A39857

Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers



UNIVERSITY OF BIRMINGHAM

School of Computer Science

Third Year Undergraduate

06-40087

LH Advanced Cryptography

Main Summer Examinations 2025

Time allowed: 2 hours

[Answer all questions]

Note

This paper is marked out of 100.

Question 1

(a) A friend of yours who graduated prior to the introduction of the "Advanced Cryptography" module is now confronted with the concept of one-time encryption at work. They have run into this concept because of the need to set up a secret sharing scheme and read several statements about one-time encryption and secret sharing (see below).

Comment on the validity of each statement (correct, incorrect/misleading) and explain (in one sentence) why they are either correct or incorrect/misleading.

A. The one-time pad encryption method $c = m \oplus k$ can be made more secure by replacing it with one-time AES encryption $c = AES(m, k)$.

B. Boolean $(2, 2)$ secret sharing of a message m is related to the one-time pad encryption of a message m.

C. Boolean (n, n) secret sharing has the property of perfect indistinguishability of shares. Therefore it is weaker than other secret sharing schemes that have the property of shares not giving any information about the message.

D. Shamir's secret sharing scheme has the property of perfect indistinguishability of shares. Therefore the distribution of shares to share holders does not require a secure channel.

E. Setting up a (t, n) Shamir's secret sharing scheme is easier than setting up a (t, n) Boolean secret sharing scheme.

[15 marks]

(b) Your friend is impressed by your grasp of cryptography and asks you for your help again. They have come across the concept of Left-Right as well as Real-Random security for one time encryption, and want your help with it in the context of a clearly insecure encryption scheme that is based on randomly reordering bits that represent a message. For instance, assume the message $m = 0001$ is meant to be encrypted. Then a one time permutation of indices $1, 2, 3, 4$ is sampled from the space of all permutations of 4 indices, e.g. the permutation could be $k = \{4, 1, 2, 3\}$. The permutation would then be used to re-arrange the bits of m such that the i-th bit in the message becomes the $k(i)$-th bit in the ciphertext: $c_{k(1)} = m_1$, thus $c_4 = m_1 = 0$; $c_{k(2)} = c_1 = m_2 = 0$; $c_{k(3)} = c_2 = m_3 = 0$; and $c_{k(4)} = c_3 = m_4 = 1$. Therefore the encryption of 0001 would be 0010. The scheme is defined in the listing below.

```
K = All Permutations of {1, 2, ..., l}
def KeyGen(K):
    k =$← K
    return k
def Enc(k, m = m_1||m_2||...||m_l):
    for i = 1 to l:
        c_{k(i)} = m_i
    return {c_1||c_2||...||c_l}
def Dec(k, c = c_1||c_2||...||c_l):
    for i = 1 to l:
        m_i = c_{k(i)}
    return {m_1||m_2||...||m_l}
```

Listing 1: Permutation based encryption

A. Give the Left world and the Right world for this encryption scheme.

B. Show via an example how the Left and Right world can be distinguished by an adversary.

C. Give the Real and Random world for this scheme.

D. Show via an example how the Real and Random Worlds can be distinguished by an adversary.

[12 marks]

(c) Your friend is now ready to consider the set up of a secret sharing scheme for their company. The company has four subsidiaries, and a headquarter. The distribution of shares must satisfy the following constraints:

- Each subsidiary must at least have one share.
- The headquarter should also receive at least one share.
- Reconstruction of the secret should be possible if either all subsidiaries come together or the headquarter and two subsidiaries come together.

They wish to share out a secret code that consists of 6 numbers (ranging from $0, \ldots, 9$), for instance a code could be 012345.

A. How many shares must each of the subsidiaries receive, and how many shares must the headquarter receive, given the stated constraints? How many shares are given out in total? **[3 marks]**

B. Explain how to set up a Shamir secret sharing scheme. Specifically, state what is suitable threshold t given the setting described above, how many shares n must be given out, what is the degree d of the polynomial, what is the size of the modulus? How are the shares generated? **[5 marks]**

Question 2

You have been drafted in as a consultant to analyse potential attack paths and mitigation options for an implementation of the block cipher Klein. The block cipher was designed for very resource constraint environments, and therefore has a small state (64 bits). Structurally, it is similar to AES. At the beginning of a round, the state is exclusive-ored with a round key (`AddRoundKey`). Then a substitution `S()` is applied to four bits of the state (thus S is applied 16 times). Thereafter, neighbouring four bits of the state are combined into a "nibble" and then the nibbles are left rotated by two positions (`RotateNibbles`). Thereafter, an operation `MixNibbles` is applied to the eight leftmost and then the eight rightmost nibbles. This process is graphically displayed in Figure 1.

(a) Explain the working principle of a differential input attack (cover all five steps). **[15 marks]**

(b) Outline two non-protocol countermeasures against differential input attacks. **[6 marks]**

(c) What type of secret sharing would be most compatible with Klein? Justify your reasoning. **[4 marks]**

(d) The Klein S-box is an invertible function that maps a four bit input to a four bit output. Suppose that an implementation with three shares is desirable, so any intermediate v is represented via (v_1, v_2, v_3).

A. Explain how v_1, v_2, and v_3 would be chosen in the case of Boolean secret sharing. **[4 marks]**

B. The implementation must be based on using look-up tables for the S-box step. Only a single further look-up table can be stored, and this will be reused for all 16 look-ups. The implementation should guard against potential Hamming distance leakage. How could this be achieved when three shares are being used? **[4 marks]**

C. Does a three share scheme give a security guarantee against a univariate side-channel key-recovery adversary that considers trace points independently of each other (no combination of trace points)? If so state the guarantee? **[1 mark]**

D. Does a three share scheme give a security guarantee against a bi-variate side-channel key-recovery adversary (bi-variate means that the adversary considers pairs of trace points)? **[1 mark]**

Question 3

This question deals with the concept of multi-party computation (MPC) and its application to solve distributed computing challenges.

(a) What is the general setting for MPC and what is the general security guarantee that we require any MPC protocol to satisfy? How is Shamir's secret sharing scheme used within a typical MPC setting? **[6 marks]**

(b) What are the two types of adversaries that are commonly considered in the context of MPC? Briefly explain the abilities of each adversary and their goal. **[8 marks]**

(c) An MPC solution for the private aggregation of input values of n clients is being designed using a $(3, 3)$ Shamir secret sharing scheme. There seems to be a problem with the implementation of the MPC addition in one of the parties. Here is a snap shot of an exemplary computation using three inputs. You can see the shares that each party has, and the aggregate that they have computed. One party's aggregate is wrong (determine this party). Correct their mistake to compute the final aggregate $a + b + c$. Hint: $\delta_1(0) = 3, \delta_2(0) = 8, \delta_3(0) = 1$. All computations happen over $\mathbb{Z}_{11}$. **[6 marks]**

Value	P_1	P_2	P_3
a	9	2	3
b	6	0	7
c	3	7	2
$a+b+c$	7	9	0

(d) Comment on the validity (correct vs incorrect/misleading) of the following statements about the BGW protocol for secure computation. Briefly explain your reasoning.

A. The BGW protocol protects against adversaries that can send incorrect share values to other parties. **[2 marks]**

B. The BGW protocol can efficiently compute Boolean functions. **[2 marks]**

C. If a multiplication needs to be carried out, then we must have that the threshold t (i.e. t parties are required to reconstruct the result at the end) satisfies that $2(t-1) \leq n$. **[2 marks]**

D. If only additions are required during a computation, then parties do not need to interact except during the initial sharing and the final reconstruction. **[2 marks]**

E. If multiplications with a constant are required during a computation, then parties do need to interact in order to perform a degree reduction. **[2 marks]**

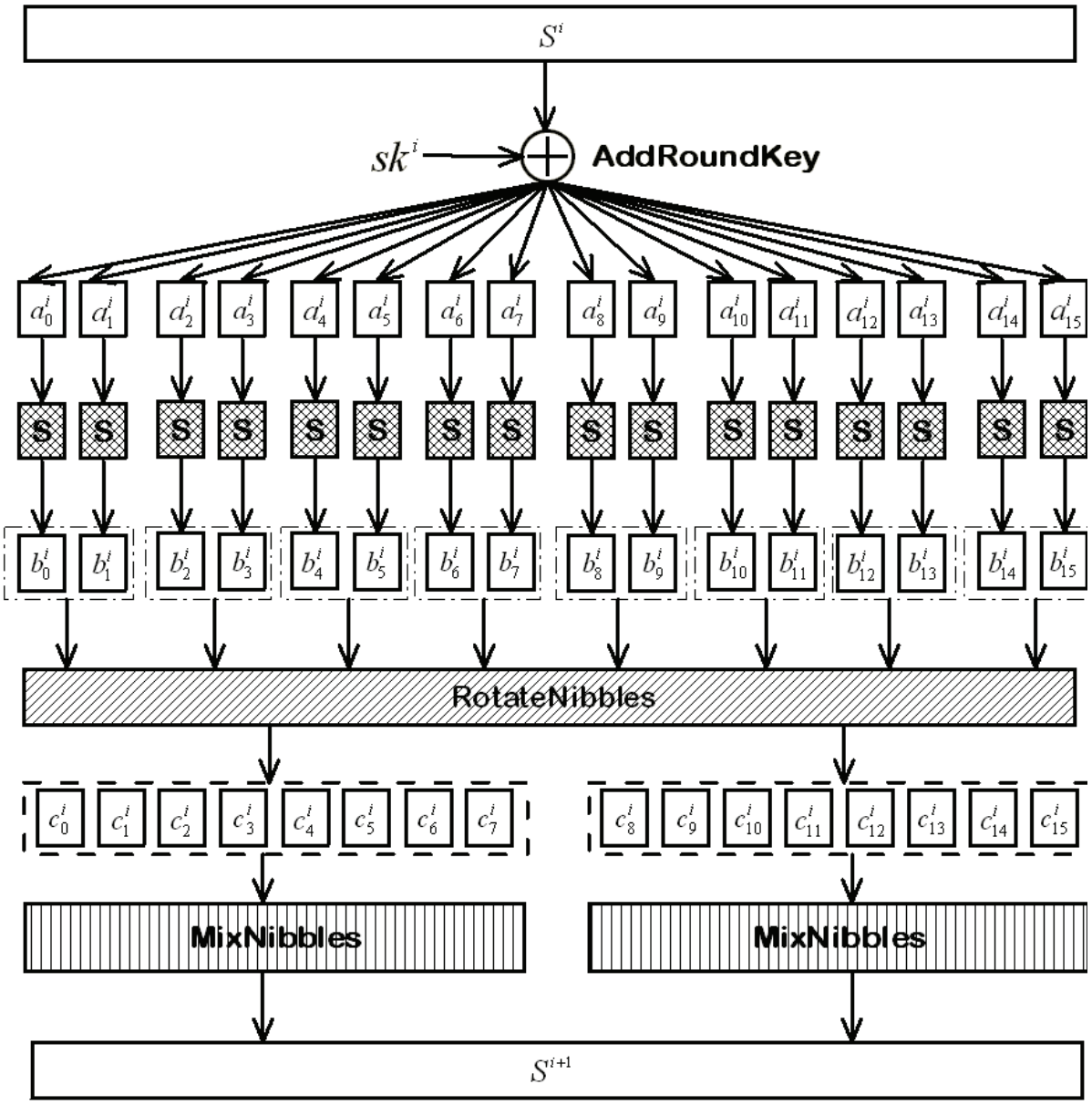


Figure 1: Klein: round function

This page intentionally left blank.

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.