T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 8: Solutions
1.4.–2.4.2003

1. We arbitrarily pick the prime $p = 5939$. We next pick a random polynomial $f \in \mathbb{Z}_p$ with $\deg f < 3$ and $f(0) = 4321$. We randomly pick $a_1 = 4$ and $a_2 = 13$ and set $f(x) = s + a_1 x + a_2 x^2 = 4321 + 4x + 13x^2$. We next evaluate the polynomial f at 5 distinct points:

$$\begin{aligned} f(1) &= 4338 \ , \\ f(2) &= 4381 \ , \\ f(3) &= 4450 \ , \\ f(4) &= 4545 \ , \quad \text{and} \\ f(5) &= 4666 \ . \end{aligned}$$

The shares are $(1, 4338)$, $(2, 4381)$, $(3, 4450)$, $(4, 4545)$ and $(5, 4666)$.

2. Since the threshold is 3, we know that the sharing polynomial have degree at most 2. Thus, $f(x) = a_0 + a_1 x + a_2 x^2 \in \mathbb{Z}_{2^{16}+1}$, where a_0 is the secret. From the known shares $(2, 19535)$, $(4, 1583)$ and $(5, 44146)$, we get the linear system

$$\begin{cases} a_0 + a_1 2 + a_2 2^2 \equiv 19535 \\ a_0 + a_1 4 + a_2 4^2 \equiv 1538 \qquad \pmod{2^{16+1}} \ . \\ a_0 + a_1 5 + a_2 5^2 \equiv 44146 \end{cases}$$

This can be solved e.g. using Gaussian elimination to give

$$\begin{cases} a_0 \equiv 159 \\ a_1 \equiv 19020 \quad \pmod{2^{16+1}} \ . \\ a_2 \equiv 60871 \end{cases}$$

Thus, the secret is 159.

3. (a) For all $i = 1, \ldots, t$, we know that $y_i = f(x_i) = a_0 + a_1 x_i + \cdots + a_{t-1} x^{t-1}$. Written in matrix form, this gives the linear system

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}$$

over $\mathbb{F}$.

(b) The coefficient matrix above is a Vandermonde matrix. By a well-know formula for the determinant of Vandermonde matrices, its determinant is

$$\prod_{1 \le j < k \le t} (x_k - x_j) \ .$$

Since $x_k \neq x_j$ for all $k \neq j$ (the shares are distinct), the determinant is nonzero. Thus, the linear system has a unique solution for $a_0, \ldots, a_{t-1}$. This solution in particular gives the secret a_0.

(c) Suppose that we know only $t-1$ shares. As above, this gives a system of $t-1$ equations in t unknowns. Suppose that the parties guess that the secret is s. Since $s = f(0) = a_0$, this gives a tth equation. Adding this equation to the $t-1$ previous ones gives a system of t equations in t unknowns of exactly the same form as in 3a. By the argument in 3b, the system has a unique solution. That is, for each possible value of the secret s, there is a unique polynomial f of degree at most $t-1$ such that $f(0) = s$ and $f(x_i) = y_i$ for $i = 1, \dots, t-1$. Hence, none of the possible values of the secret can be ruled out and the group of $t-1$ parties does not learn anything about the secret.

(d) Let A be the coefficient matrix from 3a. Since $\det A \neq 0$, we can solve $a_0, \dots, a_{t-1}$ as

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = A^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} .$$

Since $a_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} a_0 & a_1 & \cdots & a_{t-1} \end{pmatrix}^t$, we can take

$$r = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} A^{-1}$$

as the reconstruction vector. Then $a_0 = r \begin{pmatrix} y_1 & y_2 & \cdots & y_t \end{pmatrix}^t$ as required.

4. (a) If the dealer gives incorrect shares to some set of t players, there will be a unique secret determined by these t shares, and the set of t players have absolutely no way of verifying the secret.

If, however, all the shares are known, t of them can be used to reconstruct the polynomial f. All the shares (x_i, y_i) can then be verified by checking that $y_i = f(x_i)$ for all i.

(b) The situation where some of the parties submit incorrect shares to the reconstruction phase is exactly the same.

These problems can be solved using a *verifiable secret sharing scheme*. These are roughly speaking secret sharing schemes augmented with commitments to shares and zero-knowledge proofs that the shares are correct.