

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01417.html>

- *From:* wangyong <hellowy@xxxxxxx>
 - *Date:* Tue, 06 Nov 2007 20:46:47 -0800
-

On 11 7 , 12 13 , William Hughes <wpihug...@xxxxxxxxxxxx> wrote:

On Nov 6, 11:08 pm, wangyong <hell...@xxxxxxx> wrote:

how you can compute, how can you find the probability M not changed.
do not just the the result ,that is useless.

Compute the joint probability of M, K and C
(use the known probability distributions of M and K
the fact that M and K are independent, and the formula
for getting C from M and K)

Assume C fixed. Two cases.

For each case note the value of C and compute
the conditional probability of M using the known
joint probability of M, K and C and the definition
of conditional probability.

In both cases you get the same probability
distribution for M

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

– William Hughes >

--

a change in form but not in content, you just use the probability when
c is not fixed.

No. I do not use the probability when
c is not fixed. I compute the conditional probability. This
can be computed from the joint probability, but
is not the same as the unconditional probability
(the probability when c is not fixed).

– William Hughes--

--

how can you compute the probability when c is fixed,
do not use that when c is not fixed,
if use, tell why you can use.
that is why you take mistake.

.