

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01453.html>

- *From:* William Hughes <wpihughes@xxxxxxxxxxxx>
 - *Date:* Wed, 07 Nov 2007 00:51:41 -0800
-

On Nov 7, 3:33 am, wangyong <hell...@xxxxxxx> wrote:

how you get the probability???

when c fixed,

we can compute the probability distribution of M from the known joint probability distribution of M, and C. (there is only one joint probability distribution, there is no such thing as the joint probability distribution of M and C when C is fixed) We find that the probability distribution of M is not uniform.

if we suppose k uniform, then m uniform

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

– William Hughes

.