

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01864.html>

- *From:* wangyong <hellowy@xxxxxxx>
 - *Date:* Thu, 08 Nov 2007 19:08:54 -0800
-

We know Shannon first proved that OTP was perfectly secure, but his proof is very simple. Shannon just took an example, and got the result that the prior probability of plaintext is uniform. Popular detailed proofs about perfect secrecy of OTP were given by later scholars who used Shannon's proof for reference. The representative proof is as follows:

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

$$P(M = x \mid C = y) =$$

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

$$= P(M = x) \cdot P(K = (x \oplus y) \mid M = x)$$
 (K is independent of M)

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

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

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

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

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

We find $P(M = x \mid C = y)$ is gotten from the case when ciphertext is not fixed in the above proof, in that case K is independent of M and K is chosen uniformly. But when considering the case of intercepted ciphertext, the ciphertext is fixed (even though it is unknown). We can find K is not chosen uniformly and K is not independent of M , for there is a one-to-one correspondence between all the plaintexts and keys for the fixed ciphertext in OTP and the probabilities of the corresponding plaintexts and keys are the same. But when considering the posterior probability, the case should be under the condition ciphertext is fixed, so the probability $P(M = x \mid C = y)$ which is under the condition ciphertext is a random variable (but not fixed), in the above proof is not the posterior probability of plaintext. Now we will show the probability $P(M = x \mid C = y)$ which is under the condition ciphertext is a random variable is not the same as the probability $P(M = x \mid C = y)$ which is under the condition ciphertext is fixed.

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 cryptalgorithm 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[9].

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. If we make the four feet all touch the horizontal ground at the same time, there must be distortion and we should not use the shape before distortion no longer. But in the above proof, the probabilities under different conditions are confused.

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

From the angle of cryptanalyse, a cryptanalyst will use the

intercepted ciphertext and the information that each K is equally likely to find all the plaintext are equally likely, then consider the prior probability of plaintext, and make a compromise between the two probability distributions. The compromised probability distribution is usually not the same as the prior probability distribution.

.