

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg04512.html>

---

- *From:* wangyong <hellowy@xxxxxxx>
  - *Date:* Wed, 24 Oct 2007 21:01:14 -0700
- 

Huh???? So, now you \*agree\* that the probabilities of  $M=0$  and  $M=1$  are unaffected by observing  $C=0$ ? Then you should have no difficulty in also agreeing that these probabilities are unaffected by observing  $C=1$ , and, therefore, that they are unaffected by observing  $C$ , whatever value we may find that  $C$  takes. So, intercepting the message gives us no additional information about  $M$ . What's the problem? —————you mistake lies in not obeying perfect secrecy. The probability changed in the whole process. I point out OPT has good attributes.

I get the impression that you are inventing complexities where none exist. EITHER  $C$  is unknown and random (and  $M$  has its prior, or initial, distribution), OR  $C$  is known and fixed (and  $M$  has its conditional distribution). In the scenario we are discussing, the conditional distribution of  $M$  (after  $C$  is observed) is exactly the same as the prior distribution of  $M$  (before  $C$  is observed), whatever value of  $C$  actually is observed. And that's all there is to it.

—————your prior is not EITHER  $C$  is unknown and random (and  $M$  has its prior)

but shannon's is. you do not see this paper clearly. you perpetrate a fraud by substitute. we discuss perfect secrecy.