

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01506.html>

- *From:* William Hughes <wpihughes@xxxxxxxxxxxx>
 - *Date:* Wed, 07 Nov 2007 04:20:01 -0800
-

On Nov 7, 4:24 am, wangyong <hell...@xxxxxxx> wrote:

On 11 7 , 4 51 , William Hughes <wpihug...@xxxxxxxxxxxx> wrote:

... as we know that M is not uniform we conclude that the assumption that K is uniform when C is fixed is incorrect.

====yes,

Good, you understand. Now stop claiming that K must be uniform when C is fixed. It might be, but it might not be.

but what can you conclude.

That if we do not know whether or not M is uniform, we do not know if whether or not K is uniform when C is fixed.

Thus

If we consider only the OTP without considering the prior probability on M , we do not know whether of not M is uniform. So if we consider only the OTP and a fixed C we do not know whether or not K is uniform.

– William Hughes

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