

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg01420.html>

- *From:* William Hughes <wpihughes@xxxxxxxxxxxx>
 - *Date:* Tue, 06 Nov 2007 21:00:54 -0800
-

On Nov 6, 11:46 pm, wangyong <hell...@xxxxxxx> wrote:

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

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

In both cases you get the same probability
distribution for M

– 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.

I do not use the probability when c is not
fixed to compute the probability
when c is fixed. I use the joint probability of
M, K and C. [Indeed you could use the joint
probability to calculate
the probability of C when C is not fixed
(the marginal) but I do not do this.]
I use the joint probability to
calculate the probability of M or K when
C is fixed (the probability when C is fixed

Re: Confirmation of Shannon's Mistake about Perfect Secrecy of One-time-pad
is defined in terms of the joint probability)

– William Hughes

.