherent QBER of the system	indeterminable — dependent on inherent QBER of the system
mutual information	$I_{AB} = 1 + D\log_2 D + (1-D)\log_2(1-D)$, $I_{AE} = -D\log_2 D - (1-D)\log_2(1-D)$	$I_{AB} = 1$, $0 \leq I_{AE} \leq 1$	$I_{AB} = 1$, $0 \leq I_{AE} \leq 1$
photon distance	L	$4L$	$2L$
trans-mittance	$\mathcal{T}$	$\mathcal{T}^4$	$\mathcal{T}^2$

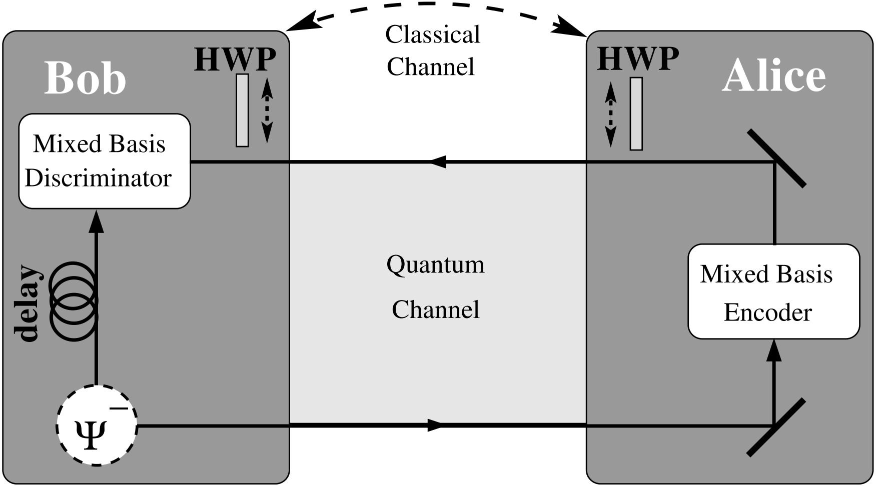
A Two-Way Probabilistic Protocol is However Possible

M. Pavičić, O. Benson, A. W. Schell, and J. Wolters, Mixed basis quantum key distribution with linear optics, [Submitted, Sep. 2016].

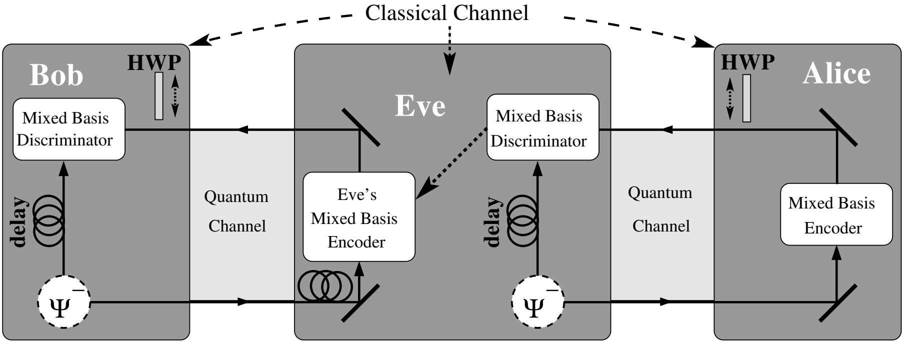
Two Bell states $|\chi^{1,2}\rangle = |\Psi^{\mp}\rangle$ + two computational basis states $|\chi^3\rangle = |H\rangle_1|H\rangle_2, \ |\chi^4\rangle = |V\rangle_1|V\rangle_2$



Mixed Basis Two-Way Protocol



Attack on the Mixed Basis Two-Way Protocol



After sifting: $I_{AEs} = 0.875$, $I_{ABs} = 0.774$.
After after error correction: $I_{AEc} = 1.54$, $I_{ABs} = 1.93$.

Thank You for Your Attention