CS 798

Assignment 4

due 11:30 AM, Tuesday, December **3**

1. (a) Suppose there exists a PHF$(N; n, m, w)$. By constructing a suitable incidence matrix, prove that there exists a $(1, w-1)$-CFF(Nm, n).

   (b) The following array is the *transpose* of a PHF$(4; 9, 3, 3)$:

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

   Construct a $(1, 2)$-CFF$(12, 9)$ from this PHF using the technique you described above. Present the CFF both in the form of an incidence matrix and in the form of a set system.

2. 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 an Nm by n incidence matrix, M (this is similar to question 1).

   step 2. Use M to set up Nm Fiat-Naor 1-KDPs, as described in the "general" BES. 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 the (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 $P \cap \mathit{users}(\mathcal{F}_{i,j})$. Use $k_{i,j}$ to encrypt s_i, for all i, j.

   step 5. Broadcast the Nm encryptions of the shares.

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

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

   (c) Given the PHF from question 1, 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.

3. (a) Suppose that the following are the nine shares in a $(6,9)$ Shamir threshold scheme implemented in $\mathbb{Z}_{1993}$:

i	x_i	y_i
1	1	187
2	2	1547
3	3	498
4	4	1407
5	5	1564
6	6	1176
7	7	795
8	8	185
9	9	603

Exactly one of these shares is defective (i.e., incorrect). Your task is to determine which share is defective, and then figure out its correct value, as well as the value of the secret. The "primitive operations" in your algorithm are polynomial interpolations and polynomial evaluations. Try to minimize the number of polynomial interpolations you perform. Hint: The question can be solved using only three polynomial interpolations.

(b) Suppose that a (k,n) Shamir threshold scheme has exactly one defective share, and suppose that $n \geq 2k$. Describe how it is possible to determine which share is defective using only two polynomial interpolations.

(c) More generally, suppose that a (k,n) Shamir threshold scheme has exactly τ defective shares, and suppose that $n \geq (\tau+1)k$. Describe how it is possible to determine which shares are defective using only $\tau+1$ polynomial interpolations.

4. 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 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) Informally describe an algorithm that can be used to determine which keys in the tree need to be updated.

(b) Describe the broadcast that is used to update the keys. Which keys are used to encrypt the new, updated keys?

(c) Illustrate (a) and (b) by describing the updated keys and the broadcast if users 18, 23 and 29 are to be revoked in a tree with depth $d = 4$. How much smaller is the broadcast in this case, as compared to the three broadcasts that would be required to revoke these three users one at a time?

5. (a) Consider the $(3, 3r^2, r^2+2r)$ 2-IPP code $\mathcal{C}$ that was described in class. Give a complete description of a $O(1)$ time algorithm TRACE, which takes as input a triple $\mathbf{f} = (f_1, f_2, f_3)$ and attempts to determine an identifiable parent of $\mathbf{f}$. If $\mathbf{f} \in \mathcal{C}$, then TRACE$(\mathbf{f}) = \mathbf{f}$; if $\mathbf{f} \in \mathsf{desc}_2(\mathcal{C}) \backslash \mathcal{C}$, then TRACE$(\mathbf{f})$ should find an identifiable parent of $\mathbf{f}$; and TRACE$(\mathbf{f})$ should return the output "fail", if $\mathbf{f} \notin \mathsf{desc}_2(\mathcal{C})$.

(b) Illustrate the execution of your algorithm in the case $r = 10$ $(q = 120)$ for the following triples: $(13, 11, 17)$; $(44, 9, 14)$; $(18, 108, 9)$.

Note: You can write a computer program to answer this question, but it is not required. If you do not write a program, give a detailed pseudo-code description of your algorithm.