

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg04160.html>

---

- *From:* wangyong <[hellowy@xxxxxxx](mailto:hellowy@xxxxxxx)>
  - *Date:* Tue, 23 Oct 2007 07:09:43 -0700
- 

Shannon misused Bayes' formula, similarly the above proof misused Bayes' formula. From  $P(M = x) \hat{=} P(K = (x?y)) = P(M = x) \hat{=} 2^{-n}$ , 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  $P(K = (x?y)) = 2^{-n}$  (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  $P(M = x) \hat{=} P(K = (x?y))$  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  $P(M = x)$ ,  $P(K = (x?y))$  and  $P(C=y)$ ,  $y$  is not fixed, otherwise we can get obviously wrong results. In such way, the Bayes's 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.