

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg05635.html>

---

- *From:* wangyong <[hellowy@xxxxxxx](mailto:hellowy@xxxxxxx)>
  - *Date:* 30 Oct 2007 00:07:14 -0700
- 

Due to the mapping of M, K and C, the probabilities of M, K and C are complicatedly interactional. For 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 key, we can gain that plaintexts are equally likely for there is a one-

to-one correspondence between all the plaintexts and keys for fixed ciphertext. There is conflict between the prior probability and the uniformly distributed probability gained above.

In order to understand the inconsistency of probability in the example

and the need for fusion of the probabilities in this case, we adopt the combinations of different conditions for the following deduction to analyze the existence of probability conflict.

For our simple example about OTP, when considering the condition that ciphertext is 0, 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 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 prior probability of plaintext being 0 we call  $P(M=0)$  is 0.9, and prior probability of plaintext being 1 we call  $P(M=1)$  is 0.1, the probability of key being 0 we call  $P(K=0)$  is 0.9, and the probability of key being 1 we call  $P(K=1)$  is 0.1 because there is a one-to-one correspondence between all the plaintexts and keys. However, according to the requirement of OTP, all the keys are equally likely, so conflict of the probabilities occurs as before.

Such conflicts show that under different conditions we may draw inconsistent probabilities, so it needs to fuse and compromise. The probabilities obtained by the different combinations of unilateral conditions are inconsistent. That is to say, the conditions in OPT can

not coexist. When all the conditions are considered, some of the conditions must change, so it is not proper to use these conditions when computing the final posterior probability. It likes four irregular feet of a same table. There is always one foot that is turnup when the table is on the horizontal ground. If the four feet should touch the horizontal ground at the same time, distortion would happen. In literature [7], formula was presented to fuse the inconsistent probabilities.

Shannon did not realize that the conditions were impossible to coexist. When taking them into the formula, there must be mistake for the conditions cannot coexist and the probabilities have changed when all the conditions are considered at the same time.

For the conditions in the example are very complex, and some are connotative, it is essential to list them and analyze the impact of the conditions on the probability. Literature [4] considered an especially understanding following which OTP could be thought perfectly secure if some added conditions were satisfied and analyzed that was unlikely to be Shannon's view. This paper analyzes the problem in detail and confirms the result that the especially understanding is not Shannon's view using the information gained from Shannon's proof.

As different conditions can gain different probability distribution, we list the conditions those impact on the probability distribution of plaintext and the corresponding probabilities of plaintext when only considering some of the conditions.

.