

Re: Jointly calculating the sum

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-07/1623.html>

From: Peter Pearson (ppearson_at_nowhere.invalid)

Date: 07/28/05

Date: Thu, 28 Jul 2005 09:52:18 -0700

Ann Brandon wrote:

> assume we have 3 partys Alice, Bob and Carol. Each party chooses a
> random value r_A, r_B, r_C in Z_p (where p is prime). Now the partys
> want to calculate the sum $r=r_A + r_B + r_C$, so that each party only
> knows its own value and the sum r .

If you don't require detection of cheating, you can do the
sum-of-ages-at-the-lunch-table trick: Alice picks a random X
and passes $X+A$ to Bob, who adds his number and passes $X+A+B$
to Carol, who passes $X+A+B+C$ to Alice, who subtracts X and
announces $A+B+C$.

--

Peter Pearson

To get my email address, substitute:

nowhere -> spamcop, invalid -> net