CSCI971/CSCI471 Modern Cryptography
Spring 2024
Assignment 2 (25 marks)
Due: 20 Oct 2024 23:30

Task A: (5 marks)
Please briefly describe how ring signatures can be used in privacy-preserving cryptocurrencies. You can refer to the descriptions from the internet but rephrasing is desired.

Task B: (5 marks)
Please show how to recover the secret key of Schnorr signature given two signatures $(R, z_1), (R, z_2)$ for different messages M_1 and M_2.

Task C: (5 marks)
We need a variant of cryptography notion to meet the following requirements:
- It is a variant based on identity-based signature (IBS).
- In normal IBS, the PKG will generate a private key for an identity ID.
- In this variant IBS, the PKG can generate an accumulated private key (i.e., a single private key) for a bunch of identities, namely ID_1, ID_2, ..., ID_n.
- The signing algorithm can generate a signature signed by ID using this bunch private key when (1) ID is inside this bunch of identities and (2) the bunch of identities are given.
- The verification is the same as the normal IBS.

Please describe the **syntax** and the **correctness requirement** for the new cryptographic scheme.

Task D: (5 marks)
Please show that the following variant of El Gamal encryption is not IND-CPA secure, i.e., you are asked to give an attack that breaks the IND-CPA security for the following scheme.

- **Key generation**:
  - Choose groups G, G_T of order q and a generator g of G, where we can perform the pairing operation e: $G \times G \to G_T$.
  - Then choose a uniform $x \in Z_q$ and compute $h = g^x$.
  - The public key is (G, G_T , e, q, g, h) and the private key is (G, G_T , e, q, g, x). The message space is G.
- **Encryption:**
  - on input a public key pk = (G, G_T , e, q, g, h) and a message $m \in G$, choose a uniform $r \in Z_q$ and output the ciphertext $(g^r, h^r \cdot m)$
- **Decryption:**
  - on input a private key sk = (G, G_T , e, q, g, x) and a ciphertext (c_1 , c_2) , output $m = c_2 (c_1^x)^{-1}$.

Task E: (5 marks)
Assume that you have encrypted a message M using the El Gamal encryption scheme and get a ciphertext $CT = (C_1, C_2) = (g^r, h^r \cdot M)$.

Qa (this question is for CSCI471 students only): You are asked to prove that $M = g^{10}$ or $M = g^{20}$without leaking any additional information.

Qb (this question is for CSCI971 students only): You are asked to prove that $M = g^{100}$ or $M = g^{200}$ without leaking any additional information.

----------END----------

Submission:

Submit the pdf file to the Moodle site.
The following information should be provided on the top.
The pdf file must be your student number only,such as 55555555.pdf

CSCI971/CSCI471 Modern Cryptography
Assignment 1
Name:_____
Student Number:_____

Plagiarism:
A plagiarised assignment will receive a zero mark (and be penalised according to the university rules).