Mid Semester - Fall, 2025
M. Tech. Cryptology & Security - 2^{nd} Year
Advanced Cryptology

September 12, 2024

Maximum Marks: 25
Maximum Time: 2 hr
Open note/book exam

Instructions

- Maximum marks is 25. Total marks provided in the paper: 30.
- Be short and precise. For example, a 5 (respectively 3) mark question's answer should not be ideally more than a page (respectively half a page) with standard hand-writing. Partial marking will be provided for a partially correct answer/attempt.
- All parts of the same questions must be done at the same place, and in order. Marks will be deducted for violating this – this will be followed strictly.
- Verbosity (e.g. unnecessary/irrelevant sentences) is highly discouraged, and may lead to deduction of marks.
- You can use any book/notes during the exam, but *not internet*.
- The seating arrangements and other regulations circulated from Dean's office must be followed adequately.

Questions

1. Alice and Bob are going for a private auction, where they want to bid in any order, but their goal is to get the item at the minimum price. The auctioneer plans to use a CPA secure encryption to hide their bids. Auctioneer has the decryption key.

   (a) Then what would be the best strategy for Alice/Bob such that they can get the item at the minimum price?

   (b) How the auctioneer can change/strengthen the scheme so that this strategy does not work any more? Explain briefly.

   (3+3 = 6)

2. Consider a simple private voting scheme with the following steps

   - There are 3 options to vote. Each voter's vote is a binary vector of dimension 3, where 1 denotes a "yes" vote, and 0 means a "no" vote. For example, a vote for the first and third option shall be denoted by a vector $(1, 0, 1)$.
   - The voting authority releases a public key for Exp-El-Gamal Encryption, for which only the authority holds the secret decryption key.

- Each party sends their votes (the vector) to the authority.

Now answer the following questions:

(a) Consider a setting, where all voters are honest, and the authority is semi-honest. So, the honest voters do not want their individual votes to get leaked to the authority. However, the authority will not diverge from the protocol steps it is supposed to execute (as it is semi-honest). Describe a protocol.

(b) Now, in addition to semi-honest authority, consider malicious voters. Assume that a voter can vote "yes" to multiple options. In that case, how the authority can verify that each encrypted votes are legitimate? (e.g. $(1, 0, 1)$ is a legitimate voting vector, whereas $(2, 3, 8)$ is not.)

(c) Finally consider that in addition to above, each voter can vote "yes" to only one option (e.g. $(0, 0, 1)$ is a legitimate voting vector, whereas $(1, 0, 1)$ is not.). Then how would the authority verify the legitimacy of each encrypted vote?

$(5+5+5 = 15)$

3. Let π be a generic two party computation (2PC) protocol which computes any boolean function $\{0,1\} \times \{0,1\} \rightarrow \{0,1\}$ between any two parties P_1 and P_2 when P_1 holds the first input x_1 and P_2 holds the second input x_2 and at the end of the protocol both of them get the output y. Now consider a *specific* function $y = f(x_1, x_2)$ which is computed by P_1 and P_2 using π. At the end of the protocol party P_1 is able to compute x_2 and party P_2 is able to compute x_1. Then answer each of the following questions with arguments.

(a) Is it possible to conclude whether π is secure or insecure? Argue with a concrete example.

(b) Now consider that the same protocol is used to compute the AND function $g(x_1, x_2) = x_1 \wedge x_2$. If P_1's input is 1 then it is able to recover P_2's input x_2. Does the conclusion about the security of π change or not?

(c) Now consider the same protocol is used to compute the OR function $h(x_1, x_2) = x_1 \vee x_2$. If P_1's input is 1 then in the end it recovers P_2's input x_2. How does this fact change your conclusion about π, if at all?

$(3+3+3 = 9)$