A wireless physically secure key distribution system

Geraldo A. Barbosa*

***Abstract*—A secure key distribution protocol protected by light's noise was introduced in 2003 [Phys. Rev. A 68, 052307 (2003)]. That protocol utilized the shot noise of light present in the optical channel (eg., an optical fiber) to restrict information leaks to an adversary. An initial shared information between the legitimate users allowed them to extract more information from the channel than the one obtained by the adversary. That original paper recognized the need for a privacy amplification step but no specific protocol was presented. More recently that original idea was improved with a specific privacy amplification protocol [arXiv:1406.1543v2 [cs.CR] 8 Jul 2015] while keeping the use of an optical communication channel. This work merges main ideas of the protection given by the light's noise in a protocol applied to wireless channels. The use of a wireless channels together with recorded physical noise was introduced from 2005 to 2007 (see eg, arXiv:quant-ph/0510011 v2 16 Nov 2005 and arXiv:0705.2243v2 [quant-ph] 17 May 2007). This work improves those embrionary ideas of wireless channels secured by recorded optical noise. The need for specific optical channels is eliminated with the wireless variation and opens up the possibility to apply the technique to mobile devices. This work introduces this new scheme and calculates the associated security level.**

***Index Terms*—Random, physical processes, cryptography, privacy amplification.**

I. Introduction

A fast and secure key distribution system is presented to operate in generic communication channels, including wireless channels. The transmitted signals are deterministic but include continuously recorded random noise that frustrates an attacker to obtain useful information. This noise affects the attacker but not the legitimate users that share an initial shared secret bit sequence c_0. The legitimate users will end up with a continuous supply of fresh keys that can be used even to encrypt information bit-to-bit in large volumes and fast rates.

The wireless key distribution system discussed in this work uses the intrinsic light noise of a laser beam to frustrate an attacker to extract meaningful signals. However, this noise is not in the communication channel (as in Ref. [1]) but it is recorded *before* reaching the communication channel.

A step-by-step description of this system will be made but is not intended to be seen as the ultimate design but just as a possible implementation of the involved ideas. Three main parts constitute the system's core: 1) A fast Physical Random Bit Generator (PhRBG) of the type described in Ref. [2]. The PhRBG extract fluctuations (shot-noise) of a laser light beam and delivers random voltage signals (V_+, V_-) –signals that can be expressed as bits– to a "bit pool". 2) A second extraction of optical fluctuations generating fluctuating voltage signals to be added to the emitted signal bits. This noise contribution replaces the intrinsic optic noise in an optical channel. 3) A Privacy Amplification Protocol (PA) as already described in Ref. [3].

These parts will be discussed in the next sections.

*G. A. Barbosa, QuantaSec – Consulting and Projects in Physical Cryptography Ltd., Av. Portugal 1558, Belo Horizonte MG 31550-000 Brazil. E-mail: GeraldoABarbosa@gmail.com

Just for short the name KeyBITS will be applied to the discussed system that generates and distribute cryptographic keys and may as well provide functions like encryption and decyption.

II. Physical Random Bit Generator, $M-$ry bases and added noise

A. PhRBG

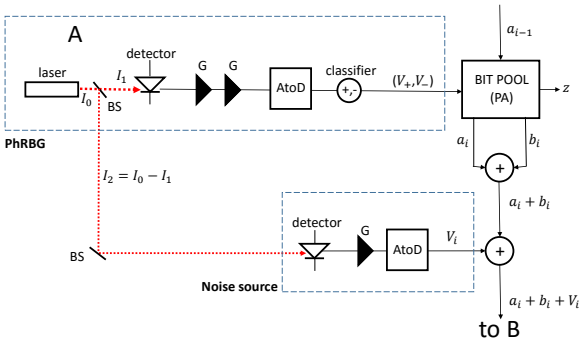

Fig. 1

Hardware to generate random bits (PhRBG), noise source and bit pool for Privacy Amplification. The bit pool contain memories and a FPGA (Field Programmable Gate Array) to perform fast operations locally.

Left upper part of Fig. 1 shows the PhRBG. A laser beam excites a multi-photon detector and the voltage output pass through amplifiers G and an analog-to-digital (ADC) converter. The laser intensity I_1 and the gain G are adjusted to enhance the optical signals well above all electronic noises but below the region where the Poissonian fluctuations are relatively small compared to the average laser signals. In other words, the desired signals are optimized optical shot-noise signals. The stream of digitalized fluctuating signals are classified within short time intervals in signals above the average value as bit 1 signals (V_+) while signals below the average are identified as bit 0 signals (V_-). These individual bit signals generated by the PhRBG arount time instants t_i will be designated by a_i and a sequence of a_i by a. Notation a sometimes designates a sequence of bits or the size of this sequence, whenever this does no give rise to notational problems.

User A wants to transmit in a secure way these random a bits to user B.

Fig. 1 also shows that signals b_i are added to a_i. The initial sequence $\{b_i\}$ is taken from an initial secret sequence c_0 of size $c_0 = ma$ shared by the legitimate users (to be discussed ahead).

Bottom part of Fig. 1 shows that a laser beam with intensity I_2 is detected, amplified and digitalized producing a sequence

of noise signals $V_N = \{V_i\}$, that is added to the signals $a_i + b_i$ and sent to B.

B. $M-ry$ bases

In order to send each a_i a modulation signal b_i defined by m random bits from c_0 is added: $a_i + b_i \equiv n_i$. The modulating random signal b_i can be seen as a transmission *basis* for a_i. One may as well see bits a_i as a message and b_i as an encrypting signal. To generate each b_i, one number among M, m bits are necessary ($m = \log_2 M$).

It is crucial to be understood that the $M-$ry coding interleaves bits in the sense that the same bit signal superposed to a basis b_k representing a bit 1 (or 0) represents the opposite bit 0 (or 1) in a neighbor basis b_{k-1} or b_{k+1}. This, together with the added noise V_N do not allow the attacker to obtain the bit a_i. Signals $a_i + b_i$ will be sent from user A to B after recorded noise signals have been added.

C. Added noise

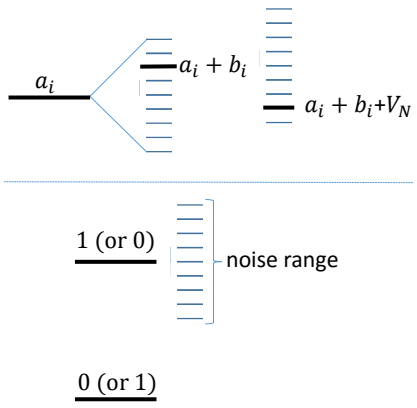

Fig. 2

TOP - THE SIGNAL REPRESENTING A GIVEN BASIS b_i IS ADDED TO THE SIGNAL REPRESENTING A BIT a_i. THE BASIS SIGNAL IS KNOWN TO USERS A AND B BUT NOT TO THE ATTACKER. A SIGNAL a_i IS TO BE SEEN AS A GIVEN BIT IN BASIS b_i (1 OR 0) BUT THIS SAME SIGNAL a_i WILL BE SEEN AS THE OPPOSITE BIT (0 OR 1) WHEN ATTACHED TO NEIGHBORING BASES b_{i+1} OR b_{i-1}. THEREFORE EVEN A SMALL NOISE V_i ADDED TO $a_i + b_i$ DO NOT ALLOW AN ATTACKER TO KNOW WHICH BASES HAVE BEEN USED. HOWEVER, BOTH A AND B KNOW b_i AND THUS THE BIT SENT a_i CAN BE EXTRACTED. BOTTOM - THE DISTANCE BETWEEN A SIGNAL a_i REPRESENTING A BIT AND THE OPPOSITE ONE IS GREATER THAN THE NOISE SPREAD. THIS ALLOWS A PRECISE BIT DETERMINATION BY THE LEGITIMATE USERS.

Besides the encrypting signals b_i a random signal V_i is added to $a_i + b_i$, giving $a_i + b_i + V_i$, before sending the deterministic signal to B. It is to be understood that although the signal sent from A to B is deterministic, V_i is a *recorded random noise*. A recorded signal is deterministic by definition because it can be perfectly copied. However, the recorded noise is an instance of an unpredictable event by nature. In Nature the noise intensity is continuous but the recorded digitalized noise is distributed among the M levels supplied by the ADC. This statistical distribution among M levels also has a characteristic deviation σ_V. This will be discussed ahead.

The noise signal V_i is derived from a split beam of intensity I_2 (see left bottom part of Fig. 1). Light from this derived beam excites a multi-photon detector, its output is amplified by G and digitalized. An extra amplifier G may be adjusted to levels compatible to the signal $a_i + b_i$. In other words, the added noise should be able to mix potential bases and bits so that the attacker could not identify either the bit or the basis sent. Fig. 2 sketches the addition of the random basis b_i and the added noise V_i. The attacker does not know either the basis b_i neither the noise V_i and, therefore, cannot deduce the bit sent a_i from the total signal $a_i + b_i + V_i$.

III. PRIVACY AMPLIFICATION AND FRESH BIT GENERATION BY A AND B

The Privacy Amplification process to be utilized is identical to the one shown in Section IX of Ref. [3]. Very briefly, the PA utilized is an application of formalism developed in Ref. ([4]).

Operationally the following steps are performed:

1) The bit pool starts with the bit sequence of size $c_0 = ms$ (bits b_i) already shared by A and B. A sequence of a bits a_i is generated by the PhRBG and stored in the bit pool by user A. The sequence a is sent from A to B after the preparation that adds bases and noise. A number of bits $a + ma$, for $\{a_i + b_i\}$, is used fo this task.

2) An instance of a universal hash function f is sent from A to B.

3) The probability for information leakage of bits sent obtained by the attacker over the sequence sent is calculated, generating the parameter t (number of possibly leaked bits). In other words, from sequence $\{0,1\}^n$ the attacker may capture $\{0,1\}^t$.

The PA protocol that uses f includes the following steps. From the $n = a + b$ bits stored in the bit pool, t bits of them are destroyed:

$$\{0,1\}^n \rightarrow \{0,1\}^{n-t}\,. \tag{1}$$

An extra number of bits λ is reduced as a security parameter [4], so that

$$\{0,1\}^n \rightarrow \{0,1\}^{n-t} \rightarrow \{0,1\}^{n-t-\lambda}\,. \tag{2}$$

The initial total amount of bits n in the bit pool is then reduced to $r = n - t - \lambda$. These bits are randomized by the PA protocol.

The PA protocols establish that the attacker has no information on these reduced and "shuffled" number of bits r.

r can be rearranged in sizes as follows

$$\begin{aligned} r &= n - t - \lambda = (a+b) - t - \lambda = (a - t - \lambda) + b \\ &= (a - t - \lambda) + ma\,. \end{aligned} \tag{3}$$

The sequence of size $z \equiv (a - t - \lambda)$ will be used as fresh bits for encryption while the sequence of size ma will form the new bases for the next round of bit distribution. The process can proceed without the legitimate users having to meet to refresh an initial sequence ma. Other rounds then may proceed.

The PA theory [4] says that after these operations, that reduces the initial number of bits from $n = a + ma$ (ma initially

shared and a fresh bits) to $r = n - t - \lambda$, the amount of information that may be acquired by the attacker is given by the *mutual information* I. Corollary 5 (pg. 1920) in Ref. [4], gives the information leaked to the attacker:

$$I_\lambda = \frac{1}{\ln 2 \times 2^\lambda} = \frac{1}{\ln 2 \times 2^{n-t-r}} \,. \tag{4}$$

IV. Leakage probability

Calculation of the mutual information I that is directly connected to the probability for an attacker to extract the correct information sent from A to B depends on the parameter t (number of possibly leaked bits in a sequence sent).

In the wireless scheme the number of levels used as bases depends on the Digital-to-Analog Converter (DAC) utilized (8 bits resolution$\rightarrow M = 256$, 10 bits$\rightarrow M = 1024$ and so on). This converter sets the maximum number of levels M. Voltage signals $V_k\,, (k = 0, 1, 2 \ldots M)$ will represent these bases and to alternate bits in nearby bases they may be chosen as

$$V_k = V_{\max} \left[\frac{k}{M} + \frac{1 - (-1)^k}{2} \right] . \tag{5}$$

At the same time, as voltage signals V_N representing recorded optical noise will be added to these values, these values should have a span smaller than $V_{\max}$ but large enough to cover some number of bases so that the attacker cannot resolve the basis b_i being used at the time a bit a_i is sent. The actual optical noise has a continuous span but the recorded region is set by digitalized levels of the ADC used. For example, setting the spacing of signals for bases similar to the spacing $V_{\max}/M$ of recorded noise levels, one could set the digitalized noise deviation, by adjusting G, such that

$$V_{\max}/M \ll \sigma_V \ll V_{\max} \,. \tag{6}$$

This condition can be mapped in the same formalism utilized in the POVM (Positive Operator Valued Measure) calculation developed in [1] and from which the leakage bit probability t can be obtained. This mapping would allow us to write the probability for indistinguishability between two levels separated by Δk, as

$$P_{\Delta k} = e^{-\frac{|\alpha|^2}{4}\left(\frac{V_{\Delta k}}{V_{\max}}\right)^2} = e^{-\frac{|\alpha|^2}{4}\frac{(\Delta k)^2}{M^2}} \equiv e^{-\frac{\Delta k^2}{2(\sigma_k)^2}} \,. \tag{7}$$

The expected deviation σ_k in the number of levels is

$$\sigma_k = \sqrt{\frac{2}{\langle n \rangle}} M \tag{8}$$

where $\langle n \rangle = |\alpha|^2$ and α is the coherent amplitude of a laser.

Calculation of the probability of error P_e for an attacker to obtain a bit sent is similar to what was done in [1]. Fig. 3 exemplifies these errors for a set of M values (number of bases) and number $\langle n \rangle$ of photons detected. For a sequence of s bits sent the parameter t (bit information leaked in s) in Eq. 4 will be $t = (0.5 - P_e) \times s$. With t calculated and the safety parameter r defined the information that could be leaked to the attacker is calculated. It can be shown [1] that $0.5 - P_e \sim 10^{-4}$ can be easily obtained. With a sequence os $s = 10^6$ bits sent, this gives $t \sim 10^2$. Fig. 4 exemplifies the PA effect (I_λ) as a function of r, $(0,1)^n \rightarrow (0,1)^r$, and t, number of bits leaked to the attacker.

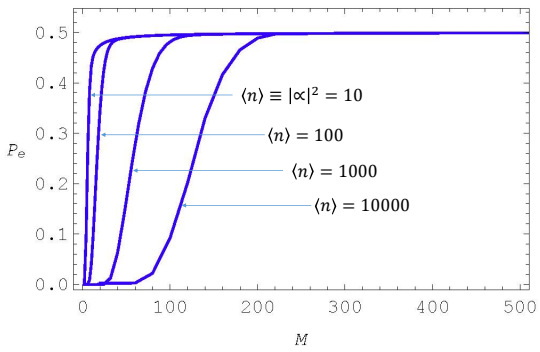

Fig. 3
Probability of error for an attacker on a bit as a function of the number M of bases used and the average number of photons $\langle n \rangle$ carrying a bit.

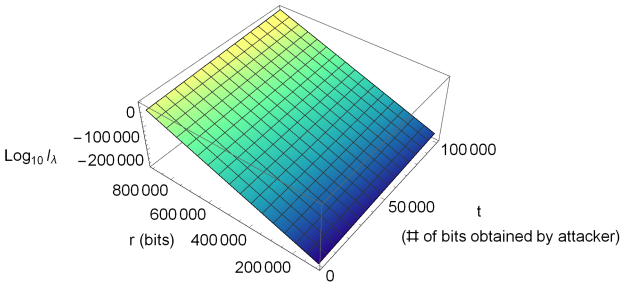

Fig. 4
$\log_{10}$ of the Information leaked to the attacker after Privacy amplification is applied. In this example 10^6 bits are sent. t gives the number of bits leaked to the attacker before PA is applied.

V. Mobile device applications

The discussed steps describe the basic parts of the KeyBITS Platform for secure communications.

The described bit generator system has been tested in laboratory benches and performed with sucess above 1GHz, passing all randomness tests to which it was submitted, including the NIST set (NIST's Special Publication 800 - A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications). Coupling to a FPGA (Field Programmable Gated Array) and memory has allowed functions like bit storage and encryption and can be easily adapted to perform the "bit pool" functions discussed in this work. The bench setup can be with a somewhat modest effort reduced to a small size with output directly coupled to a smart phone. This can provide true secure communications (bit-to-bit encryption) between users. Both Secure Data and Voice Over Internet (VOIP) can be implemented. It should be emphasized that it is impor-

tant that the key storage should be kept "outside" of the mobile device and that the flow of information between the key generation and encrypting unit should be strictly controlled, in a "diode"-like flow configuration.

Furthermore, another step, more costly, can produce an ASIC (Application Specific Integrated Circuit) to reduce the system to a pulse size (watch) device.

Another straightforward application is using KeyBITS to feed a Software-Defined-Radio (SDR) with cryptographic keys for bit-by-bit encryption/decryption capabilities. This will give absolute security for Data and Voice communications through SDR.

VI. Conclusions

It was shown how to achieve wireless secure communication at fast speeds with bit-to-bit symmetric encryption. Both the hardware requirements was described and it was shown how to calculate the security level associated to the communication. This clears the path to miniaturization steps that may allow easy coupling to mobile devices. Similarly, SDR applications present no fundamental obstacles to prevent integration with the KeyBITS Plataform. The key storage will be under control of the legitimate users and no key will ever be stored where a hacker could have command/control of the system.

References

[1] G. A. Barbosa, Physical Review A **68**, 052307 (2003).
[2] G. A. Barbosa, Enigma - Brazilian Journal of Information Security and Cryptography, Vol. **1**, 47 (2014).
[3] G. A. Barbosa and J. van de Graaf, arXiv:1406.1543v2 [cs.CR] 8 July 2015. Accepted to Enigma - Brazilian Journal of Information Security and Cryptography 2015.
[4] C. H. Bennett, G. Brassard, C. Crepeau, U. M. Maurer, IEEE Transactions on Information Theory **41**, 1915 (1995)