APPLIED MATHEMATICS

10.1126/sciadv.1500793

Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution

Jonathan Jogenfors,[1]* Ashraf Mohamed Elhassan,[2]* Johan Ahrens,[2] Mohamed Bourennane,[2] Jan-Åke Larsson[1]†

Photonic systems based on energy-time entanglement have been proposed to test local realism using the Bell inequality. A violation of this inequality normally also certifies security of device-independent quantum key distribution (QKD) so that an attacker cannot eavesdrop or control the system. We show how this security test can be circumvented in energy-time entangled systems when using standard avalanche photodetectors, allowing an attacker to compromise the system without leaving a trace. We reach Bell values up to 3.63 at 97.6% faked detector efficiency using tailored pulses of classical light, which exceeds even the quantum prediction. This is the first demonstration of a violation-faking source that gives both tunable violation and high faked detector efficiency. The implications are severe: the standard Clauser-Horne-Shimony-Holt inequality cannot be used to show device-independent security for energy-time entanglement setups based on Franson's configuration. However, device-independent security can be reestablished, and we conclude by listing a number of improved tests and experimental setups that would protect against all current and future attacks of this type.

INTRODUCTION

A Bell experiment (*1*) is a bipartite experiment that can be used to test for preexisting properties that are independent of the measurement choice at each site. Formally speaking, the experiment tests if there is a "local realist" description of the experiment that contains these preexisting properties. Such a test can be used as the basis for security of quantum key distribution (QKD) (*2*, *3*). QKD uses a bipartite quantum system shared between two parties (Alice and Bob) that allows them to secretly share a cryptographic key. The first QKD protocol (BB84) (*2*) is based on quantum uncertainty (*4*) between noncommuting measurements, usually of photon polarization. The Ekert protocol (E91) (*3*) bases security on a Bell test instead of the uncertainty relation. Such a test indicates, through violation of the corresponding Bell inequality, a secure key distribution system. This requires quantum entanglement, and because of this, E91 is also called entanglement-based QKD.

To properly show that an E91 cryptographic system is secure or, alternatively, that no local realist description exists of an experiment, a proper violation of the associated Bell inequality is needed. As soon as a proper violation is achieved, the inner workings of the system is not important anymore, a fact known as device-independent security (*5*, *6*) or a loophole-free test of local realism (*7*). In the security context, the size of the violation is related to the amount of key that can be securely extracted from the system. However, a proper (loophole-free) violation is difficult to achieve. For long-distance experiments, photons are the system of choice and one particularly difficult problem is to detect enough of the photon pairs; this is known as the efficiency loophole (*8*–*10*).

If the violation is not good enough, there may be a local realist description of the experiment, giving an insecure QKD system. Even worse, an attacker could control the QKD system in this case. One particular example of this occurs when using avalanche photodetectors (APDs), which are the most commonly used detectors in commercial QKD systems: these detectors can be controlled by a process called "blinding" (*11*), which enables control via classical light pulses. When using photon polarization in the system, and if the efficiency is low enough in the Bell test, the quantum-mechanical prediction can be faked in such a controlled system (*12*, *13*). This means that the (apparent) Bell inequality violation can be faked, making a QKD system seem secure while it is not. Note that a proper (loophole-free) violation cannot be faked in this manner.

Here, we investigate energy-time entanglement–based systems in general and the Franson interferometer (*14*) in particular. Traditional polarization coding is sensitive to polarization effects caused by optical fibers (*15*), whereas energy-time entanglement is more robust against this type of disturbance. This property has led to an increased attention to systems based on energy-time entanglement because it allows a design without moving mechanical parts, which reduces complexity in practical implementations. A number of applications of energy-time entanglement, such as QKD, quantum teleportation, and quantum repeaters are described by Gisin and Thew (*16*). In particular, Franson-based QKD has been tested experimentally by a number of research groups (*17*–*22*).

It is already known that a proper Bell test is more demanding to achieve in energy-time entanglement systems with postselection (*23*, *24*), but certain assumptions on the properties of photons also reduce the demands to the same level as for a photon polarization–based test (*25*, *26*). The property in question is the particle-like behavior of the photon: it does not "jump" from one arm of an interferometer to the other. Clearly, classical light pulses cannot jump from one arm to the other, so the question arises: Is it at all possible to control the output of the detectors using classical light pulses to make them fake the quantum correlations? Below, we answer this question in the positive and give the details of such an attack and its experimental implementation.

Moreover, not only are faked quantum correlations possible to reach at a faked detector efficiency of 100%, but also, it is even possible to fake the extreme predictions of nonlocal Popescu-Rohrlich (PR) boxes (*27*) at this high detector efficiency. These predictions reach the algebraic

[1]Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden.
[2]Department of Physics, Stockholm University, 106 91 Stockholm, Sweden.
*These authors contributed equally to this work.
†Corresponding author. E-mail: jan-ake.larsson@liu.se

maximum 4 of the CHSH (Clauser-Horne-Shimony-Holt) inequality and would make a QKD system user suspicious; an attacker would, of course, not attempt to exceed the quantum bound $2\sqrt{2}$ (*28*). Finally, there are countermeasures that reestablish unconditional security, and we list a few examples, see the study of Jogenfors and Larsson (*24*) for a more complete list.

A Bell test of device-independent security, alternatively local realism, is always associated with a Bell inequality. The relevant part of the E91 QKD protocol up to and including the Bell test looks as follows. The general setup is a central source connected to two measurement sites, one at Alice and the other at Bob. The source prepares an entangled quantum state and distributes it to Alice and Bob, who each can choose between a number of measurement settings for their devices. The output can take the values −1, 0, or +1, denoting, for example, horizontal polarization, nondetection, and vertical polarization. Here, we are considering a pulsed source so that there are well-defined experimental runs and, therefore, also well-defined nondetection events. Alice selects a random integer $j \in \{1, 2, 3\}$ and performs the corresponding measurement A_j. Bob does the same with a random number $k \in \{2, 3, 4\}$ and measurement B_k. The quantum state and measurements are such that if $j = k$, then the outcomes are highly (anti-)correlated. This preparation and measurement process is performed over and over again until enough data have been gathered.

After a measurement batch has been completed, Alice and Bob publicly announce which settings j and k were used (but not the corresponding outcomes). They can then determine which measurements used the same settings $j = k$ and use the highly (anti-)correlated outcomes for key generation. The remaining outcomes corresponding to $j \neq k$ can be used for security testing in the Bell-CHSH (*1*, *29*) inequality

$$S_2 = |E(A_1B_2) + E(A_3B_2)| + |E(A_3B_4) - E(A_1B_4)| \leq 2 \quad (1)$$

where $E(A_jB_k)$ is the expected value of the product, often called "correlation" in this context. If the experimental S_2 is larger than 2, then there is a violation and the system is secure; there can be no local realist description of the experiment. The size of the violation is related to the output key rate; the maximal quantum prediction is $2\sqrt{2}$.

However, a proper violation is difficult to achieve. There are a number of ways that the test can give $S_2 > 2$ but still fail, known as loopholes (*7*). The most serious one is the detector efficiency loophole, wherein nondetections or zeros are not properly taken into account. If the zeros are ignored, conditioning on detection at both sites gives the conditional correlation $E(A_jB_k|\text{coinc.})$ and a modified bound (*9*, *10*)

$$S_{2,c} = |E(A_1B_2|\text{coinc.}) + E(A_3B_2|\text{coinc.})| + |E(A_3B_4|\text{coinc.}) - E(A_1B_4|\text{coinc.})| \leq \frac{4}{\eta} - 2 \quad (2)$$

The efficiency η is the ratio of coincidences to local detections (*10*) and needs to be above 82% for the quantum value to give a violation. This is ignored in current experiments, with almost no exception (*30*–*32*). In the context of QKD, ignoring the zeros is allowed only if the attacker (Eve) cannot control the detectors to make no-detections depend on the local settings j and k. Unfortunately, the commonly used APDs can be controlled (*11*, *13*) unless extra precautions are taken.

For this study, we have investigated a quantum device based on energy-time entanglement with postselection. Although the results presented below are acquired from this particular device, the results apply to any such system. The Franson interferometer (*14*) is shown in Fig. 1 and is built around a source emitting time-correlated photons to both Alice and Bob. The unbalanced Mach-Zehnder interferometers have a time difference ΔT between the paths. In our pulsed setting, the time difference between a late and an early source emission is ΔT, giving rise to interference between the cases "early source emission, photons take the long path" and "late source emission, photons take the short path." There will be no interference if the photons "take different paths" through the analysis stations, and those events are discarded as noncoincident in a later step.

The analysis stations have variable phase modulators, and the setting choices are ϕ_j^A for measuring A_j at Alice and ϕ_k^B for measuring B_k at Bob. The quantum state is such that, given coincident detection, the correlation between A_j and B_k is high if $\phi_j^A + \phi_k^B = 0$. In the absence of noise, the correlation between Alice's and Bob's outcomes will be (*14*)

$$E(A_jB_k|\text{coinc.}) = \cos(\phi_j^A + \phi_k^B) \quad (3)$$

This again violates the CHSH inequality (*1*), but only if the postselection is ignored (*23*). When postselection is taken into account, one arrives at the inequality (*2*) with η = 50%, giving a bound of 6, which is no restriction. The question now is if Eve can control the system and fake the violation.

RESULTS

Using classical pulses of light as described in the Materials and Methods section, Alice and Bob measure a Bell value of

$$S_2 = 2.5615 \pm 0.0064 \quad (4)$$

which clearly violates the Bell bound 2. Figure 2 shows the variation of S_2 over 27 s as a solid black line. The stand-alone detectors have a faked efficiency of 100% when blinded; however, the detectors do not have identical optical and electrical properties. A slight adjustment of optical blinding power has therefore been used to avoid having both detectors

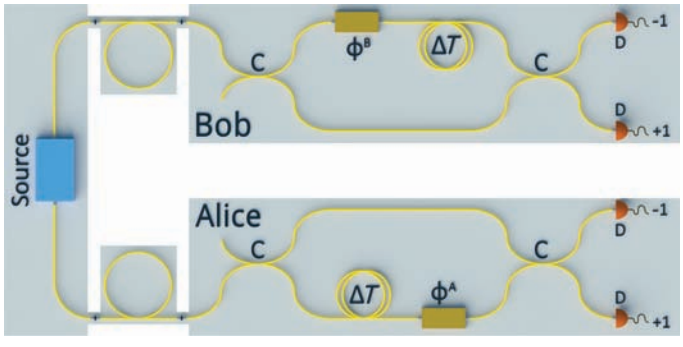


Fig. 1. Experimental setup of the Franson interferometer. The setup consists of a source, 2 × 2 couplers (C), delay loops (Δ*T*), phase modulators ϕ^A and ϕ^B, and detectors (D).

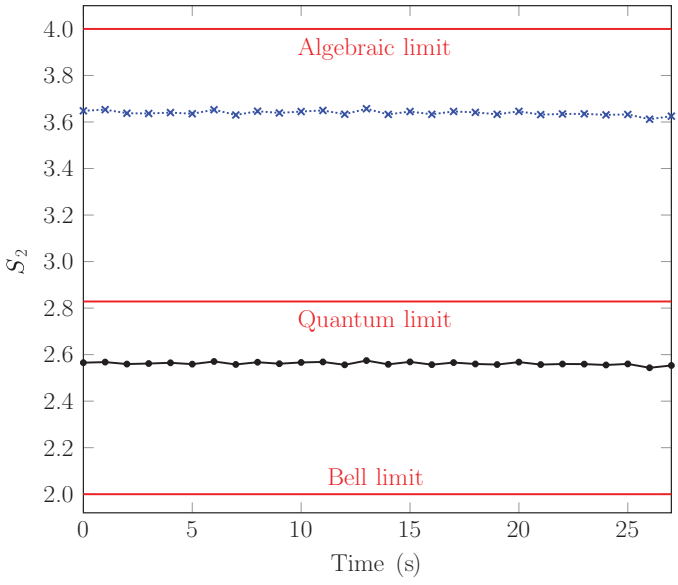


Fig. 2. The faked Bell value of our source is 2.5615 ± 0.0064 (solid black line), which clearly violates the CHSH inequality $S_2 \leq 2$. It is possible to increase the faked Bell value up to 3.6386 ± 0.0096 (dotted blue line, data for time slots where $p \leq r < 1/2 - p$ or $1/2 + p \leq r < 1 - p$). In both cases, the faked efficiency is 97.6%. Each point in the diagram corresponds to the S_2 value for 1 s worth of data.

click simultaneously. This gives a slight reduction in efficiency. Our source has a repetition rate of 5 kHz, and the average rate of clicks is 4.88 kHz, giving an average faked efficiency of 97.6%. The experimental Bell value is lower than the quantum prediction $2\sqrt{2}$ because of noise, most of which is due to unwanted clicks because pulses below the threshold are close to the threshold and are thus sensitive to small-intensity variations of the lasers.

Adjusting the source to produce fake nonlocal PR boxes (*27*) gives a faked Bell value of

$$S_2 = 3.6386 \pm 0.0096 \quad (5)$$

which is even beyond the quantum bound $2\sqrt{2}$. This is plotted in Fig. 2 as a dotted blue line. The faked efficiency remains at 97.6%, and noise still lowers the value from the ideal 4. As previously mentioned, Eve is free to combine pulses and phases at will to produce any Bell value between 0 and the above value 3.63. If the noise rate of the system is known, she can compensate by aiming for a higher Bell value and letting the noise bring it back down. This allows her to reach a faked Bell value that is indistinguishable from $2\sqrt{2}$.

DISCUSSION

Our faked Bell value seemingly violates the Bell-CHSH inequality, even though we are dealing with outcomes produced by classical light, that is, a local realist model. The more appropriate Bell inequality (2) for conditional correlations is clearly ineffective as a test of device-independent security with energy-time entanglement that uses postselection. The bound is too high. We need to improve the security tests in such a way that they unequivocally show security so that they can give a loophole-free violation of local realism.

An intuitive countermeasure to our attack is to add a power monitor to the analysis station that detects if the incoming light is too bright. If such an anomaly is detected, Alice and/or Bob are alerted and discard the relevant measurement outcomes. This modified Franson interferometer would not be vulnerable to the specific attack as described so far; however, it does not solve the postselection loophole, which is the actual issue at hand. Intuitive countermeasures such as power monitors were discussed by Lydersen *et al.* (*33*), who note that attacks can be adapted to such modifications ("a power meter at Bob's entrance…will not reveal the after-gate attack"). A similar argument already appears in the study of Lydersen *et al.* (*11*). In addition, Lydersen *et al.* (*34*) argue that loopholes should be countered by modifying the security proofs, and not by requiring manufacturers to make "frequent, possibly costly upgrades to their systems."

If we want keep the Franson interferometer unchanged, we need to use "fast switching" (*23*, *24*) and Pearle-Braunstein-Caves chained Bell inequalities (*8*, *35*) modified to apply under postselection. Fast switching refers to changing the phase setting so frequently that it is possible to have different phase settings for the two possible time delays, see Jogenfors and Larsson (*24*) for details. The chained inequalities are weakened but still produce a usable bound even after postselection on coincidence

$$\begin{aligned} S_{N,\mathrm{F}} = \; & |E(A_1B_2|\text{coinc.}) + E(A_3B_2|\text{coinc.})| + \\ & |E(A_3B_4|\text{coinc.}) + E(A_5B_4|\text{coinc.})| + \\ & \cdots + \\ & |E(A_{2N-1}B_{2N}|\text{coinc.}) - E(A_1B_{2N}|\text{coinc.})| \leq \\ & 2N-1. \end{aligned} \quad (6)$$

The standard inequalities do not condition on coincidence as is needed here, and they also have the bound $2N - 2$, which is more restrictive. Inequality (6) only gives the upper bound $S_{2,\mathrm{F}} \leq 3$ for the Bell-CHSH value, so the standard test is not useful even with fast switching. However, the quantum-mechanical prediction $S_{N,\mathrm{F}} = 2N\cos(\pi/2N)$ does violate this if $N \geq 3$, even though the violation is smaller than the standard Bell test. This reestablishes device-independent security for energy-time entangled QKD. In practice, though, the experimental requirements are high because the lowest acceptable visibility is 94.64% (*24*).

A better solution would be to eliminate the core problem: the postselection loophole. One alternative is the use of "hugging" interferometers (*24*, *36*) that gives an energy-time entangled interferometer with postselection, but without a postselection loophole. This setup is often referred to as "genuine energy-time entanglement." The drawback is the requirement of not one, but two fiber links each to Alice and Bob. A Bell violation has been shown experimentally (*37*), even with 1-km fiber length (*38*). Another alternative is to replace the first beam splitter of the analysis station with a movable mirror (*24*, *39*, *40*). This setup does not require postselection at all, and therefore, the original CHSH inequality is applicable.

In conclusion, we reiterate that Bell tests are a cornerstone of QKD and are necessary for device-independent security. Device-independent Bell inequality violation must be performed with care to avoid loopholes. Energy-time entanglement has the distinct advantage over polarization in that time and energy are more easily communicated over long distances than polarization. Therefore, energy-time entanglement may be preferable as a quantum resource to perform reliable key distribution.

Here, we have shown that QKD systems based on energy-time entanglement with postselection are vulnerable to attack if the corresponding security tests use the original CHSH inequality. Eve blinds the detectors

and uses a local hidden variable (LHV) model to fool Alice and Bob into thinking that their system violates Bell's inequality even though there is no entanglement. Eve only needs access to the source device, not Alice's or Bob's measurement devices or laboratory equipment (including computers). Still, she fully controls the key output and breaks the security of the Franson system without Alice or Bob noticing.

Our attack has been performed with a faked detector efficiency of 97.6%, which is high enough to avoid the fair sampling assumption. It also shows that our Bell violation is not due to an artificially low detector efficiency apart from the inherent postselection. We can compare this to the study of Gerhardt *et al.* (*13*), where the faked detector efficiency was 50% when using active basis choice; that attack has an upper limit of 82.8% (*9*, *10*). Even if the faked detection efficiency in our experiment were 100%, our attack would work because the inherent postselection of the Franson interferometer removes half of the events.

In addition, our attack can produce a Bell value $S_2 = 4$ at any efficiency. Given the noise rate of a QKD device, Eve can fine-tune the attack to imitate the quantum prediction to any accuracy, therefore evading detection in a simple and effective way. It remains a fact that fast switching will restrict the Bell value to be below 3, but this fine-tuning ability shows the level of control an attacker can exert onto the system.

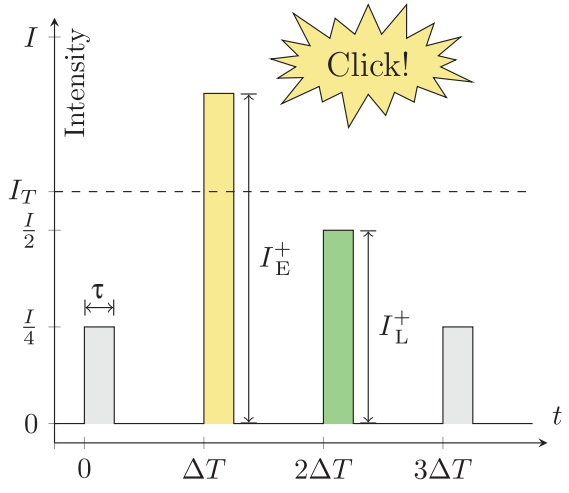
To build a device-independent QKD system based on energy-time entanglement, the designer will either have to use fast switching and replace the CHSH inequality with stronger tests such as modified Pearle-Braunstein-Caves inequalities, or use a system that does not exhibit the postselection loophole. These suggested improvements both have the essential property of establishing device independence without requiring additional assumptions and thereby maintain the powerful simplicity of device-independent QKD.

MATERIALS AND METHODS

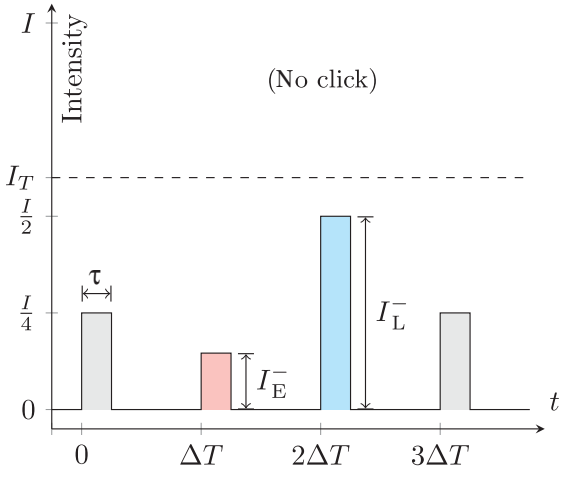
Eve performs the attack by replacing the source with a faked-state generator that blinds the APDs (see Fig. 3) and makes them click at chosen instants in time. The blinding is accomplished using classical light pulses superimposed over continuous-wave (CW) illumination (*11*). In normal operation, an APD reacts to even a single incoming photon. A photon that enters the detector will create an avalanche of electrical current, which results in a signal, or "click," when the current crosses a certain threshold. The avalanche current is then quenched by lowering the APD bias voltage to below the breakdown voltage, making the detector ready for another photon and resulting in the so-called Geiger mode operation.

Under the influence of CW illumination, the quenching circuitry will make the current through the APDs proportional to the power of the incoming light. This will change the behavior of the APD into the so-called linear mode, more similar to a classical photodiode. It will no longer react to single photons, nor register clicks in the usual Geiger-like way and is therefore said to be "blind." The appropriate choice of CW illumination intensity will make the APD insensitive to single photons, yet still register a click when a bright pulse of classical light is superimposed over the CW illumination (*11*).

What remains is to construct classical light pulses that will give clicks in the way that Eve desires, violating the Bell inequality test for the Franson interferometer. Eve uses pulses with intensity I and pulse length $\tau \ll \Delta T$ intermingled with the CW light that blinds the APDs. A single pulse emitted by the source will be split when traveling through the interferometer, resulting in two pulses in each output port with intensity $I/4$ each. Alternatively, if two pulses are emitted, separated by ΔT and with phase difference ω, these two pulses will split to three. The middle pulse of the three is built up by two parts, so that the ±1 outputs show interference



A Constructive interference at the + output gives a large early time slot intensity and a corresponding click.



B Destructive interference at the − output gives a small early time slot intensity and no corresponding click.

Fig. 3. The blinding attack causes the detector to click only for pulses of greater intensity than I_T. If Eve sends three pulses of equal intensity I, they will arrive as four after the interferometer. By changing the phase shifts ω_E and ω_L between the pulses at the source, she can control the intensity of the early and late middle pulses at the ± output ports, giving clicks as desired. Here, $\phi = 0$, $\omega_E = \pi/8$, and $\omega_L = \pi/4$. The first and last pulses have a constant intensity of $I/4$.

$$I^{+}(\phi,\omega) = I\,\cos^2\left(\frac{\phi+\omega}{2}\right)$$
$$I^{-}(\phi,\omega) = I\,\sin^2\left(\frac{\phi+\omega}{2}\right) \quad (7)$$

where ϕ is the phase setting of the local analysis station. The chosen ω controls the ϕ dependence of the output. For example, if I is just less than $2I_T$ and $\omega = 0$, there will be a +1 click for $|\phi| < \pi/2$ and a −1 click otherwise.

However, this is not enough to fake the Bell violation, because the detection time needs to depend on the local setting (*23*). To enable this, Eve makes the source emit a group of three pulses separated by ΔT, with phase difference ω_E between the first and second pulse, and ω_L between the second and third pulse. When this pulse train passes through the interferometer, the output is four pulses, where the two center pulses have controllable intensity because of interference. The intensities for these two (early/late) pulses are

$$I_E^{+}(\phi\omega_E) = I\,\cos^2\left(\frac{\phi+\omega_E}{2}\right)$$
$$I_E^{-}(\phi\omega_E) = I\,\sin^2\left(\frac{\phi+\omega_E}{2}\right)$$
$$I_L^{+}(\phi\omega_L) = I\,\cos^2\left(\frac{\phi+\omega_L}{2}\right) \quad (8)$$
$$I_L^{-}(\phi\omega_L) = I\,\sin^2\left(\frac{\phi+\omega_L}{2}\right)$$

For example, with the same choice of I as above, $\omega_E = 0$, and $\omega_L = \pi/2$, there will be an early +1 click if $\phi = 0$, and a late −1 click if $\phi = \pi/2$. Note that the pulse trains to Alice and Bob can be chosen independently.

The last step of the attack is to use the LHV model in Fig. 4, which is a discretized version of an earlier known model (*23*). This LHV model prescribes the distribution of the sign and time slot of outcomes for Alice and Bob given local settings ϕ^A and ϕ^B. Single-particle outcomes obtained in this way follow the quantum predictions (*23*). The parameter p controls the desired level of violation, and θ and r are hidden variables that are chosen randomly for each experimental trial.

For the purposes of our attack, we choose to focus on the present Bell test: $\phi_1^A = 0, \phi_3^A = \pi/2, \phi_2^B = -\pi/4$, and $\phi_4^B = -3\pi/4$, so that the hidden variable θ is a multiple of $\pi/4$. Eve randomly chooses hidden variables r and θ as stated in Fig. 4, and reads off the desired results for the two settings at Alice.

If the results are in the same time slot, she uses two pulses and can directly calculate the needed phase difference. If the results are in different time slots (this only happens for Alice), Eve uses three pulses and calculates the two phase differences. The same r and θ are used to calculate the phase difference for Bob. Repeating this procedure will produce random outcomes (to Alice and Bob) that give exactly the quantum predictions for the mentioned settings, violating the Bell-CHSH inequality.

Joint Alice-Bob trials were performed with the pulse amplitudes as described in Eqs. 7 and 8 and depicted in Fig. 3. At the desired detector and time slot, a "click" will be forced (Fig. 3A) by constructive interference, whereas destructive interference causes "no click" (Fig. 3B). The sampling time used was 1 s, and each experiment was run for at least 27 s (see Fig. 2). At each point in time, the joint probabilities of Alice's and Bob's outcomes are computed from the detector counts, and these were then used to determine the Bell value. Note that the early and late time slots are measured in different experimental runs.

By adjusting the parameter p of the LHV model, we can go even further and produce Bell values up to and including the value 4 (see Fig. 4). Of course, Alice and Bob would be suspicious if they measured this value because their experiment does not contain nonlocal PR boxes (*27*). Eve would instead tune the Bell violation to compensate for inherent noise by raising the value just enough to reach $2\sqrt{2}$.

EXPERIMENTAL SETUP

The attack was experimentally implemented as shown in Fig. 5 and is built using standard fiber optic components. The CW is produced by a CW laser, whereas the pulses are created by a pulsed laser. These two light sources are combined at a fiber optic 2 × 2 coupler and then split into one beam for Alice and one for Bob. Each of these beams is then sent into a fiber optic 3 × 3 coupler (tritters) that equally divides them into three arms. The first arm consists of a ΔT delay loop and a phase modulator ω_E, the second arm has two ΔT delay loops and a phase modulator ω_M (so that $\omega_L = \omega_M - \omega_E$), whereas the third arm performs

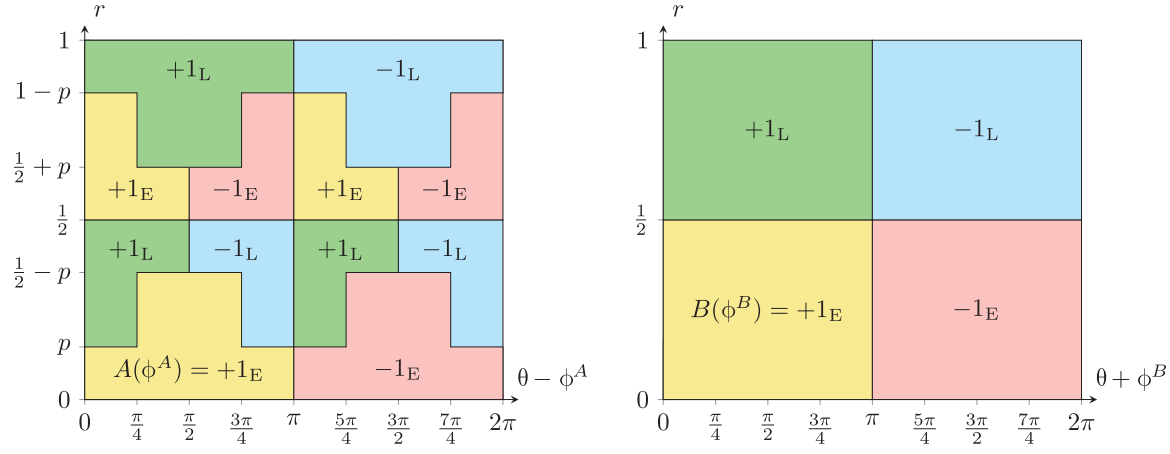


Fig. 4. Discretized LHV model (*23*) that can give any Bell value between 2 and 4. The hidden variables are $0 \le r < 1$ (a real number in the unit interval) and $\theta = n\frac{\pi}{4}$, where $0 \le n \le 7$ is an integer. The parameter $0 \le p \le 1/4$ can be chosen freely, and the output Bell value is $S_2 = 4 - 8p$, so that the "classical" $S_2 = 2$ is obtained with $p = 1/4$, the "quantum" $S_2 = 2\sqrt{2}$ is obtained with $p = (2 - \sqrt{2})/4$ (as in the figure), and the "nonlocal box" $S_2 = 4$ is obtained with $p = 0$, all at 100% faked efficiency and 50% postselection.

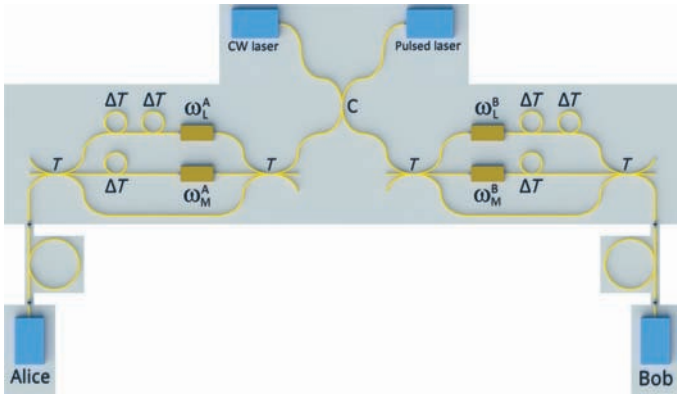


Fig. 5. Experimental setup of the attack on the Franson interferometer. The source consists of a CW laser for blinding the detectors, a pulsed laser for generating the bright classical light pulses, fiber optic couplers (C) delay loops (ΔT), phase modulators (ω and ϕ), and detectors (D). Alice and Bob have the same analysis stations as in Fig. 1.

no action. The three arms are then combined by a second 3×3 coupler into one output port that creates the output of the faked-state source generator.

The source sends bright light pulses with the setting and phase difference(s) to Alice's and Bob's analysis stations in the Franson interferometer. Each of the two analysis stations is constructed in a similar fashion: two fiber optic 2×2 couplers and one delay loop ΔT and a phase modulator ϕ^A (Alice's side) or ϕ^B (Bob's side).

The detectors used in the experiment are commercial products from Princeton Lightwave. These detectors are InGaAs avalanche photodiodes that use Geiger and biased pulse modes at the operating temperature 218 K. The detection wavelength range is 1300 to 1550 nm, giving a maximum detection efficiency of 20% at 1550 nm. The dark count rate is 5×10^{-5} ns^{-1}. Although the attack is demonstrated on this specific detector, other detector types using similar devices and circuitry are vulnerable as well.

Because the CW power becomes unevenly distributed between detectors, the efficiency of the blinding was affected. This imbalance was avoided by installing digital variable attenuators at the output ports. In addition, optical isolators were placed in front of the detectors to prevent crosstalk. The interferometers are passively stabilized and placed in a thermally and mechanically isolated environment in the form of a metal enclosure lined with styrofoam. This isolation has the effect of reducing phase drift, giving a 30-s time window in which measurements can be performed before a manual recalibration is required.

REFERENCES AND NOTES

1. J. S. Bell, On the Einstein-Podolsky-Rosen paradox. *Physics* **1**, 195–200 (1964).
2. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, paper published in the Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984.
3. A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
4. W. Heisenberg, Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik* **43**, 172–198 (1927).
5. A. Acín, N. Gisin, L. Masanes, From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
6. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
7. J.-Å. Larsson, Loopholes in Bell inequality tests of local realism. *J. Phys. A* **47**, 424003 (2014).
8. P. M. Pearle, Hidden-variable example based upon data rejection. *Phys. Rev. D* **2**, 1418–1425 (1970).
9. A. Garg, N. D. Mermin, Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Phys. Rev. D* **35**, 3831–3835 (1987).
10. J.-Å. Larsson, Bell's inequality and detector inefficiency. *Phys. Rev. A* **57**, 3304–3308 (1998).
11. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
12. J.-Å. Larsson, A practical Trojan Horse for Bell-inequality-based quantum cryptography. *Quantum Inf. Comput.* **2**, 434–442 (2002).
13. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, C. Kurtsiefer, Experimentally faking the violation of Bell's inequalities. *Phys. Rev. Lett.* **107**, 170404 (2011).
14. J. D. Franson, Bell inequality for position and time. *Phys. Rev. Lett.* **62**, 2205–2208 (1989).
15. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
16. N. Gisin, R. Thew, Quantum communication. *Nat. Photon.* **1**, 165–171, (2007).
17. Z. Y. Ou, X. Y. Zou, L. J. Wang, L. Mandel, Observation of nonlocal interference in separated photon channels. *Phys. Rev. Lett.* **65**, 321–324 (1990).
18. P. R. Tapster, J. G. Rarity, P. C. M. Owens, Violation of Bell's inequality over 4 km of optical fiber. *Phys. Rev. Lett.* **73**, 1923–1926 (1994).
19. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Violation of Bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.* **81**, 3563–3566 (1998).
20. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, N. Gisin, Distribution of time-bin entangled qubits over 50 km of optical fiber. *Phys. Rev. Lett.* **93**, 180502 (2004).
21. T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, H. Takesue, Entanglement distribution over 300 km of fiber. *Opt. Express* **21**, 23241–23249 (2013).
22. D. Grassani, S. Azzini, M. Liscidini, M. Galli, M. J. Strain, M. Sorel, J. E. Sipe, D. Bajoni, Micrometer-scale integrated silicon source of time-energy entangled photons. *Optica* **2**, 88–94 (2015).
23. S. Aerts, P. Kwiat, J.-Å. Larsson, M. Zukowski, Two-photon Franson-type experiments and local realism. *Phys. Rev. Lett.* **83**, 2872–2875, (1999).
24. J. Jogenfors, J.-Å. Larsson, Energy-time entanglement, element of reality, and local realism. *J. Phys. A* **47**, 424032 (2014).
25. J. D. Franson, Inconsistency of local realistic descriptions of two-photon interferometer experiments. *Phys. Rev. A* **61**, 012105 (1999).
26. J. D. Franson, Nonclassical nature of dispersion cancellation and nonlocal interferometry. *Phys. Rev. A* **80**, 032119 (2009).
27. S. Popescu, D. Rohrlich, Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379–385 (1994).
28. B. S. Cirel'son, Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4**, 93–100 (1980).
29. J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
30. M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, A. Zeilinger, Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227–230 (2013).
31. B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, P. G. Kwiat, Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
32. J.-Å. Larsson, M. Giustina, J. Kofler, B. Wittmann, R. Ursin, S. Ramelow, Bell-inequality violation with entangled photons, free of the coincidence-time loophole. *Phys. Rev. A* **90**, 032107 (2014).
33. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 801 (2010).
34. L. Lydersen, V. Makarov, J. Skaar, Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography" [Appl. Phys. Lett. 98, 231104 (2011)]. *Appl. Phys. Lett.* **99**, 196101 (2011).
35. S. L. Braunstein, C. M. Caves, Wringing out better Bell inequalities. *Ann. Phys.* **202**, 22–56 (1990).
36. A. Cabello, A. Rossi, G. Vallone, F. De Martini, P. Mataloni, Proposed Bell experiment with genuine energy-time entanglement. *Phys. Rev. Lett.* **102**, 040401 (2009).
37. G. Lima, G. Vallone, A. Chiuri, A. Cabello, P. Mataloni, Experimental Bell-inequality violation without the postselection loophole. *Phys. Rev. A* **81**, 040101(R) (2010).
38. A. Cuevas, G. Carvacho, G. Saavedra, J. Cariñe, W. A. T. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima, G. B. Xavier, Long-distance distribution of genuine energy-time entanglement. *Nat. Commun.* **4**, 2871 (2013).
39. J. Brendel, N. Gisin, W. Tittel, H. Zbinden, Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **82**, 2594–2597 (1999).
40. W. Tittel, J. Brendel, N. Gisin, H. Zbinden, Long-distance Bell-type tests using energy-time entangled photons. *Phys. Rev. A* **59**, 4150–4163 (1999).

Funding: J.J. and J.-Å.L. were supported by Center for Industrial Information Technology (CENIIT) at Linköpings Universitet. M.B., J.A., and A.M.E. were supported by the Swedish

Research Council, Ideas Plus (Polish Ministry of Science and Higher Education grant IdP2011 000361), and ADOPT. **Author contributions:** J.-Å.L. conceived the idea. J.J. and J.-Å.L. developed the theory. M.B., J.A., J.J., and A.M.E. designed the experiment. A.M.E. performed the experiment. J.J. and A.M.E. analyzed the data. J.J., J.-Å.L., and M.B. wrote the research article. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data used to obtain the conclusions in this paper are available in Dryad or presented in the paper and/or the Supplementary Materials.

Submitted 15 June 2015
Accepted 29 September 2015
Published 18 December 2015
10.1126/sciadv.1500793

Citation: J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, J.-Å. Larsson, Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution. *Sci. Adv.* **1**, e1500793 (2015).

Science Advances

Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution

Jonathan Jogenfors, Ashraf Mohamed Elhassan, Johan Ahrens, Mohamed Bourennane and Jan-Åke Larsson

Sci Adv **1** (11), e1500793.
DOI: 10.1126/sciadv.1500793