Exam—August 15, 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** *(11 points, counting for 25% of the grade)*

   (a) i. *(3 points)* Provide and explain the three steps/operations a single mix performs as part of a mixnet in order to destroy the link between messages that go into the mix and those that leave the mix.

   ii. *(1 point)* Explain how the timed mix flushing strategy works.

   iii. *(1 point)* Give two main security goals of a mixnet.

   iv. *(1 point)* Describe an attack against the timed mix flushing strategy.

   v. *(2 points)* Describe two other flushing strategies that can be used in a mixnet that does not suffer for the attack described in subpart (iv).

   (b) *(3 points)* Consider the dining cryptographers network shown in figure 1. 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.

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

2. **Privacy in Identity Management** *(11 points, counting for 25% of the grade)*

   (a) 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 be an element in $\mathbb{Z}_q$. Consider the statement

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

   that we want to prove in zero-knowledge, where the values X and Y are known to both the prover and the verifier.

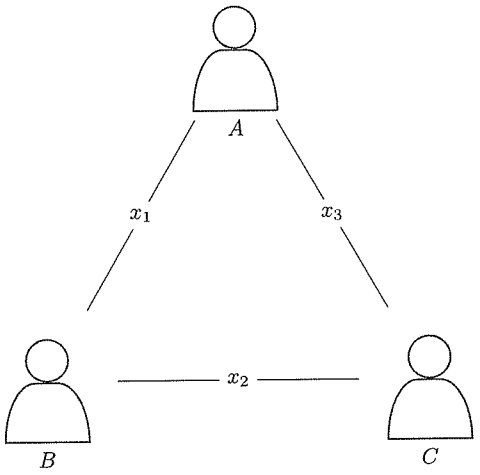

Figure 1: Visualization of a dining cryptographers network. Participant A shares the coin flip outcome x_1 with participant B, participant B shares x_2 with C, and C shares x_3 with A.

Complete the Σ-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. $r_X = g^{k_1}, r_Y =$ _____ for _____ $\in_R$ _____
Challenge. _____ $\in_R$ _____
Response. _____ (mod q)
Verification. Output TRUE if and only if _____ $= r_X \cdot X^e$ and _____

ii. *(2 points)* Prove that the protocol is special sound.

iii. *(2 points)* In subpart (i), note that in the prover's **Response**, one (or more) element(s) are sent *reduced modulo* q, *i.e.*, "(mod q)." What will happen if the prover does not reduce his response modulo q to obtain an element in $\mathbb{Z}_q$, but would return element(s) in $\mathbb{Z}$ instead?
Hint: Remember that the verifier should not learn more information about x other than the fact that the prover knows it.

(b) i. *(2 points)* Name and explain *five* security and/or privacy goals of the voting protocol by **CFS+96** as discussed in the lectures.

ii. *(1 point)* In an electronic voting scheme, participants should not be able to duplicate their votes. How could one satisfy this requirement while still achieving voter privacy?

3. **Anonymization Techniques** *(10 points, counting for 25% of the grade)*

(a) *(1 point)* Give a definition for T-closeness. Suggest 2 methods to achieve T-closeness and explain their advantages and disadvantages.

(b) Consider the table below(T0).

i. *(1 point)* Provide the K values for {Job}, {Job,Sex}, and {Job,Sex,Age} attributes.

JOB	SEX	AGE	DISEASE
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Writer	Female	35	Flu
Writer	Female	35	HIV
Dancer	Female	35	HIV
Dancer	Female	35	HIV

ii. *(1 point)* Compute the probabilities for Bob having Flu, HIV, and Hepatitis: P(Bob=Flu), P(Bob=HIV), and P(Bob=Hepatitis). (Show how you compute each of them.)

iii. *(2 points)* Make the table 3-Anonymous (T1) and then 3-Diverse (T2). Suppression is **not** allowed.

iv. *(1 point)* Compute the same probabilities for Bob having Flu, HIV, and Hepatitis: P(Bob=Flu), P(Bob=HIV), and P(Bob=Hepatitis) for T2. P(Bob=Flu), P(Bob=HIV), and P(Bob=Hepatitis)

(c) *(1 point)* Provide the 5 steps for applying differential privacy on a query.

(d) *(2 points)* Give a definition for the sensitivity function (Δf). Calculate Δf for the following query: the average grade of female students in TU Delft.

(e) *(1 point)* Explain 2 limitations of differential privacy briefly.

4. **Secure Computation** *(10 points, counting for 25% of the grade)*

(a) Consider the DGK encryption scheme from Privacy-Preserving Face Recognition paper. Encryption function is defined as follows: $E(m) = g^m h^r \bmod n$ where $n = pq$, g and h are two generators and r is a fresh random number. Recall that $m \in \mathbb{Z}_u$ where u is a small prime divisor of both $p-1$ and $q-1$.

i. *(1 point)* Explain how decryption works.

ii. *(1 point)* DGK scheme enables the key holder to check whether the encrypted message is zero or not, without decryption. Explain the advantage of this *zero-check* function. Hint: Consider the comparison protocol in the paper.

iii. *(1 point)* DGK is an additively homomorphic encryption scheme just like Paillier. Explain why DGK is used in a subprotocol in the paper, instead of Paillier, apart from zero-check function. (That is, advantages of DGK over Paillier.)

(b) For this question, you will design an OR gate with three bit input: one bit from Alice, one bit from Bob and one bit from Charles. Alice will create the garbled table and Bob will evaluate the gate.

i. *(1 point)* Provide the truth table: inputs A, B and C, output Z. Omit the carry over.

ii. *(1 point)* Provide the **garbled** truth table generated by Alice.

iii. *(2 points)* Provide the enumerated list of actions to obtain the result of the garbled gate. Consider Oblivious Transfer (OT) as a sub-protocol (no details needed).

iv. *(1 point)* Give complexity of the protocol in terms of encryption, decryption and OT per person **USING A TABLE**. Explain which encryption scheme can be used.

v. *(1 point)* Explain why Oblivious Transfer is needed.

vi. *(1 point)* If the security model is *malicious*, one can use cut-and-choose method. Explain this approach briefly.