True Random Number Generation with Beam Splitters under Combined Input Scenarios using Defined Quantum States to Increase the Security of Cryptographic Devices

Martin Suda
Austrian Institute of Technology (AIT)
Vienna, Austria
Email: martin.suda@ait.ac.at

Gerald Dißauer
Secure Information Technology Center Austria (A-SIT)
Vienna, Austria
Email: gerald.dissauer@a-sit.at

Florian Prawits
Austrian Institute of Technology (AIT)
Vienna, Austria
Email: florian.prawits@ait.ac.at

***Abstract*—Cryptographic devices, e.g., Hardware Security Modules (HSMs) are crucial to the trustworthiness of computer applications that provide critical services such as digital signature systems. Random numbers are used to strengthen the security of HSMs. Due to the problem of deterministic and thus predictable random sources and the complexity to derive true coincidence with computer systems, quantum mechanical effects can be exploited to derive perfect randomness. In this paper, we present an approach to increase the security of HSMs by using 50:50 splitters under combined input scenarios to derive true random numbers based on quantum mechanics.**

Keywords–Beam Splitter; Cryptography; Quantum Mechanics; Quantum Random Number Generation; Quantum States; Hardware Security Module; HSM; True Randomness.

I. INTRODUCTION

1) Motivation: According to our conducted research in quantum optics, the generation of quantum random numbers with Beam Splitters (BS) relying on the physical effects of light quanta is particularly underdeveloped in terms of practical applications. Such practical applications include the computation of random numbers for cryptographic protocols and Hardware Security Modules (HSMs) [1]. HSMs that rely on cryptographic protocols to engineer secure systems [2] can be used to derive cryptographic key material and store private data or master keys [3] in protected hardware devices, e.g., PCI (Peripheral Component Interconnect) devices that are optimized for cryptographic operations [4]. Therefore, such cryptographic devices are integrated into complex practical applications, e.g., to create qualified electronic signatures [5] which means that electronic documents are signed digitally. Such documents are legally valid, for instance. Other industrial applications are implemented in data centers [3] and particularly in the banking sector [1] (e.g., for mobile payment solutions) where the key management for database encryption solutions [6] are installed.

2) Problem statement: HSMs for the above mentioned industrial applications are often certified against either (1) FIPS (Federal Information Processing Standard) 140-2 [7] (newer Version: FIPS 140-3 [8]) or (2) Common Criteria [9]–[11], e.g., EAL4+ (Evaluation Assurance Level) [11] which was also codified in the ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) 15408 standard [12]–[14]. Such certifications of software-intensive products are used to validate the realized security functions (e.g., SFR - Security Functional Requirements of the Common Criteria) [10] and moreover to assure (SAR - Security Assurance Requirements of the Common Criteria) [11] the compliance of the selected product against the claimed security functions. That means that a particular minimum-level of security (e.g., EAL4+) for those integrated devices is assured.

Such certifications often require Deterministic Random Bit Generators (DRBGs) in accordance with NIST (National Institute of Standards and Technology) SP (Special Publication) 800-90A [15] or alternatively demand pseudo-random data (seed) as inputs to obtain random numbers. Feasible sources to derive seeds are the 1) system clock [10], 2) system registers [10], 3) date [10], 4) time [10], or 5) external events [15] but the aforementioned computational sources do not provide true randomness [16], unfortunately.

However, the use of true sources of randomness (i.e., True Random Number Generators - TRNGs) are increasingly required to seed deterministic random number generators and thus to increase the entropy [7][15]. Alternatively, physical sources can be used to obtain real random numbers (e.g., deriving it from noise) rather than by means of deterministic algorithms. As a result, developers must demonstrate that their used entropy sources provide a sufficient level of randomness.

Industrially relevant examples of such practical applications include 1) to increase the security of cryptographic protocols, or 2) to strengthen the device-internal cryptographic materialmanagement (e.g., for FIPS 140-2 or FIPS 140-3) of HSMs under real circumstances. Such HSMs derive random numbers from predictable algorithms and therefore those obtained random numbers do not rely on real coincidence.

In contrast, quantum random numbers are obtained from the fundamental principles of quantum mechanics which means that such random numbers are derived from the perfect randomness of quantum mechanical effects [17]. Therefore, such random number generators produce random data that are unpredictable. Quantum random number generators have been recently tested for 71-day non-stop long-term applications [18].

3) Our proposed solution: To overcome the limitations of imperfect random numbers in terms of cryptographic devices, we propose a solution to generate quantum mechanical random numbers that are derived from several input configurations under defined scenarios for 50:50 Beam Splitters. In order to assess reasonable input configurations to obtain practically

 ISBN: 978-1-61208-749-8

applicable random data outputs, we consider the following input configurations ($\hat{a}_0$ and $\hat{a}_1$, Figure 1) for our BS:

- $|0\rangle$ and $|1\rangle$ (quantum vacuum state on $\hat{a}_0$ and single-photon on $\hat{a}_1$)
- $|1\rangle$ and $|1\rangle$
- $|0\rangle$ and $|\alpha\rangle$ (coherent state on $\hat{a}_1$)
- $|\alpha\rangle$ and $|\beta\rangle$ (two Weak Coherent States - WCS)
- $|0\rangle$ and $(|0\rangle + |1\rangle)$ (superposition on $\hat{a}_1$)
- $(|0\rangle + |1\rangle)$ and $|1\rangle$
- $|1\rangle$ and $|\alpha\rangle$
- $\frac{1}{N}(|\alpha\rangle|\beta\rangle + |\beta\rangle|\alpha\rangle)$ (Entangled Coherent State - ECS)
- $|\beta\rangle$ and $\frac{1}{N}(|\beta\rangle + |-\beta\rangle)$ (Coherent Superposition State - CSS)

We, therefore, get random outputs behind the BS under the above mentioned defined input scenarios.

4) The benefit: Quantum random number generators [16], which derive real randomness with BS under defined input scenarios, can be used as physical sources to obtain perfect random numbers. As a result, it is possible to increase the security of HSMs and particularly the randomness of the key material inside of the HSM or of cryptographic protocols. That means that we are able to overcome the limitations of predictable random sources for current solutions because the underlying randomness is based on the intrinsic effects of true randomness derived from quantum mechanics.

This paper is organized as follows. After the introduction in Section I (see above), we discuss the BS (cf., II-A) and present 9 examples (cf., II-B) for the aforementioned input and related output states in Section II. Section III concludes our paper.

II. BS AND EXAMPLES

A. Beam Splitter

Below, we describe the Beam Splitter - a semi-permeable mirror - quantum mechanically. To obtain true randomness, we choose a semi-permeable BS where the incident light is transmitted with a 50% probability and thus 50% of the incident light is reflected (denoted by 50:50). Alternatively, one can choose arbitrary configurations of the BS. However, only the 50:50 configuration derives true randomness [19]. Such a device is constructed so that it has 2 input modes ($\hat{a}_0$, $\hat{a}_1$) and 2 output modes ($\hat{a}_2$, $\hat{a}_3$) (Figure 1).

The quantum mechanics of BS can be found in [20]–[24]. The most important relation is given by Heisenberg's uncertainty relation:

$$[\hat{a}_i, \hat{a}_j^+] = \delta_{ij} \ , \ \hat{a}^+\hat{a} = \hat{n} \ , \ \hat{a}\hat{a}^+ = 1 + \hat{n} \ . \qquad (1)$$

$\hat{a}^+$ is the creation operator and $\hat{a}$ the annihilation operator for photons. $\hat{n}$ is called particle operator. The matrix equation for a BS can be written as

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix} = \hat{T} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}. \qquad (2)$$

$\hat{T}$ is a unitary matrix where $\hat{T}\hat{T}^+ = \mathbb{1}$ holds. For a $50:50$ BS the following relations can be deduced (we choose, e.g., phase $i = \exp(i\pi/2)$ for reflection: $\hat{a}_2 = t\hat{a}_0 + r\hat{a}_1$ and $\hat{a}_3 = r\hat{a}_0 + t\hat{a}_1$):

$$\begin{aligned} \hat{a}_2^+ &= \tfrac{1}{\sqrt{2}}(\hat{a}_0^+ - i\hat{a}_1^+) \, , \, \hat{a}_3^+ = \frac{1}{\sqrt{2}}(-i\hat{a}_0^+ + \hat{a}_1^+) \rightarrow \\ \hat{a}_0^+ &= \tfrac{1}{\sqrt{2}}(\hat{a}_2^+ + i\hat{a}_3^+) \, , \, \hat{a}_1^+ = \frac{1}{\sqrt{2}}(i\hat{a}_2^+ + \hat{a}_3^+) \ . \end{aligned} \qquad (3)$$

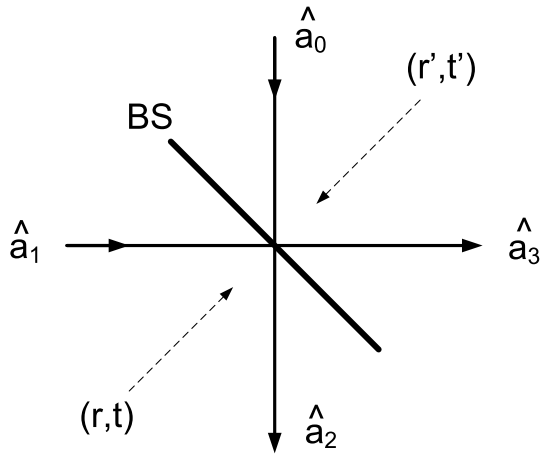

Figure 1. BS: Quantum mechanical description, r and t are reflection and transmission coefficients, respectively; see text. In principle r and t can be different for the front and back of the BS.

The examples below are given in order to demonstrate the mode of operation of a BS with genuine quantum input states and output states which are appropriate for Quantum Random Numbers (QRN) [16]. Such output states have the following structure: $(|n\rangle_2|0\rangle_3 + |0\rangle_2|n\rangle_3)$ or $(|\alpha\rangle_2|0\rangle_3 + |0\rangle_2|\alpha\rangle_3)$ where $|n\rangle$ are Fock states and $|\alpha\rangle$ are coherent states which are each entangled to the vacuum $|0\rangle$. Hence, coincidences must not appear in the output modes.

B. Examples

1) One Photon in input 1: $|0\rangle_0|1\rangle_1$*:* Now, in this first example the input state is $|0\rangle_0|1\rangle_1 = \hat{a}_1^+|0\rangle_0|0\rangle_1$. We recall that in quantum optics (e.g., [20]) a photon can be created from vacuum by means of the creation operator: $\hat{a}^+|0\rangle = |1\rangle$. Generally, for n photons, $\hat{a}^+|n\rangle = \sqrt{n+1}|n+1\rangle$ and $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$ holds. $|n\rangle$ are the Fock states of light.

Experimentally, a single photon state (denoted by $|1\rangle$) can be generated by Parametric Down-Conversion (PDC) using non-linear crystals. That means that two photons are created simultaneously, where one of those photons is used for the BS-experiment. The other one is registered in terms of synchronization purposes of the created photon pair. It is important to note that the process of PDC occurs with low probability s.t. random numbers generated by this means will show low yield [20]–[24]. To overcome this limitation, weak coherent states are able to be used for the generation of approximately single photon states (cf., case 2 below).

Using (3), one gets behind the BS:

$$\begin{aligned} |0\rangle_0|1\rangle_1 \ \rightarrow^{BS}\rightarrow \ & \frac{1}{\sqrt{2}}(i\hat{a}_2^+ + \hat{a}_3^+)|0\rangle_2|0\rangle_3 = \\ = \ & \frac{1}{\sqrt{2}}(i|1\rangle_2|0\rangle_3 + |0\rangle_2|1\rangle_3) \ . \end{aligned} \qquad (4)$$

This is an important result of a balanced BS. It means that a single input photon in mode 1 together with a vacuum input in mode 0 is equally transmitted and reflected with probability $\frac{1}{2}$. An important method of generating quantum random numbers [16] relies on this method. This result is exactly what is expected. It explains also that there are no coincidences. If one measures the photon in output port $2(3)$

no photon is measured in output $3(2)$. One can say as well that the photon is entangled with the vacuum behind the BS. Conversely one can say: If there are in fact no coincidences, then we have a genuine single photon source. Obviously, the BS is a "passive" element which neither creates nor annihilates photons.

The density operator $\hat{\rho}_{23}$ of the output states behind the BS is:

$$\begin{aligned}\hat{\rho}_{23} &= \frac{1}{2}(i|1\rangle_2|0\rangle_3 + |0\rangle_2|1\rangle_3)(-i\,{}_2\langle 1|\,{}_3\langle 0| + {}_2\langle 0|\,{}_3\langle 1|) = \\ &= \frac{1}{2}\{|1\rangle_2|0\rangle_3\;{}_2\langle 1|\,{}_3\langle 0| + |0\rangle_2|1\rangle_3\;{}_2\langle 0|\,{}_3\langle 1| + \\ &+ i|1\rangle_2|0\rangle_3\;{}_2\langle 0|\,{}_3\langle 1| - i|0\rangle_2|1\rangle_3\;{}_2\langle 1|\,{}_3\langle 0|\}\,. \end{aligned} \quad (5)$$

This density operator contains the full information of coherence. It includes all off-diagonal elements. If only one output is measured (e.g., output 2) one has to apply the partial trace over output 3:

$$\begin{aligned}\hat{\rho}_2 = Tr_3\hat{\rho}_{23} &= \sum_{n=0}^{\infty} {}_3\langle n|\hat{\rho}_{23}|n\rangle_3 = \\ &= \frac{1}{2}(|0\rangle_2\,{}_2\langle 0| + |1\rangle_2\,{}_2\langle 1|) \end{aligned} \quad (6)$$

and analog $\hat{\rho}_3 = \frac{1}{2}(|0\rangle_3\,{}_3\langle 0| + |1\rangle_3\,{}_3\langle 1|)$. Equation (6) describes a statistical mixture. After performing the measurement, no off-diagonal terms exist, which would imply coherence. The output states appear with 50% probability each and there are no coincidences. Measuring the particle number for output 2, one keeps the following result: $\bar{n}_2 = Tr_2(\hat{\rho}_2\hat{n}_2) = \frac{1}{2}({}_2\langle 0|\hat{n}_2|0\rangle_2 + {}_2\langle 1|\hat{n}_2|1\rangle_2) = \frac{1}{2}(0+1) = \frac{1}{2}$. This result signifies the mean particle number in output 2. Similar results are obtained for output 3.

2) Coherent state $|\alpha\rangle$ in input 1: $|0\rangle_0|\alpha\rangle_1$: The coherent state [20]–[24]

$$\begin{aligned}|\alpha\rangle &= e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \\ &= e^{-|\alpha|^2/2}[\,|0\rangle + \alpha|1\rangle + \frac{\alpha^2}{\sqrt{2}}|2\rangle + ...\,] \end{aligned} \quad (7)$$

is similar to a classical state. Depending on $|\alpha|^2$ (which represents the mean number of photons), a coherent state can contain a high number of photons. Hence, it is rather contrary to the highly non-classical single-photon state considered in the first example. Experimentally, a coherent state can be created by a laser beam. α is a complex number and $|\alpha|^2$ is the mean photon number. Coherent states are solutions of the eigen-value equation $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. The displacement operator $\hat{D}(\alpha) = e^{\alpha\hat{a}^+ - \alpha^*\hat{a}}$ applied on a vacuum state $|0\rangle$ is able to generate a coherent state $|\alpha\rangle$: $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$. In our example, we have in input mode 1 a coherent state and in input mode 0 a vacuum state: $|0\rangle_0|\alpha\rangle_1 = \hat{D}_1(\alpha)|0\rangle_0|0\rangle_1$. Using (3), one obtains:

$$\begin{aligned}|0\rangle_0|\alpha\rangle_1 \;\rightarrow^{BS}\rightarrow\; & e^{\frac{\alpha}{\sqrt{2}}(i\hat{a}_2^+ + \hat{a}_3^+) - \frac{\alpha^*}{\sqrt{2}}(-i\hat{a}_2 + \hat{a}_3)}|0\rangle_2|0\rangle_3 = \\ = \;& e^{(\frac{i\alpha}{\sqrt{2}})\hat{a}_2^+ - (\frac{i\alpha}{\sqrt{2}})^*\hat{a}_2}\;\times \\ & \times e^{(\frac{\alpha}{\sqrt{2}})\hat{a}_3^+ - (\frac{\alpha}{\sqrt{2}})^*\hat{a}_3}|0\rangle_2|0\rangle_3 = \\ = \;& \hat{D}_2(\frac{i\alpha}{\sqrt{2}})\hat{D}_3(\frac{\alpha}{\sqrt{2}})|0\rangle_2|0\rangle_3 = \\ = \;& |\frac{i\alpha}{\sqrt{2}}\rangle_2|\frac{\alpha}{\sqrt{2}}\rangle_3 \end{aligned} \quad (8)$$

The appropriate density operators are:

$$\begin{aligned}\hat{\rho}_{23} &= |\frac{i\alpha}{\sqrt{2}}\rangle_2|\frac{\alpha}{\sqrt{2}}\rangle_3\,{}_2\langle\frac{i\alpha}{\sqrt{2}}|\,{}_3\langle\frac{\alpha}{\sqrt{2}}| \\ \hat{\rho}_2 &= Tr_3(\hat{\rho_{23}}) = \\ &= |\frac{i\alpha}{\sqrt{2}}\rangle_2\,{}_2\langle\frac{i\alpha}{\sqrt{2}}| \end{aligned} \quad (9)$$

Equation (8) can be interpreted as follows: Similar to the classical picture in each output 2 or 3, exactly half of the photons $\frac{|\alpha|^2}{2}$ are reflected or transmitted by means of the balanced BS. The phase shift $i = e^{i\pi/2}$ of the reflected wave appears automatically. There is no entanglement with respect to coherent states. The result is a product state, as can be seen in (8).

Three important remarks:

a) For $\alpha = 0$ the coherent state $|\alpha\rangle$ achieves the vacuum state $|0\rangle$, but, e.g., for $\alpha = 1$ the 1-photon-state $|1\rangle$ is **not** obtained: $|\alpha = 1\rangle \neq |1\rangle$. $|\alpha = 1\rangle$ and $|1\rangle$ are entirely different states.

b) $\frac{1}{\sqrt{2}}(i|1\rangle_2|0\rangle_3 + |0\rangle_2|1\rangle_3)$ from (4) can be obtained in no way from $|\frac{i\alpha}{\sqrt{2}}\rangle_2|\frac{\alpha}{\sqrt{2}}\rangle_3$ of (8) because the first expression is an entangled state (no coincidences are possible) and the last one is a product state. The attempt to call a weak classical field a quantum field is misleading and absolutely incorrect. However, for $|\alpha|^2 \ll 1$ ($\alpha \approx \frac{1}{10}$ i.e., weak coherent state) the coherent state can be used very well for generating quantum numbers [25] by considering (8) and (7):

$$\begin{aligned}|\frac{i\alpha}{\sqrt{2}}\rangle_2|\frac{\alpha}{\sqrt{2}}\rangle_3 &\approx |0\rangle_2|0\rangle_3 + \\ &+ \frac{\alpha}{\sqrt{2}}\,[\,i|1\rangle_2|0\rangle_3 + |0\rangle_2|1\rangle_3\,] + ... \end{aligned} \quad (10)$$

As a result, it can be seen that mostly vacuum states are arising, but (with probability $\frac{|\alpha|^2}{2}$) the same entangled state as in (4) appears. Because parametric down-conversion (cf., (4) from Example 1) is a very rare event, the method presented here could be superior.

c) The mean particle number in output mode 2 is

$$\bar{n}_2 = Tr_2(\hat{n}_2\hat{\rho}_2) = {}_2\langle\frac{i\alpha}{\sqrt{2}}|\hat{a}_2^+\hat{a}_2|\frac{i\alpha}{\sqrt{2}}\rangle_2 = \frac{1}{2}|\alpha|^2\,. \quad (11)$$

The same is valid for output 3.

3) Input $|1\rangle_0|1\rangle_1$: Experimentally, such an input can be possible if the 2 photons simultaneously produced by means of parametric down-conversion are injected in the two input modes.

Photon $|1\rangle_0$ has two possibilities: either being transmitted or being reflected. The same applies for photon $|1\rangle_1$. One

obtains:

$$\begin{aligned} |1\rangle_0|1\rangle_1 &= \hat{a}_0^+\hat{a}_1^+|0\rangle_0|0\rangle_1 \rightarrow^{BS}\rightarrow \\ &\rightarrow \frac{1}{2}(\hat{a}_2^+ + i\hat{a}_3^+)(i\hat{a}_2^+ + \hat{a}_3^+)|0\rangle_2|0\rangle_3 = \\ &= \frac{i}{2}(\hat{a}_2^+\hat{a}_2^+ + \hat{a}_3^+\hat{a}_3^+)|0\rangle_2|0\rangle_3 = \\ &= \frac{i}{\sqrt{2}}(|2\rangle_2|0\rangle_3 + |0\rangle_2|2\rangle_3) \end{aligned} \quad (12)$$

This equation means entanglement of two photons with vacuum. There are either 2 photons in output 2 or 2 photons in output 3. There are neither coincidences using a balanced BS. But, contrary to a single photon process discussed in example 1, here the appearance of no coincidences is a matter of an interference effect between 2 possibilities of reflection or transmission at the BS.

Thus, we have no coincidences. This is indicated by (12) as well. This fact is experimentally tested in the so-called Hong-Ou-Mandel experiment [26]. A quantum random number generator based on this effect is described in [27].

Completely analog, the density operators $\hat{\rho}_{23}$, $\hat{\rho}_2$ and $\hat{\rho}_3$ can be composed using (12). For example, one gets

$$\begin{aligned} \hat{\rho}_2 &= \frac{1}{2}(|0\rangle_{2\,2}\langle 0| + |2\rangle_{2\,2}\langle 2|) \ , \\ \hat{\rho}_3 &= \frac{1}{2}(|0\rangle_{3\,3}\langle 0| + |2\rangle_{3\,3}\langle 2|) \\ \bar{n}_2 &= Tr(\hat{n}_2\hat{\rho}_2) = 1 \ , \ \bar{n}_3 = Tr(\hat{n}_3\hat{\rho}_3) = 1 \end{aligned} \quad (13)$$

This shows that the two single input photons can be used in order to generate quantum random numbers. This is an additional possibility besides the first case where only one single photon impinges the BS.

4) Input $|\alpha\rangle_0|\beta\rangle_1$*:* We discuss a case where two different coherent states $|\alpha\rangle$ and $|\beta\rangle$ are taken as input states [28]:

$$\begin{aligned} |\alpha\rangle_0|\beta\rangle_1 &= \hat{D}_1(\alpha)\hat{D}_0(\beta)|00\rangle_0 1 \ \rightarrow^{BS}\rightarrow \ |\gamma\rangle_2|\delta\rangle_3 = \\ &= |\psi\rangle_{out} \\ \gamma &= \frac{1}{\sqrt{2}}(\alpha + i\beta) \ , \ \delta = \frac{1}{\sqrt{2}}(i\alpha + \beta) \ . \end{aligned} \quad (14)$$

The density operators and mean photon numbers are, therefore,

$$\begin{aligned} \hat{\rho}_{23} &= |\psi\rangle_{out}\langle\psi| = |\gamma\rangle_2\langle\gamma| \otimes |\delta\rangle_3\langle\delta| = \hat{\rho}_2 \otimes \hat{\rho}_3 \ , \\ \bar{n}_2 &= Tr(\hat{\rho}_2\hat{n}_2) = |\gamma|^2 = \frac{1}{2}(|\alpha|^2 + |\beta|^2) = \\ &= \bar{n}_3 = |\delta|^2 \ . \end{aligned} \quad (15)$$

Again, for random numbers at the output, we have to require weak coherent input states:

$$\begin{aligned} &|\alpha|^2, |\beta|^2 \ll 1 \ , \rightarrow \\ \rightarrow \ |\psi\rangle_{out} &\approx |00\rangle_{23} + (\,\gamma\,|10\rangle_{23} + \delta\,|01\rangle_{23}) \ . \end{aligned} \quad (16)$$

5) Input $|0\rangle_0\frac{1}{\sqrt{2}}(|0\rangle_1+|1\rangle_1)$*:* Here, and in the next section, a superposition state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ is combined with a vacuum state $|0\rangle$ and a one-photon state $|1\rangle$, respectively. First, we consider the combination of vacuum with superposition state. The output clearly produces random numbers:

$$\begin{aligned} |0\rangle_0\frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1) &= \frac{1}{\sqrt{2}}(1 + \hat{a}_1^+)|00\rangle_{01} \ \rightarrow^{BS}\rightarrow \\ &\rightarrow \frac{1}{\sqrt{2}}[\,|00\rangle_{23} + \frac{1}{\sqrt{2}}(i|10\rangle + |01\rangle)_{23}\,] \end{aligned} \quad (17)$$

The mean photon numbers at the output are $1/4$ each:

$$\begin{aligned} \hat{\rho}_2 = \frac{1}{2}\,[\,&|0\rangle_2\langle 0| - \frac{i}{\sqrt{2}}|0\rangle_2\langle 1| + \frac{i}{\sqrt{2}}|1\rangle_2\langle 0| + \\ &+\frac{1}{2}|1\rangle_2\langle 1| + \frac{1}{2}|0\rangle_2\langle 0|\,] \ \rightarrow \ \bar{n}_2 = \bar{n}_3 = \frac{1}{4} \end{aligned} \quad (18)$$

6) Input $\frac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0)|1\rangle_1$*:* The combination of superposition with $|1\rangle$ gives

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0)|1\rangle_1 = \\ = \ &\frac{1}{\sqrt{2}}(1 + \hat{a}_0^+)\hat{a}_1^+|00\rangle_{01} \ \rightarrow^{BS}\rightarrow \\ \rightarrow \ &\frac{1}{\sqrt{2}}[\,\frac{1}{\sqrt{2}}(i|10\rangle + |01\rangle)_{23} + \frac{i}{\sqrt{2}}(|20\rangle + |02\rangle)_{23}\,] = \\ = \ &|\psi\rangle \ . \end{aligned} \quad (19)$$

The output state is a mixture of an output state resulting from single photon input and an output state resulting from the Hong-Ou-Mandel-effect. The mean photon number is, therefore, $3/4$:

$$\begin{aligned} \hat{\rho}_{23} &= |\psi\rangle\langle\psi| \\ \hat{\rho}_2 &= Tr_3(\hat{\rho}_{23}) = \\ &= \frac{1}{4}\,[\,|1\rangle_2\langle 1| + |1\rangle_2\langle 2| + |0\rangle_2\langle 0| + \\ &+ \ |2\rangle_2\langle 1| + |2\rangle_2\langle 2| + |0\rangle_2\langle 0|\,] \ \rightarrow \\ &\rightarrow \ \bar{n}_2 = \bar{n}_3 = \frac{3}{4} \end{aligned} \quad (20)$$

7) Input $|1\rangle_0|\alpha\rangle_1$*:* This input is described and discussed in the literature relating to the Mach-Zehnder interferometer using the Wigner function [29][30]. Here, we only consider the action of a BS with intent to create random numbers.

Immediately, we realize that the total number of input photons is $(1 + |\alpha|^2)$, of course. At the output ports 2 and 3 we expect therefore $\frac{1}{2}(1+|\alpha|^2)$ each. This is proved below.

Initially, the output state $|\psi\rangle_{out}$ is calculated as follows:

$$\begin{aligned} &|1\rangle_0|\alpha\rangle_1 = \hat{a}_0^+\hat{D}_1(\alpha)|00\rangle_{01} \ \rightarrow^{BS}\rightarrow \\ \rightarrow \ &\frac{1}{\sqrt{2}}(\hat{a}_2^+ + i\hat{a}_3^+)|\frac{i\alpha}{\sqrt{2}}\rangle_2|\frac{\alpha}{\sqrt{2}}\rangle_3 = |\psi\rangle_{out} \ . \end{aligned} \quad (21)$$

Only for a weak coherent state $|\alpha\rangle$ random numbers are possible:

$$\begin{aligned} |\alpha|^2 \ll 1 \ \rightarrow \ |\psi\rangle_{23} &\approx \frac{1}{\sqrt{2}}[\,|10\rangle + i|01\rangle\,]_{23} + \\ &+ \ \frac{i\alpha}{\sqrt{2}}[\,|20\rangle + i|02\rangle\,]_{23} \end{aligned} \quad (22)$$

Now, an exact calculation of mean photon number $\bar{n}_2$ is executed using $|\psi\rangle_{out}$. Again, the density operators $\hat{\rho}_{23}$ and $\hat{\rho}_2$ are necessary in order to determine $\bar{n}_2$ using the particle number operator $\hat{n}_2$:

$$\hat{\rho}_{23} = |\psi\rangle_{out}\langle\psi| \ , \ \hat{\rho}_2 = Tr_3(\hat{\rho}_{23}) \ , \ \bar{n}_2 = Tr_2(\hat{\rho}_2\hat{n}_2) \quad (23)$$

The trace-operation is executed by using the completeness relation of Fock states: $\mathbb{1} = \sum_{n=0}^{\infty}|n\rangle\langle n|$. We obtain

$$|\psi\rangle_{out} = \frac{1}{\sqrt{2}}\,[\,\hat{a}_2^+|\frac{i\alpha}{\sqrt{2}}\rangle_2|\frac{\alpha}{\sqrt{2}}\rangle_3 + i|\frac{i\alpha}{\sqrt{2}}\rangle_2\,\hat{a}_3^+|\frac{\alpha}{\sqrt{2}}\rangle_3\,] \quad (24)$$

 ISBN: 978-1-61208-749-8

$$\hat{\rho}_2 = \frac{1}{2}\{\hat{a}_2^+|\frac{i\alpha}{\sqrt{2}}\rangle_2\langle\frac{i\alpha}{\sqrt{2}}|\hat{a}_2 + |\frac{i\alpha}{\sqrt{2}}\rangle_2\langle\frac{i\alpha}{\sqrt{2}}|(1+\frac{|\alpha|^2}{2}) - - i\hat{a}_2^+|\frac{i\alpha}{\sqrt{2}}\rangle_2\langle\frac{i\alpha}{\sqrt{2}}|\frac{\alpha}{\sqrt{2}} + i\frac{\alpha^*}{\sqrt{2}}|\frac{i\alpha}{\sqrt{2}}\rangle_2\langle\frac{i\alpha}{\sqrt{2}}|\hat{a}_2\} \quad (25)$$

It can be shown that $Tr_2(\hat{\rho}_2) = 1$. For the mean particle number $\bar{n}_2$ in output 2, we get

$$\bar{n}_2 = \frac{1}{2}\{{}_2\langle\frac{i\alpha}{\sqrt{2}}|\hat{a}_2\hat{n}_2\hat{a}_2^+|\frac{i\alpha}{\sqrt{2}}\rangle_2 + (1+\frac{|\alpha|^2}{2})|\frac{i\alpha}{\sqrt{2}}|^2 - - i\,{}_2\langle\frac{i\alpha}{\sqrt{2}}|\hat{n}_2\hat{a}_2^+|\frac{i\alpha}{\sqrt{2}}\rangle_2\frac{\alpha}{\sqrt{2}} + + i\frac{\alpha^*}{\sqrt{2}}\,{}_2\langle\frac{i\alpha}{\sqrt{2}}|\hat{a}_2\hat{n}_2|\frac{i\alpha}{\sqrt{2}}\rangle_2\} = = \frac{1}{2}(1+|\alpha|^2)\ . \quad (26)$$

In the last step, the property of the trace $Tr(\hat{A}\hat{B}\hat{C}) = Tr(\hat{B}\hat{C}\hat{A}) = ...$ has been used. Moreover, one has to consider explicitely that $\hat{n} = \hat{a}^+\hat{a}$. The result in (26) is exactly what we expected. This outcome is valid for arbitrary parameters α.

8) Input $|\psi\rangle_{in} = \frac{1}{N}(|\alpha\rangle_0|\beta\rangle_1 + |\beta\rangle_0|\alpha\rangle_1)$*:* This input is a so-called Entangled Coherent State (ECS). It is described and discussed in [28][31][32].

From normalization ${}_{in}\langle\psi|\psi\rangle_{in} = 1$ we obtain $N = \sqrt{2(1+e^{-|\alpha-\beta|^2})}$ taking account of $\langle\beta|\alpha\rangle = e^{-|\alpha|^2/2-|\beta|^2/2+\alpha\beta^*}$. In case of $\alpha = \beta \rightarrow N = 2$.

The input state can be written as

$$|\psi\rangle_{in} = \frac{1}{N}[\,\hat{D}_0(\alpha)\hat{D}_1(\beta) + \hat{D}_0(\beta)\hat{D}_1(\alpha)\,]\,|00\rangle_{01}\ . \quad (27)$$

Initially, we discuss the mean photon number of the input. The necessary density operators are

$$\hat{\rho}_{01} = |\psi\rangle_{in}\langle\psi|\,,\ \hat{\rho}_0 = Tr_1(\hat{\rho}_{01}) \rightarrow \hat{\rho}_0 = \frac{1}{N^2}\{\,|\alpha\rangle_0\langle\alpha| + |\beta\rangle_0\langle\beta| + e^{-|\alpha|^2/2-|\beta|^2/2}\times \times [\,|\beta\rangle_0\langle\alpha|\,e^{\alpha\beta^*} + |\alpha\rangle_0\langle\beta|\,e^{\alpha^*\beta}\,]\,\}\,. \quad (28)$$

Here $\sum_n |\langle n|\alpha\rangle|^2 = 1$ and $\langle n|\alpha\rangle = \frac{\alpha^n}{\sqrt{n!}}e^{-|\alpha|^2/2}$ have been used. It can easily be shown that $Tr(\hat{\rho}_0) = 1$.

The mean number of input-photons $\bar{n}_0$ is obtained after some manipulation :

$$\bar{n}_0 = Tr(\hat{\rho}_0\hat{n}) = = \frac{1}{N^2}\,\{\,|\alpha|^2 + |\beta|^2 + e^{-|\alpha|^2-|\beta|^2+\alpha\beta^*+\alpha^*\beta}\times \times [\,\alpha\beta^* + \alpha^*\beta\,]\,\}\ . \quad (29)$$

An equivalent expression is obtained for $\bar{n}_1$. For $\alpha = \beta \rightarrow \bar{n}_0 = |\alpha|^2\ ,\ |\psi\rangle_{in} = |\alpha\alpha\rangle_{01}$.

Now, the output is considered. From (27) one gets directly (using the BS-process $\rightarrow^{BS}\rightarrow$) the normalized output state

$$|\psi\rangle_{out} = \frac{1}{N}\,[\,|\frac{\alpha+i\beta}{\sqrt{2}}\rangle_2|\frac{i\alpha+\beta}{\sqrt{2}}\rangle_3 + + |\frac{i\alpha+\beta}{\sqrt{2}}\rangle_2|\frac{\alpha+i\beta}{\sqrt{2}}\rangle_3\,]\ , \quad (30)$$

taking into account the Baker-Champbell-Hausdorff-theorem.

Special case : $\beta = -i\alpha$

$$|\psi\rangle_{out} = \frac{1}{N}\,[\,|\sqrt{2}\alpha\rangle_2|0\rangle_3 + |0\rangle_2|\sqrt{2}\alpha\rangle_3\,]\ , \quad N = \sqrt{2(1+e^{-2|\alpha|^2})}\ . \quad (31)$$

This is a coherent state $|\sqrt{2}\alpha\rangle$ in equal superposition of being in either one of two possible paths 2 or 3. This expression can be used in order to create random numbers. We calculate mean photon numbers:

$$\hat{\rho}_{23} = |\psi\rangle_{out}\langle\psi|\,,\ \hat{\rho}_2 = Tr_3(\hat{\rho}_{23}) \rightarrow \hat{\rho}_2 = \frac{1}{N^2}\{|\sqrt{2}\alpha\rangle_2\langle\sqrt{2}\alpha| + + |0\rangle_2\langle 0| + e^{-|\alpha|^2}\,[\,|0\rangle_2\langle\sqrt{2}\alpha|\ + |\sqrt{2}\alpha\rangle_2\langle 0|\,]\} \quad (32)$$

As before: $Tr(\hat{\rho}_2) = 1$.

$$\bar{n}_2 = Tr(\hat{\rho}_2\hat{n}) = \frac{|\alpha|^2}{1+e^{-2|\alpha|^2}} \quad (= \bar{n}_3)\ . \quad (33)$$

($|\alpha|^2 \ll 1 \rightarrow \bar{n}_2 \approx |\alpha|^2/2\,,\ \ |\alpha|^2 \gg 1 \rightarrow \bar{n}_2 \approx |\alpha|^2$.) Putting β to be $-i\alpha$ already at the input, one obtains $\bar{n}_0 = \bar{n}_2$ of course (see (29)).

9) Input $|\psi\rangle_{01} = |\beta\rangle_0\frac{1}{N_\beta}(|\beta\rangle_1 + |-\beta\rangle_1)$*:* This input means that we have a mixture of a coherent state $|\beta\rangle_0$ in mode 0 with a CSS (Coherent Superposition State [28][32]–[34]) in mode 1. The normalization of the wave function yields

$${}_{01}\langle\psi|\psi\rangle_{01} = 1 \rightarrow N_\beta = \sqrt{2(1+e^{-2|\beta|^2})}\ . \quad (34)$$

Now, we apply a BS which operates with the well-known Hadamard-transformation $\hat{H}$:

$$\begin{pmatrix}\hat{a}_2\\ \hat{a}_3\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\hat{a}_0\\ \hat{a}_1\end{pmatrix} = \hat{H}\begin{pmatrix}\hat{a}_0\\ \hat{a}_1\end{pmatrix}. \quad (35)$$

This transformation means transmission from the back side with phase $-1 = e^{i\pi}$, that is to say (see Figure 1):

$$\hat{a}_0^+ = \frac{1}{\sqrt{2}}(\hat{a}_2^+ + \hat{a}_3^+)\,,\ \hat{a}_1^+ = \frac{1}{\sqrt{2}}(\hat{a}_2^+ - \hat{a}_3^+) \quad . \quad (36)$$

The input state is easily transformed and the output becomes a coherent state $|\sqrt{2}\beta\rangle$ entangled with the vacuum $|0\rangle$:

$$|\psi\rangle_{01} = \hat{D}_0(\beta)\frac{1}{N_\beta}\,[\,\hat{D}_1(\beta) + \hat{D}_1(-\beta)\,]\,|00\rangle_{01}\ , \quad (37)$$

$$\rightarrow^{BS\,(\hat{H})}\rightarrow$$

$$|\psi\rangle_{23} = ... = \frac{1}{N_\beta}\,[\,|\sqrt{2}\beta\rangle_2|0\rangle_3 + |0\rangle_2|\sqrt{2}\beta\rangle_3\,] \quad (38)$$

Differently expressed, we have a coherent state $|\sqrt{2}\beta\rangle$ in equal superposition of being in either one of two possible paths 2 or 3. This is the same result we have obtained in (31) denoting β by α, however a Hadamard transformation is used for the BS.

 ISBN: 978-1-61208-749-8

III. Conclusion

In this paper, we provide insights into the complexity of generating true random numbers with Beam Splitters for cryptographic devices. Moreover, we investigate pre-defined input configurations and adopt mathematical procedures for a 50:50 Beam Splitter to derive true random data sets inside of a Hardware Security Module. The variants of the inputs are proposed, each of which are obtaining varying outputs.

As a result, we show the capability to use 50:50 Beam Splitters as quantum random number generators. We believe that the demonstrated input configurations of the quantum random number generator provide a suitable alternative to deterministic random number generators and increase the security of cryptographic devices and particularly of HSMs.

References

[1] D. Fox, "Hardware Security Module (HSM)," *Datenschutz und Datensicherheit - DuD*, vol. 33, no. 9, pp. 564–564, Sep. 2009.

[2] B. Hamid and D. Weber, "Engineering secure systems: Models, patterns and empirical validation," *Computers & Security*, vol. 77, pp. 315 – 348, 2018.

[3] R. De Prisco, A. De Santis, and M. Mannetta, "Reducing Costs in HSM-Based Data Centers," in *International Conference on Green, Pervasive, and Cloud Computing*, ser. Theoretical Computer Science and General Issues, M. H. A. Au, A. Castiglione, K.-K. R. Choo, F. Palmieri, and K.-C. Li, Eds. Springer International Publishing AG, 2017, pp. 3–14.

[4] J. A. Buchmann, E. Karatsiolis, and A. Wiesmaier, *Introduction to Public Key Infrastructures*. Springer Publishing Company, Incorporated, 2013.

[5] T. Zefferer, "A server-based signature solution for mobile devices," in *The 12th International Conference on Advances in Mobile Computing and Multimedia*, Dec. 2014, pp. 175–184.

[6] E. Shmueli, R. Vaisenberg, E. Gudes, and Y. Elovici, "Implementing a database encryption solution, design and implementation issues," *Computers & Security*, vol. 44, pp. 33–50, Jul. 2014.

[7] *Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2*, National Institute of Standards and Technology Std., May 2001.

[8] *Federal Information Processing Standards Publication 140-3 (FIPS PUB 140-3), Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology Std., Mar. 2019.

[9] *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001*, The Common Criteria Working Group Std., Apr. 2017.

[10] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002*, The Common Criteria Working Group Std., Apr. 2017.

[11] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003*, The Common Criteria Working Group Std., Apr. 2017.

[12] *ISO/IEC 15408-1:2009, Information technology Security techniques Evaluation criteria for IT security Part 1: Introduction and general model*, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Std., Jan. 2014.

[13] *ISO/IEC 15408-2:2008, Information technology Security techniques Evaluation criteria for IT security Part 2: Security functional components*, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Std., Jun. 2011.

[14] *ISO/IEC 15408-3:2008, Information technology Security techniques Evaluation criteria for IT security Part 3: Security assurance components*, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Std., Jun. 2011.

[15] E. Barker and J. Kelsey, *Recommendations for random number generation using deterministic random bit generators (NIST Special Publication 800-90A Revision 1)*, National Institute of Standards and Technology Std., Jun. 2015.

[16] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, vol. 47, no. 12, pp. 595–598, Mar. 2000.

[17] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, Apr. 2000.

[18] D. Marangon, A. Plews, M. Lucamarini, J. Dynes, A. Sharpe, Z. Yuan, and A. Shields, "Long term test of a fast and compact quantum random number generator," *Journal of Lightwave Technology*, vol. 36, no. 17, pp. 3778–3784, May 2018.

[19] K. Svozil, "Three criteria for quantum random-number generators based on beam splitters," *Physical Review A*, vol. 79, p. 054306, May 2009.

[20] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*. Cambridge: Cambridge University Press, 1995.

[21] U. Leonhardt, P. Knight, and A. Miller, *Measuring the Quantum State of Light*, ser. Cambridge Studies in Modern Optics. Cambridge: Cambridge University Press, 1997.

[22] R. Loudon, *The Quantum Theory of Light*. Oxford: OUP Oxford, 2000.

[23] W. P. Schleich, *Quantum Optics in Phase Space*. Berlin: Wiley-VCH Verlag Berlin GmbH, Feb. 2005.

[24] C. Gerry and P. L. Knight, *Introductory Quantum Optics*. Cambridge: Cambridge University Press, 2005.

[25] J. G. Rarity, P. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2435–2444, Jan. 1994.

[26] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Physical Review Letters*, vol. 59, no. 18, pp. 2044–2046, Nov. 1987.

[27] O. Kwon, Y.-W. Cho, and Y.-H. Kim, "Quantum random number generator using photon-number path entanglement," *Applied Optics*, vol. 48, no. 9, pp. 1774–1778, Mar. 2009.

[28] B. C. Sanders, "Entangled coherent states," *Physical Review A*, vol. 45, pp. 6811–6815, May 1992.

[29] X. Xu, F. Jia, L. Hu, Z. Duan, Q. Guo, and S.-j. Ma, "Quantum interference between an arbitrary-photon Fock state and a coherent state," *Journal of Modern Optics*, vol. 59, no. 18, pp. 1624–1633, Oct. 2012.

[30] A. Windhager, M. Suda, C. Pacher, M. Peev, and A. Poppe, "Quantum interference between a single-photon Fock state and a coherent state," *Optics Communications*, vol. 284, no. 7, pp. 1907–1912, Apr. 2011.

[31] B. C. Sanders, "Review of entangled coherent states," *Journal of Physics A Mathematical and Theoretical*, vol. 45, no. 24, p. 244002, Dec. 2011.

[32] Y. Israel, L. Cohen, X.-B. Song, J. Joo, H. S. Eisenberg, and Y. Silberberg, "Entangled coherent states created by mixing squeezed vacuum and coherent light," 2019. [Online]. Available: https://arxiv.org/abs/1707.01809

[33] C. Gerry and P. L. Knight, "Quantum superpositions and Schrödinger cat states in quantum optics," *American Journal of Physics*, vol. 65, no. 10, pp. 964–974, Oct. 1997.

[34] H. Jeong and M. S. Kim, "Efficient quantum computation using coherent states," *Physical Review A*, vol. 65, p. 042305, Mar. 2002.

 ISBN: 978-1-61208-749-8