On Perfect Endomorphic Ciphers

Nikolay Shenets[0000−0002−1399−1822]

Peter the Great St. Petersburg Polytechnic University, St. Petersburg 195251, Russia
shenets@ibks.spbstu.ru

Abstract. It has been 70 years since the publication of the seminal outstanding work of Claude Elwood Shannon, in which he first gave a mathematical definition of the cryptosystem and introduced the concept of perfect ciphers. He also examined the conditions in which such a ciphers exist. Shannon's results in one form or another are presented in almost all books on cryptography. One of his result deals with so-called *endomorphic ciphers* in which the cardinalities of the message space $\mathcal{M}$ and the ciphertexts $\mathcal{C}$ are the same. The Vernam cipher (one-time pad) is the most famous representative of such ciphers. Moreover, it's the only one known to be perfect.
Surprisingly, we have found a mistake in the Shannon's result. Namely, Shannon stated that an endomorphic cipher, in which the keyspace $\mathcal{K}$ has the same cardinality as message space, is perfect if and only if two conditions are satisfied. The first suggests that for any pair plaintext–ciphertext there exists only one key that translates this plaintext into this ciphertext. The second argues that the key distribution must be uniform. We show, that these two conditions are not really enough. We prove in three different ways that the plaintexts must also be equally probable. Moreover, we study the general endomorphic cipher and get the same result. It follows, that in practice perfect endomorphic ciphers do not exist.

Keywords: Perfect security · Endomorphic cipher · Shannon's theory

1 Introduction

In 1949 Claude Elwood Shannon introduced his outstanding work "Communication Theory of Secrecy Systems" [1]. He laid the foundation of modern mathematical cryptography. We do not discuss all of Shannon's results as they are well known. For example, one can refer to famous book "Cryptography: Theory and Practice" by Douglas Stinson [2]. Let us focus on only one result of Shannon related to the perfect endomorphic ciphers.

Shannon stated (see page 681 of his original work [1]): "Perfect systems in which the number of cryptograms, the number of messages, and the number of keys are all equal are characterized by the properties that (1) each M is connected to each E by exactly one line, (2) all keys are equally likely. Thus the matrix representation of the system is a "Latin square". In this statement M is the message and E is corresponding ciphertext. The phrase "is connected with

exactly one lines" means that there exists only one key which encrypts M to E. We show that this two conditions are not enough. Really, the plaintexts must also be equally probable. We prove this fact in three different ways. Therefore, there is no doubt about the truth of our contribution.

We note that some inconsistency in this Shannon's result had previously discovered by Babash and Shankin [3]. They introduced two separate notions of "*perfectness by the ciphertext*" and "*perfectness by the key*" and showed that they are not equivalent. The "perfect by the ciphertext" cipher is the same as Shannon's perfect cipher. The "perfect by the key" cipher satisfies following condition:

$$P_E(K) = P(K), \qquad \text{where } K \text{ is the key (see notations below).}$$

It means, that it is impossible to attack the key by ciphertexts. On the one hand, Shannon aims to describe all ciphers which can not be decrypted without knowing the key. On the other hand, if we can obtain a valid key, than we can decrypt ciphertext. So a really perfect cryptosystem need to be not only "perfect by the ciphertext" but also "perfect by the key". Note, that the Shannon's model is fully defined by the message distribution and the key distribution. And we don't have any contradiction with the main Shannon's theorem 6 which now is the definition of perfect cipher. From this reasoning we conclude that Shannon was wrong in his statement about perfect endomorphic ciphers.

2 Preliminaries

Recall the Shannon's cipher model and the adversary model. We try to keep all Shannon's notations. Namely, let $M \in \mathcal{M}$ be a message, $E \in \mathcal{C}$ be a ciphertext and $K \in \mathcal{K}$ be a key.

Definition 1. *A cryptosystem C is a five-tuple $\langle \mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{E}, \mathcal{D} \rangle$, where the following conditions are satisfied:*

1. *$\mathcal{K}$, the keyspace, is a finite set of possible keys;*
2. *$\mathcal{M}$ is a finite set of possible plaintexts (messages);*
3. *$\mathcal{C}$ is a finite set of possible ciphertexts;*
4. *For each $K \in \mathcal{K}$, there is an encryption rule $Enc(K, M) \in \mathcal{E}$ and a corresponding decryption rule $Dec(K, E) \in \mathcal{D}$. Each $Enc(K, M) : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ and $Dec(K, E) : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ are functions such that $Dec(K, Enc(K, M)) = M$ for every plaintext element $M \in \mathcal{M}$.*

The cryptosystem is called *endomorphic* if $|\mathcal{M}| = |\mathcal{C}|$. We use following notations:

$P(M)$ — *a priory* probability of message M;
$P(K)$ — *a priory* probability of key K;
$P_M(E)$ — conditional probability of ciphertext E if message M is chosen i.e. the sum of the probabilities of all keys which produce ciphertext E from message M;
$P_K(E)$ — conditional probability of ciphertext E if key K is chosen i.e. the sum of the probabilities of all messages which produce ciphertext E with the key K;
$P(E)$ — probability of obtaining ciphertext E from any cause;
$P_E(M)$ — *a posteriori* probability of message M if ciphertext E is intercepted;
$P_E(K)$ — *a posteriori* probability of key K if ciphertext E is intercepted;

Shannon considered the case of *ciphertext–only attack*: the adversary possesses a string of ciphertext. But at the same time, the adversary has unbounded computational resources. It is assumed in the model, that the message M and the key K are independent random variables with some distributions $P(M)$ and $P(K)$ correspondingly. Moreover, $P(M) > 0$ for all $M \in \mathcal{M}$ and $P(K) > 0$ for all $K \in \mathcal{K}$. So the ciphertext E is also random variable with distribution $P(E)$:

$$P(E) = \sum_{M \in \mathcal{M}} P_M(E) \cdot P(M), \text{ where} \tag{1}$$

$$P_M(E) = \sum_{K \in \mathcal{K}: Enc(K,M)=E} P(K). \tag{2}$$

The cryptosystem is called *perfect* by Shannon (see his theorem 6) if $P_M(E) = = P(E)$. This definition is equivalent to $P_E(M) = P(M)$ as the message M and the key K are independent. Now we reformulate the Shannon's statement that we analyze in this paper.

Theorem 1. *Let* $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$.
The cryptosystem $C = \langle \mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{E}, \mathcal{D} \rangle$ *is perfect if and only if it satisfies two conditions:*

1. *For each* M *and* E *there is only one solution to the equation* $Enc(K, M) = E$ *under the key* K.
2. *The distribution of the key is uniform, i.e.* $P(K) = \frac{1}{|\mathcal{K}|}$.

3 The Main Result

We state that the following theorem is true.

Theorem 2. *Let* $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$.
The cryptosystem $C = \langle \mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{E}, \mathcal{D} \rangle$ *is perfect if and only if it satisfies three conditions:*

1. *For each M and E there is only one solution to the equation $Enc(K, M) = E$ under the key K.*
2. *The distribution of the key is uniform, i.e. $P(K) = \frac{1}{|\mathcal{K}|}$.*
3. *The distribution of the plaintext is uniform, i.e. $P(M) = \frac{1}{|\mathcal{M}|}$.*

Proof. We prove this theorem in three different ways. We need to prove only the last statement. So we can assume that the first two are true.

The first method — by the direct calculations. Let $E = Enc(K', M)$. The following sequence of equations is true:

$$P(M) = P_E(M) = \sum_{K_i \in \mathcal{K}} P(Dec(K_i, E) = M)P(K = K_i) = P(K = K') = \frac{1}{|\mathcal{M}|}.$$

The first equations is true by the definition of perfect cipher. The second is true by the total probability low. The third equation is true by the following observation:

$$\exists!\, K_i \in \mathcal{K} : Dec(K_i, E) = M \Rightarrow P(Dec(K_i, E) = M) = \begin{cases} 1, & \text{if } K_i = K'; \\ 0, & \text{otherwise.} \end{cases}$$

The second method — by the theory of functions under random variables. Note, that the ciphertext E is the random variable which is calculated by the function Enc with two independent random arguments M and K. Moreover, from the first statement of the theorem follows, that this function is bijection under its arguments. So the random variable E has the uniform distribution.

On the other hand, $M = Dec(K, E)$, and the decryption function is also a bijection under its arguments. As the cipher is perfect, we conclude that the random variables K and E are independent. So the plaintext M of the endomorphic perfect cipher also has the uniform distribution.

The third method — by contradiction. Assume, that the plaintext M has non-uniform distribution. It is known that the condition $P_E(K) = P(K)$ for any K and E is equivalent to the condition $P_K(E) = P(E)$ for any K and E. Note, that E has the uniform distribution (see above). Obviously, $P_K(E) = = P(M)$ for the plaintext M encrypted with the key K into E. The assertion follows directly from our assumption.

Example 1. Let's consider an example. Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_3$ and $P(M = 0) = = 3/4$, $P(M = 1) = P(M = 2) = 1/8$. Choose the message $Mess = 00102000$. Suppose, the sender has chosen a sequence of keys 01122100 and encrypted the message $Mess$ by simple one-time pad to the ciphertext 01221100. Let's see what the adversary can get if she acts according to the maximum likelihood estimation method.

It is easy to see, that

$$P_{E_j}(K_i) = \frac{P_{K_i}(E_j) \cdot P(K_i)}{P(E_j)} = \frac{P(M_{ij} : M_{ij} = Dec(K_i, E_j)) \cdot 1/3}{1/3} = P(M_{ij}),$$

And therefore,

$$P_E(K) = \begin{cases} 3/4, & \text{if } K = E; \\ 1/8, & \text{otherwise.} \end{cases}, \text{ for each } K \in \mathcal{K},\ E \in \mathcal{C}.$$

Thus, the adversary simply decrypts the ciphertext 01221100 to 00000000. We see, that exactly 3/4 of the entire message $Mess$ is decrypted correctly.

Further, we study all other endomorphic ciphers. Namely, the condition $n = |\mathcal{M}| = |\mathcal{C}| < |\mathcal{K}|$ is satisfied. Obviously, it is sufficient to consider the case, when the keyspace doesn't contain the pairs (K_1, K_2) of equivalent keys, such that $Enc(K_1, M) = Enc(K_2, M)$ for all $M \in \mathcal{M}$. Otherwise, we divide the keyspace into equivalent key classes and talk about each class as a separate key. We get the following result.

Theorem 3. *Let $|\mathcal{M}| = |\mathcal{C}| < |\mathcal{K}|$ and there are no equivalent keys, i.e. $\nexists\, K_1, K_2 \in \mathcal{K} : Enc(K_1, M) = Enc(K_2, M)$ for all $M \in \mathcal{M}$. The cryptosystem $C = \langle \mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{E}, \mathcal{D} \rangle$ is perfect if and only if it satisfies conditions:*

1. *For each key $K \in \mathcal{K}$ the functions $Enc(K, M)$ and $Dec(K, E)$ are substitutions from the symmetric group S_n. Moreover, $Dec(K, E) = Enc^{-1}(K, M)$.*
2. *Both the distribution of plaintext and ciphertext are uniform, i.e. $P(M) = P(E) = 1/n$.*
3. *The distribution of keys is the solution of the linear system of equations:*

$$\sum_{K \in \mathcal{K}: Enc(K,M)=E} P(K) = 1/n \text{ for all } M \in \mathcal{M}, E \in \mathcal{C}. \tag{3}$$

Proof. The first statement of the theorem is obvious and follows from the definition 1. Indeed, for any fixed key $K \in \mathcal{K}$ the map $Enc(K, M)$ is injective. But we have $n = |\mathcal{M}| = |\mathcal{C}|$ and so it is a bijection.

Suppose, that the cipher C is perfect. Let's fix some message $M \in \mathcal{M}$ and ciphertext $E \in \mathcal{C}$. By definition (see formula (2)), we have the following equations:

$$P(M) = P_E(M) = \sum_{K \in \mathcal{K}: Dec(K,E)=M} P(K), \tag{4}$$

$$P(E) = P_M(E) = \sum_{K \in \mathcal{K}: Enc(K,M)=E} P(K). \tag{5}$$

But we know, that $Enc(K, M)$ is substitution, and if $Enc(K, M) = E$, then $Dec(K, E) = M$ and vise versa. So, both sums in the equations (4)-(5) contain the same summands. And therefore, $P(M) = P(E)$ for all $M \in \mathcal{M}$, $E \in \mathcal{C}$. This proves the second statement.

The third statement also follows from the definition of perfect cipher. Indeed, the system (3) can be obtained simply by substitution $P(E) = 1/n$ into the equation (5).

Conversely, suppose the three hypothesized conditions are satisfied. Then the cryptosystem C is easily seen to provide perfect secrecy. The proof is completed.

Remark 1. One can calculate a posteriori probability $P_E(K)$ using Bayes' theorem:

$$P_E(K) = \frac{P_K(E) \cdot P(K)}{P(E)} = \frac{P(M) \cdot P(K)}{P(E)} = P(K).$$

Thus, we see, that the perfect cipher also satisfies the "*perfectness by the key*" condition.

Remark 2. We do not know if there is a solution to the system (3) under given mappings $Enc(K, M)$ and $Dec(K, E)$. So it is an open question. But in the following statement we consider the common case, when the keys are equiprobable.

Corollary 1. *Under the conditions of theorem 3, if the distribution of keys is uniform, then the endomorphic cryptosystem C is perfect if and only if it satisfies:*

1. *For each key $K \in \mathcal{K}$ the functions $Enc(K, M)$ and $Dec(K, E)$ are substitutions from the symmetric group S_n. Moreover, $Dec(K, E) = Enc^{-1}(K, M)$.*
2. *Both the distribution of plaintext and ciphertext are uniform.*
3. *$|\mathcal{K}| = m \cdot n$, and for each pair $M \in \mathcal{M}$ and $E \in \mathcal{C}$ there are exactly m distinct keys which encrypts M to E and decrypts E to M.*

Proof. The first two statements are already proved in theorem 3. As the distribution of keys is uniform, from the equation (5) and system (3) we have:

$$P(M) = P(E) = m \cdot P(K), \text{ for some constant value } m > 1.$$

Therefore, $|\mathcal{K}| = m \cdot n$. Further, each row of the system (3) corresponds to the conditional probability $P_M(E)$. Thus, for each pair M and E there are exactly m keys which encrypts M to E. It is follows from the first statement, that these are the keys which decrypts E to M. Note, that in system (3), all rows that correspond to fixed value E do not intersect. Each column of this system contains exactly n units.

In the opposite direction, the proof is obvious. The proof is completed.

Note, that the system (3) contains exactly n^2 equations. But the number of keys can be any value from n up to $n!$. When $l = |\mathcal{K}| > n^2$, the system (3) always has a solution. But we don't aware that there is such a solution $(P(K_1), P(K_2), \ldots, P(K_l)$ that satisfies the probability distribution rule $0 \leq P(K_i) \leq 1$ for all $i = \overline{1, l}$. At the same time, the normalization condition is always met. Indeed, if we sum up all rows, we get the equation $\sum_{i=1}^{l} P(K_i) = 1$. Finally, we give some nontrivial examples.

Example 2. First, we show, that there is perfect endomorphic cipher with the non-uniform distribution of keys. We associate each key $K \in \mathcal{K}$ with substitution $Enc(K, \cdot)$. Let $\mathcal{M} = \mathcal{C} = \{1, 2, 3, 4\}$, the plaintexts are all equiprobable, and the cipher C be determined by the following substitutions from S_4:

$$K_1 \to \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \quad K_2 \to \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \quad K_3 \to \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}, \quad K_4 \to \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},$$
$$K_5 \to \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}, \quad K_6 \to \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}, \quad K_7 \to \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}, \quad K_8 \to \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}.$$

Let's make a linear system of equations for this example according to (4).

$$\begin{gathered}
P(M=1|E=1) = P(K_5) + P(K_8) = 1/4;\\
P(M=1|E=2) = P(K_1) + P(K_6) = 1/4;\\
P(M=1|E=3) = P(K_2) + P(K_4) = 1/4;\\
P(M=1|E=4) = P(K_3) + P(K_7) = 1/4;\\
P(M=2|E=1) = P(K_4) + P(K_7) = 1/4;\\
P(M=2|E=2) = P(K_2) + P(K_3) = 1/4;\\
P(M=2|E=3) = P(K_1) + P(K_8) = 1/4;\\
P(M=2|E=4) = P(K_5) + P(K_6) = 1/4;\\
P(M=3|E=1) = P(K_2) + P(K_6) = 1/4;\\
P(M=3|E=2) = P(K_5) + P(K_8) = 1/4;\\
P(M=3|E=3) = P(K_3) + P(K_7) = 1/4;\\
P(M=3|E=4) = P(K_1) + P(K_4) = 1/4;\\
P(M=4|E=1) = P(K_1) + P(K_3) = 1/4;\\
P(M=4|E=2) = P(K_4) + P(K_7) = 1/4;\\
P(M=4|E=3) = P(K_5) + P(K_6) = 1/4;\\
P(M=4|E=4) = P(K_2) + P(K_8) = 1/4;
\end{gathered}$$

The rank of this system is 7, and the solution has the form $(P(K_1), P(K_1), 1/4 - P(K_1), 1/4 - P(K_1), P(K_1), 1/4 - P(K_1), P(K_1), 1/4 - P(K_1)$. As we see, for any $0 < P(K_1) < 1/4$, $P(K_1) \neq 1/8$, there is the non-uniform distribution of keys, that corresponds to the given perfect cipher C.

Example 3. In this example, we consider more sophisticated case. Namely, we choose the key K_1 in such a way, that $P(K_1) = 1/4$. All other keys are distributed non-uniformly. To do it, we select substitutions in a special way. For the key K_1 we select the substitution $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$. And for other keys we select all substitutions that don't map 1 to 2, 2 to 3, 3 to 4 and 4 to 1. Then we get the following keys.

$$K_1 \to \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \quad K_2 \to \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad K_3 \to \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}, \quad K_4 \to \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},$$
$$K_5 \to \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, \quad K_6 \to \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \quad K_7 \to \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \quad K_8 \to \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},$$
$$K_9 \to \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}, \quad K_{10} \to \begin{pmatrix}1&2&3&4\\4&2&1&4\end{pmatrix}.$$

As in the previous example, we obtain a system of equations:

$$\begin{array}{ll}
P(M=1|E=1)=P(K_2)+P(K_3)+P(K_4) & =1/4;\\
P(M=1|E=2)=P(K_1) & =1/4;\\
P(M=1|E=3)=P(K_5)+P(K_6)+P(K_7) & =1/4;\\
P(M=1|E=4)=P(K_8)+P(K_9)+P(K_{10}) & =1/4;\\
P(M=2|E=1)=P(K_5)+P(K_8)+P(K_9) & =1/4;\\
P(M=2|E=2)=P(K_2)+P(K_6)+P(K_{10}) & =1/4;\\
P(M=2|E=3)=P(K_1) & =1/4;\\
P(M=2|E=4)=P(K_3)+P(K_4)+P(K_7) & =1/4;\\
P(M=3|E=1)=P(K_6)+P(K_7)+P(K_{10}) & =1/4;\\
P(M=3|E=2)=P(K_3)+P(K_5)+P(K_8) & =1/4;\\
P(M=3|E=3)=P(K_2)+P(K_4)+P(K_9) & =1/4;\\
P(M=3|E=4)=P(K_1) & =1/4;\\
P(M=4|E=1)=P(K_1) & =1/4;\\
P(M=4|E=2)=P(K_4)+P(K_7)+P(K_9) & =1/4;\\
P(M=4|E=3)=P(K_3)+P(K_8)+P(K_{10}) & =1/4;\\
P(M=4|E=4)=P(K_2)+P(K_5)+P(K_6) & =1/4;
\end{array}$$

The rank of this system is 7, and the solution has the form:
$(1/4, 1/4-P(K_6)-P(K_{10}), P(K_9), P(K_{10})+P(K_6)-P(K_9), P(K_{10}), P(K_6), 1/4-P(K_6)-P(K_{10}), 1/4-P(K_{10})-P(K_9), P(K_9), P(K_{10}))$. For instance, let $P(K_6)=P(K_9)=1/16$, $P(K_{10})=1/8$. Then we get the following distribution: $(1/4, 1/16, 1/16, 1/8, 1/8, 1/16, 1/16, 1/16, 1/16, 1/8)$.

4 Conclusions

We show that one of the Shannon's result has a mistake and correct it. Further, we study the general perfect endomorphic cryptosystem. Unfortunately, we show, that the perfect endomorphic cryptosystem exists only if the plaintext has uniform distribution. Therefore, in practice there is no endomorphic perfect ciphers as the plaintexts are always has non-uniform distribution. In particular, the famous one-time pad is not a perfect cipher. It is only asymptotically perfect when the length of the text tends to infinity.

Moreover, this result will have a negative impact on all stream ciphers, as their goal is to bring the encryption closer to a one-time pad. But the iterative block ciphers are still suitable and really can be proven secure against more powerful adversary. Indeed, we can assume, that the d-round block cipher encrypts the plaintext that is obtained after the $d-1$ rounds. And since we believe, that after $d-1$ rounds the plaintext has the uniform distribution, we can talk about perfectness of d-round block cypher.

Finally, we want to emphasize that we still have an unresolved problem related to the solution of the system (3). It is the interesting question when this system has a solutions and how to describe them all.

References

1. Shannon, C. E.: Communication theory of secrecy systems. Bell System Technical Journal **28**, 656–715 (1949)
2. Stinson, D. R.: Cryptography: Theory and Practice. CRC Press, Boca Raton, Florida (1995)
3. Babash, A. V., Shankin, G. P.: Cryptography. SOLON-R, Moskow, Russia (2002) (in Russian)