Invited Paper

One-Way Autocompensating Quantum Cryptography via Auto-Phase-Matched Spontaneous Parametric Down-Conversion

Zachary D. Walton, Ayman F. Abouraddy, Mark C. Booth, Alexander V. Sergienko, Bahaa E. A. Saleh, and Malvin C. Teich

Quantum Imaging Laboratory
Departments of Electrical & Computer Engineering and Physics,
Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215-2421

ABSTRACT

We present a new quantum cryptography implementation that uses frequency-correlated photon pairs to combine one-way operation with an autocompensating feature that has hitherto only been available in implementations that require the signal to make a round trip between the users. Furthermore, we describe a new scheme for creating frequency-correlated photon pairs (auto-phase-matched spontaneous parametric down-conversion). The new scheme offers several advantages over previous schemes, including the ability to generate frequency-correlated photon pairs regardless of the dispersion characteristics of the system.

Keywords: quantum cryptography, quantum key distribution, spontaneous parametric down-conversion

1. INTRODUCTION

The idea of using quantum systems for secure communications originated in the 1970s with Stephen Wiesner's intuition that the uncertainty principle, commonly derided as a source of noise, could be harnessed to detect unauthorized monitoring of a communication channel.[1] The first quantum cryptographic protocol (BB84) was published by Charles H. Bennett and Giles Brassard in 1984.[2] While rigorous proofs of the security of BB84 under realistic conditions have only recently emerged (cf. Ref. 3 and references therein), the "no-cloning theorem"[4] published in 1982 provides a one-line security proof applicable in ideal circumstances. Given the obvious choice of light as a signal carrier, the path to practical quantum cryptography was clear: develop robust experimental methods to create, manipulate, transmit, and detect single photons. For an excellent summary of progress in the theory and practice of quantum cryptography, see Ref. 5.

The nascent field of quantum cryptography took an unexpected turn in 1992 when Artur Ekert published a new protocol[6] that derived its security not from the impossibility of cloning a quantum state, but rather the seemingly distinct phenomenon of the violation of Bell's inequality.[7] The practical importance of this scheme was immediately questioned by Bennett et al.[8] They pointed out that the same hardware required for Ekert's protocol could be used to implement the more efficient BB84 protocol. This is accomplished by regarding the two-particle source together with one detection apparatus as a single entity that produces a localized quantum state (i.e., one of the four BB84 polarization states) to be detected by the other detection apparatus. Although not described as such, their objection amounted to an application of the concept of advanced waves.[9] This method, pioneered by David Klyshko, establishes a formal equivalence between two optical constructs: 1) the propagation of two entangled photons from a localized source to a pair of remote detectors, and 2) the propagation of a single photon from one detector backwards towards the source, where it is reflected, and then forward to the other detector. The advanced-wave method is a powerful tool for developing intuition about two-photon interference experiments that demonstrate entanglement in time,[10] space,[11] and, trivially, polarization. For a discussion of apparent backward-in-time processes in the more general context of quantum information theory, see Ref. 12.

Z.D.W.: E-mail: walton@bu.edu; Quantum Imaging Laboratory homepage: http://www.bu.edu/qil

Quantum Communications and Quantum Imaging, edited by Ronald E. Meyers, Yanhua Shih,
Proc. of SPIE Vol. 5161 (SPIE, Bellingham, WA, 2004) · 0277-786X/04/$15 · doi: 10.1117/12.503748

The strong interest in absolutely secure communications has fueled an ongoing effort to determine which protocol leads to the best performance in practical implementations. In 1997, Muller et al. introduced autocompensating quantum cryptography (AQC), in which the optical signal makes a round trip between the legitimate users (commonly referred to as Alice and Bob).[13] The scheme is described as autocompensating since it provides high-visibility interference without an initial calibration step or active compensation of drift in the optical apparatus; these favorable properties led the authors to refer to their scheme informally as "plug-and-play quantum cryptography." While this scheme and its refinements[14–18] represent substantial progress in the quest for a practical quantum cryptography implementation, the requirement that the signal travel both directions along the transmission line leads to non-trivial technical difficulties.

In this article, we describe one-way entangled-photon autocompensating quantum cryptography (OW-AQC)[19] in which two photons travel one way (e.g., from Alice to Bob), instead of one photon traveling back and forth, as in AQC. The formal association of OW-AQC with AQC follows directly from the advanced-wave view, just as Ekert's scheme follows from BB84. While Ekert's scheme employs entanglement to allow an alternative space-time configuration (signal source between Alice and Bob versus a source on Alice's side), OW-AQC employs entanglement to achieve immunity to interferometer drift within the original paradigm of a one-way quantum channel from Alice to Bob. Thus, our result provides a new example of a capability afforded by quantum entanglement.

This article is organized as follows. First, we briefly review the standard AQC scheme. Second, we introduce OW-AQC and show that it combines one-way operation with the insensitivity to drift that is characteristic of its predecessor. Third, we point out the formal equivalence of the two methods from the advanced-wave viewpoint using space-time diagrams. Fourth, we discuss the relative merits of OW-AQC. Finally, we describe auto-phase-matched spontaneous parametric down-conversion,[20] a new method for creating the frequency-correlated photon pairs which are required for OW-AQC.

2. ONE-WAY AUTOCOMPENSATING QUANTUM CRYPTOGRAPHY

Figure 1A contains a schematic of AQC. The protocol begins with Bob launching a strong pulse from a laser (L) into a Mach–Zehnder interferometer via a circulator (C). This interferometer splits the pulse into an advanced amplitude (P1) and a retarded amplitude (P2). The amplitudes travel through phase modulators (PM) on Bob's side and Alice's side, and are then attenuated (AT) to the single photon level and reflected by Alice back to Bob. Although both P1 and P2 will again be split at Bob's Mach–Zehnder interferometer, by gating his detector appropriately, Bob can postselect those cases in which P1 takes the long path and P2 takes the short path on the return trip. Thus, the interfering amplitudes experience identical delays on their round trip, ensuring insensitivity to drift in Bob's interferometer.

The role of the phase modulators can be readily understood by examining the space-time diagram of this protocol (see Fig. 1B). The eight boxes (A1–A4, B1–B4) refer to the phase settings on the two modulators as the two amplitudes pass through each of them twice. For example, B2 refers to the phase acquired by the delayed amplitude of the pulse that Bob sends to Alice, while B4 refers to the phase acquired by the same amplitude as it travels back from Alice to Bob. It should be understood that B1–B4 refer to settings of the same physical phase shifter at different times (and similarly for A1–A4). The probability of a detection at Bob's detector is given by

$$P_{\mathrm{d}} \propto 1 + \cos[(\mathrm{B2} - \mathrm{B1}) + (\mathrm{A2} - \mathrm{A1}) + (\mathrm{A4} - \mathrm{A3}) + (\mathrm{B4} - \mathrm{B3})]. \tag{1}$$

From this expression we see that only the relative phase between the phase modulator settings affects the probability of detection. Thus, by setting B1 = B2 and A1 = A2, Alice and Bob can implement the interferometric version of BB84 by encoding their cryptographic key in the difference settings $\Delta\phi_A \equiv \mathrm{A4} - \mathrm{A3}$ and $\Delta\phi_B \equiv \mathrm{B4} - \mathrm{B3}$. Since the resulting expression

$$P_{\mathrm{d}} \propto 1 + \cos\left(\Delta\phi_A + \Delta\phi_B\right) \tag{2}$$

is independent of the time delay in Bob's interferometer and the absolute phase settings in either modulator, Alice and Bob are able to achieve high-visibility interference without initial calibration or active compensation of drift.

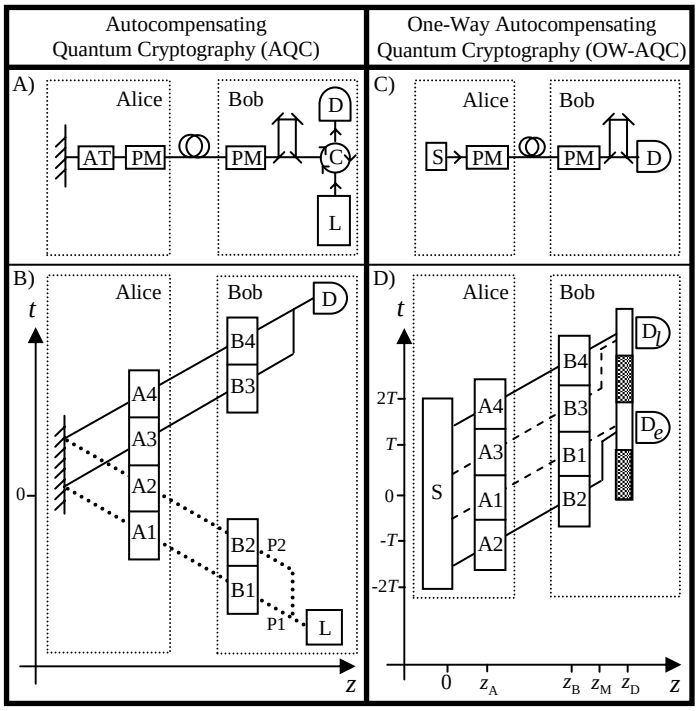

Figure 1. A) and C) depict schematics for AQC and OW-AQC, respectively. L is a source of laser pulses, S emits the two-photon entangled state $|\Psi\rangle$ described by Eq. (3), C is a circulator, AT is an attenuator, PM is a phase modulator, and (D, D_e, D_l) are detectors. B) and D) depict the associated space-time diagrams which indicate how the interference condition between the two amplitudes is controlled by both Alice and Bob. The dotted space-time traces in B) are used in the text to explain the relationship between the two methods from the viewpoint of advanced waves. In D), the four rectangles at the point $z = z_D$ correspond to the four time intervals labeled at $z = z_A$ and $z = z_B$. The unshaded boxes indicate the two time intervals during which Bob's detector is activated. The solid and dashed space-time traces depict two interfering two-photon amplitudes, as described in the text.

Figure 1C contains a schematic of OW-AQC. Alice's source (S) produces a specific two-photon state which is transmitted to Bob and analyzed with a Mach–Zehnder interferometer and a single detector that is activated for two distinct time intervals. As in AQC, Alice and Bob change the settings of their respective phase modulators at specific time intervals in order to implement BB84. The two-photon state that Alice sends to Bob consists of an early photon (which is emitted from Alice's source in the time interval $t_e \in [-2T, 0]$) and a late photon (which is emitted in the time interval $t_l \in [0, 2T]$). The joint emission times of the early photon and the late photon are described by the state $|\Psi\rangle = \int\int dt_e dt_l \; f(t_e, t_l)\, |t_e\rangle\, |t_l\rangle$, where

$$f(t_e, t_l) \propto \begin{cases} \delta(t_e + t_l) & -2T < t_e < 0 \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

This particular entangled state entails perfect anti-correlation in the time of emission of the two photons; thus, while the difference in emission time of the two photons is uniformly distributed over the interval $[0, 4T]$, the sum of the emission times is fixed at $t = 0$ for each emitted pair. By Fourier duality, the two photons are correlated in frequency. While the typical configurations for practical sources of entangled photon pairs produce frequency anti-correlation, the frequency-correlated case has been discussed in several papers.[20–25]

Figure 1D presents a space-time diagram of the OW-AQC protocol. The two-photon entangled state is sent through Alice's phase modulator at position $z = z_A$ where she sets the phase shifts (A1–A4) for the four time intervals indicated in the diagram. Next, the two-photon state is transmitted along the channel to Bob, where it is sent through Bob's phase modulator ($z = z_B$). A Mach–Zehnder interferometer ($z = z_M$) then delays a

portion of the radiation by a time τ. Finally, Bob's detector ($z = z_D$) is activated for two time intervals of length T that correspond to the second halves of the early and late photon wave packets. Gating Bob's detector in this way postselects the cases in which the advanced (delayed) portion of each photon takes the long (short) path. This postselection reduces the photon flux by half and obviates the need for rapid switching of optical paths. Since the time intervals are non-overlapping, we may consider that Bob is using two detectors that are distinguished by the ordering of their respective time windows. Thus, for the rest of the letter, we refer to two detectors on Bob's side, D_e and D_l, which correspond respectively to the early and late activation intervals of Bob's single physical detector.

The two-photon interference can be seen by examining the space-time trajectories of two specific two-photon amplitudes. In Fig. 1D, the solid space-time traces entail emission times $(t_e, t_l) = (-3T/2, 3T/2)$ and the dashed traces entail emission times $(t_e, t_l) = (-T/2, T/2)$. For delay $\tau = T$, the portion of the solid and dashed amplitudes leading to a coincidence are indistinguishable after Bob's Mach–Zehnder interferometer. This indistinguishability brings about quantum interference that varies continuously between completely constructive and completely destructive, depending on the joint phase settings A1–A4, B1–B4.

By activating detectors D_e and D_l for a duration T at times $\frac{z_D}{c} - T$ and $\frac{z_D}{c} + T$, respectively, Bob establishes the following relation between the electric-field operators $\hat{E}_{e,l}$ at his detectors and the annihilation operator $\hat{a}(t)$ associated with $|t\rangle$,

$$\hat{E}_e(t_1) \quad \propto \quad \begin{cases} e^{i(\mathrm{A2+B2})}\hat{a}(t_1 - \frac{z_D}{c} - \tau) + e^{i(\mathrm{A1+B1})}\hat{a}(t_1 - \frac{z_D}{c}) & -T < t_1 - \frac{z_D}{c} < 0 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

$$\hat{E}_l(t_2) \quad \propto \quad \begin{cases} e^{i(\mathrm{A3+B3})}\hat{a}(t_2 - \frac{z_D}{c} - \tau) + e^{i(\mathrm{A4+B4})}\hat{a}(t_2 - \frac{z_D}{c}) & T < t_2 - \frac{z_D}{c} < 2T \\ 0 & \text{otherwise,} \end{cases} \tag{5}$$

where τ is the delay in Bob's Mach–Zehnder interferometer, and c is the speed of light. Substituting into the expression for the probability of a coincidence $P_{\mathrm{C}} \propto \int\int dt_1 dt_2 \, |\langle 0|\hat{E}_e(t_1)\hat{E}_l(t_2)|\Psi\rangle|^2$, we obtain

$$P_{\mathrm{C}} \propto \Lambda\left(\frac{\tau - T}{T}\right)\left[1 + \cos\left(\Delta\phi_A + \Delta\phi_B\right)\right] + \frac{1}{2}\left[\Lambda\left(\frac{\tau - T/2}{T/2}\right) + \Lambda\left(\frac{\tau - 3T/2}{T/2}\right)\right] \quad , \tag{6}$$

where $\Lambda(x) = 1 - |x|$ for $-1 < x < 1$ and 0 otherwise. When $\tau = T$, this equation reduces to the expression for the probability of detection in AQC [see Eq. (2)]. To implement the interferometric version of BB84, Alice and Bob hold the settings of their respective phase modulators constant for the first two time intervals depicted in Fig. 1D (i.e., $A1 = A2$ and $B1 = B2$), and manipulate the difference terms, $\Delta\phi_A \equiv \mathrm{A4} - \mathrm{A3}$ and $\Delta\phi_B \equiv \mathrm{B4} - \mathrm{B3}$. The crucial point is that the interference condition is independent of the absolute setting or drift in either of the phase modulators. This demonstrates that OW-AQC achieves the insensitivity to absolute phase settings characteristic of AQC, while requiring only one pass through the optical system.

It is instructive to compare the space-time diagrams in Figs. 1B and 1D. Reflecting the dotted traces in Fig. 1B around the line $t = 0$ results in the exact space-time arrangement of Fig. 1D. This construction also provides a clear explanation of why the two-photon state described by Eq. (3) is chosen to possess frequency correlation instead of the more common frequency anti-correlation. A device that creates pairs of photons with coincident frequencies (S in Fig. 1D) is nothing more than a mirror (as required by Fig. 1B) when analyzed from the advanced-wave viewpoint. Thus, Klyshko's advanced-wave interpretation provides an intuitive justification for the equivalence between the probability of single-photon detection [Eq. (2)] and the probability of two-photon coincidence [Eq. (6)] with respect to the phase modulator settings A1–A4 and B1–B4.

Here we provide a qualitative comparison of AQC and OW-AQC. While AQC requires that only one photon travel the distance between Alice and Bob after Alice attenuates Bob's signal to the single-photon level, OW-AQC requires that two photons travel the same distance. Thus, the loss incurred in OW-AQC is approximately twice that of AQC for the same distance. However, the use of a strong pulse on the first leg of the round trip in AQC also contributes to a disadvantage relative to OW-AQC. Specifically, backscattered light from the strong pulse is guided directly into Bob's detectors and can lead to unacceptably high bit-error rates. Another advantage of OW-AQC is immunity from the "Trojan horse attack",[5] in which Eve sends an optical signal into

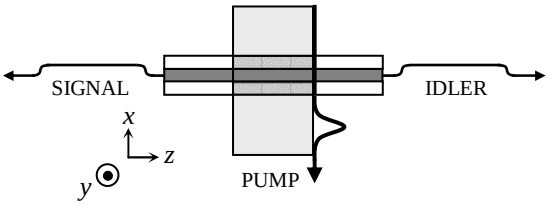

Figure 2. A schematic of auto-phase-matched SPDC, a new method for generating entangled-photon pairs with controllable frequency correlation. The z-polarized pulsed pump beam initiates counter-propagating y-polarized SPDC in the single-mode nonlinear waveguide. The joint spectrum of the down-converted beams is controlled by the spatial and temporal characteristics of the pump beam, as described in the text.

Alice's lab and measures the state of the reflected light in order to infer the setting of Alice's phase modulator. While an optical isolator can subvert this attack in the case of OW-AQC, the bidirectional flow of optical signals in AQC prevents this defence. In AQC, the probability of detection is independent of the delay τ in Bob's interferometer [see Eq. (2)], while in OW-AQC, the interference condition is independent of τ, but the visibility of this interference is not [see Eq. (6)]. Thus, while drift in the absolute values of the phase modulations will not affect the performance of OW-AQC, drift in the optical delay must be minimized to maintain high-visibility interference.

It is important to note that OW-AQC requires the frequency-correlated two-photon entangled state described in Eq. (3). This state has been investigated theoretically,[21] and several experimental methods for creating the state have been proposed.[20, 22–25] However, the state has not yet been experimentally demonstrated. While frequency-anticorrelated photon pairs are naturally generated when a monochromatic pump beam impinges on a nonlinear crystal, frequency-correlated photon pairs are only generated when a broad-band pump is used, and constraints on the phase *and* group velocities of the pump, signal, and idler are satisfied. These constraints can be satisfied in a collinear setup by exploiting the birefringence of the nonlinear crystal.[22, 23] Enhanced flexibility in satisfying these constraints can be achieved by imposing a periodic modulation of the crystal's nonlinear coefficient.[25] A second approach to satisfying these constraints is to exploit the inherent symmetry of a configuration in which a nonlinear waveguide is pumped at normal incidence such that the down-converted photons are counter-propagating.[20] The primary advantage of this auto-phase-matched method is that frequency-correlated photon pairs can be generated regardless of the dispersion characteristics of the nonlinear material.

3. AUTO-PHASE-MATCHED SPONTANEOUS PARAMETRIC DOWN-CONVERSION

The transverse-pump, counter-propagating geometry depicted in Fig. 2 has been noted as a promising source of entangled-photon pairs for both type-I[26] and type-II[27] SPDC. The most obvious advantages of this geometry over a collinear geometry pertain to the separation of the three interacting beams. In a transverse-pump, counter-propagating geometry, all three beams are traveling in different directions. Thus, the usual techniques for filtering the pump beam from the down-conversion and separating the down-converted beams at a beamsplitter are unnecessary.

The investigations in Refs. 26, 27 were limited to the case of a monochromatic pump beam. There are two primary advantages of pumping with a broadband beam perpendicular to the waveguide and arranging for type-I down-conversion. First, the dispersion relation for the pump beam plays no role in the phase-matching analysis, since the waveguide ensures phase-matching in the transverse direction. Thus, we refer to the method as *auto-phase-matched*. Second, the counter-propagating, identically-polarized signal and idler fields will be phase-matched in the long-crystal limit only if they have equal and opposite propagation vectors, a condition which entails equal frequency. Thus, the bandwidth of the pump determines the allowable range of the sum frequency of the signal and idler, and the longitudinal length of the illuminated portion of the crystal determines the allowable range of the difference frequency.

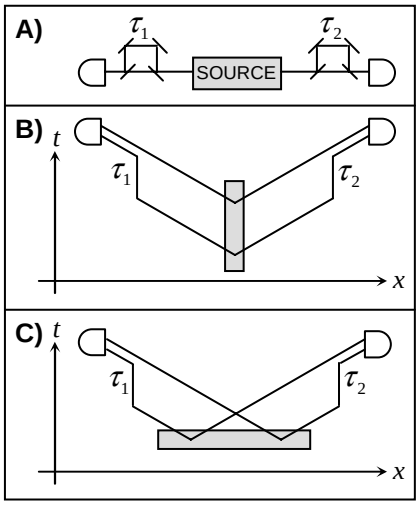

Figure 3. The Franson interferometer (A) and the two types of indistinguishability it can bring about (B and C). B) depicts the indistinguishability in time of creation of the photon pair, and C) depicts indistinguishability in position of creation of the photon pair. These two cases are shown in the text to correspond to frequency-anti-correlated photon pairs and frequency-correlated photon pairs, respectively.

We assume that the nonlinear coefficient and the propagation constants vary sufficiently slowly with frequency that they may be taken outside any frequency integrals in which they appear as integrand prefactors. Furthermore, we assume that the waveguide is long compared to the width of the pump beam such that the interaction length is controlled by the pump beam profile along the z-axis (see Fig. 2). Following the derivation in Ref. 26 of the quantum state of a counter-propagating photon pair, we have

$$|\Psi\rangle \propto \iint d\omega_l \, d\omega_r \, \tilde{E}_t(\omega_l + \omega_r) \tilde{f}_z \left[\Delta\beta(\omega_l, \omega_r)\right] \, |\omega_l\rangle_l \, |\omega_r\rangle_r, \tag{7}$$

where $\tilde{E}_t(\omega)$ and $\tilde{f}_z(\Delta\beta)$ are the respective Fourier transforms of the temporal and spatial functions describing the pump beam $E_p(t,z) = E_t(t) f_z(z)$, $\Delta\beta(\omega_l, \omega_r) = \beta(\omega_l) - \beta(\omega_r)$ is the difference in the waveguide propagation constant evaluated at ω_l and ω_r, and $|\omega\rangle_{l(r)}$ denotes a single photon at frequency ω moving to the left(right).

To investigate the dependence of $|\Psi\rangle$ on the characteristics of the pump, we choose Gaussian profiles in space and time for the pump pulse, such that $\tilde{E}_t(\omega) \propto e^{-\frac{1}{2}(\omega\tau)^2}$ and $\tilde{f}_z(\Delta\beta) \propto e^{-\frac{1}{2}(\Delta\beta W)^2}$, where τ and W are the duration and width (along the z-axis in Fig. 2) of the pump pulse, respectively. In the limit of a monochromatic pump ($\tau \to \infty$) with finite spatial extent, $\tilde{E}_t(\omega_l + \omega_r)$ is sharply peaked around the pump center frequency. Thus, the sum frequency of the signal and idler is fixed. This is the familiar frequency-anti-correlated case that is readily achievable in thin bulk crystals. In the limit of a finite-duration pump pulse of infinite spatial extent ($W \to \infty$), $\tilde{f}_z \left[\Delta\beta(\omega_l, \omega_r)\right]$ is sharply peaked around $\Delta\beta = 0$. Thus, photon pairs for which $\omega_l \approx \omega_r$ predominate. This is the frequency-correlated case that has hitherto only been achieved by imposing a group velocity matching condition.

The efficiency of this geometry in an GaAs-based waveguide of length 1 mm and transverse dimension 3 μm is calculated in Ref. 27 to range between 10^{-9} and 10^{-11} depending on the transverse profile of the waveguide. These figures compare favorably with the SPDC efficiencies achieved in more conventional bulk-crystal configurations (e.g., 10^{-13} in Ref. 28), though they are still several orders of magnitude less than that achieved in periodically poled lithium niobate waveguides (e.g., 10^{-6} in Ref. 29).

The Franson interferometer[30] is a natural tool for distinguishing frequency correlation and frequency anti-correlation. When the two delays (τ_1 and τ_2) are equal to within the reciprocal bandwidth of down-conversion, coincidence detections can be associated with indistinguishable pair-creation events (see Fig. 3A). If the down-converted photons are correlated in time (anti-correlated in frequency), the short-short two-photon amplitude

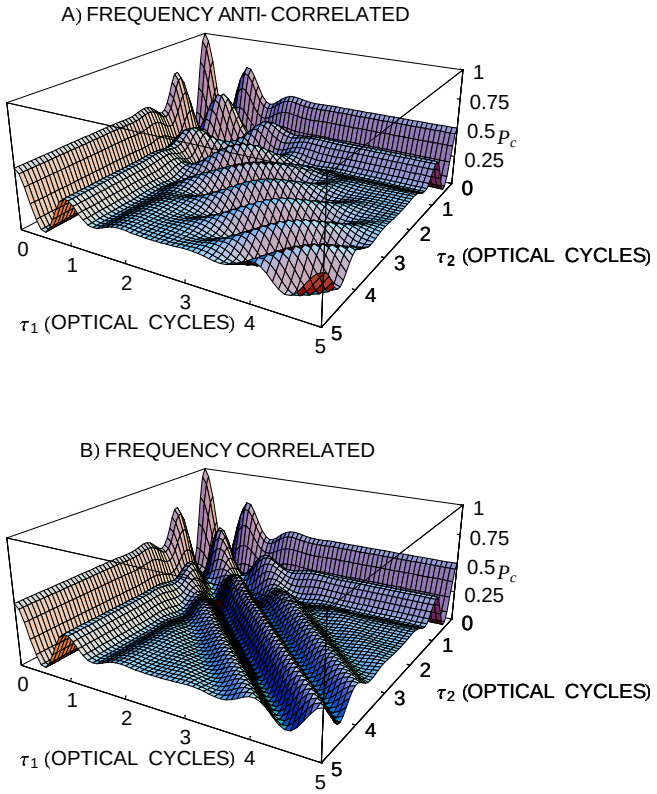

Figure 4. The probability of coincidence when frequency-anti-correlated (A) and frequency-correlated (B) states are analyzed with a Franson interferometer (see Fig. 3). The down-converted beams have center frequency $\omega_p/2$ and bandwidth $\omega_p/10$. τ_1 and τ_2 are in units of optical cycles at the center frequency of downconversion.

interferes with the long-long amplitude (see Fig. 3B). If the down-converted photons are anti-correlated in time (correlated in frequency), the short-long amplitude interferes with the long-short amplitude (see Fig. 3C). The duality between these two cases can be seen by comparing the loci of indistinguishable pair-creation events in the spacetime diagrams of Fig. 3B and Fig. 3C. The frequency-anti-correlated case depicted in Fig. 3B arises from the coherent superposition of pair-creation events at a fixed position over a range of times, while the frequency-correlated case depicted in Fig. 3C arises from the coherent superposition of pair-creation events at a fixed time over a range of positions. Note that while the interference visibility decreases in both cases as $\tau_1 - \tau_2$ approaches the reciprocal bandwidth of down-conversion, the relative phase between the interfering amplitudes depends on $\tau_1 + \tau_2$ in the frequency-anti-correlated case, and on $\tau_1 - \tau_2$ in the frequency-correlated case.

In Fig. 4 we plot the probability of coincidence in the Franson interferometer for the aforementioned limiting cases of the two-photon source: perfect frequency anti-correlation ($\tau \to \infty$, $W \to$ finite), and perfect frequency-anti-correlation ($\tau \to$ finite, $W \to \infty$). The finite values of τ and W are chosen such that the bandwidth of downconversion is $\omega_p/10$ in each case. The fourth-order fringes in the $\tau_1 \approx \tau_2 \gg 10/\omega_p$ region show that the Franson interferometer clearly distinguishes the two cases. The modulation is in the $\Delta\tau_1 = \Delta\tau_2$ direction the frequency-anti-correlated case and in the $\Delta\tau_1 = -\Delta\tau_2$ direction in the frequency-correlated case.

By establishing the signature of the perfect frequency-correlated state (the fourth-order fringes in Fig. 4B), we are able to compare the performance of experimental methods designed to produce this state. Specifically, the visibility of the fringes in Fig. 4B provides a measure of the quality of the frequency-correlated state. In Fig. 5 we plot a numerical calculation of the visibility achieved by the source described in Ref. 25 (thin line) and that achieved by our auto-phase-matched method (thick line) in a GaAs-based waveguide, for a range of interaction lengths. In the method of Ref. 25 the interaction length is the thickness of the crystal, while in our method

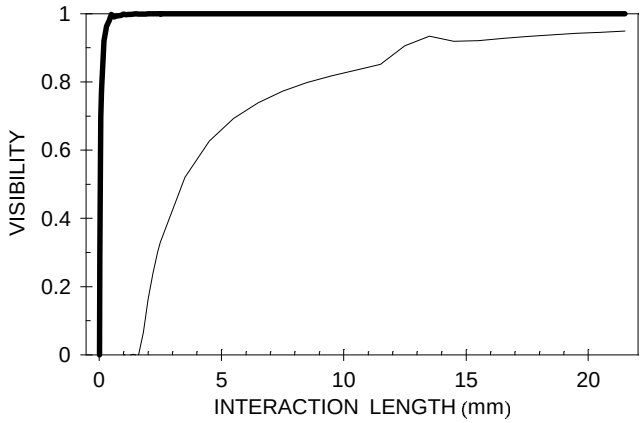

Figure 5. Numerical calculation of the fourth-order fringe visibility seen in a Franson interferometer when the perfect source of frequency-correlated photon pairs is approximated by the method described in Ref. 25 (thin line) and by the auto-phase-matched method described in the text (bold line). The plot depicts the effect of changing the interaction length of the nonlinear process while holding the bandwidth of the pump fixed.

the interaction length is the width of the pump beam in along the z-axis (see Fig. 2). In order to minimize the complicating effect of second-order interference, the visibility is calculated at the delay offset $(\tau_1, \tau_2) = (4/\sigma, 4/\sigma)$ where σ is the bandwidth of down-conversion.

4. CONCLUSIONS

We have described a new quantum cryptography implementation that exploits quantum entanglement to achieve the favorable stability of AQC without requiring a round trip between Alice and Bob. This work represents the first demonstration that quantum entanglement can offer practical advantages with respect to noise in quantum cryptography implementations. The next step in evaluating the promise of this approach for practical quantum cryptography involves explicit experimental proposals for creating the source described by Eq. (3) and quantitative performance analysis.

Both this work and Ekert's landmark paper[6] linking quantum cryptography and Bell's theorem describe two-photon interference effects that employ novel space-time configurations to perform tasks previously achieved with single-photon interference. These constructions can be seen as applications of Klyshko's theory of advanced waves, which provides a formal equivalence of one- and two-photon interference experiments.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation; the Center for Subsurface Sensing and Imaging Systems (CenSSIS), an NSF Engineering Research Center; and the Defense Advanced Research Projects Agency (DARPA).

REFERENCES

1. S. Wiesner, "Conjugate coding," *SIGACT News* **15**, pp. 78–88, 1983.
2. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing,* , pp. 175–179, 1984.
3. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *quant-ph/0212066* , 2002.
4. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, pp. 802–803, 1982.

5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, pp. 145–195, 2002.
6. A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, pp. 661–663, 1991.
7. J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics (Long Island City, N.Y.)* **1**, pp. 195–200, 1964.
8. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**, pp. 557–559, 1992.
9. A. V. Belinsky and D. N. Klyshko *Laser Phys. (Moscow)* **2**, p. 112, 1992.
10. D. N. Klyshko, "On the theory for two-photon light interference," *Laser Phys. (Moscow)* **2**, p. 997, 1992.
11. T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," *Phys. Rev. A* **52**, pp. R3429–R3432, 1995.
12. N. J. Cerf and C. Adami, "Negative entropy and information in quantum mechanics," *Phys. Rev. Lett.* **79**, pp. 5194–5197, 1997.
13. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, ""plug and play" systems for quantum cryptography," *Appl. Phys. Lett.* **70**, pp. 793–795, 1997.
14. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'plug & play' quantum key distribution," *Electron. Lett.* **34**, pp. 2116–2117, 1998.
15. M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, and J. P. Ciscar, "Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols," *J. Mod. Optics* **47**, pp. 563–579, 2000.
16. D. S. Bethune and W. P. Risk, "Enhanced autocompensating quantum cryptography system," *Appl. Opt.* **41**, pp. 1640–1648, 2002.
17. T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, ""circular type" quantum key distribution," *IEEE Photon. Tech. Lett.* **14**, pp. 576–578, 2002.
18. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," *quant-ph/0203118* , 2002.
19. Z. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "One-way entangled-photon autocompensating quantum cryptography," *Phys. Rev. A* **67**, p. 062309, 2003.
20. Z. D. Walton, M. C. Booth, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Controllable frequency entanglement via auto-phase-matched spontaneous parametric down-conversion," *Phys. Rev. A* **67**, p. 053810, 2003.
21. R. A. Campos, B. E. A. Saleh, and M. C. Teich, "Fourth-order interference of joint single-photon wave packets in lossless optical systems," *Phys. Rev. A* **42**, pp. 4127–4137, 1990.
22. T. E. Keller and M. H. Rubin, "Theory of two-photon entanglement for spontaneous parametric down-conversion driven by a narrow pump pulse," *Phys. Rev. A* **56**, pp. 1534–1541, 1997.
23. R. Erdmann, D. Branning, W. Grice, and I. A. Walmsley, "Restoring dispersion cancellation for entangled photons produced by ultrashort pulses," *Phys. Rev. A* **62**, pp. 53810–53823, 2000.
24. Y.-H. Kim and W. P. Grice, "Generation of pulsed polarization entangled two-photon state via temporal and spectral engineering," *J. Mod. Optics* **49**, pp. 2309–2323, 2002.
25. V. Giovannetti, L. Maccone, J. H. Shapiro, and F. N. C. Wong, "Generating entangled two-photon states with coincident frequencies," *Phys. Rev. Lett.* **88**, pp. 183602–183605, 2002.
26. M. C. Booth, M. Atatüre, G. Di Giuseppe, B. E. A. Saleh, A. Sergienko, and M. C. Teich, "Counter-propagating entangled photons from a waveguide with periodic nonlinearity," *Phys. Rev. A* **66**, p. 23815, 2002.
27. A. De Rossi and V. Berger, "Counterpropagating twin photons by parametric fluorescence," *Phys. Rev. Lett.* **88**, p. 043901, January 2002.
28. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.* **84**, pp. 4729–4732, 2000.
29. S. Tanzilli, H. D. Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. D. Micheli, D. B. Ostrowsky, and N. Gisin, "Highly efficient photon-pair source using periodically poled lithium niobate waveguide," *Electron. Lett.* **37**, pp. 26–28, January 2001.
30. J. D. Franson, "Bell inequality for position and time," *Phys. Rev. Lett.* **62**, pp. 2205–2208, 1989.