This document is downloaded from DR-NTU, Nanyang Technological University Library, Singapore.

Title	A wire-tap approach to enhance security in communication systems using the encoding-encryption paradigm
Author(s)	Mihaljevic, Miodrag; Oggier, Frederique
Citation	Mihaljevic, M. & Oggier, F. (2010). A wire-tap approach to enhance security in communication systems using the encoding-encryption paradigm. Information and Coding Theory Workshop, International Conference on Telecommunications (ICT) 2010.
Date	2010
URL	http://hdl.handle.net/10220/6295
Rights	

A Wire-tap Approach to Enhance Security in Communication Systems using the Encoding-Encryption Paradigm

Miodrag Mihaljević
Mathematical Institute
Serbian Academy of Sciences and Arts, Belgrade, Serbia
and Research Center for Information Security (RCIS)
Institute of Advanced Industrial Science and Technology (AIST),
Tokyo, Japan
Email:miodragm@turing.mi.sanu.ac.yu

Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
Email: frederique@ntu.edu.sg

***Abstract*—Motivated by the GSM system, we consider communication systems which employ the encoding-encryption paradigm of first encoding the data before encrypting it for transmission. We add one level of security to the existing system designs by introducing a wiretap encoder. We analyze the security from an information theoretical point of view, and prove the enhanced security of the proposed scheme, focusing on the case of known plain text attacks that can endanger not only the confidentiality of some messages but also the safety of the key used for encryption, and thus the security of the whole communication system.**

I. Introduction

Reliability in wireless communication systems has been extensively studied in the past decades. Recently, more and more attention has been paid to the fact that wireless channels are by nature more vulnerable to eavesdropping. Accordingly wireless systems should include coding algorithms for providing error-corrections as well as ciphering algorithms for encryption and decryption.

An illustrative example where the coding and ciphering are of high importance is GSM (see [2]-[1]), which is the most widespread system of mobile communications. GSM must use error correction to withstand reception errors, as well as encryption to provide privacy for the users. The GSM protocol uses the encoding-encryption paradigm: a message is first subjected to an error-correction code which considerably increases the size of the message. The encoded message is then encrypted and transmitted (see [1], Annex A). This approach contradicts to the common practice of first encrypting a message, and only then subjecting it to error-correction codes.

Note that an advantage of encoding and then encrypting is that even in a known plaintext attacking scenario, a wire-tapper can learn only a noisy version of the keystream which makes, generally speaking, the cryptanalysis of the employed keystream generator more complex. On the other hand, this approach implies encryption of more data because the error-correction encoding generates redundant data in order to provide possibility of the errors correction. Undesirability of the redundant data from the cryptographic security point of view has been pointed out even in [6] where the cryptography as a scientific topic has been established. Performing error-correction coding of a message before encryption introduces a structured redundancy, which could be an origin for mounting certain attacks against the employed keystream generator.

The question that we address in this work is a generic approach for enhancing the security of communication systems where the data is first encoded and then encrypted, of which GSM is maybe the most famous motivating example. We are mainly focusing on the security of the keystream generator, more important than the security of a given confidential message. This is done by employing an additional dedicated wire-tap channel coding. Similar ideas have recently appeared in the context of stream ciphers designs [3], [4], but the focus of this paper is very different since we deal with existing (given) encryption schemes.

The contribution of this paper is to propose and elaborate an approach for improving the security of communication systems which utilize the "first encoding then encryption" paradigm, employing a stream cipher and an error correcting code. As a starting point for our study, we consider the case of certain discrete memoryless channels (DMCs). We involve into an existing system an additional block which performs a dedicated wire-tap channel like coding. This dedicated coding provides origin for enhancing the security as a trade-off with a slight/moderate increase of the implementation complexity and the communications overhead. The improved security appears as a consequence of joint impact of the proposed dedicated wire-tap channel coding based on a linear mapping controlled by a pure randomness and a noise which is inherent in the communication channel.

We study the security of the proposed approach from an information-theoretic point. More precisely, we show that the information-theoretic security of the keystream is a decreasing function of the sample available for cryptanalysis. The achieved trade-off between the enhanced security and

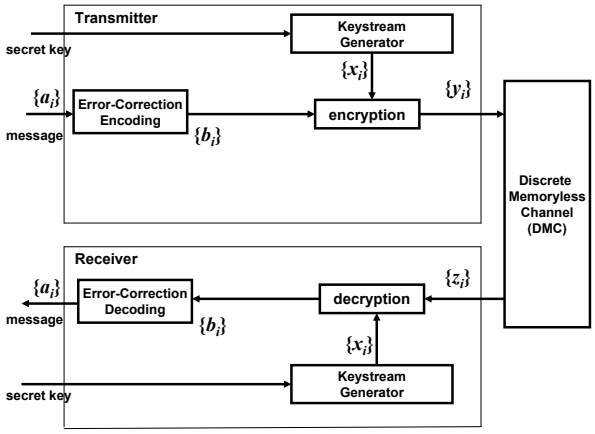

Fig. 1. Model of the communications system under consideration.

the increased implementation and communications overheads appears as very appropriate in a number of scenarios where the security is a high priority.

II. Communication Systems Model

We consider a class of communications systems which employs coding and ciphering for providing the reliability and secrecy of the transmissions, as shown in Fig. 1.

The system is composed of:

- an ℓ-dimensional binary vector of message/plaintext data $\mathbf{a} = [a_i]_{i=1}^{\ell}$ to be sent;
- an n-dimensional binary vector $\mathbf{x} = [x_i]_{i=1}^{n}$ of the keystream generator output bits used to protect the vector $\mathbf{a}$ of data;
- a noisy binary channel, represented by an n-dimensional binary vector $\mathbf{v} = [v_i]_{i=1}^{n}$ of random noise, where each coefficient v_i is the output of a random variable V_i satisfying that $\Pr(V_i = 1) = p$ and $\Pr(V_i = 0) = 1 - p$;
- $C_{ECC}(\cdot)$ and $C_{ECC}^{-1}(\cdot)$: operator of the error-correction encoding and decoding, respectively.

We assume the employed encryption is a stream ciphering. Indeed, the trick of reversing the order of encryption and error-correction is not possible if a block-cipher were to be used for encryption. Accordingly, modulo 2 addition of the corrupted binary sequence of ciphertext and the keystream yields a corrupted version of the error-correction encoded plaintext where the employed encoding provides possibility for recovering the error-free plaintext. As such, the above given system is already able to provide reliability via error correcting codes and some security via the use of the keystream generator.

To enhance the security without having to change the existing system, we incorporate a wire-tap encoder, composed of:

- an $(m-\ell)$-dimensional binary vector of random data $\mathbf{u} = [u_i]_{i=1}^{m-\ell}$ where each u_i is the realization of the random variable U_i such that $\Pr(U_i = 1) = \Pr(U_i = 0) = 1/2$;
- operators of the homophonic wire-tap channel encoding $C_H(\cdot)$ and decoding $C_H^{-1}(\cdot)$.

A. Encoding and encryption at the transmitter

The transmitter goes through the following steps:

1) Employing the random vector $\mathbf{u}$, it performs the homophonic (wire-tap channel) encoding of the plain text $\mathbf{a}$ to get
$$C_H(\mathbf{a}||\mathbf{u}),$$
where $||$ denotes the concatenation. How the wire-tap channel coding is concretely done will be discussed later on.
2) The transmitter then does the error-correction encoding of the resulting vector:
$$C_E(C_H(\mathbf{a}||\mathbf{u})). \tag{1}$$
3) Finally, it generates the ciphertext in form of an n-dimensional binary vector $\mathbf{y}$ given by
$$\mathbf{y} = C_{ECC}(C_H(\mathbf{a}||\mathbf{u})) \oplus \mathbf{x}, \tag{2}$$
where $\mathbf{x}$ is the output of the keystream generator and $\oplus$ denotes XOR or addition modulo 2.

The vector $\mathbf{y}$ is then sent over the channel.

B. Decryption and decoding at the receiver

Assuming transmission over a class of binary discrete memoryless channel (DMC), the receiver gets the noisy vector $\mathbf{z}$ given by

$$\begin{aligned} \mathbf{z} &= \mathbf{y} \uplus \mathbf{v} \\ &= C_{ECC}(C_H(\mathbf{a}||\mathbf{u})) \oplus \mathbf{x} \uplus \mathbf{v}, \end{aligned} \tag{3}$$

where $\uplus$ stands for the operations of complementation and/or erasures controlled by the vector $\mathbf{v}$ in the considered class of binary DMCs.

Upon reception, the receiver first computes

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

and then decode $\mathbf{z} \oplus \mathbf{x}$:

$$\begin{aligned} C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{x}) &= C_{ECC}^{-1}(C_{ECC}(C_H(\mathbf{a}||\mathbf{u})) \uplus \mathbf{v}) \\ &= C_H(\mathbf{a}||\mathbf{u}) \end{aligned}$$

since by assumption the error correcting code can correct the errors introduced by $\mathbf{v}$. The only things left are thus to decode the wire-tap code, and to remove the random bit string $\mathbf{u}$, namely

$$\mathbf{a} = tcat_{\ell}(C_H^{-1}(C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{x})))$$

where $tcat_{\ell}(\cdot)$ denotes truncation of the argument vector to the first ℓ bits.

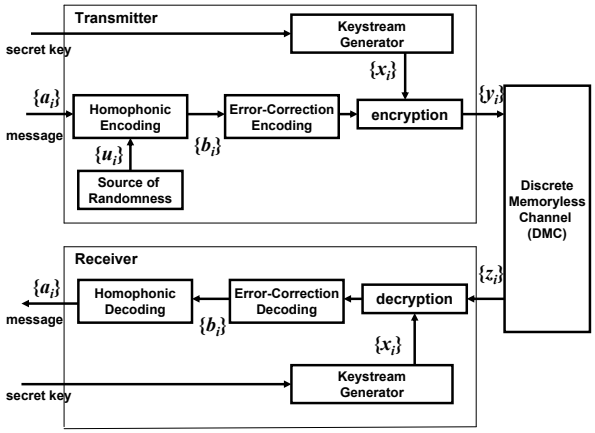

Fig. 2. A framework for enhancing security employing dedicated wire-tap channel like coding and pure randomness.

III. Wire-tap Coding

A. Generic coset coding

A generic technique for performing homophonic/wire-tap coding is the coset encoding as proposed by Wyner [7] recently also employed in a cryptographic framework in [5].

- To transmit a l-bit message, we first select a (n, k) code C, that is, a binary error correcting code that maps a k-bit message into a n-bit codeword, such that $l \leq n - k$.
- Since C is formed of 2^k codewords contained in the space $\{0,1\}^n$ of 2^n vectors, we can partition $\{0,1\}^n$ into a disjoint union of cosets of C, that is

$$\{0,1\}^n = \bigcup_{i=1}^{2^{n-k}} (\mathbf{u}_i \oplus C)$$

  where $\mathbf{u}_i$ are vectors in $\{0,1\}^n \backslash C$, and the union is over a set of representatives $\mathbf{u}_i$. Since each coset is just a translation of C, it contains the same number of vectors, namely 2^k, and thus there must be 2^{n-k} cosets of C, among which we choose 2^l cosets and let each message correspond to a chosen coset. This is the key to homophonic coding: instead of mapping one message to one codeword, we map one message to a set of codewords, namely, to a coset.
- The selection of the cosets is done in a linear fashion as explained below:
  - Suppose $\mathbf{G}^C$ is a $k \times n$ generator matrix for C with rows $\mathbf{g}_1^C, \mathbf{g}_2^C, \ldots, \mathbf{g}_k^C$.
  - We select l linearly independent row vectors $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_l$ from $\{0,1\}^n \backslash C$.
  - The coset $\mathbf{u}(\mathbf{s}) \oplus C$ corresponding to an l-bit message $\mathbf{s} = [s_1, s_2, ..., s_l]$ is determined as follows:

$$\mathbf{s} \mapsto s_1\mathbf{h}_1 \oplus s_2\mathbf{h}_2 \oplus \ldots \oplus s_l\mathbf{h}_l \oplus C.$$

- The above correspondence is deterministic, but the encoding has a random component in the selection of the employed codeword inside the coset $\mathbf{u}(\mathbf{s}) \oplus C$. The transmitted word $\mathbf{c}$ is specified by:

$$\mathbf{c} = s_1\mathbf{h}_1 \oplus s_2\mathbf{h}_2 \oplus \ldots \oplus s_l\mathbf{h}_l \oplus u_1\mathbf{g}_1^C \oplus u_2\mathbf{g}_2^C \oplus \ldots \oplus u_k\mathbf{g}_k^C$$

  where $\mathbf{u} = [u_1, u_2, \ldots, u_k]$ is a uniformly distributed random k-bit vector and $k \leq n - l$.

We can now summarize the overall encoding operation:

$$\mathbf{c} = [\mathbf{s}||\mathbf{u}] \begin{bmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \vdots \\ \mathbf{h}_l \\ \mathbf{G^C} \end{bmatrix} = [\mathbf{s}||\mathbf{u}]\mathbf{G}_H,$$

where $\mathbf{G}_H$ is a $(l + k) \times n$ binary matrix corresponding to $C_H(\cdot)$.

B. Encoding via coset coding

In our scenario, we need to combine wiretap encoding with error correction encoding, both being linear operations. Recall from (1) that the encoded vector at the transmitter is

$$C_{ECC}(C_H(\mathbf{a}||\mathbf{u})),$$

where $\mathbf{a}$ is a l-dimensional data vector, and $\mathbf{u}$ is a $m-l$ random vector. Using generic coset coding as discussed above with a $(m, m-l)$ code, we now know that

$$C_H(\mathbf{a}||\mathbf{u}) = [\mathbf{a}||\mathbf{u}]\mathbf{G}_H,$$

where $\mathbf{G}_H$ is an $m \times m$ matrix, and thus

$$\begin{aligned} C_{ECC}(C_H(\mathbf{a}||\mathbf{u})) &= C_{ECC}([\mathbf{a}||\mathbf{u}]\mathbf{G}_H) \\ &= [\mathbf{a}||\mathbf{u}]\mathbf{G}_H\mathbf{G}_{ECC} \\ &= [\mathbf{a}||\mathbf{u}]\mathbf{G} \end{aligned} \quad (4)$$

where $\mathbf{G}_{ECC}$ is an $m \times n$ binary generator matrix corresponding to $C_{ECC}(\cdot)$, and $\mathbf{G} = \mathbf{G}_H\mathbf{G}_{ECC}$ 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 $m - l$:

$$\mathbf{G}_H = \begin{bmatrix} \mathbf{G}_H^{(1)} & \mathbf{G}_H^{(2)} \\ \mathbf{I}_{m-l} & \mathbf{G}_H^{(4)} \end{bmatrix} \quad (5)$$

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 $\mathbf{G}_H^{(4)}$ is an $(m-l) \times l$ matrix.

The requirement for the matrix $\mathbf{G}_H$ are two-fold:

- In order for the decoding operator C_H^{-1} to exist, we need $\mathbf{G}_H$ to be invertible.
- Both matrices $\mathbf{G}_H$ and $\mathbf{G}_H^{-1}$ should be as sparse as possible in order to avoid implementation complexity overheads.

IV. Information Theoretical Analysis of the Security Improvement

This section analyzes the security of the proposed scheme from an information theoretical prospective. The system we consider already uses a keystream generator to protect the confidentiality of the data. Thus though an adversary may try to still mount an attack to discover a secret message, more dangerous is an attack against the keystream, which would endanger all the transmissions. We will show how the introduction of the wiretap encoding increases the protection of the key.

In what follows, we use as notation that

- u_i, random bits used in the wiretap 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, $i = 1, 2, ..., n$. We can further assume that the plain text 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: $\mathbf{A}^l = [A_i]_{i=1}^{\ell}$, $\mathbf{U}^{m-l} = [U_i]_{i=1}^{m-\ell}$, $\mathbf{X}^n = [X_i]_{i=1}^{n}$, and $\mathbf{V}^n = [V_i]_{i=1}^{n}$.

Recall from (3) and (4) that the received vector at the receiver is given by

$$\begin{aligned} \mathbf{z} &= C_{ECC}(C_H(\mathbf{a}||\mathbf{u})) \oplus \mathbf{x} \uplus \mathbf{v} \\ &= [\mathbf{a}||\mathbf{u}]\mathbf{G} \oplus \mathbf{x} \uplus \mathbf{v} \end{aligned}$$

where $\mathbf{G} = [g_{i,j}]_{i=1}^{m}{}_{j=1}^{n}$ is an $m \times n$ matrix containing both the wiretap and the error correction encoding.

Let $\mathbf{z} = [z_i]_{i=1}^{n}$, so that $\mathbf{z}$ can be written componentwise as

$$z_i = ((\bigoplus_{k=1}^{\ell} g_{k,i}a_k) \oplus (\bigoplus_{k=1}^{m-\ell} g_{\ell+k,i}u_k) \oplus x_i) \uplus v_i,\ i = 1, 2, ..., n,$$

and z_i appears as the realization of a random variable Z_i:

$$Z_i = ((\bigoplus_{k=1}^{\ell} g_{k,i}A_k) \oplus (\bigoplus_{k=1}^{m-\ell} g_{\ell+k,i}U_k) \oplus X_i) \uplus V_i,\ i = 1, 2, ..., n.$$

We further denote $\mathbf{Z}^n = [Z_i]_{i=1}^{n}$, and

$$\mathbf{Z}^n = C_{ECC}(C_H(\mathbf{A}^l||\mathbf{U}^{m-l})) \oplus \mathbf{X}^n \uplus \mathbf{V}^n. \tag{6}$$

Note that since $C_H(\mathbf{A}^l||\mathbf{U}^{m-l}) = [\mathbf{A}^l, \mathbf{U}^{m-l}]\mathbf{G}_H$, we can rewrite the wiretap encoder as

$$C_H(\mathbf{A}^l||\mathbf{U}^{m-l}) = C_{H,a}(\mathbf{A}^l) \oplus C_{H,u}(\mathbf{U}^{m-l}),$$

where $C_{H,a}$ and $C_{H,u}$ are the operators for the wiretap encoding restricted to $\mathbf{a}$, resp. $\mathbf{u}$, so that

$$\mathbf{Z}^n = C_{ECC}(C_{H,a}(\mathbf{A}^l)) \oplus C_{ECC}(C_{H,u}(\mathbf{U}^{m-l})) \oplus \mathbf{X}^n \uplus \mathbf{V}^n \tag{7}$$

since the error correcting encoding is also linear.

Before starting the analysis itself, let us give a motivating example.

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

$$z_i = x_i \oplus (\bigoplus_{k=1}^{m-\ell} g_{\ell+k,i}u_k) \uplus v_i,\ i = 1, 2, ..., n.$$

Without the wiretap encoding, the keystream x_i is corrupted and so protected as well by the noise on the channel, while with addition of the wiretap encoder, the key is further protected by the pure randomness added.

The lemma below gives a bound on the resistance of the scheme to a known plain text attack where the adversary knows both $\mathbf{a}$ and $\mathbf{z}$.

Lemma 1: The entropy of the keystream output knowing the plaintext and the received signal can be lower bounded as follows:

$$\begin{aligned} &H(\mathbf{X}^n|\mathbf{A}^l, \mathbf{Z}^n) \geq \\ &\min\{H(\mathbf{U}^{m-l}), H(\mathbf{X}^n) + H(\mathbf{V}^n)\} + \\ &\min\{H(\mathbf{V}^n), H(\mathbf{X}^n)\} - \delta(C_{ECC}), \end{aligned}$$

where

$$\begin{aligned} \delta(C_{ECC}) &= H(\epsilon) + \epsilon \log(2^{m-l} - 1) \\ &\rightarrow 0 \end{aligned}$$

with $\epsilon \rightarrow 0$.

Proof: Employing the entropy chain rule, we have that

$$\begin{aligned} & H(\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{X}^n, \mathbf{V}^n, \mathbf{Z}^n) \\ = \ & H(\mathbf{A}^l) + H(\mathbf{Z}^n|\mathbf{A}^l) + H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{Z}^n) + \\ & H(\mathbf{V}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{Z}^n) + H(\mathbf{X}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{V}^n, \mathbf{Z}^n) \\ = \ & H(\mathbf{A}^l) + H(\mathbf{Z}^n|\mathbf{A}^l) + H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{Z}^n) \\ & + H(\mathbf{V}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{Z}^n), \end{aligned}$$

since $H(\mathbf{X}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{V}^n, \mathbf{Z}^n) = 0$ using (6).

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

$$\begin{aligned} & H(\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{X}^n, \mathbf{V}^n, \mathbf{Z}^n) \\ = \ & H(\mathbf{A}^l) + H(\mathbf{Z}^n|\mathbf{A}^l) + H(\mathbf{X}^n|\mathbf{A}^l, \mathbf{Z}^n) + \\ & H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{X}^n, \mathbf{Z}^n) + H(\mathbf{V}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{X}^n, \mathbf{Z}^n) \\ = \ & H(\mathbf{A}^l) + H(\mathbf{Z}^n|\mathbf{A}^l) + H(\mathbf{X}^n|\mathbf{A}^l, \mathbf{Z}^n) \\ & + H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{X}^n, \mathbf{Z}^n), \end{aligned}$$

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

By combining the two decompositions, we deduce that

$$\begin{aligned} & H(\mathbf{X}^n|\mathbf{A}^l, \mathbf{Z}^n) \\ = \ & H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{Z}^n) + H(\mathbf{V}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{Z}^n) \\ & - H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{X}^n, \mathbf{Z}^n). \end{aligned}$$

We now reformulate $H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{Z}^n)$ and $H(\mathbf{V}^n|\mathbf{A}^l, \mathbf{U}^{m-l}, \mathbf{Z}^n)$. First, using (7) and that conditioning reduces entropy, namely,

$$H(\mathbf{U}^{m-l}|\mathbf{A}^l, \mathbf{Z}^n) \leq H(\mathbf{U}^{m-1}),$$

we compute that

$$\begin{aligned} H(\mathbf{U}^{m-l}|\mathbf{A}^l,\mathbf{Z}^n) &= \min\{H(\mathbf{U}^{m-l}), H(\mathbf{X}^n,\mathbf{V}^n)\} \\ &= \min\{H(\mathbf{U}^{m-1}), H(\mathbf{X}^n)+H(\mathbf{V}^n)\} \end{aligned}$$

since $\mathbf{X}^n$ and $\mathbf{V}^n$ are mutually independent.

Similarly, again using (7) and that

$$H(\mathbf{V}^n|\mathbf{A}^l,\mathbf{U}^{m-l},\mathbf{Z}^n) \le H(\mathbf{V}^n),$$

we obtain that

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

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

$$\begin{aligned} H(\mathbf{U}^{m-l}|\mathbf{A}^l,\mathbf{X}^n,\mathbf{Z}^n) &\le H(P_e)+P_e\log(2^{m-l}-1) \\ &\le H(\epsilon)+\epsilon\log(2^{m-l}-1)\to 0 \end{aligned}$$

since by design of the system, we may assume $P_e=\epsilon\to 0$. This concludes the proof. ∎

Let us make a few remarks about the above lemma.

The interpretation of the lemma is a bound on the resistance of the scheme to a known plain text attack. This clearly depends on two parameters:

- the keystream generator: if the output of the keystream generator has a very high entropy $H(\mathbf{X}^n) \ge H(\mathbf{U}^{m-l},\mathbf{V}^n)$, then the lemma tells that
$$H(\mathbf{X}^m|\mathbf{A}^l,\mathbf{Z}^n) \ge H(\mathbf{U}^{m-l})+H(\mathbf{V}^n)-\delta(C_{ECC}).$$
- the pure randomness put in the wiretap encoder: if we do not add it in the system, the lemma shows that
$$H(\mathbf{X}^m|\mathbf{A}^l,\mathbf{Z}^n) \ge H(\mathbf{V}^n)$$
that is, as already mentioned in Example 1, the security of the scheme depends on the channel noise.

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, we have

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

Proof: Since the channel is noisefree, $\mathbf{V}=0$ and consequently $H(V)=P_e=0$. Lemma 1 can be rewritten as

$$\begin{aligned} & H(\mathbf{X}^n|\mathbf{A}^l,\mathbf{Z}^n) \\ \ge\ & \min\{H(\mathbf{U}^{m-l}), H(\mathbf{X}^n)\} + \\ & \min\{0, H(\mathbf{X}^n)\} - \delta(C_{ECC}) \\ =\ & \min\{H(\mathbf{U}^{m-l}), H(\mathbf{X}^n)\}. \end{aligned}$$

∎

So far, we have discussed the security analysis 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 key $\mathbf{K}$ based on which it computes its outputs $\mathbf{X}^{(t)}=[X_i^{(t)}]_{i=1}^n$ in a deterministic way f for a time period of length τ:

$$\mathbf{X}^{(t)} = f^{(t)}(\mathbf{K}),\ t=1,\ldots,\tau.$$

Correspondingly, we can rewrite the whole system in terms of realizations of random variables that depends on time, over the time interval $t=1,\ldots\tau$:

- $\mathbf{A}^{(t)}=[A_i^{(t)}]_{i=1}^{\ell}$ for the plain text,
- $\mathbf{U}^{(t)}=[U_i^{(t)}]_{i=1}^{m-\ell}$ for the pure randomness used in the wiretap encoder,
- $\mathbf{V}^{(t)}=[V_i^{(t)}]_{i=1}^{n}$ for the channel noise,
- $\mathbf{Z}^{(t)}=[Z_i^{(t)}]_{i=1}^{n}$ for the received signal.

Similarly as above, we have

$$\mathbf{Z}^{(t)} = C_{ECC}(C_{H,a}(\mathbf{A}^{(t)}) \oplus C_{H,u}(\mathbf{U}^{(t)})) \oplus f^{(t)}(\mathbf{K}) \uplus \mathbf{V}^{(t)}.$$

The key $\mathbf{K}$ is represented as a vector of random variables drawn independently from a uniform distribution over $\{0,1\}$, so that $H(\mathbf{K})=|\mathbf{K}|$. We further use the following block notations:

$$\begin{aligned} \mathbf{A}^{\tau l} &= [\mathbf{A}^{(1)}||\mathbf{A}^{(2)}||\ldots||\mathbf{A}^{(\tau)}] \\ \mathbf{U}^{\tau(m-l)} &= [\mathbf{U}^{(1)}||\mathbf{U}^{(2)}||\ldots||\mathbf{U}^{(\tau)}] \\ \mathbf{V}^{\tau n} &= [\mathbf{V}^{(1)}||\mathbf{V}^{(2)}||\ldots||\mathbf{V}^{(\tau)}] \\ \mathbf{Z}^{\tau n} &= [\mathbf{Z}^{(1)}||\mathbf{Z}^{(2)}||...||\mathbf{Z}^{(\tau)}]. \end{aligned}$$

We can now state the main theorem of this paper, which describes the security of the enhanced system against known plain text attacks.

Theorem 1: When $\Pr(V_i^{(j)}=0)\neq\Pr(V_i^{(j)}=1)\neq 1/2$, $i=1,2,...,n$, $j=1,2,...,\tau$, there exists a threshold τ_{thres} such that

$$H(\mathbf{K}|\mathbf{A}^{\tau l},\mathbf{Z}^{\tau n}) \begin{cases} >0 & \text{for} \quad \tau<\tau_{thres} \\ \to 0 & \text{for} \quad \tau\ge\tau_{thres}\ . \end{cases}$$

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

When $\tau>1$ grows, we employ the following analysis.

By using two different decompositions of $H(\mathbf{A}^{\tau l},\mathbf{U}^{\tau(m-l)},\mathbf{X}^{\tau n},\mathbf{V}^{\tau n},\mathbf{Z}^{\tau n})$ via the entropy chain rule as done in Lemma 1, we get

$$\begin{aligned} & H(\mathbf{K}|\mathbf{A}^{\tau l},\mathbf{Z}^{\tau n}) \\ =\ & H(\mathbf{U}^{\tau(m-l)}|\mathbf{A}^{\tau l},\mathbf{Z}^{\tau n}) + H(\mathbf{V}^{\tau n}|\mathbf{A}^{\tau l},\mathbf{U}^{\tau(m-l)},\mathbf{Z}^{\tau n}) \\ & -H(\mathbf{U}^{\tau(m-l)}|\mathbf{A}^{\tau l},\mathbf{K},\mathbf{Z}^{\tau n}). \end{aligned} \quad (8)$$

Note that $\mathbf{Z}^{\tau n}$ can be considered as a τn-length degraded version of a binary codeword with $\tau(m-\ell)+|\mathbf{K}|$ information bits which is corrupted by a noise vector $\mathbf{V}^{\tau n}$. Assuming that the decoding error probability of this code is P_e^*, Fano's inequality implies that

$$H(\mathbf{U}^{\tau(m-l)}|\mathbf{A}^{\tau l},\mathbf{Z}^{\tau n}) < H(\mathbf{U}^{\tau(m-l)},\mathbf{K}|\mathbf{A}^{\tau l},\mathbf{Z}^{\tau n})$$

$$\leq H(P_e^*) + P_e^* \log(2^{\tau(m-\ell)+|\mathbf{K}|} - 1) \ .$$

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

In a similar manner and employing

$$H(\mathbf{V}^{\tau n}|\mathbf{A}^{\tau l}, \mathbf{U}^{\tau(m-l)}, \mathbf{Z}^{\tau n}) < H(\mathbf{V}^{\tau n}, \mathbf{K}|\mathbf{A}^{\tau l}, \mathbf{U}^{\tau(m-l)}, \mathbf{Z}^{\tau n}),$$

the decoding ability of C_{ECC} with a minimum distance decoding as used above implies that $H(\mathbf{V}^{\tau n}|\mathbf{A}^{\tau l}, \mathbf{U}^{\tau(m-l)}, \mathbf{Z}^{\tau n}) \rightarrow 0$ when τ is large enough.

To take care of $H(\mathbf{U}^{\tau(m-l)}|\mathbf{A}^{\tau l}, \mathbf{K}, \mathbf{Z}^{\tau n})$, we again use a decoding argument, since $\mathbf{Z}^{\tau n}$ is known. However, it is important to note here that $\mathbf{K}$ is known too. Thus even though we look at a block

$$\mathbf{U}^{\tau(m-l)} = [\mathbf{U}^{(1)}||\mathbf{U}^{(2)}|| \dots ||\mathbf{U}^{(\tau)}],$$

the knowledge of $\mathbf{K}$ makes each block $\mathbf{U}^{(t)}$ independent, and thus we can decode each of them separately and the probability of error is P_e^τ. Fano's equality finally yields

$$\begin{aligned} H(\mathbf{U}^{\tau(m-l)}|\mathbf{A}^{\tau l}, \mathbf{K}, \mathbf{Z}^{\tau n}) &\leq H(P_e^\tau) + P_e^\tau \log(2^{\tau(m-l)} - 1) \\ &\leq H(\epsilon^\tau) + \epsilon^\tau \log(2^{\tau(m-1)} - 1) \end{aligned}$$

and

$$H(\mathbf{U}^{\tau(m-l)}|\mathbf{A}^{\tau l}, \mathbf{K}, \mathbf{Z}^{\tau n}) \rightarrow 0 \tag{9}$$

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

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

■

The statement is intuitively clear. The security of the keystream generator depends on the length $\mathbf{K}$ of the key. This length is fixed in the system, and then the keystream generator is used for a period τ that varies. As long as $\tau < \tau_{thresh}$, the key is protected by the randomness of the noisy channel and of the wiretap encoder, but that protection cannot last forever if the adversary collects too much data.

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 $\mathbf{V}^{\tau n} = \mathbf{0}$ and the parameter τ is large enough we have:

$$H(\mathbf{K}|\mathbf{A}^{\tau l}, \mathbf{Z}^{\tau n}) = 0 \ . \tag{10}$$

V. Future Work

This paper proposed a generic approach for enhancing the cryptographic security of a class of communication systems which operate using the encoding-encryption paradigm. The enhanced security is achieved by employment of pure randomness via a dedicated wiretap coding. An information theoretical analysis of the security was provided to show the security gain offered by the wiretap encoder.

Consequently, the proposal includes a trade-off between the enhanced security and the communication as well as implementation overheads which in a number of scenarios appear as a suitable one.

The implementation overhead due to the employed dedicated coding is implied by the complexity of one vector-matrix multiplication over GF(2) when the matrix has dimension $\ell \times m$ where ℓ is dimension of the initial data vector. This expansion also implies additional implementation and communication overheads for the factor m/ℓ, and in a number of scenarios this factor is less than two.

A natural future research direction for this work is the evaluation of the cryptographic security based on a computational complexity approach. This is especially relevant since we have proven that when the same key is used over a long time interval, the security of the scheme then has to rely on computational complexity.

Acknowledgments

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 while M. Mihaljević was visiting the division of mathematical sciences, Nanyang Technological University, Singapore.

References

[1] 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.

[2] GSM Technical Specifications: European Telecommunications Standards Institute (ETSI), *Digital cellular telecommunications system (Phase 2+); Channel Coding*, TS 100 909 (GSM 05.03), http://www.etsi.org.

[3] M.J. Mihaljević and H. Imai, "An approach for stream ciphers design based on joint computing over random and secret data", *Computing*, vol. 85, no. 1-2, pp. 153-168, June 2009.

[4] M.J. Mihaljević, "A Framework for Stream Ciphers Based on Pseudo-randomness, Randomness and Error-Correcting Coding", in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, B. Preneel, at al Eds., Vol. 23 in the Series Information and Communication Security, pp. 117-139, IOS Press, Amsterdam, The Netherlands, June 2009. DOI: 10.3233/978-1-60750-002-5-117 (ISSN: 1874-6268; ISBN: 978-1-60750-002-5)

[5] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, and J.-M. Merolla, "Applications of LDPC Codes to the Wiretap Channel", *IEEE Trans. Information Theory*, vol. 53, no. 8, pp. 2933-2945, August 2007.

[6] C.E. Shannon, "Communication theory of secrecy systems", *Bell Systems Technical Journal*, vol. 28, pp. 656-715, Oct. 1949.

[7] A.D. Wyner,"The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.