

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01446.html>

- *From:* William Hughes <wpihughes@xxxxxxxxxxxx>
 - *Date:* Wed, 07 Nov 2007 00:23:10 -0800
-

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