

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg04430.html>

- *From:* matt271829-news@xxxxxxxxxxxx
 - *Date:* Wed, 24 Oct 2007 13:05:20 -0700
-

On Oct 24, 5:16 pm, wangyong <hell...@xxxxxxx> wrote:

On 10B4å, H4ö26 , matt271829-n...@xxxxxxxxxxxx wrote:

On Oct 23, 3:09 pm, wangyong <hell...@xxxxxxx> wrote:

Shannon misused Bayes' formula, similarly the above proof misused Bayes' formula. From $P(M = x) \cdot P(K = (x \cdot y)) = P(M = x) \cdot 2^{-n}$, we can see the condition that the ciphertext y is a fixed value is never considered when computing $P(M = x | C = y)$. We can get that result by reductio ad absurdum. Suppose for fixed y , if $P(K = (x \cdot y)) = 2^{-n}$ (that is used in the proof, but indeed it is wrong. It is used just to get wrong conclusion), we can get $P(M = x | C = y) = 2^{-n}$ because there is a one-to-one correspondence between all the plaintexts and keys for the fixed ciphertext in OTP. But it is obviously wrong, for the prior probabilities of all plaintexts are seldom equally likely. So $P(M = x) \cdot P(K = (x \cdot y))$ stand for the joint probability of x and y when y is not fixed. But Shannon thought of the posterior probability as the probability of plaintext when ciphertext had been

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

intercepted, we can see that there is a presupposition in $P(M = x|C = y)$ that y is fixed, but in $P(M = x)$, $P(K = (x \cdot y))$ and $P(C=y)$, y is not fixed, otherwise we can get obviously wrong results. In such way, the Bayes's formula was misused for the probability was not on the same presupposition and the equation does not come into existence. In OTP there are complex and cryptic conditions that influence the probability of plaintext, key and ciphertext, so it is essential to cognize all the conditions and carefully use probability theory. The proof did not realize the cryptic condition that ciphertext was a fixed value (even though unknown) rather than a random variable.

I suspect that a combination of typos and/or character set incompatibilities have garbaged some of your equations. So, let me have a guess at what you're saying.

Let's keep with the simple scenario where $P(M=0) = p$, $P(M=1) = 1-p$, $P(K=0) = 1/2$, $P(K=1) = 1/2$, K and M independent. $K=0$ maps $0 \rightarrow 0$, $1 \rightarrow 1$, and $K=1$ maps $0 \rightarrow 1$, $1 \rightarrow 0$. We intercept the encrypted message $C=0$.

I'm guessing that you are reasoning as follows: Given that $C=0$, there is no longer an equal chance of $K=0$ and $K=1$. Because the proof uses the fact that these probabilities are equal, the proof must be wrong.

In fact, the K -probabilities used in the calculation of the conditional probabilities must be the *a priori* probabilities=====, which are indeed equal, and the proof is sound.

-----you are wrong at this place.

I don't think so.

if you are right

=====
=====The probabilities are all the ones in the case c is a random variable, but not $C=0$.

You've obviously spent a while working with this symbolically, so you might like to try a different approach to satisfy yourself. From your affiliation I assume you are familiar with computer programming, so try running a Monte Carlo-style simulation such as the following. You will find that always $M_{\text{equals}_0} / \text{total} \sim p$, and $M_{\text{equals}_1} / \text{total} \sim 1 - p$. This demonstrates that that probabilities of $M=0$ and $M=1$ are, as expected, unaffected by the fact that $C=0$.

=====
as I have pointed out above.

Huh???? So, now you *agree* that the probabilities of $M=0$ and $M=1$ are unaffected by observing $C=0$? Then you should have no difficulty in also agreeing that these probabilities are unaffected by observing $C=1$, and, therefore, that they are unaffected by observing C , whatever value we may find that C takes. So, intercepting the message gives us no additional information about M . What's the problem?

I get the impression that you are inventing complexities where none exist. EITHER C is unknown and random (and M has its prior, or initial, distribution), OR C is known and fixed (and M has its conditional distribution). In the scenario we are discussing, the conditional distribution of M (after C is observed) is exactly the same as the prior distribution of M (before C is observed), whatever value of C actually is observed. And that's all there is to it.