<table>
<thead>
<tr>
<th>Title</th>
<th>An information-theoretic security evaluation of a class of randomized encryption schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Oggier, Frédérique; Mihaljevi, Miodrag J.</td>
</tr>
<tr>
<td>Date</td>
<td>2013</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/18744">http://hdl.handle.net/10220/18744</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2013 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<a href="http://dx.doi.org/10.1109/TIFS.2013.2294763">http://dx.doi.org/10.1109/TIFS.2013.2294763</a>].</td>
</tr>
</tbody>
</table>
An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes

Frédérique Oggier and Miodrag J. Mihaljević

Abstract—Randomized encryption techniques, where randomness is used for security enhancement, are considered. We focus on the case where the encrypted data experiences noise, e.g., is transmitted over a noisy channel, within the encoding-encryption paradigm, where the data is first encoded for error correction, before being encrypted for security. We assume that the ciphertext is subject to a corruption equivalent to its transmission through a binary symmetric channel with known probability of error. The enhanced security is based on a dedicated wire-tap channel coding that introduces extra randomness, combined with that of the communication channel noise. The encryption is based on a block-by-block modulo-2 addition between an encoded message vector and a pseudorandom vector. The goal is to enhance the protection of the secret key employed in the encryption algorithm.

Security evaluations of this model are performed employing an information-theoretic approach. Assuming a passive as well as an active attacker, we show that there is a threshold before which the wire-tap encoder guarantees an information-theoretic security (during which the equivocation of the secret key is increased), and after which the uncertainty reduces, entering a regime in which a computational security analysis is needed for estimating the computational complexity resistance against the secret key recovery.

Index Terms—Randomized Encryption; Error-Correction Coding; Homophonic Coding; Wire-tap Channel Coding; Information-Theoretic Security Evaluation.

I. INTRODUCTION

USEFULNESS of involving pure randomness into cryptographic primitives for enhancing their security has been recognized in a number of reported designs (see e.g., [26] and [32]), and in the context of wire-tap coding.

A wire-tap channel [33] is a communication system where the legitimate users communicate in the presence of a wire-tapper, and it is assumed that the channel between legitimate parties has higher capacity (lower noise) compared to the one faced by the wire-tapper. Appropriate coding techniques, referred to as wire-tap channel coding, exploit the difference of noise levels in order to provide confidential communications between legitimate parties. Wire-tap channel coding [33] is based on assigning multiple codewords to the same information vector. From that point of view, when the main channel is noise-free, it shares the same underlying idea as homophonic coding (see [14] and [19]), and wire-tap coding can also be seen as combining homophonic and error-correction coding. Wire-tap channel coding for securing noisy communications has been considered for example in [28], [11] and [29].

F. Oggier is with the Division of Mathematical Sciences, Nanyang Technological University, Singapore.
M. Mihaljević is with the Mathematical Institute, Serbian Academy of Science, Belgrade, Serbia, and with the Chuo University, Research and Development Initiative, IMAI Laboratory, Tokyo, Japan.

Randomized Encryptions. The cryptographic primitive of interest in this paper is randomized encryption. In [26], several approaches for including randomness in encryption techniques have been discussed mainly regarding block and stream ciphers. Randomized encryption is described [26] as a procedure which enciphers a message by randomly choosing a ciphertext from a set of ciphertexts corresponding to the message under the current encryption key, and it is claimed that “At the cost of increasing the required bandwidth, randomized encryption procedures may achieve greater cryptographic security than their deterministic counterparts ...”. Note that “randomized encryption” is an alternative term for “probabilistic encryption”, which is usually associated with semantic security.

Recently, joint employment of randomness and dedicated coding has been reported for enhancing the security of the following block-by-block encryption schemes: (i) in [21], where the basic keystream generator security is enhanced by employing a particular homophonic coding based on embedding of random bits; (ii) in [22], [24] and [25] where randomness and wire-tap channel coding have been employed for enhancing the security of the compact generators of pseudorandom vectors; (iii) in [30], [16], [17] and [31] where wire-tap channel coding is employed to increase the security of a DES block cipher operating in the ciphertext feedback (CFB) mode. Security improvements provided by (i)-(iii) include resistance against the generic time-memory trade-off [12] based attacks, and its generalizations and improvements including time-memory-data trade-off approach [3] and its variants (see [20], for example). Particularly, (i)-(ii) provide resistance against the decoding based cryptanalysis (see [5], for example), and (iii) provides resistance against the linear cryptanalysis [18]. All these reported results show that appropriate randomness and dedicated coding enhance cryptographic security in the computational complexity sense, and all were established in the context of the encoding-encryption paradigm.

The Encoding-Encryption Paradigm. There are two ways of handling encoding and encryption together: it is a common practice to first encrypt the data to ensure its safety, and then to encode it for reliability, though there are actually many real life applications where the reverse is done (e.g. the most widespread standard for mobile telephony GSM, standing for “Global System for Mobile Communications” [7], [6]), namely, the data is encoded first, and then encrypted, which we call the encoding-encryption paradigm. From a security perspective, there are of course pros and cons to the encoding-encryption paradigm. Since it implies encryption of redundant data (introduced by error-correction), it could be an origin for mounting attacks against the employed keystream generator.
Undesirability of redundant data from a cryptographic security point of view has indeed been already pointed out in the seminal work by Shannon [27]. On the other hand, the encoding-encryption paradigm has the advantage to offer additional protection in the case of a known plaintext attacking scenario, since an adversary can only learn a noisy version of the keystream (because decoding, i.e., error correction cannot be performed over the ciphertext), which makes the cryptanalysis of the employed keystream generator more complex.

Motivation. Many recent randomized encryption schemes (e.g., approaches (i)-(iii) mentioned above) have in common to exploit randomness and wire-tap coding (or a concatenation of homophonic and error-correction coding) in the context of the encoding-encryption paradigm. The motivation of this work is to propose a general common framework to analyze the security of this class of randomized encryption schemes from an information-theoretic point of view. To evaluate the security of systems using the encoding-encryption paradigm, both computational and information theoretical analyses are valid. In this paper, we focus on the latter, and consider the level of unconditional security implied by the posterior uncertainty about the secret key which an attacker must face, and which is independent of its computational ability. This level of unconditional security is characterized by the classical concept of equivocation which describes the posterior uncertainty of the secret key when a plaintext and corresponding ciphertext are given. Note in particular that the positive equivocation does not yield that the posterior uncertainty is equal to the entropy of the secret key, i.e., that the so-called perfect security introduced by Shannon [27] is achieved. A preliminary study of the security enhancement has been provided in [23] in the case of a passive adversary. We extend the adversary model as explained now.

Types of Adversaries. Security evaluation can be performed under two attacking scenarios, depending on whether one considers an active or passive adversary. A passive adversary’s ability is limited to monitoring (and recording) communications between the legitimate parties, so as to use the recorded data as input for mounting a known plaintext attack against the considered system. Stronger attacks come from active adversaries, which are capable of altering the data. In order to have a relevant model of active adversary, we adopt one which is motivated by the class of so-called Hopper and Blum (HB) authentication protocols [13], [15],[10],[9], which is suitable in the context of authentication and encryption algorithms where the noise is involved for the security enhancement. Following the original work by [13], HB authentication protocols are challenge-response based, where the response could be considered as the encoded and encrypted version of the challenge, which is deliberately degraded by random noise. A simple active attack on the improved HB+ authentication protocol [15] was provided in [8], where it is assumed that an adversary can manipulate challenges sent during the authentication exchange, and thus learn whether such manipulations give an authentication failure. The attack consists of choosing a constant vector and using it to perturb the challenges by computing the XOR of the selected vector with each authentication challenge vector, and that for each of the authentication rounds. To summarize, in this paper, we will assume that an active attacker has the following abilities: (i) he can modify the data in the communication channel between the legitimate parties; and (ii) he can learn the effect of the performed modification at the receiving side.

Summary of the Results. A model of randomized encryption schemes is pointed out, that encompasses several recently reported encryption techniques which have in common to provide enhanced security by involving randomness and a dedicated coding based on wire-tap channel coding or homophonic and error-correction coding. An information theoretic analysis reveals that the security of the model falls into two regimes. In the first regime, the addition of a dedicated coding provides an unconditional (and thus enhanced) security, by increasing the amount of uncertainty that the adversary must face about the secret key given all the information he could gather during different passive or active attacks he can mount. If the same secret key is used over a long period of time, the adversary gathers large enough a sample for cryptanalysis, and the uncertainty tends to zero, entering a regime in which a computational security analysis is needed for estimation of the resistance against the secret key recovery. Particularly, Lemmas 1 and 2 show tight lower bounds on the equivocation, and Theorems 1 and 2 point out the gain implied by employment of pure randomness and the asymptotic values of the equivocation. Finally, we discuss how the addition of a wire-tap encoder can enhance the security of systems using the encoding-encryption paradigm. Our goal is to increase security however by keeping a slight/moderate increase of the implementation complexity and the communications overhead.

Organization of the Paper. In Section II, a common model is established for a number of recently reported block-by-block encryption schemes which involve randomness and dedicated coding. The security analysis is done in two parts: first the passive adversary is studied in Section III, while the active one is investigated in Section IV. Practical implications of the given security analysis and some guidelines for design of security enhanced encoding-encryption based systems are pointed out in Section V. Concluding remarks including some directions for future work are given in Section VI.

II. Model

This section defines a common model for the randomized encryption schemes proposed and discussed in [21], [22], [24], [25], [30], [16] and [17].

The proposed model of encryption scheme integrates the following main underlying ideas for enhancing security:

- Joint employment of extra randomness together with a dedicated wire-tap encoder. This results in a decoding complexity without knowledge of the secret key approaching the complexity of exhaustive search for the secret key.
- A suitable trade-off between the security and the communications rate: Increase the security towards the limit implied by the secret-key length at the expense of a low/moderate decrease of the communications rate.

Since the proposed model exploits both the underlying approaches of universal homophonic coding [19] and generic
wire-tap coding when the main channel is error-free (see [33] and [28], for example), we may say either “concatenation of homophonic and error correction coding” or “wire-tap channel coding” to address the dedicated coding that enhances the security. The main feature of the dedicated coding is that the encoding is based on randomness and that the legitimate receiving party who shares a secret key with the corresponding transmitting one can perform decoding without knowledge of the randomness employed for the encoding. For simplicity, we mainly say “wire-tap channel coding” to describe the dedicated coding which provides the enhanced security.

Let $C_H(\cdot)$ denote a homophonic code encoder. To enhance the security of the system considered, it is added at the transmitter end (see Figure 1) involving a vector of pure randomness

$$u = [u_i]_{i=1}^{m-l} \in \{0,1\}^{m-l},$$

that is, each $u_i$ is the realization of a random variable $U_i$ with distribution $Pr(U_i = 1) = Pr(U_i = 0) = 1/2$.

It is important to note here that though we assume the addition of pure randomness in the wire-tap encoder, we will discuss later on the effect of adding instead pseudo-random bits, or random bits coming from the implementation itself.

Note that $C_H(\cdot)$ is invertible. The wire-tap encoding is done prior to the error-correcting encoder $C_{ECC}(\cdot)$, thus out of the $m$ bits of data to be sent, $m - l$ are replaced by the random vector $u$, letting actually only $l$ bits

$$a = [a_i]_{i=1}^{l} \in \{0,1\}^{l}$$

of plaintext, to get

$$C_{ECC}(C_H(a||u)) \in \{0,1\}^n$$

and finally

$$y = y(k) = C_{ECC}(C_H(a||u)) \oplus x \quad (1)$$

as the codeword to be sent, where $x = x(k) = [x_i]_{i=1}^{n}$ is a pseudorandom vector used for encryption, and $\oplus$ denotes XOR or modulo 2 addition. The vector $x$ could be generated by keystream generator or by a block cipher working in the cipher feedback mode (CFB) as considered in [30], [16], [17] and [31].

We denote the noise vector by

$$v = [v_i]_{i=1}^{n} \in \{0,1\}^n$$

where each $v_i$ is the realization of a random variable $V_i$ such that $Pr(V_i = 1) = p$ and $Pr(V_i = 0) = 1 - p$. Accordingly the receiver obtains

$$z = z(k) = y \oplus v = C_{ECC}(C_H(a||u)) \oplus x \oplus v \quad (2)$$

and starts with the decryption

$$y = (C_{ECC}(C_H(a||u)) \oplus x \oplus v) \oplus x = C_{ECC}(C_H(a||u)) \oplus v.$$ 

He then first decodes $C_H(a||u)$.

If the decoding is successful, he computes $a$ using $C_H^{-1}$ and let the transmitter know he could decode. Otherwise he informs the transmitter that retransmission is required. This is done by assuming that there is a noiseless feedback link that connects the receiver to the transmitter.

\[ \text{secret key} \quad \begin{array}{c} k \end{array} \]
\[ \text{algorithm for generation of pseudorandom vectors} \]
\[ a \]
\[ \text{homophonic + error-correction encoding (or wire-tap channel encoding)} \]
\[ x \]
\[ u \]
\[ \text{randomness} \]
\[ y \]
\[ z \]
\[ \text{cipher text} \]
\[ \text{noise} \]

\[ \text{secret key} \quad \begin{array}{c} k \end{array} \]
\[ \text{algorithm for generation of pseudorandom vectors} \]
\[ a \]
\[ \text{homophonic + error-correction decoding (or wire-tap channel decoding)} \]
\[ x \]
\[ u \]
\[ \text{cipher text} \]

\[ \text{Fig. 1. Model of a security enhanced randomized encryption within the encoding-encryption paradigm.} \]

Remark 1: Note that optionally, the algorithm for pseudo-random vectors generation provides a control sequence for the encoder and decoder.

Remark 2: Note also that in practice a keystream generator can be considered as a finite state machine whose initial state is determined by the secret key and some public data. For simplicity, and because it does not affect our analysis, we can consider the existence of the public data, and focus on the secret key. In this setting the output of the keystream generator is determined uniquely by the secret key, and it is enough to assume that the transmitter and receiver only share the key.

Similarly to a linear error-correction code where $C_{ECC}$ can be represented by multiplying the data vector by an $m \times n$ binary generator matrix $G_{ECC}$ of the code, we can write $C_H$, following the so-called coset encoding proposed by Wyner [33], as follows:

$$C_H(a||u) = [a||u]G_H,$$ 

where

- $G^C$ is an $(m-l) \times m$ generator matrix for an $(m, m-l)$ linear error-correction code $C$ with rows $g_1^C, g_2^C, \ldots, g_{m-l}^C$,
- $h_1, h_2, \ldots, h_l$ are $l$ linearly independent row vectors from $\{0,1\}^m \backslash C$,
- $G_H$ is an $m \times m$ binary matrix corresponding to $C_H(\cdot)$.

In words, to each $l$-bit message $a = [a_1, \ldots, a_l]$ is associated a coset determined by

$$a \mapsto a_1h_1 \oplus a_2h_2 \oplus \ldots \oplus a_lh_l \oplus C.$$

Though this correspondence is deterministic, a random codeword $c$ is chosen inside the coset by:

$$c = a_1h_1 \oplus a_2h_2 \oplus \ldots \oplus a_lh_l \oplus u_1g_1^C \oplus u_2g_2^C \oplus \ldots \oplus u_{m-l}g_{m-l}^C.$$
where \( \mathbf{u} = [u_1, u_2, \ldots, u_{m-l}] \) is a uniformly distributed random \((m-l)\)-bit vector. Finally
\[
C_{ECC}(C_H(\mathbf{a}|\mathbf{u})) = C_{ECC}(\mathbf{a}|\mathbf{u})\mathbf{G}_H = \mathbf{a}|\mathbf{u}\mathbf{G}_H\mathbf{G}_{ECC} = \mathbf{a}|\mathbf{u}\mathbf{G}
\]
where \( \mathbf{G} = \mathbf{G}_H\mathbf{G}_{ECC} \) is an \(m\times n\) binary matrix summarizing the two successive encodings at the transmitter.

Since \( \mathbf{G}_H \) multiplies the vector \( \mathbf{a}|\mathbf{u} \) where \( \mathbf{a} \) is an \( l\)-dimension vector and \( \mathbf{u} \) an \((m-l)\) dimension vector, it makes sense to write the \( m \times m \) matrix \( \mathbf{G}_H \) by blocks of size depending on \( l \) and \( m-l \):
\[
\mathbf{G}_H = \begin{bmatrix} \mathbf{G}_H^{(1)} & \mathbf{G}_H^{(2)} \\ \mathbf{I}_{m-l} & \mathbf{G}_H^{(3)} \end{bmatrix}
\]
where \( \mathbf{G}_H^{(1)} \) is an \( l \times (m-l) \) matrix, \( \mathbf{G}_H^{(2)} \) is an \( l \times l \) matrix, \( \mathbf{I}_{m-l} \) denotes the \((m-l) \times (m-l)\) identity matrix, and finally \( \mathbf{G}_H^{(3)} \) is an \((m-l) \times l \) matrix.

III. Security against a Passive Adversary

This section analyzes the security of the proposed scheme against a passive adversary, that is an adversary limited to monitoring and recording communications. The system we consider already uses a generator of pseudorandom vectors (controlled by the secret key) to protect the confidentiality of the data. Thus although a passive adversary may try to discover confidential messages, more dangerous is an attack against the secret key, which would endanger all the transmissions. Based on what a passive adversary can do, this means mounting a plaintext attack in order to recover the secret key. In the passive known plaintext attack scenario, with no enhanced security, the adversary possesses the pair
\[
(\text{plaintext, noisy ciphertext}) = (\mathbf{a}, \mathbf{z} = C_{ECC}(\mathbf{a}) \oplus \mathbf{x} \oplus \mathbf{v}),
\]
from which he calculates
\[
C_{ECC}(\mathbf{a}) \oplus \mathbf{z} = \mathbf{x} \oplus \mathbf{v}.
\]
He can then use \( \mathbf{x} \oplus \mathbf{v} \) for further processing in an attempt to recover the key which generated \( \mathbf{x} \). We will show how the introduction of the wire-tap encoding increases the protection of the key against such attacks.

In what follows, we set that
- \( u_i \): random bits used in the wire-tap encoder,
- \( x_i \): output bits of the keystream generator,
- \( v_i \): random components of the additive noise are realizations of certain random variables \( U_i, X_i \) and \( V_i \), respectively, \( i = 1, 2, \ldots, n \). We can further assume that the plaintext is generated randomly, and thus see \( a_i \) as a realization of a random variable \( A_i \) as well. The corresponding vectors of random variables are denoted as follows: \( A^l = [A_i]_{i=1}^l, U^{m-l} = [U_i]_{i=1}^{m-l}, X^n = [X_i]_{i=1}^n \) and \( V^n = [V_i]_{i=1}^n \).

Recall from (2) and (4) that the received vector at the receiver is given by
\[
\mathbf{z} = C_{ECC}(C_H(\mathbf{a}|\mathbf{u})) \oplus \mathbf{x} \oplus \mathbf{v} = [a_i|u_i]G \oplus x \oplus v
\]
where \( \mathbf{G} = [g_{i,j}]_{i=1}^m_{j=1} \) is an \(m \times n\) matrix containing both the wire-tap and the error correction encoding.

Let \( \mathbf{z} = [z_i]_{i=1}^n \), so that \( \mathbf{z} \) can be written componentwise as
\[
z_i = (\bigoplus_{k=1}^l g_{k,i}a_k) + (\bigoplus_{k=1}^{m-l} g_{k+l,i}u_k) + x_i \oplus v_i, \quad i = 1, 2, \ldots, n,
\]
and \( z_i \) appears as the realization of a random variable \( Z_i \):
\[
Z_i = ((\bigoplus_{k=1}^l g_{k,i}A_k) + (\bigoplus_{k=1}^{m-l} g_{k+l,i}U_k) + X_i) \oplus V_i, \quad i = 1, 2, \ldots, n.
\]
We further denote \( \mathbf{Z}^n = [Z_i]_{i=1}^n \), and
\[
\mathbf{Z}^n = C_{ECC}(C_H(A^l||U^{m-l})) \oplus \mathbf{X}^n \oplus \mathbf{V}^n.
\]
From (5), we have
\[
C_H(A^l||U^{m-l}) = [A^l, U^{m-l}] \mathbf{G}_H = [A^l, U^{m-l}] \begin{bmatrix} \mathbf{G}_H^{(1)} & \mathbf{G}_H^{(2)} \\ \mathbf{I}_{m-l} & \mathbf{G}_H^{(3)} \end{bmatrix}
\]
and we can rewrite the wire-tap encoder as
\[
C_H(A^l||U^{m-l}) = C_{H,a}(A^l) \oplus C_{H,u}(U^{m-l}),
\]
where \( C_{H,a} \) and \( C_{H,u} \) are the operators for the wire-tap encoding restricted to \( a \), resp. \( u \):
\[
C_{H,a}(A^l) = [A^l \mathbf{G}_H^{(1)}, A^l \mathbf{G}_H^{(2)}], \quad C_{H,u}(U^{m-l}) = [U^{m-l}, U^{m-l} \mathbf{G}_H^{(3)}].
\]
Since the error correcting encoding is linear, we finally get
\[
\mathbf{Z}^n = C_{ECC}(C_{H,a}(A^l)) \oplus C_{ECC}(C_{H,u}(U^{m-l})) \oplus \mathbf{X}^n \oplus \mathbf{V}^n.
\]

Our main results for the case of a (passive) known plaintext attack are given in Lemma 1 and Theorem 1 below. The purpose of Lemma 1 is to justify that the considered encryption model provides a certain level of the posterior uncertainty about its secret elements (i.e., positive equivocation) assuming that the sample for cryptanalysis is (very) short. Theorem 1 next shows that this positive equivocation cannot be preserved, when the sample for cryptanalysis increases, and that it tends to zero assuming a large enough sample implying that the uncertainty about the secret key employed in the keystream generator tends to zero, i.e., it can be correctly recovered by (potentially hard) computational efforts. The analog statements correspond to Lemma 2 and Theorem 2 to be discussed in the next section in the context of an active and known plaintext security evaluation scenario.

The lemma below gives an estimation on the resistance of the scheme to a known plaintext attack where the adversary knows the pair \((\mathbf{a}, \mathbf{z})\).

**Lemma 1:** When \( H(X^n) = n \geq H(U^{m-l}) + H(V^n) \),
the equivocation of the keystream output knowing the plaintext and the received signal fulfills the following tight lower bound:
\[
H(X^n|A^l, \mathbf{Z}^n) \geq H(U^{m-l}) + H(V^n) - \delta(C_{ECC}),
\]
\(^1\)Note that \( H(X^n) = n \) is equivalent to say that each \( X_i \) takes value 0 or 1 with probability 1/2.
where for a given positive $\epsilon \to 0$

$$\delta(C_{ECC}) = H(\epsilon) + \epsilon \log(2^{m-l} - 1) \to 0.$$  

Proof: Employing the entropy chain rule, we have that

$$H(A^l, U^{m-l}, X^n, V^n, Z^n)$$

$$= H(A^l) + H(Z^n|A^l) + H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, X^n, U^{m-l}, Z^n)$$

$$= H(A^l) + H(Z^n|A^l) + H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, X^n, U^{m-l}, Z^n)$$

$$= H(A^l) + H(Z^n|A^l) + H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, X^n, U^{m-l}, Z^n),$$

noticing that $H(V^n|A^l, U^{m-l}, X^n, Z^n) = 0$ using again $V^n = C_{ECC}(C_H(A^l|U^{m-l})) \oplus Z^n \oplus X^n$ from (6).

Repeating the entropy chain rule but with another decomposition, we further get that

$$H(A^l, U^{m-l}, X^n, V^n, Z^n)$$

$$= H(A^l) + H(Z^n|A^l) + H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, X^n, U^{m-l}, Z^n)$$

$$= H(A^l) + H(Z^n|A^l) + H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, X^n, U^{m-l}, Z^n),$$

noticing that $H(V^n|A^l, U^{m-l}, X^n, Z^n) = 0$ using again $V^n = C_{ECC}(C_H(A^l|U^{m-l})) \oplus Z^n \oplus X^n$ from (6).

By combining the two decompositions under the lemma assumption that $H(X^n) \geq H(U^{m-l}) + H(V^n)$, we deduce that

$$H(X^n|A^l, Z^n)$$

$$= H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, U^{m-l}, Z^n)$$

$$- H(U^{m-l}|A^l, X^n, Z^n).$$

We now reformulate $H(U^{m-l}|A^l, Z^n)$ and $H(V^n|A^l, U^{m-l}, Z^n)$ as follows.

For $H(U^{m-l}|A^l, Z^n)$, using (7), we have that

$$C_{ECC}(C_{H,u}(U^{m-l})) = C_{ECC}(C_{H,a}(A^l)) \oplus Z^n \oplus X^n \oplus V^n,$$

where $X^n \oplus V^n$ can take $2^{H(X^n \oplus V^n)}$ different values, and $H(C_{ECC}(C_{H,u}(U^{m-l}))) = H(C_{ECC} \oplus C_H)$ since $C_{ECC}$ and $C_H$ are invertible. Accordingly, taking into account that conditioning does not increase entropy we have

$$H(U^{m-l}|A^l, Z^n) \leq \min\{H(U^{m-l}), H(X^n \oplus V^n)\},$$

and the lemma assumption that $H(X^n) = n$ implies,

$$H(U^{m-l}|A^l, Z^n) = H(U^{m-l}).$$

Similarly, again using (7) to get that

$$V^n = C_{ECC}(C_{H,u}(U^{m-l})) + C_{ECC}(C_{H,a}(A^l)) \oplus Z^n \oplus X^n$$

we obtain that

$$H(V^n|A^l, U^{m-l}, Z^n) \leq \min\{H(V^n), H(X^n)\},$$

and the lemma assumption yields,

$$H(V^n|A^l, U^{m-l}, Z^n) = H(V^n).$$

We are finally left with bounding $H(U^{m-l}|A^l, X^n, Z^n)$. Recovering $U^{m-l}$ when $A^l, X^n$ and $Z^n$ are given is the decoding problem of removing the noise $V^n$ employing the code $C_{ECC}$ with the error probability $P_e = \epsilon$. This can be bounded using Fano’s inequality:

$$H(U^{m-l}|A^l, X^n, Z^n) \leq H(P_e) + P_e \log(2^{m-l} - 1)$$

$$\leq H(\epsilon) + \epsilon \log(2^{m-l} - 1) \to 0$$

since by design of the system, we may assume $\epsilon \to 0$. Note that no inequality was used before Fano’s equality, which is known to provide a tight lower bound on the error probability in terms of the entropy [4]. This concludes the proof.

Lemma 1 can be interpreted as a bound on the resistance of the scheme to a passive known plaintext attack and it depends on the following:

a) The keystream generator: if the output of the keystream generator has the highest entropy $H(X^n) = n \geq H(U^{m-l}, V^n) = H(U^{m-l}) + H(V^n)$, then the lemma yields

$$H(X^n|A^l, Z^n) \geq H(U^{m-l}) + H(V^n) - \delta(C_{ECC}).$$

b) The involved randomness: the considered scheme involves two random vectors $u$ and $v$ (see (2)) which are realizations of the random variables $U^{m-l}$ and $V^n$ with entropy $H(U^{m-l})$ and $H(V^n)$, respectively, such that $H(U^{m-l}) \leq m-l$, $H(V^n) < n$, and $H(U^{m-l}) + H(V^n) < n$. Note that although $H(U^{m-l}) = m-l$ could be employed, corresponding to pure/uniform randomness, this is not a necessary request. In order to achieve decoding with an arbitrary small probability of decoding error, we need $H(V^n) \ll n$. Accordingly, $u$ and $v$ can be generated by a simple source of randomness, and in certain scenarios employing the channel noise only or/and the environmental noise. Particularly note that without employment of $u$, Lemma 1 shows that

$$H(X^n|A^l, Z^n) \geq H(V^n)$$

that is the information-theoretic security of the keystream depends on the channel noise. We stress that the proof of Lemma 1 does not require that we involve pure randomness, and involvement of any randomness would increase the security level as well. Accordingly, the contribution of the extra randomness through the vector $u$ is given by $H(U^{m-l})$. We illustrate the last claim with an example.

Example 1: Consider the case of a known plaintext attack when $a = 0$. We then have

$$z_i = x_i \oplus \bigoplus_{k=1}^{m-l} g t_{k,i} u_k \oplus v_i, \ i = 1, 2, ..., n.$$  

Without the homophonic encoding, the keystream $x_i$ is corrupted and so protected as well by the noise on the channel, while with addition of the homophonic encoder, it is further protected by the pure randomness involved in homophonic encoding.

Also note that the entropy of a block of keystream, given only the corresponding block of ciphertext (not the plaintext), can be no larger than $m + H(V^n)$, and $H(V^n) < n - m$ in order to make the error correction possible. In practice, the noise $V^n$ is often less powerful than one with entropy $n - m$,
which results in information leakage about the keystream from the ciphertext. Such an attack is described for GSM in [1].

The special case where the channel is noisefree is detailed in the corollary below. This further illustrates the effect of pure randomness involved in the wire-tap channel coding.

**Corollary 1:** In a noisefree channel when \( H(X^n) = n > H(U^{m-\ell}) \),
\[
H(X^n|A^l, Z^n) = H(U^{m-\ell}).
\]

**Proof:** Since the channel is noisefree, \( v^n = 0 \) and consequently \( H(V^n) = P_e = 0 \). Accordingly, Lemma 1 directly implies the corollary statement.

Also note that when \( x^n \) is the realization of a random vector where ones and zeros appear with the same probability equal to \( 1/2 \), Corollary 1 follows from the situation where we have a system of \( n + (m - \ell) \) variables which directly implies that there are \( 2^{m-\ell} \) equally likely solutions.

So far, we have discussed the security of a given keystream generator output, for one instance of transmission. We now move to a more realistic scenario. Transmission takes place over time \( t = 1, 2, \ldots \), and the keystream generator uses a secret key \( K \) based on which it computes its outputs \( X(t) = [x(t)_i]_{i=1}^{\ell} \) in a deterministic way depending on \( f \) for a time period of length \( \tau \):
\[
X(t) = X(t)(K) = f(t)(K), \ t = 1, \ldots, \tau.
\]
Note that \( f(t)(K) \) is an expansion of the secret key \( K \) via a finite state machine and can be considered as an encoding of \( |K| \) bits into a long binary codeword. Correspondingly, we can rewrite the whole system in terms of realizations of random variables that depends on time, over the time interval \( t = 1, \ldots, \tau \):
- \( A(t) = [A(t)_i]_{i=1}^{\ell} \) for the plaintext,
- \( U(t) = [U(t)_i]_{i=1}^{m-\ell} \) for the pure randomness used in the wire-tap encoder,
- \( V(t) = [V(t)_i]_{i=1}^{n} \) for the channel noise,
- \( Z(t) = [Z(t)_i]_{i=1}^{n} \) for the received signal.

Similarly as above, we have
\[
Z(t) = C_{ECC}(C_{H,a}(A(t)) \oplus C_{H,u}(U(t))) \oplus f(t)(K) \oplus V(t).
\]

The key \( K \) is represented as a vector of random variables drawn independently from a uniform distribution over \( \{0,1\} \), so that \( H(K) = |K| \). We further use the following block notations:
\[
A^l = \{A(1)|[A(2)|\ldots|A(\tau)\}
\]
\[
U^{m-\ell} = \{U(1)|[U(2)|\ldots|U(\tau)\}
\]
\[
V^n = \{V(1)|[V(2)|\ldots|V(\tau)\}
\]
\[
Z^n = \{Z(1)|[Z(2)|\ldots|Z(\tau)\}.
\]

We can now state the main theorem of this section, which describes the security of the enhanced system against a passive adversary regarding the secret key recovery and points out the impacts of involving pure randomness via dedicated coding.

**Theorem 1:** Let \( H^*(K|A^l, Z^n) \) denote \( H(\cdot) \) in the special case when \( m = l \), i.e. when the pure random bits are not involved. When \( \Pr(V(i)^{(j)} = 0) = 1 - \Pr(V(i)^{(j)} = 1) = 1 - p > 1/2, i = 1, 2, \ldots, n, j = 1, 2, \ldots, \tau \), we have
\[
H(K|A^l, Z^n) - H^*(K|A^l, Z^n) = H(U^{m-l}|A^l, Z^n) - H(U^{m-l}|A^l, K, Z^n),
\]
and there exists a threshold \( \tau_{\text{thres}} \) such that
\[
H(K|A^l, Z^n) \begin{cases} > 0 & \tau < \tau_{\text{thres}} \\ \rightarrow 0 & \tau \geq \tau_{\text{thres}} \end{cases},
\]
assuming that \( n \leq |K| \ll \tau_{\text{thres}} \) and \( \tau_{\text{thres}} \) is not too large compared to \( n/2 \).

**Proof:** Using two different decompositions of \( H(A^l, U^{m-l}, X^n, V^n, Z^n) \) via the entropy chain rule as done in Lemma 1, we get
\[
H(K|A^l, Z^n) = H(U^{m-l}|A^l, Z^n) + H(V^n|A^l, U^{m-l}, Z^n) - H(U^{m-l}|A^l, K, Z^n).
\]

This above decomposition directly implies the first theorem claim because, when \( m = \ell \) we have:
\[
H(U^{m-l}|A^l, Z^n) = H(U^{m-l}|A^l, K, Z^n) = 0,
\]
and \( H(V^n|A^l, U^{m-l}, Z^n) \) is independent of any particular realization of \( U^{m-l} \).

The second theorem claim is justified as follows.

When \( \tau = 1 \), \( X(1) = X^n = f(1)(K) \) and accordingly \( H(X(1)) + n \), thus Lemma 1 directly implies that \( H(X^n|A^l, Z^n) = H(K|A^l, Z^n) > 0 \) is achievable.

When \( \tau > 1 \) grows, we employ the following argument. Note that knowing \( A^l, Z^n \) can be considered as a \( \tau n \)-length degraded version of a binary codeword with \( \tau (m - \ell) + |K| \) information bits which is corrupted by a noise vector \( V^n \).

Indeed, without knowing the key, decoding \( U^{m-l} \) is not possible, so the adversary also needs to try to decode \( K \).

Assuming that the decoding error probability of this code is \( P_e \), Fano’s inequality implies
\[
H(U^{m-l}|A^l, Z^n) \leq H(P_e) + P_e \log(2^{m-l}+|K| - 1).
\]

Combining the decoding ability of \( C_{ECC} \) with a minimum distance decoding yields a decoding error for the aggrigated code of size \( 2^{m-l}+|K| \) that tends to zero provided long enough codewords, that is \( P_e \rightarrow 0 \), and accordingly \( H(U^{m-l}|A^l, Z^n) \rightarrow 0 \) when \( \tau \) is large enough.

In a similar manner and employing
\[
H(V^n|A^l, U^{m-l}, Z^n) < H(V^n, K|A^l, U^{m-l}, Z^n),
\]
the decoding ability of \( C_{ECC} \) with a minimum distance decoding as used above implies that
\[
H(V^n|A^l, U^{m-l}, Z^n) \rightarrow 0 \text{ when } \tau \text{ is large enough.}
\]

To take care of \( H(U^{m-l}|A^l, K, Z^n) \), we again use a decoding argument, since \( Z^n \) is known. However, it is important to note here that \( K \) is known too. Thus even though we look at a block
\[
U^{m-l} = [U(1)|[U(2)|\ldots|U(\tau)],
\]
the knowledge of $K$ makes each block $U^{(t)}$ independent, and thus we can decode each of them separately and the probability of error is $P_e^r$. Fano’s equality finally yields

$$H(U^{(m-l)}|A^{rl}, K, Z^{rn}) \leq H(P_e^r) + P_e^r \log(2^{r(m-l)} - 1) \leq H(e^r) + r^l \log(2^{r(m-1)} - 1)$$

and

$$H(U^{(m-l)}|A^{rl}, K, Z^{rn}) \rightarrow 0 \tag{10}$$

since $P_e \rightarrow 0$ by design of $C_{ECC}$.

The above consideration of the cases $r = 1$ and $r > 1$ also implies the existence of a threshold $\tau_{thres}$.

Theorem 1 has different implications. First, together with Lemma 1, it shows that the considered encryption scheme cannot achieve perfect security [27] because the equivocation of the secret key is always smaller than its entropy. Second, it implies that the involvement of randomness increases the uncertainty about the secret key in the passive attack scenario, and that a computational evaluation is required to understand how hard it is for the adversary to recover the key.

Note that all this analysis is true for “realistic channels” where the noise is not uniformly distributed. The uniformly distributed noise in the communication channel makes error-correction infeasible, which explain the assumption in the above theorem.

Theorem 1 directly implies the following corollary for noiseless channels.

**Corollary 2:** When $V^n = 0$ and the parameter $r$ is large enough we have:

$$H(K|A^{rl}, Z^{rn}) = 0. \tag{11}$$

IV. SECURITY AGAINST AN ACTIVE ADVERSARY

There are many possible scenarios for an active adversary. Following the active attack scenarios considered in [8], [9] and [10], in this work we assume that:

1) he can modify the data on the communication channel, that is, inject additional noise,
2) he can learn the effect of the modified channel at the receiving side, by listening to the feedback link that tells whether decoding was successful.

Let us be more precise. While the transmitter sends $y = C_{ECC}(C_H(a||u)) \oplus x$ in an already security enhanced setting (1), the receiver sees its noisy version

$$z = y \oplus v.$$

The active adversary is allowed to inject some extra noise $v^*$ over the channel, so that now, the legitimate receiver sees $y \oplus v^*$, where $v^*$ contains both the noise $v$ coming from the channel and the noise $v^*$ controlled by the adversary:

$$z = y \oplus v \oplus v^* = C_{ECC}(C_H(a||u)) \oplus x \oplus v \oplus v^*. \tag{12}$$

As earlier (Section II), the receiver first decrypts its message using its secret key and locally generated keystream

$$z \oplus x = C_{ECC}(C_H(a||u)) \oplus v \oplus v^*$$

and then try to decode $z \oplus x$:

$$C_{ECC}^{-1}(z \oplus x) = C_{ECC}^{-1}(C_{ECC}(C_H(a||u)) \oplus v \oplus v^*) = C_H(a||u)$$

under the assumption that the error correcting code can correct the errors introduced by $v$, so as to get

$$a = C_{H}^{-1}(C_{ECC}^{-1}(z \oplus x)).$$

Because of the extra noise $v^*$, the probability of decoding correctly at the receiver may decrease. In the meantime, the active attacker can listen to the feedback channel so that he knows whether the decoding failed or was successful. His goal is again to find the key. His strategy then consists in adding different noise vectors $v^*$ and to observe the feedback channel to see whether the chosen noise made the decoding fail, in order to gather information.

We keep our earlier notation, that is

- $u_i$, random bits used in the wire-tap encoder,
- $x_i$, output bits of the keystream generator,
- $v'_i$, random components of the additive noise $v' = v \oplus v^*$,
- $a_i$, bits of the plaintext,
- $z_i$, bits of the received message

are realizations of certain random variables $U_i, X_i, V'_i, V_i, V_i^*$, $Z_i, i = 1, 2, \ldots, n$ and $A_i, i = 1, \ldots, l$. The corresponding vectors of random variables are denoted as follows: $A = [A_i]_{i=1}^l$, $U^{m-l} = [U_i]_{i=1}^{m-l}$, $X^n = [X_i]_{i=1}^n$, $V^n = [V'_i]_{i=1}^n$, $V^n = [V_i]_{i=1}^n$, $V^* = [V_i^*]_{i=1}^n$, and $Z^n = [Z_i]_{i=1}^n$. Similarly to (7),

$$Z^n = C_{ECC}(C_{H,a}(A^l)) \oplus C_{ECC}(C_{H,u}(U^{m-l})) \oplus X^n \oplus V^n \oplus V^* \oplus V^n. \tag{13}$$

Finally, let $f_d$ be a binary flag which indicates whether the decoding result is indeed $a$ or has failed, and accordingly $f_d$ can be considered as a realization of a binary random variable $F_d$.

The lemma below gives a tight bound on the resistance of the scheme to an active attack where the adversary not only controls the noise but also knows $a$, $z$ and $f_d$.

**Lemma 2:** When $H(X^n) = n \geq H(U^{m-l}) + H(V^n|F_d)$, the equivocation of the keystream segment knowing the plaintext, the received signal, and the decoding tag, fulfills the following tight lower bound:

$$H(X^n|A^l, Z^n, F_d) \geq H(U^{m-l}) + H(V^n|F_d) - \delta(C_{ECC}). \tag{14}$$
where for the probability of decoding error $P_e$ to 0,
$$\delta(C_{ECC}) = H(P_e) + P_e \log(2^{m-l} - 1) \to 0.$$

**Proof:** As in Lemma 1, we start with two different chain rule decompositions of the same joint entropy. On the one hand,
$$H(A_l^l, U^{m-l}, X^n, V^n, Z^n, F_d) = H(A_l^l) + H(Z^n|A_l^l) + H(U^{m-l}|A_l^l, Z^n) + H(F_d|A_l^l, U^{m-l}, Z^n) + H(V^n|A_l^l, U^{m-l}, Z^n, F_d) + H(V^n|A_l^l, U^{m-l}, Z^n, F_d),$$

since from (13) we have that $X^n = C_{ECC}(C_H(A_l^l||U^{m-l}))) \oplus Z^n \oplus V^n$ implying $H(X^n|A_l^l, U^{m-l}, V^n, Z^n, F_d) = 0$, and

$$H(F_d|A_l^l, U^{m-l}, Z^n) = 0,$

since $A_l^l$ and $Z^n$, decoding can be performed on $Z$ and the decoded value can be compared to $A_l^l$ yielding $F_d$.

On the other hand,
$$H(A_l^l, U^{m-l}, X^n, V^n, Z^n, F_d) = H(A_l^l) + H(Z^n|A_l^l) + H(X^n|A_l^l, Z^n) + H(F_d|A_l^l, U^{m-l}, X^n, Z^n, F_d) + H(V^n|A_l^l, U^{m-l}, X^n, Z^n, F_d),$$

noticing that $H(V^n|A_l^l, U^{m-l}, X^n, Z^n, F_d) = 0$, again using from (13) that $V^n = C_{ECC}(C_H(A_l^l||U^{m-l}))) \oplus Z^n \oplus X^n$, and

$$H(F_d|A_l^l, U^{m-l}, Z^n) = 0$$

for the same reason as above.

By combining the two decompositions, we deduce that
$$H(X^n|A_l^l, Z^n) = H(U^{m-l}|A_l^l, Z^n, F_d) + H(V^n|A_l^l, U^{m-l}, Z^n, F_d) - H(U^{m-l}|A_l^l, X^n, Z^n, F_d),$$

where
$$H(U^{m-l}|A_l^l, Z^n, F_d) \leq \min\{H(U^{m-l}), H(X^n \oplus V^n|F_d)\}$$

since $C_{ECC}(C_H(U^{m-l})) = C_{ECC}(C_H(A_l^l)) \oplus Z^n \oplus X^n \oplus V^n$, and employing the same arguments as in the corresponding part of Lemma 1 proof, as well as Lemma 2 assumption, we obtain
$$H(U^{m-l}|A_l^l, Z^n, F_d) = H(U^{m-l}).$$

Similarly, again using (13) we obtain that
$$H(V^n|A_l^l, U^{m-l}, Z^n, F_d) \leq \min\{H(V^n|F_d), H(X^n)\},$$

and since Lemma 2 assumption, we have
$$H(V^n|A_l^l, U^{m-l}, Z^n, F_d) = H(V^n|F_d).$$

To summarize, Equation (15) is now given by
$$H(X^n|A_l^l, Z^n) = H(U^{m-l}) + H(V^n|F_d) - H(U^{m-l}|A_l^l, X^n, Z^n, F_d) \text{ where } V^n \to V^n \oplus V^{*n} \text{ and } V^{*n} \text{ is known to the adversary.}$$

We are finally left with bounding $H(U^{m-l}|A_l^l, X^n, Z^n, F_d)$. For the adversary, recovering $U^{m-l}$ when $A_l^l$, $X^n$ and $Z^n$ are given is the decoding problem of removing the noise $V^n$ (he knows $V^{*n}$) employing the code $C_{ECC}$ with error probability $P_e$. This can be bounded using Fano's inequality, which gives a tight bound as in Lemma 1:

$$H(U^{m-l}|A_l^l, X^n, Z^n, F_d) = H(U^{m-l}|A_l^l, X^n, Z^n) \leq H(P_e) + P_e \log(2^{m-l} - 1)$$

since knowing whether the receiver could decode the worst noise does not affect the error capability of $C_{ECC}$. This concludes the proof.

Let us compare the result of Lemmas 1 and 2:

$$H(X^n|A_l^l, Z^n) \geq H(U^{m-l}) + H(V^n) - \delta(C_{ECC}),$$

$$H(X^n|A_l^l, Z^n, F_d) \geq H(U^{m-l}) + H(V^n|F_d) - \delta(C_{ECC}),$$

where
$$\delta(C_{ECC}) = H(P_e) + P_e \log(2^{m-l} - 1) \to 0,$$

since $P_e \to 0$. As expected, the equivocation in the case of an active adversary is smaller than for a passive adversary, since

$$H(V^n|F_d) \leq H(V^n).$$

Based on the above, we easily get a countertop theorem 1 for the case of an active adversary.

**Theorem 2:** Let $H^*(K|A^{τl}, Z^{τn}, F_d)$ denote $H(\cdot)$ in the special case when $m = l$, i.e., when the pure random bits are not involved. When $Pr(V_i^{τ(l)} = 0) = 1 - Pr(V_i^{τ(l)} = 1) = 1 - p > 1/2$, $i = 1, 2, ..., n$, $j = 1, 2, ..., τ$, we have

$$H(K|A^{τl}, Z^{τn}, F_d) - H(K|A^{τl}, Z^{τn}, F_d) = H(U^{τ(m-l)}|A^{τl}, Z^{τn}, F_d) - H(U^{τ(m-l)}|A^{τl}, K, Z^{τn}, F_d),$$

and there exists a threshold $τ_{thres, act}$ such that

$$H(K|A^{τl}, Z^{τn}, F_d) \begin{cases} > 0 & \text{for } τ < τ_{thres, act} \\ \to 0 & \text{for } τ \geq τ_{thres, act} \end{cases},$$

assuming that $n \leq |K| \leq τ_{thres, act} n$ and $τ_{thres, act} n \leq τ_{thres, act} n/2$.

Also we have that $τ_{thres, act} < τ_{thres}$, the threshold for a passive adversary.

**Proof:** When $τ \geq 1$, we know from (9) that

$$H(K|A^{τl}, Z^{τn}, F_d) = H(U^{τ(m-l)}|A^{τl}, Z^{τn}, F_d) + H(V^{τn}|A^{τl}, U^{τ(m-l)}, Z^{τn}, F_d) - H(U^{τ(m-l)}|A^{τl}, K, Z^{τn}, F_d).$$

The above decomposition directly implies the first theorem claim because, when $m = l$ we have:

$$H(U^{τ(m-l)}|A^{τl}, Z^{τn}, F_d) = H(U^{τ(m-l)}|A^{τl}, K, Z^{τn}, F_d) = 0,$$

and $H(V^{τn}|A^{τl}, U^{τ(m-l)}, Z^{τn}, F_d)$ is independent of any particular realization of $U^{τ(m-l)}$.

When $τ = 1$, $X^{(1)} = X^n = f(1)(K)$, Lemma 2 directly implies that $H(X^n|A^l, Z^n, F_d) = H(K|A^l, Z^n, F_d) > 0$ is achievable.

Now it is shown in the proof of Theorem 1 that every term in the above decomposition tends to zero, using a decoding
argument, which will hold similarly here, since the knowledge of \( F_d \) cannot make the decoding more difficult.

Similarly as in the passive attacking scenario, involvement of randomness increases the uncertainty about the secret key in the active attack scenario, but this uncertainty reduces to zero if long enough samples are collected.

V. Practical Implications and Applications Issues

This section provides a generic discussion of the usefulness and possible applications of the proposed approach, to secure a system using the encoding-encryption paradigm by adding a wire-tap encoder.

A. Implications of the security evaluation

The analysis given in Sections III and IV shows that in systems where the encoding-encryption paradigm is employed, an increased cryptographic security can be achieved via a dedicated homophonic and error-correction coding instead of error-correction only. This enhanced security in known-plaintext cryptanalytic scenarios is an implication of the increased equivocation of the secret key.

The performed information-security evaluation more precisely points out the following desirable security properties of the proposed approach: (i) When the sample available for cryptanalysis is below a certain size, the scheme provides uncertainty, that is an information-theoretic security, about the secret key; (ii) Even when the equivocation of the secret key tends to zero which means that the security depends only on the computational complexity of the cryptanalysis, the involved randomness may induce a significantly higher complexity in comparison with that of recovering the secret key without the randomization.

The main consequence of (i) is that independently of the cryptanalytic approach employed, the nonzero equivocation about the secret key implies that even if exhaustive search is employed for the secret key recovery, the number of candidates is large, in fact, it could be so large that the posterior uncertainty of the secret key is hardly reduced in comparison with the prior one. Regarding (ii), note the following two issues which indicate a potential for the claimed increase of the cryptanalytic scenarios is an implication of the increased equivocation of the secret key.

The main consequence of (i) is that independently of the cryptanalytic approach employed, the nonzero equivocation about the secret key implies that even if exhaustive search is employed for the secret key recovery, the number of candidates is large, in fact, it could be so large that the posterior uncertainty of the secret key is hardly reduced in comparison with the prior one. Regarding (ii), note the following two issues which indicate a potential for the claimed increase of the cryptanalytic complexity. The examples for cryptanalysis of the considered encryption, in general case, correspond to codewords of a random binary block code. The corresponding decoding problem is NP-complete [2] which implies that in the worst-case scenario, the complexity of decoding is exponential in the secret key length. Also the statement (ii) is in accordance with the proofs of Theorems 1 and 2, where the reduction to zero of the posterior uncertainty about the secret key appears assuming a decoding which has complexity proportional to the exhaustive search over all possible secret keys.

The above features (i) and (ii) hold not only in a passive attacking scenario where the attacker performs cryptanalysis based on recording the ciphertext from a public communication channels, but also in certain active attacking scenarios where the attacker can modify the ciphertext and learn the effects of these modifications.

B. Framework for applications

Consider a communication system using the encoding-encryption paradigm as described in Figure 2.

![Communication system model](image)

The transmitter first encodes a binary message/plaintext

\[ a = [a_i]_{i=1}^n \in \{0,1\}^n \]

to get its encoded version using an error-correcting code \( C_{ECC} \) that maps an \( m \)-dimensional plaintext to an \( n \)-dimensional encoded message, \( n > m \). The encryption is done using a keystream generator, which takes as input the secret key \( k \) of the transmitter, and outputs

\[ x = x(k) = [x_i]_{i=1}^n \in \{0,1\}^n \]

yielding

\[ y = y(k) = C_{ECC}(a) \oplus x = [y_i]_{i=1}^n \in \{0,1\}^n \] (17)

as the message to be sent over the noisy channel.

As before, we denote the noise vector by

\[ v = [v_i]_{i=1}^n \in \{0,1\}^n \]

where each \( v_i \) is the realization of a random variable \( V_i \) such that \( \Pr(V_i = 1) = p \) and \( \Pr(V_i = 0) = 1 - p \). Upon reception of the corrupted encrypted binary sequence of ciphertext

\[ z = z(k) = y \oplus v \]

\[ = C_{ECC}(a) \oplus x \oplus v = [z_i]_{i=1}^n \in \{0,1\}^n, \]

the receiver who shares the secret key \( k \) with the transmitter can decrypt first the message

\[ (C_{ECC}(a) \oplus x \oplus v) \oplus x = C_{ECC}(a) \oplus v \in \{0,1\}^n, \]

and then decode \( a \) despite the noise thanks to the error-correction code.

The encoding-encryption paradigm enjoys the following desirable properties: (i) When the decryption is performed by bitwise XORing the keystream to the ciphertext, an error in a bit before decryption causes an error in the corresponding bit after decryption, without any error-propagation, and (ii)
Provides non-availability of the error-free keystream when the communication channel is a noisy one.

We now discuss what would be the cost to upgrade such a communication system to include a wire-tap encoder. The implementation assumption is that the employed, already existing, binary block error-correction code \((m, n)\) which encodes \(m\) bits into a codeword from the finite field \(GF(2^m)\), could be replaced with a binary block code \((m', n)\) with the same error correction capability but with \(m' > m\). Accordingly, \(m' - m\) random bits can be concatenated with \(m\) information bits and mapped into the new \(m'\)-bits via a homomorphic encoder. The obtained output from homomorphic encoder is the input for the error-correcting one. Taking into account the notation from Section 2, the previous means that \(G_H(\cdot)\) should map \([a, u]\) so that in the resulting vector each bit of data from \(a\) is affected by at least one random bit from \(u\), to make sure that each bit of data is protected. \(3\) Sparsity. Both the matrices \(G_H\) and \(G_H^1\) should be as sparse as possible, to avoid too much computation and communication overheads.

Since by (3), the \(m - l\) last rows of \(G_H\) form a generator matrix of a \((m, m - l)\) error correction code \(C\) in systematic form, it has rank \(m - l\). The first \(l\) rows are then obtained by adding linearly independent vectors not in \(C\), thus completing a basis of \(\{0, 1\}^m\), resulting automatically in an invertible matrix. A simple way to do so is to choose \(G_H^{(1)} = 0_{l \times (m - l)}\) and \(G_H^{(2)} = I_l\), so that (5) becomes

\[
G_H = \begin{bmatrix}
0_{l \times (m - l)} & I_l \\
I_{m - l} & G_H^{(4)}
\end{bmatrix},
\]

and \(G_H^{(4)}\) has no column with only zeroes (it is a block of an error correction code), we have that indeed each bit of data from \(a\) is affected by at least one random bit from \(u\).

The choice of \(G_H^{(1)} = 0_{l \times (m - l)}\) and \(G_H^{(2)} = I_l\) makes the \(l\) first rows of \(G_H\) as sparse as possible.

\[\text{Example 2:} \text{ Take } m = 4, l = 2 \text{ so that } m - l = 2, \text{ and}\]

\[
G_H = \begin{bmatrix}
G_H^{(1)} & G_H^{(2)} \\
I_2 & G_H^{(4)}
\end{bmatrix} = \begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{bmatrix}.
\]

Clearly \(G_H\) is invertible. The error correction code described by rows 3 and 4 is simply the repetition code.

\section{VI. Conclusion}

This paper proposed a generic model of randomized encryption schemes, that encompasses those presented in [21, 22, 24, 25, 30, 16] and [17].

The issue addressed is an information-theoretic security evaluation of this model, whose enhanced security relies on the use of extra randomness together with a dedicated wire-tap coding technique. Note that the involved randomness is not employed for encryption purposes (as it is in the one-time pad encryption systems) but for enhancing the security of the secret key controlled component for generation of pseudorandom vectors based on which the encryption is performed.

The information-theoretic security evaluation shows that with the aid of a dedicated wire-tap encoder, the amount of uncertainty that the adversary must face about the key given all the information he could gather during different passive or active attacks he can mount, is increased in comparison with the system without this dedicated coding but it is a decreasing
function of the sample available for cryptanalysis. This means that the wire-tap encoder can indeed provide an information theoretical security level over a period of time, after which a large enough sample is collected and the function tends to zero, entering a regime in which a computational security analysis is needed.

Interesting issues for further work are the characterization of the transition region in which the uncertainty drops to close to zero as well as the computational complexity based evaluation of the proposed class of randomized encryptions.

Acknowledgements

The research of F. Oggier is supported in part by the Singapore National Research Foundation under Research Grant NRF-RF2009-07 and NRF-CRP2-2007-03, and in part by the Nanyang Technological University under Research Grant M58110049 and M58110070. This work was done partly while M. Mihaljevic was visiting the division of mathematical sciences, Nanyang Technological University, Singapore, and partly while F. Oggier was visiting the Research Center for Information Security, Tokyo. M. Mihaljevic is partly supported via the Project # 174008, Ministry of Science and Technology, Belgrade, Serbia.

References

[6] GSM Technical Specifications: European Telecommunications Standards Institute (ETSI), Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path; General description, TS 100 573 (GSM 05.01), http://www.etsi.org.