Untappable communication channels over optical fibers from quantum-optical noise

Geraldo A. Barbosa[1] and Jeroen van de Graaf[2]

[1] QuantaSec**
[2] Universidade Federal de Minas Gerais, Brazil

Abstract. Coherent light, as produced by lasers, gives rise to an intrinsic noise, known as quantum noise, optical noise or shot noise. AlphaEta is a protocol which exploits this physical phenomenon to obtain secure data encryption or key distribution over a fiber-optic channel in the presence of an eavesdropper. In this paper we focus on the cryptographic aspects of AlphaEta and its variants. Moreover, we propose a new protocol for which we can provide a rigorous proof that the eavesdropper obtains neglible information. In comparison to single-photon quantum cryptography, AlphaEta provide much higher throughputs combined with a well-known technology.

1 Introduction and outline

1.1 Motivation

It has been known for a long time (see for instance [1]) that fiber-optical communication can be eavesdropped easily, and we know that this is not a mere theoretical possibility, but that large-scale wire tapping actually takes a place. Less well-known is the fact that there exists a family of protocols, called AlphaEta, which can accomplish virtually untappable channels using fiber optics. The underlying techiques are very similar to the ones used in traditional fiber optical communication, and herefore many existing, off-the-shelve components can be used to implement Alpha-Eta.

Alpha-Eta and its variants can achieve a throughput of 10 Gb/s and more[2]. This is below the throughput with current fiber optic channels if tappability is not a concern. However, this is still 4 orders of magnitude better than single-photon quantum cryptography à la Bennett and Brassard [BB84], where achieving more than 1 Mb/s seems to be hard, especially at large distances (see for instance [3]). And if the untappable channel is part of a large bundle, it can be used as a reliable channel for key distribution, where the information on the other fibers is encrypted using some symmetric algorithm. In this case, the cost for the Alpha-Eta channel gets amortized over all the fibers in the bundle, usually a few hunderd, and becomes negligible.

1.2 This paper

Whereas many previous publications on AlphaEta focused on the physics and implementation details, this paper approaches the AlphaEta family of protocols from a cryptographic point of view. We do this as follows:

1. In the first part (Sections 2 and 3) we show that Alpha-Eta can be viewed as a communication channel $\mathcal{C}$ in which the sender *Alice* can reliably transmit bits to the receiver *Bob*, while the eavesdropper *Eve* is faced with an intrinsic error which is bounded from below by a certain threshold, δ. Actually we will argue that δ can be made to be close to 1/2. We do this under the assumption that *Alice* and *Bob* dispose of an optical fiber or any other optical channel with appropriate equipment, and that they share some initial random string unkown to *Eve*. We prove this even under the unrealistic assumption that Eve obtains a perfect copy of the light pulse sent by Alice. In fact, due to the intrinsic light noise in the channel, any copy of the signal will carry a distinct noise and, therefore, the signal obtained in each copy will never be identical to each other.

** QuantaSec—Consulting, Projects and Research in Physical Cryptography Ltd., Av. Portugal 1558, Belo Horizonte (MG), 31550-000 Brazil.

2. Subsequently, given that *Alice* and *Bob* share an almost errorless communication channel $\mathcal{C}$ while *Eve* faces an error of at least $\delta \gg \epsilon > 0$, and assuming the existence of an additional communication channel to which *Eve* has access but which she cannot jam, we give an explicit construction of how *Alice* and *Bob* can obtain a shared uniformly random string z to be used as a one-time pad key. See Section 4.
   We proceed to prove the security of this construction. We prove, intuively speaking, that for each bit of z, *Eve*'s error converges to $1/2$. Tecnically speaking, we prove something slightly different: we prove that the amount of Shannon entropy that *Eve* can obtain about z is less then $1/(\ln(2)2^{\lambda})$, where λ is some fixed security parameter; see Theorem 2.
   This establishes the first rigorous proof of the security of an AlphaEta protocol variant, constituting the main contribution of this paper. Our construction is very flexible, since the protocol parameters can easily adjusted to *Eve*'s estimated error rate δ; ours is the first AlphaEta variant that has this property.

1.3 A comparison to single-photon quantum cryptography

In many respects AlphaEta is different from single-photon quantum cryptography, of which BB84 [4] is the prime example:

(a) AlphaEta uses light pulses of medium-range (sometimes called *mesoscopic*) energy and thus consisting of many photons (typically between 100 and 10000) per pulse, whereas in BB84 single photons are sent.
(b) The underlying quantum-mechanical description is different: in AlphaEta the description is based on coherent (Glauber) states, which are quite different from the discrete Hilbert space used in BB84. For instance, there are no qubits in AlphaEta.
(c) The underlying physical principle used to prove security is different. Whereas AlphaEta is based on quantum-optical noise, BB84 is based on the idea that in order to extract information from a quantum state, one necessarily disturbs it.
(d) The attack models are different: in AlphaEta we can give a perfect copy of the quantum state sent by *Alice* to *Eve*, since the latter is confronted with quantum noise. This would not make sense in a security proof for BB84.
(e) As has been said already: mesoscopic light pulses are easier to deal with, use cheaper technology and achieve much higher throughput then BB84.

2 Traditional fibre-based communication

2.1 Modulation and encoding of values

In laser-based communication, a light pulse is sent through a fiber, a very transparent medium with a thickness less than a human hair. Often the phase of the pulse is used as a modulation method. A total of $2M$ different values can be encoded by dividing the full phase circle into $2M$ equal parts, leading to increments of π/M radians. See Figure 1.

Actually, for reasons that will become clear later on, we find it easier to describe each of the $2M$ values as a pair $\langle a, b\rangle$ where $a \in \{0, 1\}$ and $b \in \{0 \dots M-1\}$. *Alice* encodes a message $\langle a, b\rangle$ to the phase angle $\phi_{a,b} = b\pi/M + a\pi$ and sends a light pulse to *Bob* using the fibre-optical channel. Identifying b with $b\pi/M$, we call it the base chosen by A, whereas the bit a only decides whether $\phi = b\pi/M$, or its opposite (relative to the phase circle) value $\phi = b\pi/M + \pi$ will be used. Demodulation is straightforwards: *Bob* measures the phase angle ϕ' and maps it to the nearest phase angle which is a multiple of π/M, from which it is easy to determine the original value $\langle a, b\rangle$.

A natural question to ask is how big M can be in pinciple. That is, how many values can be encoded in one light pulse so that the demodulation process works reliably. This question naturaly translates to the question: What is the accuracy with which *Bob* can measure the phase angle of the light pulses received? On measuring ϕ', *Bob* is confonted with several kinds of noise, such as thermal noise. This kind of noise has no lower bound; in principle: one can always imagine *Bob* constructing a better measurement apparatus which reduces the noise.

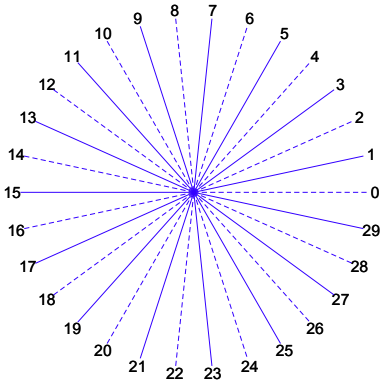

Fig. 1. *Representation of a signal modulation scheme, (also known as a constellation diagram) for traditional fiber-optical communication with the (artificially low) value* $2M = 30$.

However, this is **not** true for a phenomenon called **optical shot noise**, also called **quantum noise**, which has a fundamental origin and cannot be reduced technically. More precisely, it is well-known that, in the setting outlined above, *Bob* is confronted with an intrinsic limitation to measure the phase angle. This noise is inversely proportional to the square root of the average energy of the pulse, i.e. the photon number n. To be more precise, it turns out that the phase angle ϕ is no longer an exact physical quantity, but that it fluctuates around a certain value with a standard deviation of $\Delta\phi = \pm\frac{1}{\sqrt{n}}$. See the next subsection for a brief explanation.

This is bad news for traditional fiber-based communication since it puts a hard limit on M, the number of values that can be modulated in one pulse. For instance, a given n and M may be applied such that $\Delta\phi = 2\pi/M$ is smaller than the standard deviation of the noise asociated with a phase measurement [5]. Therefore, signals will have a signal-to-noise ratio below 1. However, it is good news for cryptographers, because we can create a perfect communication channel between *Alice* and *Bob*, while *Eve* will be confronted with an inherent lower bound on her error probability due to quantum noise, as is shown in Section 3.

2.2 A very brief primer on quantum-optical noise

The AlphaEta protocol can, in some sense, be considered to be based on the Heisenberg uncertainty relations. The (classical) harmonic oscillator $A(t) = Ae^{i\omega t}$ is a precise mathematical description of the physical idea of a wave phenomenon: a particle with mass attached to a spring, a vibrating atom, or light. The quantum extension of this model is called the quantum harmonic oscillator, which is the formalism to describe an electro-magnetic field (among other phenomena).

One important consequence of this model, combined with the postulates of quantum mechanics, is that energy can only assume discrete values, called quanta. Another consequence is that light is described using quadratures, p and q. In another context these variables would correspond to position and momentum, but in the case of photons the notion of position has no physical meaning, only a mathematical one.

Note that p and q are orthogonal variables and do satisfy an uncertainy relation:

$$\Delta p \Delta q \geq 1/2.$$

This implies that neither p nor q can ever be 0, because this would violate this relation.

The physical meaning of this is that even in a vacuum the electro-magnetic field has a positive energy and oscillates. Observe that this oscillation is a result of the quantum mechanical description of the electro-magnetic field; it has no classical equivalent. *It is this intrinsic oscillation of the electro-magnetic field in a vacuum which can be interpreted as the origin of quantum noise.*

Light pulses produced by lasers are best described by coherent states, and it is well-known that the amount of photons (quanta of energy) produced in each pulse cannot be fixed, but follows a Poisson distribution with parameter $\langle n \rangle$, where n is called the photon number. It follows therefore

that the sequence of pulses sent by the laser beam is subject to statistical fluctuations caused by it obeying the Poisson distribution, known as quantum noise, optical noise or shot noise. From this description it should be clear that this noise is not due to imperfections of equipment, but can be considered *intrinsically* quantum.

However, we have only established quantum fluctuations with respect to n, the amount of photons per pulse, whereas in the previous section we claimed that the receiver faces uncertainty with respect to the phase angle ϕ. It turns out that n and ϕ are related. Define the state amplitude as α, we then have that the energy equals $|\alpha|^2 = n$. Through a simple geometric argument it can be shown that in an intense coherent state the amplitude α and the phase ϕ obey the relation $\Delta\phi|\alpha| \geq 1/2$. This results in a Heisenberg-like uncertainty relation

$$\Delta\phi\Delta n \geq 1/2.$$

These two quantities, $\Delta\phi$ and Δn, do have a physical meaning; in particular, the phase angle $\Delta\phi$ defines an upper bound on the resolution with which *Bob* can perform its measuresments, whereas Δn represents the variation in the number of photons sent, as discussed earlier. Note that ϕ and n are not strictly complementary variables; the latter uncertainty relation is a direct consequence of the former one between p and q, combined with the transformation to polar coordenates in state space.

For the interested reader: Wikipedia's entries for *coherent state*[6] and *shot noise*[7] are very (if not too) informative. Additional explanations can be found in [8] and [9], among others.

A comparison to single-photon quantum cryptography BB84 is sometimes said to be based on the Heisenberg uncertainty principle, but this is in fact not correct. The physical principle underlying its security proof is the inference-disturbance principle, which tells us that it is impossible to infer information from a quantum state without disturbing it. In addition it tells us that the more information is retrieved, the higher is the disturbance of the quantum state. Observe that if it were possible to copy a quantum state, this would violate this principle. See [10].

Inference-disturbance is the underlying physical principle that protects *Alice* and *Bob* from an eavesdropper *Eve*: if the latter would try to measure some quantum state transmitted between *Alice* and *Bob*, this would cause a disturbance of this state in a way that *Alice* and *Bob* (who are cooperating) will notice an unusual high error rate, leading them to discard this run of the protocol.

From the preceding paragraph one can see that the physical principles underlying AlphaEta and BB84, though related, are truly different. This is emphasized by the fact that in the security analysis of AlphaEta it is assumed that *Eve* gets a similar copy of the quantum state. Such an assumption would make proving BB84 secure impossible.

3 Alpha-Eta

3.1 The AlphaEta encoding

In this section we show a different encoding which can be used by *Alice* and *Bob* that makes it impossible for an eavesdropper *Eve* to measure the signal without error; in fact we can make *Eve*'s minimal error rate δ approach $1/2$.

Instead of using the fiber-optical channel to send M different symbols, *Alice* and *Bob* will use it to send only two symbols, 0 and 1. In order to send a 0, *Alice* will send $\phi = i\pi/M$ with i an arbitrary even number, $i \in \{0 \dots 2M-1\}$. Similarly for sending 1, but with i an odd number. Since even and odd values are spread equally along the phase circle (see Figure 2), this means that, for sufficiently large M, *Eve* cannot determine which bit was sent without error due to the intrinsic phase uncertainty. The same would be true for the legitimate receiver *Bob*, however.

To solve this problem we assume that *Alice* and *Bob* share some uniformly random string b, about which *Eve* knows nothing. How b is generated is actually one of the main design aspects of the AlphaEta variants, which we will postpone to future sections; for now we assume that b is given to *Alice* and *Bob* in some unspecified way. So *Bob*, when receiving the pulse, knows in which base b to measure and can distinguish perfectly between $\phi' = b\pi/M$ and its opposite $\phi' = b\pi/M + \pi$.

However, *Eve*, who does not know b, cannot distinguish perfectly and is faced with quantum noise, as described in the previous section.

Specifically, when *Alice* sends a bit a she first chooses a basis $b\pi/M$ and then sends either $\phi = b\pi/M$ or $\phi = b\pi/M + \pi$. In order for this to work we need a 0 and 1 on opposite sides of the phase circle, which implies that M is odd.

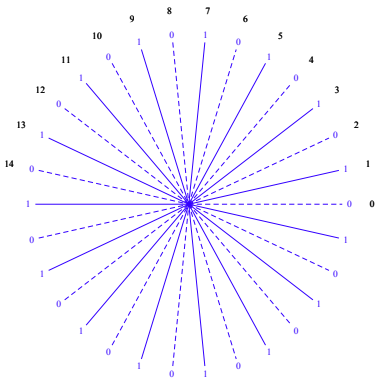

Fig. 2. *Alternative encoding scheme as used by AlphaEta for* $M = 15$*. The inner circle represent the bit values to be transmitted; observe that the bits are alternating, and that the bit coded by phase angle* ϕ *and phi* $+ \pi$ *are always opposite. The outer semi-circle represent the bases.*

This corresponds to the following encoding scheme: If the basis b is even, then a 0 correponds to a phase angle of $\phi_{0,b} = b\pi/M$ where as a 1 correponds to $\phi_{1,b} = b\pi/M + \pi$. If the basis b is odd, then a 0 correponds to a phase angle of $\phi_{0,b} = b\pi/M + \pi$ where as a 1 correponds to $\phi_{1,b} = b\pi/M$.

3.2 The basic Alpha-Eta protocol

In this section we give a formal description of the AlphaEta protocol where a sequence of s light pulses, or s samplings within a continuous light stream modulated by bits, is used to send s bits in each round. We give a basic description in the sense that we do not discuss any of the technical details, nor are we, for the moment, concerned with the origin of the bit string a and the base string b. We assume that a is provided by *Alice* in some way. In addition, as mentioned already, b is presumably shared beforehand between *Alice* and *Bob*, while *Eve* has no information about a or b.

We introduce the following notation:

Parameters

$\langle n \rangle$	average number of photons per pulse
M	the number of bases used
$m = \lceil \log_2(M) \rceil$	the number of bits needed to specify a basis
s	the number of pulses sent in one round of the protocol.

Variables

	Symbols with primes $'$ are those received by *Bob*
$a, a' \in \{0,1\}^s$	the bit sequence sent by *Alice*/ received by *Bob*
$b, b' \in \{0 \ldots M\text{-}1\}^s$	a sequence of uniformly random, shared basis used by *Alice*/ by *Bob*
$a[j] \in \{0,1\}$	the bit sent by *Alice* in position j
$b[j] \in \{0 \ldots M\text{-}1\}$	the bases used by *Alice* in position j

We obtain the following protocol.

Protocol 1: AlphaEta with parameters (n, M, s)

INITIALIZATION
Alice and Bob share b of size sm.

For $j = 1, 2, 3, \ldots s$ do:

ALICE

Step	Action	Comment
1	$\mathsf{Bit} = a[j]$	
2	$\mathsf{Basis} = b[j]$	
3	$\mathsf{CodeAndSend}(\mathsf{Bit}, \mathsf{Basis})$	send bit a over the optical channel in phase angle $\phi_{a,b}$

BOB

1		(no matching step compared to *Alice*)
2	$\mathsf{Basis} = b[j]$	
3	$a'[j] = \mathsf{ReceiveAndDecode}(\mathsf{Basis})$	receive the bits on the quantum-optical channel measuring in the basis $b\pi/M$

3.3 Attacks by Eve

As long as *Bob* agrees with *Alice* on the basis b in which to measure, he can distinguish between a 0 and a 1 sent with almost perfection (bit error rates below 10^{-9}). However, assuming she does not know b, *Eve*'s situation is completely different.

Even generously supplying *Eve* with a copy of the quantum state of the pulse as sent by *Alice*, the eavesdropper, unlike *Bob*, does not know the modulation basis used by *Alice*, does not know in which basis to measure, and her probability of error is therefore much higher. In particular, *Eve*'s measurement of the phase of the pulses sent is subject to the intrinsic phase uncertainty, as explained in Section 2.

More specifically, by an appropriate choice of the optical parameters, in particular $\langle n \rangle$ and M, it is possible to assure that the standard deviation of *Eve*'s phase noise straddles several multiples of $\Delta\phi$, giving away very little information about the bit values sent. For instance, figure 3 in [5] shows that $\delta > 0.40$ can easily be achieved. This corresponds to roughly $\tau = I(\delta = 0.40) = 1 - H_2(0.40) = 1 - 0.97 = 0.03$ bits of Shannon information as a lower bound on the amount of information that *Eve* can obtain through eavesdropping. (Here $H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary Shannon entropy function.) Also see [11] and [9].

We summarize these results by the following theorem. The formal details of its proof require advanced knowledge of quantum optics and are beyond the scope and purpose of this paper.

Theorem 1. *Suppose that Alice and Bob use AlphaEta encoding, that Eve does not know the random value b shared by Alice and Bob for the basis, and that Eve can only measure one pulse at a time. Then it is possible to choose the optical parameters $\langle n \rangle$, the average number of photons per pulse, and $\Delta\phi = \pi/M$, the difference in phase between a 0 and a 1 as determined by M, in such a way that ϵ, the error between Alice and Bob, is less then 10^{-9}, while Eve's error δ can be made to approach 1/2.*

We actually believe that there is no need to restrict *Eve* to single-pulse measurements since, by assumption, she gets a copy of the pulse. However, for the protocol presented in Section 4 this argument does not hold any longer since *Eve* will have access to additional information.

3.4 Variants of Alpha-Eta

The encoding and modulation scheme used in each AlphaEta variant is as described in the previous subsection, but note that the basic protocol only works for one round of blocks of size s. In reality we have a large plaintext message $\overrightarrow{x}$ divided in blocks $(x_1, x_2, \ldots)$ of size s each that *Alice* wants to transmit to *Bob* in a secure fashion. Different AlphaEta variants employ different strategies on how $\overrightarrow{x}$ is enciphered and how the bases $(b_1, b_2, \ldots)$ used in subsequent rounds are generated. (Observe that we use subscripts $i = 1, 2, \ldots$ to denote successive rounds of Protocol 1.) In other words, the protocols differ in where the $(a_1, a_2, \ldots)$ and $(b_1, b_2, \ldots)$ come from.

Data encryption or key distribution In the initial variants of AlphaEta [12, 13, 11], the string a_i sent by *Alice* is directly coming from the plaintext message x_i. In this data encryption approach the bits encoded in the light pulses correspond one-to-one to bits of the plaintext. So any information that *Eve* might gain from a measurement has direct bearings on some message bit $x[j]$. It also implies that any processing on a bit $a[j]$, for instance to improve its randomness, is impossible. Though it is true that some variants propose encrypting the plaintext with a linear shift feedback register to do entropy smoothing, this cannot lead to rigorously provable secure systems.

We prefer variants in which the a_i are pseudo-random or truly random [5], leading to a sequence of random bits shared by *Alice* and *Bob* which is then used as a key for a one-time pad: s bits are sent in each round i, which are used to create the key stream $\overrightarrow{z}$ to be xored bitwise with the plaintext $\overrightarrow{x}$. So we have that $y_i = \mathsf{OTP}(x_i, z_i) = x_i \oplus z_i$ to encrypt and $x_i = \mathsf{OTP}(y_i, z_i) = y_i \oplus z_i$ to decrypt.

But now, instead of $z_i = a_i$, *Alice* and *Bob* can perform some postprocessing on a_i to yield a random string z_i of high entropy about which *Eve* knows nothing. We believe this approach results in robuster protocols and easier proofs. In particular, this is also the approach taken in Section 4 of this paper, which would be infeasible if a consisted of plaintext bits.

Pseudo-random or truly random *a* One issue that comes up with key distribution is whether the bit sequence $(a_1, a_2, \ldots)$ is generated pseudo-randomly, or comes from a truly random source. Most proposals of AlphaEta use a pseudo-random generator to generate the a_i, possibly because generating true random bits at very high speeds is not trivial. But if done naively, this weakens the protocol, since the whole sequence of bit strings $(a_1, a_2, \ldots)$ can be reconstructed if the initial seed value c leaks. We therefore prefer to use a true, physical random number generator; the one proposed in [14] achieves sufficient throughput.

Origin of the bases string *b* Another question is how the randomness for the modulation bases b is generated. Most versions of AlphaEta generate the sequence $b_1, b_2, \ldots$ pseudo-randomly, initially by a linear shift feedback register initiated with some initial value c, later substituted by AES in Output Feedback mode [11, 12].

In [5] a different recursive process is used: the random bases b_{i+1} for the $(i+1)^{\text{th}}$ round are derived from the random bits a_i generated by *Alice* and transmitted to *Bob* through the AlphaEta channel in round i. In the first round both *Alice* and *Bob* can simply use the initial secret string c of size ms to obtain b. But for the second and subsequent rounds there is a problem since ms bits are necessary for modulation bases b, whereas only s fresh random bits are introduced in the system.

This is solved by sending m consecutive pulses using the *same* transmission bases but using a *decreased* energy level, making the adversary's task harder. So in the first round, b_1 is determined by copying b_0, that is, $b_1 = \mathsf{DetBases}(b_0)$. In all subsequent rounds, b_i is determined by taking the first m bits from a_{i-1} to define $b[1]$ to $b[s]$ thus repeating the basis s times, then the next m bits from a_{i-1} are taken to define another set of s bases, and so forth. However, repeating the same bases for a block of consecutive bits does not seem a good idea and is unnecessary, as we show in Section 4.

3.5 A comparison to single-photon quantum cryptography

Before we start a new section proposing a new variant of AlphaEta, we pause to make a comparison with the BB84 protocol [4].

If we set the average number of photons per pulse $\langle n \rangle$ to 1 and the number of bases M to 2 in the AlphaEta Protocol, we use the same encoding as BB84. Again, we stress that the underlying quantum-mechanical description of medium-energy (mesoscopic) optics differs from single-photon optics.

The BB84 protocol uses a different strategy to obtain a secret key z: the bitstring a and the basisstring b are chosen at random by *Alice* and she sends s photons. *Bob* chooses his bases b' at random and measures the photons he receives accordingly. Then, through some conventional communication channel, *Alice* sends b to *Bob*. In response, *Bob* tells in which positions he used the same bases, i.e. the values of $J = \{j \in [1, s] : b[j] = b'[j]\}$. Subsequently, both *Alice* and *Bob* and use $a[j] : j \in J$ as a way to obtain z. The bits a_j with $j \notin J$ are discarded.

It therefore might seem that in BB84 no prior secret string is needed to bootstrap the protocol, but this is not true. The reason is that the conventional communication channel used in the final steps is public, meaning that *Eve* has full access to it. So in order to authenticate the messages sent through this channel, *Alice* and *Bob* need a common secret string. Conclusion: the assumption made in all the AlphaEta variants that *Alice* and *Bob* share some random string is implicitly made in BB84 as well.

4 Using a randomness pool and privacy amplification

The previous section established a setting in which *Alice* and *Bob* can send bits through a perfectly reliable communication channel, where *Alice* and *Bob* suspect that *Eve* might be wiretapping but is exposed to an error rate of at least δ per pulse.

Such scenarios have been extensively studied in information theory. For instance, Csiszár and Körner [15] showed that if *Alice* and *Bob* share a communication channel with error ϵ, eavesdropped by *Eve* with error $\delta > \epsilon$, then *Alice* and *Bob* can establish secure, untappable communication without interaction. Maurer [16] proved something much stronger if *Alice* and *Bob* can interact reliably: in the satellite scenario *Alice*, *Bob* and *Eve* receive a signal from a common source of randomness but with error rates ϵ_A, ϵ_B and δ respectively. Now even if *Eve* has a stronger antenna and therefore $\delta < \epsilon_A, \epsilon_B$, *Alice* and *Bob* can obtain a secure channel, though the construction is not very efficient. See [17] for a nice explanation. Our situation is much more confortable since $\delta \gg 10^{-9} \geq \epsilon$.

So just like BB84 and Maurer, we assume that, beside the AlphaEta channel, *Alice* and *Bob* can exchange messages through some additional, authenticated communication channel to which *Eve* may have access as well. Note that one could implement this channel using the same channel that AlphaEta uses, but there might be better alternatives. In this setting we present a protocol which allows *Alice* and *Bob* to produce an infinite sequence of random keys $(z_1, z_2, \ldots)$ about which *Eve* has virtually no information. Though our construction combines existing techniques, the idea to use two synchronous pools of randomness for *Alice* and *Bob* together with privacy amplification seems to be novel.

4.1 Using pools of random bits

In order to provide an operating system and its calling applications with good randomness, many random bit generators maintain a pool of random bits. More sophisticated designs make even use of entropy estimation, which are lower bounds on the amount of entropy certain processes are contributing to the pool[18]. And each time a system process calls random bits from the randomness pool, it verifies whether sufficient entropy is present; if not, the process blocks until sufficient entropy is present.

We use this pool idea to redesign the protocol: we have a physical random bit generator at *Alice* which inserts randomness into *Alice*'s pool. This fresh randomness is also forwarded to *Bob* over the AlphaEta channel, thus ensuring the identical contents of pool A and pool B. Then *Alice* and *Bob* use an identical procedure to extract the random bits used for the encryption key stream.

In the previous section we saw that the AlphaEta channel leaks information. However, as long as the amount of information that *Eve* gets out per round is less than s bits (i.e. less than one bit of leaked information per bit sent), we have more entropy entering the system than leaving it, so at least in principle we should be able to keep the pools full with entropy. The question is how to design the system in such a way that its security is easy to prove and easy to implement.

Here we propose a solution which is secure in an information-theoretical sense. The idea is the following: Let c_0 be the initial state of Pool A and Pool B. First the pools will be used to extract ms random bits for the transmission bases b. Then, for subsequent rounds $i = 1, 2, \ldots$ *Alice* and *Bob* apply some identical, recursive procedure to the pool's current state c_{i-1} concatenated with the freshly generated random bit string a_i; the result will be the new pool state c_i. In order to maximize the entropy of the new new pool state c_i and the key z_i we use privacy amplification.

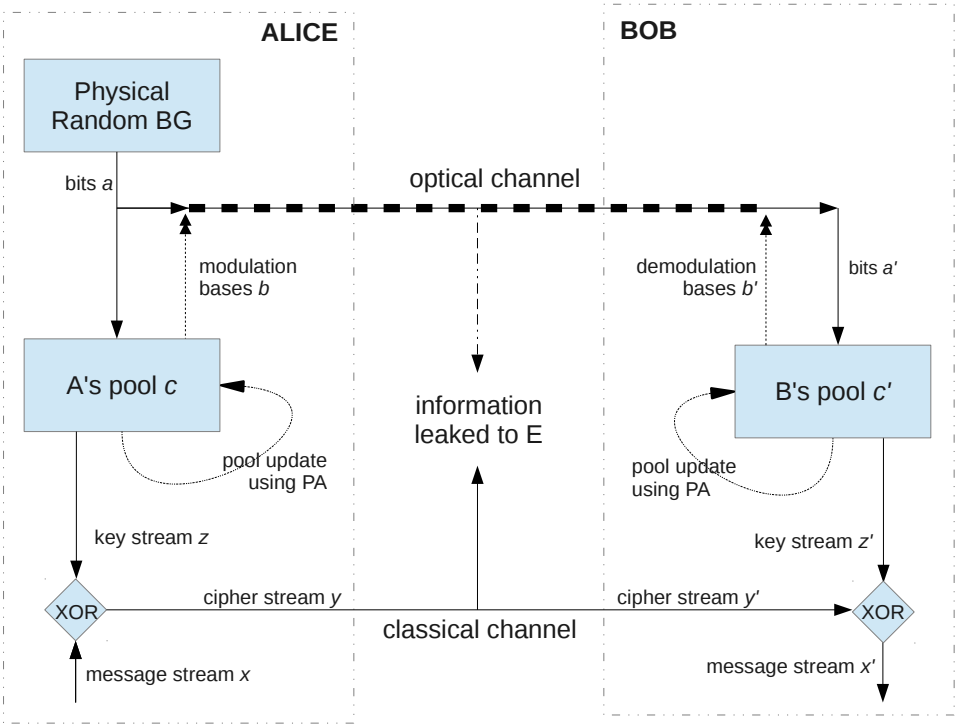

Fig. 3. *The new protocol using randomness pools for Alice and for Bob, which are completely synchronized. Reseeds come from PhRBG on Alice's side, synchronicity is maintained by forwarding the bits to Bob through the quantum-optical channel, and pool updates are based on privacy amplification. The quantum-optical channel leaks* some *information to Eve; the classical channel leaks* all *information.*

4.2 Privacy Amplification

Privacy Amplification (PA) (see [19]) is a general technique in which *Alice* and *Bob*, who share a random string c of size l, assume that the adversary has obtained at most t bits of Shannon information about c. To reduce *Eve*'s information, they enter in a public exchange of messages to which *Eve* has access, resulting in a shorter string $\overline{c}$ about which *Eve* has exponentially little information.

One intuitive (but maybe not efficient) way to extract one privacy-amplified bit from c is as follows: *Alice* generates a random bit string r_1 of the same length, l, and sends it to *Bob* over the

public channel. Both parties compute the parity of the bitwise xor of c and r_1, which is equivalent to the mod 2 inner product $c \cdot r_1$ of c and r_1 when interpreted as vectors in $\{0,1\}^l$. This bit is the first bit of $\overline{c}$, i.e. $\overline{c}[1]$. The other bits of $\overline{c}$ are determined by choosing more random bit strings $r_2, r_3, \ldots$ and computing $\overline{c}[k] = c \cdot r_k$. To reduce *Eve*'s information of t bits about c, one has to repeat this process $l - t$ times. The question is then: how much information does *Eve* have about $\overline{c}$?

The Privacy Amplification Theorem [19] tells us that *Eve* has at most $1/\ln(2)$ bits of information about $\overline{c}$. More importantly, it tells us that if we compute $\overline{c}[k] = c \cdot r_k$ only $l - t - \lambda$ times, i.e. we deliberately choose $\overline{c}$ to be λ bits shorter than $l-t$, then, after PA, *Eve* is left with only $1/(\ln(2)2^{\lambda})$ bits of information about $\overline{c}$. Here λ is a constant security parameter.

4.3 The improved AlphaEta protocol

The ideas outlined in the previous subsections lead to the following protocol.

Protocol 2: Improved AlphaEta with pools and privacy amplification

INITIALIZATION
Alice and Bob share c_0 of size and entropy at least ms.
For $i = 1, 2, 3, \ldots$ do:

ALICE

Step	Action	Comment
1a	$a_i = \mathsf{PhRBG}()$	get bitstring from PhRBG
1b	$b_i = c_{i-1}[1, ms]$	extract ms bits from pool for the bases b
1c	$\mathsf{CodeAndSend}(a_i, b_i)$	send over the AlphaEta channel
2	$\mathsf{SendCC}(f)$	send a description of an instance of a universal hash function f from $\mathcal{F}$ to *Bob* over the conventional channel
3a	$c_i = f(c_{i-1}\|\|a_i)$	Alice applies PA from $ms+s$ bits to $ms+s-t-\lambda$ bits
3b	$z_i = c_i[ms+1, ms+s-t-\lambda]$	Alice uses $\overline{s} = s-t-\lambda$ bits from the pool as bits for the key stream z. In the Step 1b of the next round she will use the remaining (first) ms bits to determine the bases b.

BOB

1'a		(has no matching protocol step compared to *Alice*)
1'b	$b_i = c_{i-1}[1, ms]$	get bases bits from initial pool value
1'c	$a_i = \mathsf{ReceiveAndDecode}(b_i)$	receive the bits on the AlphaEta channel
2'	$\mathsf{ReceiveCC}(f)$	receive a description of an instance of a universal hash function $f \in \mathcal{F}$
3'a	$c_i = f(c_{i-1}\|\|a_i)$	Bob applies PA from $ms+s$ bits to $ms+s-t-\lambda$ bits
3b'	$z'_i = c'_i[ms+1, ms+s-t-\lambda]$	Bob uses $\overline{s} = s-t-\lambda$ bits as bits for the key stream z'. In the Step 1b' of the next round he will use the remaining (first) ms bits to determine the bases b'.

4.4 Security properties

For the security of Protocol 2 it is essential that the bases b used to modulate are random, and that the OTP output stream z is random. The following theorem established that this condition is fulfilled if the pool is initiated with sufficient entropy shared by *Alice* and *Bob*.

Theorem 2. *Let λ be the security parameter for privacy amplification and set $\overline{s} = s - t - \lambda > 0$, where $\overline{s}$ denotes the length of the output stream z_i per round. If the pool is initiated with ms random bits shared by Alice and Bob, then the sequence $z_1, z_2, ...$ produced by the protocol is statistically indistinguishable from the uniform distribution.*

Before we give the proof we recall that λ is a constant, and therefore, supposing that m is determined by optical considerations, the block size s can always be chosen such that the condition $\overline{s} = s - t - \lambda > 0$ is satisfied.

Proof: Since we have s fresh bits coming in, and we lose $t + \lambda$ bits when updating the pool, the length of the output stream z per round, $\overline{s}$, cannot exceed $s - t - \lambda$ bits if we don't want to lose entropy in the pool. Thus to ensure that after PA we end up with ms bits for the bases in the next round, plus $s - t - \lambda$ bits as net output of the process, the result of PA must yield $ms + s - t - \lambda$ bits. Whereas the input must be of size $ms + s$ bits. This means that we need a universal hash function f from $ms + s$ bits to $ms + s - t - \lambda$ bits.

The following table shows how pool evolves during one round of the protocol, beginning with ms bits of entropy and ending with ms bits of entropy.

step	state of the pool	number of bits in the pool	entropy of the pool	*Eve*'s information about pool
	initial state	ms	ms	0
1b	ms bits are used for b	ms	ms	0
1c	s bits are sent over the channel and added to the pool about which *Eve* might have at most $t = \tau s$ bits of information	$ms + s$	$ms + s - t$	t
3a	PA with parameters $ms + s, ms + s - t, \lambda$ is applied	$ms + s - t - \lambda$	$ms + s - t - \lambda$	0
3b	$\overline{s} = s - t - \lambda$ bits are extracted for the OTP key stream z	ms	ms	0

Eve may be able to get some information about a, but this is eliminated because of privacy amplification. What she needs is information about z_i which, by construction, are copied from c_i, which was subjected to PA. Because of the main theorem in [19], *Eve* gets at most $1/(\ln(2)2^{\lambda})$ bits of information about each $z_i \in \{0,1\}^{\overline{s}}$, meaning that each z_i is statistically indistinguishable from the uniform distribution. □

It may seem a surprise that entropy can be maintained in an information theoretic sense. But first note that even though ms random bits are used in each round, only $t = \tau s$ bits leak to *Eve*. In addition, it must be stressed that *universal* hashing is used, and that the randomly chosen universal hash function f used by *Alice* and *Bob* changes in each round. So in each round an enormous amount of randomness is added to the system Even though observed by *Eve*, *Alice* and *Bob* can obtain a random string.

5 Discussion and conclusion

5.1 On the practical difficulty of combined measurements

For the sake of simplicity we made the assumption that *Eve* must measure each light pulse right away. Even though the theory of quantum mechanics does not *Eve* exclude the possibility of storing a light pulse and making a combined measurement of several (or all) pulses once they have been received, this is in practice very difficult.

Recall that photons are not particles in the sense that they can be localized or stored. For a light signals of frequency ω_0 there exists a frequency interval around ω_0 where one could detect photons. This interval is known as the bandwidth around ω_0, and this bandwidth could be enormous. So any attempt to record the signals as faithful as technologically possible will demand a prohibitive amount of memory. Moreover, if one considers weak signals and take phase as the bit encoding method, it was shown [20] that the measure of phase is dependent on every specific experimental setup used for the measurement. This shows the complexity of recording a faithful representation of weak light signals in communication channels. Perhaps, the best practical delay *Eve* could try is to build an optical delay line and get her measurements after Alice and Bob protocols are over – if it proceeds in a very short time.

5.2 Which class of universal hash functions to use

Our intuitive description of PA can be described as a matrix multiplication $\overline{c} = Rc$ where R has rows $r_1, \ldots r_{(ms+s-t-\lambda)}$. So R is an $(ms+s) \times (ms+s-t-\lambda)$ random matrix. There exist classes of universal hash functions with a more succinct description, such as $\mathcal{F} = \{f(x) = Ux+V\}$, where U, x, V are elements in $\mathbb{F}_{2^{ms+s}}$. In this case the numbers of bits to describe a randomly chosen $f \in \mathcal{F}$ is $2(m+1)s$. One can also consider to use random $(ms+s) \times (ms+s-t)$ Toeplitz matrices as the class $\mathcal{F}$; this leads to description of f also of size $2(m+1)s$, but to faster operations. In fact there are many more classes of universal hash functions to choose from. The actual choice will depend on implementation considerations.

5.3 An alternative way to communicate the function f

A problem of the protocol presented is that needs a lot of bandwidth to send the universal hash function f from *Alice* to *Bob*: for every block of $\overline{s}$ bits of the streaming key, we need to send $2(m+1)s$ bits to specify the f used for privacy amplification in each round. This implies an expansion of at least a factor $2m+1$ (where m is typically 10).

Instead of *Alice* generating f randomly and sending it over the public channel, which allows *Eve* to get a copy too, we can imagine a different solution. The universal hash function f to be used in PA will be generated pseudo-randomly by *Alice* and *Bob* who share an additional initial seed value e_0 to this end. In addition, we assume that *Eve* does not know this initial e_0, and therefore *Eve* is kept in the dark about the exact function f that *Alice* and *Bob* use for PA. The quality of the PRBG that is used for f can be based on various assumptions.

The implicit claim of this construction is that *Eve* in the new situation (i.e. with f generated by a PRBG whose values she does not know) is not better off than in the old situation (with f truly random and known to *Eve*). This seems intuitively true, but may be hard to prove. For that reason it might be interesting to base the PRBG on some hard assumption: AES, SERPENT, an NP-Hard or NP-Complete problem.

Another option would be to fix the function f forever and presume that *Eve* knows it too. This strategy seems justified as long as we can assume that *Eve* cannot influence the noise[21]. However, these arguments have been made in the context of classical noise, and would have to be re-evaluated. In our case *Eve* cannot really influence the noise, but has some influence on how she sees it since she can choose which measurements to perform.

5.4 Error correction

We mentioned that the error between *Alice* and *Bob* is very small, $\epsilon \leq 10^{-9}$. However, in our proposed solution a simple bit error will be catastrophic since PA will amplify any bit error, and Pool A and Pool B would be out of sync. And with throughputs of 10 Gb/s this is expected to happen ten times per second.

We therefore need to use some error correcting code to reduce ϵ to 10^{-15} or below. For instance a $(1023, 1013)$-Hamming code corrects one error at the cost of sending $u = 10$ additional parity bits. If burst errors are a problem, then interleaving (spreading the errors over different codewords) might be necessary. More advanced solution, all using parity bits, exist; see for instance [22].

The point is that these u parity bits must be transmitted from *Alice* to *Bob* consuming some bandwidth. However, even if we suppose that we give *Eve* full access to these parity symbols, the amount of information she gains from them is relatively small, meaning that the assumption that she only obtains t bits of information can be made by redefining $t_{\text{new}} = t_{\text{old}} + u$.

6 Open questions

Protocols based on quantum optical noise appear to be a wonderful source of research questions, and we finish this article raising a few:

- *What is the practical value of the new protocol?* Plans exist to implement this protocol with off-the-shelve components, but the universal hash function needs to be implemented at very high speeds for telecommunication (1Gb/s and up). This may be a bottle-neck, so maybe pragmatic choices need to be made to reach a protocol that can be implemented in practice, as discussed in Subsection 5.3.
- *What is the theoretical security of our protocol?* At this point, the exact theoretical status of our protocol is not yet clear. We think we can prove it secure under a wide class of very reasonable attacks, but we still cannot claim unconditional security. In this context it is not clear what a general, global attack means. An attack can proceed several ways, and we do not know how to encompass everything in a single frame. In other words, even if one could map, say, all the photons of a laser beam (say 10^{20} photons or more) in Hilbert spaces, what mapping would be necessary to represent all possible physical actions on this beam or on these individually treated photons? The number of physical actions possible is infinity.
- Nevertheless, from a pragmatic point of view: even if the protocol can not be proven secure in the widest possible model allowed by quantum mechanics, *it may very well be secure making some reasonable additional assumption* about time, or about *Eve*'s technical limitations (like the limitation to store many photons without actually measuring them), etc. After all, the algorithms which are used in practice (RSA, AES) also make assumptions, and the security provided by our protocol may be stronger and more adequate in certain situations. Applied cryptographers do not care about the scientific beauty of a protocol, but whether it is secure in practice, and efficient.
- In the wider context of cryptographic protocols our approach begs the following question: *Can quantum-optical noise be used to implement oblivious transfer*, thus implying bit commitments and multi-party computation? Since it is well-known that any kind of classical noisy channel can be used to implement these primitives[23], the answer seems to be YES. On the other hand we have the no-go theorems of Mayers and of Lo and Chau related to quantum bit commitment[24, 25]. We presume they apply here too, but maybe these questions must be looked at again in more detail. Quantum noise exists! How can it be used constructively for cryptographic purposes?

We plan to work on these questions in the future and invite other researchers to do the same.

7 Conclusion

We presented an improved construction of the cryptographic aspects of AlphaEta by introducing pools of randomness for both *Alice* and *Bob*. The effect of this pool is smoothing of the entropy, and hiding the relationship between bits sent over the optical channel and those used in the one-time pad, implying a significant security improvement.

Acknowledgement

We acknowledge the support of Ministério da Ciência, Tecnologia e Inovação (MCTI)-Finep(0276/12)-Fundep(19658)-Comando do Exército(DCT)-RENASIC. The authors thank Gabriel Almeida for helpful discussions. JvdG thanks Harry Burhman for curing him from his quantum allergy.

References

1. G. Schmid, "On the existence of a global system for the interception of private and commercial communications (ECHELON interception system)." `http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN`, 2001.
2. G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Communications Magazine*, vol. Nov 2009, 2009.
3. A. Dixon, Z. Yuan1, J. Dynes, A. Sharpe, and A. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Physical Review A*, vol. 68, no. 052307, 2003.
4. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing (Bangalore, India*, pp. 175–179, 1984.
5. G. A. Barbosa, "Fast and secure key distribution using mesoscopic coherent states of light," *Physical Review A*, vol. 68, no. 052307, 2003.
6. Wikipedia, "Coherent States." http://en.wikipedia.org/wiki/Coherent_state, 2013.
7. Wikipedia, "Shot noise." http://en.wikipedia.org/wiki/Shot_noise, 2013.
8. U. Leonhardt, *Essential Quantum Optics: From Quantum Measurements to Black Holes.* Cambridge University Press, 2010.
9. G. A. Barbosa, "Information theory for key distribution systems secured by mesoscopic coherent states," *Physical Review A*, vol. 71, no. 062333, 2005.
10. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.
11. R. Nair, H. Yuen, E. Corndorf, T. Eguchi, and P. Kumar, "Quantum Noise Rondomized Ciphers," *Physical Review A*, vol. 74, 2006. `http://arxiv.org/pdf/quant-ph/0603263`.
12. G. A. Barbosa, E. Corndorf, P. Kumar, and H. Yuen, "Secure communication using mesoscopic coherent states," *Physical Review Letters*, vol. 90, no. 227901, 2003.
13. H. Yuen. unpublished.
14. G. A. Barbosa, "Harnessing Nature's Randomness: Physical Random Number Generator." unpublished.
15. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, 1978.
16. U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.
17. S. Wolf, "Unconditional security in cryptography," in *Lectures on Data Security*, vol. 1561 of *Lecture Notes in Computer Science*, pp. 217–250, Springer, 1998.
18. N. Ferguson and B. Schneier, *Practical Cryptography.* Wiley & Sons, 2003.
19. C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.
20. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics.* Cambridge University Press, 1995.
21. H. Chabanne and G. Fumaroli, "Noisy Cryptographic Protocols for Low-Cost RFID Tags," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3562–3566, 2006.
22. B. Smith, A. Farhood, A. Hunt, F. Kschischang, and J. Lodge, "Staircase Codes: FEC for 100 Gb/s OTN ," *IEEE Journal of Lightwave Technology*, vol. 30, no. 1, pp. 110–117, 2012. See also `arxiv.org/pdf/1201.4106.pdf`.
23. C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions (extended abstract)," in *FOCS*, pp. 42–52, 1988.
24. D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Physical Review Letters*, vol. 78, pp. 3414–3417, 1997.
25. H.-K. Lo and H. F. Chau, "Is quantum bit commitment really possible?," *Physical Review Letters*, vol. 78, pp. 3410–3413, 1997.