Robust and Efficient Sifting-Less Quantum Key Distribution Protocols

Frédéric Grosshans

Robust and Efficient Sifting-Less Quantum Key Distribution Protocols

Frédéric Grosshans

Laboratoire de Photonique Quantique et Moléculaire, ENS de Cachan, UMR CNRS 8735, 94235 Cachan cedex, France[*]
(Dated: July 16, 2009, version 1.2)

We show that replacing the usual sifting step of the standard quantum-key-distribution protocol BB84 [1] by a one-way reverse reconciliation procedure increases its robustness against photon-number-splitting (PNS) attacks to the level of the SARG04 protocol [2, 3] while keeping the raw key-rate of BB84. This protocol, which uses the same state and detection than BB84, is the $m = 4$ member of a protocol-family using m polarization states which we introduce here. We show that the robustness of these protocols against PNS attacks increases exponentially with m, and that the effective keyrate of optimized weak coherent pulses decreases with the transmission T like $T^{1+\frac{1}{m-2}}$.

Over the last 25 years, quantum key distribution (QKD) has emerged as the main application of quantum information. In most experimental realizations [4], the legitimate partners — traditionally named Alice and Bob — use the BB84 protocol [1] with weak-coherent-pulses (WCP), *i.e.* Alice sends polarized coherent states to Bob, and Bob measures their polarization to obtain the raw-key. Alice and Bob then post-select a subset of the measurement to obtain the sifted-key from which the cryptographic key is extracted. If Alice sends perfect single-photons, there is no way for an eavesdropper — traditionally named Eve — to learn anything about the sifted key without introducing errors. But, with WCPs, Alice only approximates single-photon, and she sometimes sends multiphoton pulses, on which Eve can get all the information through photon-number-splitting (PNS) attack [5]. SARG04 [2, 3] showed that, with the same modulation and detection than BB84, one can construct a protocol more robust against PNS, since Eve only gains partial information from 2 photons pulse and needs to wait for the rarer 3 photons pulses to gain the full information. However, for the same pulse intensity, SARG04's rate is the half of BB84 at low losses, because of the lower rate of it sifting. As shown in [3] SARG04's robustness can be increased by using m polarizations instead of 4, at the price of a lower sifting rate $\propto m^{-3}$. This article shows that this price is not necessary, and that it is possible to have the best of both protocols, *i.e.* BB84's rate and SARG04's robustness against photon number-splitting attacks.

BB84 and SARG04 are sifting based protocols *i.e.* protocols where a part of the data is "sifted away" because Alice's state and Bob's measurement are not in the "same basis". We will look here at sifting-less protocols, *i.e.* protocols where this discussion is absent, and therefore, where the "wrong-basis" data are kept in the raw-key.

Protocol description. Alice randomly choses one linear polarization and sends the corresponding phase-randomized weak coherent pulse (WCP). Let $m \geq 3$ the total number of possible polarizations. To simplify the analysis, we will suppose that the polarizations are uniformly distributed along a great circle of Poincaré's sphere. Let $|0\rangle$ and $|1\rangle$ be the state of two orthogonally polarized single photons. If the pulse contains n photon, Alice sends the state $|x, n, m\rangle := |x\theta_m\rangle^{\otimes n}$ with $\theta_m := \frac{2\pi}{m}$, x uniformly chosen in $[\![0, m-1]\!]$, and $|\theta\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$. If $m = 4$, one has the 4 states used in BB84, SARG04 as well as LG09 [6].

Bob measures the polarization of the pulses after a propagation into a channel of transmission T. The public comparison of a small subset of the measurements allows Alice and Bob to statistically determine the characteristic of the channel, namely T and its qubit error rate (QBER). In this first analysis, we will suppose this statistical evaluation to be exact, neglecting the finite size effects [7]. We will also limit ourselves to the error-less case, where the QBER is 0, excepted in the conclusion where the influence of errors is briefly studied.

There are several possibilities for Bob's measurement. We will limit Bob's apparatus to single-photon detector based set-ups, similar to the one used in the BB84 and SARG04 protocols. This will prevent Alice and Bob to extract all the information allowed by the Holevo bound $S(X:Y) = T \log 2$, or to use continuous-variable detection set-up [6].

Since Bob's measurement is based on single photon detectors, Alice and Bob need to postselect-away the event when Bob has received no photon *i.e.* when Bob's detectors do not click. This can be done by one-way classical communication from Bob to Alice. The kept events constitute a fraction $1 - e^{-T\mu} \simeq T\mu$ of the sent pulses if the sent WCP have a mean photon number of μ. They constitute the raw key, X for Alice and Y for Bob.

When Bob receives a single photon, he makes the POVM $\left\{\frac{2}{m}\left|y\theta_m + \pi\right\rangle\left\langle y\theta_m + \pi\right|\right\}_{y \in [\![0, m-1]\!]}$. The π dephasing doesn't change anything if m is even, but increases the mutual information $S(X:Y)$ between Alice and Bob when m is odd. In particular, it ensures that, for any state sent by Alice, one outcome ($y = x$) of Bob's measurement is impossible. One can then easily show $S(Y) = \log m$;

$$\mathcal{P}(y|x, m) = \frac{1}{m}\left(1 - \cos(y - x)\theta_m\right); \qquad (1)$$

$$S(Y|X) = \log m - \frac{1}{m} \sum_{k=0}^{m-1} (1 - \cos k\theta_m) \log(1 - \cos k\theta_m); \tag{2}$$

$$S(X{:}Y) = \frac{1}{m} \sum_{k=0}^{m-1} (1 - \cos k\theta_m) \log(1 - \cos k\theta_m). \tag{3}$$

The mutual information between Alice and Bob $S(X{:}Y|m)$ decreases slightly with m, from $\log \frac{3}{2} = 0.5850$ bits for $m = 3$ to $\frac{1}{2\pi} \int (1 - \cos k\theta) \log(1 - \cos k\theta) d\theta = 0.4427$ bits in the continuous limit $m \to \infty$. For $m = 4$, we have $S(X{:}Y|m=4) = \frac{1}{2} \log 2$.

When Bob receives more than one photon, several detectors can click. This gives him more information than single clicks, so neglecting this case , as done above, is pessimistic. This corresponds to Bob randomly chosing between the various detection results.

In a reverse reconciliation (RR) scheme [8, 9], Alice and Bob can share a common key of length $S(X{:}Y)$ provided Bob sends to Alice $S(Y|X)$ bits of information. For example, when $m = 4$, Bob needs to send 1.5 bits per pulse. This can be done by revealing his measurement basis (1 bit/pulse) and using the syndrome of a good erasure correcting (see *e.g.* [10, Chapter 50]) code which will be slightly over $\frac{1}{2}$ bit long per pulse. Indeed, when Bob has revealed his basis measurements, Alice knows which bits of Y she knows (the one with the right basis), and the one she does not know (the other ones), and this corresponds to an erasure channel of rate $\frac{1}{2}$.

Eavesdropping. Their use of erasure correcting codes instead of interactively throwing some bits away is at the heart of the resistance of this protocol against PNS attacks : on 2-photon pulses, Eve can keep a copy of the pulse sent by Alice, and, even if she knows the basis of Bob's measurement, she ignores whether Alice sent a state in the right basis or not. Therefore, in this case, Eve measurement has at best a 25% error-rate, giving her at most $h(\frac{1}{4}) = 0.1887$ bits of information — where $h(\cdot)$ is the binary entropy — while Alice still has half a bit. The net key rate of 2-photon pulses is then 0.3113 bits. In BB84, on the contrary, Alice reveals her basis choice, living her on equal footing with Eve for 2-photons pulses.

Note that when m is even, the above idea for the reconciliation can be generalized *i.e.* Bob reveals $\log m - \log 2$ bits for the basis $y \mod \frac{m}{2}$ and use the appropriate error correcting code for the remaining information. We are then in a situation where Alice has different known error rates $\frac{1}{2}(1 - \cos(x - y \mod \frac{m}{2})\theta_m)$ for different bits while Eve only sees the average error rate. The following paragraphs will study the above affirmations more formally, in the asymptotic and error-less regime.

Of course, if Alice sends perfect single photon pulses, the lack of errors guarantees a perfect secrecy of the $S(X{:}Y)$ key. However, if Alice uses weak coherent pulses (WCP) some attacks become possible without introducing errors, namely *intercept resend with unambiguous state*

discrimination (IRUD) and *photon number splitting attacks* (PNS), as well as a combination of the two.

In any case, since Alice's pulses are phase randomized, Eve optimal attack starts by a quantum non-demolition measurement of the photon number n of Alice's pulse [5]. The state sent by Alice is then projected onto

$$|x, n, m\rangle = |x\theta_m\rangle^{\otimes n} = 2^{-\frac{n}{2}} (|0\rangle + e^{ix\theta_m} |1\rangle)^{\otimes n} \tag{4}$$

$$= 2^{-\frac{n}{2}} \sum_{b=0}^{2^n - 1} e^{i\|b\|\theta_m} |b\rangle, \tag{5}$$

where $|b\rangle$ is the tensorial binary development of b and $\|b\|$ its Hamming weight. Note that all terms with the same Hamming weight w modulo m have the same phase prefactor $e^{iw\theta_m}$. These $\binom{n}{w[m]}$ vectors are orthogonal. We have defined

$$\binom{n}{w[m]} := \sum_{d=0}^{\infty} \binom{n}{w + dm}, \tag{6}$$

where we have used the usual convention for the binomial coefficient $\binom{n}{w} = 0$ for $w > n$. Let's define, for each $w \in [\![0, m-1]\!]$,

$$|w[m]\rangle_n := \frac{1}{\sqrt{\binom{n}{w[m]}}} \sum_{\substack{b \in [\![0, 2^n - 1]\!] \\ b \equiv w[m]}} |b\rangle. \tag{7}$$

We can then rewrite the state $|x, n, m\rangle$ as

$$|x, n, m\rangle = 2^{-\frac{n}{2}} \sum_{w=0}^{m-1} e^{iw\theta_m} \sqrt{\binom{n}{w[m]}} |w[m]\rangle_n. \tag{8}$$

When Eve measures n photons, she can either block the pulse, perform an IRUD attack or a PNS attack.

IRUD *attacks.* If Eve makes an IRUD attack, her success probability is given in [11] as

$$\mathcal{P}(\Delta|m, n) = 2^{-n} m \min_{w \in [\![0, m-1]\!]} \binom{n}{w[m]}. \tag{9}$$

This probability is not null iff $n \geq m - 1$, and its value increases each time n increases by 2. Its first nonzero value is $2^{-m+1}m$ for $n \in \{m + 1, m + 2\}$. If Eves blocks a fraction b_n of the n-photon pulses, these can be a the ones where an unambiguous discrimination has failed. She can then resend with no error a fraction u_n of the original pulses as big as

$$u_n = \max\left(\frac{\mathcal{P}(\Delta|n, m)}{1 - \mathcal{P}(\Delta|n, m)} b_n; 1 - b_n\right). \tag{10}$$

In other words, she can intercept and resend $\frac{\mathcal{P}(\Delta|n, m)}{1 - \mathcal{P}(\Delta|n, m)}$ pulses for each pulse she blocks, without introducing any error.

On remaining $p_n = 1 - b_n - u_n$ pulses, she can perform a PNS attack, keeping $n - 1$ photons and transmitting the remaining one unperturbed to Bob. We have

$$p_n = \min\left(\frac{1 - \mathcal{P}(\Delta|n, m) - b_n}{1 - \mathcal{P}(\Delta|n, m)}; 0\right). \tag{11}$$

One can construct a Markov chain $Y \leftrightarrow X \rightarrow |x, n-1, m\rangle$, and since the latter is the state held by Eve when she performs a PNS attack, $S(Y{:}E|n, \textsc{pns}) < S(Y : X)$. The inequality is strict because the last transition is not reversible. In other words, PNS attacks without IRUD can never reduce the net RR-keyrate $K_n = S(Y : X) - S(Y{:}E|n, \textsc{pns})$ to 0, contrarily to the BB84 protocol.

The net key rate is 0 when all transmitted pulses can be explained by IRUD attacks, *i.e.* when $\forall n, p_n = 0$. Let T_c be the critical transmission below which our protocol ceases to work. At T_c, all the $1 - e^{-T_c\mu} \simeq T_c\mu$ transmitted pulses correspond to the $e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} \mathcal{P}(\Delta|n, m)$ successful IRUD attacks. We have then

$$T_c = -\frac{1}{\mu} \ln \left[1 - e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} \mathcal{P}(\Delta|n, m) \right] \simeq \frac{m}{2 \cdot m-1!} \left(\frac{\mu}{2} \right)^{m-2},$$

(12)

where the last approximation holds when $\mu \ll 1$. We essentially have $T_c \propto \mu^{m-2}$, showing the exponentially increasing robustness of the protocol for increasing m. This dependency is the same as SARG04, but not as BB84, where $T_c \simeq \frac{\mu}{2}$.

PNS *attack.* In order to compute the efficiency of the PNS-attack, one needs to compute the density matrices associated with n-photon pulses. The density matrix corresponding to the state defined in (8)

$$|x, n, m\rangle \langle x, n, m| = 2^{-n} \sum_{w,w'=0}^{m-1} e^{i(w-w')x\theta_m} \sqrt{\binom{n}{w[m]}\binom{w'[m]}{n}}$$

$$\times |w[m]\rangle \langle w'[m]| \quad (13)$$

$$= \sum_{D=1-m}^{m-1} e^{iDx\theta_m} \mathbb{M}_{D,m,n}, \quad (14)$$

where we have defined, for any integer $D \in [\![1-m, m-1]\!]$, the (shifted) $m \times m$ diagonal matrix

$$\mathbb{M}_{D,m,n} := 2^{-n} \sum_{w=\min(0,D)}^{m-1+\min(0,D)} \sqrt{\binom{w[m]}{n}\binom{w+D[m]}{n}} |w[m]\rangle \langle w+D[m]|.$$

(15)

Let $\rho_{n,m}$ be the average n-photon state sent by Alice. One has then

$$\rho_{n,m} = \sum_{x=0}^{m-1} \frac{1}{m} |x, n, m\rangle \langle x, n, m| = \mathbb{M}_{0,m,n}. \quad (16)$$

When Bob measures $Y = y$, and Eve keeps n photons, her state conditioned on Bob's measurement is given by

$$\rho_{y,n,m} = \sum_{x=0}^{m-1} \frac{1}{m} (1 - \cos(x-y)\theta_m) |x, n\rangle \langle x, n| \quad (17)$$

$$= \mathbb{M}_0 - \frac{e^{-iy\theta_m}}{2}(\mathbb{M}_{m-1} + \mathbb{M}_{-1}) - \frac{e^{iy\theta_m}}{2}(\mathbb{M}_{-m+1} + \mathbb{M}_1). \quad (18)$$
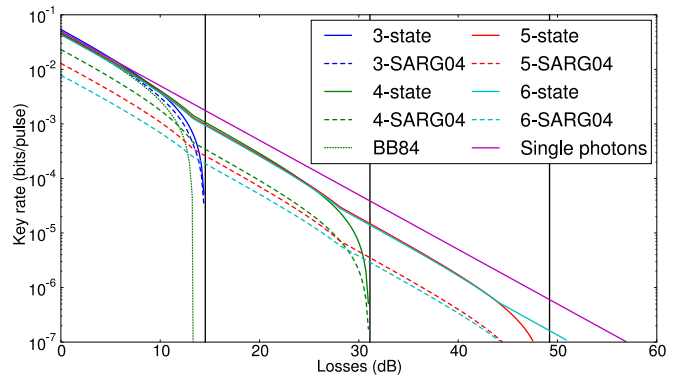

FIG. 1: Key rates of the m-states protocols compared to m-state SARG04 and BB84 with WCPS for $\mu = 0.1$ and $m \in [\![3, 6]\!]$. The vertical lines represent the values of T_c given by (12).
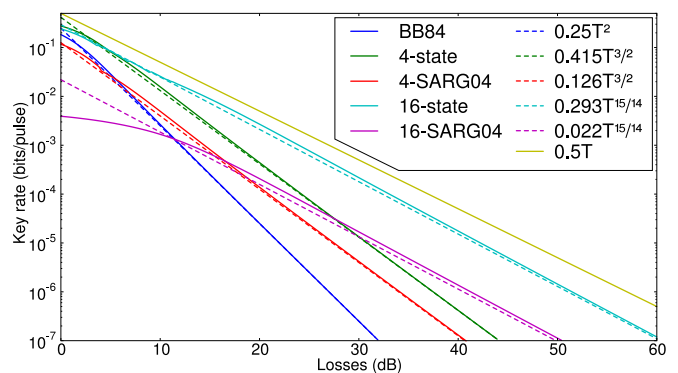

FIG. 2: Key rates with optimized μ for BB84, the m-states protocol, m-state for $m = 4$ and $m = 16$.

Note that in the above equations, the indices m and n have been omitted for $\mathbb{M}_D$ for the sake of simplification.

The Holevo limit of the information Eve can gather on Bob's measurement through a collective PNS attack is

$$S(Y{:}E|n, \textsc{pns}) := S(E|n, \textsc{pns}) - S(E|Y, n, \textsc{pns}) \quad (19)$$

$$= S(\rho_{n-1,m}) - S(\rho_{y,n-1,m}). \quad (20)$$

These entropies are easily computed numerically and decrease slowly with n.

They are independent of m iff $n \leq m - 1$, which means that the corresponding $S(Y{:}E)$ will also be identical in this case. In other words, the information leaked to Eve in m-state protocols are identical to the continuous $m \rightarrow \infty$ limit for n-photon pulses when $n \leq m - 2$, and the only difference at $n = m - 1$ comes from the IRUD attack.

Key-Rate. The net key rate $K(T, \mu)$ for wcp with μ photons/pulse on average is therefore

$$K(T, \mu) = \sum_{n=1}^{\infty} e^{-\mu} \frac{\mu^n}{n!} p_n K_n \text{ with } K_n := S(X:Y) - (Y:E|n, \text{PNS})$$
(21)

$$= \sum_{n=1}^{\infty} e^{-\mu} \frac{\mu^n}{n!} K_n - \sum_{n=1}^{\infty} e^{-\mu} \frac{\mu^n}{n!} b_n \frac{K_n}{1 - \mathcal{P}(\Delta|n, m)}. \quad (22)$$

When $T \geq T_c$ the optimal attack is for Eve to block the pulses with the biggest values of $\frac{K_n}{1-\mathcal{P}(\Delta|n,m)}$. This corresponds only roughly to the pulses with the lowest photon number. The corresponding rates for fixed $\mu = 0.1$ are shown in figure 1.

One can also numerically optimize μ for each value of the transmission T, as shown in figure 2. If the optimal key rate is achieved close to T_c, we have, for $\mu \ll 1$,

$$K \simeq K'_{m-1} \left(T\mu - \mathcal{P}(\Delta|m-1, m)\frac{\mu^{m-1}}{m-1!} \right) \quad (23)$$

with K'_{m-1} being the $(m-1)$th value of the $\frac{K_n}{1-\mathcal{P}(\Delta,n,m)}$ coefficients in decreasing order. Optimizing this quantity for μ is straightforward and gives

$$\mu_{\text{opt}} \simeq 2 \left(\frac{2 \cdot m - 2!}{m} \right)^{\frac{1}{m-2}} T^{\frac{1}{m-2}} \quad (24)$$

$$K_{\text{opt}} \simeq K'_{m-1} \frac{2}{m-1} \left(\frac{2 \cdot m - 2!}{m} \right)^{\frac{1}{m-2}} T^{1+\frac{1}{m-2}} \quad (25)$$

i.e. the key rate essentially varies as $K \propto T^{1+\frac{1}{m-2}}$ with a prefactor which slowly decreases with m. This approximation seems in agreement with numerical results, at least for reasonably low m (below 16). The bigger m is, the closer one is to the ideal single-photon case, where $K = \frac{T}{2} \log 2$.

Conclusion The sifting-less protocols described here are as efficient as BB84 and more robust against PNS-attack. This robustness lies in the preservation of non-orthogonality of the sent-states by the lack of sifting.

Furthermore, this also allows to extract a reasonable key for high m, while benefiting of the robustness brought by the increased overlap of the sent states, on the contrary to the m-state SARG04 variant, which while robust, have a sifting factor $\propto m^{-3}$ [3].

The most robust variant limit of this protocol is the limit of continuous phase modulation $m \to \infty$, which actually prevents the IRUD attack. It is straightforward to show that replacing the m-state POVM used in the above description by the simpler 4-State POVM used in standard BB84 does not change the key-rate in this limit.

Before using this protocol, we still need to investigate its security in presence of a non-zero QBER. For perfect single photons and a QBER ϵ, one can bound Eve's information by writing the state shared by Alice, Bob

and Eve under the form [4] $|\Psi_{ABE}\rangle = \sqrt{\lambda_1}|\Phi^+\rangle|E_1\rangle + \sqrt{\lambda_2}|\Phi^-\rangle|E_2\rangle + \sqrt{\lambda_3}|\Phi^+\rangle|E_3\rangle + \sqrt{\lambda_4}|\Phi^-\rangle|E_4\rangle$, and optimizing Eve's Holevo information $S(Y:E)$. One then straightforwardly find $S(Y:E|n = 1, \epsilon) = h(\epsilon)$. For $m = 4$, we have $S(X:Y) = \frac{1}{2}(\log 2 - h(\epsilon))$, which gives a net key rate $K = \frac{1}{2}(\log 2 - 3h(\epsilon))$, cancelling for a QBER $\epsilon = 6.14\%$. The expression is less elegant for other values of m, but the critical value of ϵ does not change much, varying between 6.89% for $m = 3$ and 5.93% for $m \to \infty$. Of course, for a practical application of these protocols, the combination of QBER and PNS attacks still needs to be investigated, as well as finite-size effects [7].

Another direction worth investigating would be an unbalanced version of our protocol, similar to BB84 with biased basis choice [12], allowing to double the key rate to ~ 1 bit/pulse instead of $\sim .5$ in the low-loss regime.

---

* Electronic address: frederic.grosshans@ens-cachan.fr

[1] Charles H. Bennett and Gilles Brassard, *"Quantum Cryptography: Public Key Distribution and Coin Tossing"*, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–9

[2] Valerio Scarani, Antonio Acín, Grégoire Ribordy and Nicolas Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations", *Phys. Rev. Lett.* **92** 057901 (2004), arXiv:quant-ph/0211131.

[3] Antonio Acín, Nicolas Gisin, and Valerio Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks", *Phys. Rev. A* **69** 012309(2004), arXiv:quant-ph/0302037.

[4] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf , Miloslav Dušek, Norbert Lütkenhaus, Momtchil Peev, "The Security of Practical Quantum Key Distribution", arXiv:0802.4155 (2008). To appear in *Rev. Mod. Phys.*.

[5] Norbert Lütkenhaus, "Security against individual attacks for realistic quantum key distribution", *Phys. Rev. A* **61** 052304 (2000), arXiv:quant-ph/9910093.

[6] Anthony Leverrier and Philipper Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation", *Phys. Rev. Lett.* **102** 180504 (2009), arXiv:0812.4246.

[7] Raymond Y.Q. Cai, Valerio Scarani, *New J. Phys.* **11** 045024, arXiv:0811.2628.

[8] F. Grosshans and Ph. Grangier, in *Proc. 6th International*

Conference on Quantum Communications, Measurement, and Computing, edited by J. H. Shapiro and J. O. Hirota (Rinton Press, December 2002), p. 351, arXiv:quant-ph/0204127.

[9] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and Philippe Grangier, *Nature* (London) **421** 238 (2003), arXiv:quant-ph/0312016.

[10] David J. C. MacKay, "Information Theory, Inference and Learning Algorithms", Cambridge University Press (2003). `http://www.inference.phy.cam.ac.uk/mackay/itila`.

[11] Anthony Chefles and Stephen M. Barnett, "Optimum unambiguous discrimination between linearly independent symmetric states", *Phys. Lett. A* **250** 223(1998).

[12] Hoi-Kwong Lo, H. F. Chau, M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security", *J. Cryptology* **18** 133 (2005), arXiv:quant-ph/0011056; and "Efficient Quantum Key Distribution Scheme", arXiv:quant-ph/9803007 (1998).