World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:6, No:3, 2012

Decoy-pulse protocol for frequency-coded quantum key distribution

Sudeshna Bhattacharya, Pratyush Pandey, and Pradeep Kumar K

Abstract—We propose a decoy-pulse protocol for frequency-coded implementation of B92 quantum key distribution protocol. A direct extension of decoy-pulse method to frequency-coding scheme results in security loss as an eavesdropper can distinguish between signal and decoy pulses by measuring the carrier photon number without affecting other statistics. We overcome this problem by optimizing the ratio of carrier photon number of decoy-to-signal pulse to be as close to unity as possible. In our method the switching between signal and decoy pulses is achieved by changing the amplitude of RF signal as opposed to modulating the intensity of optical signal thus reducing system cost. We find an improvement by a factor of 100 approximately in the key generation rate using decoy-state protocol. We also study the effect of source fluctuation on key rate. Our simulation results show a key generation rate of 1.5×10^{-4}/pulse for link lengths up to 70km. Finally, we discuss the optimum value of average photon number of signal pulse for a given key rate while also optimizing the carrier ratio.

Keywords—B92, decoy-pulse, frequency-coding, quantum key distribution

I. Introduction

PHOTONIC technology has become the ubiquitous choice for implementing quantum key distribution (QKD) protocols as it provides low-loss, long-distance transmission, and operation in C-band (1550nm). Ideally, QKD implementation requires a light source that emits single-photon pulses. However, due to non-availability of commercial single-photon sources (SPSs), a majority of QKD experiments use faint laser pulse source (FLPS) in place of SPSs. The photon emission from a FLPS follows a Poisson distribution with an average photon number μ/pulse. A FLPS emits multi-photon pulse with a non-zero probability $1-\exp(-\mu)$. It has been shown that secure key rate slows down considerably if channel loss is greater than multi-photon emission probability; however security of key bits is not compromised. To overcome this problem, Hwang proposed the idea of using decoy-pulses to place an upper bound on the single-photon transmittance and hence the number of secure key bits in the sifted bit string [1]. In a decoy-pulse method, Alice transmits decoy pulses interleaved with signal pulses, the location of which is known only to her. As Eve cannot distinguish between signal and decoy pulses, she is forced to use the same attack against both types of pulses. At the end of key transmission, Alice estimates quantum bit error rate (QBER) due to signal and decoy pulses and aborts the protocol if the yield of decoy pulses is abnormally high.

Sudeshna Bhattacharya is with Center for Laser Technology, Indian Institute of Technology Kanpur, Kanpur-208016, India (email: sudeshna@iitk.ac.in)
Pradeep Kumar K is with Department of Electrical Engineering, and Center for Laser Technology, Indian Institute of Technology Kanpur, Kanpur-208016, India (email: pradeepk@iitk.ac.in)

In this paper, we extend decoy-pulse method to frequency-coded setups. In a frequency-coded setup, key bits are transmitted as sidebands relative to an optical carrier. An electro-optic phase modulator generates optical sidebands by modulating an optical carrier of frequency ω_0 by a microwave signal of frequency Ω and phase ϕ:

$$\begin{aligned}|\omega_0\rangle \rightarrow J_{-1}(m)e^{-j\phi}\,|\omega_0-\Omega\rangle + J_0(m)\,|\omega_0\rangle \\ + J_1(m)e^{j\phi}\,|\omega_0+\Omega\rangle\,,\end{aligned} \tag{1}$$

where we have neglected terms of higher order under the assumption of low modulation index ($m \ll 1$). The average photon number of the carrier and sidebands after phase modulation is μJ_0^2 and μJ_1^2 respectively. A lossless modulator conserves the total number of photons from input to output. Hence a straight forward extension of decoy pulse method to frequency-coded setup is not possible as any change in the average photon number of sidebands reflects in the carrier. Eve can distinguish between signal and decoy pulses by monitoring the optical power in carrier thus defeating the purpose of using decoy pulses. We suggest methods to overcome this problem by optimizing the carrier ratio of decoy-to-signal pulses.

The rest of the paper is organized as follows. In Section II, we describe briefly the elements of frequency-coding setup for B92 protocol. In Section III, we describe our decoy-pulse method for frequency-coding setup. We discuss the notion of carrier optimization, its effect on QBER and key rate and the effect of source fluctuation on the key length in Section IV. Finally, we conclude by summarizing our results.

II. Frequency-Coded Scheme

Fig. 1 shows elements of frequency-coded scheme to implement B92 QKD protocol. In this scheme, key bits are transmitted as phase of sidebands relative to an optical carrier [2]. Alice modulates the optical carrier of frequency ω_0 and average photon number/pulse μ_L by a microwave signal of frequency Ω and phase ϕ_A to generate:

$$\begin{aligned}|\omega_0\rangle \rightarrow J_{-1}(m)e^{-j\phi_A}\,|\omega_0-\Omega\rangle + J_0(m)\,|\omega_0\rangle \\ + J_1(m)e^{j\phi_A}\,|\omega_0+\Omega\rangle\,,\end{aligned} \tag{2}$$

where m is the modulation index and we have neglected terms of higher order under the assumption $m \ll 1$. She transmits the modulated signal (2) to Bob who in turn modulates (2) with a microwave signal of frequency Ω and phase ϕ_B. Bob's detector registers a photon if Alice and Bob's phases are identical. Alice and Bob retain those slots in which Bob detects photons to form a sifted bit string and discard the rest. They then apply error correction and privacy amplification to generate

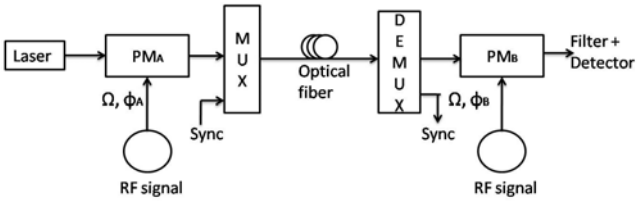


Fig. 1. Elements of frequency-coded scheme. $\mathrm{PM}_{A,B}$: Alice and Bob's phase modulators. Sync: Synchronization channel.

a final bit string. From (2) we see that the average photon number of carrier and sidebands after modulation are given by $\mu_0 = \mu_L J_0^2(m)$ and $\mu_{\pm 1} = \mu_L J_1^2(m)$ respectively [3]. However, due to propagation inside a fiber and other optical losses, μ_L at the receiver L km from the transmitter is

$$\mu_L(L) = \mu_L 10^{-\alpha_{tot}/10}, \tag{3}$$

where $\alpha_{tot} = 2\alpha_{mod} + 2\alpha_{mux} + \alpha_e + \alpha_f L$ represents link loss (See Table I). At the output of Bob's detector we have

$$\mu_0 = \mu_L(L)(J_0^2 + 2J_1^2\cos(\Delta\phi))^2, \tag{4a}$$

$$\mu_{\pm 1} = 4\mu_L(L)|J_0 J_1|^2 \cos^2(\Delta\phi/2), \tag{4b}$$

where $\Delta\phi = |\phi_B - \phi_A|$. The QBER of the frequency-coded setup is given by

$$\mathrm{QBER} = \frac{P_{noise}}{2P_{noise} + P_{sig}}, \tag{5}$$

where P_{noise} and P_{sig} are noise and signal probabilities respectively. P_{noise} includes contributions from the detector dark count, out of band noise due to insufficient carrier suppression, and cross-talk noise due to synchronization channel [3]. P_{sig} is given by

$$P_{sig} = 1 - e^{-\mu_{\pm 1}}, \tag{6}$$

where $\mu_{\pm 1}$ is given in (4b).

TABLE I
SYSTEM PARAMETERS FOR CALCULATING QBER.

Phase modulator(PM) IL,α_{mod}	1dB
Mux/deMUX IL,α_{mux}	3dB
Extra losses,α_e	3dB
Fiber loss,α_f	0.25dB
FP filter extinction ratio,η_f	40dB
GAPD dark current probability,P_{dark}	0.6×10^{-5}
Crosstalk from synchronous channel,P_{sync}	10^{-4}

III. Decoy-pulse protocol for frequency-coding scheme

A. Description of protocol

We consider a two decoy-state protocol with vacuum as one of the decoy states [4]. The vacuum pulse is used to estimate dark count rate (DCR) of the detector and background noise [5]. To implement the protocol, Alice interleaves decoy pulses along with signal pulses, the exact locations of which is known only to her [1]. After bit transmission using a QKD protocol, say B92, Alice estimates the yield of decoy pulses. If the yield of decoy pulses is abnormally higher than that of signal pulses she abandons bit transmission and informs Bob. The QKD protocol can be implemented using polarization, phase, or frequency-coding schemes. In this paper, we restrict ourselves to frequency-coding scheme.

We denote the average number of photon/pulse of signal and decoy states by μ and ν respectively. Alice chooses μ, ν and the number of signal (N_μ) and decoy pulses (N_ν) be transmitted to Bob. Since decoy pulses do not contribute to the final key, it is essential to maximize N_μ. We achieve this by choosing $\mu < \nu$ and $N_\mu > N_\nu$ while keeping the product μN_μ approximately equal to νN_ν.

B. Key generation rate

The expression for secure key generation rate for an implementation of QKD protocol that uses FLPS is given by [6]:

$$R \geq q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{7}$$

where $q = N_\mu^S/N$ is the ratio of number of signal pulses when both Alice and Bob's basis are identical to the total number of pulses transmitted by Alice [5]. In (7), E_μ and Q_μ are QBER and gain of multi-photon signal pulse respectively; e_1 and Q_1 are the QBER and gain of the single-photon pulse respectively; $f(x)$ is the bi-directional error correction rate [7]; and $H_2(x)$ is the binary entropy function for x. The key generation rate R is non-zero provided single-photon transmittance is higher than multi-photon transmittance as can be seen from (7).

The parameters E_μ and Q_μ are measured experimentally by transmitting multi-photon pulses. Although we could theoretically estimate e_1 and Q_1 using (4b) and (6), in practice we use the following formulae to estimate the quantities :

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}(Q_\nu^L e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - Y_0^U \frac{\mu^2 - \nu^2}{e_0 \mu^2}), \tag{8a}$$

$$e_1 \leq e_1^U = \frac{E_\mu Q_\mu - e_0 Y_0^L e^{-\mu}}{Q_1^L}, \tag{8b}$$

where

$$Q_\nu^L = Q_\nu(1 - \frac{u_\alpha}{\sqrt{N_\nu Q_\nu}}), \tag{9a}$$

$$Y_0^L = Y_0(1 - \frac{u_\alpha}{\sqrt{N_0 Y_0}}), \tag{9b}$$

$$Y_0^L = Y_0(1 + \frac{u_\alpha}{\sqrt{N_0 Y_0}}), \tag{9c}$$

where Y_0 is the sum of DCR of the detector and background noise [5]. The value of the parameters used in simulation are listed in Table II.

TABLE II
PARAMETERS TO ESTIMATE KEY RATE. ADDITIONAL DATA FROM [5].

Parameter	Value	Parameter	Value
Y_0	0.6×10^{-5}	u_α	10
e_0	0.51	q	0.319
$f(E_\mu)$	≤ 1.22	N	105 Mbits
μ	0.4	ν	1
N_μ	$0.635N$	N_ν	$0.203N$
N_0	$0.162N$		

C. Optimization of carrier ratio

At the transmitter, average number of photons in carrier and sidebands are given by

$$\mu_0 = \mu_L J_0^2(m_x), \tag{10a}$$

$$\mu_1 = \mu_L J_1^2(m_x), \tag{10b}$$

where μ_L is the input average photon number, m_x is the modulation index of the phase modulator with $x = s, d$ denoting signal and decoy pulses respectively. We define carrier ratio CR as the ratio of decoy-to-signal pulse carrier photon number:

$$\text{CR} = \frac{J_0^2(m_d)}{J_0^2(m_s)}, \tag{11}$$

Since a lossless phase modulator conserves total number of photons, any change in μ_1 produces a detectable change in μ_0 which in turn affects carrier ratio. Eve can now distinguish between signal and decoy states by measuring the carrier photon number without affecting other statistics. Hence, a direct extension of decoy-pulse protocol to frequency-coding scheme in which Alice switches between signal and decoy pulses results in loss of security.

We overcome this loophole by optimizing CR to be as close to unity as possible. We do this by choosing appropriate values of m_s and m_d for a given μ_L such that CR≈ 1 while $\nu > \mu$. Fig. 2 shows carrier ratio and QBER as a function of input average photon number μ_L for $\mu = 0.4$ and $\nu = 1$.

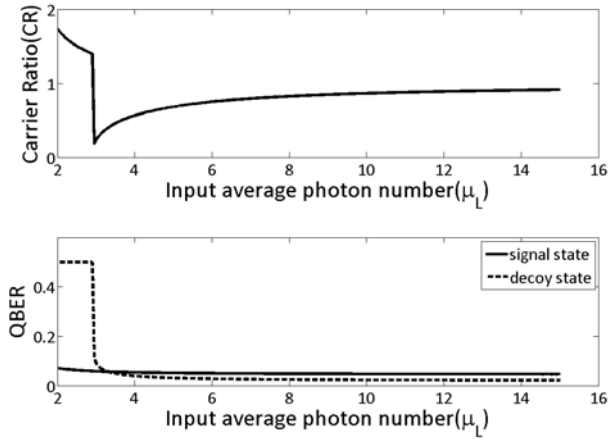


Fig. 2. Carrier ratio and QBER as a function of μ_L for a 70km link.

We see from Fig. 2 that for μ_L slightly above 6, CR is closer to unity and QBER < 0.25. Since maximum allowable QBER for B92 protocol is 0.25, we require $\mu_L > 6$ to optimize CR as well as to keep QBER < 0.25.

D. Improvement in key rate using decoy states

The key generation rate experiences an improvement when using decoy-state method. We performed numerical simulations to obtain key generation rate with and without decoy states. Fig. 3 shows the results. We find that the key generation rate exhibits an improvement by a factor of 100 approximately with decoy state. The maximum secure transmission distance also increases significantly in case of decoy-state.

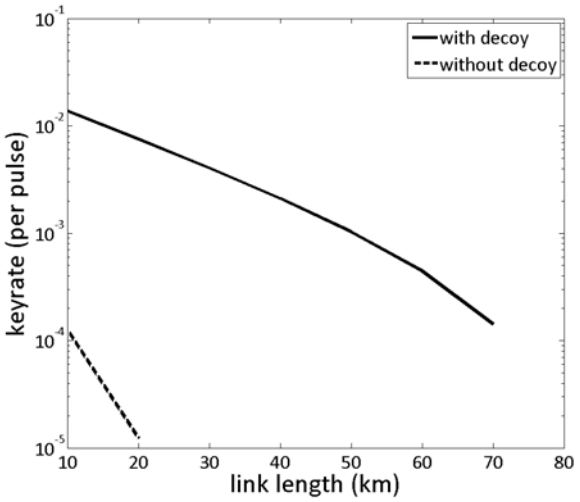


Fig. 3. Key generation rate as a function of link length with and without decoy states.

E. Effect of source fluctuation

Alice generates both the decoy and signal pulses at any instant i by attenuating a common father pulse. The fluctuation of the final output pulse from Alice's side comprises of father pulse fluctuation and device (attenuator) parameter fluctuation [8]. Thus the actual intensity of the ith outgoing pulse is given by:

$$decoy : \mu_{id} = \mu_d(1 + \delta_i)(1 + \epsilon_{id}), \tag{12a}$$

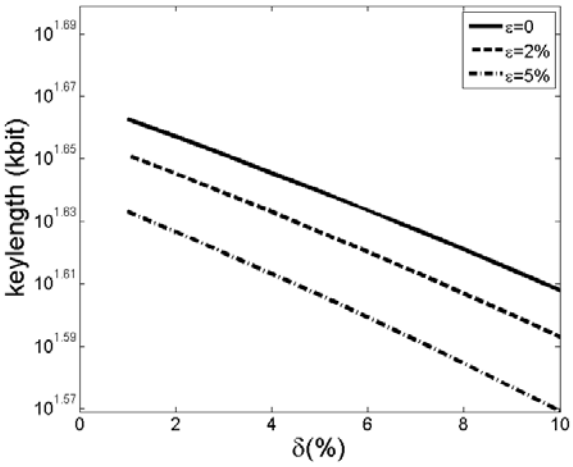
$$signal : \mu_{is} = \mu_s(1 + \delta_i)(1 + \epsilon_{is}), \tag{12b}$$

where δ_i is the intensity fluctuation in the ith father pulse,and ϵ_{id} (or ϵ_{is}) are the device parameter fluctuation in the ith decoy (or signal) pulse respectively. We observe from Fig. 4 that the key length decreases slightly with the father pulse intensity variation. However, the device parameter fluctuation degrades the key length severely. Thus device parameters need to be much stable to avoid significant degradation in key length.

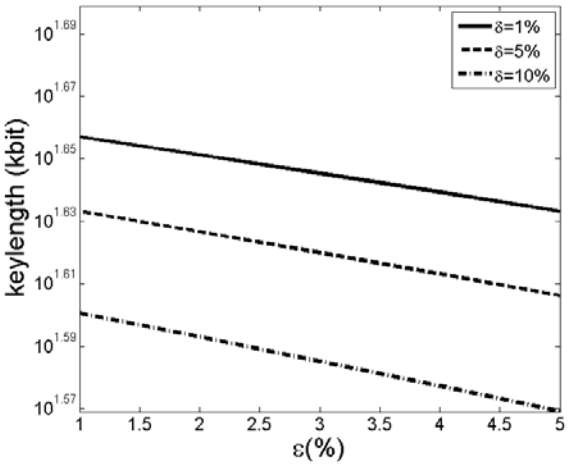
F. Optimal secure key length

The choice of m_s and m_d for a given μ_L leads to optimization of CR but affects secure key generation rate. The optimum values of secure key rate and key length corresponding to optimum values of m_s and m_d are given in Table III. As described earlier, we keep $\mu_L > 6$.

We see from Fig. 5 that as the carrier ratio increases beyond 0.6 the key length also increases. When carrier ratio < 0.6 then $\mu \not< \nu$ and also either μ or ν or both are greater than 1 so that region is not acceptable for operation. One can obtain suitable CR by varying m_d for a given value of μ_L and m_s. Fig. 6 shows the evolution of key length L ($= NR$) with increasing μ_L as well as μ. We have estimated the usable range of input average photon number μ_L and average photon



(a) Key length with father pulse intensity fluctuation.



(b) Key length with device fluctuation.

Fig. 4. Key length with source fluctuation.

TABLE III
OPTIMUM VALUES OF SECURE KEY RATE AND KEY LENGTH FOR A 70KM LINK.

Parameter	value	Parameter	value
CR	0.7647	μ_L	6.3
μ	0.4	ν	1
m_s	0.518	m_d	0.877
E_μ	0.0495	Q_μ	0.0021
E_ν	0.0270	Q_ν	0.0039
R^L	1.5315×10^{-4}/pulse	$L(=NR)$	16.080kbits

number in signal sideband μ to obtain maximum key length along with carrier ratio optimization. We see from Fig. 6 that to obtain higher key length μ must be greater than 0.3 and μ_L must be less than 12. We find that the key length does not change appreciably for $6 < \mu_L < 12$. Hence for carrier ratio optimization and higher key length we choose $0.3 < \mu < 0.5$ and $6 < \mu_L < 12$.

We have obtained the lower bound on key rate to be 1.5315×10^{-4}/pulse and thus a final key length of 16kbit from simulations. These simulations also indicate that the maximum

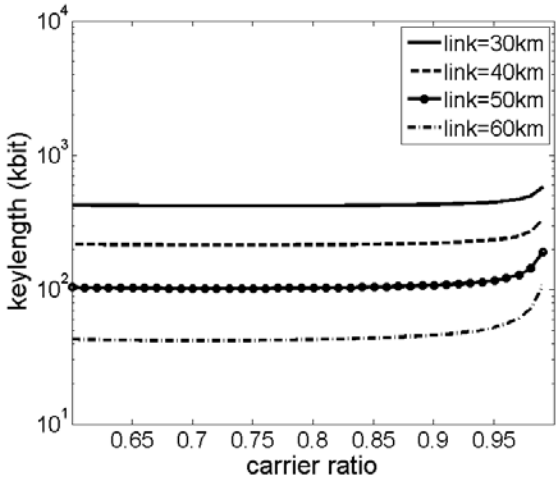


Fig. 5. Key length as a function of carrier ratio for various link lengths.

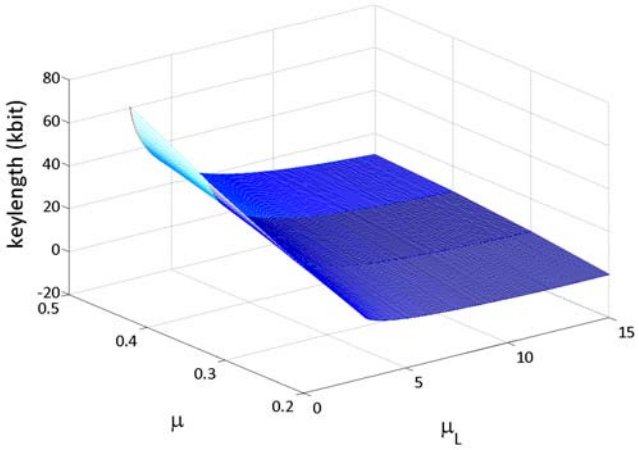


Fig. 6. 3D plot of key length as a function of μ_L and μ (Parameters for calculation are listed in Table II).

link length for secure transmission is about 70km. Thus, our method is promising for long distance communication.

IV. CONCLUSION

We have numerically studied a two decoy-pulse protocol suitable for frequency-coded quantum key distribution. A direct extension of decoy-pulse method to frequency-coding scheme leads to security loophole as it allows an eavesdropper to distinguish between signal and decoy pulses by monitoring carrier power. Thus, the very objective of using decoy-pulses seems to be lost. We overcome this problem by optimizing the ratio of carrier photon number of decoy-to-signal pulses to be as close to unity as possible. We achieve this by switching the amplitude of signal and decoy pulses in the RF domain which reduces overall system cost. Our simulations reveal that the key length improves by a factor of 100 approximately using decoy states. We analyze the effect of fluctuations of source on key length. we find that the device parameter fluctuation undermine the key length drastically as compared to father

pulse intensity fluctuation. We also study optimum values of μ and μ_L to obtain an optimum CR and key rate for fixed ν. Our simulation shows key generation rate of $\approx 1.5 \times 10^{-4}$/pulse at link lengths up to 70km thus indicating that our method can be used for long distance secure communication.

REFERENCES

[1] W. Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 057901, 2003.
[2] J. M. Merolla *et al.*, "Phase-modulation transmission system for quantum cryptography," *Opt. Lett.*, vol. 24, 1999.
[3] P. Kumar and A. Prabhakar, "Bit error rates in a frequency coded quantum key distribution system," *Optics Communications*, vol. 282, no. 18, pp. 3827–3833, 2009.
[4] X. Ma *et al.*, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 012326, 2005.
[5] Y. Zhao *et al.*, "Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber," in *Proceedings of IEEE International Symposium on Information Theory*, 2006, pp. 2094–2098.
[6] D. Gottesman *et al.*, "Security of quantum key distribution with imperfect devices," *Quantum Information and Computation*, vol. 4, p. 325, 2004.
[7] G. Brassard and L. Salvail, "Advances in cryptology eurocrypt'93," *Lecture Notes in Computer Science*, vol. 765, pp. 410–423, 1994.
[8] J.-Z. Hu and X.-B. Wang, "Reexamination of the decoy-state quantum key distribution with an unstable source," *Phys. Rev. A*, vol. 82, p. 012331, 2010.