Review & Approval

Prepare Request
Search Requests
Generate Reports
Approvals
Help
Wizard

Search Requests
New Search
Refine Search
Search Results

Clone Request
Edit Request
Cancel Request

Search Detail

Submittal Details

Document Info

Title : Review of Entangled State Quantum Cryptography: Eavesdropping on teh Ekert Protocol

Document Number : 5240581 SAND Number : 2006-1297 P

Review Type : Electronic Status : Approved

Sandia Contact : DEBENEDICTIS,ERIK P. Submittal Type : Report

Requestor : DEBENEDICTIS,ERIK P. Submit Date : 02/28/2006

Comments : Due to a malfunction in the Web application, a relevant comment cannot be entered in this field. See the first page of the document.

Peer Reviewed? : N

Author(s)

DEBENEDICTIS,ERIK P.

Partnership Info

Partnership Involved : No

Partner Approval : Agreement Number :

Patent Info

Scientific or Technical in Content : Yes

Technical Advance : No TA Form Filed : No

SD Number :

Classification and Sensitivity Info

Title : Unclassified-Unlimited Abstract : Document : Unclassified-Unlimited

Additional Limited Release Info : None.

DUSA : None.

Routing Details

Role	Routed To	Approved By	Approval Date
Derivative Classifier Approver	MCDONALD,TIMOTHY S.	MCDONALD,TIMOTHY S.	02/28/2006
Conditions: A few editorial suggestions have been communicated to the auther.			
Classification Approver	WILLIAMS,RONALD L.	WILLIAMS,RONALD L.	03/01/2006
Conditions:			
Common Look & Feel Approver	BRITTENHAM,PHILLIP W.	BRITTENHAM,PHILLIP W.	03/02/2006
Conditions: If this is published as a journal article include Sandia Funding Statement. Checks positioning on headings.			
Manager Approver	PUNDIT,NEIL D.	PUNDIT,NEIL D.	03/02/2006
Conditions:			
Sandia Contact	DEBENEDICTIS,ERIK P.	DEBENEDICTIS,ERIK P.	03/02/2006
Agreement: Sandia Contact has agreed to incorporate above listed conditions prior to release. Comments:			
Administrator Approver	LUCERO,ARLENE M.	CANDELARIA,ALYCIA D.	04/24/2007

Please add funding statement: Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Created by WebCo Problems? Contact CCHD: **by email** or **at 845-CCHD** (2243).

For Review and Approval process questions please contact the **Application Process Owner**

Approved for public release
SAND2006-1297P

Review of Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol

Erik P. DeBenedictis
Sandia National Laboratories

Quantum cryptography is an emerging technology for completely secure communications. This article reviews a specific paper [1] reporting early experimental work on a quantum cryptographic link. The article focuses on how the field developed around ideas in the reviewed paper. Notably, the maximum distance between stations has increased dramatically since the paper, driven by both equipment and improved protocols.

PACS numbers: 03.67.Dd

The Role of Quantum Cryptography

The paper under review is about Quantum Cryptology, an emerging technology that can fix a pending vulnerability in data protection. Classical cryptology protects data by mathematical scrambling that is nominally hard to reverse for unauthorized parties [2]. However, future quantum computers are expected to be able to break the most popular codes [3]. Much existing data is now vulnerable to an adversary eavesdropping on a data stream, recording it, and cracking the code with a quantum computer in some future year. The fact that today's secrets will be exposed someday creates concern for parties with secrets that should be long-lived.

Quantum cryptography protects secrets through a physical process rather than data scrambling and thus fills a slightly different role. In effective quantum cryptography, unauthorized parties are unable to get protected information through eavesdropping and thus have no data to record and subsequently analyze.

The paper and later work study quantum cryptology at several levels of security. At the higher level, quantum cryptology can secure against a potential adversary that has the most powerful equipment permitted under the laws of physics [4]. It is a challenge to achieve long distances with quantum cryptology; curve ① in FIG 1 could represent maximum distance feasible for unbreakable quantum cryptography. Curve ① will be monotonically increasing because once technology is perfected it is not taken away.

However, those interested in protecting secrets have another option. Curve ② in FIG 1 achieves greater distance by using a quantum cryptology method that may be imperfect but is good enough to foil the best equipment an adversary is believed to have at the time of transmission. Since eavesdropping of quantum encrypted data must occur in real time, the standard of curve ② is enough to assure perpetual protection of secrets. Curve ② may go up or down representing relative progress of encryption versus interception technology.

As will be described below, some improvements raise curve ①, curve ②, or both.

Overall Architectures

Quantum cryptography is envisioned as using Quantum Key Distribution (QKD) to distribute an encryption key of hundreds to thousands of bits that is subsequently used for classical encryption of the actual data [5]. The quantum methods are used only to establish a shared secret random key between two communicating parties safe against any hypothetical eavesdropper (given pseudonyms Alice, Bob, and Eve in the literature and in this document). Symmetric encryption methods for securing the actual data are believed sufficiently secure and not a topic of the reviewed paper or this review.

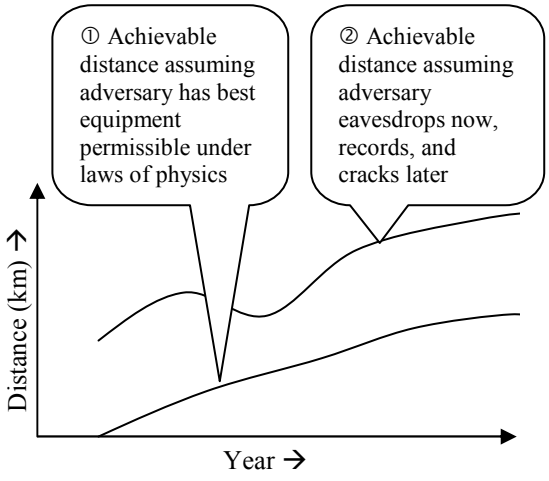

FIG 1. Future progress in quantum cryptography, illustrating roles of systems with perfect and imperfect security.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

The architectures that will be described below all involve nominal single photons being transmitted via fiber or free space link. The receiver will have sampling timeslots and a classical link to the sender.

BB84 and Attenuated Lasers

The BB84 protocol [6] is historically the oldest and arguably the least flexible. The BB84 protocol requires a single photon source, which is polarization-modulated by Alice before transmission to Bob. An attenuated laser is simple and sufficient as a single photon source, yet the relatively high rate of double photons creates a security vulnerability to the Photon Number Splitting (PNS) attack. The primary mitigation for PNS attacks is to reduce link distance. Low link distances opened the door for this simpler protocol to be challenged by the Ekert and other protocols more effective at longer distances.

Ekert Protocol and Bell Pairs

The Ekert protocol [7] uses entangled photon pairs (Bell states) as a source and achieves somewhat greater flexibility than the BB84 protocol. In the Ekert protocol, Alice and Bob share and measure a Bell pair. In accordance with well-known properties of Bell pairs, Alice's and Bob's measurements are correlated, yet this correlation is not available to Eve. See Ref. 1 for a diagram. As will be explained later in this paper, the Ekert and related protocols achieve equal security to the BB84 protocol but at longer distances.

Decoy State Protocols and Quantum Repeaters

The Ekert protocol is itself limited and may be giving way to other methods capable of reaching longer distances. BB84, Ekert, and their many variant protocols prohibit signal "regeneration" (seeing it as an attempt to eavesdrop) and are thereby confronted by an exponential loss of signal with distance (which eventually becomes limiting). Protocols including decoy states to foil PNS attacks can achieve remarkable distances for unamplified signals (perhaps 300 km), but even these are a long way from the needed transcontinental distances. There are also "quantum repeater" protocols [8] for extending entanglement (the basis of the Ekert protocol) by a factor of *n* in *log n* steps [9]. These ideas could be seen as enhancements to the Ekert protocol or as completely new protocols.

PNS Attack Limits Distance

The distance of a quantum cryptographic link is limited by a host of factors, including the security model (choice of curve ① vs. ② of FIG 1). PNS attacks are not feasible with today's technology and thus they can be mitigated either by clever technology or the designer choosing only the security model of curve ② of FIG 1. On the other hand, lower loss fibers and better receivers will increase link distance for both curves ① and ② of FIG 1. Since PNS attack mitigation involves design tradeoffs (as opposed to simple technology improvements), they will be discussed first.

Realistic single photon sources have some probability of emitting double or multiple photons. These extra photons represent a security vulnerability because they are in the same state as data-bearing photons. Although there is R&D on true single-photon sources [11], such sources are immature and all reported experiments use attenuated lasers and parametric down conversion that exhibit Poisson statistics for multiple photon emission.

For attenuated lasers, the Poisson statistics control performance. If the average photon number per timeslot is μ, the probability of 2, 3… photon emissions is $\mu^2/2!$, $\mu^3/3!$… Since the probability that a photon emission event has multiple photons is $O(\mu)$, multiple photon emissions can be reduced by cutting μ. Unfortunately, μ is also the signal power and cutting it results in more empty timeslots and less system throughput.

While Bell pair emission in the Ekert protocol (e.g. by parametric downconversion) obeys Poisson statistics as well, the designer can exploit the fact that an emission event creates coincident trigger events for both Alice and Bob. There are a variety of strategies in use or proposed [5, 12] where Alice (who now knows which timeslots contain events) can squeeze out empty time slots, resulting in an average photon number of O(1) of which fraction μ have multiple photons. The direct consequence is more signal power, but the design point can be changed as a second order effect to decrease the fraction of multiple photon events.

In a PNS attack, Eve separates double photon events into a single photon that she saves and sends the remainder to Bob. If there are enough double photons, the saved photons contain enough information to defeat the encryption.

The vulnerability to a PNS attack is created by excessive link distance, and can thus be seen as a distance-limiting characteristic per curve ① of FIG.

1. To defeat the encryption with PNS, Eve needs almost as much information Bob. Eve must get this information solely from multiple photon events, because this is all she can intercept. This is possible only if Eve can intercept enough multiple photon events to reconstruct the entire data stream to Bob. Say the Alice-Bob link transmittance is η. In a PNS attack, Eve installs a zero-loss shunt and apparatus that converts the fraction $\mu \leq \eta$ proportion of double photon events into single photon events (destroying the original single photon events) that are passed along to Bob. Eve keeps a copy to perform unauthorized decryption, but Bob sees the same total number of packets and is thus oblivious to the eavesdropping.

The obvious mitigation is to limit the link distance such that $\mu > \eta$ so there are not enough double photon events available to Eve.

Performance of the Ekert Protocol

The paper reviewed an experiment carried out on a lab bench, but nonetheless addressing issues identified in the references for reaching long distances with high security. One of the references [13] illustrated the state of the art in understanding distance estimation as of the year 2000. The author has coded Ref. 13's equations into a computer program and duplicated to the extent possible the data from that paper. (The author then updated the technology assumptions to understand the impact on advances between 2000 and now, more on this later.) The sections below will include a summary of the performance model pertinent to the reviewed paper.

Error Correction

Some photons will be detected incorrectly due to natural equipment imperfections, but the same observed behavior could also arise from eavesdropping. In either case, the errors must be corrected with limited disclosure to a potential eavesdropper. There are several approaches, primarily (1) discarding erroneous bits, (2) bi-directional error reconciliation [14] and (3) unidirectional error correction code. The performance model in Ref. 13 uses method (2) and reports overheads for typical error rates of e=.01-.15 of $f[e]$=16-35%.

Privacy Amplification

Privacy amplification mitigates vulnerability if Eve obtains a few key bits unnoticed. A scenario of this vulnerability is that Eve acquires perhaps a few dozen bits of a much longer key by measuring some photons and intercepting classical communications. While a few dozen bits does not disclose the key, it could cut runtime for a brute force search by a factor of $2^{few\ \ dozen}$. Privacy amplification neutralizes this advantage by hashing the key into a bit string shorter by fraction τ_1. The number of bits reduced by privacy application depends on many factors. However, τ_1 should shorten by at least as many bits as were disclosed during error correction and by as many bits are were carried multiple photon packets (unless there is a different mitigation to PNS attacks).

As an example, shortening due to bi-directional error correction protocols is given in Ref. 13 as

$\tau_1(e) = \log_2(1 + 4e - 4e^2)$ for $e \leq .5$

$\tau_1(e) = 1$ for $e > .5$

Multiple Photon Events

As discussed previously, Parametric DownConversion (PDC) sources create single photon streams with fewer multiple photon events to be subsequently eliminated by privacy amplification. S_m is the fraction of photons that are part of multi-photon events and is given below for Weak Coherent Pulses (WCP) and PDC.

WCP: $S_m = 1 - (1 + u)\, e^{-u}$

PDC: $S_m = p_{post}\, u^2/(1+u)^2$,

where p_{post} is the probability that Alice accepts a photon at her local detector as a valid part of the Ekert protocol.

It should be noted here that the reviewed paper demonstrated a "six state" protocol [15], where polarizations are prepared by Alice and detected by Bob along $\pm X$, $\pm Y$, and $\pm Z$ axes. While this method cuts the amount of information available to Eve and hence the number of bits that must be removed in privacy amplification, it was not a method destined to drive subsequent progress.

The equation below from Ref. 13 gives the throughput $G^{(\text{multi})}$ in terms of key bits per timeslot, valid for both WCP and PDC (Ekert) protocols depending on the value of S_m.

$$G^{(\text{multi})} = \tfrac{1}{2}\, p_{\text{post}}\, p_{\text{exp}} \left\{ \frac{p_{\text{exp}} - S_m}{p_{\text{exp}}} \times \left[1 - \log_2 \left[1 + 4e \frac{p_{\text{exp}}}{p_{\text{exp}} - S_m} - 4 \left[e\, \frac{p_{\text{exp}}}{p_{\text{exp}} - S_m} \right]^2 \right] \right] + f[e]\, [e \log_2 e + (1-e) \log_2 (1-e)] \right\}$$

where p_{exp} is the probability of an event in a timeslot.

Curves ①-④ on the left of FIG 2 were plotted using the equations in Ref. 13, including the

equations given above and based on technology similar to or the same as in the paper reviewed [1].

Lower Detector Dark Count

Subsequent to when the paper under review was written, some of the same scientists developed apparatus capable of much longer distances [12]. The approach involved better detectors (more sensitivity and lower dark count). Better detectors improve distance for both curves ① and ② in FIG. 1, suggesting the value in recent developments in high-efficiency, low dark count detectors [16, 17] called Transition Edge Sensors (TESs).

As link attenuation increases (longer fibers), the number of detected photons drops exponentially. This exponentially reduces bandwidth but the link continues to work – except for the problem of detector dark count. When detector dark counts exceed the signal from valid photon detections, even the few good photons get lost in the noise [13].

The Transition Edge Sensor (TES) is a superconducting detector comprised of a 25μm^2 Tungsten square at 110 mK. The raw detector can detect single photons with 89% efficiency. However, the Los Alamos team applied elaborate filtering to screen out extraneous photons (cutting efficiency to 65%) but resulting in measured dark count of 27 Hz. They estimate a more refined filtering scheme could achieve a dark count of .03 Hz.

The Los Alamos team performed an experimental test based on a 50 km spool of fiber in the laboratory. Based on the performance of this configuration, they estimate maximum distance of 138 km. However, the paper also indicates that an improved filter for stray light (termed a "non crude" detector) would increase peak distance to 271 km.

FIG 2 also includes curves on the analytical performance estimate for quantum cryptographic links based on the improved detectors.

Decoy States and PNS Attack Resistance

However, there is a "decoy state" countermeasure [18, 19] that defeats the PNS attack with negligible distance loss. In the decoy countermeasure, Alice intentionally injects nominally two-photon events into the fiber at known locations. Based on data returned by Bob as part of the protocol, Alice can calculate the transmittance of nominally single and nominally double photon events. A uniformly absorbing link will have an easily calculated effect on single and double photon events, but a PNS attack would absorb all single photon events and transmit multiple photon events with unnaturally high probability. Thus, the decoy state countermeasure would seem to fix the problem of multiple photon sources without a distance compromise.

Curves ⑤-⑧ in FIG 2 apply the performance equations applicable to the paper under review to

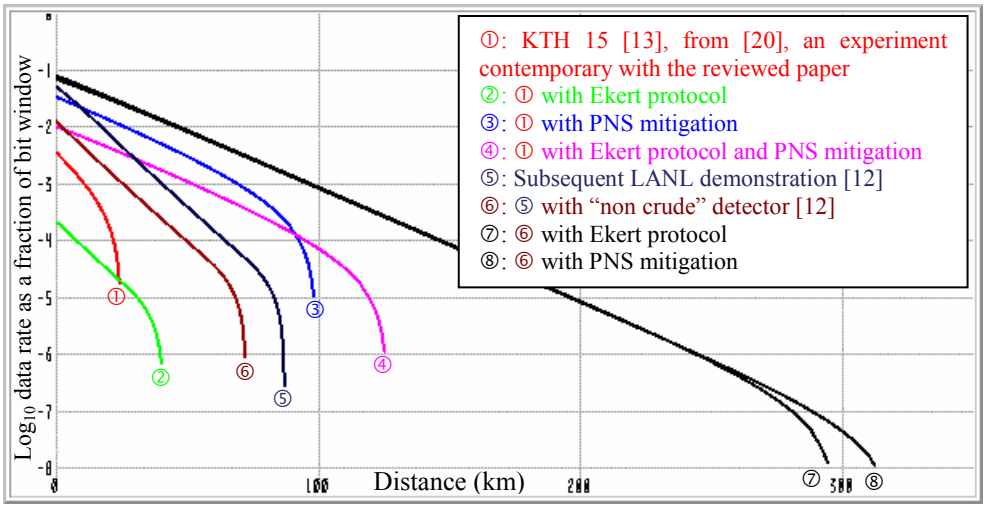

FIG 2. Output from author's computer program showing throughput rate for optimally configured quantum cryptology protocols. Includes protocol in reviewed paper reporting on an experiment [1] (which matches results from [13]) and variants that were proposed at the time or subsequently. Note: curves ⑦ & ⑧ achieve great distance, yet the data rate would be 1 MHz × 10^{-8}, or 1 bit per 100 seconds.

hypothetical systems employing improved detectors and decoy states to mitigate PNS attacks.

Conclusions

The paper under review offered early experimental verification of one of (what was then) two approaches to quantum cryptography. It is interesting to see changes in the field that occurred in the six years that followed.

Notably, the paper reviewed an experiment with Alice and Bob connected by a short fiber. Six years later, there is a 50 km spool of Telco standard optical fiber in the experiment. Extrapolation to longer spools suggests that the experiment should work across 83 km to 138 km of fiber and speculation some equipment redesign could increase the distance to ~300 km.

For O(100 km) links, the significance of the Eckert protocol seems to have diminished. Six years ago, the Ekert protocol enabled longer links or a stronger security model (curve ① vs. ② in FIG. 1), but subsequent development of decoy states and better detectors dilute the advantage of the Ekert protocol (to wit the similarity of curves ⑦ and ⑧ of FIG 2).

The prospects of extending single fiber links to transcontinental distances seem dim. There is an entanglement extension method that may permit transcontinental distances, eclipsing existing methods in distance and importance. Whether this is a new protocol or an extension of the Ekert protocol is a matter of how one chooses to assign credit.

It is easy to see the importance of BB84 and the Ekert protocols in current work, but it is clear that other advances have been very important as well. In particular, decoy states produce a major uptick in link distance whereas the 6 state vs. 4 state measurements in the paper reviewed were much less effective.

References

[1] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733–4736 (2000).

[2] The code book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Fourh Estate, London (1999).

[3] P. W. Shor, SIAM Review, **41**, 303 (1999).

[4] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, IEEE Transactions on Information Theory, Vol. 49, No. 2, pp. 457-475.

[5] Quantum Cryptography, quant-ph/0101098, submitted to Reviews of Modern Physics Oct. 10, 2005.

[6] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

[7] A. K. Akert, Phys. Rev. lett, **67**, 1991.

[8] H.-J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[9] L. Childress, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, quant-ph/0502112 [this us unlikely to be the original reference]

[10] G. Brassard, N. Lukenhaus, T. Mor, B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[11] ARDA Quantum Information Science and Technology Roadmap, Part 2, section 6.3.

[12] D. Rosenberg, S. W. Nam, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, arXiv:quant-ph/0510062.

[13] N. Lutkenhaus, quant-ph/9910093

[14] G. Brassard and L. Salvail in Advances in Cryptology – EUROCRYPT '93, Vol. 765 of Lecture Notes in Computer Science, edited by T. Helleseth (Springer, Berlin, 1994, pp. 410-423.

[15] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1999).

[16] D. Rosenburg, A. E. Lita, A. J. Miller, S. Nam, and R. E. Schwall, IEEE Trans. Appl. Supercond. **15** (2) 575 June 2005.

[17] D. Rosenberg, A. E. Lita, A. J. Miller, S. W. Nam, Phys. Rev. A **71**, 061803(R) (2005).

[18] Quantum Key Distribution with High Loss: Toward Global Secure Communications, Won-Young Hwang, Phys. Rev. Lett. **91**, 057901.

[19] J. W. Harrington, J. M. Ettinger, R. J. Hughes, J. E. Nordholt, arXiv:quant-ph/0503002.

[20] B. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999).