Poster on XI International Conference on Quantum Optics in Minsk, Belarus, May 26–31, 2006

Faked states attack exploiting detector efficiency mismatch on BB84, phase-time, DPSK, and Ekert protocols

***Vadim Makarov*[1,2], *Johannes Skaar*[1], *and Andrey Anisimov*[2]**

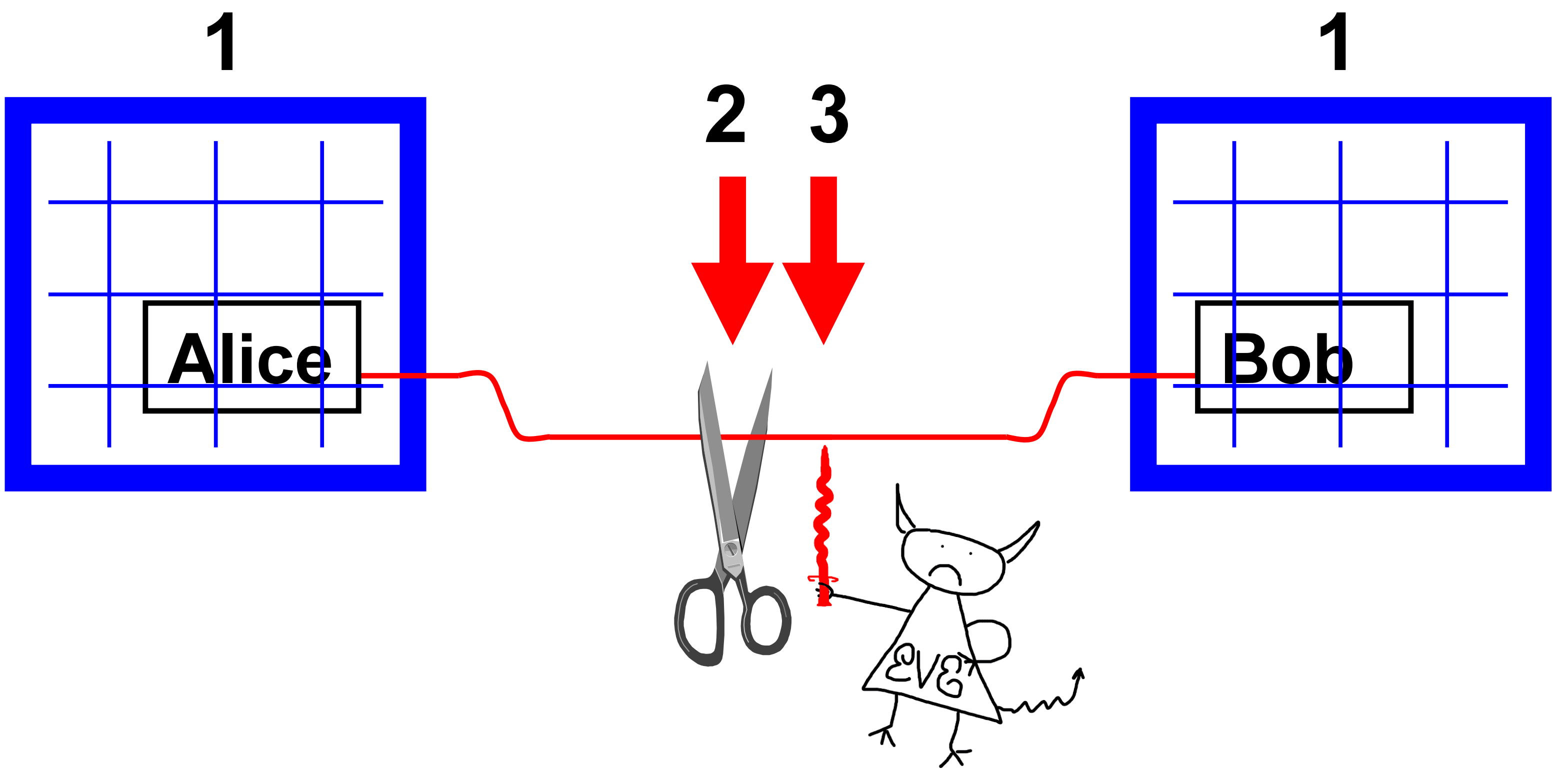
[1]Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

[2]Radiophysics Department, St. Petersburg State Polytechnic University, Politechnicheskaya street 29, 195251 St. Petersburg, Russia

NTNU
Norwegian University of Science and Technology

SPbSPU
St. Petersburg State Polytechnic University

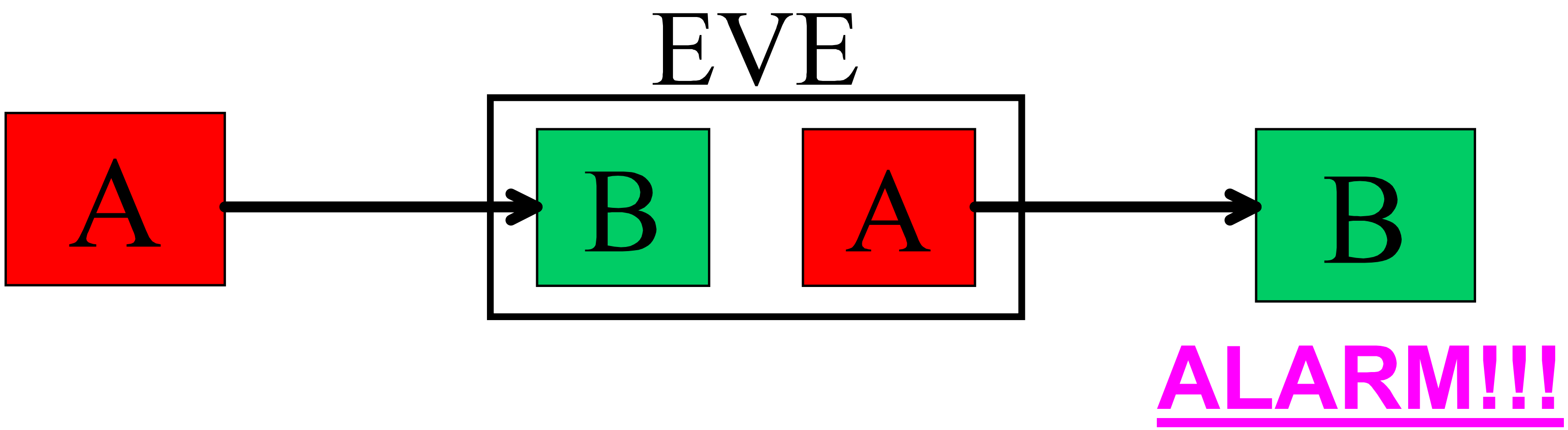
Quantum key distribution: components of security



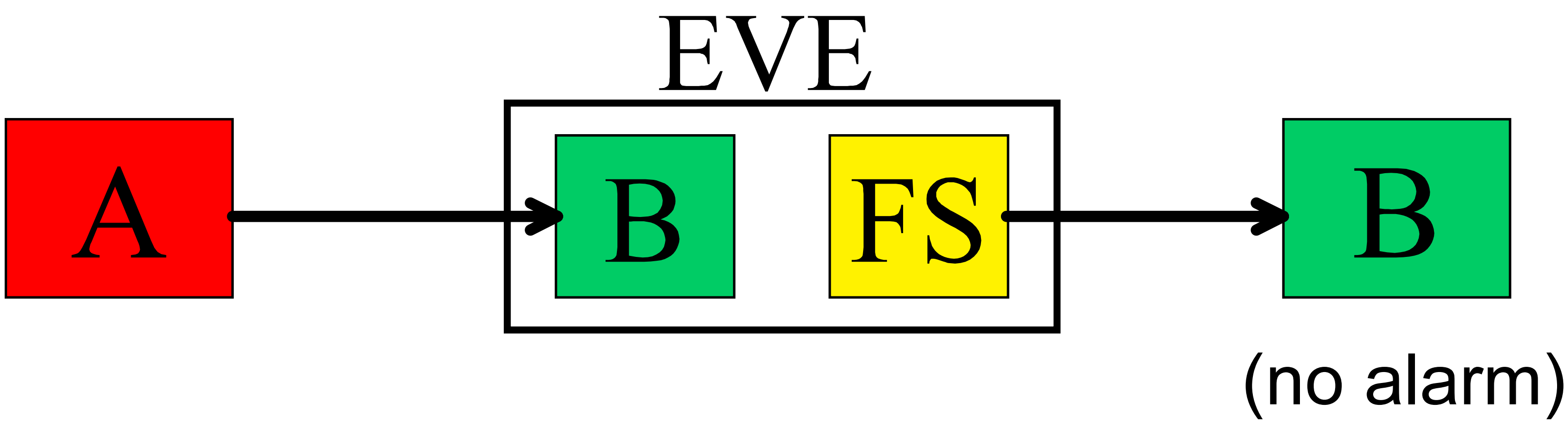
1. Conventional security; trusted equipment manufacturer
2. Security against quantum attacks
3. Loopholes in optical scheme
   – attacks that don't deal with quantum states, but use loopholes and imperfections in implementation

Faked states attack

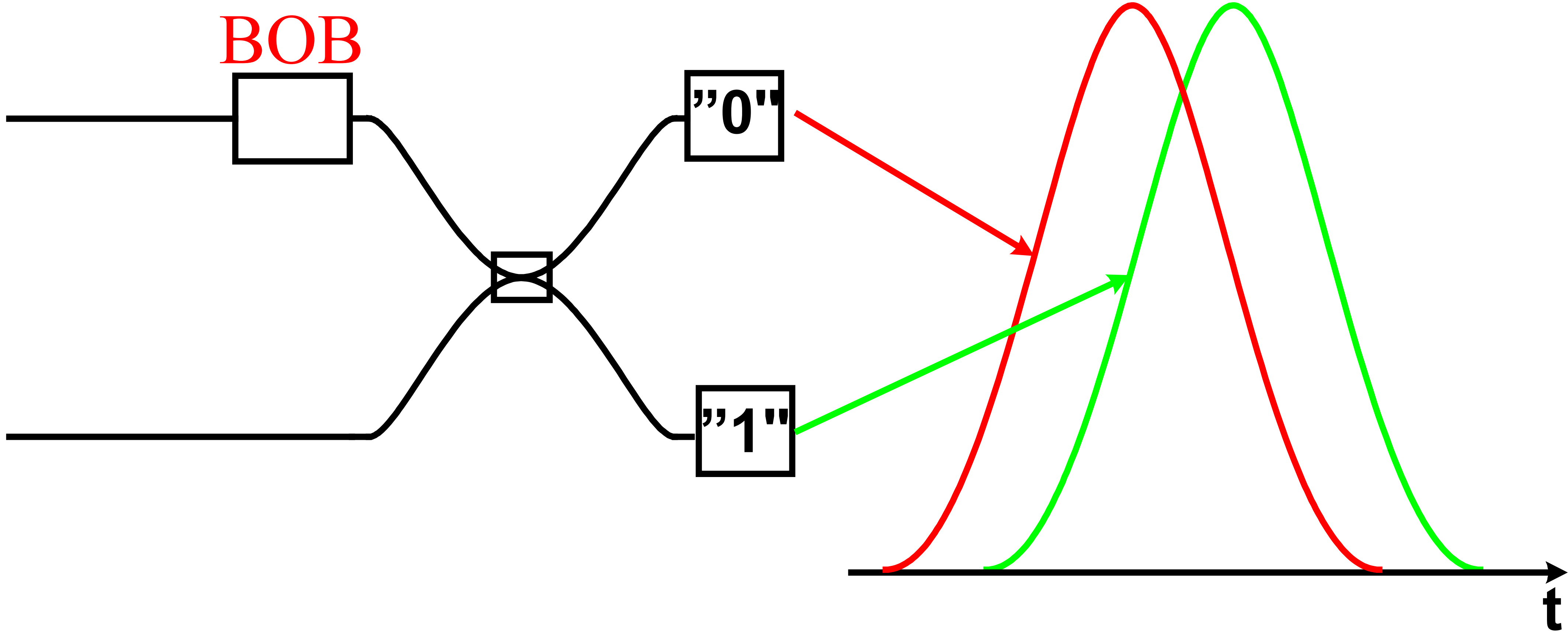
Conventional intercept/resend:



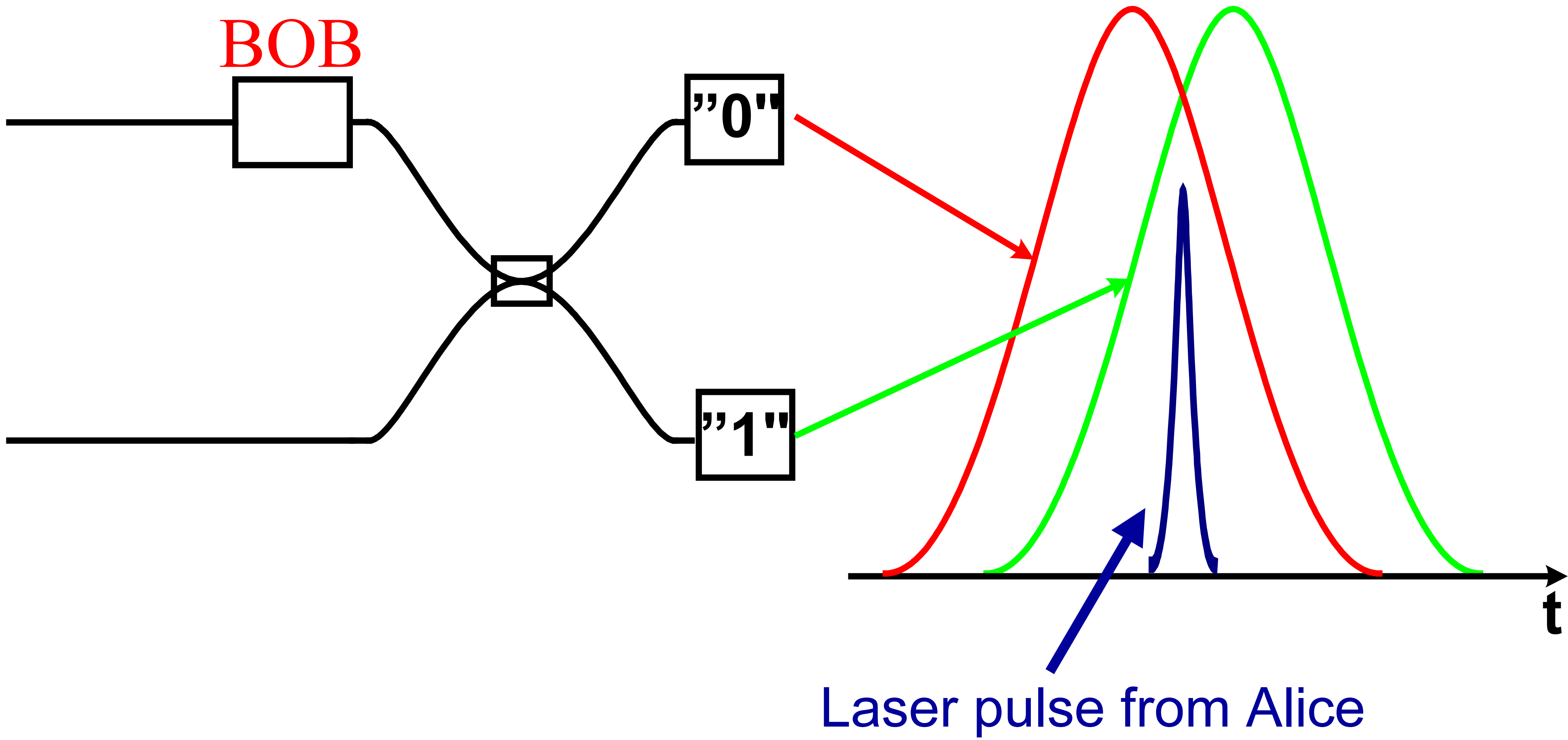
Faked states attack:



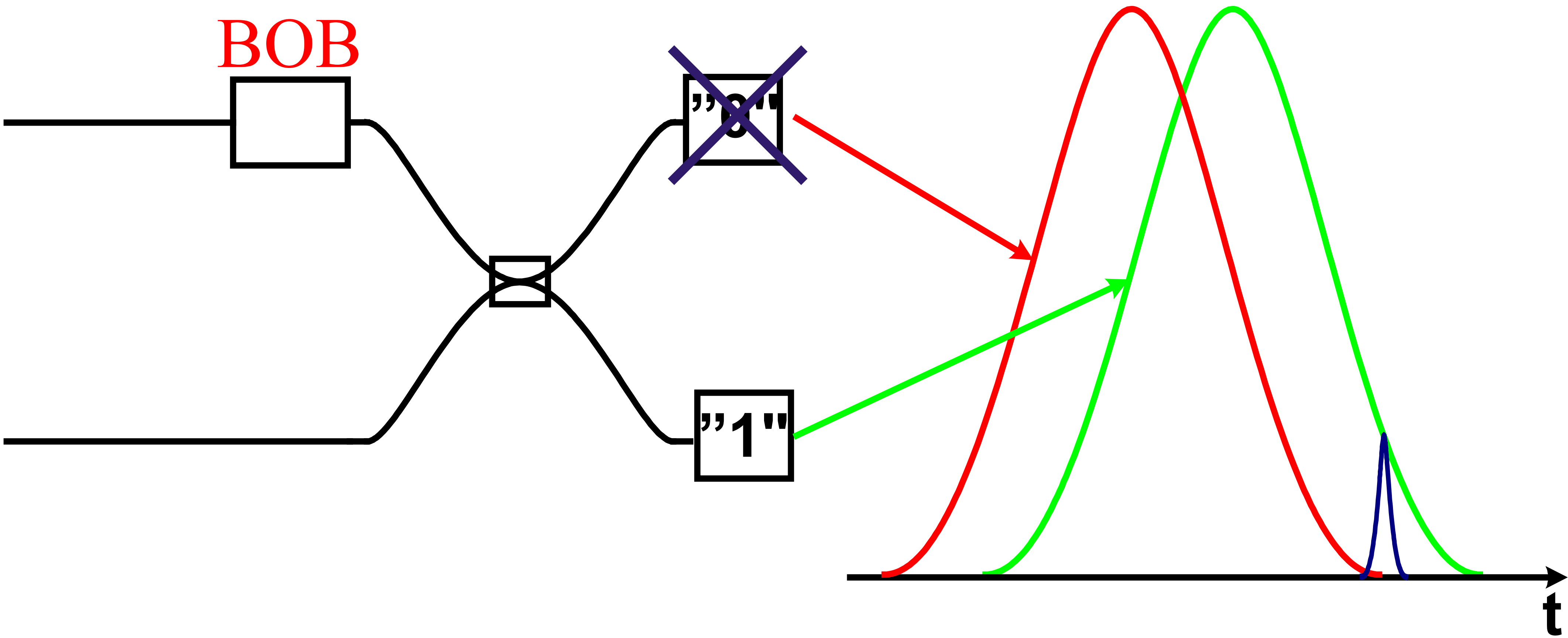
Exploiting common imperfection: detector gate misalignment



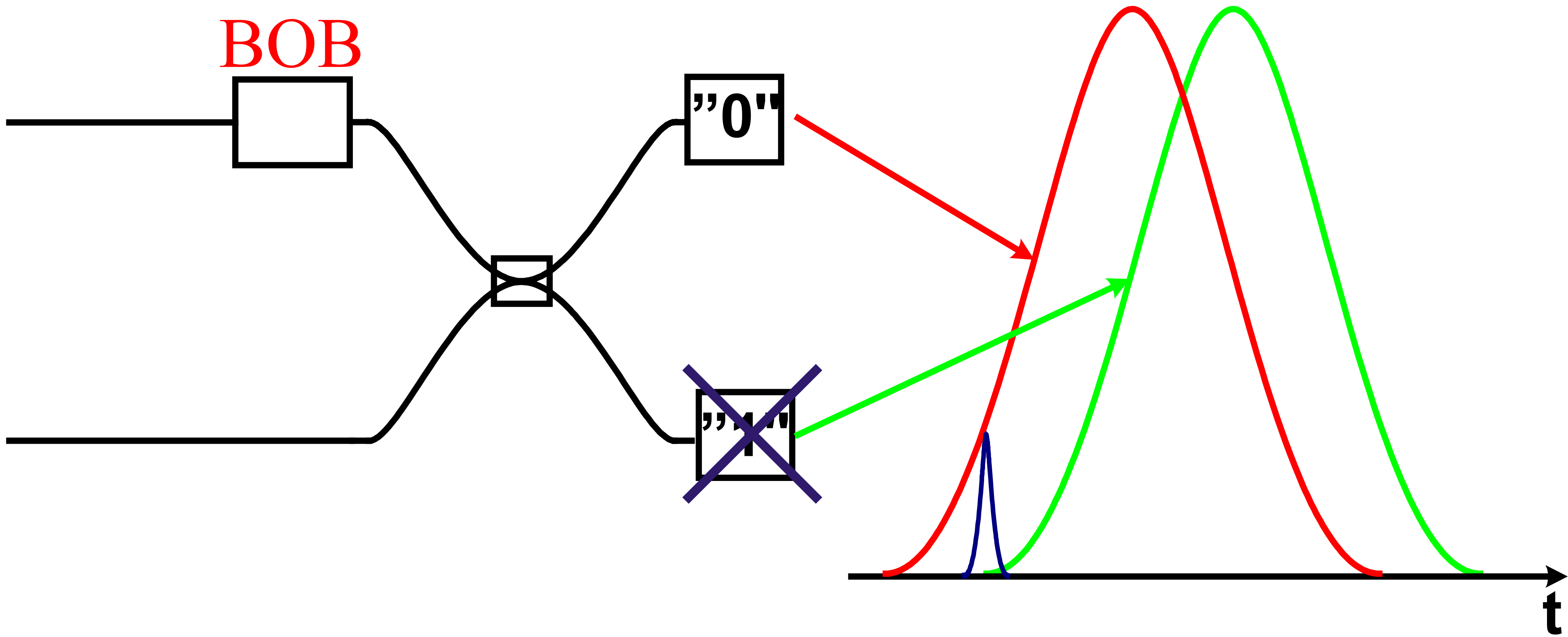
Detector gate misalignment



Detector gate misalignment

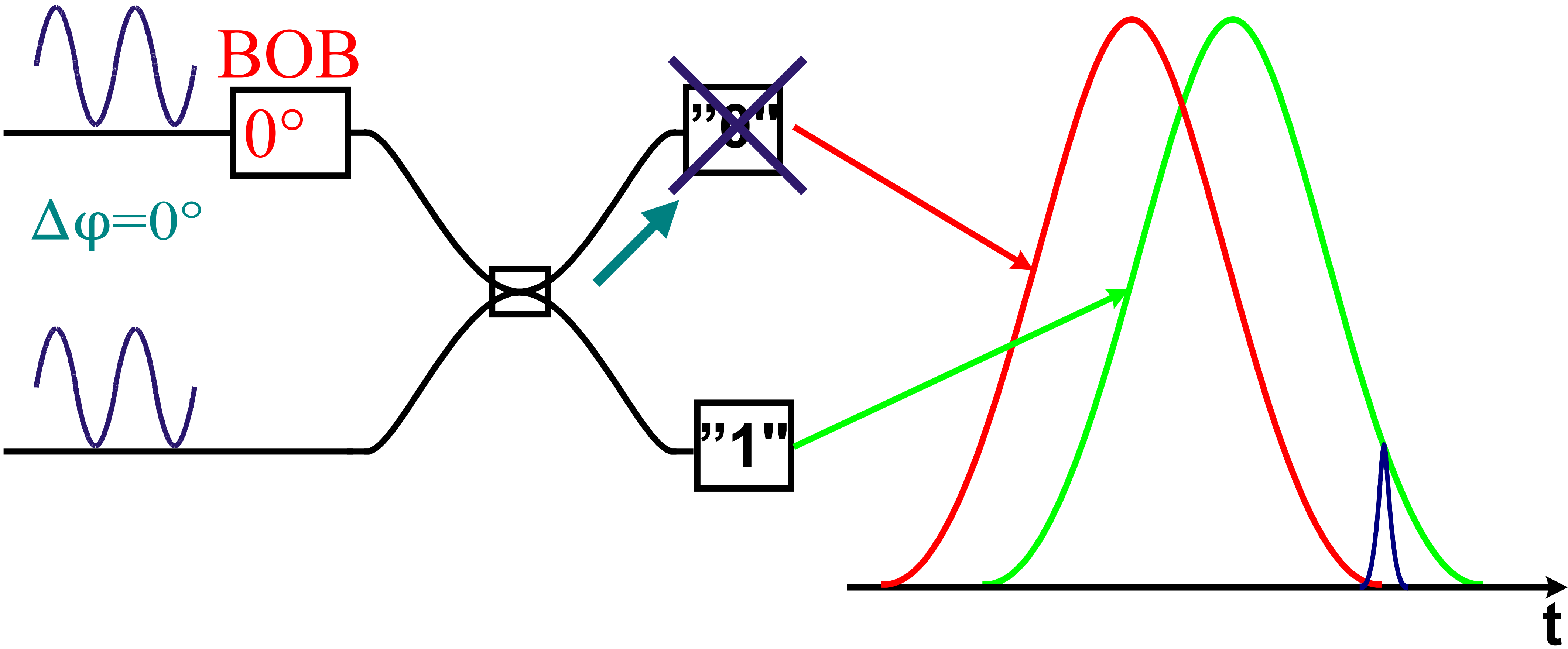


Detector gate misalignment



Detector gate misalignment

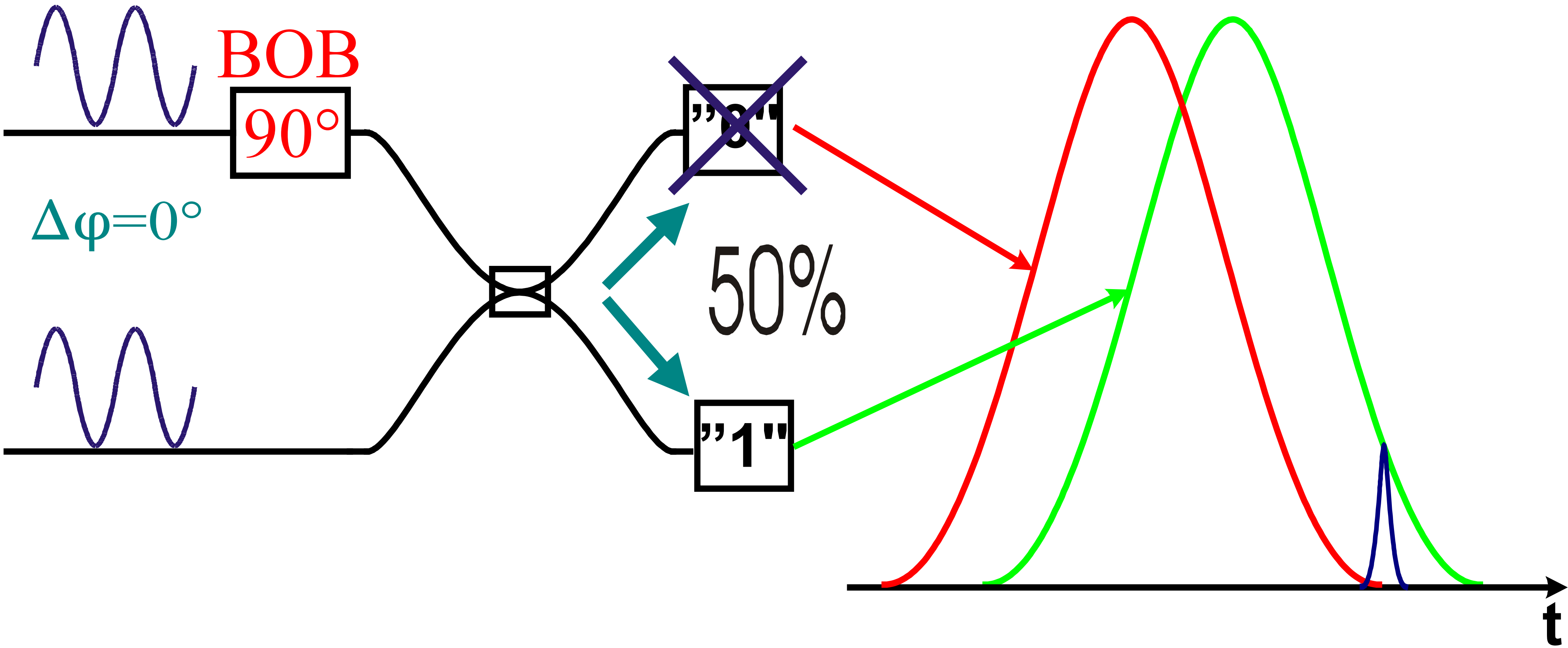
Example: Eve measured with basis Z (90°), obtained bit “1”



(Eve resends opposite bit “0” in opposite basis (X), shifted in time)

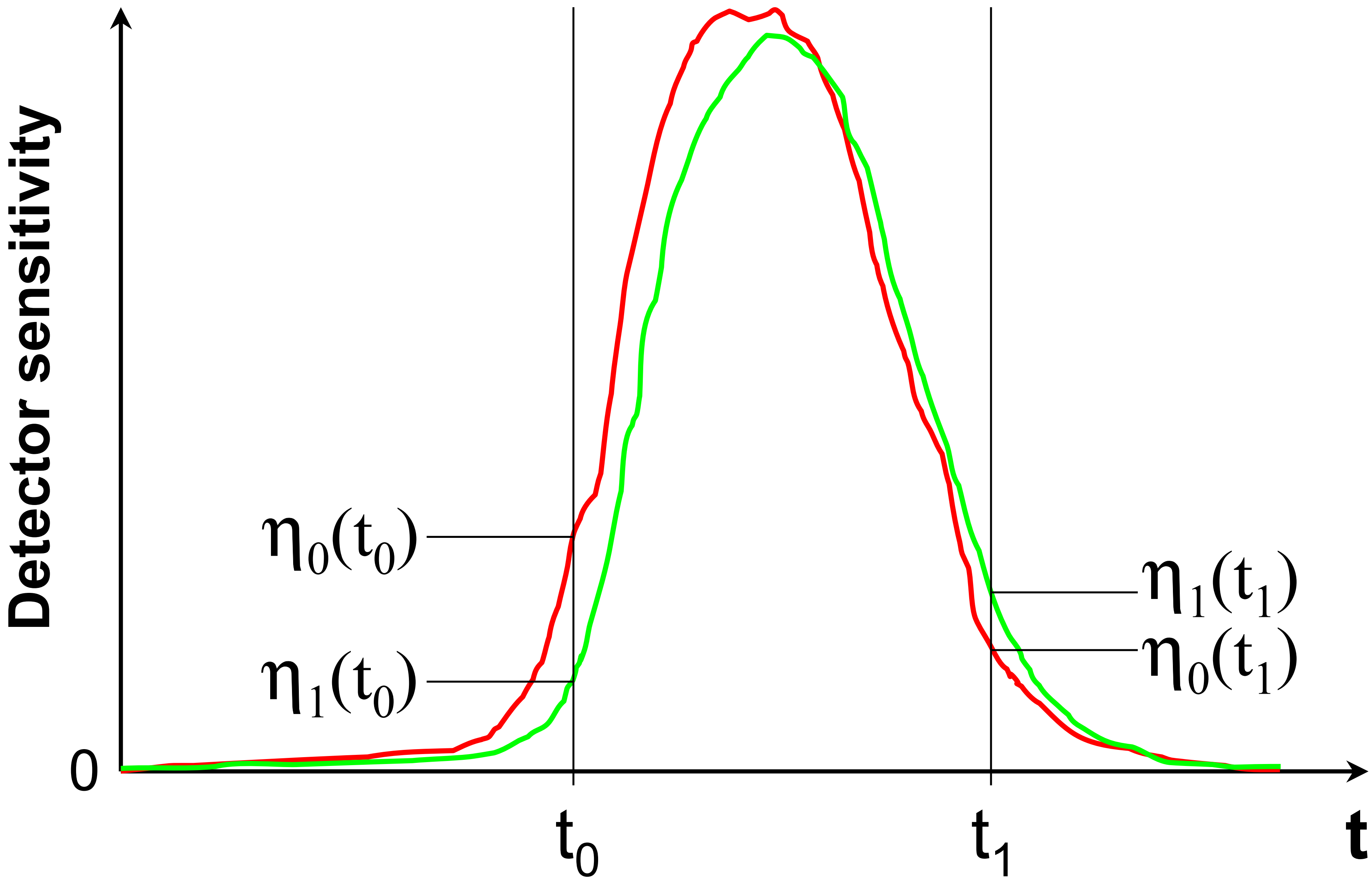
Detector gate misalignment

Example: Eve measured with basis Z (90°), obtained bit “1”



- ✓ Eve’s attack is not detected
- ✓ Eve obtains 100% information of the key

Partial sensitivity mismatch



A. Practical intercept-resend attack

Alice	→Eve	Eve→	Bob		Probability	Sifting
Z0	Z0	X1t_0	Z	0,	$\frac{1}{2}\eta_0(t_0)$	keep
				1,	$\frac{1}{2}\eta_1(t_0)$	keep
				–,	$1-\frac{1}{2}\eta_0(t_0)-\frac{1}{2}\eta_1(t_0)$	lost
Z0	Z0	X1t_0	X	0,	0	discard
				1,	$\eta_1(t_0)$	discard
				–,	$1-\eta_1(t_0)$	lost
Z0	Z0	X1t_0	Z	0,	$\frac{1}{2}\eta_0(t_0)$	keep
				1,	$\frac{1}{2}\eta_1(t_0)$	keep
				–,	$1-\frac{1}{2}\eta_0(t_0)-\frac{1}{2}\eta_1(t_0)$	lost
Z0	Z0	X1t_0	X	0,	0	discard
				1,	$\eta_1(t_0)$	discard
				–,	$1-\eta_1(t_0)$	lost
Z0	X0	Z1t_0	Z	0,	0	keep
				1,	$\eta_1(t_0)$	keep
				–,	$1-\eta_1(t_0)$	lost
Z0	X0	Z1t_0	X	0,	$\frac{1}{2}\eta_0(t_0)$	discard
				1,	$\frac{1}{2}\eta_1(t_0)$	discard
				–,	$1-\frac{1}{2}\eta_0(t_0)-\frac{1}{2}\eta_1(t_0)$	lost
Z0	X1	Z0t_1	Z	0,	$\eta_0(t_1)$	keep
				1,	0	keep
				–,	$1-\eta_0(t_1)$	lost
Z0	X1	Z0t_1	X	0,	$\frac{1}{2}\eta_0(t_1)$	discard
				1,	$\frac{1}{2}\eta_1(t_1)$	discard
				–,	$1-\frac{1}{2}\eta_0(t_1)-\frac{1}{2}\eta_1(t_1)$	lost

A. Practical intercept-resend attack

$$\text{QBER} = \frac{P(\text{error})}{P(\text{arrive})} = \frac{2\eta_0(t_1) + 2\eta_1(t_0)}{\eta_0(t_0) + 3\eta_0(t_1) + 3\eta_1(t_0) + \eta_1(t_1)}$$

In the symmetric case $\frac{\eta_1(t_0)}{\eta_0(t_0)} = \frac{\eta_0(t_1)}{\eta_1(t_1)} = \eta$

For $\eta \leq 0.066$ (~ 1:15), QBER ≤ 11%.

Eve can compromise security if mismatch is larger than 1:15

B. General security bound

Secure key generation rate:

$$R = 1 - 2h(\delta),$$

where δ is the actual bit error rate.

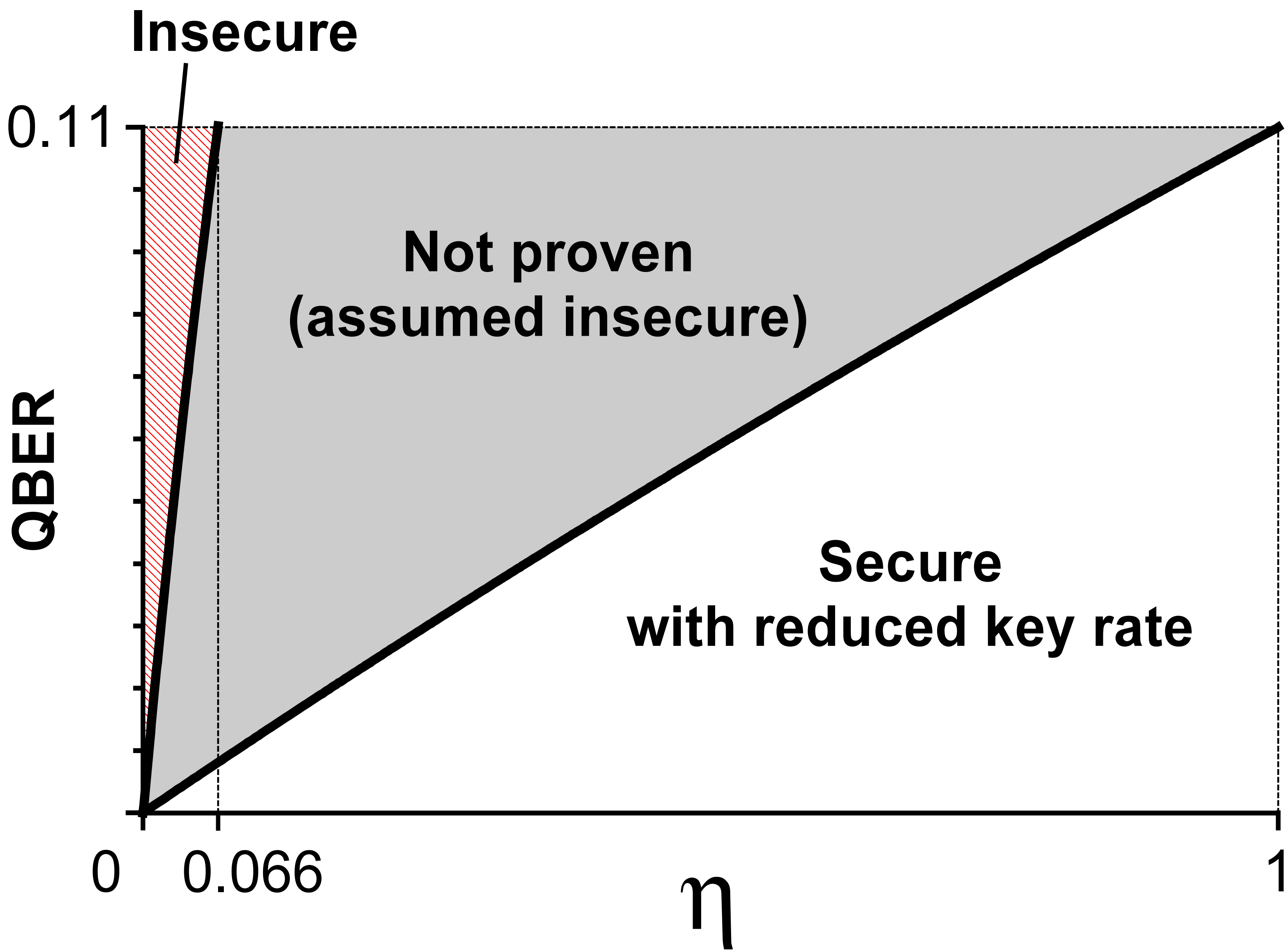
For $\eta_0(t) \neq \eta_1(t)$,

$$\mathrm{QBER} = \frac{\eta\delta}{1 + \eta\delta - \delta} \approx \eta\delta,$$

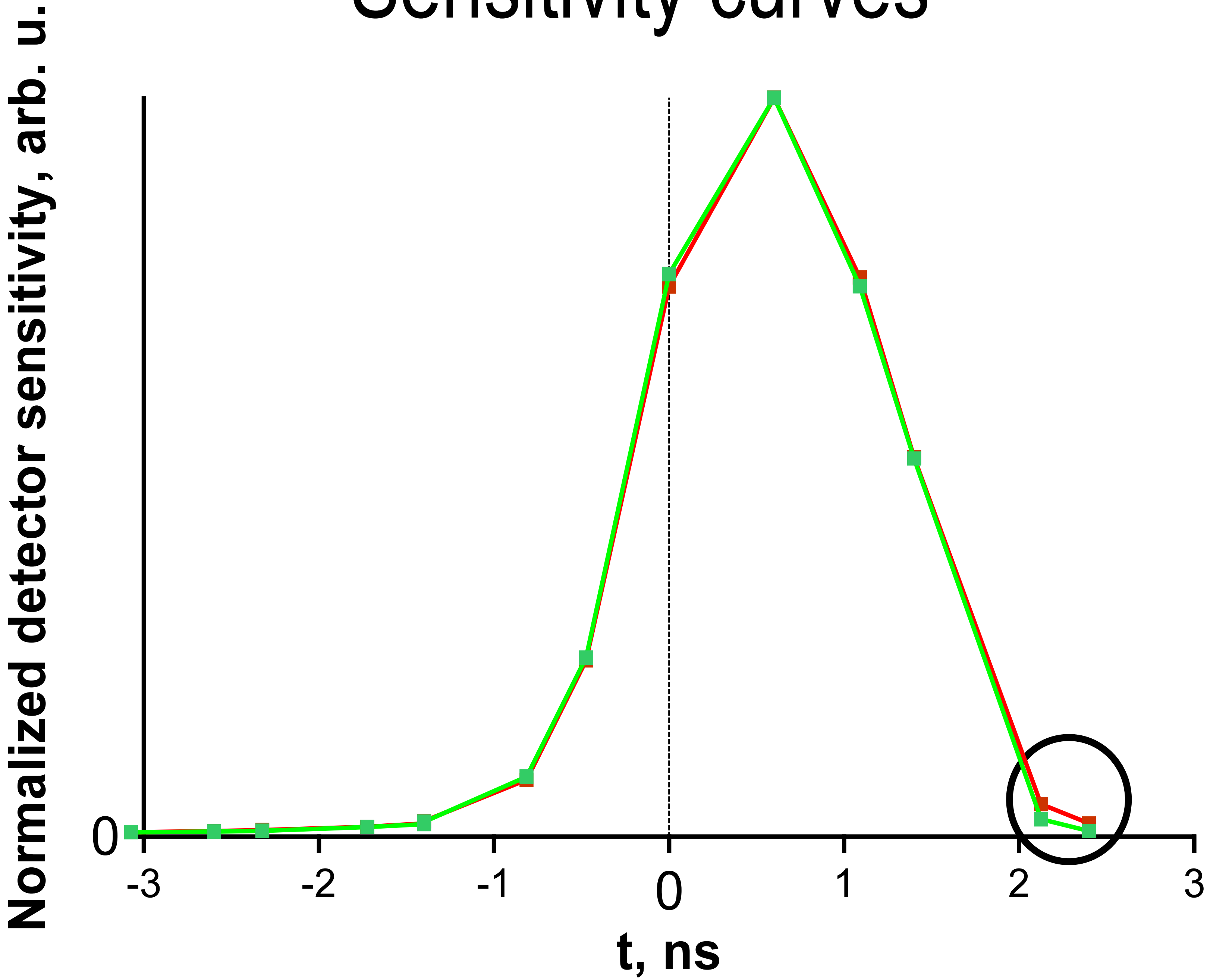
where

$$\eta = \min\left\{\min_t \frac{\eta_1(t)}{\eta_0(t)}, \min_t \frac{\eta_0(t)}{\eta_1(t)}\right\}$$

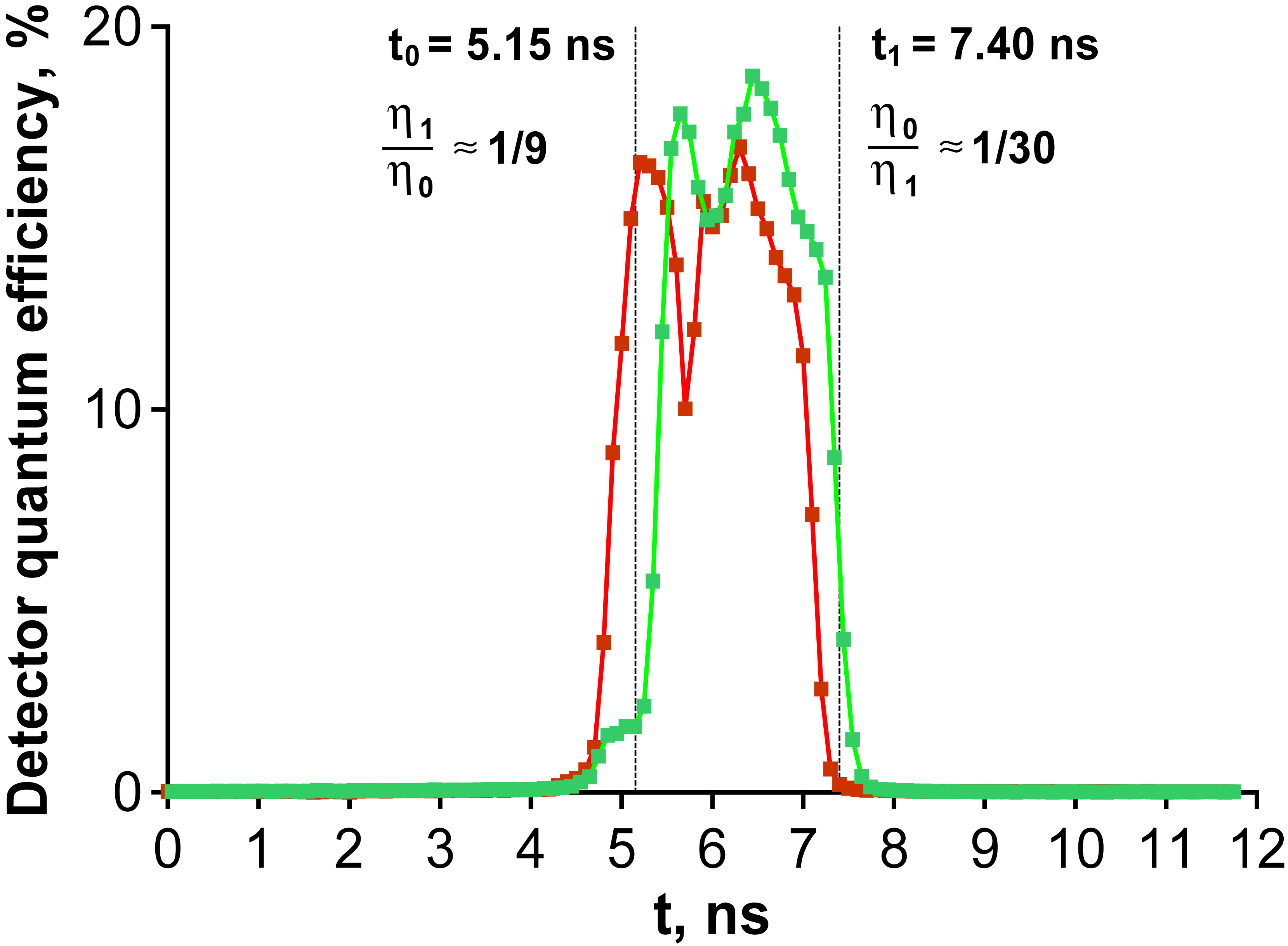
Security state of QKD system



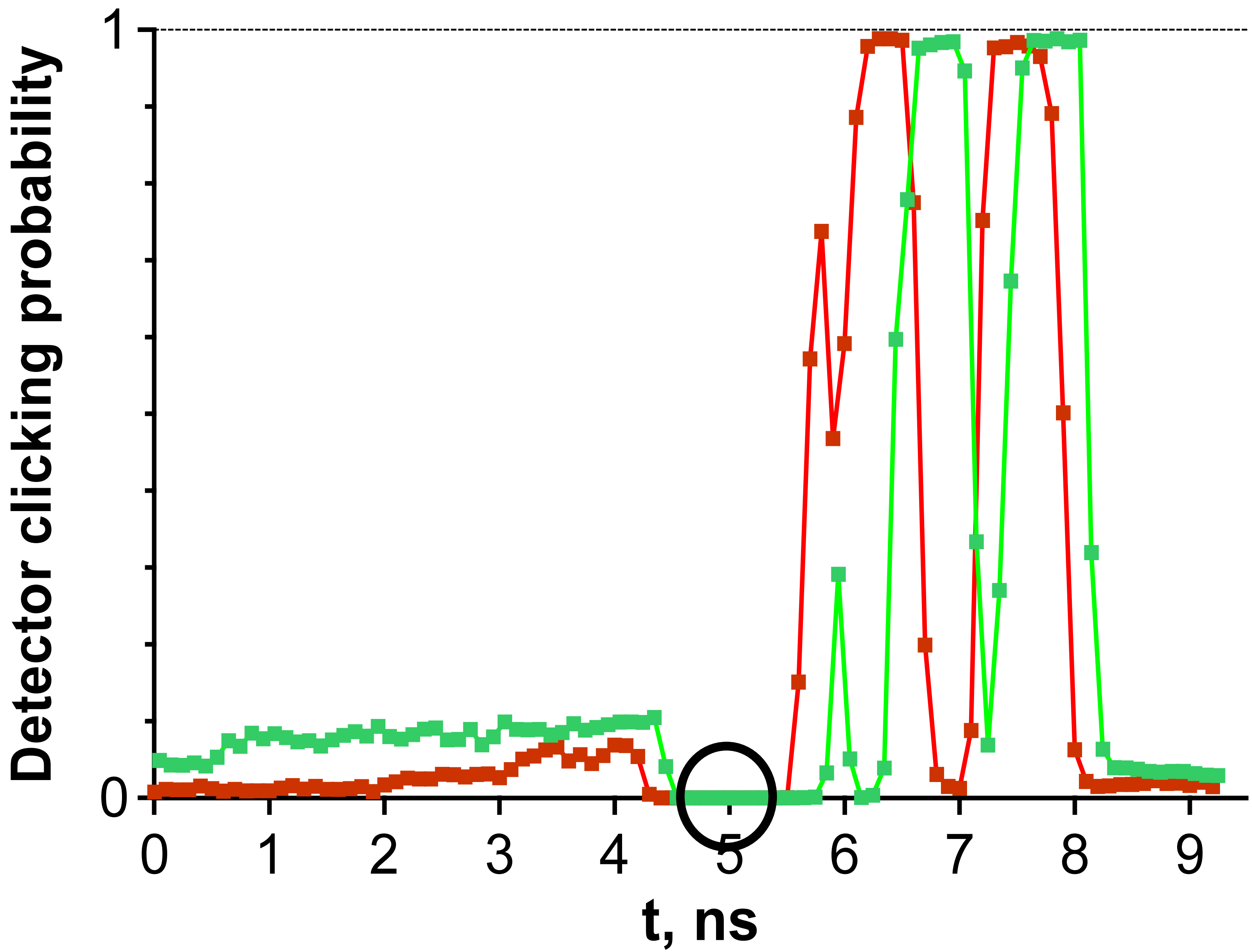
Detector model 1. Sensitivity curves



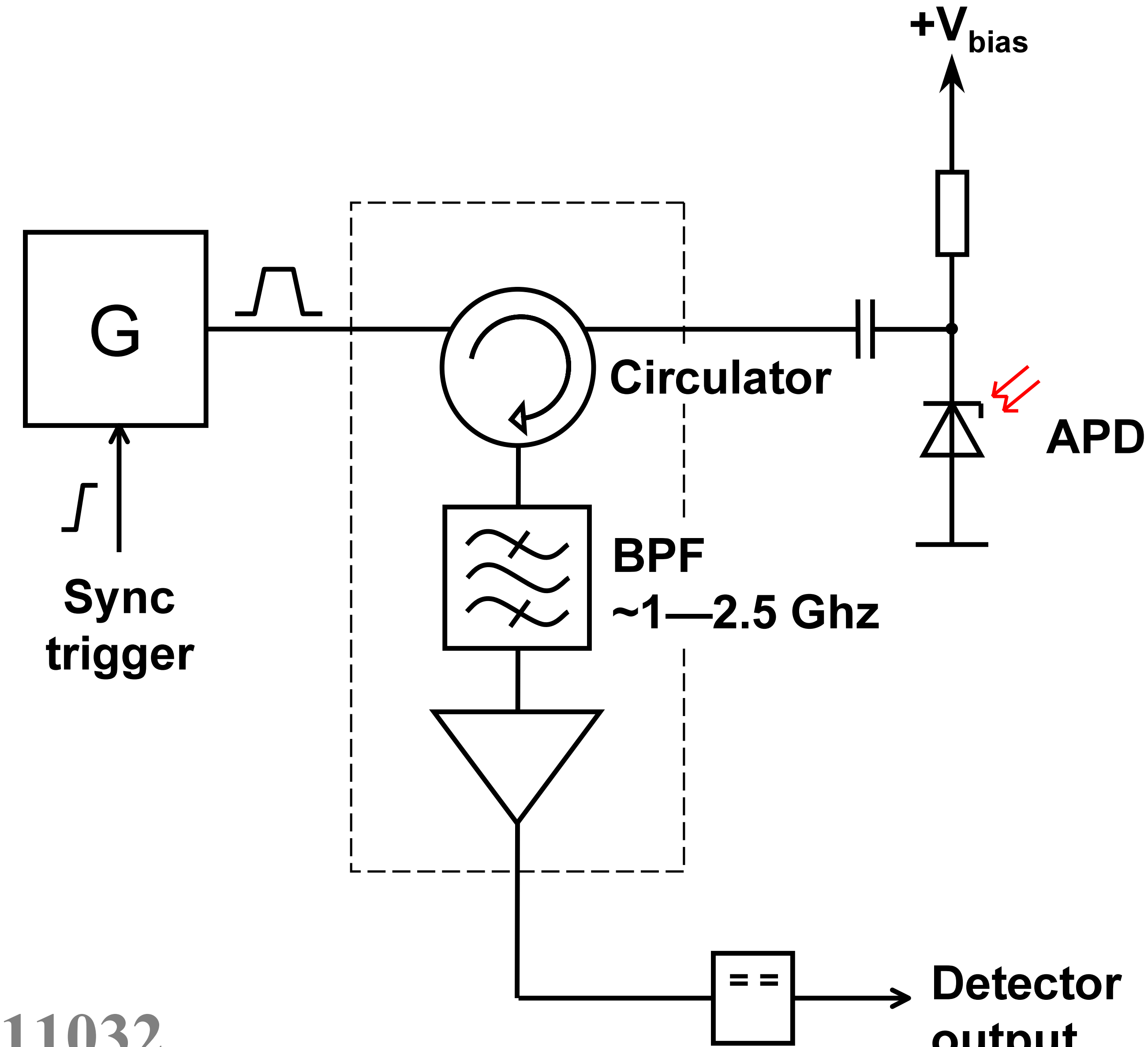
Detector model 2.
Sensitivity curves at low photon number μ=0.5



Detector model 2. Sensitivity curves at photon number μ=500



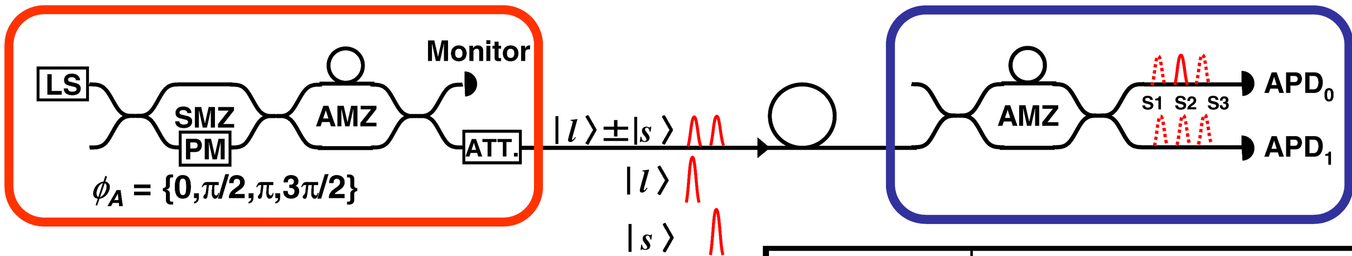
Detector model 2.
Equivalent diagram of a single channel

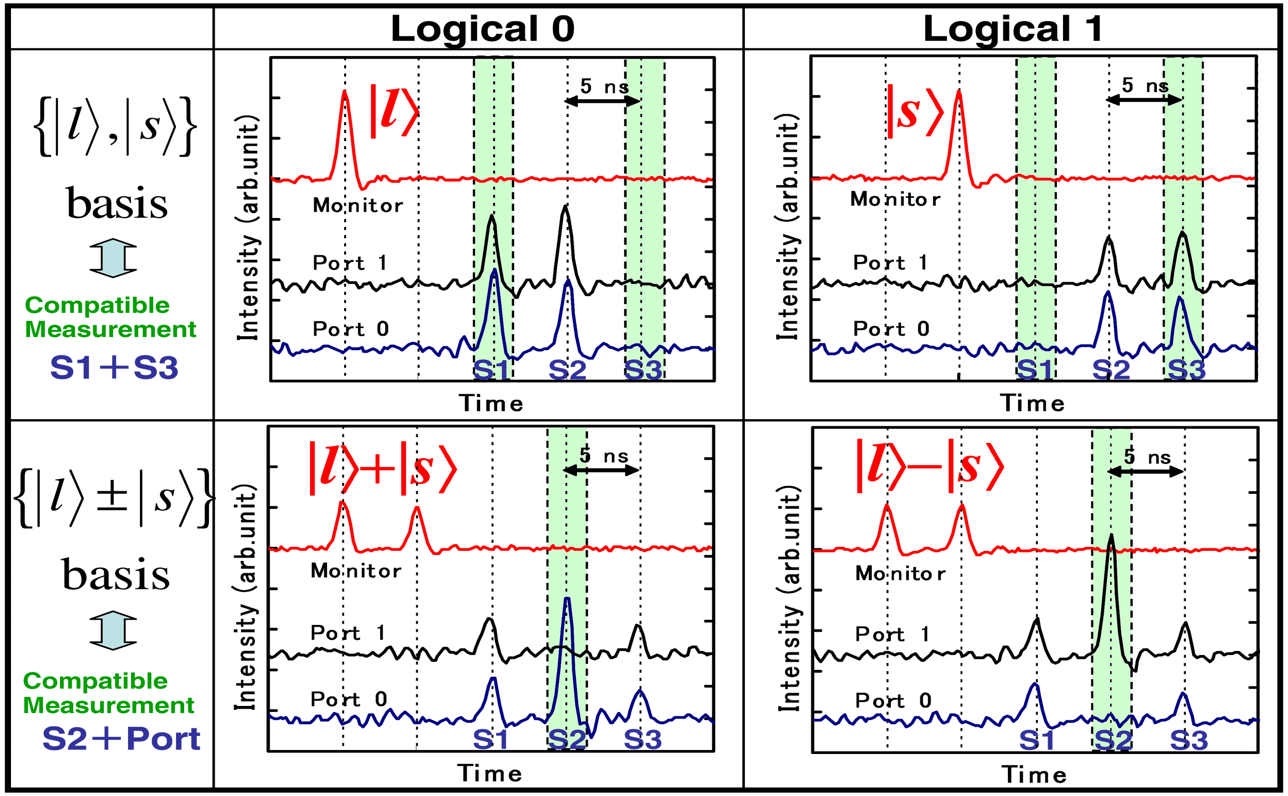


quant-ph/0511032

Phase-time coding

[Y. Nambu, T. Hatanaka, and K. Nakamura, "BB84 quantum key distribution system based on silica-based planar lightwave circuits," Jap. J. Appl. Phys. **43**, L1109–L1110 (2004)]

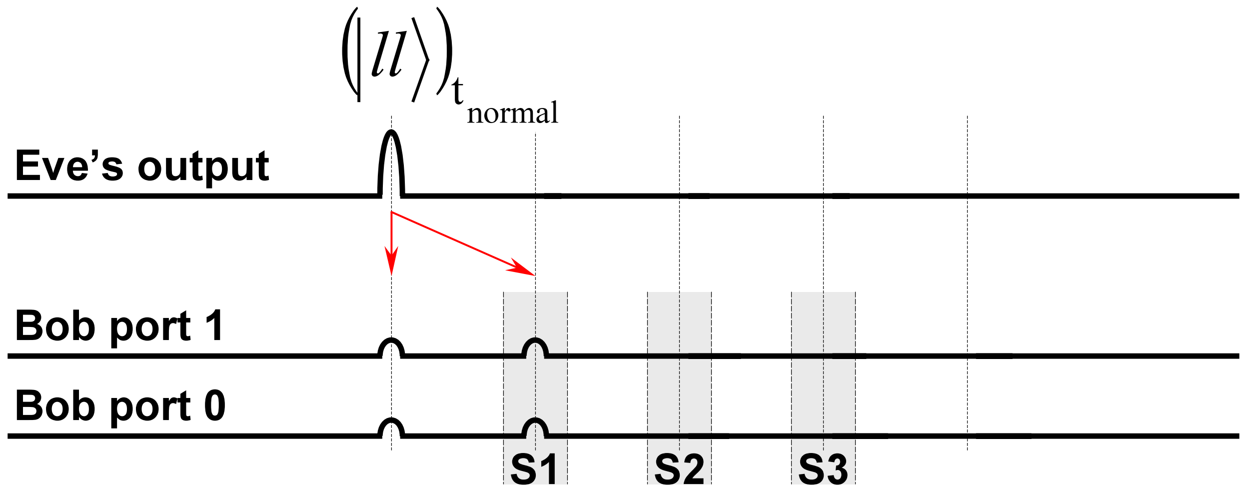
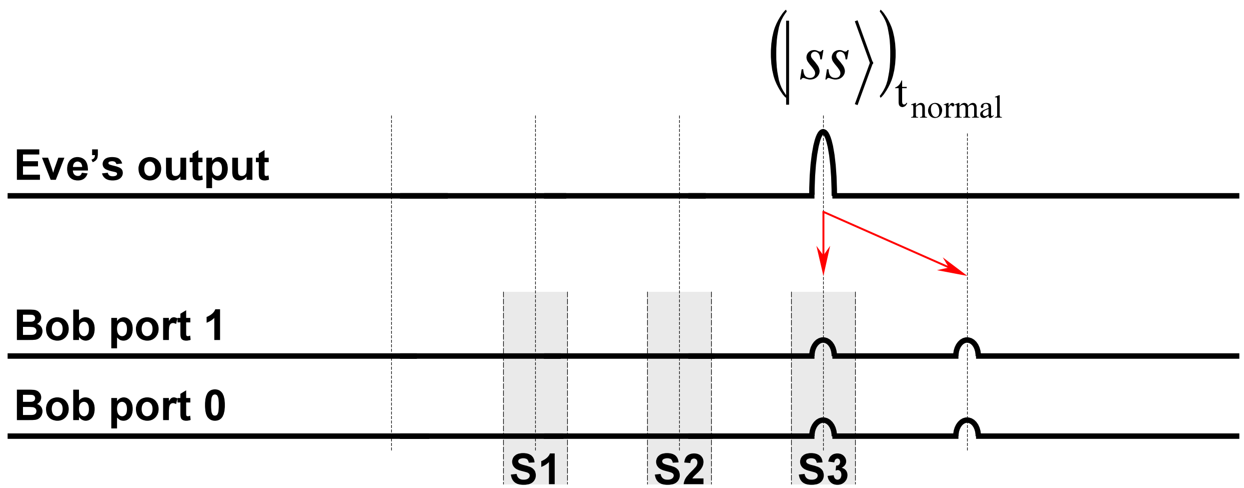




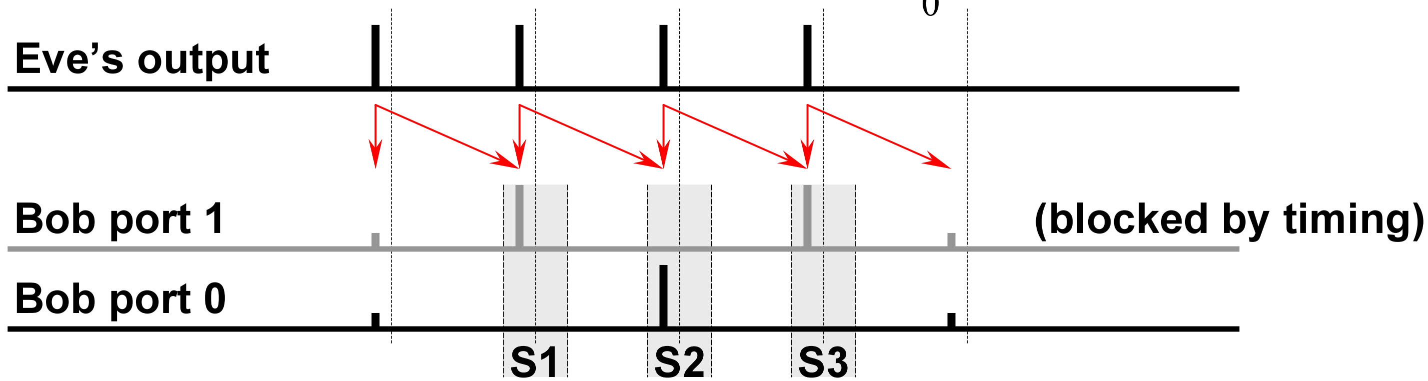
Also used in [W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. **84**, 4737–4740 (2000)]

Phase-time coding: faked states

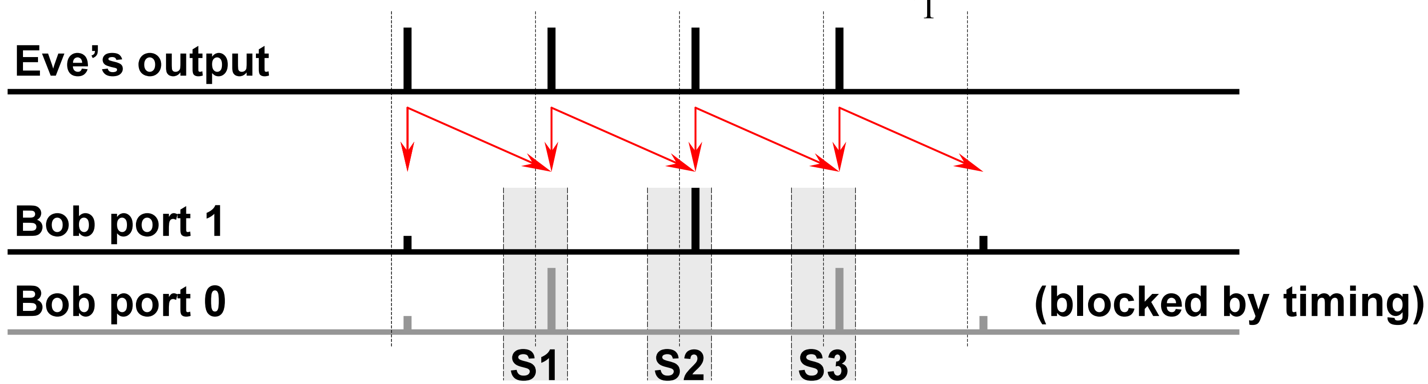
(assume use of gated detectors, total efficiency mismatch)

Eve's detection result	Faked state
S1	
S3	

Eve's detection result	Faked state
$S2_0$	$\left(\lvert ll\rangle - \lvert l\rangle - \lvert s\rangle + \lvert ss\rangle\right)_{t_0}$

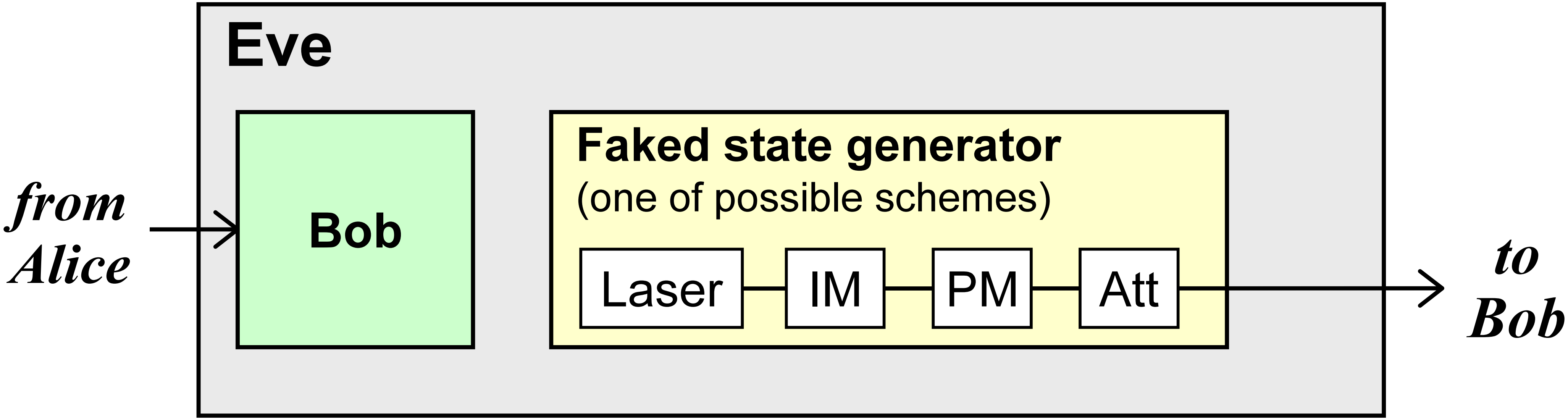


Eve's detection result	Faked state
$S2_1$	$\left(\lvert ll\rangle + \lvert l\rangle - \lvert s\rangle - \lvert ss\rangle\right)_{t_1}$



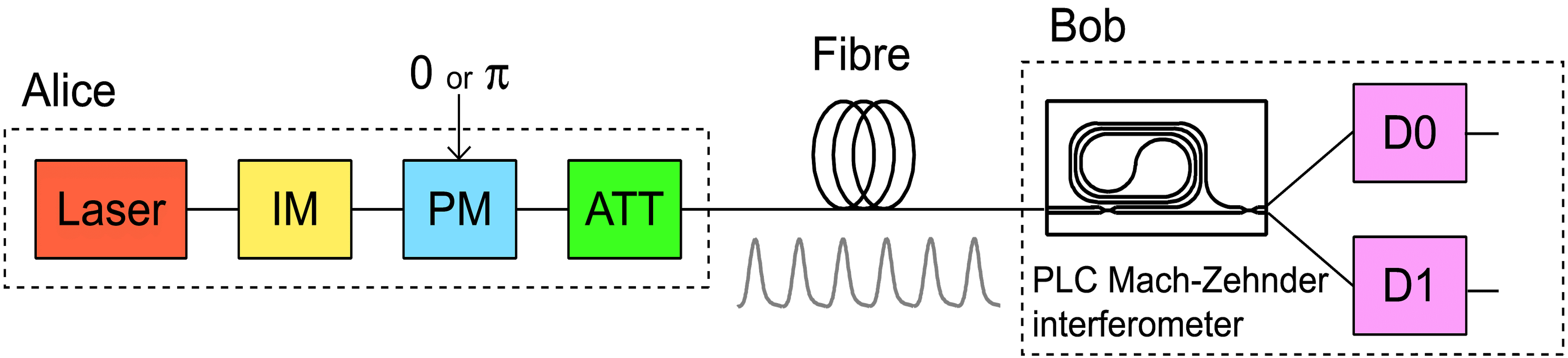
Note that in the case of ***partial*** efficiency mismatch, only Eve's faked states for $S2_0$ and $S2_1$ contribute to QBER. The faked states for S1 and S3 remain error-free.

Phase-time coding:
Eve's setup



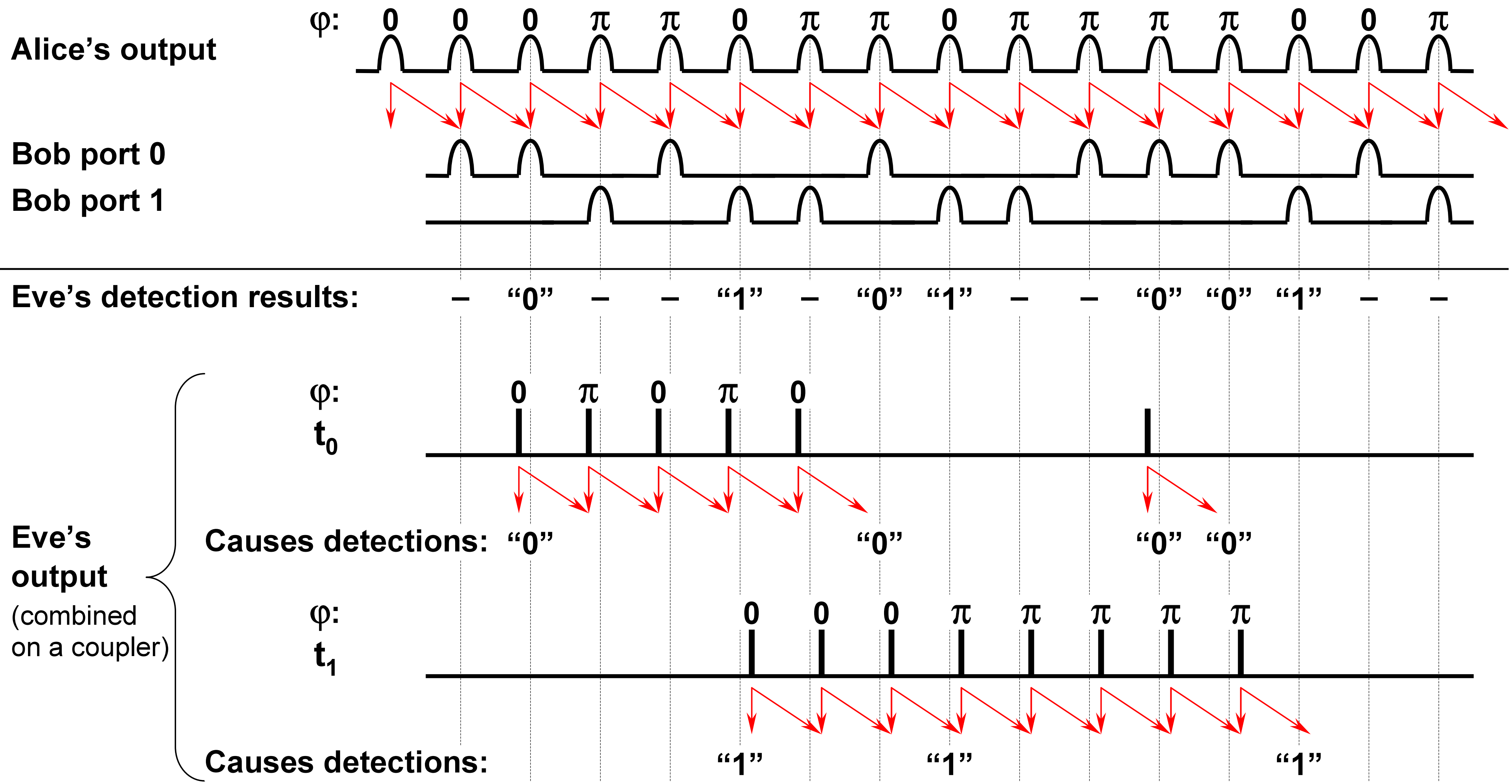
DPSK

[H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105 km fibre," New J. Phys. **7**, 232 (2005)]

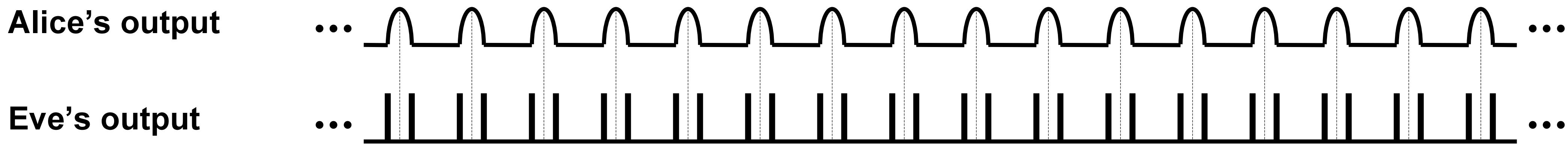


DPSK: long, overlapping faked states

(assume total efficiency mismatch)



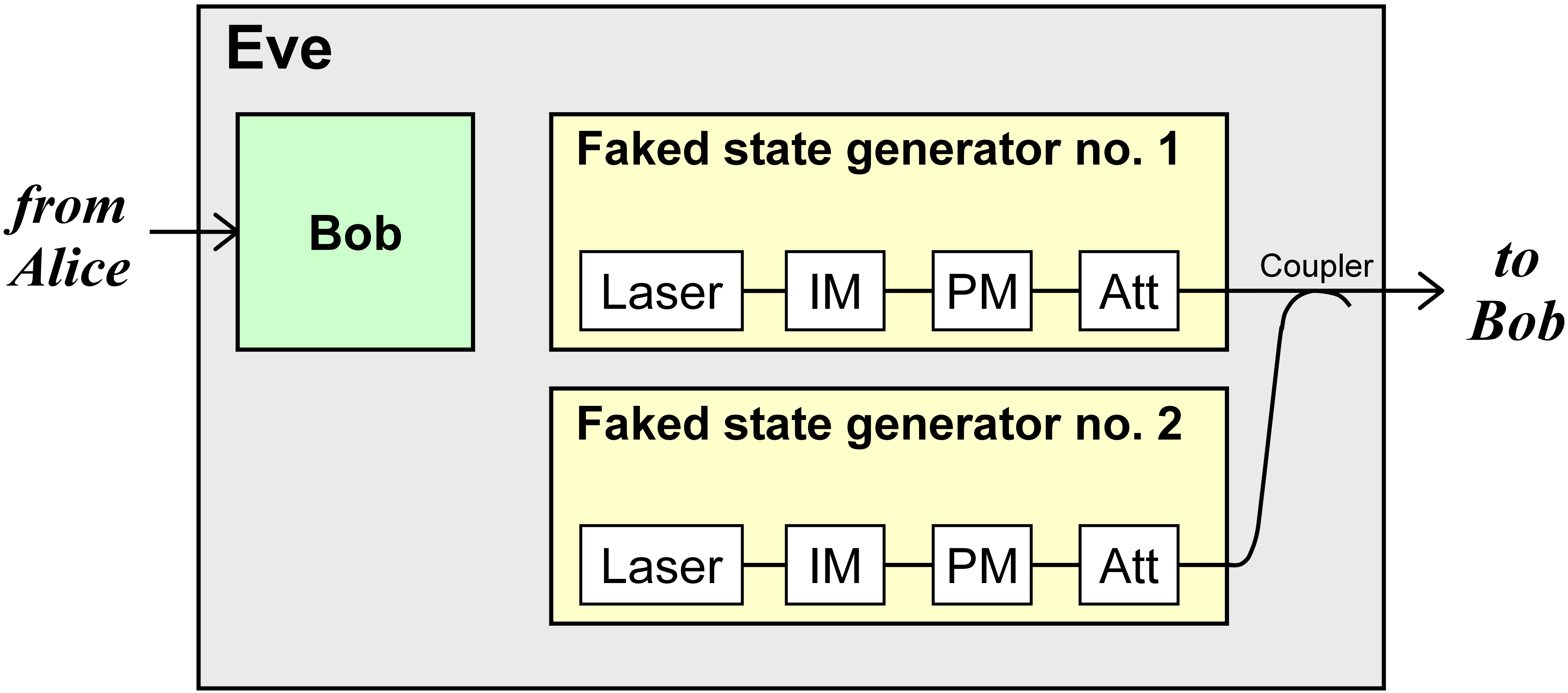
DPSK:
in limit: two continuous trains of pulses from Eve



(We don’t know yet if conditions exist under which such a continuous faked state is advantageous in the case of partial efficiency mismatch.)

NB! In this DPSK scheme, the control parameter **t** Eve uses to select Bob’s detector may not be necessarily time, but e.g. wavelength (might be useful with upconversion detectors).

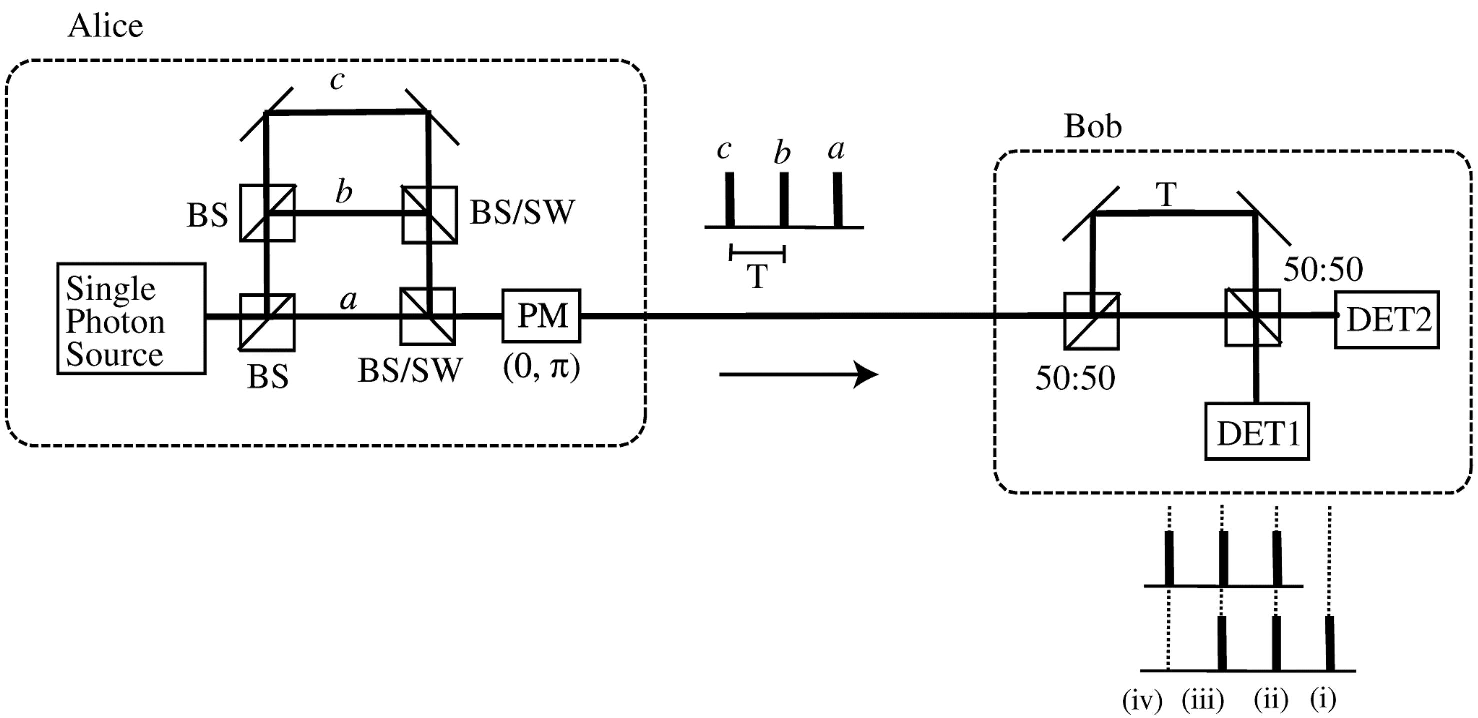
DPSK: Eve's setup



DPSK with limited-length states

can be eavesdropped on using the methods considered above

[K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” Phys. Rev. Lett. **89**, 037902 (2002)]

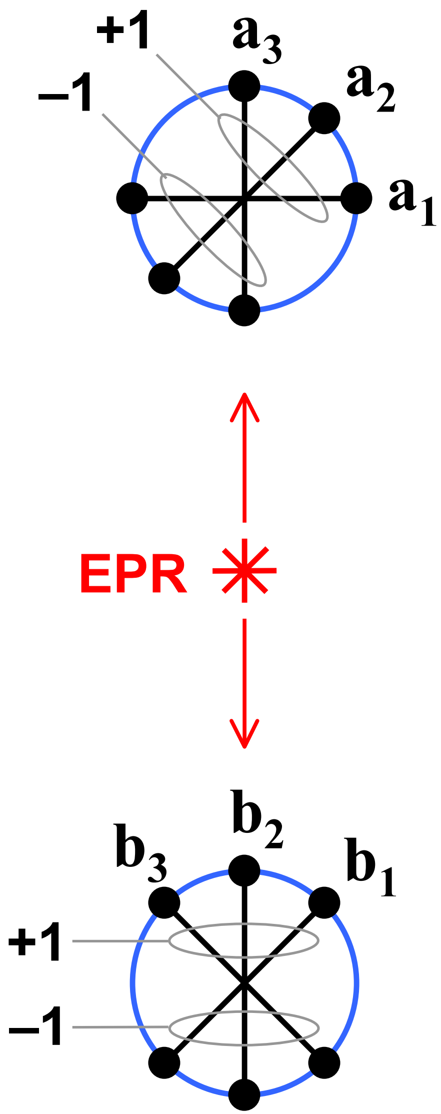


Normal counting ratio → 1 : 2 : 2 : 1
(used to check for eavesdropping)

Yet longer states in [W. Buttler, J. Torgerson, and S. Lamoreaux, “New, efficient and robust, fiber-based quantum key distribution schemes,” Phys. Lett. A **299**, 38–42 (2002)]

Ekert protocol

[A. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991)]



Correlation coefficient

$$E(a_j,b_j)=P_{++}(a_j,b_j)+P_{--}(a_j,b_j)-P_{+-}(a_j,b_j)-P_{-+}(a_j,b_j)$$

Key obtained from two perfect anticorrelations

$$E(a_2,b_1)=E(a_3,b_2)=-1$$

Checking for eavesdropping via CHSH quantity

$$S=E(a_1,b_1)-E(a_1,b_3)+E(a_3,b_1)+E(a_3,b_3)=-2\sqrt{2}$$

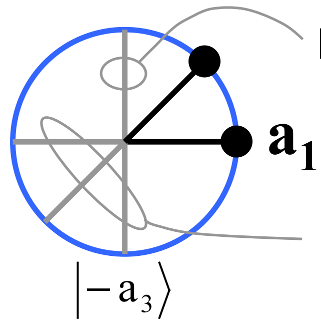
The next slide shows ***pairs of faked states*** to break Ekert protocol when there is total efficiency mismatch, and no additional consistency checks besides checking that $S=-2\sqrt{2}$.

A. Sent with P_A = 0.41
contributes equally to all correl. coeff. = **–1**

$$\left\{\begin{matrix}(\text{random state})_{t_{+1}} \\ (\text{random state})_{t_{-1}}\end{matrix}\right. \quad \text{or} \quad \left\{\begin{matrix}(\text{r.st.})_{t_{-1}} \\ (\text{r.st.})_{t_{+1}}\end{matrix}\right.$$

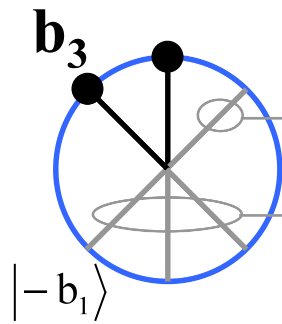
B. Sent with P_B = 0.59
contributes $\boldsymbol{E(a_1,b_3) = 1}$ (and three other correl. coeff. not used in the protocol)

$$\left\{\begin{matrix}\left(|-a_3\rangle\right)_{t_{+1}} \\ \left(|-b_1\rangle\right)_{t_{+1}}\end{matrix}\right. \quad \text{or} \quad \left\{\begin{matrix}\left(|a_3\rangle\right)_{t_{-1}} \\ \left(|b_1\rangle\right)_{t_{-1}}\end{matrix}\right.$$



blocked by state

blocked by t_{+1}



blocked by state

blocked by t_{+1}

If only A is sent, $S = -1+1-1-1 = -2$

If A and B are sent, $S = -1+\left(3-2\sqrt{2}\right)-1-1 = -2\sqrt{2}$

Conclusion

- **Detector efficiency mismatch is a problem in many protocols and encodings: BB84, phase-time, DPSK; also in implementations with source of entangled pairs placed outside Alice and Bob (e.g. Ekert protocol).**
- **The worst-case mismatch must be characterized and accounted for during privacy amplification.**
- **Active protection measures are possible (monitoring of incoming pulses at Bob).**