



Article

Integrating Classical Preprocessing into an Optical Encryption Scheme

Hai Pham ^{1,2,†} , Rainer Steinwandt ^{1,†} and Adriana Suárez Corona ^{3,*,†} 

¹ Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL 33431, USA; hpham9@my.fau.edu (H.P.); rsteinwa@fau.edu (R.S.)

² West Campus Mathematics Division, Valencia College, Orlando, FL 32811, USA; hpham29@valenciacollege.edu

³ Department of Mathematical Sciences, Universidad de León, 24071 León, Spain

* Correspondence: asuac@unileon.es

† These authors contributed equally to this work.

Received: 25 July 2019; Accepted: 3 September 2019; Published: 7 September 2019

Abstract: Traditionally, cryptographic protocols rely on mathematical assumptions and results to establish security guarantees. Quantum cryptography has demonstrated how physical properties of a communication channel can be leveraged in the design of cryptographic protocols, too. Our starting point is the AlphaEta protocol, which was designed to exploit properties of coherent states of light to transmit data securely over an optical channel. AlphaEta aims to draw security from the uncertainty of any measurement of the transmitted coherent states due to intrinsic quantum noise. We present a technique to combine AlphaEta with classical preprocessing, taking into account error-correction for the optical channel. This enables us to establish strong provable security guarantees. In addition, the type of hybrid encryption we suggest, enables trade-offs between invoking a(n inexpensive) classical communication channel and a (more complex to implement) optical channel, without jeopardizing security. Our design can easily incorporate fast state-of-the-art authenticated encryption, but in this case the security analysis requires heuristic reasoning.

Keywords: symmetric encryption; all-or-nothing transform; optical channel; provable security

1. Introduction

The fast development of telecommunications and the increase of (potentially sensitive) data stored and exchanged by companies or individuals through public networks has made cryptography particularly important to guarantee the privacy, integrity and authenticity of users. The current approach to protect data involves the use of combinations of secret key [1] and public-key solutions [2], which base their security on empirical evidence or on the difficulty of solving certain mathematical problems respectively. A different approach has been explored since the 1980s, after Bennet and Brassard [3] proposed their seminal quantum key distribution protocol. Today research in quantum cryptography goes well beyond quantum key distribution [4,5].

Quantum-based cryptographic schemes have the conceptual appeal that security guarantees can potentially be argued based on fundamental laws of physics. However, popular quantum protocols, based on [3,6], commonly rely on single photon sources, which can be challenging to implement. As a result, in recent years, the idea of using mesoscopic coherent states has gathered interest, and the AlphaEta protocol is a prominent example of such a design (see, e.g., [7–10]). Its security has been the topic of several papers, including [9,11–14]. AlphaEta is also cited in Lloyd's work on quantum enigma machines [15]; Lloyd notes the open problem *to construct a provably secure quantum enigma machine using linear optics and coherent states*. As an alternative to AlphaEta, other optical cryptographic solutions were considered, including the use of double random phase encoding (DRPE) [16–18]. It deserves

noting that not only has academia been focusing on quantum technologies, but several industries have started to commercialize quantum cryptographic tools [5], specifically for quantum key distribution and quantum random number generation.

Capturing security guarantees that rely on physical assumptions with common security models for encryption poses somewhat of a challenge, especially when trying to integrate computationally secure primitives as well. Barbosa and van de Graaf rightfully point out that protocols based on quantum optical noise appear to be a wonderful source of research questions [10], though. It is tempting to harvest both the strength of existing (computationally secure) efficient cryptographic constructions and the features offered by an AlphaEta-type protocol, where an eavesdropper faces an additional, physical, hurdle.

Our Contribution

A protocol is proposed which takes advantage of the physical security guarantee offered from the AlphaEta setup and builds on this using classical constructions. In Section 2, we review the AlphaEta protocol and some definitions and results about *all-or-nothing transforms* (AONTs), a tool that has already proved to be useful in Li et al.'s work [19]. To be able to work conveniently with individual bits when discussing security, we introduce the notion of a *restricted* AONT and present a way of constructing these type of transformations. We propose a security model for encryption schemes using "hybrid ciphertexts", invoking both an optical channel (like AlphaEta does) and a classical communication channel. We present an (efficient) construction, building on AlphaEta, offering security in our model.

The security guarantee we establish is information-theoretic: we leverage the optical channel so that (physical) guarantees should prevent the adversary from learning any bit of the payload. Standalone, this may not be satisfying for applications yet, but we can integrate classical (high-speed) authenticated encryption. Then, with a heuristic argument, we create a situation where an adversary is unlikely to even intercept the correct *ciphertext*, offering a conceptually interesting additional layer of security: in traditional attack models, knowledge of the ciphertext is commonly considered as granted. It seems fair to say that we offer the first formalized proposal dealing with such hybrid ciphertexts, provably establishing the aforementioned advantage. It adds the physical security guarantee, but is easier/more flexible to implement since not the whole ciphertext needs to be transmitted through the optical channel.

2. Background and Tools

A protocol we will make use of is AlphaEta, and we briefly review the essential pieces, following mainly [8].

2.1. The AlphaEta Protocol

Ciphertexts in AlphaEta are a sequence of light pulses, where each pulse consists of many photons. They are represented using coherent states, and throughout, we use the following notation:

- $\langle n \rangle$: average number of photons per pulse
- β : number of bases used
- s : number of pulses sent in one round of the protocol

The two communicating parties are assumed to share a uniformly random $(b_1, \dots, b_s) \in \{0, \dots, \beta - 1\}^s$ that is unknown to the adversary and determines the bases used. Given a plaintext $a = (a_1, \dots, a_s) \in \{0, 1\}^s$, the sender will transmit each bit a_i in phase angle

$$\varphi_{a_i, b_i} = \left(\frac{b_i}{\beta} + a_i \right) \cdot \pi \quad (1)$$

to the receiver using the optical channel. Knowing the bases b_i , the receiver measures φ_{a_i, b_i} and maps it to the nearest phase angle to determine the original plaintext bit a_i .

The number of photons in each pulse follows a Poisson distribution with parameter $\langle n \rangle$. This statistical fluctuation is the quantum noise, which is intrinsic and cannot be avoided. This $\langle n \rangle$ is also related to the phase angle φ used to modulate light pulses. Hence, there are fluctuations in the phase angle φ as well. The security of a protocol using coherent states is based on the difficulty of determining the right phase angle if the basis is not known. An eavesdropper, not knowing the basis, faces an intrinsic error that can be bounded from below by a value that can be made close to $1/2$. Whereas the intended recipient, knowing the shared basis in which to measure, can recover any plaintext bit almost perfectly (bit error rates are below 10^{-9}).

In [8], it is shown that if a plaintext bit is chosen uniformly at random, which is typical for a key transport application, then the minimum probability of error P_e that an eavesdropper can achieve in the bit determination can be arbitrarily close to $1/2$ by choosing the appropriate parameters β and $\langle n \rangle$ (see ([8] Figure 3)). Therefore, the entropy about a bit of the plaintext given the measurement is reduced by only a small quantity ϵ and the mutual information of both random variables approaches that value ϵ (see ([8] Figure 4)).

In the next section, we recall a theoretical tool which will enable us to split a payload between two different types of channels—an optical one and a classical one—without jeopardizing security.

2.2. All-or-Nothing Transforms

Let ℓ, s be positive integers such that $1 \leq \ell \leq s$ and X be a finite set with $|X| = v$. We say that $\phi : X^s \rightarrow X^s$ is an (ℓ, s, v) -all-or-nothing transform (AONT) provided that all of the following holds:

1. ϕ is a bijection.
2. If any $s - \ell$ of the s output values y_1, \dots, y_s are fixed, then any ℓ of the input values x_i ($1 \leq i \leq s$) are completely undetermined, in an information-theoretic sense.

Following [20,21], throughout we use a definition of AONTs in terms of the entropy function H :

Definition 1. Let $X_1, \dots, X_s, Y_1, \dots, Y_s$ be random variables taking values from the finite set X , with $|X| = v$. These $2s$ random variables define an (ℓ, s, v) -AONT provided that the following conditions, are satisfied:

1. $H(Y_1, \dots, Y_s | X_1, \dots, X_s) = 0$,
2. $H(X_1, \dots, X_s | Y_1, \dots, Y_s) = 0$
3. For all $\mathcal{X} \subseteq \{X_1, \dots, X_s\}$ with $|\mathcal{X}| = \ell$, and for all $\mathcal{Y} \subseteq \{Y_1, \dots, Y_s\}$ with $|\mathcal{Y}| = \ell$, it holds that

$$H(\mathcal{X} | \{Y_1, \dots, Y_s\} \setminus \mathcal{Y}) = H(\mathcal{X}). \tag{2}$$

The definition of a linear AONT is the obvious one:

Definition 2. Let X be a finite field. An all-or-nothing transform is linear if each y_i is an X -linear function of x_1, \dots, x_s .

The following theorem provides a method to obtain linear AONTs [21]:

Theorem 1. Let q be a prime power and $M \in \mathbb{F}_q^{s \times s}$ invertible. Then M defines a linear (ℓ, s, q) -AONT

$$\begin{aligned} \phi : \mathbb{F}_q^s &\longrightarrow \mathbb{F}_q^s \\ x &\longmapsto xM^{-1} \end{aligned} \tag{3}$$

if and only if every ℓ by ℓ submatrix of M is invertible.

3. Results

With this preparation, we are ready to discuss the type of encryption schemes we are interested in here more formally.

3.1. Symmetric-key Encryption Using Mesoscopic Coherent States

Motivated by AlphaEta, we consider symmetric key encryption, where parts of the ciphertext can be non-classical: it can be a sequence of coherent states. When decrypting a ciphertext, a measurement should be done to obtain a classical bitstring from the coherent states. This together with the classical part forms the *reconstructed ciphertext*. Afterwards, from the reconstructed ciphertext, the plaintext can be recovered:

Definition 3. A symmetric-key encryption scheme using mesoscopic coherent states is a triple of algorithms as follows:

- **KeyGen:** Given a key length, outputs a corresponding secret key k .
- **Enc:** Given a plaintext m and secret key k , it outputs a ciphertext c , consisting of a sequence of coherent states and a bitstring:

$$c = (|\psi_1\rangle, \dots, |\psi_j\rangle, c_1, \dots, c_\ell) \quad (4)$$

- **Dec:** This process consists of two phases. Given a ciphertext c and a secret key k , the sequence of coherent states in c is measured in the first phase. Now c can be considered a classical bitstring when entering the second phase of the decryption. The final output of the algorithm is the plaintext m .

Remark 1. We allow the sequence of coherent states or the classical bitstring to be empty to include both classical and purely quantum symmetric-key encryption schemes, such as AlphaEta.

Figure 1 illustrates the overall structure of a symmetric-key encryption scheme using mesoscopic coherent states, highlighting the two different communication channels.

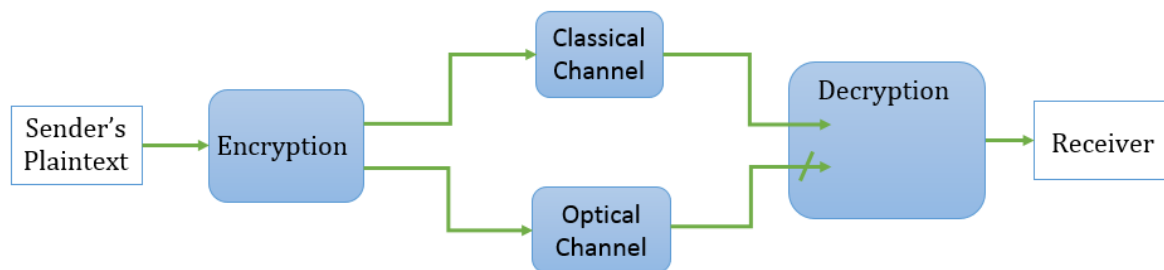


Figure 1. Overview of a symmetric-key encryption scheme using mesoscopic coherent states.

For such a scheme to be useful, we assume that the intended recipient, knowing the secret key and leaving aside channel imperfections, can recover correctly the plaintext from the ciphertext. This is captured by correctness:

Definition 4. A symmetric-key encryption scheme using mesoscopic coherent states is δ -correct if $(\text{Dec}_k \circ \text{Enc}_k)(m) = m$ except with a probability smaller than δ , for all k generated by **KeyGen** and all plaintexts m .

Notice that AlphaEta satisfies Definition 4, as discussed in [10]; the intended recipient can recover a plaintext bit with an error rate below 10^{-9} .

A user or adversary not knowing the secret information, should obtain as little information about a plaintext bit as possible. The entropy of a plaintext bit given the reconstructed ciphertext should not be very different from the entropy about that plaintext bit. We use this as motivation for

the following security definition. One could consider stronger security notions, in particular when allowing ciphertext expansion, but the following notion seems adequate when aiming at a composition with a classical scheme as discussed in Section 4.1.

Definition 5. Let $(\text{KeyGen}, \text{Enc}, \text{Dec})$ be a symmetric-key encryption scheme using mesoscopic coherent states. Let P_i denote the random variable taking the value of a plaintext bit and C_i denote the random variables taking the value of classical ciphertext bits. Let $\tilde{C}_1, \dots, \tilde{C}_\ell$ represent the random variables taking the value of the reconstructed ciphertext bits, i.e., \tilde{C}_i s correspond to the bits obtained after the corresponding measurement of the coherent states. We say that $(\text{KeyGen}, \text{Enc}, \text{Dec})$ is ϵ -secure if for $1 \leq i \leq s$:

$$|H(P_i | \tilde{C}_1, \dots, \tilde{C}_\ell, C_{\ell+1}, \dots, C_s) - H(P_i)| \leq \epsilon \quad (5)$$

Remark 2. The AlphaEta protocol satisfies Definition 5, assuming the a priori probability distribution for a bit is the discrete uniform probability.

As discussed in [10], the amount of information that the adversary, not knowing the bases, can obtain through eavesdropping can be made sufficiently small by choosing the parameters $\langle n \rangle$ and β appropriately. For example, for $\langle n \rangle = 100$ and $\beta = 5$, the minimum probability of error is $P_e^E \approx 0.476$. So $H(P | \tilde{C}) = -P_e^E \log_2 P_e^E - (1 - P_e^E) \log_2 (1 - P_e^E) \approx 0.998$. Since $H(P) = 1$, this will imply AlphaEta is ϵ -secure for $\epsilon = 0.002$ for the chosen parameters.

Moreover, the mutual information of the plaintext bit and reconstructed ciphertext is equal to ϵ , since $I(P, \tilde{C}) = H(P) - H(P | \tilde{C})$. A graph of P_e^E and $I(P, \tilde{C})$ as a function of $\langle n \rangle$ and β can be found in [10], where it can be seen how they can be made as close to $1/2$ and 0 , respectively, as desired by choosing the appropriate parameters.

Once the secret key is exposed, previous transmissions using the exposed key could become vulnerable. An adversary may have obtained previous ciphertexts, which, knowing the secret key, could potentially be decrypted and the messages would be known. Owing to the fact that in a symmetric-key encryption scheme using mesoscopic coherent states, parts of the ciphertext may be non-classical and we assume the adversary to conduct measurements on those parts, we can hope for some type of forward secrecy, however:

Definition 6. For $t \in \mathbb{N}$, let P_i^t be the random variable taking the value of a plaintext bit, and C_i^t the random variables taking the value of classical ciphertext bits at time t . Let $\tilde{C}_1^t, \dots, \tilde{C}_\ell^t$ represent the random variables taking the value of the reconstructed ciphertext bits, i.e., \tilde{C}_i^t s correspond to the bits obtained after the corresponding measurement of coherent states at time t . Let K^1, \dots, K^t represent the sequence of random variables taking the values of the symmetric key, i.e., values in $\{0, \dots, \beta - 1\}^s$. We assume after time t (when the ciphertext has been sent and the measurements without knowing K^t have been realized), K^1, \dots, K^t is revealed. A symmetric-key encryption scheme using mesoscopic coherent states is ϵ -forward secure if for all t we have

$$|H(P_i^t | \tilde{C}_1^t, \dots, \tilde{C}_\ell^t, C_{\ell+1}^t, \dots, C_s^t, K^1, \dots, K^t) - H(P_i^t)| \leq \epsilon. \quad (6)$$

3.2. A Hybrid Construction

Instead of applying a symmetric-key encryption scheme using mesoscopic coherent states directly to plaintexts, we will apply preprocessing. This will enable us to send (large) parts of the ciphertexts over a (potentially cheaper) classical communication channel without sacrificing security. One benefit is that the somewhat subtle problem of error correction on the optical channel, can be localized to a smaller payload.

3.2.1. Description and Design Rationale

Suppose party A wants to send an s -bit message to party B . We would like to invoke a linear AONT to transform the ciphertext such that if some blocks are missing, the entropy about other blocks is not reduced. We are particularly interested in the situation $q = 2$ and $l = 1$, with field elements representing bits. We try to “hide” individual input bits of an AONT where almost the complete output of the AONT is potentially available to an adversary. Unfortunately, the conditions of Theorem 1 cannot be satisfied when $\ell = 1$, $q = 2$ and $s \geq 2$, since the matrix in which all entries equal 1 is not invertible. To fix this issue, consider an s by s matrix M with entries in \mathbb{F}_2 with exactly $s - 1$ entries equal to zero. From [21] (Lemma 7), M is invertible over \mathbb{F}_2 if and only if the zero entries occur in $s - 1$ different rows and in $s - 1$ different columns. We will consider such matrices M with the zero-entries being arranged as follows:

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 \end{bmatrix}$$

So the first row of M contains all entries equal to 1. This means that each x_j value of the input depends on the value y_1 of the output. Thus, if y_1 is unknown, any value of the input is completely undetermined. Therefore, if we consider this restriction, the above linear transformation M behaves as an AONT. As with Definition 1, we can define a restricted AONT.

Definition 7. Let $X_1, \dots, X_s, Y_1, \dots, Y_s$ be random variables taking on values in the finite set X . These $2s$ random variables define a $\{1\}$ -restricted AONT provided that the following conditions are satisfied:

1. $H(Y_1, \dots, Y_s | X_1, \dots, X_s) = 0$
2. $H(X_1, \dots, X_s | Y_1, \dots, Y_s) = 0$
3. For all i such that $1 \leq i \leq s$, $H(X_i | Y_2, \dots, Y_s) = H(X_i)$.

We can generalize Definition 7 to an Y -restricted AONT.

Definition 8. Let $X_1, \dots, X_s, Y_1, \dots, Y_s$ be random variables taking on values in the finite set X . These $2s$ random variables define an Y -restricted AONT provided that the following conditions are satisfied:

1. $H(Y_1, \dots, Y_s | X_1, \dots, X_s) = 0$
2. $H(X_1, \dots, X_s | Y_1, \dots, Y_s) = 0$
3. Let $\mathcal{Y} = \{Y_v : v \in Y\}$ represent the collection of hidden bits. For all i such that $1 \leq i \leq s$, it holds that

$$H(X_i | \{Y_1, \dots, Y_s\} \setminus \mathcal{Y}) = H(X_i). \tag{7}$$

For convenience, we will simply speak of an ℓ -restricted AONT instead of an $\{1, \dots, \ell\}$ -restricted AONT.

Proposition 1. Let $M \in GL_s(\mathbb{F}_2)$. Let $\mathbf{x} = (x_1 x_2 \dots x_s)$ and $\mathbf{y} = (y_1 y_2 \dots y_s)$ where $\mathbf{x} = \mathbf{y}M$. If ℓ coordinates of \mathbf{y} are unknown, then there are 2^ℓ possible preimages \mathbf{x} .

Proof. Suppose one hides l values of \mathbf{y} . Since each bit has two possibilities, this leads to 2^l possible choices for \mathbf{y} . Since M is a bijection, it implies that there are also 2^ℓ candidates for the correct preimage \mathbf{x} . \square

Remark 3. While being strong, one should note that the guarantees of our restricted AONT are also limited: if available, two y_i -values can be combined to obtain the corresponding sum of x_i -values. Specifically, one can express \mathbf{y} in terms of \mathbf{x} as $\mathbf{y} = \mathbf{x}M^{-1}$ where

$$M^{-1} = \begin{bmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{bmatrix}$$

if s is even. If s is odd, the form of M^{-1} is similar except that $m_{11} = 1$. It can be observed that $y_i = x_1 + x_i$, for all $i = 2, \dots, s$. Thus, one may take the sum of y_p and y_q to obtain the sum of x_p and x_q (for $p, q \neq 1$):

$$\begin{aligned} y_p + y_q &= x_1 + x_p + x_1 + x_q \\ &= x_p + x_q \end{aligned} \tag{8}$$

Proposition 1 applies to linear restricted AONTs, and we will proceed by applying an ℓ -restricted AONT as in Definition 8. The bits represented by \mathcal{Y} will be transmitted to party B through the optical channel with AlphaEta, while the rest can be sent through a public classical channel.

It is crucial that the bits sent through the optical channel are received correctly. Otherwise, because of the properties of the (restricted) AONT, no bit of the plaintext could be recovered. Thus we will apply an error-correcting code to the bits indexed by \mathcal{Y} beforehand. One concern here is the impact of this added redundancy on security, and we will stick here to an embarrassingly trivial approach: For each bit in \mathcal{Y} , we will repeat it r times with r being odd. Barbosa pointed out that in this case the system can be designed to a desired security level P_e^E , through the correct choice of $\langle n \rangle$ and β [8]. Thus, even with the r -repeated sequence, the adversary’s error probability can be made close to $1/2$.

Figure 2 shows the main components of our protocol. A more detailed description of the algorithms as described in Definition 3 is provided in Figure 3.

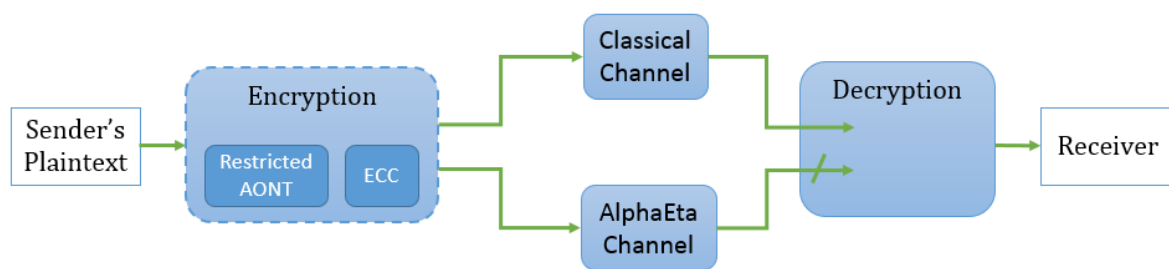


Figure 2. How a message is sent using the new construction.

Remark 4. The protocol describes how to encrypt a single s -bit plaintext block. To handle arbitrary length plaintexts, one could in a first approach break the plaintext into blocks of length s (using padding if needed) and apply the protocol block by block. However, more elaborate “modes of operation” could be explored and analyzed, e.g., a “tree construction”: the restricted AONT is applied to multiple blocks individually and afterwards, several bits of the corresponding resulting blocks are chosen and fed into the restricted AONT again. After that step, one chooses the bits to be sent through the AlphaEta channel and the ones to be sent classically. We leave the analysis of such modes of operation to future work.

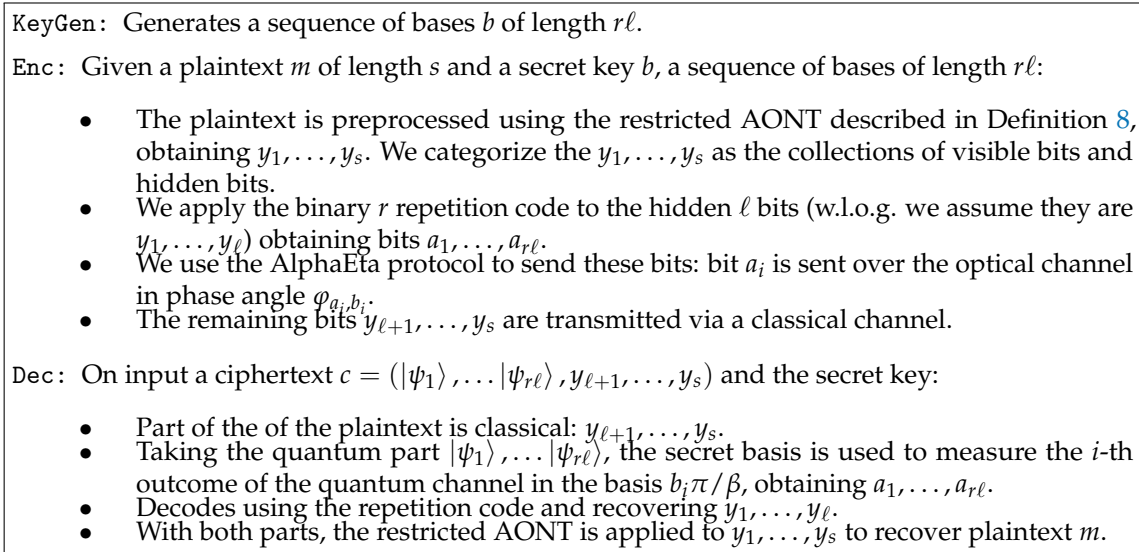


Figure 3. A quantum symmetric-key encryption scheme.

3.2.2. Security Analysis

The proposed hybrid construction, satisfies the notion of correctness and security as defined in Section 3.1:

Proposition 2. Let \mathcal{T} be an ℓ -restricted AONT on \mathbb{F}_2^s , let \mathcal{C} be a binary repetition code of odd length r , and assume that AlphaEta is δ -correct. Then the protocol in Figure 2 is δ' -correct according to Definition 4 where

$$\delta' = 1 - \left(\sum_{i=0}^{\frac{r-1}{2}} \binom{r}{i} \delta^i (1 - \delta)^{r-i} \right)^\ell. \tag{9}$$

Proof. The recipient receives all but $r\ell$ elements of the plaintext through the classical channel and the missing $r\ell$ elements via AlphaEta. Using the shared key of the AlphaEta protocol, since this protocol is δ -correct, the recipient recovers each of the corresponding $r\ell$ elements with probability of error smaller than δ . Since \mathcal{C} is a binary repetition code, each codeword containing up to $(r - 1)/2$ errors can be decoded correctly. This can be done with probability greater than

$$\sum_{i=0}^{\frac{r-1}{2}} \binom{r}{i} \delta^i (1 - \delta)^{r-i}. \tag{10}$$

Therefore, the recipient can recover all ℓ bits sent through the AlphaEta channel and therefore obtain the s elements of the plaintext with probability of error smaller than

$$1 - \left(\sum_{i=0}^{\frac{r-1}{2}} \binom{r}{i} \delta^i (1 - \delta)^{r-i} \right)^\ell. \tag{11}$$

□

Remark 5. By ([10] Theorem 1), for the AlphaEta protocol δ is less than 10^{-9} . As shown in Section 4.2, this allows acceptably small values for δ' .

In the proof of the following theorem, we are assuming the probability of $Y_i = 0$ and $Y_i = 1$ equals $1/2$ to use the results in [8] and assume the measurements and the values sent through AlphaEta to be

close to independent. In case we would like to provably ensure this as part of the protocol, we could apply a one-time pad (only) to the bits $a_1, \dots, a_{r\ell}$ prior to sending them through the AlphaEta channel.

Theorem 2. *Let \mathcal{T} be an ℓ -restricted AONT on \mathbb{F}_2^s , let \mathcal{C} be a binary repetition code of odd length r , and assume that AlphaEta is ϵ -secure. Then the protocol in Figure 2 is ϵ -secure according to Definition 5.*

Proof. We will use some properties about the entropy function. In particular, we recall the Chain Rule for entropy and a Corollary. For any random variables X, Y and Z , the following holds:

$$H(Y|X) = H(X, Y) - H(X) \tag{12}$$

$$H(X|Z) = H(X, Y|Z) - H(Y|X, Z) \tag{13}$$

Throughout the proof, we will use capital letters to denote the random variables taking the values of the corresponding plaintext and ciphertext bits.

The ciphertext for our protocol is of the form $c = (|\psi_1\rangle, \dots, |\psi_{r\ell}\rangle, y_{\ell+1}, \dots, y_s)$ as described in Figure 3. Let X_i denote the random variable corresponding to a bit of plaintext. After measuring the non-classical part, one should obtain $a_1, \dots, a_{r\ell}$. Not knowing the bases, one obtains $\tilde{a}_1, \dots, \tilde{a}_{r\ell}$. Thus, the reconstructed ciphertext is of the form $y = \tilde{a}_1, \dots, \tilde{a}_{r\ell}, y_{\ell+1}, \dots, y_s$. The entropy of the i -th bit of plaintext is hardly reduced after seeing the reconstructed ciphertext:

$$\begin{aligned} H(X_i|Y) &= H(X_i|Y_{\ell+1}, \dots, Y_s, \tilde{A}_1, \dots, \tilde{A}_{r\ell}) \\ &= H(Y_{\ell+1}, \dots, Y_s, X_i|\tilde{A}_1, \dots, \tilde{A}_{r\ell}) - H(Y_{\ell+1}, \dots, Y_s|\tilde{A}_1, \dots, \tilde{A}_{r\ell}) \\ &= H(Y_{\ell+1}, \dots, Y_s, X_i) - H(Y_{\ell+1}, \dots, Y_s) - \epsilon \\ &= H(X_i|Y_{\ell+1}, \dots, Y_s) + H(Y_{\ell+1}, \dots, Y_s) - H(Y_{\ell+1}, \dots, Y_s) - \epsilon \\ &= H(X_i) - \epsilon \end{aligned} \tag{14}$$

The second equality comes from the Corollary of the chain rule of entropy. Since the AlphaEta protocol provides the guarantee that the $\tilde{A}_1, \dots, \tilde{A}_{r\ell}$ are randomly independent from any Y_1, \dots, Y_s (as discussed in Section 2.1, seeing \tilde{a}_i provides only a small information about the sent bits, ϵ), the third equality holds. By applying the Chain rule of entropy to the term $H(Y_{\ell+1}, \dots, Y_s, X_i)$, we get the fourth equality. The last equality comes from the guarantee of our restricted AONT. \square

3.3. Forward Security

Following the motivation in Section 3.1, we want to show that our hybrid construction satisfies the forward security property on a bit-wise level. We let x_i^t represent a plaintext bit and $y^t = \tilde{a}_1^t, \dots, \tilde{a}_{r\ell}^t, y_{\ell+1}^t, \dots, y_s^t$ represent the reconstructed ciphertext at time period t for $t \in \mathbb{N}$. Let k^1, \dots, k^t represent the sequence of the secret keys. We assume after time t (when the ciphertext has been sent and the measurements without knowing k^t have been realized), k^t becomes public information. Even with knowledge of k^1, \dots, k^t , the entropy of the random variable taking the value of a plaintext bit X_i^t is hardly reduced:

Theorem 3. *If AlphaEta is ϵ -secure in transmitting a single bit, \mathcal{C} a binary repetition code with odd length r , and \mathcal{T} an ℓ -restricted restricted AONT on \mathbb{F}_2^s , then, the protocol in Figure 4 is ϵ -forward secure according to Definition 6.*

Proof. According to Bayes' Rule of entropy, for any random variables X, Y ,

$$H(Y|X) = H(X|Y) - H(X) + H(Y). \tag{15}$$

We will use capital letters to denote the random variables taking the values of the corresponding plaintext bits, reconstructed ciphertext and the keys. Hence, $H(X_i^t|Y^t, K^1, \dots, K^t)$ is equal to

$$\begin{aligned}
 & H(Y^t, X_i^t|K^1, \dots, K^t) - H(Y^t|K^1, \dots, K^t) \text{(Coroll.)} \\
 = & H(K^1, \dots, K^t|Y^t, X_i^t) - H(K^1, \dots, K^t) + \\
 & H(Y^t, X_i^t) - H(Y^t|K^1, \dots, K^t) \quad \text{(Bayes' R.)} \\
 = & H(Y^t, X_i^t) - H(Y^t|K^1, \dots, K^t) \\
 = & H(Y^t) + H(X_i^t|Y^t) - H(Y^t|K^1, \dots, K^t) \text{(Chain R.)} \\
 = & H(Y^t) + H(X_i^t) - \epsilon - H(Y^t|K^1, \dots, K^t) \quad \text{(Th. 2)} \\
 \geq & H(Y^t) + H(X_i^t) - H(Y^t) - \epsilon \\
 = & H(X_i^t) - \epsilon
 \end{aligned}
 \tag{16}$$

Since the secret keys K^1, \dots, K^t have been revealed, $H(K^1, \dots, K^t|Y^t, X_i^t)$ as well as $H(K^1, \dots, K^t)$ are zero. Hence, the third equality holds. In addition, the inequality holds since $H(Y^t|K^1, \dots, K^t) \leq H(Y^t)$. \square

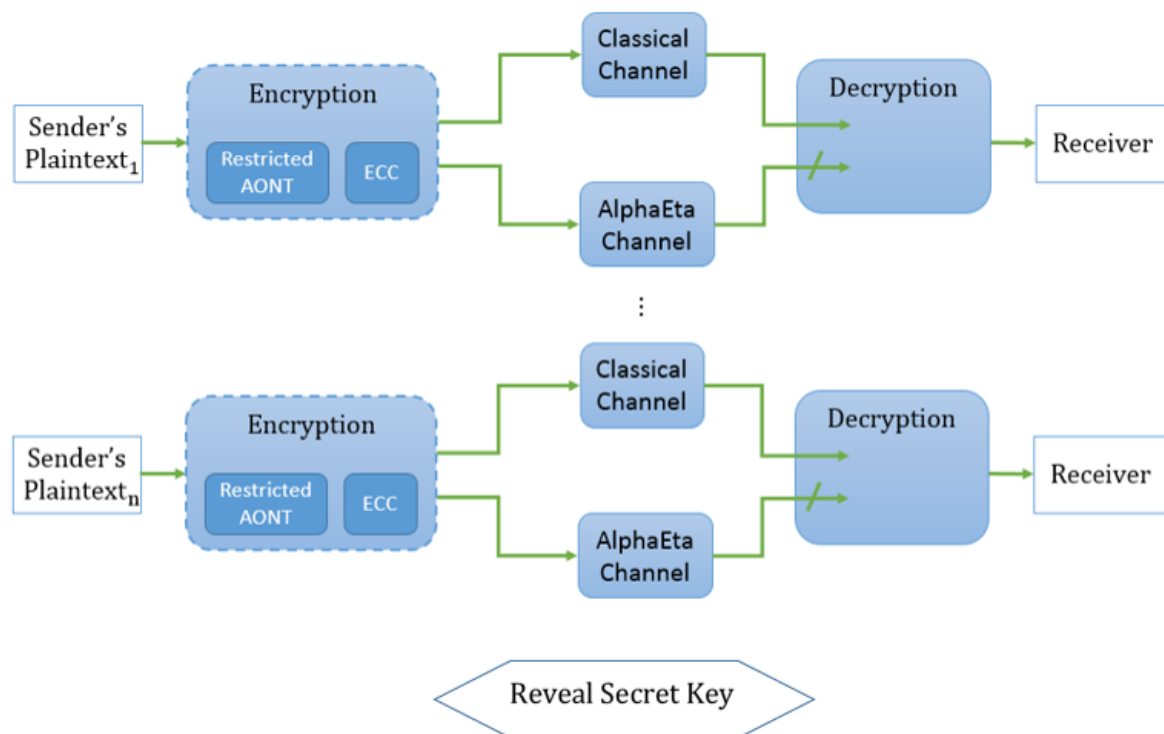


Figure 4. Description of an AlphaEta-based forward secure protocol.

4. Discussion

In our security discussion of the protocol, the plaintext was assumed to be comprised of independently uniformly chosen bits. Moreover, we did so far not address the problem of ensuring authentication or integrity.

4.1. Integrating Classical Authenticated Encryption

A pragmatic approach to address these issues is to apply a (high-speed) authenticated encryption to the plaintext, prior to the use of the restricted AONT. Specifically, here we choose the encrypt-then-MAC approach, leveraging the popular combination of the ChaCha20 stream cipher and Poly1305 authenticator [22].

Applying this combination results in a ciphertext that is (computationally) indistinguishable from random. (The ChaCha20 block function is a pseudo-random function (PRF) [23]. In addition, the last step of Poly1305 adds a fresh pseudo-random string, which can be derived using the ChaCha20 block function [22] and results in an authenticator that is (computationally) indistinguishable from random.) An overview of integrating such an additional classical preprocessing in our protocol is shown in Figure 5. Details are given in Figure 6.

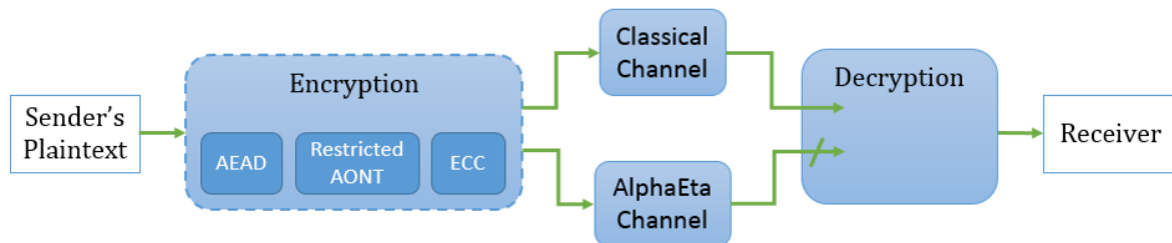


Figure 5. How the message is sent using the hybrid construction with authenticated encryption scheme; AEAD represents the application of ChaCha20 and Poly1305.

KeyGen: Generates a sequence of bases b of length $r\ell$ and a symmetric key for the AEAD (ChaCha20 and Poly1305).

Enc: Given a plaintext m of length s and a secret key b , a sequence of bases of length $r\ell$, as well as the secret key for the AEAD:

- The plaintext is preprocessed using the AEAD, obtaining x_1, \dots, x_s .
- The plaintext is preprocessed using the restricted AONT described in Definition 8 obtaining y_1, \dots, y_s . We categorize the outcome as the collections of visible bits and hidden bits.
- We apply the binary r repetition code to the hidden ℓ bits (w.l.o.g. we assume they are y_1, \dots, y_ℓ) obtaining bits $a_1, \dots, a_{r\ell}$.
- We use the AlphaEta protocol to send these bits: bit a_i is sent over the optical channel in phase angle φ_{a_i, b_i} .
- The visible bits $a_{\ell+1}, \dots, a_s$ will be transmitted via a classical channel.

Dec: On input a ciphertext $c = (|\psi_1\rangle, \dots, |\psi_{r\ell}\rangle, c_{\ell+1}, \dots, c_s)$ and the secret key:

- Part of the of the plaintext is classical: $c_{\ell+1}, \dots, c_s$.
- Taking $|\psi_1\rangle, \dots, |\psi_{r\ell}\rangle$, the secret basis is used to measure the i -th outcome of the AlphaEta channel in the basis $b_i\pi/\beta$, obtaining $c_1, \dots, c_{r\ell}$.
- Decodes using the repetition code and recovering a_1, \dots, a_ℓ .
- With both parts, the restricted AONT is applied to a_1, \dots, a_s to recover x_1, \dots, x_s .
- The AEAD is reversed and the plaintext is recovered.

Figure 6. A symmetric-key encryption scheme using mesoscopic coherent states with incorporated AEAD.

4.2. Choosing Parameters

The inputs of the AEAD using ChaCha20 cipher and Poly1305 Authenticator include a 256-bit key, a 96-bit nonce, an arbitrary length plaintext, and an arbitrary length additional authenticated data. For simplicity, here we assume the latter to be empty, though one could consider a situation for our protocol where parts of the payload does not require confidentiality. The output of the AEAD is a ciphertext of the same length as the plaintext and a 128-bit tag. It seems reasonable to choose 128 bits as a block size for the input and output of the AEAD. For further detailed parameters of the AEAD, one can refer to [22].

Once we have preprocessed the plaintext using the AEAD, we will apply the restricted AONT. We use the linear construction based on the matrix M^{-1} as defined in Section 3.2.1. To take advantage of the property of the restricted AONT, we would like its input to be greater than 128 bits. Let us consider the case where the inputs are 256-bit blocks. That means the matrix M^{-1} will have dimension

256 by 256. The outputs of the restricted AONT are also 256-bit blocks. We collect the first 128 bits as the hidden bits to be sent over the AlphaEta channel. The remaining bits will be sent over the classical channel.

We apply a binary repetition code of odd length to our collection of hidden bits. Recall the probability of error for transmitting one bit:

$$P_{err} = 1 - \sum_{i=0}^{\frac{r-1}{2}} \binom{r}{i} \delta^i (1-\delta)^{r-i} \quad (17)$$

where r is the length of the code and δ is the channel error probability. Table 1 (computed by means of the computer algebra system Magma [24]) demonstrates the probability of error δ' for transmitting 128 hidden bits given the length of the binary repetition code and the channel error probability.

Table 1. Probability of error for transmitting 128 bits with a repetition code.

r	$\frac{r-1}{2}$	δ	δ'
3	1	10^{-9}	3.84×10^{-16}
		10^{-5}	3.84×10^{-8}
		10^{-1}	0.9736
7	3	10^{-9}	4.48×10^{-33}
		10^{-5}	4.48×10^{-17}
		10^{-1}	0.2951
101	50	10^{-9}	2.56×10^{-428}
		10^{-5}	2.56×10^{-224}
		10^{-1}	1.47×10^{-22}

One can see the improvement in the correctness parameter of the symmetric-key encryption scheme using mesoscopic coherent states.

5. Conclusions

In this paper, we give a definition for a symmetric-key encryption scheme using mesoscopic states, including a security definition for such a scheme. We provide an example of such schemes using AlphaEta in combination with a variant of a classical AONT and error correction. Leveraging both an optical and a classical communication channel, we obtain an efficient construction with an interesting (information-theoretic) security guarantee. A forward security property is from a classical point of view quite remarkable: even after revealing the complete secret key, due to the underlying physical principle, the individual bits of the payload still remain hidden. In combination with a classical authenticated encryption, our design creates a situation where an adversary, based on physical principles, does not have even access to the classical output of a cipher, adding a conceptually interesting layer of security to a classical cipher, this being the main advantage over classical solutions.

When using repetition codes in our construction, the correctness parameter is improved, while the security parameter does not change, and only some part of the ciphertext is transmitted through the optical channel, which poses an advantage with respect to purely quantum schemes. From an implementation point of view, it deserves noting that our design integrates naturally with existing experimental setups for AlphaEta. All the steps we add can be seen as pre-processing and post-processing of the payload, cf. Figure 2. Therefore, for potential users, e.g., in industry, the experimentally demanding implementation of the optical channel does not have to be altered to be able to benefit from the security guarantees our approach offers. In addition, if one is willing to work with heuristic security arguments, the integration of classical authenticated encryption as outlined in Section 4.1 appears fairly attractive.

In general, symmetric-key encryption schemes using mesoscopic states as defined here, should interface naturally with schemes like AlphaEta, as the cryptographic processing assumes certain (abstract) guarantees provided by the invoked optical channel only. In this paper we leave the integration of more involved error correction techniques as future work; it seems fair to say that already our basic design offers a reasonably efficient combination of classical and physical techniques for securing a data transmission.

Author Contributions: Individual contributions to this article: conceptualization, H.P., R.S., and A.S.C.; methodology, H.P., R.S., and A.S.C.; software, H.P.; validation, H.P., R.S., and A.S.C.; formal analysis, H.P. and A.S.C.; investigation, H.P., R.S., and A.S.C.; resources, R.S. and A.S.C.; data curation, H.P.; writing—original draft preparation, H.P., R.S., and A.S.C.; writing—review and editing, H.P., R.S., and A.S.C.; visualization, H.P.; supervision, R.S.; project administration, R.S. and A.S.C.; funding acquisition, R.S. and A.S.C.

Funding: This research was funded in part by the NATO Science for Peace and Security Programme under grant G5448, through research project MTM2017-83506-C2-2-P by the Spanish MICINN, and through AFRL/RIKF Award No. FA8750-15-2-0047.

Acknowledgments: We would like to thank Martin Roetteler, who brought [15] to our attention, and Shane Kepley for helpful discussions. We also would like to thank the anonymous referees for constructive suggestions to improve the original manuscript.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. FIPS PUB 197, *Advanced Encryption Standard (AES)*; National Institute of Standards and Technology; U.S. Department of Commerce: Washington, DC, USA, 2001.
2. Rivest, R.L.; Shamir, A.; Adleman, L.M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 9–12 December 1984; p. 175.
4. Broadbent, A.; Schaffner, C. Quantum Cryptography Beyond Quantum Key Distribution. *Des. Codes Cryptogr.* **2016**, *78*, 351–382. [CrossRef]
5. Shenoy-Hejamadi, A.; Pathak, A.; Radhakrishna, S. Quantum Cryptography: Key Distribution and Beyond. *Quanta* **2017**, *6*, 1–47. [CrossRef]
6. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
7. Barbosa, G.A.; Corndorf, E.; Kumar, P.; Yuen, H.P. Secure communication using mesoscopic coherent states. *arXiv* **2003**, arXiv:quant-ph/0212018v2.
8. Barbosa, G.A. Fast and secure key distribution using mesoscopic coherent states of light. *arXiv* **2004**, arXiv:quant-ph/0212033v4.
9. Yuen, H.P.; Nair, R.; Corndorf, E.; Kanter, G.S.; Kumar, P. On the security of $\alpha\eta$: Response to 'some attacks on quantum-based cryptographic protocols'. *Quantum Inf. Comput.* **2006**, *6*, 561–582.
10. Barbosa, G.A.; van de Graaf, J. Untappable communication channels over optical fibers from quantum-optical noise. *IACR Cryptol. Eprint Arch.* **2014**, *2014*, 146.
11. Lo, H.K.; Ko, T.M. Some Attacks on Quantum-based Cryptographic Protocols. *arXiv* **2003**, arXiv:quant-ph/0309127. Available online: <https://arxiv.org/abs/quant-ph/0309127> (accessed on 4 September 2019).
12. Nishioka, T.; Hasegawa, T.; Ishizuka, H.; Imafuku, K.; Imai, H. How much security does Y-00 protocol provide us? *Phys. Lett. A* **2004**, *327*, 28–32. [CrossRef]
13. Yuen, H.P.; Kumar, P.; Corndorf, E.; Nair, R. Security of Y-00 and similar quantum cryptographic protocols. *arXiv* **2004**, arXiv:quant-ph/0407067. Available online: <https://arxiv.org/abs/quant-ph/0407067> (accessed on 4 September 2019).

14. Hirota, O.; Kurosawa, K. An immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol. *arXiv* **2006**, arXiv:quant-ph/0604036. Available online: <https://arxiv.org/abs/quant-ph/0604036> (accessed on 4 September 2019).
15. Lloyd, S. Quantum enigma machines. *arXiv* **2013**, arXiv:quant-ph/1307.0380. Available online: <https://arxiv.org/abs/1307.0380> (accessed on 4 September 2019).
16. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [[CrossRef](#)] [[PubMed](#)]
17. Jaramillo, A.; Barrera, J.F.; Vlez-Zea, A.; Torroba, R. Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment. *Opt. Lasers Eng.* **2018**, *102*, 119–125. [[CrossRef](#)]
18. Chen, H.; Zhao, J.; Liu, Z.; Du, X. Opto-digital spectrum encryption by using Baker mapping and gyrator transform. *Opt. Lasers Eng.* **2015**, *66*, 285–293. [[CrossRef](#)]
19. Li, Y.B.; Song, T.T.; Huang, W.; Zhan, W.W. Fault-Tolerant Quantum Secure Direct Communication Protocol Based on Decoherence-Free States. *Int. J. Theor. Phys.* **2015**, *54*, 589–597. [[CrossRef](#)]
20. Stinson, D.R. Something About All or Nothing (Transforms). *Des. Codes Cryptogr.* **2001**, *22*, 133–138. [[CrossRef](#)]
21. D’Arco, P.; Esfahani, N.N.; Stinson, D.R. All or Nothing at All. *Electr. J. Comb.* **2016**, *23*, 4–10.
22. Nir, Y.; Langley, A. ChaCha20 and Poly1305 for IETF Protocols. *Internet Res. Task Force* **2015**, doi:10.17487/rfc7539. [[CrossRef](#)]
23. Procter, G. A Security Analysis of the Composition of ChaCha20 and Poly1305. *IACR Cryptol. Eprint Arch.* **2014**, *2014*, 613.
24. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. *J. Symb. Comput.* **1997**, *24*, 235–265. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).