

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01664.html>

- *From:* wangyong <hellowy@xxxxxxx>
 - *Date:* Wed, 07 Nov 2007 23:01:37 -0800
-

On 11 8 , 9 44 , William Hughes <wpihug...@xxxxxxxxxxxx> wrote:

On Nov 7, 8:31 pm, wangyong <hell...@xxxxxxx> wrote:

On 11 7 , 11 45 , William Hughes <wpihug...@xxxxxxxxxxxx> wrote:

On Nov 7, 10:15 am, wangyong <hell...@xxxxxxx> wrote:

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

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

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.

An assumption that "get[s] the result" that
P is uniform is only correct if P is uniform.
If P is not uniform the assumption is incorrect.

So any conclusion you draw
from this
assumption will be correct

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

only if
P is uniform.

==> just get P is uniform

And this is only correct 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.

=====>they are obvious contradiction.

No

An *incorrect* conclusion that P is uniform
does not contradict the fact the P is not uniform.

- William Hughes

--

--

<snip evasion>

My comment was that

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

Your reply was

they are obvious contradiction

Do you continue to maintain this position?

– William Hughes– –

– –

=====I just to show the two conclusion is imperfect and incorrect.I
do not say any of them are correct, just to say they are contradiction
and do not coexist, then the compromise. just like the four feet of
a table.

YOu just insist one is correct and one is incorrect.

you just insist key uniform incorrect, but P Prior correct. but the
latter is also incorrect.

.