

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg03295.html>

---

- *From:* wangyong <hellowy@xxxxxxx>
  - *Date:* Fri, 16 Nov 2007 18:03:03 -0800 (PST)
- 

On 11A1å, H7ö37 , matt271829-n...@xxxxxxxxxxxx wrote:

On Nov 11, 3:18 am, wangyong <hell...@xxxxxxx> wrote:

On 11 10 , 8 53 , matt271829-n...@xxxxxxxxxxxx wrote:

On Nov 10, 3:23 am, wangyong <hell...@xxxxxxx> wrote:

On 11 9 , 8 02 ,  
matt271829-n...@xxxxxxxxxxxx wrote:

Just for a moment, forget  
the OTP problem. Pretend  
that you've never  
even heard of the OTP.  
Please study the following  
question.

I have two coins, one red  
and one blue. Both are  
marked "0" on one  
side and "1" on the other,  
and both are fair (i.e. they  
both come up  
"0" with probability 1/2, and

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

"1" with probability 1/2). I  
toss both  
coins. The red coin comes  
up with the number R. The  
blue coin comes up  
with the number B. I  
calculate  $C = R \text{ Xor } B$ , and I  
find that  $C = 0$ .  
Given that  $C = 0$ , what is the  
probability that  $R = 0$ ?

Do you think that this  
question has a well-defined  
single numerical  
answer?

(Please try to give a direct  
reply to the actual question  
that I have  
asked. If possible, please  
begin your reply with the  
word "yes" or the  
word "no".) --

--

yes

Great. I think that's the first of your replies that I've  
completely  
understood!

Now let me change the problem slightly. Instead of the red  
coin being  
fair, it will be biased. I'll state the new problem in full:

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

I have two coins, one red and one blue. Both are marked "0" on one side and "1" on the other. The red coin is biased and comes up "0" with probability  $p$  and "1" with probability  $1-p$ . The blue coin is fair: it comes up "0" with probability  $1/2$ , and "1" with probability  $1/2$ . I toss both coins. The red coin comes up with the number  $R$ . The blue coin comes up with the number  $B$ . I calculate  $C = R \text{ Xor } B$ , and I find that  $C = 0$ . Given that  $C = 0$ , what is the probability that  $R = 0$ ?

Do you think that this new problem has a well-defined single answer (in terms of  $p$ )?

If so, what do you think the answer is?--

--

you just no see the contrastion. take the question easy.  
If  $c$  fixed,  $k$  and  $P$  are dependant,  
but you just use the probablity  $c$  not fixed, that is a mixture, and  
changed the probablity characteristic,including the value.  
can you prove probabilities when  $c$  not fixed, the same as  
probabilities when  $c$  not fixed.

I have no idea what you are talking about.

I asked you two simple questions:

1. Do you think that this new problem has a well-defined single answer (in terms of  $p$ )?
2. If so, what do you think the answer is?

Please just answer the questions. Please answer "yes" or "no" to question 1. If you answered "yes" to question 1 then please also

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

answer question 2. -  $I \ll (W -$

-  $>: (, W -$

-----this new problem

what problem??? you just not tell? how can i answer.

.