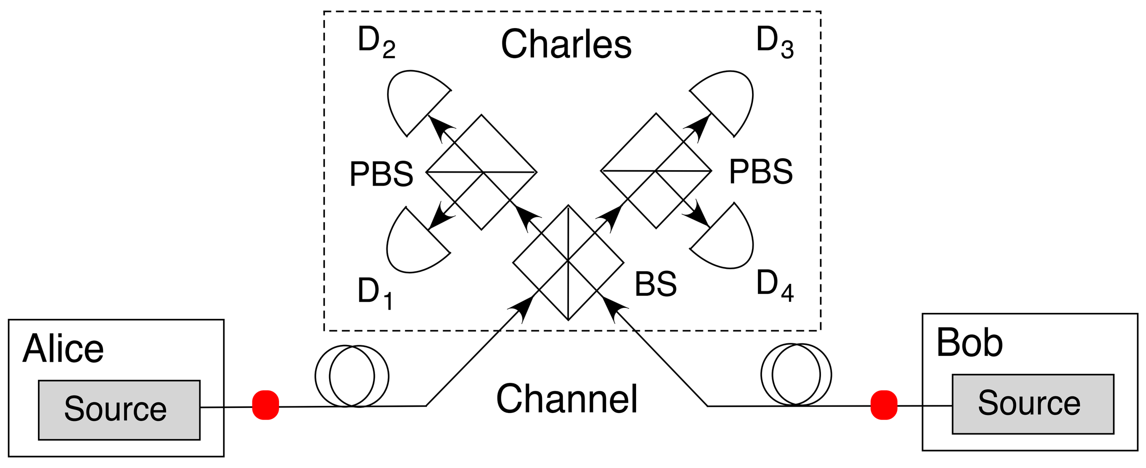
Insecurity of detector-device-independent quantum key distribution

Shihan Sajeed[1,2]
Anqi Huang[1,2]
Shihai Sun[3]
Feihu Xu[4]
Vadim Makarov[5,1,2]
Marcos Curty[6]

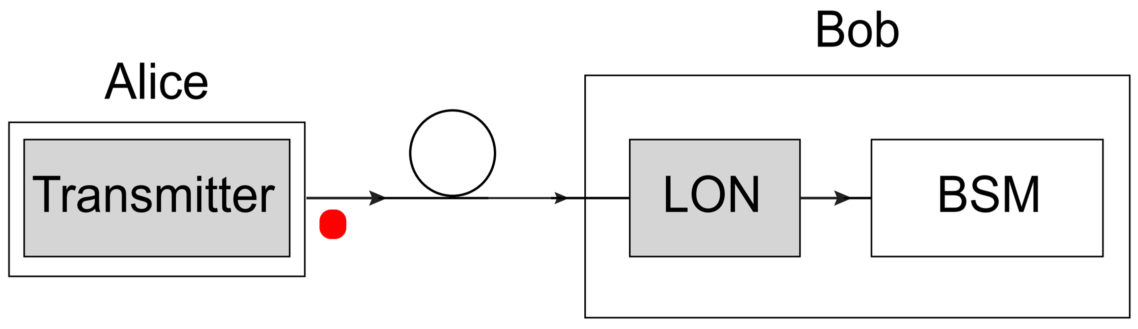
From mdi QKD to ddi QKD

Measurement device independent (mdi) QKD



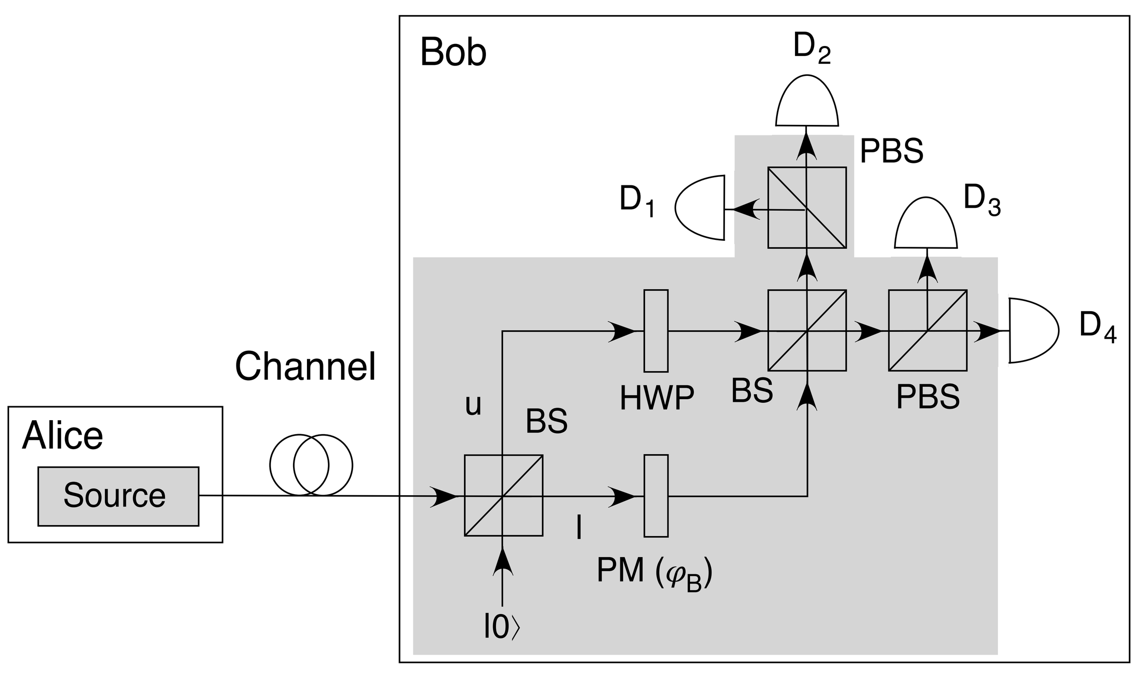
Features:
- Guaranteed security at the detection side
- Two-photon interference required
- Low key rate
- Difficult to implement

Detector device independent (ddi) QKD



Features:
- Alice and Bob Encode on the same photon
- No two-photon interference required
- higher key rate
- Easy to implement
- Pomise to provide mdi-QKD security

Example of a ddi-QKD realization



fully characterized and trusted

D_1 - D_4 not characterized but trusted

Alice: $\frac{1}{\sqrt{2}}(|H\rangle + e^{i\theta_A}|V\rangle)$

Bob: $\frac{1}{\sqrt{2}}(|u\rangle + e^{i\varphi_B}|l\rangle)$

Bell state: $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_p|u\rangle_s \pm |V\rangle_p|l\rangle_s)$

$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_p|l\rangle_s \pm |V\rangle_p|u\rangle_s)$

Detection:
A single click projects to a Bell state

ddi QKD ≠ mdi QKD

The state just before measurement:

$$|\psi\rangle = \left|\frac{\sqrt{\mu}}{2}(e^{i\phi_E}+e^{i\varphi_B})\right\rangle_{D_1} \otimes \left|\frac{\sqrt{\mu}}{2}(1+e^{i(\phi_E+\varphi_B)})\right\rangle_{D_2} \otimes \left|\frac{\sqrt{\mu}}{2}(e^{i\phi_E}-e^{i\varphi_B})\right\rangle_{D_3} \otimes \left|\frac{\sqrt{\mu}}{2}(1-e^{i(\phi_E+\varphi_B)})\right\rangle_{D_4}.$$

Lets assume, only D1 is used?

mdi QKD: secure
ddi QKD: insecure

In this case:
Eve can do a faked-state attack

Intensity at D1

$$\mu/2 < \mu_{\mathrm{th}} < \mu$$

D1 output

$\varphi_B \setminus \phi_E$	0	$\pi/2$	π	$3\pi/2$
0	click	-	-	-
$\frac{\mu}{2}$	-	click	-	-
π	-	-	click	-
$\frac{3\pi}{2}$	-	-	-	click

The security of ddi QKD cannot be based on post-selected entanglement

What about double clicks?

Full scheme with four detectors

(a) $\phi_E = 0$

φ_B	D_1	D_2	D_3	D_4
0	μ	μ	0	0
$\frac{\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
π	0	0	μ	μ
$\frac{3\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$

(b) $\phi_E = \frac{\pi}{2}$

φ_B	D_1	D_2	D_3	D_4
0	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{\pi}{2}$	μ	0	0	μ
π	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{3\pi}{2}$	0	μ	μ	0

(c) $\phi_E = \pi$

φ_B	D_1	D_2	D_3	D_4
0	0	0	μ	μ
$\frac{\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
π	μ	μ	0	0
$\frac{3\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$

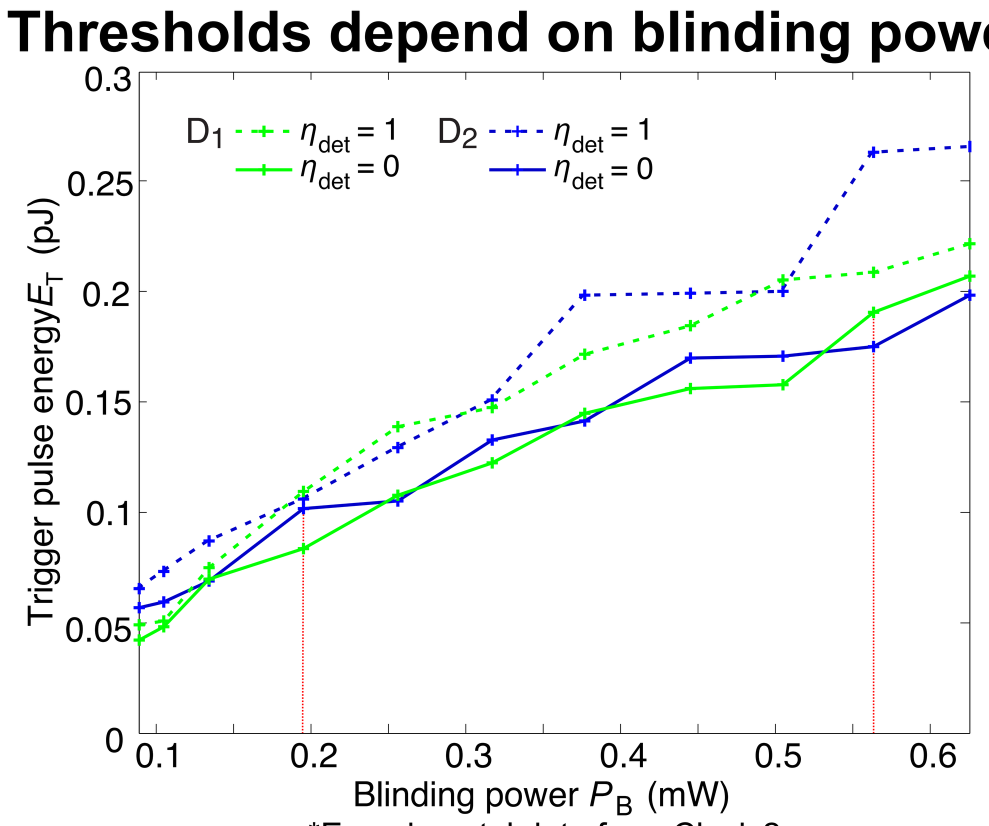
(d) $\phi_E = \frac{3\pi}{2}$

φ_B	D_1	D_2	D_3	D_4
0	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{\pi}{2}$	0	μ	μ	0
π	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{3\pi}{2}$	μ	0	0	μ

Drawback: detector blinding attack produces double-clicks

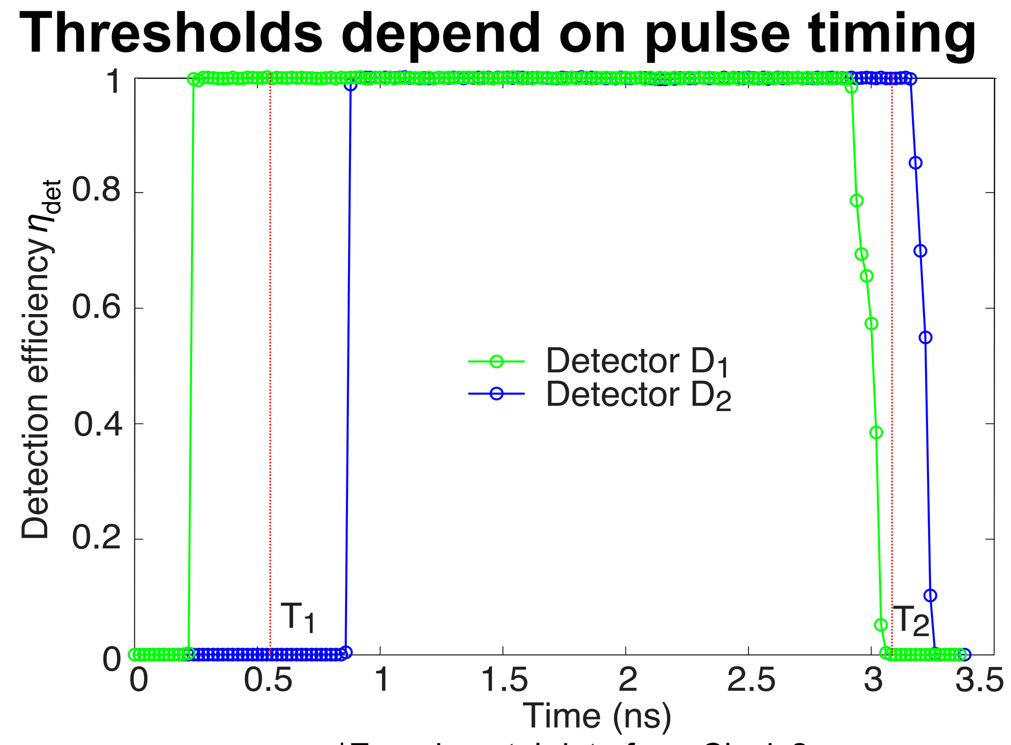
Avoiding double clicks

Strategy 1:
Thresholds depend on blinding power



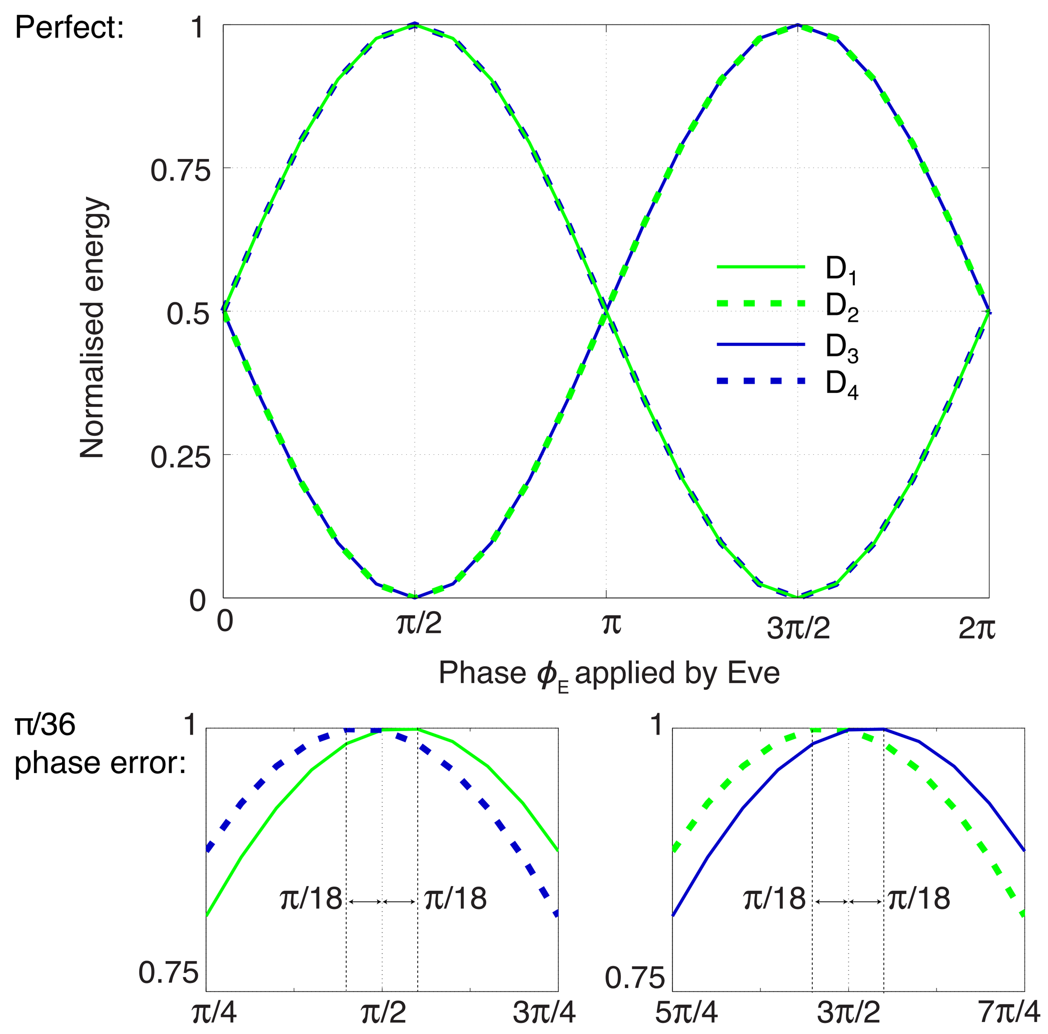
*Experimental data from Clavis2

Strategy 2:
Thresholds depend on pulse timing

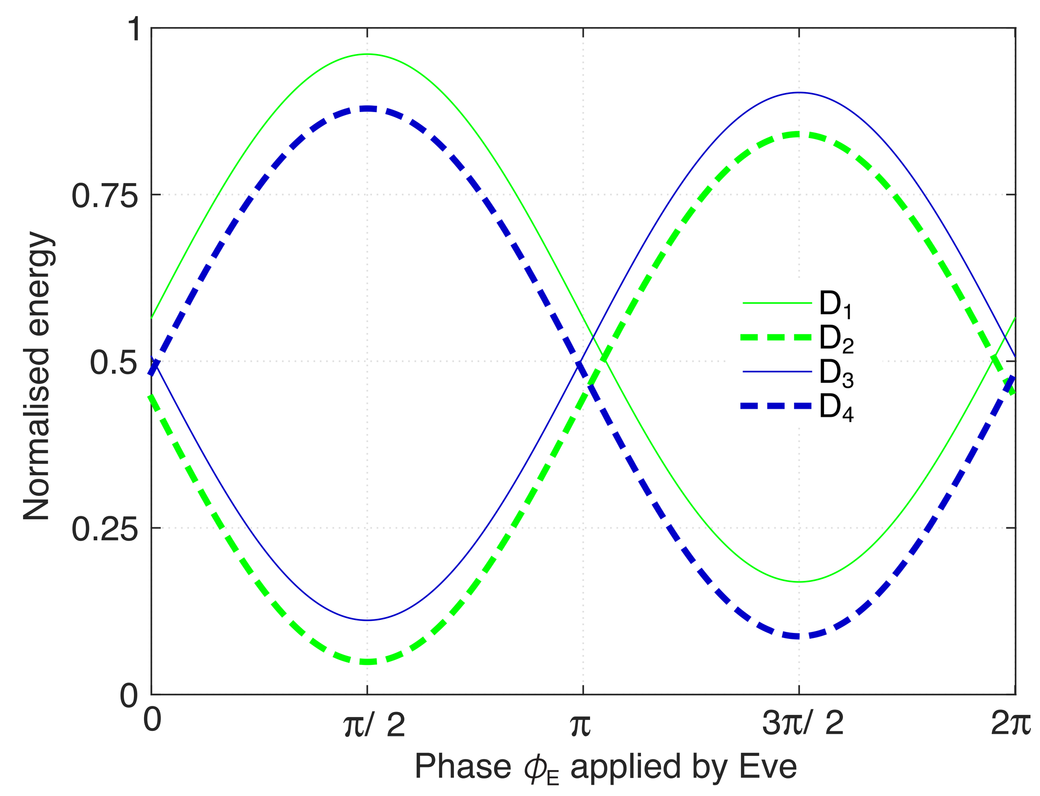


*Experimental data from Clavis2

Strategy 3:
Imperfection of phase modulator



Strategy 4:
Imperfection of beam splitter



* BS splitting ratio 44: 56

[1] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[3] College of Science, National University of Defense Technology, Changsha 410073, China
[4] Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
[5] Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[6] Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain