This is the accepted manuscript made available via CHORUS. The article has been published as:

Secure Communication via a Recycling of Attenuated Classical Signals

A. Matthew Smith

Phys. Rev. Applied **7**, 014010 — Published 12 January 2017

DOI: 10.1103/PhysRevApplied.7.014010

Secure communication via a recycling of attenuated classical signals

A. Matthew Smith
Quantum Information Science Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA

(Dated: August 2015)

We describe a simple method of interleaving a classical and quantum signal in a secure communication system at a single wavelength. The system transmits data encrypted via a one-time pad on a classical signal and produces a single photon reflection of the encrypted signal. This attenuated signal can be used to observe eavesdroppers and produce fresh secret bits. The system can be secured against eavesdroppers, detect simple tampering or classical bit errors, produces more secret bits than it consumes and does not require any entanglement or complex wavelength division multiplexing, thus making continuous secure two-way communication via one-time pads practical.

PACS numbers: 03.67.Ac,03.67.Dd

I. INTRODUCTION

Secure communication is a vital requirement in many fields and has applications from finance to infrastructure security such as smart grid automation via Supervisory Control And Data Acquisition (SCADA) networks. Encryption of messages is commonly performed by asymmetric (also called public key) encryption. Shor's quantum algorithm is known to break public key encryption [1]. Symmetric encryption such as the AES standard requires the sender and receiver to possess the same identical key for each message but even this is not secure against a quantum computer [2]. Grover's algorithm effectively reduces the size and therefore the difficulty of breaking AES keys by a factor of 2 in key size [3]. This would make 128 bit keys breakable and 256 bit keys dubious with current classical computers [3]. Future proofing secure communication, particularly against quantum devices, is therefore of practical interest.

The motivation for this work is to describe a secure two-way communication system and to establish that such a system has a practical lower bound on the classical bit rate at useful distances. There have been numerous proposals for quantum secured communication. The system as described below is simpler than previously proposed methods [4].

One simple encryption method that is known to be secure against any attack with any type of computer (quantum or classical) is the One-Time Pad (OTP) [5]. The OTP was proven to be unconditionally secure in that the transmitted message contains no information about the secret message other than is maximum possible length [5]. The inherent draw back to OTPs is that the sender and receiver must have identical truly random keys of length equal to the message and the key cannot be reused in part or whole in any way [5]. Distributing sufficient random key material in a secure fashion is the main obstacle to the wide spread use of OTPs.

We propose to implement secure communication by tightly integrating the process of creating shared random strings used in a OTP and classical communication in an inherently inseparable fashion (i.e., not simply putting two boxes in a bigger box). This is done by sending a classical signal, creating a "quantum reflection" of that signal and using the reflection to create new secret data. This has a number of advantages in simplicity over other methods such as wavelength division multiplexing [4] or Deterministic secure Quantum Communication. (DSQC) and Quantum Secure Direct Communication (QSDC) methods [6]. It also does not require any entangled resources, on demand single photons or a dedicated dark fiber. The proposed method is independent of the details of the secret key building algorithm (e.g., BB84 [7], SARG04 [8]). Deng and Long described a similar system but with several import differences in implementation [9, 10].

In [10] Deng and Long proposed a system in which randomly phase modulated weak coherent pulses are sent from Bob to Alice and eventually returned to Bob. Alice encodes an additional phase transformation representing classical information before returning the pulses to Bob. Bob can remove the random phase modulation he initially applied and recover the classical information corresponding to Alice's message. Thus Deng and Long's method is a one direction QSDC system (Alice to Bob), with a similar premise to the quantum reflection [10].

We do not perform QSDC and the quantum reflection described here is generated from an attenuated classical signal rather than a returned quantum signal. Both systems use weak coherent pulses that are much easier to produce than on demand single photons. The security of [10, 11] is based on Alice and Bob both randomly deciding to use a subset of the pulses for eavesdropper detection and reconciling those pulses, whereas the proposed system is based on the standard security methods of non-deterministic QKD with an untrusted source [12].

Section II describes the operation of the system, both the physical transmission of pulses and the logical operations in sending a secure message. Section III briefly describes the security assumptions and Section IV gives a numerically analysis of the system performance.

II. METHOD

The Alice and Bob nodes are assumed to be trusted nodes connected by a long pair of single mode fibers

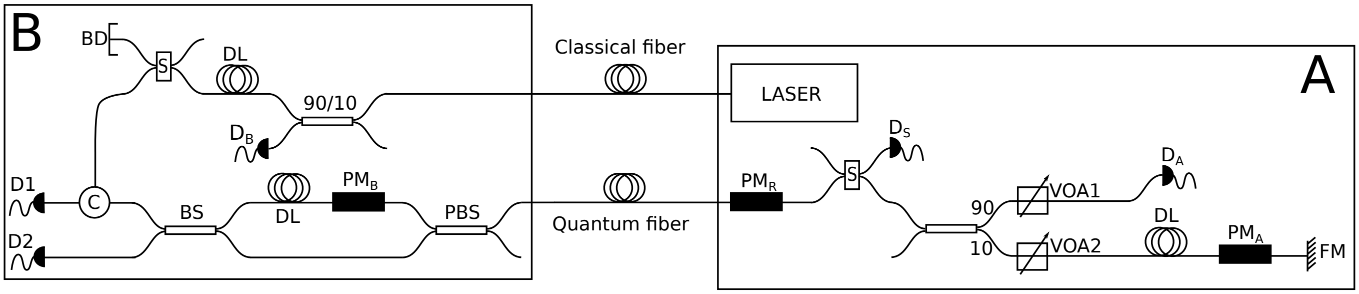

FIG. 1. **Diagram of device** The proposed device uses two fibers for two way secure communication. The encoded classical communication on both channels is secured by the QKD-like subsystem. DL are delay lines, PM are the three phase modulators, (P)BS are (polarizing) beam splitters, BD is a beam dump, D1 & D2 are single photon detectors, VOA is a variable optical attenuator, FM is a Faraday mirror, C is a circulator and S are optical switches, 90/10 are asymmetric beam splitters (this ratio is somewhat arbitrary) and D$_x$ are APDs.

(SMF). Such paired fibers are commonly used to extend ethernet networks and are common in SCADA networks. One fiber will be used to send classical signals from Alice to Bob. This is called the classical fiber and is the upper fiber in Fig. 1. The second fiber (lower fiber in Fig. 1) will be used to send classical signals from Bob to Alice as well as return the single photon level reflection for the QKD subsystem. This subsystem is the common non-deterministic phase encoded “plug-and-play” variant of QKD. The fibers themselves are identical, we differentiate them only due to their current use.

One of the main advantages of this system is its simplicity. The proposed system requires only one laser operating at a single frequency and only two single photon detectors. The rest of the components are relatively simple and low cost. There is no need for wavelength division multiplexing [4], no entangled states and no on demand photons sources. Other effects like channel cross talk are minimal. Thus we have a two way secure and endless OTP based communication system that is practical and relatively low cost.

Alice contains a fiber coupled laser at 1550nm wavelength capable of generating pulses at a preset rep-rate f_{rep}. The pulses are sent via a single fiber to Bob. Alice will generate pulses in groups of size N_f. Each pulse is a bright or macroscopic pulse consisting of many photons; each group of pulses is called a frame. At a preset frequency F Alice and Bob encode classical data on the occupation number (i.e., in the presence or absence) of a frame in a given time window. If an entire frame occupies that time window it represents a “1” bit. If no frame is present it represents a “0” bit. Alice and Bob use a constant preset rate rate F (which is dependent on the physical system and can be known by an eavesdropper Eve) to transmit the classical data.

A. Physical Transmission

To send a message Alice launches encoded frames on the classical fiber and sends them to Bob in Fig. 1. Bob will sample a small percentage of each pulse and thus detect their arrival time of each frame in detector D$_B$. D$_B$ is a avalanche photo diode or APD (not a single photon detector). This allows Bob as well as Eve to read the classical data sent from Alice by detecting the time between arriving frames and comparing it to the known frame rate F as well as to synchronize the QKD subsystem to Alice’s pulses. The start of each message will require some initial standard synchronization signal such that Bob doesn’t miss the start of a message.

The remainder of the signal in Bob is sent into the QKD subsystem which uses the quantum fiber. The still macroscopic pulses are split into two pulses each by an unbalanced interferometer (BS to PBS in Fig. 1) and both are sent to Alice, on the quantum fiber, similar to standard commercially available phase encoded QKD systems. This splitting is much less than the time between any two consecutive pulses in a frame. Alice applies a random phase modulation to one each of the incoming pulse pairs. Note that this is a security feature described in [12], used to prevent tampering and is not a part of the communication protocol as in DL04 [10]. Alice also contains a switch to dump the incoming signal to a detector D$_S$ similar to [12].

Alice detects a portion of each pulse in the returning frames via another synchronization detector D$_A$ similar to Bob. This allows the added feature of Alice detecting the message that Bob received, unlike the methods of [9–11] where only parts of the transmission are revealed to both parties as part of eavesdropper checks. If the signal Alice receives from Bob does not match that which Alice sent to Bob it indicates either tampering or some other failure and the transmission can be scrapped.

Alice attenuates the pulses in the frame to the weak coherent approximation of single photons and phase modulates similar to a standard QKD system. By this method Alice and Bob are effectively performing QKD with the “reflected” frames or equivalently the “1”s classical bits originally sent in Alice’s message. The OTP encoding is such that on average half of the bits Alice sends will be “1”s regardless of Alice’s classical message. In standard

QKD the frames or "bits" sent between Bob and Alice are all "1"s and contain no classical information.

If Bob wishes to send a message to Alice he may tell Alice (via a classical side channel) to send a stream of unencoded frames all of which are "1"s. The all "1"s signal contains no information other than that Bob wishes to send a message and the maximum possible length of the message. These are the same security constraints as the OTP [5].

Bob detects and synchronizes to each frame as above. Bob can transmit information in the occupation number of the frames to Alice by actuating an optical switch that routes entire frames either back to Alice on the quantum fiber for "1" bits or to a beam dump BD in Fig. 1 for "0" bits. As the frame rate is rather low the switching and synchronization requirements are not strenuous for state of the art components. Alice detects and synchronizes her operation to the arriving frames. Since Alice sent the pulses originally and because Alice knows the line length of the round trip from Alice to Bob and back, Alice can easily detect both the "0" and "1" bits. The QKD subsystem operates in the same manner as described above.

B. Logical Operations

The section above describes the physical movement of pulses and the device operation. Here we describe the encryption method. Given the tightly convoluted nature of the classical communication and the quantum reflection it can be difficult to interpret the order of operations.

First note that regardless of the direction of communication a classical bit (frame of pulses) doesn't correspond to any quantum bit that may be created from its reflection, nor is there any information correlated between the pair. This can be seen from the classical "0" bits (empty frame) never creating a reflection and the classical "1" creating multiple bits each, half of which are 0 and half are 1 bits. Also the error correction (e.g cascade algorithm) and privacy amplification require the bit strings to be pseudo-randomly shuffled. The QKD algorithms assumed here operate on large blocks of data rather than dynamically on each detection event as they occur.

At its most basic the proposed system operates as follows. The sender Alice has a message to send and takes a sequence of pulses from an unknown and untrusted source similar to [12]. the source is in reality Alice herself, but because the pulses were sent to Bob we must assume that Eve can tamper with them. Therefore Alice randomizes the phases and performs other security checks as described in ref. [12]. Alice attenuates the pulses to the weak coherent approximation of single photons. Each photon is then independently modulated by one of four phases and Alice records each value, similar to BB84 [7]. The photons are then sent to Bob. Bob applies an additional modulation chosen from the same four phases and measures. If the total phase modulation adds up to 0, π or 2π the detection outcome is deterministic, else it is random [7]. After well known error correction (BB84 sifting, cascade, privacy amp.) methods Alice and Bob now share a string of bits [7] that can be used as a key in a OTP.

As long as each classical "1" bit generates on average more than 2 secure key bits then the system will never run out of key material and the OTP can effectively run indefinitely.

To transmit a secure encoded message the system requires an initial reservoir of secret bits. This can be installed in the factory or simply built by the secure QKD subsystem by sending a classical message of all "1". Thus the QKD subsystem is always "ahead" of the OTP and as the system uses the initial key bits, it generates more bits than it uses via the reflection. The receiver can decode the message using the current key material and in the process of doing so (due to the reflection effect of the classical communication) both sides are building more secret bits for use with future messages. If a block of bits transmitted on the quantum channel as weak coherent pulses is ever deemed to be insecure due to the presence of Eve (i.e. measured by high quantum bit error rate, decoy states, trojan horse detectors, etc.), then those bits can be disposed off. In this case no information is leaked to Eve about a message not even its length. Indeed a message might not even exist yet when the bits are created and or disposed of.

C. Endless Two-way Secure Communication

The proposed system is capable of simultaneous two-way secure communication. Unlike the description above where Alice and Bob took turns to communicate at the same bit rate, the nodes can communicate simultaneously but at different bit rates. Alice encodes her message as described above, i.e. by subtracting frames from an unencoded stream of frames. Bob is able to read Alice's message directly. As Bob is reading and returning the classical pulses to Alice, Bob can encode data on the occupation number of the "1"s in Alice's message by the same process of subtraction. If Bob receives a "1" from Alice an wishes to send a "0" for his bit, Bob can activate his switch and send the frame to the beam dump in Fig.1. If Bob receives a "1" and wishes to send a "1" he lets the frame pass. If Bob receives a "0" he does nothing and waits for the next frame on which to encode his bit. Alice can decode Bob's message by comparing the returning frames occupation number to the message she originally sent to determine with frames Bob blocked or allowed to pass. Alice's message consists of (by definition

TABLE I. Two Way Encoding at Different Data Rates

Unencoded frames	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Alice's message	1	0	1	0	0	1	1	0	1	0	0	1	0	1	1	0	0	1
Bob's return message	0	-	1	-	-	1	0	-	1	-	-	0	-	1	0	-	-	0

of the OTP) 50% “1”s [5]. See Table I for an illustrative example of the encoding by subtraction at each node.

Key management for the system simply requires the two nodes to agree on how to divide up the generated key, approximately 2/3 for Alice to Bob and 1/3 for Bob to Alice communication.

As shown in Table I, Bob will be able to transmit on average at half the rate of Alice. The other drawback to such a system is that each frame that survives passing through Bob must now generate 4 secure key bits rather than 2. As will be shown bellow this limits communication rate in both directions and the effective range.

III. SECURITY

The security of the system as currently conceived is based on the security of the phase encoded “plug and play” style of QKD on which it is built. Such a system has been shown by Zhao, Qi, and Lo to be theoretically secure under realistic conditions [12] and our numerical modeling is based on the same system as [12]. The work is in turn based on that of Gottsman, Lo, Lutkenhaus and Preskill [13] which gives the secure key rate for BB84 as,

$$R \ge \frac{1}{2}\{-Q_e f(E_e) H_2(E_e) + \underline{Q\Omega}[1 - H_2(\frac{Q_e E_e}{\underline{Q\Omega}})]\} \quad (1)$$

Y. Zhao, B. Qi, and H.-K. Lo extend that model in [12] with their equation (9) to an untrusted source such as we have described as,

$$R \ge \frac{1}{2}\{-Q_e f(E_e) H_2(E_e) + (\underline{Q} + \underline{P_o} + \overline{P_1} - 1) \\ \times[1 - H_2(\frac{Q_e E_e}{(\underline{Q} + \underline{P_o} + \overline{P_1} - 1)})]\} \quad (2)$$

where underlined terms represent lower bounds and overlined terms are upper bounds. The plug and play QKD sub-system that the proposed method is based on is identical to that which is described by [12]. Rather than repeat the full details here, we will simply use these results. For the full numerical detail see [12, 13].

Our system has the same conditions, parameters and similar limitations to plug and play QKD, such as a maximum distance at which secure secret bits can be sent. Implementation vulnerabilities in the plug and play system will also exist in this system however the basic principle of building secret data out of an attenuated reflection of a classical signal is not dependent the QKD method.

The method proposed here also depends on the OTP which is known to be unconditionally secure by anything but a brute force calculation of every possible permutation of bits and even if a logical outcome is reached confirming it was the actual message sent is impossible [2]. In other words, in Fig.1 the communication on the classical fiber can be easily sampled but can’t be decrypted without knowing the quantum signal.

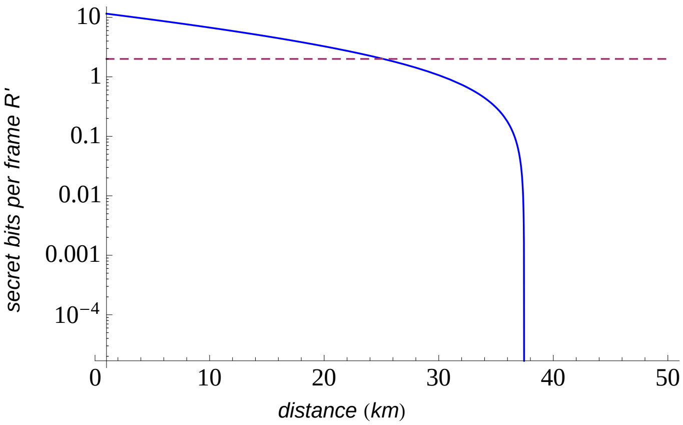

FIG. 2. **Lower bound of secret key rate per frame vs distance.** The dashed line is at the important value of 2 secret bits per frame and our system never runs out of data for the one time pad when above this line. The intersection is at ≈ 25km and N_f is 1230. Note that this is a horizontal cross section of the data in Fig. 3

.

The messages are secure against decryption as long as there is sufficient secret material available. In the event that the system does run out of secret key bits (due to a prolonged period of high loss in the QKD fiber or DoS attack) the system can simply pause the classical communication and rebuild a reservoir via simple QKD. Also at any point when the system is not sending message data the QKD subsystem can be run to produce excess key material. The OTP cannot be defeated with better than brute force effort without defeating the QKD subsystem which has been proven to be unconditionally secure [12].

The message is also tamper evident. To change a bit sent from Alice to Bob, a frame must be either inserted or blocked on the classical fiber. This signal is returned to Alice as bright pulses so the tampering must then be undone on the quantum channel or Alice can trivially detect the change. However any tampering on the quantum channel directly effects the QKD sub system. Any discrepancy in the frame sequence (equivalent to altering the classical data) on the quantum fiber will produce a spike in the instantaneous QBER. This is due to the phase modulations on the two nodes going out of sequence with each other as one node detects more or fewer frames than the other. Also the message is sent classically therefore standard error correction and protection methods such as parity checks and hash numbers can be used to detect tampering or random classical bit errors.

IV. THEORETICAL SYSTEM PERFORMANCE

Here we analysis the simpler one directional communication system. The important figures of merit for the proposed system are the number of secret bits generated by the QKD sub-system per frame R' and the frame rate

F. We denote the secret bit per frame rate as R' to distinguish it from the secret bit rate per pulse R in Equ. (2) from [12, 13]. The number of secret bits per frame must be at least 2. This requirement is set by the OTP sending on average half "1"s and half "0"s regardless of the actual message and that the OTP requires one secret bit consumed per classical bit sent. Each classical 1 bit (i.e. a frame of $N_f \approx 1000$ pulses) must therefore generate on average at least 2 secret bits. If the R' rate is greater than 2 the system will never run out of secret data on which to perform the one-time pad regardless of the volume of communication, the content of the message or the frame rate.

Physically the the secret bit rate per frame R' is determined by the QKD algorithm, the error correction and privacy amplification algorithms, the number of pulses in a frame, the mean photon number per pulse in the "quantum reflection" and the losses in the quantum channel from Alice to Bob.

The secret bit rate per pulse R of the phase encoded "plug-and-play" QKD system using BB84 is well established as Eq.(2) [7, 12, 13]. Building on the numerical model of Zhao, Qi and Lo in particular we can find the lower bound for the secret bit rate per frame R' of our system by simply modifying Equ.(2) from [12] as $R' = N_f R$. Here we use the discussion on a lower bound with an untrusted source (as Eve might be able to influence the classical pulses in some malicious way) and no decoy states; see [12] section V for details of the numerical simulation. We choose this model as a lower bound as it is known that using decoy state models can significantly increase the range at which a secure key can be made [12].

We make some conservative assumptions based on realistic devices. The laser repetition rate is a modest f_{rep} = 5MHz. The mean photon number is,

$$\mu = N\lambda = 10^6 * 10^{-7} = 0.1 \qquad (3)$$

where N is the number of photons per pulse and λ is the variable transmittance of the Alice node [12]. We assume Bob will use relatively high efficiency detectors $\eta_b = 40\%$ with an intrinsic 3% error rate [14]. Cooled SPADS (not cryogenic) with such parameters are commercially available and superconducting nanowire single photon detectors (SNSPD) are available with $\eta_b > 85\%$. We assume the more affordable and less efficient SPADS will be used. We assume a background rate of 10^{-6}, a fiber attenuation of $\alpha = 0.2$ dB/km and $N_f = 1230$ pulses per frame.

In Fig.(2) we show the lower bound for the secret bit rate per frame. We find that the device with the proposed parameters is effective ($R' > 2$) to at least $\approx$ 25km and likely beyond. R' is not the only quantity of interest there is also the frame rate.

The frame rate F is dependent on the round trip time of flight for a frame and the size of the frame itself. The phase encoded QKD device on which the described system is based is limited in that there should only be one frame traveling on the fiber at a time and it must fit in Alice's delay line DL in Fig. 1. This is because the classical pulses as sent on the quantum channel pass through each phase modulator twice (out and back) at times that vary with the dynamically changing line-length. For instance, if an outgoing frame passes through Bob's phase modulator at the same time as Bob is modulating a returning frame of single photons; the outbound frame's phase will be randomized. It may be possible to place more frames on the fiber with careful timing of the round trip but for a lower bound we assume a single frame at a time. Thus the lower bound on the frame rate is dependent on the line-length and the length of Alice's delay line. Clearly there is a diminishing return with increasing N_f and distance.

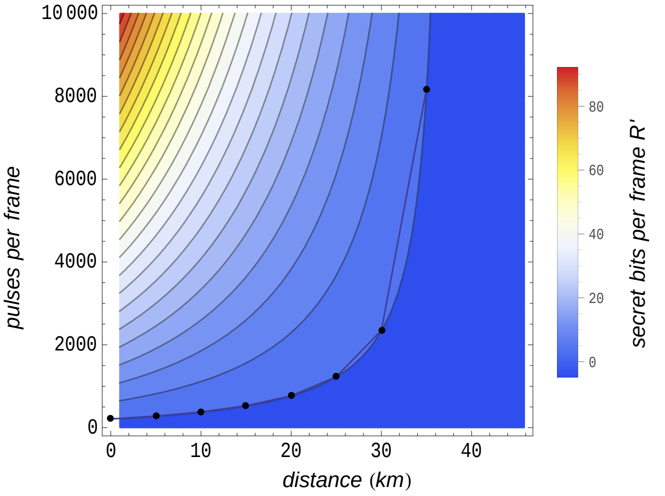

FIG. 3. **Lower bound of secret bit rate per frame R′ as a function of distance L and number of pulse per frame N_f.** The first contour is $R' = 2$ and the dots along it are the N_f data in Table II. The need for larger fames at long ranges is due to fiber loss on the quantum channel becoming the dominant loss mechanism.

Assuming the same parameters as above, particularly the $f_{rep} = 5$MHz laser rep rate and a conservative speed of light in a fiber of $2 * 10^8$m/s, the classical bit rate is determined by the number of pulses in a frame N_f and the line length required for maintaining $R' \geq 2$. The frame rate F is simply one over the round trip flight time T_{rt} on the quantum channel (the time to go from Alice to Bob on the classical channel has no effect),

$$F = c/(2(L + c(f_{rep} * N_f)/2)) \qquad (4)$$

The quantity $c(f_{rep} * N_f)$ is the length of 1 frame in meters and is divided by 2 as Alice's delay line only needs to be half the frame length. L is the length of fiber between Alice and Bob, we ignore fiber in Bob and additional fiber in Alice. The quantity $2(L + c(f_{rep} * N_f)/2)$ is then the total length of fiber traveled to first order and c over the quantity is the frequency. Minimum frame sizes for various line-lengths and the corresponding lower bound frame rates F in bits per second are shown in Table II

TABLE II. Minimum frame sizes and lower bounds of the classical bit rates

km	N_f	F (b/s)
≤1	210	23,800
5	280	9,400
10	380	5,600
15	530	3,900
20	770	2,800
25	1230	2,000
30	2350	1,300
35	8180	500
40	N/A	N/A

and correspond to the data points in Fig.3. Clearly the farther separated the nodes become the larger the frames must be due to loss in fiber between them and in Alice's increasing delay line. This results in longer round trip times and lower frame rates F.

Fig. 3 shows the R' vs N_f and distance. The minimum frame size is on the first contour which is $R' = 2$. Larger frames produce excess secret bits and smaller frames do not produce enough.

We stress that these are lower bounds and should be easily beatable in practice. Several ways of doing so include increasing the laser rep rate f_{rep} which decreases the size of the delay line Alice needs or increasing Bob's detection efficiency η_b which decreases the minimum N_f. To increase the range one can decease the mean photon number μ while increasing η_b and or N_f to compensate or by applying decoy states protocols [12]. We also note the rates in Table II assumes the worst case of continuous classical communication. If the classical communication is paused or intermittent (as it likely will be in practice) the QKD sub system can build excess secure bits allowing for faster bursts of classical data transmission outside the normal operation of the device.

V. CONCLUSION

We have proposed a new method for communication based on quantum security by using a quantum scale attenuated classical signal and the OTP. The large amount of secret data that in most OTP systems is prohibitive is created dynamically by the system via the "quantum reflection" of a classically transmitted and encoded message. We have performed a numerical analysis of realistic devices using conservative values and found a practical lower bound for the secure classical bit rate. At 25km we find a lower bound for the bit rate of at least 2kb/s of unbreakable secure classical data transmitted one direction at a time. This lower bound (for range or bit rate) can in practice be beaten and we have suggested several ways of doing so.

The device also reduces the number of sources and single photon detectors while avoiding complex physical encoding methods such as ultra dense WDM. It does not require entangled resources or on demand photons. Each of these features eliminates a major barrier to cost and practicality. Such a device is practical and well within current technological and commercial capabilities.

VI. ACKNOWLEDGMENTS

The author would like to thank P. G. Evans for helpful discussions and B. Qi for assistance with the numerical method. The author would like to thank the Air Force Research Laboratory for time to complete the publication of this manuscript. This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan(http://energy.gov/downloads/doe-public-access-plan).

[1] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1994).

[2] J. Daemen, L.R. Knudsen, and V. Rijmen, "The block cipher square," Fast Software Encryption **LNCS 1267**, 149–165 (1997).

[3] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," SIAM J. on Computing **26**, 1510–1523 (1997).

[4] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 gbps data encryption over a single fiber," New Journal of Physics **12**, 063027 (2010).

[5] C. E. Shannon, "Communication theory of secrecy systems," Bell System Tech. J. **28**, 656–715 (1949).

[6] G. L. Long, F. G. Deng, C. Wang, and X. Li, "Quantum secure direct communication and deterministic secure quantum communication," Front. of Phys. China **2(3)**, 251 (2007).

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. of IEEE conf. on Comp., Systems and Signal Processing , 175–179 (1984).

[8] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states," Phys. Rev. A **72**, 032301 (2005).

[9] F. G. Deng and G. L. Long, "Secure direct communication with quantum one-time pad," Phys. Rev. A **69**, 05319 (2004).

[10] F. G. Deng and G. L. Long, "Bidirectional quantum key distribution protocol with practical faint laser pulses," Phys Rev. A. **70(1)**, 012311 (2004).

[11] H. Lu, C.-H. F. Fung, X. Ma, and Q. Cai, "Unconditional security proof of a deterministic quantum key distribution with a two-way channel." Phys. Rev. A **84**, 042344 (2011).

[12] Y. Zhao, B. Qi, and H.-K. Lo, "Quantum key distribution with an unknown and untrusted source," Phys. Rev. A **77**, 052327 (2008).

[13] D. Gottsman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. , 175–179 (1984).

[14] L. C. Comandar, B. Frhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Ghz-gated ingaas/inp single-photon detector with detection efficiency exceeding 55% at 1550 nm," J. Appl. Phys. **117**, 083109 (2015).