

# Re: Confirmation of Shannon s Mistake about Perfect Secrecy of One-time-pad

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg03986.html>

---

- *From:* [matt271829-news@xxxxxxxxxxx](mailto:matt271829-news@xxxxxxxxxxx)
  - *Date:* Mon, 22 Oct 2007 07:07:40 -0700
- 

On Oct 22, 5:22 am, wangyong <hell...@xxxxxxx> wrote:

Confirmation of Shannon s Mistake about Perfect Secrecy of One-time-pad

Yong WANG

School of Computer and Control, GuiLin University Of Electronic Technology ,Guilin, 541004, Guangxi Province, China  
hell...@xxxxxxx

Abstract: This paper analyzes Shannon s proof that one-time-pad is perfectly secure and discusses all the possibilities, and then confirms which of them is Shannon s notion. The confirmed notion is found to be wrong for its neglect of the prior probability and the absolutely irreconcilable conditions. Therefore, one-time-pad is not perfectly secure.

Keywords: one-time system, cryptography, perfect secrecy, information theory, probability

## 1. Introduction

Shannon put forward the concept of perfect secrecy and proved that one-time-pad (one-time system, OTP) was perfectly secure [1, 2]. For a long time, OPT has been thought to be unbroken and is still used to encrypt high security information. In literature [3], example was given to prove that OPT was not perfectly secure. In literature [4], detailed analyses about the mistake of Shannon s proof were given.. It was proven that more requirements are needed for OTP to be perfectly secure and homophonic substitution could make OTP approach perfect secrecy [5]. Literature [6] analyzed the problem and gave ways to disguise the length of plaintext. In literature [7], the cryptanalysis method based on probability was presented, and the method was used to attack one-time-pad. Literature [4] considered an especially understanding following which OTP could be thought perfectly secure if some added conditions were satisfied. In this paper, I will confirm that the especially understanding is not Shannon s notion and analyze the source of his mistake.

## 2. Counterexample of Shannon s Conclusion

For the moment, we do not consider the inaccessible limitation that the length of any plaintext must be the same as the length of ciphertext in OTP. The following discussion supposes the all the

## Re: Confirmation of Shannon's Mistake about Perfect Secrecy of One-time-pad

plaintexts, ciphertexts and keys are the same in length.

We give a simple example of OPT to discuss the problem, plaintext space is  $M = \{0,1\}$ , ciphertext space is  $C = \{0,1\}$  and key space is  $K = \{0,1\}$ . According to the information that cryptanalysts got beforehand, they can get the prior probability of plaintext as  $P(M=0) = 0.9$  and  $P(M=1) = 0.1$ . Later the ciphertext  $C=0$  is intercepted. When only considering  $C=0$  and the cryptosystem (regardless of the prior probability of plaintext), we can deduce that the plaintexts are equally likely, for there is a one-to-one correspondence between all the plaintexts and keys for  $C=0$ . The prior probabilities of plaintexts are seldom the same, so the two probability distributions of plaintexts gained from different conditions are conflicting. Then the compromise of the two probability distributions is indispensable. The compromised posterior probability of the plaintext would be between the two corresponding probabilities of the two sectional conditions. When  $C=0$  is intercepted, the posterior probability  $P(M=0)$  is between 0.9 and 0.5, and  $P(M=1)$  is between 0.1 and 0.5. The compromised posterior probability of the plaintext isn't equal to the prior probability, so OTP is not perfectly secure.

[Repost due to continuing problems with Google Groups. Apologies for any duplications.]

Let's say that the prior probabilities are  $\Pr(M=0) = p$  and  $\Pr(M=1) = 1-p$ . We assume that the key is chosen randomly, independently of  $M$ . So,  $\Pr(K=0) = 1/2$  and  $\Pr(K=1) = 1/2$ , independent of  $M$ . And let's say, just to be explicit, that  $K=0$  maps  $0 \rightarrow 0, 1 \rightarrow 1$ , and  $K=1$  maps  $0 \rightarrow 1, 1 \rightarrow 0$ . We intercept the encrypted message  $C=0$ . Then,

$$\Pr(M=0|C=0) = \Pr(M=0 \& C=0)/\Pr(C=0) = (p \cdot 1/2)/(p \cdot 1/2 + (1-p) \cdot 1/2) = p$$

$$\Pr(M=1|C=0) = \Pr(M=1 \& C=0)/\Pr(C=0) = ((1-p) \cdot 1/2)/(p \cdot 1/2 + (1-p) \cdot 1/2) = 1-p$$

So, intercepting and reading the message has, as expected, yielded no new information.

.