

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01448.html>

---

- *From:* wangyong <hellowy@xxxxxxx>
  - *Date:* Wed, 07 Nov 2007 00:33:03 -0800
- 

On 11 7 , 4 23 , William Hughes <wpihug...@xxxxxxxxxxxx> wrote:

On Nov 7, 12:09 am, wangyong <hell...@xxxxxxx> wrote:

-----a change in form but not in content,you just use the probability when c is not fixed.  
you use the the joint probability of M,K and C when c is not fixed.

I use the joint probability distribution of M,K and C.

a change in form but not in content

but the the joint probability of M,K and C is not the same when c is fixed as when c is not fixed.

There is no such thing as the joint probability distribution of M,K and C when c is fixed.

– William Hughes

how you get the probability???

when c fixed, if we suppose k uniform, then m uniform  
if we suppose m as its prior, then k is corronspand as prior.  
Indeed we dont know the probability of M and k when c fixed, you just use the case c is not fixed.