Privacy Engineering (70018)

MPC 1 - Questions

For the BGW protocol the coursework provides an excellent opportunity to study the protocol.

1.1 Give at least 3 situations where the protocol for average salary(example 1) fails?

1.2 For the Millionaires' problem if Alice's wealth is £3M, Bob's is £6M and the range of their wealth is £1M to £10M, what will Alice and Bob learn about the range of the other's wealth on completion of the protocol.

1.3 For the Millionaires' problem if Alice's wealth is £6M, Bob's is £3M and the range of their wealth is £1M to £10M, what will Alice and Bob learn about the range of the other's wealth on completion of the protocol.

1.4 For the Millionaires' problem in the slides with Alice = £2M, Bob=£1M show that

(i) $Z_1 = r \bmod p$ (ii) $Z_2 \neq r \bmod p$

1.5 How can the Millionaires' problem be adapted for equality?

1.6 In Yao's solution why is there is a requirement that the values in the list Z differ from each other by at least 2?

1.7 Why is the list Z used for partitioning the sent list? What if Y was sent instead, e.g. Alice sent Y[1], Y[2], Y[3], Y[4], Y[5]+1, Y[6]+1. Assume RSA public/private keys are used.

1.8 How could you use a secure multiplication protocol to determine if Alice and Bob where interested in dating each other? What if Alice lied and said she was interested when she wasn't? This can be answered without knowing the details of the protocol.

1.9 Optional. Challenging.

(i) Alice has a number A, Bob a number B. Devise a protocol to securely multiply the two numbers (mod prime p) Use Carol to help with the computation - she has no number (provides no input).
Hint: split A into shares a1, a2, a3, and B into shares b1, b2, b3. Distribute them like in secure voting, then devise sub-expressions for Alice, Bob and Carol and combine them to get the final answer.

(ii) Why is secure addition used could we not just add the sub-expressions computed by Alice, Bob, Carol. **Hint**: consider the case when Alice knows sB.

(iii) Is secure multiplication still secure if Carol colludes with Alice or Bob?