

Re: How much is Alice worth to Bob?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-03/2141.html>

From: David Wagner (*daw_at_taverner.cs.berkeley.edu*)

Date: 03/28/04

Date: Sun, 28 Mar 2004 04:15:28 +0000 (UTC)

Nicol So wrote:

>> *Hence, you've shown that Alice can transmit*

>> *X just about as efficiently without knowing S as if she did know S.*

>

>*That's an interesting observation. I think I'd point out that the two*
>*cases differ not only in Alice's knowledge of S, but also in the error*
>*probability.*

Yes, that's true. However, the error probability in your protocol can be made exponentially small with only a linear increase in communication complexity. For all intents and purposes, an exponentially small error probability might as well be zero. (If the probability of error due to your protocol is much smaller than the probability of a cosmic ray causing a bit error in your computation, you might as well ignore the possibility of an error due to your protocol.) So I think the difference in error probability, while it does exist, is not hugely significant.