

Analyses of Mistake on Proof about Perfect Secrecy of One-time-pad

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg03896.html>

- *From:* wangyong <hellowy@xxxxxxx>
 - *Date:* Sun, 21 Oct 2007 18:58:58 -0700
-

Analyses of Mistake on Proof about Perfect Secrecy of One-time-pad

Yong WANG

School of Computer and Control, GuiLin University Of Electronic
Technology ,Guilin City, Guangxi Province , China, 541004

hellowy@xxxxxxx

Abstract: This paper analyzes the proofs that one-time system is perfectly secure, and confirms that they are wrong. The mistakes lie in that the conditions of the probabilities are not the same when using probability theory to compute the probabilities. One example is shown to undress the mistakes and bring forth the need of compromise of probabilities.

Keywords: one-time-pad, cryptography, perfect secrecy, probability, unbreakable

1. Introduction

Shannon put forward the concept of perfect secrecy and proved that one-time-pad (OTP) is perfectly secure [1, 2]. For a long time, OPT has been thought to be unbreakable and is still used to encrypt high security information. In literature [3], one example was given to prove that OPT was not perfectly secure. In literature [4], detailed analysis about the mistakes of Shannon's proof was given. It was proven that more conditions were needed for OTP to be perfectly secure and homophonic substitution enabled OTP to approach perfect secrecy[5]. Literature [6] analyzed this problem and presented the approach to disguise the length of plaintext. In literature [7], the cryptanalysis method based on probability was presented to attack one-time-pad. All the above studies analyzed Shannon's proof on the problem. We know Shannon first proved that OTP was perfectly secure, but his proof is very simple. Detailed proofs about perfect secrecy of OTP were given by later scholars who used Shannon's proof for reference. This paper aims to analyze these proofs other than Shannon's and confirms that they are wrong.

2. Representative Proof about Perfect Secrecy of OTP

There are many proofs about perfect secrecy of OTP. Some proofs directly draw the conclusion that all plaintexts are equally likely. But it is obviously wrong, for the prior probabilities of all plaintexts are seldom equally likely. Others are generally identical with minor differences. The representative proof is as follows:

Analyses of Mistake on Proof about Perfect Secrecy of One-time-pad

Theorem: OTP is perfectly secure.

Proof: Assume that M and C are n bits long.

then

$$P(M = x | C = y) =$$

$$P(M = x | C = y) = P(M = x \wedge K = (x \oplus y))$$

$$= P(M = x) \cdot P(K = (x \oplus y)) \quad (K \text{ is independent of } M)$$

$$= P(M = x) \cdot 2^{-n} \quad (K \text{ is chosen uniformly from bit strings of length } n)$$

$$\text{Also, } P(C = y) = \sum_x P(M = x \wedge C = y)$$

$$= \sum_x P(M = x) \cdot 2^{-n} \quad (\sum_x P(M = x) = 1)$$

$$= 2^{-n} \quad (\text{that is, each } C \text{ is equally likely}).$$

$$\text{So, } P(M = x | C = y) = P(M = x)$$

3. Mistake Analyses on Proof

Shannon misused Bayes' formula, similarly the above proof misused Bayes' formula. From $P(M = x) \cdot P(K = (x \oplus y)) = P(M = x) \cdot 2^{-n}$, we can see the condition that the ciphertext y is a fixed value is never considered when computing $P(M = x | C = y)$. We can get that result by reductio ad absurdum. Suppose for fixed y, if $P(K = (x \oplus y)) = 2^{-n}$ (that is used in the proof, but indeed it is wrong. It is used just to get wrong conclusion), we can get $P(M = x | C = y) = 2^{-n}$ because there is a one-to-one correspondence between all the plaintexts and keys for the fixed ciphertext in OTP. But it is obviously wrong, for the prior probabilities of all plaintexts are seldom equally likely. So $P(M = x) \cdot P(K = (x \oplus y))$ stand for the joint probability of x and y when y is not fixed. But Shannon thought of the posterior probability as the probability of plaintext when ciphertext had been intercepted, we can see that there is a presupposition in $P(M = x | C = y)$ that y is fixed, but in $P(M = x)$, $P(K = (x \oplus y))$ and $P(C = y)$, y is not fixed, otherwise we can get obviously wrong results. In such way, the Bayes' formula was misused for the probability was not on the same presupposition and the equation does not come into existence.

In OTP there are complex and cryptic conditions that influence the probability of plaintext, key and ciphertext, so it is essential to cognize all the conditions and carefully use probability theory. The proof did not realize the cryptic condition that ciphertext was a fixed value (even though unknown) rather than a random variable.

4. Example Analyses on the Change of Probability

In order to make the mistakes recognized more distinctly, the following example is given to show that OTP is not perfectly secure.

The plaintext space is $M = \{0, 1\}$, according to the prior condition that is generally the correspondence context, it is known beforehand that the prior probability of plaintext being 0 is 0.9, while the prior probability of plaintext being 1 is 0.1. The ciphertext space is $C = \{0, 1\}$ and the key space is $K = \{0, 1\}$, with the keys being equally likely. The cryptosystem is OTP. Later the information is obtained that the ciphertext is 0. When only the later information is considered (regardless of the prior probability of plaintext), for the fixed ciphertext, there is a one-to-one correspondence between all the plaintexts and keys, so it can be concluded that the plaintexts are equally likely, that is, the probability of plaintext being 1 is 0.5.

As the probability obtained above isn't consistent with the prior probability, compromise is needed. The compromised posterior

probability of the plaintext would be between the two corresponding probabilities of the two conditions. The compromised posterior probability of the plaintext is not equal to the prior probability, so OTP is not perfectly secure.

According to the mapping of M, K and C, the probabilities of M, K and C are complicatedly interactional. In the above example, the probability of plaintext changes when the ciphertext is fixed, even though the ciphertext is unknown.

When only considering the fixed ciphertext and the equiprobability of the key, we can see that all the plaintexts are equally likely for there is a one-to-one correspondence between all the plaintexts and keys for the fixed ciphertext. There is conflict between the prior probability and the uniformly distributed probability gained above.

In order to make clear the inconsistency of probability in the example and the need for fusion of the probability in this case, we can adopt the combinations of different conditions for the following deduction to analyze the existence of probability conflict.

For the above simple example about OTP, when considering the condition that the ciphertext is 0, it can be easily concluded that the probability of ciphertext being 0 is 1, and the probability of ciphertext being 1 is 0. But according to the prior probability distribution of plaintexts given and uniformly distributed keys, we can easily find that the ciphertext is uniformly distributed, that is to say, all ciphertext are equally likely. We can see the two probability distributions of ciphertext in different conditions are conflictive.

When only considering that the intercepted ciphertext is 0 and the prior probability of plaintext is 0, we call $P(M=0)$ is 0.9, and $P(M=1)$ is 0.1, the probability of the key being 0 we call $P(K=0)$ is 0.9, and $P(K=1)$ is 0.1 because there is a one-to-one correspondence between the plaintext and the key. However, according to the requirement of OTP, the key is equiprobable, so conflict of the probabilities occurs as before.

Such conflicts show that on different conditions we may draw inconsistent probabilities, so it need fuse and compromise. The probabilities obtained from different combinations of unilateral conditions are inconsistent. Just like four irregular feet of a table, there is always one foot that is turnout when the table is on the horizontal ground. In literature [7], a formula was presented to fuse the inconsistent probabilities.

5. Conclusion

The paper further confirms that there is a mistake in the proof about perfect secrecy of OTP. From the above analyses, we can find that OTP is not perfectly secure. In despite of that, it has good cryptographic property. We can take measures to improve its security. The mistakes may result from the limitations of information theory and probability theory, which ignore the random uncertainty of probability and always take probability as a fixed value, but not random variable [8, 9].

Reference

[1]. Bruce Schneier, Applied Cryptography Second Edition: protocols, algorithms, and source code in C[M], John Wiley & Sons, Inc, 1996.

- [2]. C. E. Shannon, Communication Theory of Secrecy Systems[J], Bell System Technical journal, v.28, n. 4, 1949, 656–715.
- [3]. Yong WANG, Security of One-time System and New Secure System [J], Netinfo Security, 2004, (7):41–43
- [4]. Yong WANG, Fanglai ZHU, Reconsideration of Perfect Secrecy, Computer Engineering, 2007, 33A9
- [5]. Yong WANG, Perfect Secrecy and Its Implement [J], Network & Computer Security, 2005(05)
- [6]. Yong WANG, Fanglai ZHU, Security Analysis of One-time System and Its Betterment, Journal of Sichuan University (Engineering Science Edition), 2007, supp. 39(5):222–225
- [7]. Yong WANG, Shengyuan Zhou, On Probability Attack, Information Security and Communications Privacy, 2007, (8) 9–40
- [8]. Yong WANG, On the Perversion of information s Definition, presented at First National Conference on Social Information Science in 2007, Wuhan, China, 2007.
- [9]. Yong WANG, On Relativity of Probability, www.paper.edu.cn, Aug, 27, 2007.