# Exam—June 28, 2018

## Privacy Enhancing Technologies (201500042)

- The exam consists of 4 pages and 4 questions, *each question counting for 25% of the exam's overall grade.*
- Write your answers for each question on a **separate** sheet of paper and do not forget to put your name and student number on every sheet!
- The teachers need to understand how you got to your answers. Make sure that you take this into account by motivating and explaining your answers. Thus, just stating the final result of your answer without motivation/explanation qualifies for 0 (zero) points.
- During the exam, you may use a simple calculator. Scientific and graphic calculators, laptops, cell phones, books and other materials are not permitted.

### 1. Anonymous Communication

(a) Consider the following four scenarios.

A. Alice casts her vote for the national election at a polling station. She doesn't want her neighbor, Eve, to eavesdrop what she voted for.

B. Bob casts his vote for the European parliament via regular mail from the US. He doesn't want the NSA nor the US mail to learn what he voted for.

C. Charlie and his class mates regularly visit a news website. He doesn't want the website owner to be able to track him or his class mates and show them personalized advertisements.

D. Dave invites his friends for a party via encrypted email using the Bcc field. He doesn't want that his friends know which other friends he invited.

i. *(2 points)* Recall the three privacy definitions of "*sender anonymity*," "*receiver anonymity*," and "*unlinkability*."
Indicate for each scenario whether sender anonymity, receiver anonymity, or unlinkability is required (*e.g.*, "Scenario X. Sender anonymity: required; receiver anonymity: required; unlinkability: not required"). Motivate your answer by explaining what the privacy definitions guarantee.

ii. *(2 points)* Recall the four properties of an attacker, "*capability*" (active vs. passive), "*visibility*" (global vs. partial), "*mobility*" (static vs. dynamic), and "*participation*" (internal vs. external).
For each scenario, define a suitable attacker model in terms of these four properties. Motivate why you consider this attacker model. Note that there are multiple correct answers here. It is therefore important that you motivate your defined attacker model (*e.g.*, regarding implicit assumptions you make).

(b) *(4 points)* Consider the example of a Chaum mix network in figure 1. Chaum's paper explains how participant $x$ can anonymously sent messages to participant $y$. Additionally, Chaum explains how $y$ can respond to $x$, while still keeping the identity of $x$ secret from $y$. How could one achieve this idea of an anonymous reply to the original sender? (If you forgot Chaum's proposal, you may come up with your own idea.)

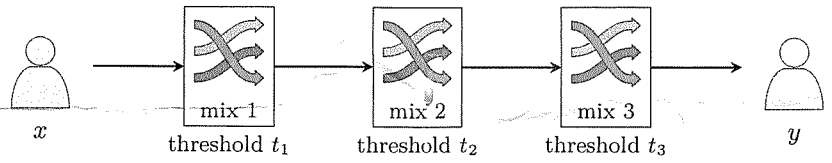


Figure 1: Visualization of a mix network.

(c) Consider the dining cryptographers network shown in figure 2. Suppose the network is used to determine whether someone has paid for dinner. At most one participant will indicate that he has paid, *i.e.*, at most one participant will announce the opposite of his observation.

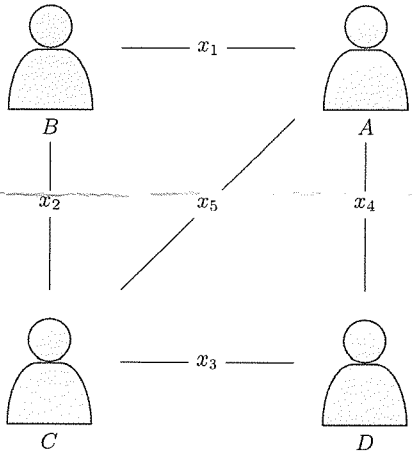


Figure 2: Visualization of a dining cryptographers network. Participant $A$ shares the coin flip outcome $x_1$ with participant $B$, $x_4$ with $D$ and $x_5$ with $C$. Note that participant $B$ and $D$ do not share a coin flip outcome.

i. *(3 points)* Consider the announcement $(1, 0, 1, 1)$, *i.e.*, participant $A$ announces 1, $B$ announces 0, $C$ announces 1, and $D$ announces 1. Did someone pay for dinner? If so, motivate your answer **and** give all possible coin tosses $x_1$, $x_2$, $x_3$, $x_4$, and $x_5$ for the case that $A$ is the payer and the case that $B$ is the payer (the cases that $C$ and $D$ are the payer are not needed). If not, explain why.

ii. *(1 point)* Assume the provided network of figure 2 is used by one of the participants to communicate a single byte. Consider the following announcement sequence for participants $A$, $B$, $C$, and $D$: (1,0,1,0), (0,1,1,1), (1,0,0,0), (0,0,0,1), (0,1,0,1), (1,1,0,0), (1,1,1,1), (0,1,1,0). What is the message that is being sent?

2. **Privacy in Identity Management**

(a) i. *(2 points)* Can a commitment scheme be both information-theoretically binding and information-theoretically hiding? If so, give an example of such a scheme (describe the algorithms Setup, Commit, and Decommit). If not, explain why or prove why it cannot exist.

ii. *(2 points)* Can a commitment scheme be both computationally binding and computationally hiding, but neither information-theoretically binding nor information-theoretically hiding? If so, give an example of such a scheme (describe the algorithms Setup, Commit, and Decommit). If not, explain why or prove why it cannot exist.
*Hint:* Consider a very simple scheme by using a cryptographic hash function.

(b) i. *(4 points)* Let $g$, $h$, $X$, and $Y$ be elements of a prime order cyclic group $\mathbb{G}$ of order $q$. Furthermore, let $x$ and $z$ be elements in $\mathbb{Z}_q$. Consider the statement

$$\mathrm{PK}\{(x,z)\colon X = g^x \wedge Y = g^x h^z\}$$

that we want to prove in zero-knowledge, where the values $X$ and $Y$ are known to both the prover and the verifier.
Complete the $\Sigma$-protocol given below (no explanation required).
**NOTE:** Do NOT fill out your answers into this exam sheet! Write your solution on an answer sheet (with your name etc.)!

**Commitments.** $r_X =$ _____, $r_Y = g^{k_1}h^{k_2}$ for _____ $\in_R \mathbb{Z}_q$
**Challenge.** _____ $\in_R \mathbb{Z}_q$
**Response.** $s_x =$ _____, $s_z = k_2 +$ _____ (mod $q$)
**Verification.** Output TRUE if and only if _____ and _____

ii. *(2 points)* Prove that the protocol is honest-verifier zero-knowledge.

3. **Multi-party Computation**

For this question, consider the additively homomorphic Paillier encryption scheme. Alice has the decryption key ($sk$), Bob and Charles have the encryption key ($pk$). Bob and Charles have two integer numbers of size $\ell$-bits: $b$, and $c$, respectively. They would like to compute the encrypted product of these numbers: $[bc]$. We are assuming all parties act according to the semi-honest security model.

(a) *(4 points)* Write a protocol where Bob and Charles obtains the product $[bc]$. Provide your assumptions for the protocol design.

(b) *(2 points)* Provide the complexity analysis per person in terms of operations on ciphertext, i.e. encryption, decryption, exponentiation, multiplication, and number of ciphertext transmitted.

(c) *(2 points)* Argue what information is leaked to Alice, Bob and Charles.

(d) *(2 points)* For the same protocol, **explain** whether DGK encryption scheme could be used or not.

(e) *(2 points)* For the Paillier encryption of a value, a fresh randomness $r$ is needed. Explain how decryption function removes randomness from the ciphertext.

OT-transfer

4. **Anonymization Techniques**

Table 1: Original data, Table T0.

| Gender | Birthdate | Occupation | Disease |
|---|---|---|---|
| Female | 12/11/1987 | Farmer | flu |
| Male | 03/05/1986 | Engineer | ulcer |
| Female | 05/06/1985 | Manager | gastritis |
| Female | 11/04/1985 | Manager | bronchitis |
| Male | 12/11/1986 | Engineer | gastritis |
| Female | 07/11/1987 | Farmer | flu |

(a) *(8 points)* For Table 1, answer the following questions.

1. (2 points) Draw DGH's for Birthdate with 3 levels of anonymization ($B_0, B_1, B_2$) and Occupation with 2 levels of anonymizations($O_0, O_1$) where $B_0$ and $O_0$ indicate no anonymization.
2. (2 points ) Decide the value of $k$ (as in k-anonymous) in T0 for a) (Birthdate), and b) (Gender, Occupation) tuples.
3. (2 points) Provide the following tables: $T_1(G_0, B_1, O_0)$ and $T_2(G_0, B_2, O_1)$. Do they satisfy $k$-anonymity for $k = 2$? ($G_0$ indicates no anonymization on Gender attribute.)
4. (2 points) Compute the discernibility metric for T1 and T2. DM is defined as

$$DM(T) = \sum_{qid_i} |T[qid_i]|^2 ,$$

where $|T[qid_i]|$ is $qid_i$ group size.

(b) *(4 points)* Determine the global sensitivity ($\Delta f$) for the following queries and explain your answer.

1. The height of students in TU Delft.
2. The total surface area of tulip fields in the Netherlands.
3. The number of women in Delft who are older than 40.
4. The total number of birds per species in the Hague area.