Hacking the Franson interferometer

Faking an extreme violation of the CHSH inequality with classical light

Jonathan Jogenfors[*], Ashraf Abdelrazig[†], Mohamed Bourennane[†] and Jan-Åke Larsson[*]

[*] Information Coding Group, Dept. of Electrical Engineering, Linköping University
[†] Quantum Information and Quantum Optics Group, Dept. of Physics, Stockholm University.

jonathan.jogenfors@liu.se

QCrypt 2014, Paris
September, 5.

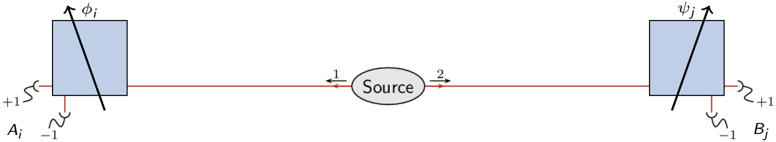
LiU expanding reality

The promises of the Bell test

The Bell inequality has been proposed as a security test for E91.

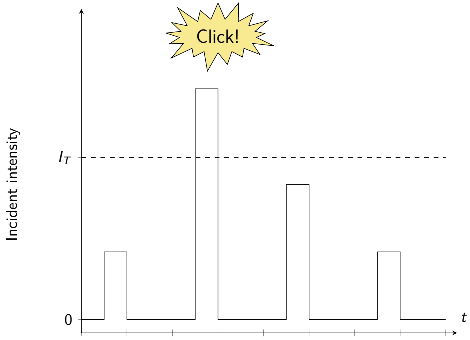
Later this concept has evolved into *device-independent security*.

The implementation of the measurement system does not matter as long as Bell's inequality is violated (and the settings don't leak out from the laboratory).



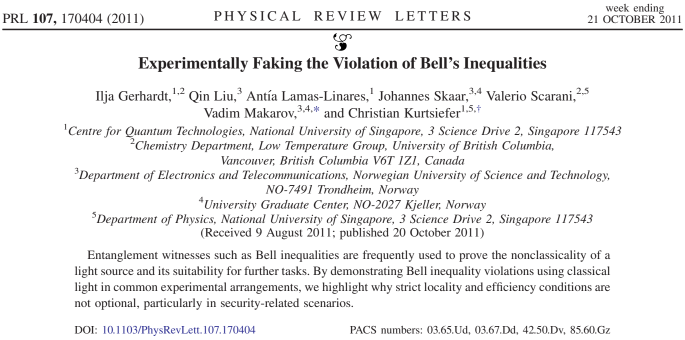
Avhalance photodetectors can be blinded

Lydersen et al. (Nat. Photon. 2010) demonstrated an attack on APD:s that allows remote control with bright illumination.



This trick prevents a single-photon detector from seeing incoming pulses below an intensity threshold I_T. Only the second pulse will give a click.

The blinding attack was used to break the security of E91



PRL **107,** 170404 (2011) PHYSICAL REVIEW LETTERS week ending 21 OCTOBER 2011

Experimentally Faking the Violation of Bell's Inequalities

Ilja Gerhardt,[1,2] Qin Liu,[3] Antía Lamas-Linares,[1] Johannes Skaar,[3,4] Valerio Scarani,[2,5]
Vadim Makarov,[3,4,*] and Christian Kurtsiefer[1,5,†]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2]*Chemistry Department, Low Temperature Group, University of British Columbia, Vancouver, British Columbia V6T 1Z1, Canada*
[3]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[4]*University Graduate Center, NO-2027 Kjeller, Norway*
[5]*Department of Physics, National University of Singapore, 3 Science Drive 2, Singapore 117543*

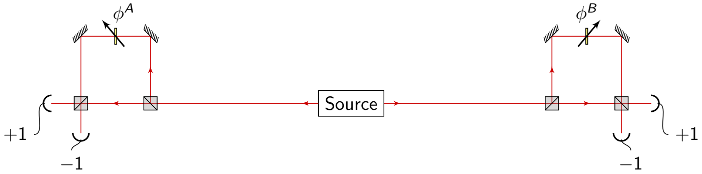
(Received 9 August 2011; published 20 October 2011)

Entanglement witnesses such as Bell inequalities are frequently used to prove the nonclassicality of a light source and its suitability for further tasks. By demonstrating Bell inequality violations using classical light in common experimental arrangements, we highlight why strict locality and efficiency conditions are not optional, particularly in security-related scenarios.

DOI: 10.1103/PhysRevLett.107.170404 PACS numbers: 03.65.Ud, 03.67.Dd, 42.50.Dv, 85.60.Gz

Gerhardt et al. (PRL 2011) successfully attacked a commercial QKD system. Note, however, that their faked detector efficiency of the attack is low (50 %).

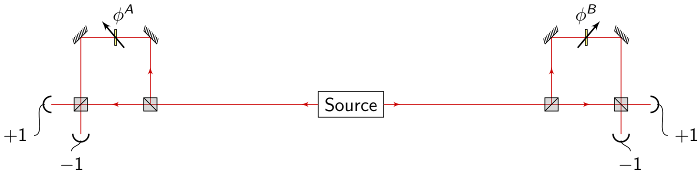
The Franson interferometer



- Photon pairs are sent at unknown moments in time
- Some photons are delayed, and some are not
- If they are simultaneously detected (coincident), they can either both be delayed or not

$$E(A(\phi_i^A)B(\phi_j^B)|\text{coinc.}) = \cos(\phi_i^A + \phi_j^B)$$

The Franson interferometer



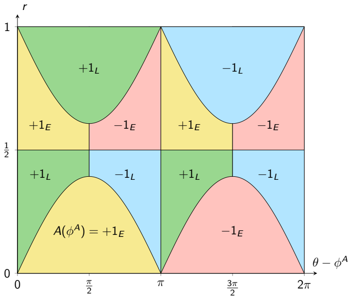
- The appropriate ϕ_i^A and ϕ_j^B give

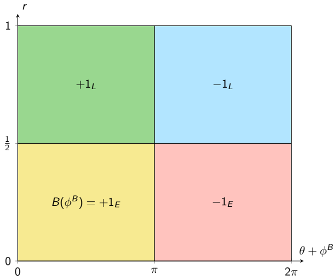
$$\left|E(A(\phi_1^A)B(\phi_2^B)|\text{coinc.}) + E(A(\phi_3^A)B(\phi_2^B)|\text{coinc.})\right|$$
$$+ \left|E(A(\phi_3^A)B(\phi_4^B)|\text{coinc.}) - E(A(\phi_3^A)B(\phi_4^B)|\text{coinc.})\right| = 2\sqrt{2}$$

- The quantum-mechanical predictions violate the Bell inequality (≤ 2) when we ignore the postselection.
- However, we will demonstrate an attack that imitates the quantum prediction with classical light.

There exists a local hidden variable model that gives the same predictions

Aerts et al. (PRL 1999) presented an LHV model that we will use and modify for our attack.

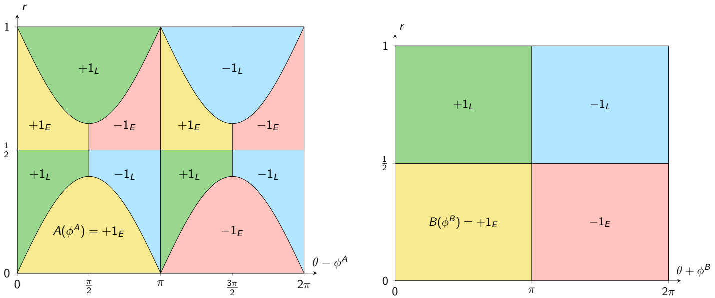




The hidden variables are θ and r.

There exists a local hidden variable model that gives the same predictions

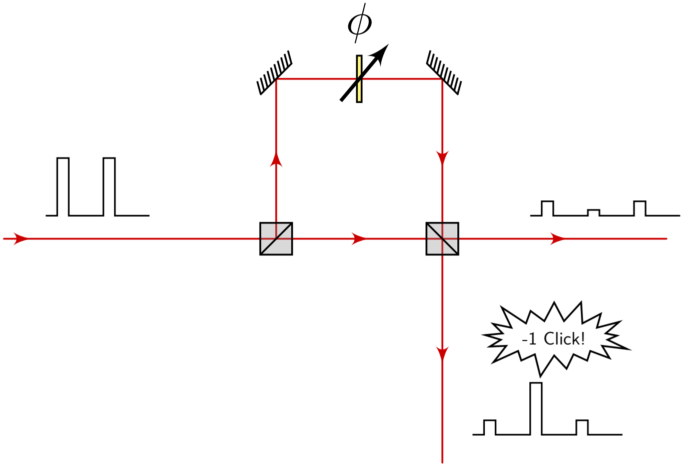
Aerts et al. (PRL 1999) presented an LHV model that we will use and modify for our attack.



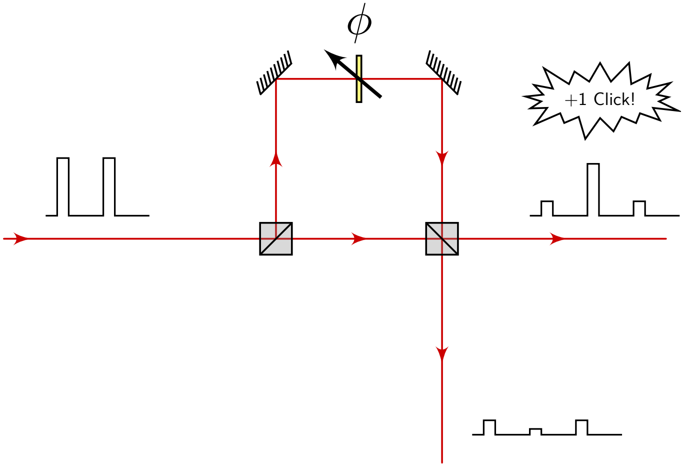
The hidden variables are θ and r.

Let's combine this model with blinding!

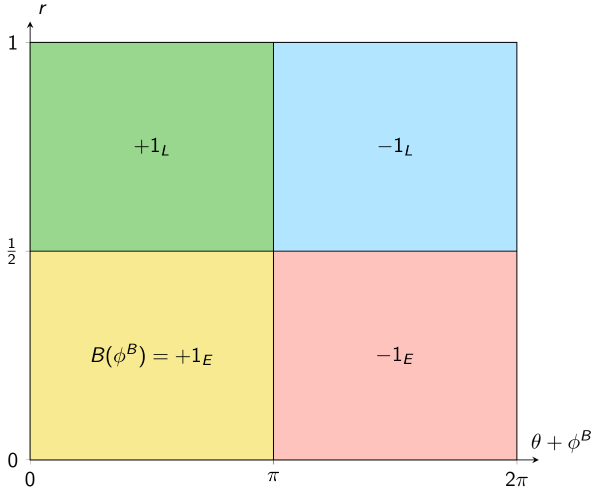
Two input pulses: ϕ changes the sign of the outcome



Two input pulses: ϕ changes the sign of the outcome

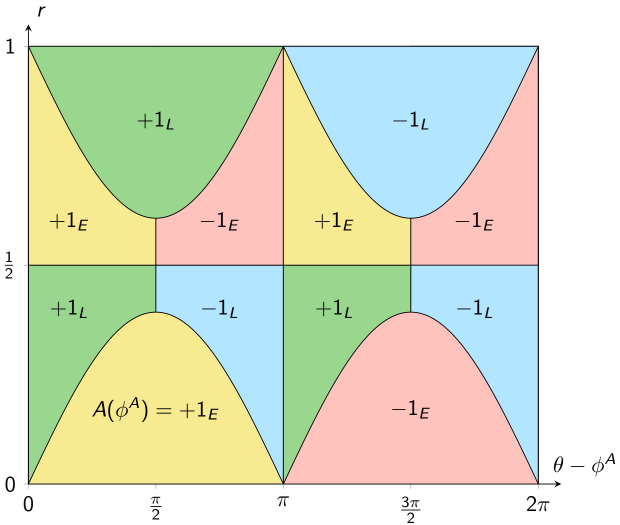


The LHV model for Bob uses two pulses



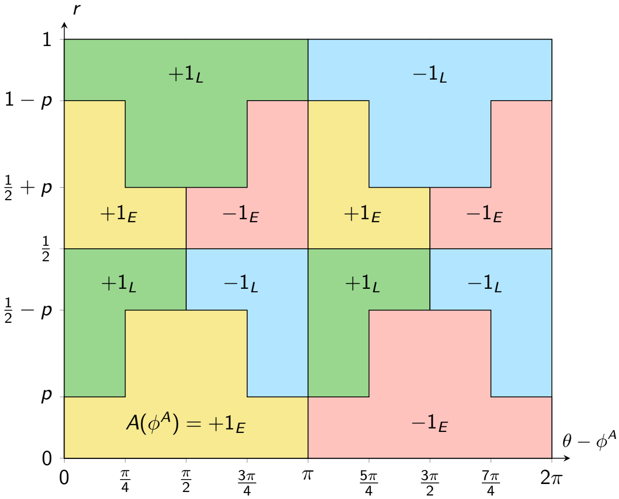
Varying ϕ^B changes the sign but *not* the detection time.

For Alice we need to add complexity



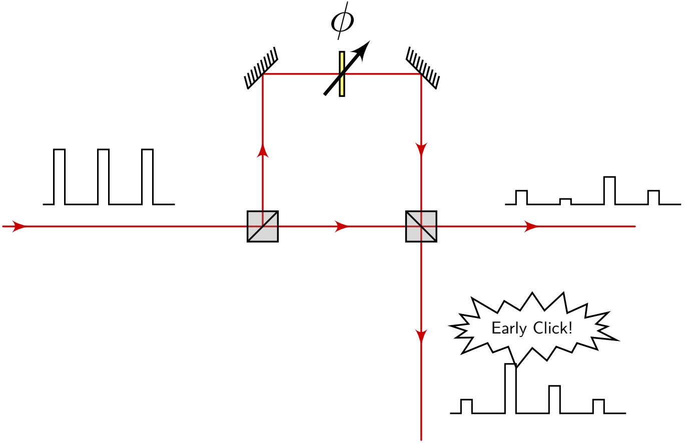
Varying ϕ^A changes *both* the detection time and the sign.

To simplify, we discretize the model



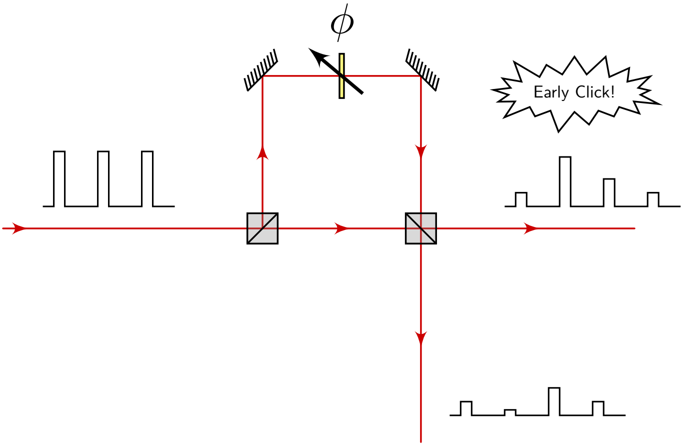
With $p = (2-\sqrt{2})/4$ we get the Bell value $2\sqrt{2}$, just like the quantum prediction.

Three input pulses controls time and sign



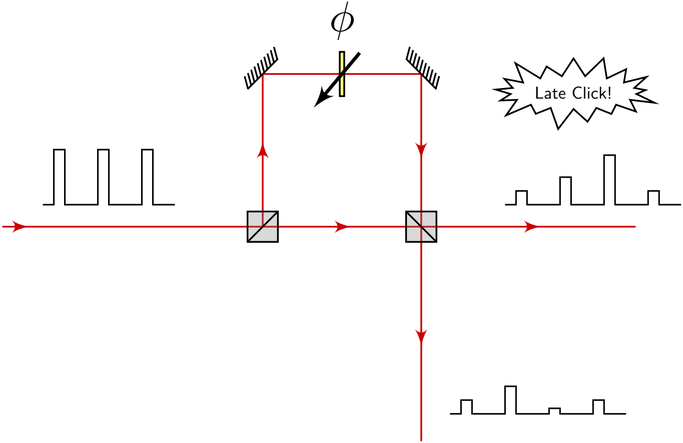
Phase shifted input pulses do the trick.

Three input pulses controls time and sign



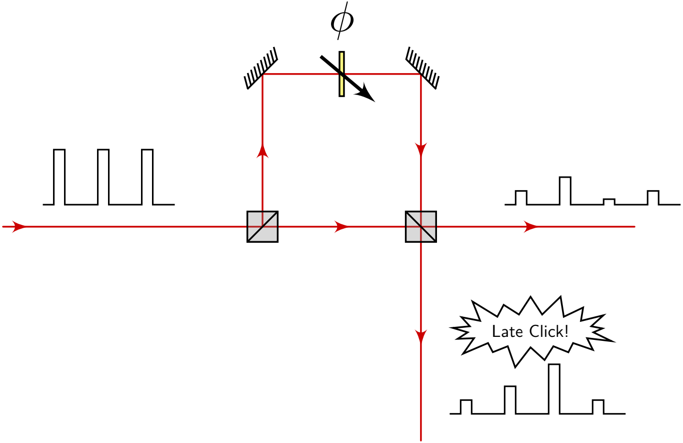
Phase shifted input pulses do the trick.

Three input pulses controls time and sign



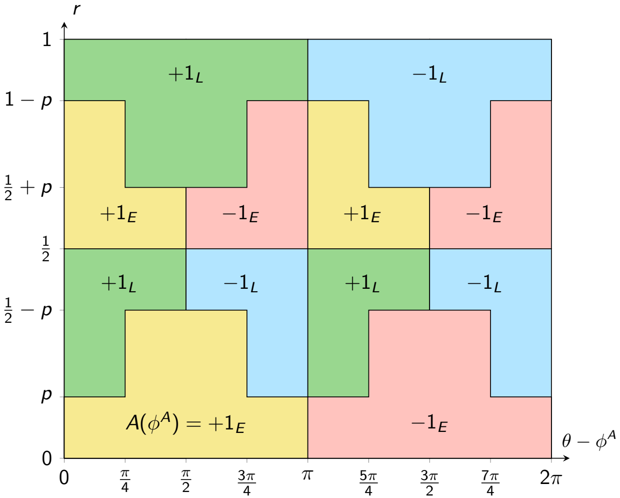
Phase shifted input pulses do the trick.

Three input pulses controls time and sign



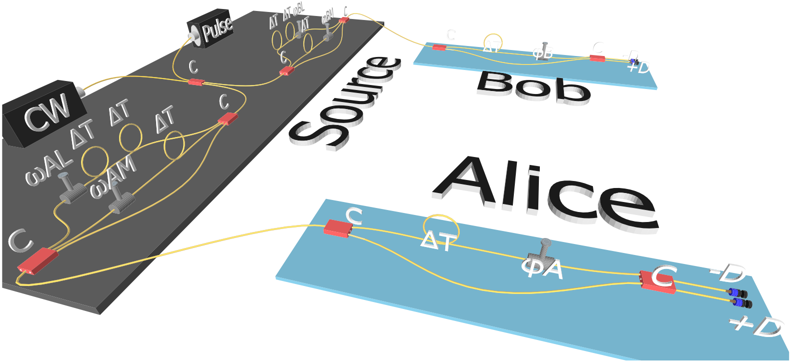
Phase shifted input pulses do the trick.

To simplify, we discretize the model

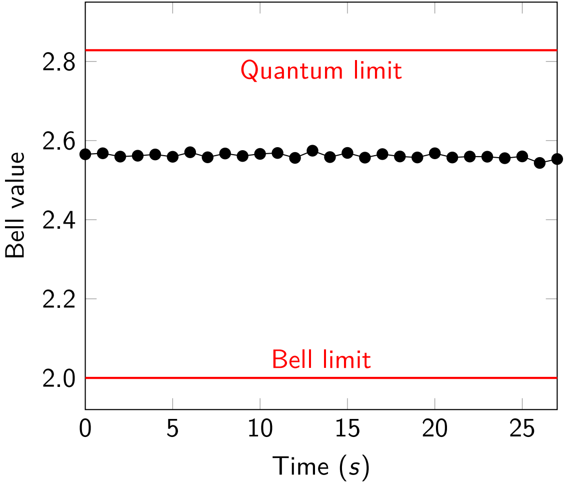


With $p = (2-\sqrt{2})/4$ we get the Bell value $2\sqrt{2}$, just like the quantum prediction.

Experimental implementation

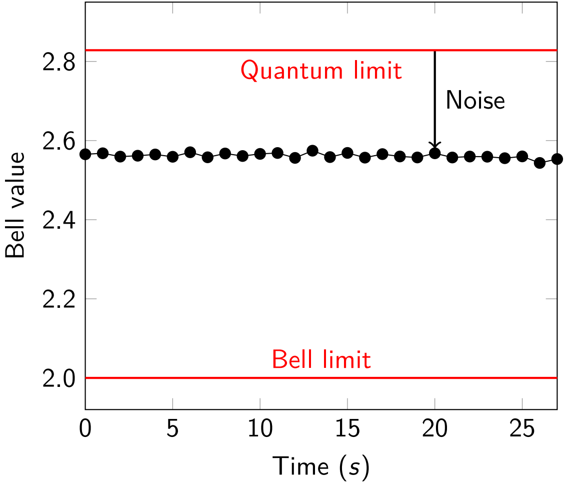


The experiment clearly violates Bell



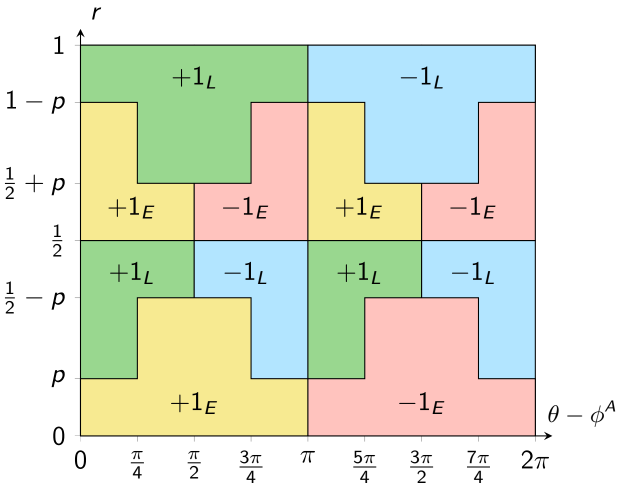
Our experimental faked Bell value is 2.5615 ± 0.0064. The efficiency is at 97.6 %. The reduction from $2\sqrt{2}$ is caused by noise.

The experiment clearly violates Bell



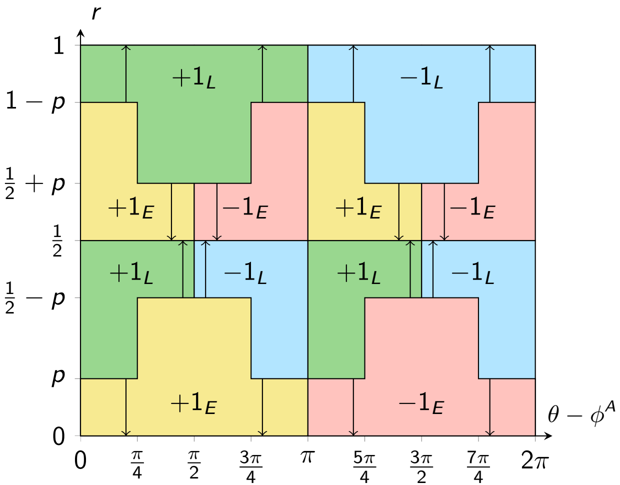
Our experimental faked Bell value is 2.5615 ± 0.0064. The efficiency is at 97.6 %. The reduction from $2\sqrt{2}$ is caused by noise.

But wait, there's more!



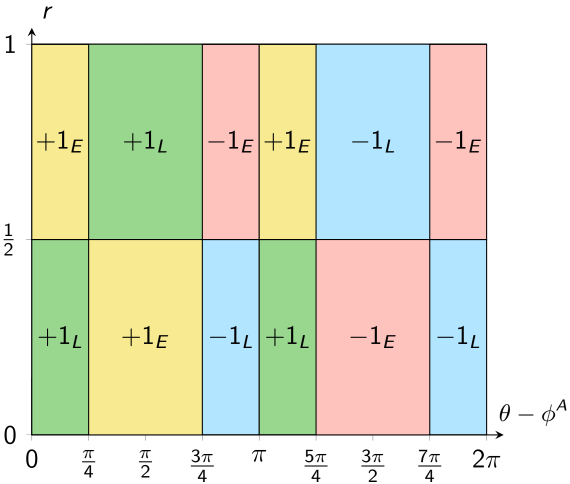
Let's go back to Alice's model and let $p \to 0$.

But wait, there's more!



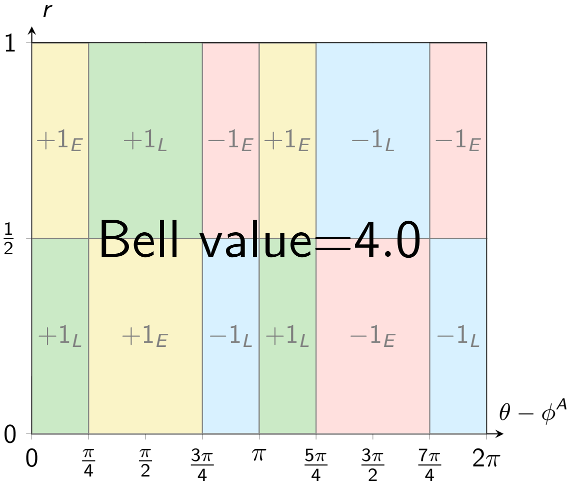
Let's go back to Alice's model and let $p \to 0$.

But wait, there's more!



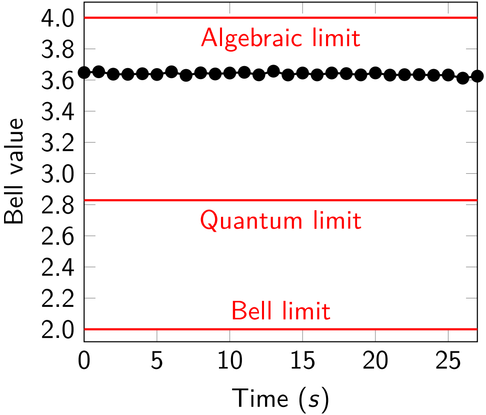
...which will lead to a model like this.

But wait, there's more!



...which will lead to a model like this.

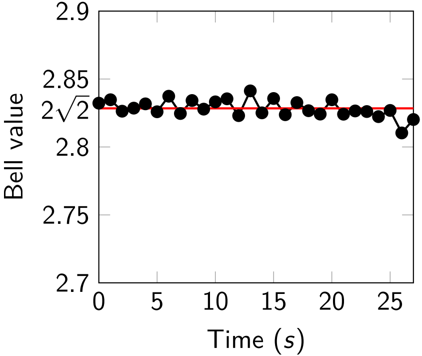
Extreme violations are possible



The maximum experimental Bell value is as high as 3.6386 ± 0.0096, imitating a Popescu-Rohrlich box. Efficiency is still at 97.6 %.

We can tune the attack to compensate for noise

- The first attack produced a Bell value of 2.5615 ± 0.0064 when we really wanted $2\sqrt{2} = 2.828\ldots$.
- However, Eve is free to combine pulses and phases to produce *any* Bell value between 0 and 3.6386 ± 0.0096.



Are there any countermeasures?

Our attacks works even if detectors have 100 % efficiency!

- Fast switching[1]: Not good enough[2].
- Chained Bell inequality[3]: Challenging experimental requirements[2].

The core of the problem for the Franson interferometer is the postselection loophole.

There are time-energy-entangled systems without postselection: Genuine energy-time entanglement[4], Check out poster number 23.

[1] Aerts et al., PRL 1999

[2] Jogenfors and Larsson, JPhysA 2014 (Accepted), arxiv:1103.6131

[3] Braunstein and Caves, Ann. Phys. 1990

[4] Lima et al., PRA 2010 and Cuevas et al., Nat. Comm. 2013

We have attacked and conquered the Franson interferometer

Our attack. . .

We have attacked and conquered the Franson interferometer

Our attack...

...can reach extreme Bell violations (up to 4)

We have attacked and conquered the Franson interferometer

Our attack...

...can reach extreme Bell violations (up to 4)

...has very high efficiency: 96.7 %.

We have attacked and conquered the Franson interferometer

Our attack. . .

. . . can reach extreme Bell violations (up to 4)

. . . has very high efficiency: 96.7 %.

. . . can compensate for noise.

We have attacked and conquered the Franson interferometer

Our attack. . .

. . . can reach extreme Bell violations (up to 4)

. . . has very high efficiency: 96.7 %.

. . . can compensate for noise.

. . . makes all output statistics look like the quantum-mechanical predictions.

We have attacked and conquered the Franson interferometer

Our attack...

. . . can reach extreme Bell violations (up to 4)

. . . has very high efficiency: 96.7 %.

. . . can compensate for noise.

. . . makes all output statistics look like the quantum-mechanical predictions.

. . . also works if the detectors are 100 % efficient.

We have attacked and conquered the Franson interferometer

Our attack. . .

. . . can reach extreme Bell violations (up to 4)

. . . has very high efficiency: 96.7 %.

. . . can compensate for noise.

. . . makes all output statistics look like the quantum-mechanical predictions.

. . . also works if the detectors are 100 % efficient.