Model-Exam Questions

Privacy Enhancing Technologies (201500042)

(Total number of achievable points: 0)

Introductory remarks.

- This is not an exam! Rather, it is a collection of questions as they could appear in an exam.
- The questions in this paper are meant as preparation for the exam. Some questions are potentially more difficult (and more time consuming) than what you can expect in the exam.
- You might want to use a simple calculator. It is advisable to not make use of scientific and graphic calculators, laptops, cell phones, books and other materials when answering the questions.
- It is important to understand *how* you get to your answers. Please try to take this into account by motivating and explaining your answers.

1. **Anonymous Communication** *(0 points)*

   (a) *(0 points)* Consider the following example (Figure 1) of a Chaum mix network in which you are the only participant (and no messages have been sent yet): Mixes A, B, and C are threshold mixes with different thresholds n_A, n_B, and

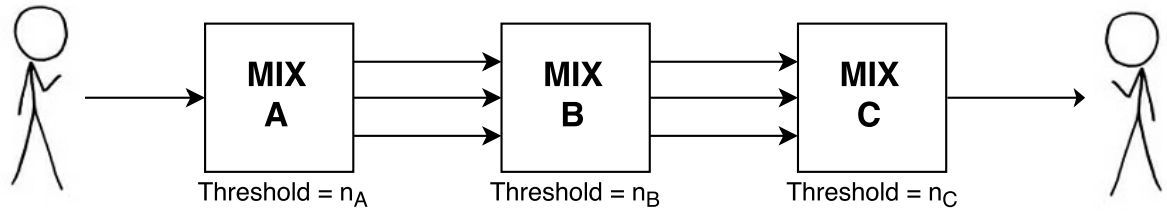

Figure 1: Visualization of a mix network.

   n_C, respectively. Since you are the only participant, you can see all inputs to mix A and all outputs of mix C. Suppose that you see the input-output behavior of the overall mixnet when sending messages as shown in Table 1.

   Determine the threshold of each mix in the mix network (and describe how you determine it with arguments on why it works)!

   (b) *(0 points)* Recall that Onion Routing is not secure against a global passive attacker. Describe a concrete *passive* attack that completely breaks both sender- and receiver-anonymity in Onion Routing! Explain why your attack is successful.

   Would your attack also work if the *passive* attacker can only compromise parts of the Onion Routing network (i.e., it becomes a partial passive attacker)?

   (c) *(0 points)* In TOR, Onion Proxies establish routes/circuits consisting of 3 Onion Routers whereas 3 is the default route length. Provide arguments on why this default is not set to 2 or to 4?

Input to mix A	Output of mix C (# of msgs)	Input to mix A	Output of mix C
1st msg	0	13th msg	0
2nd msg	0	14th msg	0
3rd msg	0	15th msg	0
4th msg	0	16th msg	0
5th msg	0	17th msg	0
6th msg	4	18th msg	4
7th msg	0	19th msg	0
8th msg	0	20th msg	0
9th msg	4	21st msg	4
10th msg	0	22nd msg	0
11th msg	0	23rd msg	0
12th msg	4	24th msg	4

Table 1: Input-output behavior of the given mix network.

2. **Privacy in Identity Management** *(0 points)*

In this question, we let G be a cyclic group of prime order q, generated by g, such that the Decisional Diffie-Hellman (DDH) problem is hard in G (this implies that also the DLP is hard in G). Furthermore, let $h \in G$ such that $\text{dlog}_g(h)$ is unknown.

(a) *(0 points)* Provide the formal definition of the binding and of the hiding property in commitment schemes.

(b) *(0 points)* Consider the commitment scheme

$$C(x, r) := (g^r, h^r \cdot x)$$

and show that it is computationally hiding and information-theoretically binding.

Hint: Notice the similarity to the ElGamal encryption scheme with the only difference that $\text{dlog}_g(h)$ is unknown in the above commitment scheme.

(c) *(0 points)* 1. Complete the following Σ-protocol that wants to prove the following statement in zero-knowledge:

$$PK\{(x, a) : y = h^x g^a\}.$$

Commitment. $r = h^{k_1} \cdot$ _____ for random $k_1, k_2 \in \mathbb{Z}_q$

Challenge. _____

Response. $(s_1, s_2) =$ (_____, $k_2 + ae \bmod q$)

Verification. Outputs **TRUE** $\iff$ $h^{s_1} \cdot$ _____ = _____ $\cdot r$

2. Show that the above Σ-protocol has the *completeness* property!
3. Devise a non-interactive version of the above Σ-protocol by following the Fiat-Shamir heuristic!

(d) *(0 points)* Have another look at the Credential Verification protocol of the Chase-Meiklejohn-Zaverucha anonymous credential system on slide 27 of lecture unit 4 "Privacy in Identity Management - Part 2". Note that in an actual exam, the relevant excerpt from the slide would be provided.

1. Would there be a privacy problem, if the prover would not randomize the aMAC in the first line of the verification protocol? If so, what exactly would break?
2. What is the purpose of the Pedersen commitments on the actual messages/attribute values m_i in the second line of the verification protocol? Why is a simple Schnorr identification not enough?
3. Why is the third line of the verification protocol required? What is it used for?

3. **Anonymization Techniques** *(0 points)*

For the date given in Table 2, the combination of job, sex and age attributes is considered to be a quasi identifier. For the following question, consider the table and provide clear answers.

(a) *(0 points)* Give a definition for K-Anonymity. And determine the value of K for the quasi identifier.

(b) *(0 points)* A person, Bob, knows that his neighbor Alice is around 30 years old and she is working in an art gallery. Bob also saw her in the morning and she was looking healthy. Based on this information what are the probabilities for Alice being i) Hepatitis, ii) HIV and iii) Flu?

(c) *(0 points)* Alter the database in such a way that the side information in question (b) will be not sufficient to identify Alices health condition and justify your answer. [Hint: There can be multiple ways of achieving this goal.]

(d) *(0 points)* Consider the disease attribute. If the person with flu is removed, it is clear that all females in this table have HIV. Propose a method of obfuscation such that any person in the table has at least two diseases. And discuss briefly how your solution affects the utility.

Table 2: Anonymized dataset

Job	Sex	Age	Disease
Professional	male	[35-40)	Hepatitis
Professional	male	[35-40)	Hepatitis
Professional	male	[35-40)	HIV
Artist	female	[35-40)	Flu
Artist	female	[35-40)	HIV
Artist	female	[35-40)	HIV
Artist	female	[35-40)	HIV

4. **Secure Computation** *(0 points)*

(a) *(0 points)* Alice and Bob want to compute $c = a + b$, where a and b are private input bits of Alice and Bob, respectively.

1.) Assume that Alice creates the garbled circuit for the OR gate. Give in tabular format the encryptions she computes.
2. Upon receiving the garbled circuit from Alice, explain what Bob should do to obtain the correct key for his input. What are the principles of that mechanism, explain briefly.

3. Imagine that Alice has pk_B, that is Bob's Paillier public key and $E_{pk_B}(a)$ and Bob has sk_B and b.
   (a) Design a secure addition protocol such that Alice obtains $E_{pk_B}(a+b)$. Alice should not see b and Bob should not obtain a.
   (b) Give the complexity of your protocol in terms of operations, i.e. number of encryptions, exponentiations, and any other operation you need for your protocol.
   (c) Compare the overall complexity of the protocol that uses garbled circuit to your protocol.