Fundamentals for immediate implementation of a quantum secured Internet

Geraldo A. Barbosa∗
QuantaSec–Research in Quantum Cryptography Ltd.,
Av. Portugal 1558, Belo Horizonte MG 31550-000 Brazil.

(Dated: 16 August 06. A typo in the eigenvalues in version V1 was corrected and a few short comments added.)

This work shows how a secure Internet for users A and B can be implemented through a fast key distribution system that uses physical noise to encrypt information transmitted in deterministic form. Starting from a shared secret random sequence between them, long sequences of fresh random bits can be shared in a secure way and not involving a third party. The shared decrypted random bits -encrypted by noise at the source- are subsequently utilized for one-time-pad data encryption. The physical generated protection is not susceptible to advances in computation or mathematics. In particular, it does not depend on the difficulty of factoring numbers in primes. Also, there is no use of Linear Feed Back Shift Registers. The attacker has free access to the communication channels and may acquire arbitrary number of copies of the transmitted signal without lowering the security level. No intrusion detection method is needed.

PACS 03.67.Dd, 05.40.Ca

INTRODUCTION

Are there conditions to have a physical-noise secured Internet (NSI) -instead of a relying on the difficulty of factoring numbers in primes- implemented for common users? The answer is Yes; and the associated cost is very low – this paper shows how it can be immediately implemented.

Let us start with the following classical scenario: User A (Alice) uses a (private) laptop with no network or web access to encrypt a message X onto a file C to be sent to end user B (Bob). The encryption is done with a one-time-pad key sequence of truly random bits stored in his computer. This random sequence was beforehand shared with B. File C is fully characterized and transferred to a computer with web access. From this point on file C is appended with all identification information, split into different packets -as demanded by the Internet protocol (IP) stack [1]– and routed through any available physical link to the end user B. All modifications are done according to the requirements of the Open Systems Interconnection (OSI) layers and protocols [2] including particularities demanded by web service providers. Among these procedures error correction protocols are included. At the destination, file C is assembled bit-by-bit and delivered to B. Stripped from communication information attached to it, B checks for file integrity and decrypt C using the shared random sequence. The obtained message has unconditionally proven confidentiality and authentication. These procedures are independent of any established Internet security protocol. It is expected that Internet should not modify the bit content of the original file after its full recover by B. In case A and B are performing a commercial operation, non-repudiation is easily assured to both users. The one-time-pad protocol is not intended to modify the Internet protocols in anyway. It is a complementary method for secure communication between two users that works independently and on top of all IP protocols. A and B have their secure communication totally under their control. This way, the users know that their protection does not rely on mathematical difficulties to factoring number in primes nor they depend on third parties to assure the desired security.

The reader may be saying: But this is a classical encryption between two users and well known to be secure; there is nothing physical or new here. However, is this scenario realistic if A and B wishes to use it continuously? The answer to this question has been negative: The practical difficulties for A and B to keep sharing long sequences of one-time-pad keys makes this scenario highly inefficient and, therefore, useless for most uses. Practical systems have not yet been devised that allow A and B to use the starting secret $K_0$ as a support to transfer or exchange fresh sequences of random numbers.

This work shows a practical way that allows A and B to share through the Internet these new sequences of random keys in a secure way. This could bring life to the starting scenario. The basic ingredients needed are a very simple software, a physical random generator (not a pseudo random generator) coupled to the private computer and a starting secret key $K_0$ shared by A and B. This starting sequence $K_0$ will seed a long sequence of truly random bits. In a sense, it can be seen as a one-time-pad booster: Starting from a shared seed $K_0$, A and B end up sharing a sequence of $L (>> K_0)$ random bits. No third party is used to establish the key sequences to be used by A and B. No need for intrusion detection exists. Furthermore, all of these elements allow immediate implementation – even commercial (truly) random generators exist [3] for moderate speeds.

One may also argue that some quantum protocols exist that are proven secure as the well known single photon protocol BB84 [4] to distribute random bit sequences and, therefore, what novelty is being offered? Single-
photons. Other consequences, no intrusion detection mechanism will be guaranteed by the one-time-pad method itself. As an obscure the transmission for protection. The cipher message sent over any physical channel with no need to further discuss this fundamental problem and the proposed puzzle with a solution presented in this work. Before net secure sequences of random bits. There resides the special value of this system and does not decrease the physical protection tied to the signals. The key distribution procedure uses the installed communication network but its protection depends on physical laws instead of mathematical complexities. 2) The data is prepared in any convenient form for the underlying OSI layers with no need for modification of the IP in use. A simple binary file can be prepared by A or B to be sent through the OSI stack. These characteristics will not be dependent of security procedures established at the OSI’s “Presentation” layer. Normal data manipulation demanded by OSI protocols can be applied. The only and usually expected requirement is that the end user receives the data file as it was delivered by the sender, bit-by-bit. This presupposes use of error correction protocols to guarantee perfect delivery of the ciphered message to the end user. The IP protocols in use are then left untouched; just a private protection layer is added by the users. This added layer, under user’s control, presents no risk in the eventual creation of algorithms for fast factoring of numbers in primes. Also, even creation of a quantum computer or quantum processors does not decrease the physical protection tied to the signals. There resides the special value of this system and its proposition as a secure layer for users that demand protection based on physical principles.

The central problem is how to distribute over the Internet secure sequences of random bits $R_i$. This is the main puzzle with a solution presented in this work. Before discussing this fundamental problem and the proposed solution, one may state that if this is true, it is clear that ciphered messages based on one-time-pad could be sent over any physical channel with no need to further obscure the transmission for protection. The cipher message could even be made public because the protection is guaranteed by the one-time-pad method itself. As another consequence, no intrusion detection mechanism will be needed.

Use of classical carriers to carry recorded quantum information is a normal process that is often not perceived. Scientific journals use this process constantly—although they do not require a special protection. Understanding quantum phenomena as sets of probable events or different possible quantum trajectories, the classical information obtained from instrumental clicks is nothing more than recording one amongst the many possible quantum trajectories. Repetition of the same measurement operation may lead to a very distinct result; that is to say, a record of another trajectory among the possible ones. The files to be sent over the Internet are to be obtained in samplings of single events (bits). The information protection desired relies on the multitude of possible quantum trajectories that generates each single bit of the random sequence. This is completely different from using pseudo noise generated in a deterministic process (hardware stream ciphers), whose generation mechanism can be searched, discovered and used by the attacker [6]. One may easily argue, for example, that phase fluctuations on a laser output or in thermal radiation are not quantum. Both can be represented by Gaussian random processes. Several definitions (e.g. Glauber’s Positive $P$ representation [7] or Mandel’s $Q$ parameter [8]) can be utilized to classify these fluctuations as Poissonian or super-Poissonian. Light in a coherent state will be at the boundary between the “classical” and “quantum” realms. Although the question if electromagnetic radiation can be classified as classical or quantum is probably a philosophical question, the importance of the uncontrollable or unpredictable physical fluctuation in both representations is the important aspect to be utilized in this work. Sometimes the expression “quantum fluctuations” will be utilized by the author to express fluctuations associated with the light field. The reader may ignore the “quantum” adjective with no harm for ideas presented. A quantum calculation is often quite adequate to deal with light fluctuations and will be utilized.

This work will discuss the physically built-in properties of these secure files. It will also explains why one-time-pad keys can be created and shared by A and B through the Internet. This is basically about physics, not a discussion about software or deterministic (pseudo-random) stream cipher hardware. The security is intrinsically connected with fluctuations of the light field. Before discussing the information content in this process, the Section will describe the basic standard distribution protocol. After this description, it is explained how the recorded files carry the noise protection.

THE DISTRIBUTION PROTOCOL

The deterministic signals going through arbitrary communication channels are encrypted by random signals obtained from optical sources and are described by non-orthogonal $M$-ry bases. Distribution of secure data
and key distribution over optical channels using M-ry bases has been discussed on recent publications [11–13]. The security of the key distribution process described here relies on a few points: 1) A shared secrecy by users A and B on a starting key sequence $K_0$ and 2) a bit-by-bit uncertainty Nature-made noise associated to each bit and recorded on a interleaved M-ry non-orthogonal bases.

In short, knowledge of $K_0$ gives the legitimate users the first mapping of the bases generated by the emitter and allow B to recover each bit inscribed on every basis used. Sequences of fresh random bits, by its turn, will be generated by a truly random process and sent one-by-one between users A and B. Subsequent privacy amplification procedures statistically exclude the eventually compromised fraction of shared bits. The batch of secure shared secret bits (distilled bits) will be used for one-time-pad encryption. The physical noise from the bit generator protects each bit from the attacker E (Eve) and provides encryption. The physical noise from the bit generator will be used for one-time-pad procedures statistically exclude the eventually compromised fraction of shared bits. The batch of secure shared secret bits (distilled bits) will be used for one-time-pad encryption. The physical noise from the bit generator protects each bit from the attacker E (Eve) and provides the information security level associated with all $R_i$.

The signals associated to the key sequences $R_i$ are created by a physical random generator (PhRG). The noise $N_i$ associated with each bit $R_i$ inscribed onto the M-ry nonorthogonal basis ($M \geq 2$) produces the uncertainty seen by the attacker. This implies that the emitter has to be equipped to detect and record the signals generated by the PhRG. In other words, the definition of the measuring system is made by the emitter, not the attacker. The signal sent is the signal controlled and measured by the emitter with a detection system of his choice. No restrictions are placed on the attacker to obtain the exchanged signals on a public channel. Perfect copies of the transmission signals can be made public. Among the properties of the proposed system are: 1) Any public channel may be used for transmission (optical fibers, TV, microwave, and so on); 2) The deterministic signals can be amplified with no security loss; 3) Signals can be converted from electromagnetic to electrical and back to electromagnetic with no security loss; 4) Wavelength multiplexing is allowed on the network; 5) Current Network and IP protocols can be used with no modifications for users in any IP classes.

Fig. 1 shows a block diagram for one cycle of the key distribution system. Just to describe the protocol and make contact with some of the available literature ([11] to [13]) on M-ry cryptography, a description starting with a M-ry system of levels uniformly distributed on the phase circle will be presented. At the end, the M-ry system will be simplified to $M = 2$ for a speed-up in the communication process with no security loss.

**The protocol**

A and B share a starting random key sequence (#1) designated by $K_0$ (#2) of length $L$ (See Fig. 1). These $L$ bits are divided into blocks of size $k_M$ ($b(k_M), b(k_M-1), ..., b(1)$) and each block defines randomly a basis $k_0i$ over a nonorthogonal set of bases. As an example, a uniformly distributed set of bases can be used, being described on a ciphering wheel (#3) [11] with $M$ bases, where $M = 2^{k_M}$.

$$k_0i = b(k_M)2^{k_M-1} + b(k_M-1)2^{k_M-2} + ... + b(1)2^{0} \quad (1)$$

The phase values defining each basis are then given by

$$\phi_{k_0i} = \pi \left[ k_0i \left( \frac{1 - (-1)^{k_0i}}{2} \right) \right], \quad k_0i = 0, 1, ..., M - 1. \quad (2)$$

In these bases, a bit 1 will be inscribed displaced by $\pi$ with respect to bit 0 over each basis.

A PhRG (#5) generates random bits $R_{ii}$ (#6) that A would like to transfer securely to B. These signals contain noise $N_{ii}$ (#7) with a natural phase distribution (e.g., noise inherent to coherent states) of width $\sigma_\phi$. $R_{ii}$ can be understood in phase units (rd): values 0 or $\pi$ for bits 0 and 1. For mesoscopic coherent states this noise is approximatively Gaussian distributed with width $\sigma_\phi$ (set such that $\sigma_\phi < \pi/2$). The signal to be sent over the generic Internet communication channel (#8) (network and servers) is $Y_1 = R_{ii} + N_{ii}$. The combined effects of $N_{ii} + k_{0i}$ is to hide the bit value $R_{ii}$ on the ciphering wheel (#9). Although containing random information $Y_1$ is a deterministic signal and as such can be amplified and converted into different signals through arbitrary Internet nodes without any loss of security.

B has to extract $R_{ii}$ from $Y_1$. To this end he utilizes the same sequences from $K_0$ utilized by A to generate the base values $k_{0i}$ (#4). He subtracts this value from $Y_1$ and obtains $R_{ii} + N_{ii}$ (#10) and obtain signals in

![Fig. 1: A sketch of one cycle of operations of the key distribution process in the Noise Secured Internet is shown.](image-url)
**THE PHYSICAL RANDOM GENERATOR**

The random generator is the principal equipment needed to implement NSI for users A and B. After a brief description of a possible random generator, its physical aspects will be discussed. For secure transmission of signals physical randomness is necessary because no known mathematical algorithm has been proven to generate true random numbers. Several physical sources may be used to this end such as optical or thermal sources. Optical sources can be much faster than the thermal ones and are therefore necessary when speed is required. It is important to say that commercial truly random generators already exist for moderate speeds [3] what makes immediate NSI implementations possible. Fig. 2 shows a sketch of a PhRG with a coherent light source modulus. While several design variations are possible, the PhRG shown can achieve fast speeds compatible with optical channels. The laser beam is divided by a beam splitter BS. The upper part shows a detecting system where signals $V_i$ are generated corresponding to the sign of the generated signal with respect to the average signal intensity. The phase uncertainty is approximatelly given (see Refs. [11] and [12]) by the Gaussian distribution

$$p_\theta \approx e^{-(\Delta \phi)^2/2\sigma_\phi^2},$$

(3)

where $\sigma_\phi = \sqrt{2/(\langle n \rangle)}$ and $\langle n \rangle$ is the average number of photons in one bit. Availability of PhRG modules in public places like a cybercafe may be convenient and less costly for many users. They may generate and record on portable memories a batch of secure keys or use them to exchange one-time-pad ciphered information.

**SIMPLIFIED BASES**

Use of a non-uniform set of bases leads to a more economical system: instead of the uniformly spaced circle of phases given by Eq. (2) one may use just a sector of phase values where the number of bases is just $M = 2$. See Fig. 3. $\Delta \phi_1$ is the space between two bases and should be kept $\Delta \phi_1 \ll \pi/2$. $\langle n \rangle$ is adjusted so that $\pi/2 > \sigma_\phi \gg \Delta \phi_1$. Two states or bits can be inscribed on each basis (binary states), one should recall that the noise added and recorded on B’s binary basis is negligible because $\sigma_\phi < \pi/2$ and his decision on the bit value is easy; therefore, he obtains $R_{2i}$ (#6). From the received sequence $R_i$ he forms bit blocks of length $k_M$ and constructs a new base sequence $k_{2i}$. The next steps are similar to the first ones. Bob’s PhRG (#12) generates signal containing bits $R_{2i}$ (#13) associated to noise $N_{2i}$ (#14). The signal $Y_2 = R_{2i} + N_{2i} + k_{1i}$ is sent over the communication channel (#8). The bit value $R_{2i}$ is hidden by the overall noise $N_{2i} + k_{1i}$ (#15). From her knowledge of $R_{2i}$ (#6) and, therefore, $k_{1i}$ (#14), Alice subtracts $k_{1i}$ from $Y_2$ and obtains $R_{2i} + N_{2i}$ (#16). On her binary basis she easily obtains $R_{2i}$ (#13). The first cycle is complete. A and B continue to exchange random sequences as in the first cycle. The shared sequences $(R_{1i}, ..., R_{2i}, ...)$, after privacy amplification, are the random bits to be subsequently utilized for one-time-pad cipher.

Note that while for noiseless signals $Y_1 = b$ and $Y_2 = b$ carrying a repeated bit $b$, one has $Y_i \oplus Y_1 = 0$, noisy signals give $Y_1 = b + N_1$ and $Y_1 = b + N_2$ and, therefore, $Y_i \oplus Y_1 = N_1 + N_2 = 0$ or 1). This frustrates correlation attacks and algebraic attacks constituted of addition-mod2 between bits. These attacks are efficient against pseudo random encrypted signals in a noiseless carrier.
\[ \Delta \phi_i \] describes the possibilities is
\[ \frac{1}{4} \begin{pmatrix} 1 & \rho_{0,\phi_1} & \rho_{0,\pi} & \rho_{0,\pi+\Delta \phi_1} \\ \rho_{\pi,0} & 1 & \rho_{\pi,\phi_1} & \rho_{\pi,\phi_1+\Delta \phi_1} \\ \rho_{\pi+\Delta \phi_1,0} & \rho_{\pi+\Delta \phi_1,\phi_1} & 1 & \rho_{\pi+\Delta \phi_1,\pi} \\ \rho_{\pi+\Delta \phi_1,\pi+\Delta \phi_1} & 1 & \rho_{\pi+\Delta \phi_1,\pi+\Delta \phi_1} & 1 \end{pmatrix} \]
(7)

From now on the notation \( |\phi_i \rangle \) will be used for the modulated coherent states. As the interest is on small angular separation \( \Delta \phi_1 \), one may write the matrix elements of \( \hat{\rho} \) up to the first order \( O(\Delta \phi_1^2) \):

\[ \langle \phi_i | \rho | \phi_k \rangle = \frac{1}{4} \begin{pmatrix} 1 & \rho_{0,\phi_1} & \rho_{0,\pi} & \rho_{0,\pi+\Delta \phi_1} \\ \rho_{\pi,0} & 1 & \rho_{\pi,\phi_1} & \rho_{\pi,\phi_1+\Delta \phi_1} \\ \rho_{\pi+\Delta \phi_1,0} & \rho_{\pi+\Delta \phi_1,\phi_1} & 1 & \rho_{\pi+\Delta \phi_1,\pi} \\ \rho_{\pi+\Delta \phi_1,\pi+\Delta \phi_1} & 1 & \rho_{\pi+\Delta \phi_1,\pi+\Delta \phi_1} & 1 \end{pmatrix} \]

where

\[ \rho_{0,\Delta \phi_1} = \rho_{\pi,\pi+\Delta \phi_1} = (1 + i|\alpha|^2) \Delta \phi_1 \tanh(2|\alpha|^2), \]
\[ \rho_{\phi_1,0} = \rho_{\pi+\Delta \phi_1,\pi} = (1 - i|\alpha|^2) \Delta \phi_1 \tanh(2|\alpha|^2), \]
(8)

and all other terms \((i \neq k)\) are equal to \( \rho_{ik} = \text{sech}(2|\alpha|^2) \).

Diagonalization of \( \langle \phi_i | \rho | \phi_k \rangle \) and ortho-normal eigenstates \( |\Psi_i \rangle \) (up to order \( \Delta \phi_1 \)):

\[ \lambda_1 = 0, \]
\[ |\Psi_1 \rangle = \frac{1}{N} \left( e^{i \phi C} |0 \rangle - |\Delta \phi_1 \rangle - e^{i \phi C} |\pi \rangle + |\pi + \Delta \phi_1 \rangle \right), \]
(9)
\[ \lambda_2 = \text{sech}(2|\alpha|^2) \sinh^2(|\alpha|^2), \]
\[ |\Psi_2 \rangle = \frac{1}{N} \left( -e^{i \phi C} |0 \rangle - |\Delta \phi_1 \rangle + e^{i \phi C} |\pi \rangle + |\pi + \Delta \phi_1 \rangle \right), \]
(10)
\[ \lambda_3 = 0, \]
\[ |\Psi_3 \rangle = \frac{1}{N} \left( -e^{i \phi T} |0 \rangle + |\Delta \phi_1 \rangle - e^{i \phi T} |\pi \rangle + |\pi + \Delta \phi_1 \rangle \right), \]
(11)
\[ \lambda_4 = \frac{1}{2} \left( 1 + \text{sech}(2|\alpha|^2) \right), \]
\[ |\Psi_4 \rangle = \frac{1}{N} \left( e^{i \phi T} |0 \rangle + |\Delta \phi_1 \rangle + e^{i \phi T} |\pi \rangle + |\pi + \Delta \phi_1 \rangle \right), \]
(12)

where

\[ \lambda_2 + \lambda_4 = 1, \quad N = 2 \sqrt{2(1-e^{-n})}, \quad \phi_C = \arctan \left( \frac{1}{\Delta \phi_1 \coth(n)} \right) \right) \quad \text{and} \quad \phi_T = \arctan \left( \frac{n}{\Delta \phi_1 \tanh(n)} \right). \]

(13)
The eigenvalues give the probability of occurrence of the states \( |\Psi_i \rangle \). Due to the non-orthogonality of the bases used, a modulated state \( |\phi_i \rangle \) has projections on all eigenstates \( |\Psi_i \rangle \).

**Von Neumann and Shannon entropies**

Statistically, the Von Neumann entropy \( H(\alpha) \) associated with the random bits is given by the eigenvalues of \( \hat{\rho} \):

\[ H(\alpha) = -\lambda_2 \log_2 \lambda_2 - \lambda_4 \log_2 \lambda_4. \]
(14)
the definition of phase state will be adopted here. Thus, in terms of number state bases, distributions that have been frequently used. They will introduced simple definitions for phase state and phase cal states are established with less controversy. Ref. [14] versies –for a short review, see [8]. Mesoscopic and classi-
tum regime has been subject of intense study and contro-
mum Shannon entropy (as the classical limit of Von Neumann’s entropy) $H_S = 2 \times (1/2) \log_2(1/(1/2)) = 1$.

**Phase distribution**

The experimental determination of phase in the quantum regime has been subject of intense study and controverses –for a short review, see [8]. Mesoscopic and classical states are established with less controversy. Ref. [14] introduced simple definitions for phase state and phase distributions that have been frequently used. They will be adopted here. Thus, in terms of number state bases, the definition of phase state will be

$$|\phi\rangle = \frac{1}{\sqrt{q+1}} \sum_{n=0}^{q} e^{i n \phi} |n\rangle,$$  \hspace{1cm} (15)

where $q$ is the number of states taken on a truncated space of the oscillator Hilbert space [14]. It leads to a classical phase state for large $q$ and it is quite adequate for numerical calculations. Introduce a discrete, orthonormal and complete set of these states

$$\phi_{dm} = \frac{2\pi m}{q+1} \quad (m = 0, 1, ... q),$$   \hspace{1cm} (16)

defined up to an arbitrary fixed reference phase value (The index $d$ is just to identify the discrete character of this phase). Thus, $\langle \phi_{dk} | \phi_{dl} \rangle = \delta_{kl}$. A phase operator is defined by

$$\hat{\phi} = \sum_{m=0}^{q} \phi_{dm} |\phi_{dm}\rangle \langle \phi_{dm}|.$$ \hspace{1cm} (17)

Given a density operator $\hat{\rho}$, the phase distribution $p(\phi)$ is obtained as

$$p(\phi_{dm}) = \langle \phi_{dm} | \hat{\rho} | \phi_{dm} \rangle,$$ \hspace{1cm} (18)

with normalization $\sum_{m=0}^{q} p(\phi_{dm}) = 1$. From the density matrix, Eq. (6), the phase distribution (18) for all possible realizations of the phase assignments can be calculated. It gives

$$p(\phi_{dm}) = \frac{e^{-\langle n \rangle}}{4(q+1)} \sum_{\phi_i} \left[ \left( \sum_{n=0}^{q} \frac{|\alpha|^m}{\sqrt{n!}} \cos n(\phi_i - \phi_{dm}) \right)^2 + \left( \sum_{n=0}^{q} \frac{|\alpha|^m}{\sqrt{n!}} \sin n(\phi_i - \phi_{dm}) \right)^2 \right],$$ \hspace{1cm} (19)

where $\phi_i = (0, \Delta \phi_1, \pi, \pi + \Delta \phi_1)$ and $m$ is the phase index introduced in Eq. (16). Fig. 5 illustrates phase distributions for a set of $\Delta \phi_1$ and $\langle n \rangle = 25$. Large $\Delta \phi_1$ values imply that recognition for the attacker of the basis used by the user is easy and leads to bit recover. On the other hand, for small $\Delta \phi_1$ the linewidth well exceeds it.

A phase recorded by the sender is sent to the end user and assumed recorded by the attacker as well. Recovering the bit sent is the aim of both the end user and the attacker’s. To the end user, bit recovered is easy because it is just a decision between angle ranges ($-\pi/2, \pi/2$) or from ($\pi/2, 3\pi/2$). The attacker, not knowing the basis used, has to decide between a phase value or the neighbor phase, distant from it by $\Delta \phi_1$.  

---

**FIG. 4: Von Neumann entropy showing the fast transition from the quantum regime to the classical bit regime. $|\alpha| = \sqrt{\langle n \rangle}$, where $\langle n \rangle$ is the average number of photons per bit signal.**

**FIG. 5: Phase distribution for $\langle n \rangle = 25$ as a function of $\Delta \phi_1$ values. For large values of $\Delta \phi_1$ the decision over $\pi$ or $\pi + \Delta \phi_1$ is easily made. For small $\Delta \phi_1$ the two distributions merge together. $q = 300$ was used to truncate Eq. (19).**
Signal-to-noise ratio for phase measurements

A measure of the attackers ability to recover a phase \( \phi_i \) sent is given by the fundamental signal-to-noise ratio expressed by

\[
SNR_{\phi_i} = \frac{\langle \phi_i | \phi | \phi_i \rangle^2}{\langle \phi_i | \phi^2 | \phi_i \rangle - \langle \phi_i | \phi | \phi_i \rangle^2}.
\]  

(20)

The phase expected value \( \langle \hat{\phi} \rangle \) and \( \langle \hat{\phi}^2 \rangle \) are given by

\[
\langle \phi_i | \hat{\phi} | \phi_i \rangle = 4 \sum_{m=0}^{q} \phi_{dm} p(\phi_{dm})_{\phi_i},
\]  

(21)

and

\[
\langle \phi_i | \hat{\phi}^2 | \phi_i \rangle = 4 \sum_{m=0}^{q} \phi_{dm}^2 p(\phi_{dm})_{\phi_i}.
\]  

(22)

\( p(\phi_{dm})_{\phi_i} \) is the \( \phi_i \) contribution to \( p(\phi_{dm}) \). The attacker, \( E \), cannot succeed for \( SNR_{\phi_i} \leq 1 \). It should be emphasized that the attacker does not have the capability to perform measurements on the PhRG output. She obtains single records sent by the user. Not even an ensemble of data for each bit is sent by the user. A single recording of a single measurement performed by the user’s instruments is the only data available to the attacker. Fig. 6 shows the signal-to-noise ratio \( SNR_{\phi_i} \) for \( \langle n \rangle = 25 \) and \( \langle n \rangle = 400 \) as a function of \( \Delta \phi_1 \). It is seen that for a given \( \langle n \rangle \) a small range of \( \Delta \phi_1 \) values satisfy \( SNR_{\phi_i} \leq 1 \). Within this range, the attacker cannot succeed to obtain the correct bit values (or corresponding phase values). His probability of error by guessing over the recorded data will be 1/2.

ATTACKS

One may wonder about the cost of a brute force attack to determine the starting key \( K_0 \) from the transmitted signals. Under the assumption that the uncertainty presented to the attacker cover some of the bases, the attacker would know that the basis \( k_i \) used in a given transmission is around a given region within the uncertainty \( N_\sigma \).

For the \( M \)-ry system of uniformly spaced bases this amounts that only a set of less relevant bits \( b_k \) hide the correct basis. These \( b_k \) bits could be permuted in \( b_k! \) ways. As each bit could be either 0 or 1 the total number of permutations to be searched for each bit emission would be \( (\log_2 N_\sigma)!N_\sigma \). For the total number of bits the number of combinations would be

\[
C = 2^{K_0} (\log_2 N_\sigma)!N_\sigma.
\]  

(23)

Under this example of a uniform ciphering wheel exemplified by Eq. (2), it is understood that the attacker may know the fraction \( 1 - (N_\sigma/M) \) of the total number of shared bits \( k_M \) used by A and B to cipher a fresh generated bit. For a sequence of \( L \) shared bits, Eve may obtain \( L/[1 - (N_\sigma/M)] \) bits among \( L \) because they were not covered by noise. An attack on the key cannot succeed due to simple reasons: \( K_0 \) can be chosen with a size that makes direct search computationally unfeasible (exponential complexity in \( K_0 \)). After exchange of each random sequence \( R_i \) equally long as \( K_0 \) privacy amplification procedures will be applied, leading to a shorter random sequence for one-time-pad. One should stress in this key distribution procedure the starting key \( K_0 \) is never to be open to the attacker. This eliminates any possibility for \( E \) to explore correlations between \( K_0 \) and the distilled keys after privacy amplification. In fact, \( K_0 \) can be destroyed after being used. Therefore, applying key-search trials for ciphertext decryption on a known-plaintext attack is doomed due the attacker’s computational capability.

For the \( M = 2 \) system all neighbouring levels are covered by noise \( (N_\sigma \geq 2) \). For this case, the same \( C \sim 2^{K_0} \) makes unfeasible a brute force attack.

CONCLUSIONS

It has been shown that Internet users will succeed in generating and sharing, in a fast way, a large number of secret keys to be used in one-time-pad encryption. They have to start from a shared secret sequence of random bits and have a “hardware” modulus (Physical Random Generator-PhRG) added to their computers. The physical noise level is adjusted to hide the random bits being sent. Although the transmitted signals could be openly accessed, physical noise inherent to these signals provide the protection. No intrusion detection method is necessary. Privacy amplification protocols (dependent on the \( M \)-ry system used) eliminate any fraction of information that may have eventually obtained by the attackers. As the security is not based on protocols
supported by mathematical complexities in current use, the security is not dependent on the difficulties of factoring large numbers in their primes. It was then shown that by sharing secure secret key sequences and subsequent data encryption a secure Internet can be practically implemented. The system can be easily adjusted to follow any computational advance while providing security. The random generator works at optical speeds and the system does not require special Internet communication protocols. Any network in current use is adequate for this kind of operation. This system is proposed as a possible new paradigm for a secure Internet.

*E-mail: GeraldoABarbosa@hotmail.com

[1] For definition, see http://en.wikipedia.org/wiki/Internet_Protocol.
[2] For definition, see http://en.wikipedia.org/wiki/OSI_model.
[3] id Quantique offers an optical random number generator based on reflection/transmission of single photons. See http://www.idquantique.com/products/quantis.htm
[4] C. Bennett, G. Brassard, Quantum cryptography, Public key distribution and coin tossing, in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India, 1984, pp. 175 to 179.
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).
[6] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, JM Merolla and L. Larger, Physics Letters A, In Press, online 17 April 2006.
[7] R. J. Glauber, Phys. Rev. 130, 2766 (1963); Phys. Rev. 131, 2766 (1963); Quantum Optics and Electronics, eds. C. DeWitt, A. Blandin, C. Cohen-Tannoudji (Dunod, Paris 1964), Proc. École d’Été de Physique Théorique de Les Houches, 1964.
[8] L. Mandel and E. Wolf, Optical Coherence and Quantum Optics (Cambridge University Press, 1995), Section 10.7. See also D. T. Pegg, S. M. Barnett, R. Zambrini, S. Franke-Arnold, and M. Padgett, New J. of Phys. 7, 82 (2005).
[9] G. A. Barbosa, E. Corndorf, P. Kumar, H. P. Yuen, Phys. Rev. Lett. 90, 227901 (2003).
[10] E. Corndorf, G. A. Barbosa, C. Liang, H. P. Yuen, P. Kumar, Opt. Lett. 28, 2040 (2003). G. A. Barbosa, E. Corndorf, and P. Kumar, Quantum Electronics and Laser Science Conference, OSA Technical Digest 74, 189 (2002).
[11] G. A. Barbosa, Phys. Rev. A 68, 052307 (2003). US Pat. Appl. 11/000,662, Publ. No. US2005/0152540 A1. See also quant-ph/0212033 2002 v4 28 Apr 2004 pp. 1 to 10.
[12] G. A. Barbosa, Phys. Rev. A 71, 062333 (2005).
[13] H. P. Yuen, R. Nair, E. Corndorf, G. S. Kanter, and P. Kumar, quant-ph/0509091 v1 13 Sep 2005.
[14] D. T. Pegg and S. M. Barnett, Europhys. Lett. 6, 483 (1988).