Privacy Engineering (408)

Secure Multiparty Computation

Exercises

1. 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 do Alice and Bob know about the range of the other's wealth.

2. 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 do Alice and Bob know about the range of the other's wealth.

3. How can the Millionaires' problem be adapted for equality?

4. For the Millionaires' problem in the slides with Alice = £4M, Bob=£3M show that (i) Z_3= R mod p, (ii) $Z_4 \neq$R mod p.

---

5. Consider the following 1-from-*n* oblivious transfer protocol in an honest-but-curious (semi-honest) model.

   1. Alice generates *n* random public-private key pairs

      $(pub_1, priv_1), \ldots (pub_n, priv_n)$

      Alice sends the public keys $pub_1, ..., pub_n$ to Bob.

   2. Bob generates *n* random symmetric keys $k_1, ..., k_n$ and computes

      $G_b = E_{pub_b}(k_b)$ and $G_z = k_z$ for all $z \in \{1..n\}$ and $z \neq b$

      Bob sends G_1 to G_n to Alice

   3. Alice computes

      $H_z = D_{priv_z}(G_z)$,

      $C_z = E_{H_z}(M_z)$ for all $z \in \{1..n\}$

      Alice sends C_1 to C_n to Bob

   4. Bob computes $M_b = D_{k_b}(C_b)$

   For this protocol:

   i) Show that Bob's output equals M_b.

ii) Explain why Alice learns nothing about b. What assumptions do you have to make about the two cryptosystems for this to be true?

iii) Explain why Bob learns nothing about M_z for $z \neq b$. What assumptions do you have to make about the two cryptosystems for this to be true?

iv) If Alice were dishonest, is there anything she could do to learn b? If so, describe how. If not, explain why not.

v) If Bob were dishonest, is there anything he could do to learn messages other than M_b? If so describe how. If not, explain why not.

6. Consider the following *1*-from-*2* oblivious transfer protocol based on the well-known Diffie-Hellman key-exchange protocol in an honest-but-curious setting.

1. Alice generates a random number a (from $\mathbb{Z}p$). Similarly, Bob generates a random number b. Bob's message selection bit is m.

2. Alice sends $A=g^a$ to Bob. g is a suitable generator for the group.

3. If $m=0$ Bob sends $B=g^b$ to Alice.
   If $m=1$ Bob sends $B=$ Ag^b to Alice.

4. Alice computes $k_0=Hash(B^a)$, $k_1=Hash((B/A)^a)$,
   $C_0 = E_{k0}(M_0)$, $C_1 = E_{k1}(M_1)$
   Alice sends C_0 and C_1 to Bob.

5. Bob computes $k = Hash(A^b)$, $M_m = D_m(C_m)$,

For this protocol:

i) Explain why Bob's output equals M_m.

ii) Explain why Alice learns nothing about m and why Bob learns nothing about M_z for $z \neq m$. What assumptions do you have to make about the two cryptosystems for this to be true?

iii) Explain what, if any, issues arise if Alice sets a to 0. What if Bob sets b to 0 (with Alice generating a random number a as normal)?

---

7. Three privacy rights campaigners are having dinner around a table at a restaurant in South Kensington. The restaurant owner tells them that their dinner has been paid for, anonymously, either by one of them, or by Bookface. The three campaigners respect each other's right to make an anonymous payment but they would like to know if Bookface is paying. They decide to find out whether it is Bookface who has paid, or one of them, without exposing which one of them it is. They devise the following protocol:

    1. Each campaigner flips a coin and shows it to their left neighbour, i.e. each campaigner will see the outcome of two coin flips: their own and that of the right neighbour.

    2. Each campaigner then announces whether the outcomes of the two coin flips that they have seen are the "*Same*" or "*Different*". If the campaigner is the payer, the campaigner says the opposite (i.e. lies).

    For this protocol show that:

    i) An odd number of "*Same*" announcements means that Bookface is paying, while an even number means that one of them is paying.

    ii) A non-paying campaigner cannot tell which of the other two is the payer, if Bookface is not paying.

8. Devise an alternative protocol to Q7 based on the message passing scheme used for average salary.

---

9. Alice has a number A, Bob a number B. Devise a protocol to securely multiply the two numbers. 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.

10. How could you use the 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?

11. Is secure multiplication still secure if Carol colludes with Alice or Bob?

12. Optional. In secure multiplication 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.