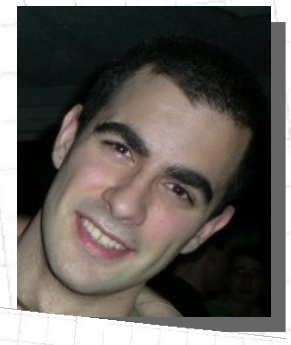
Cryptographic Protocols for Secure Computation

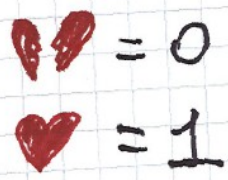


Claudio Orlandi

Alice and Bob want to find out whether they are interested in each other

But they are shy, so neither of them wants to make the first move (they are afraid of rejection)

So they would like to compute the "AND" of their interest level



The computation should be:

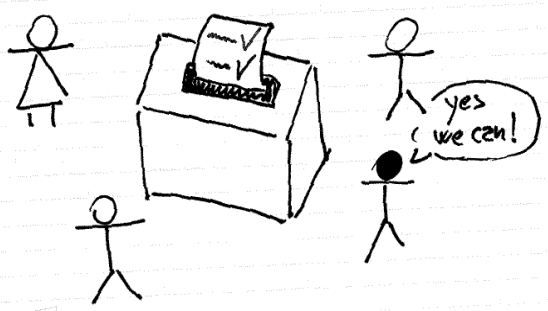
Correct: the output is really $a \wedge b$

Private: the computation doesn't leak a, b but just $a \wedge b$

Using Cryptography we can help Alice and Bob !!

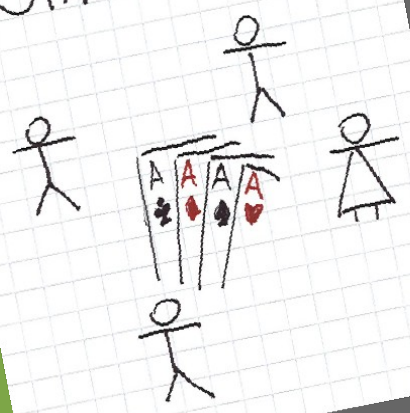
In many real applications the problem of **secure multy party computation** is solved using a **trusted server**

Electronic Voting



Online Auctions

Online Poker



We can replace the trusted server with a **Cryptographic Protocol!**