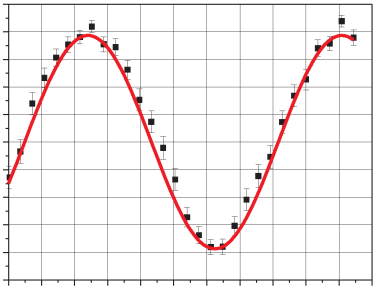
Distribution of time-bin entangled qubits over 50km of optical fiber



Verteilung von zeitverschränkten Qubits über 50km Glasfaser

Autor: N. Gisin et al.

Übersetzung: Dipl.- Ing. Björnstjerne Zindler, M.Sc.

www.Zenithpoint.de

Erstellt: 30. März 2023 – Letzte Revision: 30. Oktober 2024

Inhaltsverzeichnis

Literatur

[I.] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré and N. Gisin. Distribution of time-bin entangled qubits over 50 km of optical fiber, https://arxiv.org/abs/quant-ph/0404124.

---

1 Distribution of time-bin entangled qubits over 50km of optical fiber

[I.]

I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré and N. Gisin
Group of Applied Physics-Optique, University of Geneva, CH-1211, Geneva 4, Switzerland

We report experimental distribution of time-bin entangled qubits over 50km of optical fibers. Using actively stabilized preparation and measurement devices we demonstrate violation of the CHSH Bell inequality by more than 15 standard deviations without removing the detector noise. In addition we report a proof of principle experiment of quantum key distribution over 50km of optical fibers using entangled photon.

In the science of quantum information a central experimental issue is how to distribute entangled states over large distances. Indeed, most protocols in quantum communication require the different parties to share entanglement. The best-known examples are Quantum Teleportation [1] and Ekert's Quantum Key Distribution (QKD) protocol [2]. Note that even in protocols that do not explicitly require entanglement, like the BB84 QKD protocol [3], security proofs are often based on „virtual entanglement", i.e. on the fact that an ideal single photon source is indistinguishable from an entangled photon pair source in which one photon is used as a trigger [4]. From a more practical point of view, entanglement over significant distances can be used to increase the maximal distance a quantum state can cover, as in quantum repeater [5] and quantum relay [6] protocols. Finally, entanglement is also treated as a resource in the study of communication complexity [7].

As entanglement cannot be created by shared randomness and local operations, it must be somehow distributed. Recently there have been some proposals to use satellites for long distance transmission [8]. Also some experiments through open space have been performed either for QKD (over 50 m) [9] or for the transmission of entangled qubits (over 600 m) [10]. Despite the weather and daylight problems, this is an interesting approach. Another possibility, that we follow in this work, is to use the worldwide implemented optical fiber network. This, however, implies some constraints. One should operate at telecommunication wavelengths (1.3 or 1.55μm), in order to minimize losses in optical fibers, and the encoding of the qubits must be robust against decoherence in optical fibers. Likely the most adequate way to encode qubits is to use energy-time [11] or it's discrete version time-bin encoding [12]. The major drawback of this kind of encoding, compared to polarization type, is that the creation and the measurement is more complex: it relies on stable interferometers. In this letter we report a way to create and to measure time-bin entangled qubits which allows us to violate Bell inequalities over 50 km of optical fibers and to show a proof of principle for entanglement based QKD over long ranges. Moreover it allows to demonstrate stability of our entire set-up over several hours.

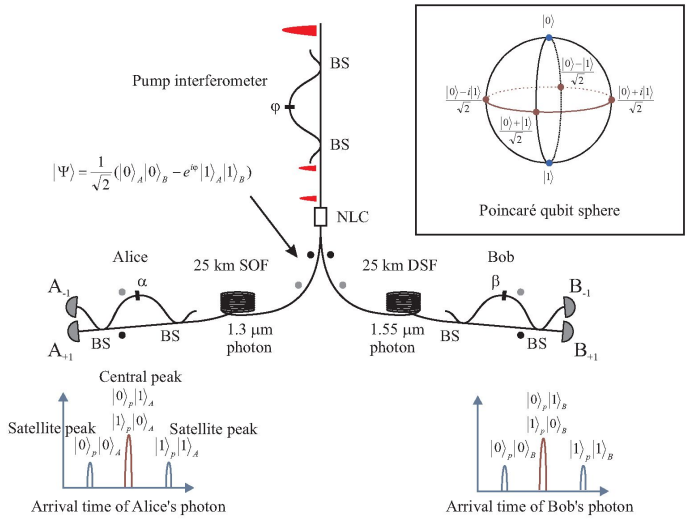


Fig. 1: Scheme of the experimental set-up. Time bin qubits are prepared by passing a fs pulse through the pump interferometer and a non-linear crystal (NLC). Eventually, a pair of entangled photons is created in the crystal. They are sent to Alice and Bob through 25.3 km of optical fibers. Alice and Bob analyze photons using interferometers equally unbalanced with respect to the pump interferometer. All three interferometers are built using passive 50-50 beam-splitters (BS). Alice's and Bob's detection times are also represented.

Let us first remind the reader how to create and measure time-bin entangled qubits. They are created by sending a short laser pulse first through an unbalanced interferometer (denoted as the pump

interferometer) and then through a non-linear crystal where eventually a pair of photons is created by spontaneous parametric down conversion (SPDC)(see Fig.1). The state can be written:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \cdot \left(|0\rangle_A |0\rangle_B - e^{i\cdot\varphi} |1\rangle_A |1\rangle_B\right) \tag{1}$$

where $|0\rangle$ represents a photon in the first time bin (having passed through the short arm) and $|1\rangle$ a photon in the second time-bin (having passed through the long arm). The index A and B represents Alice's and Bob's photon. The phase φ is defined with respect to a reference path length difference between the short and the long arm $\Delta\tau$. The photons A and B are then sent to Alice and Bob who perform projective measurements, by using a similar unbalanced interferometer. There are three detection times on Alice's (Bob's) detectors with the respect to the emission time of the pump laser (see Fig.1). The first and the last peak (denoted as satellite peaks) corresponds to events which are temporally distinguishable: the left (right) peak corresponds to a photon created in the first (second) time-bin which passed through the short (long) arm of Alice's interferometer. When detected in the left (right) satellite peak, the photon is projected onto the vector $|0\rangle$ ($|1\rangle$) (the poles on the Poincaré qubit sphere). Photons detected in the central peak can be either due to events where the created photon is in the first timebin and then it passes through the long arm of Alice's interferometer or due to events where the photon is created in the second time-bin and then passes through the short arm of Alice's interferometer. In this case the photon is projected onto the vector $|0\rangle + e^{i\alpha}|1\rangle$ (i.e. on the equator of the Poincaré qubit sphere). Note that when Alice records the central peak she does not observe single photon interference by changing the phase of her interferometer because which-path information can be found by recording the emission time of Bob's photon. With reference to experiments using polarization entangled photons, we refer to this as rotational invariance [13]. If Alice and Bob both record counts in their central peaks, they observe second order interference by changing either the phase in Alice's, in Bob's or in the pump interferometer. The coincidence count rate between Alice's and Bob's detectors $A_i B_j$, is then given by:

$$R_{A_i,B_j}(\alpha,\beta,\varphi) \propto 1 + i\cdot j\cdot V\cdot\cos(\alpha+\beta+\varphi) \tag{2}$$

where i and $j = \pm 1$ (see Fig.1) and V is visibility of the interference fringes (which can in principle reach the value of 1). We define the imbalance of the pump interferometer as the reference time difference $\Delta\tau$ between the first and the second time-bin, the phase φ is thus taken to be zero. The correlation coefficient is defined as:

$$E(\alpha,\beta) = \frac{\sum\limits_{i,j} i\cdot j\cdot R_{A_iB_j}(\alpha,\beta)}{\sum\limits_{i,j} R_{A_iB_j}(\alpha,\beta)} \tag{3}$$

and by inserting Eq.2 into Eq.3 the correlation coefficient becomes:

$$E(\alpha,\beta) = V\cdot\cos(\alpha+\beta) \tag{4}$$

The Bell inequalities define an upper bound for correlations that can be described by local hidden variable theories (LHVT). One of the most frequently used forms, known as the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [14], is:

$$S = \left|E(\alpha,\beta) + E\left(\alpha,\beta'\right) + E\left(\alpha',\beta\right) - E\left(\alpha',\beta'\right)\right| \leq 2 \tag{5}$$

Quantum mechanics predicts that S has a maximum value of $S = 2\sqrt{2}$ with $\alpha = 0^\circ, \alpha' = 90^\circ, \beta = 45^\circ$ and $\beta' = -45^\circ$. It has been also shown that when the correlation function has sinusoidal form of Eq.4 and when there is rotational invariance, the boundary condition of Eq.5 can be written as:

$$S = 2\sqrt{2}\cdot V \leq 2 \tag{6}$$

thus $V \geq \frac{1}{\sqrt{2}}$ implies violation of the CHSH Bell inequality, i.e. correlations can not be explained by LHVT.

Our experimental set-up is the following (see Fig.1): A 150 femtosecond laser pulse with a 710 nm wavelength and with a repetition rate of 75 MHz is first sent through an unbalanced, bulk, Michelson interferometer with an optical path difference of $\Delta\tau = 1.2ns$ and then through a type I LBO (lithium

triborate) non-linear crystal where collinear non-degenerate photon pairs at 1.3 and 1.55μm wavelength can be created by SPDC. The pump beam is then removed with a silicon filter and the pairs are coupled into an optical fiber. The photons are separated with a wavelength-division-multiplexer, the 1.3μm photon is sent through 25.3 km of standard optical fiber (SOF) to Alice and the 1.55μm photon through 25.3km of dispersion shifted fiber (DSF) to Bob [15]. Alice's photon is then measured with a fiber Michelson interferometer and detected by one of two liquid nitrogen cooled passively quenched Germanium avalanche photo-diodes (APD) A_{+1} or A_{-1}. Their quantum efficiency is of around 10% with 20 kHz of dark counts. In order to select only the central peak events and also to reduce the detector dark counts, a coincidence is made with the emission time of the laser pulse. This signal then triggers Bob's detectors (B_{+1} and B_{-1}) which are two InGaAs APDs (IdQuantique) working in so called gated mode. Although both detectors have similar quantum efficiencies of 20 %, one of the detectors (B_{+1}) dark count probability is two times smaller than the other one (B_{-1}), and is around 10^{-4} /ns. To reduce chromatic dispersion in optical fibres and the detection of multiple pairs [16], we use interference filters with spectral width of 10 nm for 1.3μm photons and 18 nm for the 1.55 μm photons. Using 70 mW of average input power (measured after the pump interferometer) the probability of creating an entangled qubit per pulse is around 8 %. Bob's analyzer is also a Michelson type interferometers built with optical fibers. To better control the phase and to achieve long term stability all three interferometers are passively and actively stabilized. Passive stabilization consists of controlling the temperature of each interferometer. Active stabilization consists of probing the interferometer's phase with a frequency stabilized laser at 1.534 μm (Dicos), and to lock them to a desired value via a feedback loop on a piezo actuator (PZA) included in each interferometer. In order to change path diff erence in the bulk pump-interferometer, one of the mirrors is mounted on a translation stage including a PZA with the range of around 4 μm. In the analyzing interferometers the long fiber path is wound around a cylindric PZA with a circumference variation range of 60 μm. Contrary to the bulk interferometer which is continuously stabilized, the phase of the fiber interferometers can not be stabilized during the measurement period. Thus we continuously alternate between measurement periods of 100seconds and stabilization periods of 5 seconds. This method allows us not only to stabilize the entire set-up during several hours, but also to have good control over the changes of both phases α and β .

In order to show a violation of the CHSH Bell inequality after 50 km of optical fibers, we proceed in two steps: first we scan Bob's phase β while Alice's phase α is kept constant. We obtain a raw visibility of around $78 \pm 1.6\%$ (see Fig.2) from which we can infer an S parameter of $S = 2.206 \pm 0.045$ (Eq.6) leading to a violation of the CHSH Bell inequality by more than 4 standard deviations. The coincidence count rate between any combination of detectors $A_i B_j$ is of around 3 Hz.

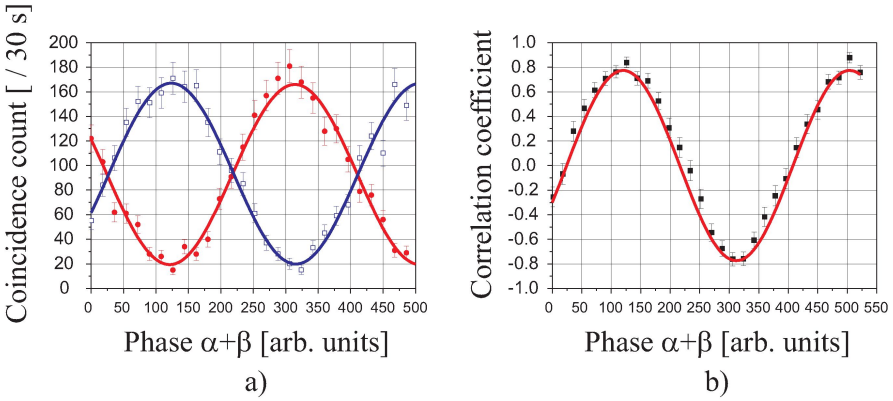


Fig. 2: a) Coincidence counts between detectors $A_{+1}B_{+1}$ (circles) and $A_{+1}B_{-1}$ (open squares) b) Correlation coefficient $E(\alpha,\beta)$ measured from four different coincidence counts (Eq.3). Alice's phase α is kept constant and Bob's phase β is scanned

The raw visibility of the correlation function is mainly reduced due to the creation of multiple pairs (around 9 %), due to accidental coincidence counts (related to dark counts of our detectors, around 8 %) and due to the misalignment of the interferometers (around 5 %). In principle one could reduce the creation of multiple pairs by reducing the input power, but then the coincidence count rate would also decrease.

With our new interferometers we are able to perform for the first time with time-bins the second step: measure the CHSH Bell inequality according to Eq.5, i.e. lock the phase to the desired value in

order to measure the four diff erent correlation coefficients one after the other. To reduce statistical fluctuations, we measure the correlation coefficient (Eq.3) during almost an hour for each setting. The obtained S parameter is $S = 2.185 \pm 0.006$ which shows a violation of the CHSH Bell inequality by more than 15 standard deviations (see Fig.3).

It has been proven that when the Bell inequality is violated the entangled photons can be used in quantum cryptography [17]. Our QKD protocol is analogous to the BB84 protocol using time-bin entangled photons [18]. Hence, Alice and Bob use two maximally conjugated measurement basis.

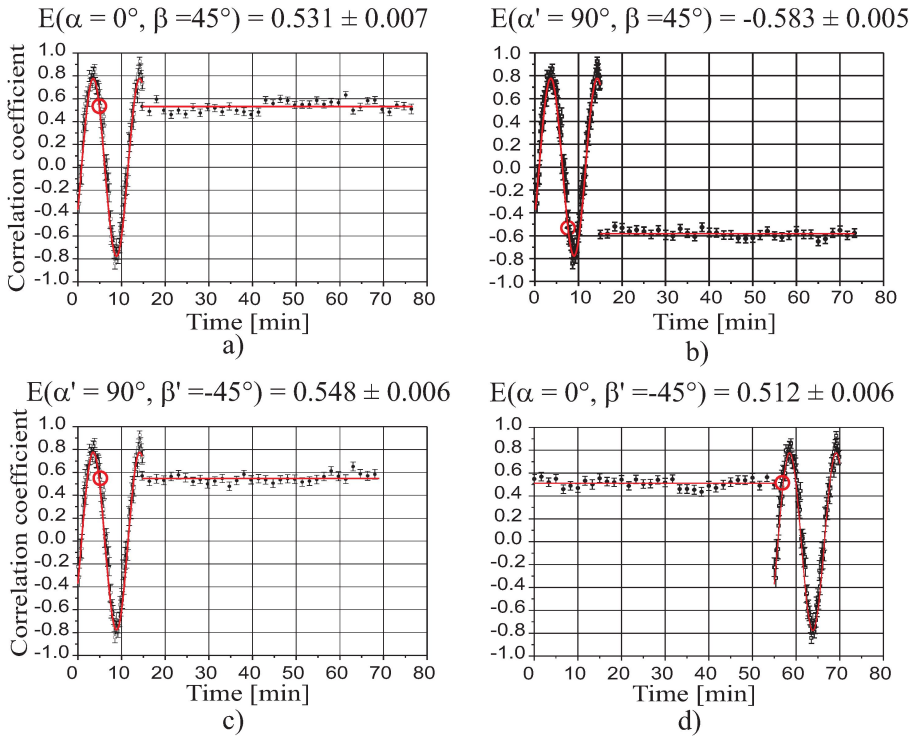


Fig. 3: Correlation coefficients for continuous scan and four different settings. Each data point is derived from a 100 s integration time of coincidence counts between four different combinations of two detectors (Eq.3). As α and β are defined relatively to the pump-interferometer's phase, we use the first three measurement a), b) and c) to define four different phases: $\alpha = 0°$, $\alpha' = 90°$, $\beta = 45°$ and $\beta' = -45°$. The last measurement d) completes the proof of a violation of the CHSH Bell inequality. The open circles represent the correlation coefficient value for which the CHSH Bell inequality would be maximally violated when the maximum visibility is 78 %.

The first basis is defined by two orthogonal vectors $|0\rangle$ and $|0\rangle$ represented on the poles of the Poincaré qubit sphere (Fig.1). The projection onto this basis is performed whenever a photon is detected in a satellite peak. Let us illustrate how Alice and Bob encode their bits: whenever Alice detects her photon in the first (second) satellite peak she knows that the pair is created in the first (second) time-bin and thus Bob can either detect the twin photon in the first (second) satellite peak or in the central peak, however he can never detect it in the second (first) satellite peak. Thus, after suppressing central peak events with the basis reconciliation, Alice and Bob encode their bits as 0 (1) if the photon is detected in the first (second) satellite peak. The second basis is defined by two orthogonal vectors represented on the equator of the Poincaré sphere (for example $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$). The projection onto this basis is performed when a photon is detected in the central peak. Alice and Bob have to correctly adjust their interferometers such that they have perfect correlation between detectors $A_{+1}B_{+1}$ and $A_{-1}B_{-1}$. The encoding of bits 0 and 1 in this basis is thus defined by which detector fires. As Alice's and Bob's photon passively choose their respective measurement basis, there is 50 % probability that they are detected in the same basis which ensures the security against photon number splitting attack [17].

We report a proof of principle of entanglement based QKD over 50 km of optical fiber. In our experimental set-up, Alice sequentially selects one of the three detection windows by looking at the arrival time of her photon with respect to the emission of the laser pulse (see Fig.1). This signal is then used to trigger Bob's detectors. In the first measurement basis the measured quantum bit error

rate (QBER) [19] is of $12.8 \pm 0.1\%$ and the measured raw bit rate of around 5 Hz. The QBER is due to accidental coincidence counts (around 8 %) and to creation of multiple pairs (around 4.5 %, see Fig.4a)). In the second measurement basis the measured QBER is of $10.5 \pm 0.09\%$ (Fig.4b)), with a bit rate of 6Hz. In this case the QBER is due to accidental coincidence count probability (around 4 %), to creation of multiple pairs (around 4.5 %) and to slight misalignment of our interferometers (around 2 %). In order to have a low statistical error the integration time for both basis is of around six hours. The difference of the QBER measured in two basis is due to the fact that in the first measurement basis the detectors are opened during two time-windows instead of one in the second basis. However in the first basis the misalignment of interferometers does not introduce any error. Note that by using two InGaAs APDs with the same low dark count probability as detector B_{+1}, the QBER in the first measurement basis would be reduced to 10.8 % and in the second basis to 9.8 %.

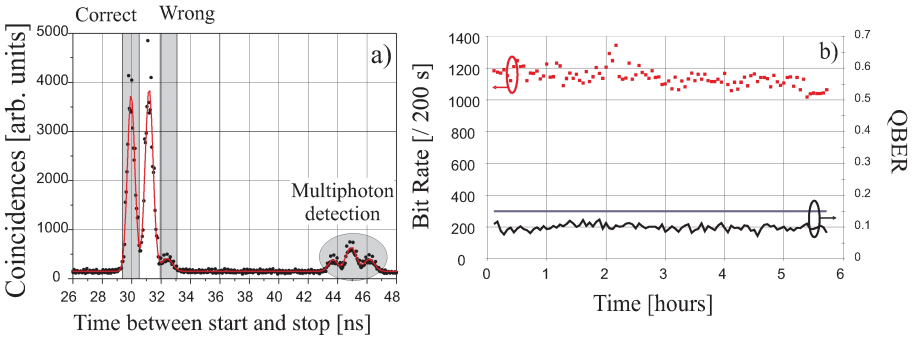


Fig. 4: Experimental results. a) Coincidence count between Alice's and Bob's detector where Alice selects bit 0 in the first measurement basis. Bob detects photons projected onto $|0\rangle$ vector (denoted as correct events) or onto $|0\rangle + e^{i\beta}|1\rangle$ vector (these events are removed by basis reconciliation). The presence of multiphotons leads to wrong detections and thus to the increase of the QBER. b) Bit rate results for the second basis (squares) and a QBER measurement (line), which is clearly below the QBER limit of 15 % secure against individual attacks (straight line) [21].

For a true implementation of QKD using time-bin entangled photons it is necessary that Alice and Bob can monitor detections in all three time windows at the same time and not as presented here, one after the other. In addition, as Alice has to trigger Bob's detectors, it is important to ensure that Eve does not get any information about Alice's detection times. This extensions would require more coincidence electronics but can be easily implemented. Finally, note that Alice's trigger signal has to arrive at Bob's before the photon, thereby putting constraints on the distance between Alice, Bob and the source of entangled photons. These limitations are suppressed by using assively quenched InGaAs APDs (work in progress) or detectors based on superconductivity [20].

In this letter we present an experimental distribution of time-bin entangled photons over 50 km of optical fiber. Using active phase stabilization with a frequency stabilized laser and feedback loop, long term stability and control of the interferometer's phase is achieved. In the first experiment, the CHSH Bell inequality is violated by more than 15 standard deviation without removing the detector noise. The possibility of changing the phase in a controlled way allowed us also to show a proof of principle of entanglement based quantum key distribution over 50 km of optical fiber. An average Quantum Bit Error Rate of 11.5% is demonstrated which is small enough to establish quantum keys secure against individual attacks [21]. Finally, a long term set-up stability opens the road for future demonstrations of more complicated quantum communication protocols requiring long measurement times as is the case for the entanglement swapping protocol.

The authors would like to thank Claudio Barreiro and Jean-Daniel Gautier for technical support. Financial support by the Swiss NCCR Quantum Photonics, and by the European project RamboQ are acknowledged.

[1] C.H. Bennett et al., Phys. Rev. Lett. 70, 1895 (1993)
[2] A. Ekert, Phys. Rev. Lett. 67, 661 (1991)
[3] C. Bennett and G. Brassard, in Proceedings of the IEEE ICCSSP, Bangalore (IEEE, New York, 1984), p.175
[4] P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000)
[5] H.-J. Briegle et al., Phys. Rev. Lett. 81, 5932 (1998)
[6] E. Waks et al., Phys. Rev. A 65, 052310 (2002), B. C. Jacobs et al., Phys.Rev.A 66 052307 (2002), D. Collins et al., submitted, quant-ph/0311101
[7] G. Brassard, Found. Phys. 33, 1593 (2003)
[8] M. Aspelmeyer et al., IEEE J. Sel. Top. Quant. 9, 1541 (2003)
[9] A. Beveratos et al., Phys. Rev. Lett. 89, 187901 (2002)
[10] M. Aspelmeyer et al., Science 301, 621 (2003)
[11] J. D. Franson, Phys. Rev. Lett. 62, 2205 (1989), W. Tittel et al., Phys. Rev. Lett. 81, 3563 (1998)
[12] J. Brendel et al., Phys. Rev. Lett. 82, 2594 (1999), R.T. Thew et al., Phys. Rev. A 66, 062304 (2002)
[13] J.F. Clauser and M.A. Horn, Phys. Rev. D 10, 526 (1974)
[14] J.F. Clauser et al., Phys. Rev. Lett. 23, 880 (1969).
[15] In order to prevent overlapping of different time-bins dispersion has to be minimized using DSF or compensating fibers (see S. Fasel et al., submitted, quant-ph/0403144)
[16] I.Marcikic et al., Phys. Rev. A 66, 062308 (2002)
[17] N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002)
[18] W. Tittel et al., Phys. Rev. Lett. 84, 4737 (2000)
[19] The QBER is defined as the ratio of error rate to total rate.
[20] R. Sobolewski et al., IEEE Transactions on applied superconductivity, 13, 1151 (2003)
[21] C.A. Fuchs et al., Phys. Rev. A 56, 1163 (1997)

2 Verteilung von zeitverschränkten Qubits über 50km Glasfaser

I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré und N. Gisin
Gruppe für Angewandte optische Physik, Universität Genf, CH-1211, Genf 4, Schweiz

Wir berichten über die experimentelle Verteilung von Time-Bin-verschränkten Qubits über 50km Glasfasern. Unter Verwendung aktiv stabilisierter Präparations- und Messgeräte demonstrieren wir die Verletzung der CHSH-Bell-Ungleichung um mehr als 15 Standardabweichungen, ohne das Detektorrauschen zu entfernen. Darüber hinaus berichten wir über ein Proof-of-Principle-Experiment zur Verteilung von Quantenschlüsseln über 50km Glasfasern unter Verwendung verschränkter Photonen.

In der Wissenschaft der Quanteninformation ist eine zentrale experimentelle Frage, wie verschränkte Zustände über große Entfernungen verteilt werden können. Bei den meisten Protokollen der Quantenkommunikation müssen die verschiedenen Parteien die Verschränkung teilen. Die bekanntesten Beispiele dafür sind die Quantenteleportation [1] und das Quantenschlüsselverteilungsprotokoll (QKD) von Ekert [2]. Man beachte, dass selbst bei Protokollen, die Verschränkung nicht ausdrücklich voraussetzen, wie das BB84 QKD-Protokoll [3], Sicherheitsbeweise häufig auf „virtueller Verschränkung“ beruhen, d. h. auf der Tatsache, dass eine ideale Einzelphotonenquelle nicht von einer verschränkten Photonenpaarquelle zu unterscheiden ist, bei der ein Photon als Auslöser verwendet wird [4]. Aus praktischerer Sicht kann die Verschränkung über beträchtliche Entfernungen verwendet werden, um die maximale Entfernung zu erhöhen, die ein Quantenzustand zurücklegen kann, wie in Quanten-Repeater- [5] und Quanten-Relais-Protokollen [6]. Schließlich wird die Verschränkung auch als Ressource bei der Untersuchung der Kommunikationskomplexität behandelt [7].

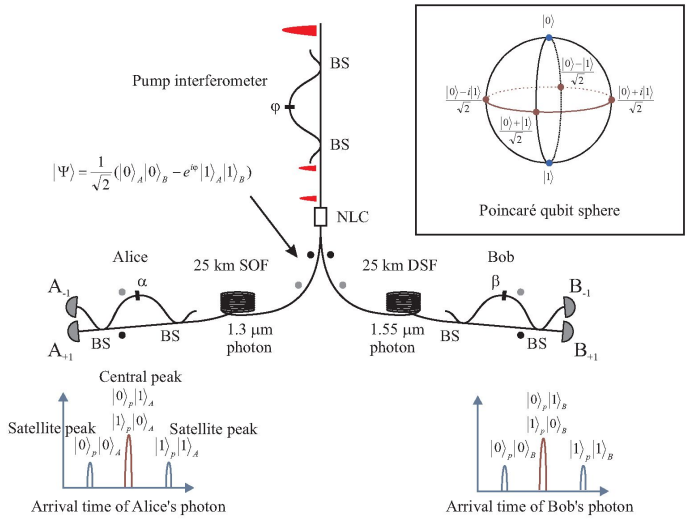


Abb.1: Schema des Versuchsaufbaus. TBQs werden vorbereitet, indem ein fs-Impuls durch das Pumpinterferometer und einen nichtlinearen Kristall (NLC) geleitet wird. Schließlich entsteht im Kristall ein Paar verschränkter Photonen. Sie werden über 25,3km Glasfaser an Alice und Bob gesendet. Alice und Bob analysieren Photonen mit Interferometern, die in Bezug auf das Pumpinterferometer gleichermaßen unausgeglichen sind. Alle drei Interferometer sind mit passiven 50/50-Strahlteilern (BS) aufgebaut. Die Detektionszeiten von Alice und Bob sind ebenfalls dargestellt.

Da Verschränkung nicht durch geteilte Zufälligkeit und lokale Operationen erzeugt werden kann, muss sie irgendwie verteilt werden. Kürzlich gab es einige Vorschläge zur Verwendung von Satelliten für Langstreckenübertragungen [8]. Auch einige Experimente durch den offenen Raum wurden entweder für QKD (über 50m) [9] oder für die Übertragung von verschränkten Qubits (über 600m) [10] durchgeführt. Trotz Wetter- und Tageslichtproblematik ein interessanter Ansatz. Eine andere Möglichkeit, der wir in dieser Arbeit folgen, ist die Nutzung des weltweit implementierten Glasfasernetzes. Dies bringt jedoch einige Einschränkungen mit sich. Man sollte bei Telekommunikationswellenlängen (1,3 oder 1,55μm) arbeiten, um Verluste in Glasfasern zu minimieren und die Codierung der Qubits muss robust gegen Dekohärenz in Glasfasern sein. Wahrscheinlich ist die adäquateste Art, Qubits zu codieren, die Verwendung der Energie-Zeit- [11] oder ihrer diskreten Version der Time-Bin[1]-Codierung[2] [12]. Der Hauptnachteil dieser Art der Codierung im Vergleich

[1] deutsch Zeitfenster
[2] engl. time-bin-encoding, **TBE**

zur Polarisationsart besteht darin, dass die Erstellung und Messung komplexer ist. Sie ist auf stabile Interferometer angewiesen[3]. In diesem Brief berichten wir über eine Methode zur Erstellung und Messung von Time-Bin-verschränkten Qubits[4], die es uns ermöglicht, Bell-Ungleichungen über 50km Glasfasern zu verletzen und einen Grundsatznachweis für verschränkungsbasierte QKD über große Entfernungen zu zeigen. Darüber hinaus ermöglicht es, die Stabilität unseres gesamten Aufbaus über mehrere Stunden zu demonstrieren.

Erinnern wir den Leser zunächst daran, wie man TBQs erstellt und misst. Sie werden erzeugt, indem ein kurzer Laserimpuls zuerst durch ein unsymmetrisches Interferometer (hier als Pumpinterferometer bezeichnet) und dann durch einen nichtlinearen Kristall gesendet wird, wo schließlich ein Photonenpaar durch spontane parametrische Abwärtskonvertierung (SPDC) erzeugt wird (siehe Abb.1). Der Zustand kann beschrieben werden durch:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \cdot \left(|0\rangle_A|0\rangle_B - e^{i\cdot\varphi}|1\rangle_A|1\rangle_B\right) \tag{1}$$

Wobei $|0\rangle$ für ein Photon im ersten Time-Bin steht (das den kurzen Arm durchlaufen hat) und $|1\rangle$ für ein Photon im zweiten Time-Bin (das den langen Arm durchlaufen hat). Der Index A bzw. B steht für Alices und Bobs Photon. Die Phase φ wird als Referenz der Pfadlängendifferenz zwischen dem kurzen und dem langen Arm $\Delta\tau$ definiert. Die Photonen A und B werden dann an Alice und Bob gesendet, die mit einem ähnlichen unsymmetrischen Interferometer projektive Messungen durchführen. An den Detektoren von Alice (Bob) gibt es drei Detektionszeiten in Bezug auf die Emissionszeit des Pumplasers (siehe Abb.1). Der erste und der letzte Peak (als Satellitenpeaks bezeichnet)[5] entsprechen zeitlich unterscheidbaren Ereignissen, der linke (rechte) Peak entspricht einem Photon, das im ersten (zweiten) Zeitfenster erzeugt wurde und den kurzen (langen) Arm des Interferometers von Alice durchlaufen hat. Wenn das Photon im linken (rechten) Satellitenpeak entdeckt wird, wird es auf den Vektor $|0\rangle$ ($|1\rangle$) projiziert (die Pole auf der Poincaré-Qubit-Kugel). Photonen, die im mittleren Peak[6] entdeckt werden, können entweder auf Ereignisse zurückzuführen sein, bei denen sich das erzeugte Photon im ersten Zeitbereich befindet und dann den langen Arm von Alices Interferometer durchläuft, oder auf Ereignisse, bei denen das Photon im zweiten Zeitbereich erzeugt wird und dann den kurzen Arm von Alices Interferometer durchläuft. In diesem Fall wird das Photon auf den Vektor $|0\rangle + e^{i\alpha}|1\rangle$ projiziert (d. h. auf den Äquator der Poincaré-Qubit-Kugel). Man beachte, dass Alice bei der Aufzeichnung des zentralen Peaks keine Einzelphotoneninterferenz beobachtet, indem sie die Phase ihres Interferometers ändert, da die Information über den Weg durch die Aufzeichnung der Emissionszeit von Bobs Photon ermittelt werden kann. In Bezug auf Experimente mit polarisationsverschränkten Photonen bezeichnen wir dies als Rotationsinvarianz [13]. Wenn Alice und Bob beide Zählungen in ihren zentralen Peaks aufzeichnen, beobachten sie Interferenz zweiter Ordnung, indem sie entweder die Phase in Alices, in Bobs oder im Pumpinterferometer ändern. Die Koinzidenzzählrate zwischen den Detektoren von Alice und Bob, A_iB_j, ist dann gegeben durch:

$$R_{A_i,B_j}(\alpha,\beta,\varphi) \propto 1 + i\cdot j\cdot V\cdot\cos(\alpha+\beta+\varphi) \tag{2}$$

Wobei i und $j = \pm 1$ (siehe Abb.1) und V die Visibilität der Interferenzstreifen ist (die im Prinzip den Wert 1 erreichen kann). Die Unsymmetrie des Pumpinterferometers definieren wir als die Referenzzeitdifferenz $\Delta\tau$ zwischen dem ersten und dem zweiten Zeitfenster, die Phase φ wird also als Null angenommen. Der Korrelationskoeffizient ist definiert als:

$$E(\alpha,\beta) = \frac{\sum_{i,j} i\cdot j\cdot R_{A_iB_j}(\alpha,\beta)}{\sum_{i,j} R_{A_iB_j}(\alpha,\beta)} \tag{3}$$

Durch Einsetzen von Gleichung 2 in Gleichung 3 ergibt sich der Korrelationskoeffizient:

$$E(\alpha,\beta) = V\cdot\cos(\alpha+\beta) \tag{4}$$

[3] weitere Informationen als Einstieg zum Forschungsthema Temperaturstabilität siehe:
https://de.wikipedia.org/wiki/Time-Bin-Konfiguration#Literatur
https://www.nadirpoint.de/Dokumentenserver.html#MAS

[4] **T**ime-**B**in-**Q**ubits, **TBQ**

[5] in der **T**ime-**B**in-**K**onfiguration **TBK$_{SZS}$** der voraus- **(SZS)** bzw. nacheilende **(SZS)** Satellit

[6] in der **TBK$_{SZS}$** als eigentlicher Informationsträger der Zentralpeak **(SZS)**

Die Bell-Ungleichungen definieren eine Obergrenze S für Korrelationen, welche durch die lokale Theorien verborgener Variablen (Local Hidden-Variable Theories - LHVT) beschrieben werden können. Eine der am häufigsten verwendeten Formen, die so genannte Clauser-Horne-Shimony-Holt (CHSH) Bell-Ungleichung [14] lautet:

$$S = \left|E(\alpha,\beta) + E(\alpha,\beta') + E(\alpha',\beta) - E(\alpha',\beta')\right| \leq 2 \tag{5}$$

Die Quantenmechanik sagt voraus, dass S einen maximalen Wert von $S = 2\sqrt{2}$ mit $\alpha = 0°, \alpha' = 90°, \beta = 45°$ und $\beta' = -45°$ aufweist. Es wurde auch gezeigt, dass, wenn die Korrelationsfunktion eine sinusförmige Form aufweist, wie Gl.4 und wenn es eine Rotationsinvarianz gibt, dass dann die Randbedingung von Gl.5 geschrieben werden kann wie bei:

$$S = 2\sqrt{2} \cdot V \leq 2 \tag{6}$$

Somit impliziert $V \geq \frac{1}{\sqrt{2}}$ ein Verstoß gegen die CHSH-Bell-Ungleichung, d.h. die Korrelationen können durch die LHVT nicht erklärt werden.

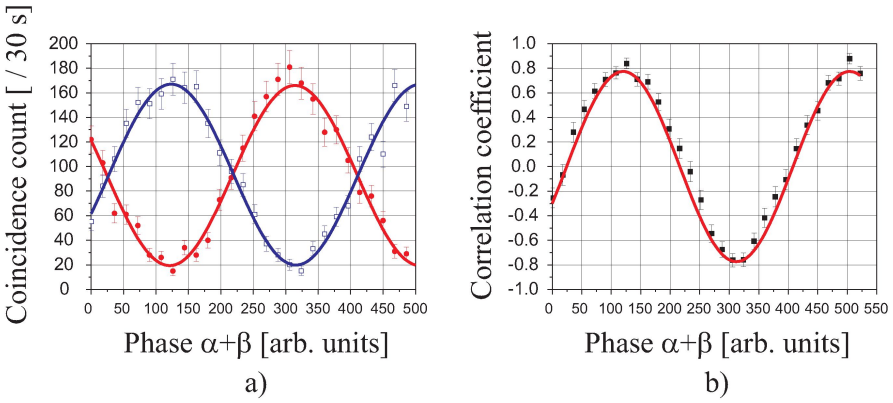


Abb.2: a) Zufallszahlen zwischen den Detektoren $A_{+1}B_{+1}$ (Kreise) und $A_{+1}B_{-1}$ (offene Quadrate) b) Korrelationskoeffizienten $E(\alpha,\beta)$ gemessen aus vier differenten Zufallszahlen (Gleichung 3). Alice's Phase α wird konstant gehalten und Bobs Phase β wird gescannt.

Unser experimenteller Aufbau ist der folgende (siehe auch Abb.1). Ein 150fs-Laserpuls mit einer Wellenlänge von 710nm und einer Wiederholrate von 75MHz wird zunächst durch ein unsymmetrisches Michelson-Interferometer mit einer optischen Wegdifferenz von $\Delta\tau = 1.2$ns und dann durch einen nichtlinearen LBO-Kristall (Lithiumtriborat) vom Typ I geschickt, in dem kollineare, nicht entartete Photonenpaare bei $1,3$ und $1,55\mu$m Wellenlänge durch SPDC erzeugt werden können. Der Pumpstrahl wird dann mit einem Siliziumfilter entfernt und die Paare werden in eine optische Faser gekoppelt. Die Photonen werden mit einem Wellenlängen-Division-Multiplexer getrennt. Das $1,3\mu$m-Photon wird durch eine $25,3$km optische Standardfaser (SOF) an Alice und das $1,55\mu$m-Photon über eine $25,3$km dispersionsverschiebende Faser (DSF) nach Bob [15] gesendet. Das Photon von Alice wird dann mit einem Faser-Michelson-Interferometer gemessen und von einer der beiden mit flüssigem Stickstoff gekühlten, passiv gequenchten Germanium-Avalanche-Photodioden (APD) A_{+1} oder A_{-1} detektiert. Ihre Quanteneffizienz liegt bei etwa 10% mit 20kHz Dunkelzählung. Um nur die zentralen Spitzenereignisse zu selektieren und die Dunkelzählungen des Detektors zu reduzieren, wird eine Koinzidenz mit der Emissionszeit des Laserpulses hergestellt. Dieses Signal triggert dann Bobs Detektoren (B_{+1} und B_{-1}), bei denen es sich um zwei InGaAs-APDs (IdQuantique) handelt, die im sogenannten Gated Mode arbeiten. Obwohl beide Detektoren eine ähnliche Quanteneffizienz von 20% haben, ist die Dunkelzählwahrscheinlichkeit des einen Detektors (B_{+1}) doppelt so groß wie die des anderen (B_{-1}) und liegt bei etwa 10^{-4}ns^{-1}. Um die chromatische Dispersion in den Glasfasern und die Erkennung mehrerer Paare zu verringern [16], verwenden wir Interferenzfilter mit einer spektralen Breite von 10nm für $1,3\mu$m-Photonen und 18nm für die $1,55\mu$m-Photonen. Bei einer durchschnittlichen Eingangsleistung von 70mW (gemessen nach dem Pumpinterferometer) liegt die Wahrscheinlichkeit der Erzeugung eines verschränkten Qubits pro Puls bei etwa 8%. Bobs Analysator ist ebenfalls ein Interferometer vom Michelson-Typ, das mit Glasfasern gebaut wurde. Um die Phase besser kontrollieren zu können und Langzeitstabilität zu erreichen, werden alle drei Interferometer passiv und aktiv stabilisiert. Bei der aktiven Stabilisierung wird die Phase der Interferometer mit einem frequenzstabilisierten Laser bei $1,534\mu$m (Dicos) gemessen und

über eine Rückkopplungsschleife an einem Piezoaktor (PZA), der in jedem Interferometer enthalten ist, auf einen gewünschten Wert eingestellt. Um die Wegdifferenz im Pump-Interferometer ändern zu können, ist einer der Spiegel auf einer Translation am PZA mit einer Weglängenänderung von ca. 4μm montiert. Bei der Analyse der Interferometer ist der lange Faserweg mit einem zylindrischen PZA umwickelt, der dadurch eine Umfangänderung von 60μm aufweist. Im Gegensatz zum Pump-Interferometer, das kontinuierlich stabilisiert wird, kann die Phase des Faserinterferometers während der Messperiode nicht stabilisiert werden. Daher wechseln wir kontinuierlich zwischen Messperioden von 100s und Stabilisierungsperioden von 5s. Mit dieser Methode können wir nicht nur den gesamten Aufbau über mehrere Stunden hinweg stabilisieren, sondern haben auch eine gute Kontrolle über die Änderungen der beiden Phasen α und β.

Um eine Verletzung der CHSH-Bell-Ungleichung nach 50km Glasfaserstrecke zu zeigen, gehen wir in zwei Schritten vor: Zunächst scannen wir Bobs Phase β, während Alices Phase α konstant gehalten wird. Wir erhalten eine Rohvisibilität von etwa $78 \pm 1.6\%$ (siehe Abb.2), aus der wir den S-Parameter mit $S = 2.206 \pm 0.045$ (Gleichung 6) ableiten können, der zu einer Verletzung der CHSH-Bell-Ungleichung um mehr als 4 Standardabweichungen führt. Die Koinzidenzzählrate zwischen einer beliebigen Kombination von Detektoren $A_i B_j$ liegt bei etwa 3Hz.

Die Rohvisibilität der Korrelationsfunktion wird hauptsächlich durch die Bildung von Mehrfachpaaren (ca. 9%), durch zufällige Koinzidenzzählungen (im Zusammenhang mit Dunkelzählungen unserer Detektoren, ca. 8%) und durch die Fehlausrichtung der Interferometer (ca. 5%) verringert. Im Prinzip könnte man die Bildung von Mehrfachpaaren reduzieren, indem man die Eingangsleistung verringert, aber dann würde auch die Koinzidenzzählrate sinken.

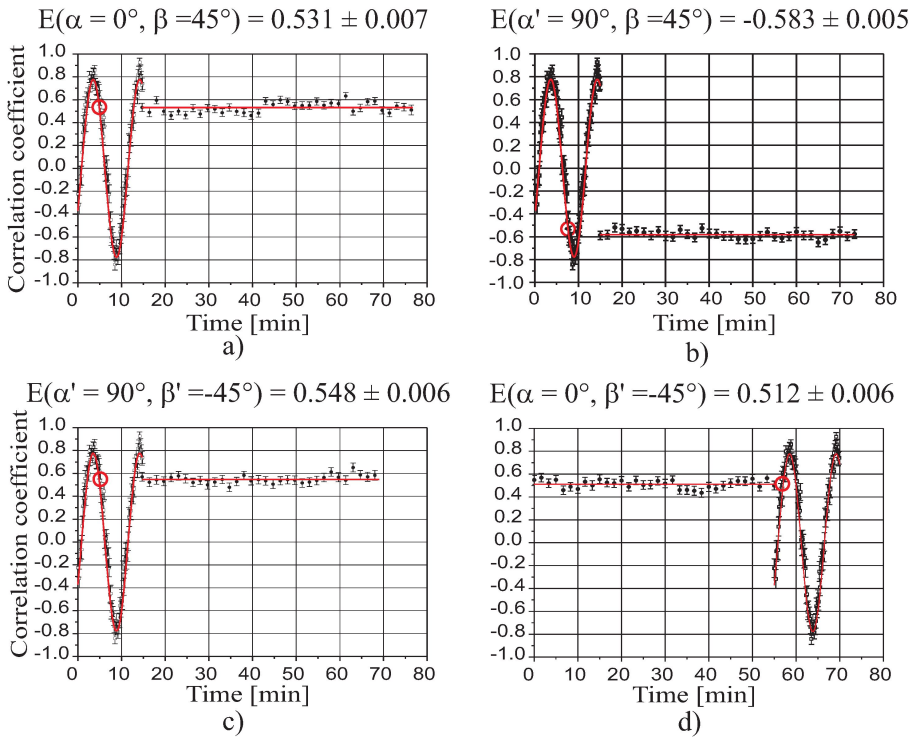


Abb.3: Korrelationskoeffizienten bei kontinuierlichem Scan und vier verschiedenen Einstellungen. Jeder Punkt wurde mit einer Integrationszeit von 100s über Koinzidenzzählungen zwischen vier verschiedenen Kombinationen von zwei Detektoren abgeleitet (Gl.3). Da α und β relativ zur Phase des Pump-Interferometers definiert sind, verwenden wir die ersten drei Messungen a), b), c), um vier verschiedene Phasen zu definieren: $\alpha = 0°$, $\alpha' = 90°$, $\beta = 45°$, $\beta' = -45°$. Die letzte Messung d) vervollständigt den Nachweis einer Verletzung der CHSH-Bell-Ungleichung. Die Kreise stellen den Wert des Korrelationskoeffizienten dar, für den die CHSH-Bell-Ungleichung maximal verletzt wäre, wenn die Visibilität 78% maximal wäre.

Mit unseren neuen Interferometern sind wir zum ersten Mal in der Lage, den zweiten Schritt mit Time-bins durchzuführen: Es wird die CHSH-Bell-Ungleichung nach Gl.5 gemessen, d.h. die Phase auf den gewünschten Wert fixiert, um dann nacheinander die vier verschiedenen Korrelationskoeffizienten zu messen. Um statistische Schwankungen zu reduzieren, messen wir den Korrelationskoeffizienten (Gl.3) über fast einer Stunde für jede Einstellung. Der erhaltene S-Parameter ist $S = 2.185 \pm 0.006$, der eine Verletzung der CHSH-Bell-Ungleichung um mehr als 15 Standardab-

weichungen zeigt (siehe Abb.3).

Es wurde bewiesen, dass die verschränkten Photonen in der Quantenkryptographie verwendet werden können, wenn die Bell-Ungleichung verletzt wird [17]. Unser QKD-Protokoll ist analog zum BB84-Protokoll, das zeitverschränkte Photonen verwendet [18]. Alice und Bob verwenden also zwei maximal konjugierte Messbasen.

Die erste Basis ist durch zwei orthogonale Vektoren $|0\rangle$ und $|0\rangle$ definiert, die auf den Polen der Poincaré-Qubit-Kugel dargestellt sind (Abb.1). Die Projektion auf diese Basis wird immer dann durchgeführt, wenn ein Photon in einem Satellitenpeak entdeckt wird. Lassen Sie uns veranschaulichen, wie Alice und Bob ihre Bits kodieren: Immer wenn Alice ihr Photon im ersten (zweiten) Satellitenpeak entdeckt, weiß sie, dass das Paar im ersten (zweiten) Zeitfenster entstanden ist, und so kann Bob das Zwillingsphoton entweder im ersten (zweiten) Satellitenpeak oder im zentralen Peak entdecken, aber niemals im zweiten (ersten) Satellitenpeak. Nach der Unterdrückung der Zentralpeak-Ereignisse durch die Basisabstimmung kodieren Alice und Bob ihre Bits also als 0 (1), wenn das Photon im ersten (zweiten) Satellitenpeak entdeckt wird. Die zweite Basis wird durch zwei orthogonale Vektoren definiert, die auf dem Äquator der Poincaré-Kugel dargestellt werden (z.B. $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ und $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$). Die Projektion auf diese Basis wird durchgeführt, wenn ein Photon im Zentralpeak entdeckt wird. Alice und Bob müssen ihre Interferometer so einstellen, dass sie eine perfekte Korrelation zwischen den Detektoren $A_{+1}B_{+1}$ und $A_{-1}B_{-1}$ haben. Die Kodierung der Bits 0 und 1 in dieser Basis wird also dadurch bestimmt, welcher Detektor ausschlägt. Da die Photonen von Alice und Bob passiv ihre jeweilige Messbasis wählen, besteht eine 50-prozentige Wahrscheinlichkeit, dass sie in der gleichen Basis detektiert werden, was die Sicherheit gegen einen Angriff durch Photonenzahlsplitting gewährleistet [17].

Wir berichteten über einen Grundsatzbeweis für verschränkungsbasierte QKD über 50km Glasfaser. In unserem Versuchsaufbau wählt Alice nacheinander eines der drei Detektionsfenster aus, indem sie die Ankunftszeit ihres Photons im Verhältnis zur Emission des Laserpulses betrachtet (siehe Abb.1). Dieses Signal wird dann verwendet, um Bobs Detektoren auszulösen. In der ersten Messbasis liegt die gemessene Quantenbitfehlerrate (QBER) [19] bei $12.8 \pm 0.1\%$ und die gemessene Rohbitrate bei etwa 5Hz. Die QBER ist auf zufällige Koinzidenzzählungen (ca. 8%) und auf die Bildung von Mehrfachpaaren (ca. $4,5\%$ zurückzuführen (siehe Abb.4a)). Bei der zweiten Messbasis liegt die gemessene QBER bei $10.5 \pm 0,09\%$ (Abb.4b)), mit einer Bitrate von 6Hz. In diesem Fall ist die QBER auf eine zufällige Koinzidenz-Zählwahrscheinlichkeit (ca. 4%), auf die Bildung von Mehrfachpaaren (ca. $4,5\%$) und auf eine leichte Fehlausrichtung unserer Interferometer (ca. 2%) zurückzuführen. Um einen geringen statistischen Fehler zu erhalten, beträgt die Integrationszeit für beide Basen etwa sechs Stunden. Der Unterschied zwischen den QBER-Messungen in den beiden Basen ist auf die Tatsache zurückzuführen, dass die Detektoren in der ersten Messbasis während zweier Zeitfenster geöffnet werden, anstatt während eines in der zweiten Basis. In der ersten Basis führt die falsche Ausrichtung der Interferometer jedoch zu keinem Fehler. Bei Verwendung von zwei InGaAs-APDs mit der gleichen niedrigen Dunkelzählwahrscheinlichkeit wie Detektor B_{+1} würde sich die QBER in der ersten Messbasis auf $10,8\%$ und in der zweiten Messbasis auf $9,8\%$ verringern.

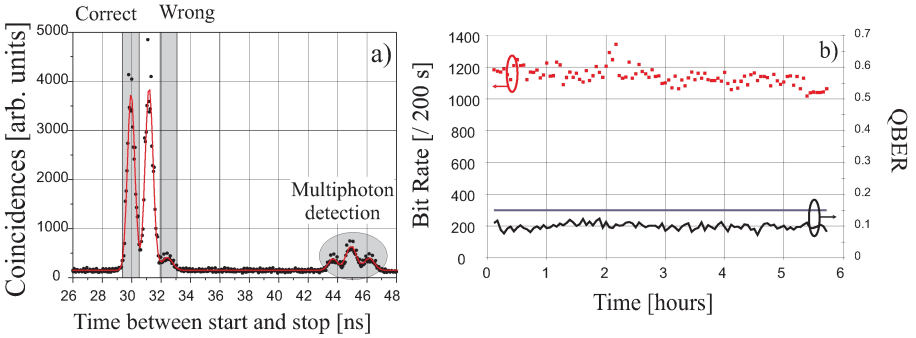


Abb.4: Experimentelle Ergebnisse. a) Koinzidenzzählung zwischen dem Detektor von Alice und Bob, wobei Alice in der ersten Messbasis das Bit 0 auswählt. Bob detektiert Photonen, die auf den $|0\rangle$-Vektor (als korrekte Ereignisse bezeichnet) oder auf den $|0\rangle + e^{i\beta}|1\rangle$-Vektor projiziert werden (diese Ereignisse werden durch Basisabgleich entfernt). Das Vorhandensein von Mehrphotonen führt zu falschen Erkennungen und damit zu einer Erhöhung der QBER. b) Bitratenergebnisse für die zweite Basis (Quadrate) und eine QBER-Messung (Linien), die deutlich unter der QBER-Grenze von 15% Sicherheit gegen individuelle Angriffe liegt (gerade Linien) [21].

Für eine echte QKD-Implementierung mit zeitlich verschränkten Photonen ist es notwendig, dass Alice und Bob die Detektionen in allen drei Zeitfenstern gleichzeitig überwachen können und nicht, wie hier dargestellt, eine nach der anderen. Da Alice die Detektoren von Bob auslösen muss, muss außerdem sichergestellt werden, dass Eve keine Informationen über die Detektionszeiten von Alice erhält. Diese Erweiterung würde mehr Koinzidenzelektronik erfordern, kann aber leicht implementiert werden. Schließlich ist zu beachten, dass das Auslösesignal von Alice vor dem Photon bei Bob eintreffen muss, wodurch die Entfernung zwischen Alice, Bob und der Quelle der verschränkten Photonen begrenzt wird. Diese Einschränkungen werden durch die Verwendung von assoziativ gequenchten InGaAs-APDs (in Arbeit) oder auf Supraleitung basierenden Detektoren [20] unterdrückt.

In diesem Artikel stellen wir eine experimentelle Verteilung von zeitlich verschränkten Photonen über 50km Glasfaser vor. Durch aktive Phasenstabilisierung mit einem frequenzstabilisierten Laser und einer Rückkopplungsschleife wird eine langfristige Stabilität und Kontrolle der Phase des Interferometers erreicht. Im ersten Experiment wird die CHSH-Bell-Ungleichung um mehr als 15 Standardabweichungen verletzt, ohne dass das Detektorrauschen entfernt wird. Die Möglichkeit, die Phase kontrolliert zu verändern, ermöglichte es uns auch, einen Grundsatzbeweis für die verschränkungsbasierte Quantenschlüsselverteilung über 50km Glasfaser zu erbringen. Es wurde eine durchschnittliche Quanten-Bitfehlerrate von $11,5\%$ nachgewiesen, die klein genug ist, um Quantenschlüssel zu erstellen, die gegen individuelle Angriffe sicher sind [21]. Schließlich eröffnet die Langzeitstabilität des Aufbaus den Weg für künftige Demonstrationen von komplizierteren Quantenkommunikationsprotokollen, die lange Messzeiten erfordern, wie es beim Verschränkungsaustauschprotokoll der Fall ist.

Die Autoren bedanken sich bei Claudio Barreiro und Jean-Daniel Gautier für die technische Unterstützung. Wir danken für die finanzielle Unterstützung durch den Schweizer NCCR Quantum Photonics und das europäische Projekt RamboQ.

[1] C.H. Bennett et al., Phys. Rev. Lett. 70, 1895 (1993)

[2] A. Ekert, Phys. Rev. Lett. 67, 661 (1991)

[3] C. Bennett and G. Brassard, in Proceedings of the IEEE ICCSSP, Bangalore (IEEE, New York, 1984), p.175

[4] P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000)

[5] H.-J. Briegle et al., Phys. Rev. Lett. 81, 5932 (1998)

[6] E. Waks et al., Phys. Rev. A 65, 052310 (2002), B. C. Jacobs et al., Phys.Rev.A 66 052307 (2002), D. Collins et al., submitted, quant-ph/0311101

[7] G. Brassard, Found. Phys. 33, 1593 (2003)

[8] M. Aspelmeyer et al., IEEE J. Sel. Top. Quant. 9, 1541 (2003)

[9] A. Beveratos et al., Phys. Rev. Lett. 89, 187901 (2002)

[10] M. Aspelmeyer et al., Science 301, 621 (2003)

[11] J. D. Franson, Phys. Rev. Lett. 62, 2205 (1989), W. Tittel et al., Phys. Rev. Lett. 81, 3563 (1998)

[12] J. Brendel et al., Phys. Rev. Lett. 82, 2594 (1999), R.T. Thew et al., Phys. Rev. A 66, 062304 (2002)

[13] J.F. Clauser and M.A. Horn, Phys. Rev. D 10, 526 (1974)

[14] J.F. Clauser et al., Phys. Rev. Lett. 23, 880 (1969).

[15] In order to prevent overlapping of different time-bins dispersion has to be minimized using DSF or compensating fibers (see S. Fasel et al., submitted, quant-ph/0403144)

[16] I.Marcikic et al., Phys. Rev. A 66, 062308 (2002)

[17] N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002)

[18] W. Tittel et al., Phys. Rev. Lett. 84, 4737 (2000)

[19] The QBER is defined as the ratio of error rate to total rate.

[20] R. Sobolewski et al., IEEE Transactions on applied superconductivity, 13, 1151 (2003)

[21] C.A. Fuchs et al., Phys. Rev. A 56, 1163 (1997)

LaTeX 2_ε