Secret Key Generation by Continuous Encryption Before Quantization

Ahmed Maksud, *Student Member, IEEE*, and Yingbo Hua, *Fellow, IEEE*

***Abstract*—Secret key generation (SKG) is a fundamental signal processing problem for security applications including wireless network security and biometric template security. For SKG, a pair (or more) of highly correlated secret vectors (SVs) need to be respectively quantized into a pair (or more) of almost identical sequences of binary bits (i.e., keys). The literatures on SKG in the wireless community almost uniformly default on a direct quantization on SVs. On the other hand, many works on biometric template security advocate a quantization on the output of a one-way function of SVs. In this paper, we present a generalized approach for SKG called continuous encryption before quantization (CEbQ). By CEbQ, a pair of SVs of limited dimension are first transformed by a continuous encryption function into a pair of sequences of quasi-continuous pseudorandom numbers (QCPRNs) of any desired length, and then these QCPRNs are quantized into keys. We show that CEbQ can yield a much lower key error rate than direct quantization subject to standardized randomness tests. Comparisons with other methods are also provided.**

***Index Terms*—Biometric security, continuous encryption, network security, quantization, secret key generation, wireless security.**

I. Introduction

Secret key generation (SKG) is a long standing problem for network security applications. For wireless security, a pair of nodes (Alice and Bob) in a wireless network can exploit their reciprocal channel state information to generate a secret key, e.g., see [1]–[19]. Such a key shared by Alice and Bob can be then used as a symmetric key for information encryption between them over any networks [20]. For biometric security, a biometric feature of a person can be collected to generate a secret key for future authentication of this person over any networks, e.g., see [21]–[26].

We can view the biometric feature vector collected from a person at one time as the secret vector of “Alice” and a corresponding biometric feature vector collected from the same person at a future time as the secret vector of “Bob”. This connection allows the problem of SKG to transcend both fields of wireless security and biometric security. However, unlike many prior works on information-theoretic capacities of SKG, e.g., see [27]–[29], this paper focuses on practical algorithms for SKG with useful tradeoffs.

A central issue of SKG is how to best transform a pair of highly correlated secret vectors (SVs) at Alice and Bob respectively into a pair of nearly identical sequences of binary bits (i.e., keys). The SVs are in practice quasi-continuous (due to finite precision of real number representation). Since the two SVs collected at Alice and Bob are generally not equal, the probability of the generated keys being unequal, i.e., key error rate (KER), is generally nonzero. So a central objective of SKG is to minimize KER.

The major steps of SKG for both wireless security and biometric security are: extraction of SVs which should be maximally correlated with each other and contain the minimal amount of non-secret, quantization of SVs with KER as small as possible, and reconciliation and privacy amplification for improved key, e.g., see [4], [5]. *In this paper, we focus on the problem of quantization to turn a pair of SVs into a pair of keys with any length, small KER and sufficient randomness.*

To reduce KER caused by quantization of SVs, there are two approaches: guardband quantization (GQ) and adaptive quantization (AQ). The GQ approach was proposed in [1] and further studied in [2], [3], [6]–[9], [11] and [12], where the range of each parameter in a feature vector is partitioned into a number of quantization regions separated by guardbands. When the realization of a parameter falls onto a guardband, that realization is discarded. Using guardbands helps to reduce KER but at a cost of key size. The AQ approach was proposed in [13] and further studed in [2], [14]–[19] under such names as coset source coding and over-quantization, where each parameter of a feature vector is assigned with multiple interleaved sub-quantizers. For each realization of a parameter, Alice determines the best sub-quantizer based on her measurement, and Bob is informed of this via public channel. Both Alice and Bob effectively apply the same sub-quantizer to quantize their measurements of the corresponding parameter respectively. Unlike the GQ approach, the AQ approach allows more cooperation between Alice and Bob and is more adaptive to each realization of a random parameter. Prior studies such as [2] suggest that the AQ approach in general outperforms the GQ approach in terms of robustness against the noises in SVs.

The above works on quantization all apply a direct quantization (DQ) on SVs. But many prior works on biometric template security, such as random projection (RP) [21], [22], dynamic random projection (DRP) [23], [24] and others [25],

Manuscript received May 17, 2022; accepted June 14, 2022. Date of publication June 20, 2022; date of current version July 13, 2022. This work was supported in part by the Army Research Office under Grant W911NF-17-1-0581 and in part by the Department of Defense under Grant W911NF-20-2-0267. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Yunlong Cai. *(Corresponding author: Yingbo Hua.)*

The authors are with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, CA 92521 USA (e-mail: amaks002@ucr.edu; yhua@ee.ucr.edu).

Digital Object Identifier 10.1109/LSP.2022.3184253

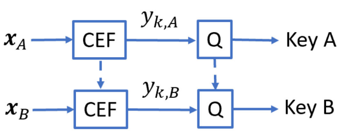

Fig. 1. Illustration of CEbQ for SKG.

[26], advocate indirect quantization on SVs, e.g., quantization on the output of a continuous one-way transformation of a secret biometric feature vector to produce cancellable passwords. But the keys from RP and DRP fail to pass randomness tests.

In this paper, we present a generalized approach for SKG as shown in Fig. 1, also referred to as continuous encryption before quantization (CEbQ). By CEbQ, we first use a continuous encryption function (CEF) [30] to encrypt a pair of highly correlated SVs of limited dimension into a pair of sequences of quasi-continuous pseudorandom numbers (QCPRNs) of any desired length. Unlike the conventional PRNs-generators, the desired CEF must be a continuous function of SV. These QCPRNs are then quantized into keys. The quality of keys will be measured by not only KER but also correlation tests and randomness tests.

In section II, we further discuss the properties of a desired CEF needed in Fig. 1, introduce a singular-value-decomposition (SVD) based CEF, and explain why the SVD-CEF yields the desired QCPRNs. In section III, we provide simulation results to demonstrate the advantage of CEbQ using SVD-CEF over DQ and two other indirect quantization methods. We will highlight the impact of a leakage of SVs (due to over-quantization) on KER for several methods.

II. Continuous Encryption Before Quantization

1) CEF and QCPRNS: As illustrated in Fig. 1, the proposed SKG method requires a CEF to produce QCPRNs from SVs. We will use the expression $y_k = f_k(\mathbf{x})$ to denote a CEF with $\mathbf{x} \in \mathcal{R}^N$ as its $N \times 1$ real-valued input vector and y_k as its kth real-valued output sample with $k \geq 1$. We say that a CEF can produce a sequence of QCPRNs if the following conditions are met: 1) The output of the CEF has a practically indefinite length; 2) The CEF is continuous, i.e., the output of the CEF has a finite sensitivity to a small perturbation on the input of the CEF; 3) The CEF is hard to invert, i.e., given any parts of y_k with $k \geq 1$, there is no known method with a polynomial complexity in terms of N (i.e., N^p for $p < \infty$) to determine an estimate $\hat{\mathbf{x}}$ of the input (or an estimate $\hat{s}(\mathbf{x})$ of a substitue input) such that $y_k = f_k(\mathbf{x}) \approx f_k(\hat{\mathbf{x}})$ (or $y_k = g_k(s(\mathbf{x})) \approx g_k(\hat{s}(\mathbf{x}))$) for all $k \geq 1$; 4) It can be verified empirically that the distribution of y_k is invariant to k when $\mathbf{x}$ consists of N independent and identically distributed (i.i.d.) entries; and 5) It can be verified empirically that y_k with $1 \leq k \leq K$ have near-zero correlations with $K \gg N$ and $\mathbf{x}$ consisting of i.i.d. entries.

The above notions of QCPRNs as the output of a desired CEF are similar to those defined for a good CEF in [30]. Such a good CEF is from a family of SVD-CEFs, which is described as follows. Let $\mathbf{Q}_{k,l} \in \mathcal{R}^{N \times N}$ be a pseudorandom unitary matrix for each pair of k and l where $l = 1, \ldots, N$ and $k \geq 1$. Both the seed and algorithm for generating these pseudorandom matrices are assumed to be in the public domain. For each of $k \geq 1$, define a modulated matrix of $\mathbf{x}$ as $\mathbf{M}_{k,x} = [\mathbf{Q}_{k,1}\mathbf{x}, \ldots, \mathbf{Q}_{k,N}\mathbf{x}]$. A SVD-CEF could define its kth output sample as any component of the SVD of $\mathbf{M}_{k,x}$, which would make $\mathbf{x}$ generally hard to compute from the output samples. But for desired statistical properties, we choose the kth output sample y_k of the SVD-CEF to be an entry (such as the 1st entry) of the left principal singular vector $\mathbf{u}_{k,\mathbf{x},1}$ of $\mathbf{M}_{k,x}$. Note that $\mathbf{M}_{k,x}\mathbf{M}_{k,x}^T = \sum_{l=1}^N \mathbf{Q}_{k,l}\mathbf{x}\mathbf{x}^T\mathbf{Q}_{k,l}^T$. So, $\mathbf{X} \doteq \mathbf{x}\mathbf{x}^T$ is a valid substitute input of the SVD-CEF.

It is obvious from the above description of the SVD-CEF that y_k is a nonlinear function of $\mathbf{x}$, y_k is invariant to the norm $\|\mathbf{x}\|$, y_k is a continuous function of $\mathbf{x}$ for almost all $\mathbf{x}$ subject to a typical (randomly chosen) set $\mathbf{Q}_{k,1:N} \doteq \{\mathbf{Q}_{k,l}; 1 \leq l \leq N\}$, and the sensitivity of y_k to a perturbation on $\mathbf{x}$ depends on the corresponding $\mathbf{Q}_{k,1:N}$. Other properties of the SVD-CEF are discussed below.

2) Hardness to Invert SVD-CEF: It is shown empirically in [30]–[32] that the SVD-CEF is hard to invert due to the fact that finding the solution of the input $\mathbf{x}$ (up to a scalar and sign) or the substitute input $\mathbf{X}$ from any subset of y_k for $k \geq 1$ amounts to solving a set of 2nd-order multivariate polynomial equations in more than N unknowns.

3) Noise Sensitivity of SVD-CEF: Without loss of generality, we can write $\mathbf{x}_B = \mathbf{x}_A + \partial\mathbf{x}$ where $\partial\mathbf{x}$ is the difference between the two secret vectors at Alice and Bob. Using the same SVD-CEF, if $y_{k,A}$ is the output at Alice from $\mathbf{x}_A$, then the output at Bob from $\mathbf{x}_B$ can be written as $y_{k,B} = y_{k,A} + \partial y_k$. It is clear that we do not want ∂y_k to be too sensitive to $\partial\mathbf{x}$. Let $\mathtt{SNR}_{\mathtt{in}} = \frac{\|\mathbf{x}_A\|^2}{\mathcal{E}\{\|\partial\mathbf{x}\|^2\}}$ be the input signal-to-noise ratio (SNR) at Bob, and $\mathtt{SNR}_{\mathtt{out},k} = \frac{\|y_{k,A}\|^2}{\mathcal{E}_{\partial\mathbf{x}}\{\|\partial y_k\|^2\}}$ be the output SNR at Bob for each k. A figure-of-merit (FoM) of the SVD-CEF for each k can be defined as $\eta_{k,\mathbf{x}_A} \doteq \sqrt{\frac{\mathtt{SNR}_{\mathtt{in}}}{\mathtt{SNR}_{\mathtt{out},k}}}$, which measures how much the input noise for Bob (relative to Alice's input) is amplified at the output for Bob.

Theorem 1: Assume that $\partial\mathbf{x}$ consists of i.i.d. entries with zero mean and an arbitrarily small variance. Then, $\eta_{k,\mathbf{x}_A} = \sqrt{\frac{1}{N}\sum_{j=1}^{N-1}\sigma_j^2}$ where $\sigma_1 > \cdots > \sigma_N = 0$ are the singular values of

$$\mathbf{T} = \left(\sum_{j=2}^{N} \frac{1}{\lambda_1 - \lambda_j} \mathbf{u}_{k,\mathbf{x}_A,j}\mathbf{u}_{k,\mathbf{x}_A,j}^T\right) \cdot \left(\sum_{l=1}^{N} \mathbf{Q}_{k,l}\left[(\mathbf{x}_A^T\mathbf{Q}_{k,l}^T\mathbf{u}_{k,\mathbf{x}_A,1})\mathbf{I}_N + \mathbf{x}_A\mathbf{u}_{k,\mathbf{x}_A,1}^T\mathbf{Q}_{k,l}\right]\right) \quad (1)$$

which has the rank $N-1$, and $\mathbf{u}_{k,\mathbf{x}_A,j}$ and λ_j are the jth pair of eigenvector and eigenvalue of $\mathbf{M}_{k,\mathbf{x}_A}\mathbf{M}_{k,\mathbf{x}_A}^T$. Here, λ_j is in the descending order.

Proof: See the proof of (62) in [30]. ■

It is important to note that for given $\mathbf{x}_A$ and $\mathbf{Q}_{k,1:N}$, $\eta_{k,\mathbf{x}_A}$ can be computed by Alice. For example, if $\eta_{k_0,\mathbf{x}_A}$ is larger than a threshold, Alice can inform Bob (i.e., the left dash arrow line in Fig. 1) so that they can both avoid the use of the corresponding $\mathbf{Q}_{k_0,1:N}$. In this way, the noise amplification by the SVD-CEF is under a control. In theory, an attacker may gain some information about $\mathbf{x}_A$ from knowing $\eta_{k_0,\mathbf{x}_A}$ exceeding a threshold. But computing $\mathbf{x}_A$ from this knowledge does not seem trivial.

The above theorem also explains why an entry of the principal eigenvector (instead of other eigenvectors) of $\mathbf{M}_{k,\mathbf{x}}\mathbf{M}_{k,\mathbf{x}}^T$ is chosen as the output of the SVD-CEF. See $\frac{1}{\lambda_1-\lambda_j}$ in (1).

4) Statistics of QCPRNs From SVD-CEF: It is shown empirically via simulation in [30] that if N is moderate or large (such as $N \geq 15$), $\mathbf{Q}_{k,1:N}$ is typical and $\mathbf{x}$ has the Gaussian distribution $\mathcal{N}(0, \sigma_x^2\mathbf{I}_N)$, then the probability density function (PDF) of y_k is approximately given by

$$f_{y_k}(y) = C_N(1-y^2)^{\frac{N-3}{2}} \tag{2}$$

with $C_N = \frac{\Gamma(N/2)}{\sqrt{\pi}\Gamma((N-1)/2)}$ and $-1 < y < 1$. This known PDF of y_k is important for optimal quantization on y_k. (In fact, the PDF of y_k is relatively invariant to the PDF of the i.i.d. entries of $\mathbf{x}$ because each entry of $\mathbf{M}_{k,\mathbf{x}}$ is a weighted sum of the entries in $\mathbf{x}$ and hence tends to be Gaussian in general. This gives an additional advantage to CEbQ over direct quantization (DQ) on $\mathbf{x}$. Without a good knowledge of the PDF of $\mathbf{x}$, the performance of a DQ on $\mathbf{x}$ generally suffers.) Furthermore, we have observed via simulation that for a typical set $\mathbf{Q}_{1:K,1:N} \doteq \{\mathbf{Q}_{1,1:N}, \ldots, \mathbf{Q}_{K,1:N}\}$, the output samples of the SDV-CEF, i.e., $y_1, y_2, \ldots, y_K$, have near-zero (normalized) correlations.

The above can be explained by the following analysis. Assume $\mathbf{x} \sim \mathcal{N}(0, \sigma_x^2\mathbf{I}_N)$. Then $\mathcal{E}\{\mathbf{X}\} = \mathcal{E}\{\mathbf{x}\mathbf{x}^T\} = \sigma_x^2\mathbf{I}_N$. Let $\mathbf{R}_{k,\mathbf{x}} = \mathbf{M}_{k,\mathbf{x}}\mathbf{M}_{k,\mathbf{x}}^T$ and $\mathbf{W} = \mathbf{X} - \sigma_x^2\mathbf{I}_N$. It follows that $\mathbf{R}_{k,\mathbf{x}} = \mathbf{R}'_{k,\mathbf{x}} + N\sigma_x^2\mathbf{I}_N$ with $\mathbf{R}'_{k,\mathbf{x}} = \sum_{l=1}^N \mathbf{Q}_{k,l}\mathbf{W}\mathbf{Q}_{k,l}^T$. Clearly, $\mathbf{R}_{k,\mathbf{x}}$ and $\mathbf{R}'_{k,\mathbf{x}}$ have the same eigenvectors. It also follows that $\mathcal{E}\{\mathbf{W}\} = 0$, $\mathcal{E}\{w_{i,i}^2\} = 2\sigma_x^4$, $\mathcal{E}\{w_{i,j}^2\} = \sigma_x^4$ for $i \neq j$, and $\mathcal{E}\{w_{i,j}w_{l,m}\} = 0$ for $(i,j) \neq (l,m)$.

Let $\mathbf{q}_{k,l,i}$ be the ith column of $\mathbf{Q}_{k,l}$. Then $\mathbf{R}'_{k,\mathbf{x}} = \sum_{s=1}^N \sum_{v=1}^N (\sum_{l=1}^N \mathbf{q}_{k,l,s}\mathbf{q}_{k,l,v}^T) w_{s,v}$. Let $\mathbf{G}_{k,s,v} = \sum_{l=1}^N \mathbf{q}_{k,l,s}\mathbf{q}_{k,l,v}^T$. Then

$$\mathbf{R}'_{k,\mathbf{x}} = \sum_{s=1}^N \mathbf{G}_{k,s,s}w_{s,s} + \sum_{N\geq s>v\geq 1} (\mathbf{G}_{k,s,v} + \mathbf{G}_{k,s,v}^T)w_{s,v} \tag{3}$$

where we have applied $w_{s,v} = w_{v,s}$. We see that $\mathbf{R}'_{k,\mathbf{x}}$ consists of $N(N+1)/2$ uncorrelated terms corresponding to $w_{s,v}$ for $s \geq v$. Each term typically has the full rank N.

The principal eigenvector of $\mathbf{R}'_{k,\mathbf{x}}$ is therefore highly dependent on $\mathbf{W}$. Based on the variances of $w_{s,v}$, we see that the $N(N+1)/2$ uncorrelated terms in (3) have about the same weight on $\mathbf{R}'_{k,\mathbf{x}}$. For this reason, we can conjecture that the principal eigenvector $\mathbf{u}_{k,\mathbf{x}}$ of $\mathbf{R}'_{k,\mathbf{x}}$ tends to appear uniformly on the $N-1$ dimensional sphere of unit radius $\mathcal{S}^{N-1}(1)$. Assuming that $\mathbf{u}_{k,\mathbf{x}}$ is uniform on $\mathcal{S}^{N-1}(1)$, the PDF of y_k as shown in (2) can be proven (see proof of (82) in [30]).

Also, since $\mathbf{R}'_{m,\mathbf{x}}$ depends on a set of basis matrices totally different from those of $\mathbf{R}'_{k,\mathbf{x}}$ for $k \neq m$, the trajectory of $\mathbf{u}_{m,\mathbf{x}}$ is hence uncorrelated with that of $\mathbf{u}_{k,\mathbf{x}}$ as $\mathbf{W}$ or equivalently $\mathbf{x}$ changes. This explains why the output values of the SVD-CEF, i.e., y_k for $1 \leq k \leq K$ (even with a large $K \gg N$), have near-zero correlations.

5) Adaptive Quantization: Finally, to complete the description of CEbQ, we now discuss an adaptive quantizer (AQ) or over-quantization algorithm shown in [2]. This algorithm is summarized below:

For each of $y_{k,A}$ and $y_{k,B}$, the number of desired bits (per QCPRN sample) is set to be m. Alice and Bob share the same L-level equiprobable quantizer $\mathcal{Q}_L$ where $L = 2^{m+l}$ and the boundary values, t_i for $i = 0, \ldots, L$, satisfy $\int_{-1}^{t_i} f_{y_k}(y)dy = \frac{i}{L}$. A sample that falls into $[t_i, t_{i+1})$ will be quantized to the integer i represented by the standard $m+l$ bits.

For each k, Alice uses $\mathcal{Q}_L$ to quantize $y_{k,A}$ into $m+l$ bits. She keeps the m most significant bits (MSBs) as the kth part of her key $\mathcal{K}_A$ of total key length $L_{key} = mK$ and transmits to Bob publicly the l least significant bits (LSBs). The l LSBs do not reveal any information about the m MSBs if $y_{k,A}$ for all k are independent. In simulation, we will choose $l = 0, 1, 3$.

For each k, Bob obtains $\mathcal{C}_{2^m,k}$ consisting of the center points of a subset of 2^m intervals from $\mathcal{Q}_L$, corresponding to the l LSBs received from Alice. Bob then determines $j_k = \arg\min_{c_j \in \mathcal{C}_{2^m,k}} |y_{k,B} - c_j|$. The m-bit representation of j_k are the kth part of his key $\mathcal{K}_B$ of total key length $L_{key} = mK$.

If $\mathcal{K}_A = \mathcal{K}_B$, there is no key error. Otherwise, a key error occurs. The key error rate (KER) will be based on $R = 10^4$ realizations of $y_{k,A}$ and $y_{k,B}$ with $k = 1, 2, \ldots, K$, which correspond to $R = 10^4$ random realizations of each of $\mathbf{x}_A$ and $\mathbf{w}$ subject to $\mathbf{x}_B = \mathbf{x}_A + \mathbf{w}$ and a fixed $\mathbf{Q}_{1:K,1:N}$. We will choose $\mathbf{x}_A \sim \mathcal{N}(0, \mathbf{I}_N)$ and $\mathbf{w} \sim \mathcal{N}(0, \frac{1}{\mathtt{SNR}_x}\mathbf{I})$ where $\mathtt{SNR}_x$ denotes the SNR in $\mathbf{x}_B$ relative to $\mathbf{x}_A$.

Note that for DQ on $\mathbf{x}_A$ and $\mathbf{x}_B$, $y_{k,A}$ and $y_{k,B}$ for $k = 1, \ldots, K$ in the algorithm will be replaced by the entries of $\mathbf{x}_A$ and $\mathbf{x}_B$ respectively, and hence $K = N$ and $L_{key} = mN$. Also the PDF $f_{y_k}(y)$ in the algorithm needs to be replaced by the PDF of the entry of $\mathbf{x}$. For most applications, $\mathbf{x}_A$ and $\mathbf{x}_B$ have the same PDF.

III. Simulation Results and Comparisons

In this section, we will refer to CEbF using SVD-CEF simply as SVD-CEF.

1) Prior Methods for SKG Using Indirect Quantization: In the field of biometric template security, there have been many efforts on using continuous one-way functions to transform a secret vector before quantization to obtain so called cancellable passwords, e.g., see [22] and [24]. Two notable such transformations are random projection (RP) [21] and dynamic random projection (DRP) [23]. But these two transformations can be both inverted with a polynomial complexity [30]. Moreover, the output samples of RP are highly correlated with each other, which after quantization results in a key with highly correlated bits. So, we will not further consider RP. For DRP, we will consider the "Function II" version in [23], which can be described as follows. A $N \times 1$ secret vector $\mathbf{x}$ is first transformed into a $K \times 1$ vector $\mathbf{v} = \mathbf{R}\mathbf{x}$ with $\mathbf{R}$ being an orthonormal pseudorandom matrix, then the kth entry v_k of $\mathbf{v}$ is quantized (or "indexed") into an integer l_k subject to $1 \leq l_k \leq L$ which is then used to determine one of L pseudorandom Gaussian vectors $\mathbf{a}_{1,k}, \ldots, \mathbf{a}_{L,k}$. The kth output of DRP is $y_k = \mathbf{a}_{l_k,k}^T\mathbf{x}$, which can be then quantized into a key. In our simulation, we will use the AQ for quantizing v_k with $L = N/2$, and also for quantizing y_k for each k into 1 bit, which is an improved version from [23]. For the resulting key of each realization of $\mathbf{x}$, $L_{key} = K$.

TABLE I
PEAK CORRELATION VALUES OF BITS IN KEYS

L_{key} →	32	64	128	256	512
DQ	0.0224	0.0263	0.0246	0.0361	NA
SVD-CEF	0.0231	0.0277	0.0279	0.0306	0.0306
DRP	0.1057	0.1058	0.1201	0.1149	0.1308
IoM	0.1593	0.1700	0.2127	0.2178	0.2543

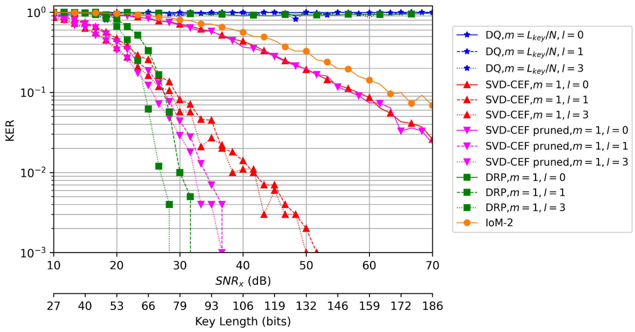

Fig. 2. KER versus $L_{key} = \frac{N}{2}\log_2(1 + \mathrm{SNR}_x)$.

Another method to turn $\mathbf{x}$ into a key is called index-of-max (IoM) hashing [25]. For each of $1 \leq k \leq K$, IoM first generates V pseudorandom permutations of $\mathbf{x}$, then produces a vector $\mathbf{v}_k$ by computing the element-wise products of the V vectors, and finally determines the index of the largest entry in $\mathbf{v}_k$. The resulting key has the size $L_{key} = K \log_2 N$. As shown in [30], IoM can be inverted with a complexity no more than $\mathcal{O}(2^N)$, and its KER is not as good as the SVD-CEF. In this section, we will provide further results on IoM assuming $V = 3$.

2) Correlation Tests: A basic requirement on a generated key is that the bits in the key should be practically uncorrelated with each other subject to $\mathbf{x}$ consisting of independent entries and all used pseudorandom transformations being fixed. To test the correlation, we map each key of L_{key} bits, generated from $\mathbf{x}$, onto an $L_{key} \times 1$ vector $\mathbf{b}$ consisting of 1's and -1's (corresponding to 1's and 0's). We are interested in the largest off-diagonal element in $\mathbf{C_b} = \mathcal{E}_\mathbf{x}\{\mathbf{b}\mathbf{b}^T\}$, i.e., $c_{\max} = \max_{i \neq j} |(\mathbf{C_b})_{i,j}|$. Table I compares $c_{\max}$. For $L_{key} = 512$ (and $N = 16$), DQ would need to extract out 32 bits per entry of $\mathbf{x}$ and was not feasible on our computer. For other choices of L_{key}, we see that DQ and SVD-CEF have comparable values of $c_{\max}$, which are much smaller than those of DRP and IoM. This result is based on 2×10^4 realizations of $\mathbf{x} \sim \mathcal{N}(0, \mathbf{I}_N)$ with $N = 16$.

3) Key Error Rate: To compare the KERs, we set $L_{key} = \frac{N}{2}\log_2(1 + \mathrm{SNR}_x)$ which is the theoretical limit, i.e., mutual information between $\mathbf{x}_A$ and $\mathbf{x}_B = \mathbf{x}_A + \mathbf{w}$ where $\mathbf{x}_A \sim \mathcal{N}(0, \mathbf{I}_N)$ and $\mathbf{w} \sim \mathcal{N}(0, \frac{1}{\mathrm{SNR}_x}\mathbf{I}_N)$. Fig. 2 is based on $R = 10^4$ realizations of $\mathbf{x}_A$ and $\mathbf{w}$ with $N = 16$. In Fig. 2, m is the number of secret bits per y_k, and l is the number of over-quantized bits. The latter also corresponds to a leakage of $\mathbf{x}_A$ for DQ, a leakage of v_k and y_k for DRP, and a leakage of y_k for SVD-CEF. We see that the DQ fails badly in terms of KER for all SNR_x with or without leakage, and so does DRP without leakage. With some leakage, both DRP and SVD-CEF can have rather small KERs at a high SNR_x. In principle, the leakage for DQ does not reduce the secrecy of the key assuming statistical independence of the entries in $\mathbf{x}_A$. But the leakage for DRP and SVD-CEF potentially does due to the use of CEF. But unlike DRP, SVD-CEF is hard to invert from y_k [30], and hence the leakage for SVD-CEF is hard to be exploited by attacker. For pruned SVD-CEF, the realizations of $\mathbf{Q}_{1:K,1:N}$ with $\eta_{k,\mathbf{x}_A} > 2.5$ were dropped. Note that the quality of the keys from DRP in terms of the peak correlation was shown to be bad. It is shown next that DRP also fails on standardized randomness tests.

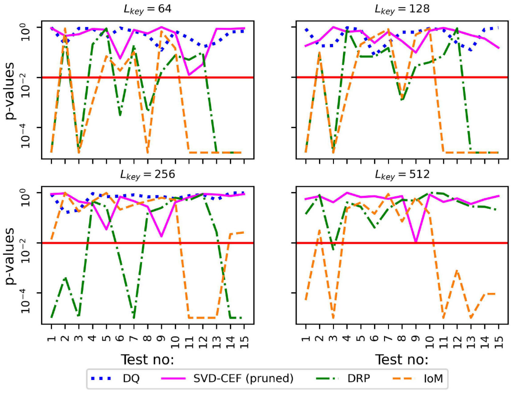

Fig. 3. The p-values of 15 randomness tests.

4) Randomness Tests: Finally, we consider 15 tests of randomness [33]: T1-Frequency test (monobit); T2-Frequency test within a block; T3-Run Test; T4-Longest Run of ones in a block; T5-Binary matrix rank test; T6-Discrete Fourier transform (spectral) test; T7-Non-overlapping template matching test; T8-Overlapping template matching test; T9-Maurer's universal statistical test; T10-Linear complexity test; T11-Serial test A; T12-Serial test B; T13-Approximate entropy test; T14-Cummulative sums (forward) test; T15-Cummulative sums (reverse) test. Each test was done on a binary sequence of RL_{key} bits, consisting of concatenated R keys from R realizations of $\mathbf{x} \sim \mathcal{N}(0, \mathbf{I}_N)$ with $R = 4 \times 10^4$ and $N = 16$ (and all other parameters are fixed). The p-values of these tests are shown in Fig. 3. We see that DRP and IoM failed on a number of tests while DQ and SVD-CEF pass all tests with their p-values larger than 0.01. More interestingly, for $L_{key} = 512$, while DQ could not deliver any key, the key from SVD-CEF still passed all randomness tests (including the random excursions test [33] not shown here).

IV. CONCLUSION

We have presented a novel method for SKG. Simulation results show that at a moderate or high SNR, subject to a required quality of key randomness, and comparing to other methods based on DQ, DRP and IoM, the proposed method called CEbQ has the best reliability in terms of KER. The main reason for this improved reliability is that after continuous encryption, a lower rate quantizer per encrypted sample can be applied without reduction of key size. Furthermore the SVD-CEF used with CEbQ is a good QCPRNs-generator, which ensures a good randomness of a long key generated from a secret vector of a limited dimension. A controlled leakage for both DRP and SVD-CEF due to over-quantization yields a major improvement or reduction of KER. Future research on the security impact of such leakage is needed.

References

[1] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Rexnik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. MobiCom: Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 128–139.

[2] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[3] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[4] C. Huth, R. Guillaume, T. Strohm, P. Duplys, and I. A. Samuel, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 109, pp. 84–104, 2016.

[5] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[6] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, Jul. 2018.

[7] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 18–33, Jan. 2019.

[8] W. Xu, S. Jha, and W. Hu, "LoRa-Key: Secure key generation system for LoRa-based network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6404–6416, Aug. 2019.

[9] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2692–2705, 2020.

[10] D. Guo, K. Cao, J. Xiong, D. Ma, and H. Zhao, "A lightweight key generation scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12137–12149, Aug. 2021.

[11] Z. Ji *et al.*, "Wireless secret key generation for distributed antenna systems: A joint space-time-frequency perspective," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 633–647, Jan. 2022.

[12] G. Li, Y. Xu, W. Xu, E. Jorswieck, and A. Hu, "Robust key generation with hardware mismatch for secure MIMO communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 5264–5278, 2021.

[13] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar. 2003.

[14] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[15] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2008, pp. 3013–3016.

[16] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[17] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[18] L. Huang, D. Guo, J. Xiong, and D. Ma, "An improved CQA quantization algorithm for physical layer secret key extraction," in *Proc. Int. Conf. Wireless Commun. Signal Process.*, 2020, pp. 829–834.

[19] G. Li, C. Sun, E. A. Jorswieck, J. Zhang, A. Hu, and Y. Chen, "Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 968–982, 2021.

[20] FIPS 197, "Advanced encryption standard (AES)," vol. 197, Nov. 2001.

[21] A. B. J. Teoh and C. T. Young, "Cancelable biometrics realization with multispace random projections," *IEEE Trans. Syst., Man Cybern.*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.

[22] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 1–17, 2008.

[23] E. B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *Proc. IEEE Int. Conf. Biometrics: Theory Appl. Syst.*, 2010, pp. 1–7.

[24] D. V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[25] Z. Jin, Y.-L. Lai, J. Y. Hwang, S. Kim, and A. B. J. Teoh, "Ranking based locality sensitive hashing enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensic Secur.*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[26] S. Kirchgasser, C. Kauba, Y.-L. Lai, J. Zhe, and A. Uhl, "Finger vein template protection based on alignment-robust feature description and index-of-maximum hashing," *IEEE Trans. Biom., Behav., Ident. Sci.*, vol. 2, no. 4, pp. 337–349, Oct. 2020.

[27] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security trade-offs in biometric security systems - Part I: Single use case," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 1, pp. 122–139, Mar. 2011.

[28] H. Boche, R. F. Schaefer, S. Baur, and H. V. Poor, "On the algorithmic computability of the secret key and authentication capacity under channel, storage, and privacy leakage constraints," *IEEE Trans. Signal Process.*, vol. 67, no. 17, pp. 4636–4648, Sep. 2019.

[29] S. Wu and Y. Hua, "Total secrecy from anti-eavesdropping channel estimation," *IEEE Trans. Signal Process.*, vol. 70, pp. 1088–1103, 2022.

[30] Y. Hua and A. Maksud, "Continuous encryption functions for security over networks," Nov. 2021. [Online]. Available: https://arxiv.org/pdf/2111.03163.pdf

[31] Y. Hua, "Reliable and secure transmission for future networks," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2020, pp. 5260–5264.

[32] Y. Hua and A. Maksud, "Unconditional secrecy and computational complexity against wireless eavesdropping," in *Proc. IEEE 21st Int. Workshop Signal Process. Adv. Wireless Commun.*, 2020, pp. 1–5.

[33] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Nat. Inst. Standards Technol.*, Washington, DC, USA, Tech. Rep. 800-22. Revision 1a, Apr. 2010.