

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01516.html>

- *From:* wangyong <hellowy@xxxxxxx>
 - *Date:* Wed, 07 Nov 2007 06:15:21 -0800
-

On 11/7, 8:53, William Hughes <wpihug...@xxxxxxxxxxxx> wrote:

On Nov 7, 7:38 am, wangyong <hell...@xxxxxxx> wrote:

i consider C fixed, k uniform, regardless P prior

This assumption is only correct if
P is uniform.

So any conclusion you draw from this
assumption will be correct only if
P is uniform.

If P is not uniform, the conclusion that
P is uniform is incorrect.

So there is no contradiction between
the incorrect conclusion that P
is uniform and the fact that P
is not uniform.

– William Hughes

i consider C fixed, k uniform, regardless P prior
This assumption is only correct if
P is uniform.
====it is This assumption to get the result that
P is uniform.

So any conclusion you draw from this
assumption will be correct only if
P is uniform.
==i just get P is uniform

If P is not uniform, the conclusion that

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

P is uniform is incorrect.

So there is no contradiction between
the incorrect conclusion that P
is uniform and the fact that P
is not uniform.

=====they are obvious contradiction.

I just get that under my precondition, I use the probability under
imperfect conditions to compromise.

.