CS 758

Assignment 4

due by 1:00 PM on Tuesday July 26, 2016

General Instructions

- Assignments must be handed in by the designated time. Please hand in a *hard copy*. Due to the large number of students in the class, **no extensions will be given**.
- You are permitted to discuss assignment questions *informally* with a partner. However, when you hand in the assignments you must indicate who you had discussions with, and all solutions must be written up separately. **No copying of solutions or computer code is allowed.** Copied assignments are considered to be plagiarism and are subject to severe penalties.
- It is recommended that you attempt to solve every question on your own. If you do use an external information source (a book or a research paper, for example), **give an appropriate citation**.
- Computational questions can be done using any desired programming tools, languages or calculators. Maple is *strongly recommended* as the easiest way to do the questions. **Please include all source code, and sufficient output so I can verify the main steps in the computations.**
- I am available to provide extra help or hints if you get stuck on a question.

Questions

1. We describe a $(4, r^3, r^2)$ 2-IPP code. The alphabet is $Q = \mathbb{Z}_r \times \mathbb{Z}_r$. The code $\mathcal{C} \subseteq Q^4$ consists of the following set of r^3 4-tuples:

$$\{((a,b),(a,c),(b,c),(a+b \bmod r, c)) : a,b,c \in \mathbb{Z}_r\}.$$

   Suppose that this code is constructed when $r = 100$. For each of the following 4-tuples $\mathbf{f}$, determine if $\mathbf{f}$ is a descendant of two codewords, and if it is, find at least one of the parents.

   (a) ((37,71),(37,96),(71,96),(12,96))

   (b) ((25,16),(83,54),(16,54),(41,54))

   (c) ((19,11),(19,12),(11,15),(30,12))

   (d) ((32,40),(32,50),(50,40),(82,30)).

2. Suppose we want to revoke r users, say $U_{i_1}, \ldots, U_{i_r}$, **at the same time** in the LKH scheme. Assuming that the tree depth is d and the nodes are labelled as described in class, we can assume that $2^d \leq U_{i_1} < \cdots < U_{i_r} \leq 2^{d+1} - 1$.

   (a) Present an algorithm that can be used to determine which keys in the tree need to be updated. (Give a pseudocode description of your algorithm and a brief explanation.)

(b) Give a precise description of the broadcast that is used to update the keys. Specify which keys are used to encrypt the new, updated keys.

(c) Illustrate your algorithms from (a) and (b) by describing the updated keys and the broadcast if users 18, 19, 24 and 27 are to be revoked in a tree with depth $d = 4$. How much smaller is the single broadcast required in this case, as compared to the total size of the four broadcasts that would be required to revoke these four users one at a time?

3. Recall the definition of a (n, m, w)-*perfect hash family* (PHF) from slide 362. PHF can be used for broadcast encryption. The following description summarizes how this can be done.

step 1. Given a PHF$(N; n, m, w)$, construct a certain Nm by n incidence matrix (entries are 0's and 1's), denoted by M.

step 2. Use M to set up Nm Fiat-Naor 1-KDPs, similar to the decription on slide 306. Denote these schemes as $\mathcal{F}_{i,j}$, $1 \leq i \leq N$, $1 \leq j \leq m$.

step 3. Split the secret $K \in \mathbb{Z}_p$ into N shares, using an (N, N) threshold scheme in which the secret is the modulo p sum of the shares. Denote these shares as $s_1, \ldots, s_N$.

step 4. Let P be the subset to which K is being broadcast. For all i, j, let $k_{i,j}$ be the group key for $P \cap \text{users}(\mathcal{F}_{i,j})$. Use $k_{i,j}$ to encrypt s_i, for all i, j.

step 5. Broadcast the Nm encryptions of the shares.

(a) Describe how to construct the Nm by n incidence matrix from the PHF.

(b) Describe how each user in P can decrypt the broadcast, finding K.

(c) Explain why the scheme is secure against coalitions of size w.

(d) Given the PHF depicted below, describe in detail how the scheme is set up (and list the keys held by each user); how the group keys would be constructed for the set $P = \{1, 2, 3, 4\}$; and how the broadcast is formed.

A PHF$(4; 9, 3, 3)$

0	0	0	0
0	1	1	1
0	2	2	2
1	0	1	2
1	1	2	0
1	2	0	1
2	0	2	1
2	1	0	2
2	2	1	0