Coherence modulation at the photon-counting level: A new scheme for secure communication

To cite this article: William T Rhodes et al 2016 J. Phys.: Conf. Ser. 672 012011

View the article online for updates and enhancements.

Related content

- Hydrogen molecular ions: new schemes for metrology and fundamental physics tests
  Jean-Philippe Karr, Sayan Patra, Jeroen C J Koelmeij et al.

- A PHOTON-COUNTING IMAGING FABRY-PEROT SPECTROMETER FOR KINEMATIC STUDIES OF EXTENDED ASTRONOMICAL OBJECTS
  P. Seema, B. G. Anandarao, D. P. K. Banerjee et al.

- Statistical approach to noise in stellar speckle interferometry
  Claude Aime
Coherence modulation at the photon-counting level: A new scheme for secure communication

William T Rhodes¹,², Abdellatif Boughanmi¹ and Yezid Torres Moreno³

¹ Florida Atlantic University, Department of Computer & Electrical Engineering and Computer Science, Boca Raton, Florida 33431, USA
² Universidad Industrial de Santander, GOTS, Grupo de Óptica y Tratamiento de Señales, Escuela de Física, Facultad de Ciencias, Bucaramanga, Colombia

E-mail: wrhodes@fau.edu, latif2178@yahoo.com, ytorres@uis.edu.co

Abstract. When operated at the photon-counting level, coherence modulation can provide quantifiably secure binary signal transmission between two entities, security being based on the nonclonability of photons.

1. Introduction

The secure communication paradigm is illustrated in Figure 1. Alice and Bob want to communicate in complete secrecy; Eve wants to “listen in” on their communication. Three standard methods are identified for secure communication: (a) steganography, where the message is disguised as something else; (b) system hardening, where the communication link is made physically inaccessible; and (c) cryptography, where the message is encrypted in such a way that it is meaningless without the key. In this paper we consider a forth method: transmit the encrypted message in such a way that Bob can receive it correctly, but if Eve attempts to intercept it, it takes the form of random noise.

![Figure 1. The secure communication paradigm.](image)

The case of conventional cryptography is illustrated in Figure 2. In order to “break” the code, Eve must have access to the ciphertext. In our scheme, we prevent Eve from accessing the ciphertext by physical processes that—for her but not for Bob—convert it to a string of random 1's and 0's. The underlying method is referred to as key-specified coherence modulation, operating in our case at very low, photon-counting, light levels. As we will show, Bob, knowing the transmission key, can receive the message virtually error-free. Eve, not knowing the transmission key, detects a succession of

3 Corresponding author.
random 1’s and 0’s. Furthermore, in tapping into the low-intensity light transmitted by Alice to Bob, Eve betrays her presence. In contrast to the case of conventional cryptography, the security of the transmission is guaranteed by laws of physics—by the non-clonability of individual photons—rather than by wished-for unbreakability of a particular encryption scheme. Clearly the scheme has much in common with quantum key distribution, a secure communication scheme that has received considerable attention during the past several decades [1].

Figure 2. Conventional cryptography. To break the code Eve must have access to the ciphertext. Our scheme prevents Eve's this access; instead, she sees only random 1's and 0's.

Before continuing, we recall two basic principles of cryptography. First, it is assumed that Eve knows the encryption algorithm. Second, it is also assumed that Eve is extraordinarily capable: she has the best code breakers, the best possible science, absolutely outstanding technology, etc. A corollary is that security lies in having a strong key and in keeping that key secret (in combination with a good algorithm, of course).

The remainder of the paper is organized as follows: Section 2 describes how 1’s and 0’s can be communicated by means of zero-pi phase shifting in an interferometer. In Section 3 coherence modulation for “secure” communication is introduced. Section 4 describes a possible high-light-level attack by Eve that gives her access to the ciphertext. Section 5 shows how operation at the photon-counting level precludes a successful attack by Eve. A specific example of a statistical analysis is presented in Section 6, and concluding remarks are made in Section 7.

2. Communicating 1’s and 0’s by a phase-shifting interferometer
Figure 3 shows a Mach-Zehnder interferometer with a phase shifter in one arm that allows the phase $\phi$ of the light in that arm to be switched (achromatically, i.e., for all wavelengths) by zero or pi radians. Switching $\phi$ conveys the value of the bit to be communicated: if $\phi = 0$, signifying a 1-bit, all the light exits the interferometer to the right; if $\phi = \pi$, signifying a 0-bit, all the light exits to the top. Although the figure shows laser light input, the device works with white light too, so long as the phase shift $\phi$ is independent of wavelength and so long as the path length difference for the two arms of the interferometer is small compared to the coherence length of the light.

Figure 3. Phase shifting Mach-Zehnder interferometer. All the light exits to the right if $\phi = 0$, signifying a 1-bit. If $\phi = \pi$, all the light exits to the top, signifying a 0-bit.
3. Coherence modulation for “secure” communication

Figure 4 shows the phase shifting interferometer but now with the addition of two time delays, one controlled by Alice ($T_A$, top arm), the other controlled by Bob ($T_B$, bottom arm). If $T_A$ equals $T_B$, phase switching still works, even for white light. However, if $|T_A - T_B| \gg \tau_c$, the coherence time of the light, there is no interference; light goes to both outputs in equal amounts.

The idea underlying “secure” communication via coherence modulation (the word secure is in quotes, because, as explained below, the scheme is, in fact, quite insecure) is thus the following [2]:
- Alice and Bob share a key in the form of the delay time sequence.
- They both use the same delays in synchronism.
- The set of possible time delays is drawn from a set of $M$ different delays.
- They keep the time delay sequence secret from Eve.

4. The problem with coherence modulation at high light levels: A possible attack by Eve

Since Eve does not know the sequence of delays, it would appear that she cannot receive the information transmitted by Alice. In fact, however, the system is not secure. Different possible attacks have been identified. In order for Eve to be successful with these attacks, it is only necessary that the light intensities at the output ports be sufficiently high, i.e., in a “classical” or non-photon-counting regime. One possible attack is illustrated in Figure 5. In this attack, Eve has $M$ “receivers” operating in parallel, each corresponding to one of the $M$ possible time delays used by Alice and Bob (recall, it is assumed that Eve knows the algorithm, is lacking only the key).

![Diagram](image_url)
In this attack, the light is split equally between all “receivers,” one for each of the $M$ possible time delays. One of the output ports has zero output, telling Eve which time delay $T_d$ was used by Alice. Eve thus knows both the time delay $T_d$ and the bit, 0 or 1. Eve can send light on to Bob with the correct properties, thereby hiding her presence. As noted, this attack requires that the light in the system be at high intensity levels. As discussed in the next section, operation by Alice and Bob at the photon-counting level can prevent Eve from gaining such information.

5. How operation at the photon-counting level precludes a successful attack by Eve

We begin with a key observation regarding operation at photon-counting light levels. As suggested in Figure 6, in going from the classical light level case (top) to the photon counting case (bottom), a given light intensity is replaced with the probability of a photon count. Specifically, when the output light intensity is reduced to the level of photon counting, the probability of detecting a photon at a particular output port is proportional to the classical intensity of the light at that port. In the figure, ideal operation is assumed. Switching $\phi$ has the same result even if light is attenuated to the photon-counting level. Figure 7 illustrates the bit-transmission scheme at photo-count levels: $\phi = 0$ produces a photo-count at one output port, whereas $\phi = \pi$ produces a photo-count at the other port.

![Figure 6. Reducing light to photon-counting level. Light intensities are replaced by photo-count probabilities.](image)

![Figure 7. Interferometer operation at the single photon level.](image)

It is assumed in figures Figure 6 and Figure 7 that the interferometer is adjusted for equal time delays in the upper and lower arms. With unequal time delays, things are different, as suggested in Figure 8. Specifically, if $|T_A - T_B| \gg \tau_c$, where $\tau_c$ is the coherence time of the light, photo-counts occur with equal probability at both output ports. No information is conveyed.
Is it possible for Eve to attack the system in the low-light-level regime? With high light levels (classical light) it was easy for Eve to perform many interference experiments simultaneously, in parallel, using all possible time delays, and to determine the time delay used by Alice, along with the associated bit value. Unfortunately (for Eve), the exhaustive parallel-detection attack does not work at the photon-counting level with small numbers of photons. In that case, Eve gains virtually no information. Figure 9 shows Eve’s system in the photon-counting regime. As before, classical light intensities are replaced by photo-count probabilities, unit quantum efficiency being assumed. With single photons, the probability of detecting a photon is $1/2M$ at all of Eve’s ports except the one with the correct delay $T_A$. For that port, the probabilities are zero and $1/M$ respectively. The problem for Eve is that her photo-counts are almost completely randomly distributed: in effect, she has a serious signal-to-noise ratio problem.

6. Example statistical analysis
We consider one specific example of an attack by Eve. Let the number of possible time delays $M$ equal 10 and assume that in a given modulation interval Alice transmits a light pulse that results in 15 photo-counts. As illustrated in Figure 10, almost all of Bob’s photocounts are at 0-bit output port (a single dark count appears at the 1-bit output). Eve’s, on the other hand, are more or less randomly distributed.
distributed. Bob can conclude with a high degree of certainty that a 0-bit was sent, whereas Eve’s results are far from conclusive.

![Image](image_url)

**Figure 10.** Photo counts for Bob and for Eve. Bob’s clearly signify a 0-bit, whereas Eve’s are essentially randomly distributed between 0-bits and 1-bits.

What can Eve do? In a simple attack, Eve can wait until she has ruled out all but a single time delay and associated phase value. She can then send light with the same characteristics on to Bob without betraying her presence. In order to do so, Eve must have access to a sufficiently large number of photons—a condition Alice and Bob will want to preclude. The detection of photons at interferometer output ports is governed by Poisson random processes. These processes are independent from output port to output port. The expected (mean) value of the photon count at a given output port is in proportion to the classical light intensity that would be observed at that port. Assuming that Eve has ideal components (consistent with the assumption that she has extraordinary capabilities), the probability that she determines the correct time delay $T_A$ and associated bit value is given by

$$\left[1 - \exp\left(-\bar{n}_{\text{tot}} / 2M\right)\right]^{2^{(M-1)}} \left[1 - \exp\left(-\bar{n}_{\text{tot}} / M\right)\right]$$

where $\bar{n}_{\text{tot}}$ is the mean number of detected photons and $M$ is the number of different possible time delays.

The results of calculation of Eve’s probability of identifying the correct time delay and phase for four different values ($M$) of possible coherence modulation time delays are shown in Figure 11. For the case of 10 possible time delays, Eve will require 65 photocounts on average (expected value) to achieve a probability exceeding 0.5 of selecting the correct time delay and bit value, information on both of which she must send to Bob in order to avoid detection of her presence. For a 0.9 probability of being correct, the mean number of photons she requires exceeds 100. Larger values of $M$ reduce even further her probability of being correct.

![Image](image_url)

**Figure 11.** Eve’s probability of determining correct time delay and bit value.
7. Concluding remarks
There are other attack strategies available to Eve, one of which is alluded to in Ref. [3]. All must be analyzed in detail. Various other points are noted here for consideration.

- Alice and Bob will want to operate in such a way that the mean number of photocounts available to Eve in a modulation interval is, with sufficiently high probability, less than the number she requires for a sufficiently high probability of correctly determining $T_A$ and $\phi$.
- The number of possible time delays can range from tens to perhaps thousands, depending on the technology used. Clearly the more the better.
- We assume that Eve can work with a perfect system—unity quantum detection efficiency, no dark count, etc.—whereas Bob and Alice face real-world limitations.
- The fraction of information Eve can gain with each transmitted bit is determined by the laws of physics. Quantum mechanics prevents Eve from cloning the photons to allow successful exhaustive parallel searches for the information.
- Whereas for maximal security quantum key distribution (QKD) requires that only a single photon be in the system at a time, the coherence modulation scheme allows—in fact encourages—multiple photons per bit, the mean number increasing with increasing numbers of possible time delays.
- The coherence modulation scheme allows for the transmission of general messages—plaintext, ciphertext, or keys for one-time pad use—with quantifiable security guaranteed by laws of physics.
- A minor modification of the system, to be described in another paper, allows direct implementation of the BB84 QKD protocol.
- Eve can betray her presence between Alice and Bob in a variety of ways. The various possible ways are currently under investigation.
- The effects of non-ideal components, dark current, quantum efficiency of detectors, etc., can be reduced through classical coding of the transmitted bit stream to compensate for a noisy channel.
- Difficulty of maintaining optical pathlength differences to fractions of wavelengths over long distances of, e.g., fiber, is a major concern. Candidate common-path interferometer implementations are under investigation.

References

[1] Barnett S M and Phoenix S J D 1996 Philosophical Transactions: Mathematical, Physical and Engineering Sciences 354 (1708) 793
[2] Gutiérrez-Martínez C, Porte H, and Goedgebuer J P (1995) 10 66
[3] Wacogne B and Jackson D A 1996 IEEE Photon. Technol. Lett. 8 470