

Article

An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors

Miodrag J. Mihaljević ^{1,2,*} , Lianhai Wang ¹ and Shujiang Xu ¹

¹ The Shandong Provincial Key Laboratory of Computer Networks, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China; wanglh@sdas.org (L.W.); xushj@sdas.org (S.X.)

² Mathematical Institute, The Serbian Academy of Sciences and Arts, 11000 Belgrade, Serbia

* Correspondence: miodragm@turing.mi.sanu.ac.rs; Tel.: +381-65-2663-257

Abstract: An approach for the cryptographic security enhancement of encryption is proposed and analyzed. The enhancement is based on the employment of a coding scheme and degradation of the ciphertext. From the perspective of the legitimate parties that share a secret key, the degradation appears as a transmission of the ciphertext through a binary erasure channel. On the other hand, from the perspective of an attacker the degradation appears as a transmission of the ciphertext over a binary deletion channel. Cryptographic security enhancement is analyzed based on the capacity of the related binary deletion channel. An illustrative implementation framework is pointed out.

Keywords: encryption; cryptographic security enhancement; erasure error correction; channel with deletion errors; mutual information; channel capacity; the probability of classification error



Citation: Mihaljević, M.J.; Wang, L.; Xu, S. An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors. *Entropy* **2022**, *24*, 406. <https://doi.org/10.3390/e24030406>

Academic Editor: Zouheir Rezki

Received: 14 February 2022

Accepted: 11 March 2022

Published: 14 March 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Enhancing the security of certain cryptographic primitives by employing randomness has been employed in a number of reported designs (see, e.g., [1,2]), as well as in the context of wire-tap coding. Following these approaches, two main directions have appeared. One approach is based on the employment of a cryptographic key control of error correction encoding and decoding, given, for example, in [3–7]. The other approach is the employment of error-correction coding and noisy channels for cryptographic security enhancement of a given encryption scheme: This approach has been reported, for example, in [8–15].

Motivation. The employment of coding and noisy channel based techniques for the security enhancement of given encryption appears as an important topic. In particular, this approach could significantly increase the cryptographic security margin of a lightweight encryption scheme. On the other hand, this approach also implies additional complexity overhead. Accordingly, it appears as an interesting issue to design security enhancement with a number of parameters that provide control over desired security enhancement and required implementation and execution overheads of the encryption. The main motivation for this paper was addressing the security enhancement of a given encryption that provides the opportunity for trade-off between the security margin increasing and the required overhead.

Summary of the Results. This paper proposes a novel approach for the security enhancement of an encryption scheme. The proposed encryption is analyzed employing certain results of information theory. The enhancement is based on the employment of an error-correction coding scheme and degradation of the ciphertext. From the perspective of the legitimate parties that share a secret key, the degradation appears as a transmission of the ciphertext through a binary erasure channel. On the other hand, from the perspective of an attacker, the degradation appears as a transmission of the ciphertext over a binary deletion channel. The degradation is performed by employing a simulated noisy channel

that consists of two sub-channels so that an additional flexibility is provided for the selection of the parameters to achieve the desired security and the enhancement overhead. Cryptographic security enhancement is analyzed based on the capacity of the related binary deletion channel. It is shown that the enhancement is a function of the following parameters: probabilities of deletion in the sub-channels, capacity of the sub-channels, and the probability of the sub-channel selection for a transmission. An illustrative implementation framework is pointed out which employs a stream cipher.

Organization of the Paper. A novel scheme for cryptographic security enhancement of an encryption employing error-correction coding and a simulated channel that on an attacker’s side appears as a channel with synchronization errors is proposed in Section 2. Preliminaries and background for the security evaluation are given in Section 3. Section 4 provides a cryptographic security evaluation of the proposed enhanced encryption. An illustrative approach for the implementation is discussed in Section 5. Concluding notes are given in Section 6.

2. Proposal for a Security Enhanced Encryption

This section proposes the cryptographic security enhancement of an encryption scheme employing error-correction coding and a simulator of a channel with synchronization errors displayed in Figure 1.

We use the following notation. The message, a data vector subject to encryption is denoted by $\mathbf{m} \in \{0, 1\}^{n'}$ and we assume that it is a realization of the binary vector variable \mathbf{M} . Encrypted form of \mathbf{m} is denoted by $\mathbf{c} \in \{0, 1\}^{n'}$ and we assume that it is a realization of the binary vector variable \mathbf{C} :

$$\mathbf{c} = Enc_{\mathbf{k}}(\mathbf{m}) ,$$

where $Enc_{\mathbf{k}}(\cdot)$ denotes the encryption mapping controlled by the secret key \mathbf{k} . The vector \mathbf{x} denotes the encoded version of \mathbf{c} employing an error-correction encoding $Encode(\cdot)$, that performs mapping $\{0, 1\}^{n'} \rightarrow \{0, 1\}^n, n > n'$:

$$\mathbf{x} = Encode(Enc_{\mathbf{k}}(\mathbf{m}))$$

and \mathbf{x} is a realization of a random binary variable \mathbf{X} .

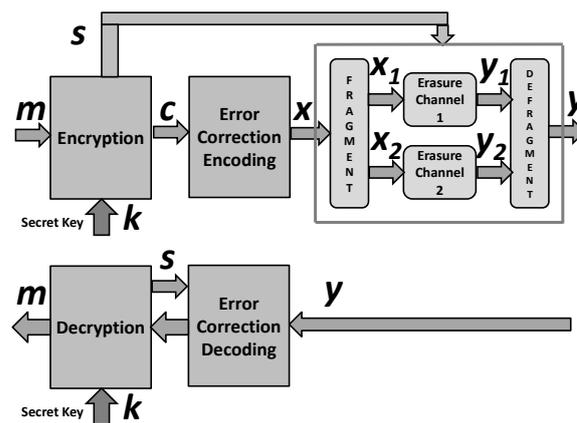


Figure 1. Security enhanced encryption scheme.

We consider a channel in which the input sequence is divided into subsequences and these subsequences are transmitted through independent i.i.d. binary deletion channels and the arrived bits after the deletion channels are combined preserving their order in the original input sequence. Consequently, the resulting channel is an i.i.d. binary deletion channel with parameters which depend on the parameters of the considered subchannels.

A simulator of the considered channel is controlled by a vector \mathbf{s} generated by the encryption algorithm which is considered as a realization of a binary random vector \mathbf{S} .

An attacker on the encryption scheme at Figure 1 faces the problem of cryptanalysis in a known plaintext attack displayed in Figure 2.

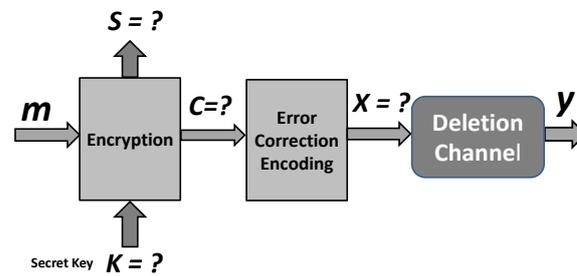


Figure 2. Model of encryption for cryptanalysis at the attacker’s side under known plaintext attack.

Note that the legitimate parties face the problem of decoding after a binary erasure channel, but the attacker faces a much harder problem of dealing with the decoding after a deletion channel. The knowledge of attackers is limited to the following. Each channel input bit is transmitted through Channel 1 with probability λ , and through Channel 2 with probability $\bar{\lambda}$, independently of each other. If transmitted through Channel 1 a bit is deleted with the probability d_1 , and if transmitted through Channel 2 a bit is deleted with the probability d_2 . The attacker does not know the specific realization of the “individual channel selection events”, i.e., they do not know which specific sub-channel bit is transmitted through, and which specific sub-channel each output symbol is received from.

An illustrative instantiate of the proposed framework is given in Section 5.

3. Preliminaries and Background

3.1. Entropy, Mutual Information, and Shannon Capacity

This section provides a summary explanation on the entropy, mutual information and Shannon capacity. A random variable is denoted by an upper-case letter (e.g., A) and its realization is denoted by a lower-case letter (e.g., a). The entropy of a random object A is denoted by $H(A)$, and the mutual information between two random objects A and B is denoted by $I(A; B)$. The binary entropy function is denoted by $h(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$.

The entropy of a random variable A is defined as:

$$H(A) := \sum_{x \in \text{support}(A)} Pr[A = x] \log_2 \frac{1}{Pr[A = x]}, \tag{1}$$

The mutual information $I(A; B)$ between jointly distributed random variables A and B is defined as follows:

$$I(A; B) := H(A) - H(A|B) = H(B) - H(B|A) \tag{2}$$

where conditional entropy is defined as:

$$H(A|B) = \sum_{b \in \text{supp}(B)} Pr(B = b) H(A|B = b) \tag{3}$$

and:

$$H(A|B = b) = \sum_{a \in \text{supp}(A)} Pr(A = a|B = b) \log_2 \frac{1}{Pr(A = a|B = b)} \tag{4}$$

Consequently, the conditional mutual information when the third variable Z is given as:

$$I(A, B|Z) := H(A|Z) - H(A|B, Z) = H(B|Z) - H(B|A, Z). \tag{5}$$

The Shannon capacity of a channel is denoted by C and is defined as:

$$C := \sup\{I(A; B)\}, \tag{6}$$

where A corresponds the channel input, B corresponds to the channel output, and the supremum is over the choice of the distribution of A .

3.2. Mutual Information and Capacity of the Deletion Channel with Fragmentation

The considered communication channel is displayed in Figure 3 and it consists of two sub-channels: Ch_1 and Ch_2 .

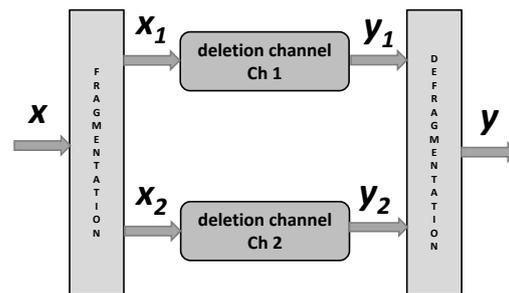


Figure 3. Model of the deletion channel with fragmentation.

An i.i.d. binary input deletion channel is considered in which every transmitted bit is either randomly deleted with probability d or received correctly with probability $1 - d$ while there is no information about the values or the positions of the lost symbols at the transmitter or at the receiver. In the transmission of n symbols through the channel, the input sequence is denoted by $\mathbf{x} = (x_1, \dots, x_n)$ in which $x_i \in \{0, 1\}$, and $\mathbf{x} \in \{0, 1\}^n$. The output binary sequence is denoted by $\mathbf{y} = (y_1, \dots, y_m)$ in which m is a realization of a binomial random variable with parameters n and d (due to the characteristics of the i.i.d. deletion channel).

Let \mathbf{x} and \mathbf{y} denotes input and output codewords of the considered channel, respectively.

Further on, let \mathbf{x}_i denotes part of the codeword \mathbf{x} transmitted through Ch_i , $i = 1, 2$, and let n_i denotes numbers of the codeword bits transmitted through Ch_i , $i = 1, 2$. Finally, let \mathbf{y}_i denotes the vector received through Ch_i when the channel input is \mathbf{x}_i , $i = 1, 2$. We assume that the vectors \mathbf{x} , \mathbf{y} , \mathbf{x}_i , \mathbf{y}_i and n_i , are realizations of the random variables \mathbf{X} , \mathbf{Y} , \mathbf{X}_i , \mathbf{Y}_i and N_i , respectively, $i = 1, 2$.

In continuation, we consider $I(\mathbf{X}_i, \mathbf{Y}_i)$, $i = 1, 2$, following [16]:

$$\begin{aligned} I(\mathbf{X}_i, \mathbf{Y}_i) &= I(\mathbf{X}_i, \mathbf{Y}_i, N_i) - I(\mathbf{X}_i, N_i | \mathbf{Y}_i) \\ &= I(\mathbf{X}_i, \mathbf{Y}_i | N_i) + I(\mathbf{X}_i, N_i) - I(\mathbf{X}_i, N_i | \mathbf{Y}_i) \\ &\leq I(\mathbf{X}_i, \mathbf{Y}_i | N_i) + H(N_i) \\ &\leq I(\mathbf{X}_i, \mathbf{Y}_i | N_i) + \log_2(N + 1) \\ &= \sum_{n_i=0}^n P(N_i = n_i) I(\mathbf{X}_i, \mathbf{Y}_i | N_i = n_i) + \log_2(N + 1), \end{aligned} \tag{7}$$

where in deriving the first inequality we have used the fact that:

$$H(N_i | \mathbf{X}_i) = 0 \quad \text{and} \quad I(\mathbf{X}_i, N_i | \mathbf{Y}_i) \geq 0,$$

and in deriving the second equality the fact that:

$$\begin{aligned} H(N_i) &= - \sum_{n=1}^N \binom{N}{n} \lambda^n \bar{\lambda}^{N-n} \log_2(\binom{N}{n} \lambda^n \bar{\lambda}^{N-n}) \\ &\leq \log_2(N + 1). \\ I(\mathbf{X}_i, \mathbf{Y}_i | N_i = n_i) &\leq n_i C(d_i) + H(D_i | N_i = n_i), \end{aligned} \tag{8}$$

where d_i denotes the probability of deletions through the transmission of n_i bits over the i -th channel and d_i , is realization of the corresponding random variable D_i , $i = 1, 2$.

Accordingly:

$$\begin{aligned}
 & H(D_i|N_i = n_i) \\
 &= -\sum_{n=1}^{n_i} \binom{n_i}{n} d_i^n \bar{d}_i^{n_i-n} \log_2(\binom{n_i}{n} d_i^n \bar{d}_i^{n_i-n}) \\
 &\leq \log_2(n_i + 1) .
 \end{aligned} \tag{9}$$

and

$$\begin{aligned}
 I(\mathbf{X}_i, \mathbf{Y}_i) &\leq \sum_{n_i=0}^n P(N_i = n_i)(n_i C(d_i) + \log_2(n_i + 1)) \\
 &\quad + \log_2(n + 1) \\
 &\leq \text{Exp}\{N_i\}C(d_i) + 2\log_2(n + 1) ,
 \end{aligned} \tag{10}$$

where $\text{Exp}\{N_i\}$ denotes the expected value of the variable N_i and the last inequality results since $\log_2(n_i + 1) \leq \log(n + 1), i = 1, 2$. Finally:

$$I(\mathbf{X}_i, \mathbf{Y}_i) \leq \lambda_i n C(d_i) + 2\log_2(n + 1) , \quad i = 1, 2. \tag{11}$$

It is shown in [16] that:

$$\begin{aligned}
 I(\mathbf{X}, \mathbf{Y}) &\leq n\lambda C(d_1) + n\bar{\lambda}C(d_2) + 4\log_2(n + 1) \\
 &+ n\bar{d}\log_2(\bar{d}) + n\lambda\bar{d}_1\log_2(\lambda\bar{d}_1) + n\bar{\lambda}\bar{d}_2\log_2(\bar{\lambda}\bar{d}_2) \\
 &= \Psi(n, \lambda, d_1, d_2, C(d_1), C(d_2))
 \end{aligned} \tag{12}$$

where $\bar{d} = 1 - d, d = \lambda d_1 + \bar{\lambda}d_2, \bar{\lambda} = 1 - \lambda, \bar{d}_1 = 1 - d_1, \bar{d}_2 = 1 - d_2$.

3.3. The Probability of Error and the Equivocation after a Noisy Channel

Suppose the random variables A and B represent input and output messages (out of m possible messages), and the given conditional entropy $H(A|B)$ represents the average amount of information lost on A when B is given. According to [17,18], for example, we have the following general upper bound on the equivocation:

$$H(A) - I(A, B) \leq h(P_{err}) + P_{err}\log_2(m - 1), \tag{13}$$

where $h(\cdot) \leq 1$ is the binary entropy function and $P_{err} = 1 - \Pr(A = a|B = b)$, and following [15], when A is such that it has the maximum possible entropy $H(A) = m$, we have:

$$1 - \frac{I(A, B)}{m} \leq \frac{1}{m} + \frac{P_{err}}{m} \log_2(m - 1). \tag{14}$$

4. Security Evaluation of the Enhanced Encryption

4.1. Security Notation

We employ a traditional approach for analyzing cryptographic security (see [19], for example) based on the following two issues: (i) a description of what a “break” of the scheme means, and (ii) a specification of the assumed power of the adversary. A cryptographic scheme is considered as a secure one in a computational sense, if for every probabilistic polynomial-time adversary \mathcal{A} performing an attack of some specified type, and for every polynomial $p(n)$, there exists an integer N such that the probability that \mathcal{A} succeeds (where success of the attack is also well-defined) is less than $\frac{1}{p(n)}$ for every $n > N$. Accordingly, the following two definitions specify a security evaluation scenario and a security statement.

Definition 1 ([19]). *The Adversarial Indistinguishability Experiment consists of the following steps:*

1. *The adversary \mathcal{A} chooses a pair of messages $(\mathbf{m}_0; \mathbf{m}_1)$ of the same length n , and passes them on to the encryption system for encrypting.*
2. *A bit $b \in \{0,1\}$ is chosen uniformly at random, and only one of the two messages $(\mathbf{m}_0; \mathbf{m}_1)$, precisely \mathbf{m}_b , is encrypted into ciphertext $\text{Enc}(\mathbf{m}_b)$ and returned to \mathcal{A} ;*
3. *Upon observing $\text{Enc}(\mathbf{m}_b)$, and without knowledge of b , the adversary \mathcal{A} outputs a bit b_0 ;*

4. The experiment output is defined to be 1 if $b_0 = b$, and 0 otherwise; if the experiment output is 1, denoted shortly as the event $(\mathcal{A} \rightarrow 1)$, we say that \mathcal{A} has succeeded.

Definition 2 ([19]). An encryption scheme provides indistinguishable encryption in the presence of an eavesdropper, if for all probabilistic polynomial-time adversaries \mathcal{A} :

$$\Pr[\mathcal{A} \rightarrow 1 | \text{Enc}(\mathbf{m}_b)] \leq \frac{1}{2} + \epsilon, \tag{15}$$

where $\epsilon = \text{negl}(n)$ is a negligibly small function.

Definitions 1 and 2 are more precisely discussed in [19].

4.2. Evaluation of the Security Gain

We consider the encryption/decryption scheme proposed in Section 2 which is a security enhanced scheme of a certain basic one. Our goal is to estimate the advantage of \mathcal{A} in the indistinguishability game specified by Definition 1 when $\mathbf{c} \leftarrow \text{Enc}(\mathbf{m}_b)$ where \mathbf{c} is a particular realization of \mathbf{C} , assuming that the advantage of \mathcal{A} is known when \mathbf{m}_0 and \mathbf{m}_1 are two chosen realizations of \mathbf{M} and the corresponding realization \mathbf{c}'_b of \mathbf{C}' is given, i.e., the advantage of \mathcal{A} is known for the basic (security non-enhanced) scheme.

We assume that in the corresponding statistical model, the considered encryption scheme is such that:

$$I(\mathbf{S}, \mathbf{Y}) = 0 \quad \text{and} \quad I(\mathbf{S}, \mathbf{Y} | \mathbf{M}) = 0, \tag{16}$$

i.e., the knowledge of \mathbf{Y} and \mathbf{M} does not leak (provide) any information on \mathbf{S} .

Lemma 1. We consider the advantage of the adversary \mathcal{A} (specified by Definition 2) to win the indistinguishability game (specified by Definition 1), assuming that the mapping of \mathbf{m} into \mathbf{c}' is such that $\frac{1}{2} + \epsilon$ equals the advantage of the adversary to win the game. Under these assumptions:

$$\begin{aligned} \Pr[\mathcal{A} \rightarrow 1 | \mathbf{Y} = \mathbf{y}] &= \frac{1}{2} + \epsilon \cdot \delta, \\ \delta &\triangleq \Pr(\mathbf{X} = \mathbf{x}''_b | \mathbf{Y} = \mathbf{y}). \end{aligned} \tag{17}$$

Proof. For simplicity, it is assumed that $\frac{1}{2} + \epsilon$ equals the advantage of the adversary \mathcal{A} (specified by Definition 2) to win the indistinguishability game. Consequently, let b which denotes the index of the selected message by realization of the random variable B .

The probability $\Pr(B = b | \mathbf{Y} = \mathbf{y})$ that \mathcal{A} wins the game is determined by the following:

$$\begin{aligned} \Pr(B = b | \mathbf{Y} = \mathbf{y}) &= \frac{\Pr(B=b, \mathbf{Y}=\mathbf{y})}{\Pr(\mathbf{Y}=\mathbf{y})} \\ &= \frac{\sum_{\mathbf{x}} \Pr(B=b, \mathbf{Y}=\mathbf{y}, \mathbf{X}=\mathbf{x})}{\Pr(\mathbf{Y}=\mathbf{y})} \\ &= \frac{\sum_{\mathbf{x}} \Pr(B=b | \mathbf{Y}=\mathbf{y}, \mathbf{X}=\mathbf{x}) \Pr(\mathbf{Y}=\mathbf{y}, \mathbf{X}=\mathbf{x})}{\Pr(\mathbf{Y}=\mathbf{y})} \\ &= \frac{\sum_{\mathbf{x}} \Pr(B=b | \mathbf{X}=\mathbf{x}) \Pr(\mathbf{Y}=\mathbf{y}, \mathbf{X}=\mathbf{x})}{\Pr(\mathbf{Y}=\mathbf{y})}. \end{aligned} \tag{18}$$

The lemma assumption implies:

$$\Pr(B = b | \mathbf{C} = \mathbf{c}_b) = \frac{1}{2} + \epsilon, \tag{19}$$

where \mathbf{c}_b corresponds to the selected \mathbf{m}_b , and:

$$\Pr(B = b | \mathbf{X} = \mathbf{x}) = \frac{1}{2} \quad \text{for any } \mathbf{c} \neq \mathbf{c}_b. \tag{20}$$

Note that the encoding mapping $\mathbf{c} \rightarrow \mathbf{x}$ is a deterministic one-to-one mapping and consequently has no impact on the advantage of adversary \mathcal{A} , i.e., we have:

$$\Pr[\mathcal{A} \rightarrow 1 | \mathbf{X} = \mathbf{x}] = \Pr[\mathcal{A} \rightarrow 1 | \mathbf{C} = \mathbf{c}] = \frac{1}{2} + \epsilon . \tag{21}$$

Consequently:

$$\begin{aligned} \Pr(B = b | \mathbf{Y} = \mathbf{y}) &= \\ &= \frac{\Pr(B = b | \mathbf{X} = \mathbf{x}_b) \Pr(\mathbf{Y} = \mathbf{y}, \mathbf{X} = \mathbf{x}_b)}{\Pr(\mathbf{Y} = \mathbf{y})} + \\ &= \frac{\sum_{\mathbf{x}: \mathbf{x} \neq \mathbf{x}_b} \Pr(B = b | \mathbf{X} = \mathbf{x}) \Pr(\mathbf{Y} = \mathbf{y}, \mathbf{X} = \mathbf{x})}{\Pr(\mathbf{Y} = \mathbf{y})} , \end{aligned}$$

Finally, we obtain:

$$\begin{aligned} \Pr(B = b | \mathbf{Y} = \mathbf{y}) &= \\ &= \frac{(\frac{1}{2} + \epsilon) \Pr(\mathbf{Y} = \mathbf{y}, \mathbf{X} = \mathbf{x}_b) - \frac{1}{2} \Pr(\mathbf{Y} = \mathbf{y}, \mathbf{X} = \mathbf{x}_b)}{\Pr(\mathbf{Y} = \mathbf{y})} \\ &+ \frac{\frac{1}{2} \sum_{\mathbf{x}} \Pr(\mathbf{Y} = \mathbf{y}, \mathbf{X} = \mathbf{x})}{\Pr(\mathbf{Y} = \mathbf{y})} \\ &= \frac{1}{2} + \epsilon \cdot \Pr(\mathbf{X} = \mathbf{x}_b | \mathbf{Y} = \mathbf{y}) . \end{aligned} \tag{22}$$

QED. \square

Definition 1 implies that the security of an encryption scheme increases as the difference on the adversary \mathcal{A} advantage from $\frac{1}{2}$ decreases: The factor $\delta < 1$ shows the reduction rate of the advantage, and so we call it the advantage reduction factor.

Theorem 1. We consider the adversary \mathcal{A} (specified by Definition 2) to win the indistinguishability game (specified by Definition 1). Let the basic encryption mapping $\{0, 1\}^n \rightarrow \{0, 1\}^n$ of \mathbf{m} into \mathbf{c}' , be such that $\frac{1}{2} + \epsilon$ equals the advantage of the adversary. Consequently, the advantage of the adversary \mathcal{A} , in the security enhanced scheme specified in Section 2 is:

$$\Pr[\mathcal{A} \rightarrow 1 | \mathbf{Y} = \mathbf{y}] < \frac{1}{2} + \epsilon \cdot \frac{\Psi(n, \lambda, d_1, d_2, C(d_1), C(d_2)) + 1}{\log_2(2^n - 1)} . \tag{23}$$

where:

$$\begin{aligned} \Psi(n, \lambda, d_1, d_2, C(d_1), C(d_2)) &= \\ &= \lambda C(d_1) + n \bar{\lambda} C(d_2) + 4 \log_2(n + 1) \\ &+ n \bar{d} \log_2(\bar{d}) + n \lambda \bar{d}_1 \log_2(\lambda \bar{d}_1) + n \bar{\lambda} \bar{d}_2 \log_2(\bar{\lambda} \bar{d}_2) \end{aligned} \tag{24}$$

and $\bar{d} = 1 - d$, $d = \lambda d_1 + \bar{\lambda} d_2$, $\bar{\lambda} = 1 - \lambda$. $\bar{d}_1 = 1 - d_1$, $\bar{d}_2 = 1 - d_2$.

Proof. According to the (14) we have:

$$1 - \frac{I(\mathbf{X}, \mathbf{Y})}{n} \leq \frac{1}{n} + \frac{P_{err}}{n} \log_2(2^n - 1) , \tag{25}$$

and taking into account that:

$$P_{err} = 1 - \Pr(\mathbf{X} = \mathbf{x}_b | \mathbf{Y} = \mathbf{Y}) \tag{26}$$

we obtain:

$$\begin{aligned} &\frac{1}{n} \Pr(\mathbf{X} = \mathbf{x}_b | \mathbf{Y} = \mathbf{y}) \log_2(2^n - 1) \\ &\leq -1 + \frac{I(\mathbf{X}, \mathbf{Y})}{n} + \frac{1}{n} + \frac{1}{n} \log_2(2^n - 1) \\ &< \frac{I(\mathbf{X}, \mathbf{Y})}{n} + \frac{1}{n} , \end{aligned} \tag{27}$$

and:

$$\Pr(\mathbf{X} = \mathbf{x}_b | \mathbf{Y} = \mathbf{y}) < \frac{I(\mathbf{X}, \mathbf{Y}) + 1}{\log_2(2^n - 1)} . \tag{28}$$

Finally, taking into account (12) we have:

$$\Pr(\mathbf{X} = \mathbf{x}_b | \mathbf{Y} = \mathbf{y}) < \frac{\Psi(n, \lambda, d_1, d_2, C(d_1), C(d_2)) + 1}{\log_2(2^n - 1)}. \tag{29}$$

Substitution of (29) into the statement of Lemma 1 yields the proof. QED. □

Lemma 1 shows that the encryption mapping $\mathbf{m} \rightarrow \mathbf{c}$ enhances the security because the probability that \mathcal{A} wins the game becomes closer to $\frac{1}{2}$, which corresponds to random guessing, by the factor δ , and Theorem 1 shows that the upper bound on δ is $\ll 1$.

5. Notes on Implementation Issues

As an illustration, this section proposes an instantiate of the generic framework given in Section 2. This section yields particular designs for the following three main parts of the generic framework: (i) encryption scheme; (ii) coding scheme; (iii) simulated noisy channel. *Encryption.* The following Figure 4 displays a model of the encryption box based on a stream cipher: The inputs are the session secret key \mathbf{k} and the plaintext message \mathbf{m} , and the outputs are the ciphertext \mathbf{c} and the control \mathbf{s} of simulated noisy channel.

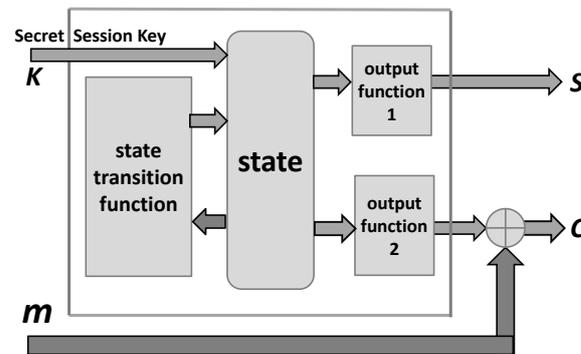


Figure 4. Model of encryption based on a stream cipher.

Note that the above scheme provides all vectors (sequences) required by encryption box in Figure 1, and in particular the vector \mathbf{s} required for the simulation of a noisy channel. *Coding.* As an option for suitable error correction coding we point to the LDPC codes reported in [20,21]. The time and space complexity of these codes is $O(n \log_2 n)$ and $O(n)$, respectively. In order to keep decoding complexity as claimed, the number of errors introduced by the simulated noisy channel should be below the error capability of the employed code, [22]. Otherwise if we are at the error-correcting capability limit we face an increase of the decoding complexity. We assume that up to Δ errors can be corrected with the claimed complexity. In a particular case as reported in [21] (Algorithm C), the time complexity will be $O(g_{max}^2 n)$, where g_{max} is a parameter, providing at the same decoding error-rate.

As an alternative option for suitable error correction coding we also point to the polar codes proposed in [23] and considered in [6,7,24], for example.

Simulated Noisy Channel. The simulated noisy channel box takes the sequence \mathbf{s} as the input and performs its mapping block-by-block in order to obtain three sequences required for the simulated noisy channel composed of two binary erasure channels. Let $\mathbf{s}^{(n)}$ denotes an n -bit segment of \mathbf{s} , and let the functions $f_i(\cdot), i = 1, 2, 3$, perform mapping $\{0, 1\}^n \rightarrow \{0, 1\}^n$ generating the following three binary n -dimensional vectors:

$$\begin{aligned} \ell^{(n)} &= [\ell_i]_{i=1}^n = f_1(\mathbf{s}^{(n)}), \\ \mathbf{e}^{(n,1)} &= [e_i^{(1)}]_{i=1}^n = f_2(\mathbf{s}^{(n)}), \\ \mathbf{e}^{(n,2)} &= [e_i^{(2)}]_{i=1}^n = f_3(\mathbf{s}^{(n)}). \end{aligned}$$

We assume that the functions are such that the following is valid, where $W(\cdot)$ and $Exp(\cdot)$ are the vector weight and the expected value of the weight: (i) $Exp(W(\ell^{(n)})) = n\lambda$; (ii) $Exp(W(\mathbf{e}^{(n,1)})) = nd_1$; (iii) $Exp(W(\mathbf{e}^{(n,2)})) = nd_2$.

Let $\mathbf{x}^{(n)} = [x_i]_{i=1}^n$ be the codeword after the encoding box, and $\mathbf{y}^{(n)} = [y_i]_{i=1}^n$ denotes the degraded codeword after the simulated noisy channel according to the following algorithm. Please note that in order to keep the number of the erased bits within the error correction capability of the employed code, the parameter Δ^* is used: When the number of already erased bits is greater than Δ^* , the probability of erasures should be reduced, and accordingly, there are two different rules regarding appearance of the output bit as "?". Consequently, we consider the following simulator of the noisy channel.

Simulated Noisy Channel

- *Input:* $\mathbf{x}^{(n)} = [x_i]_{i=1}^n$, the parameter $\Delta^* < \Delta$
- set $w = 1$.
- do $i = 1, n$
 - if $w \leq \Delta^*$
 - $y_i = ?$ and $w = w + 1$ if $\ell_i \cdot e_i^{(1)} = 1$ or $\ell_i \cdot e_i^{(2)} = 1$
 - $y_i = x_i$ otherwise
 - if $w > \Delta^*$
 - $y_i = ?$ if $\ell_i \cdot e_i^{(2)} = 1$
 - $y_i = x_i$ otherwise
- *Output:* $\mathbf{y}^{(n)} = [y_i]_{i=1}^n$

Note that for the legitimate receiver, $\mathbf{y}^{(n)}$ appears as the codeword $\mathbf{x}^{(n)}$ after the binary erasures channels. On the other hand, because the attacker does not know the sequence \mathbf{s} , $\mathbf{y}^{(n)}$ appears as the codeword $\mathbf{x}^{(n)}$ after the binary deletion channels displayed in Figure 3.

6. Conclusions

This paper proposes a generic design for a measurable cryptographic security enhancement of certain secret key encryption schemes. This security enhancement is based on the following (see Figure 1): (i) employment of an error correction coding, (ii) splitting the codeword into two parts in the secret key dependent manner; and (iii) degradation each of the codeword parts by simulated binary erasure channels where the erasures are secret key dependent.

Note that for an attacker that does not know the secret key, the resulting channel appears as a simulated deletion channel. The security enhancement is quantified employing reported results on the capacity of the related two parallel binary deletion channels. The reported upper bound on the resulting channel capacity is established employing the upper bound on the mutual information between the inputs and outputs of the component deletion channels. The final lower bound on the achieved security gain is derived by employing relations between the probability of correct decoding and the mutual information between input and output of the resulting channel.

It is shown that the enhancement is a function of the following parameters: probabilities of deletion in the sub-channels, capacity of the sub-channels and the probability of the sub-channel selection for the transmission. Consequently, a desirable security enhancement, as well as, the implementation complexity could be achieved based on a suitable selection of the parameters related to the the employed channels and the coding scheme.

Accordingly, the main contributions of this paper are: (i) novel design of an encryption scheme which employs dedicated coding and simulated noisy channels that, from an attacker perspective, appear as binary deletion channels; and (ii) its cryptographic security evaluation, based on mutual information between input and output of certain channel with bits deletion, employing the adversarial indistinguishably experiment. It is out of the scope

of this paper to discuss in detail particular implementations of the proposed framework, and so just illustrative notes are given regarding a possible implementation approach.

Author Contributions: conceptualization, M.J.M.; methodology, M.J.M.; validation, M.J.M., L.W. and S.X.; formal analysis, M.j.M; writing—original draft preparation, M.J.M.; writing—review and editing, M.J.M., L.W. and S.X.; supervision, L.W. and S.X.; project administration, L.W. and S.X.; funding acquisition, L.W. and S.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Shandong Provincial Key Research and Development Program (2020CXGC010107, 2019JZZY020129), the Science, Education and Industry Integration Innovation Program of Qilu University of Technology (Shandong Academy of Science) (2020KJC-GH11).

Conflicts of Interest: The authors declare no conflict of interest.

References

- Rivest, R.; Sherman, T. Randomized Encryption Techniques. In *Advances in Cryptology: Proceedings of CRYPTO '82*; Plenum: New York, NY, USA, 1983; pp. 145–163.
- Willett, M. Deliberate noise in a modern cryptographic system. *IEEE Trans. Inf. Theory* **1980**, *26*, 102–104. [[CrossRef](#)]
- Esmaili, M.; Dakhilalian, M.; Gulliver, T.A. New secure channel coding scheme based on randomly punctured quasi-cyclic-low density parity check codes. *IET Commun.* **2014**, *8*, 2556–2562. [[CrossRef](#)]
- Esmaili, M.; Gulliver, T.A. Joint channel coding-cryptography based on random insertions and deletions in quasi-cyclic-low density parity check codes. *IET Commun.* **2015**, *9*, 1555–1560. [[CrossRef](#)]
- Esmaili, M.; Gulliver, T.A. A Secure Code Based Cryptosystem via Random Insertions, Deletions, and Errors. *IEEE Commun. Lett.* **2016**, *20*, 870–873. [[CrossRef](#)]
- Hooshmand, R.; Aref, M.R.; Eghlidos, T. Physical layer encryption scheme using finite-length polar codes. *IET Commun.* **2015**, *9*, 1857–1866. [[CrossRef](#)]
- Hooshmand, R.; Aref, M.R. Efficient Polar Code-Based Physical Layer Encryption Scheme. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 710–713. [[CrossRef](#)]
- Mihaljević, M.J.; Imai, H. An approach for stream ciphers design based on joint computing over random and secret data. *Computing* **2009**, *85*, 153–168. [[CrossRef](#)]
- Khiabani, Y.S.; Wei, S.; Yuan, J.; Wang, J. Enhancement of Secrecy of Block Ciphered Systems by Deliberate Noise. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1604–1613. [[CrossRef](#)]
- Mihaljević, M.J. An Approach for Light-Weight Encryption Employing Dedicated Coding. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 892–898. ISBN 978-1-4673-0919-6.
- Wei, S.; Wang, J.; Yin, R.; Yuan, J. Trade-Off Between Security and Performance in Block Ciphered Systems with Erroneous Ciphertexts. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 636–645.
- Oggier, F.; Mihaljević, M.J. An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 158–168. [[CrossRef](#)]
- Mihaljević, M.J.; Kavčić, A.; Matsuura, K. An Encryption Technique for Provably Secure Transmission from a High Performance Computing Entity to a Tiny One. *Math. Probl. Eng.* **2016**, *2016*, 7920495. [[CrossRef](#)]
- Mihaljević, M.J.; Oggier, F. Security Evaluation and Design Elements for a Class of Randomized Encryptions. *IET Inf. Secur.* **2019**, *13*, 36–47. [[CrossRef](#)]
- Mihaljević, M.J. A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security. *Entropy* **2019**, *21*, 701. [[CrossRef](#)] [[PubMed](#)]
- Rahmati, M.; Duman, T.M. Upper Bounds on the Capacity of Deletion Channels Using Channel Fragmentation. *IEEE Trans. Inf. Theory* **2015**, *61*, 146–156. [[CrossRef](#)]
- Tebbe, D.L.; Dwyer, S.J., III. Uncertainty and the Probability of Error. *IEEE Trans. Inf. Theory* **1968**, *IT-24*, 516–518. [[CrossRef](#)]
- Feder, M.; Merhav, N. Relations between entropy and error probability. *IEEE Trans. Inf. Theory* **1994**, *40*, 259–266. [[CrossRef](#)]
- Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2007.
- Luby, M.G.; Mitzenmacher, M.; Shokrollahi, M.A.; Spielman, D.A. Efficient Erasure Correcting Codes. *IEEE Trans. Inf. Theory* **2001**, *47*, 569–584. [[CrossRef](#)]
- Pishro-Nik, H.; Fekri, F. On Decoding of Low-Density Parity-Check Codes Over the Binary Erasure Channel. *IEEE Trans. Inf. Theory* **2004**, *50*, 439–454. [[CrossRef](#)]
- Rybin, P.; Andreev, K.; Zyablov, V. Error Exponents of LDPC Codes under Low-Complexity Decoding. *Entropy* **2021**, *23*, 253. [[CrossRef](#)]
- Arkan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 3051–3073. [[CrossRef](#)]
- Thomas, E.K.; Tan, V.Y.F.; Vardy, A.; Motani, M. Polar coding for the binary erasure channel with deletions. *IEEE Commun. Lett.* **2017**, *21*, 710–713. [[CrossRef](#)]