14.4 Exercises

Exercise 14.4.1
Let p be a prime number, g a primitive root mod p, $a \in \{0, 1, \ldots, p-2\}$, and $A = g^a \bmod p$. Describe a zero-knowledge proof for the knowledge of the discrete logarithm a of A mod p to the base g.

Exercise 14.4.2
In the Fiat-Shamir scheme, let $n = 143$, $v = 82$, $x = 53$, and $e = 1$. Determine a valid response that proves the knowledge of a square root of v mod n.

Exercise 14.4.3 (Feige-Fiat-Shamir protocol)
The Feige-Fiat-Shamir protocol is a modification of the Fiat-Shamir protocol. In this protocol, a cheating verifier is discovered with much higher probability. A simplified version works as follows. Alice uses an RSA modulus n. She chooses random numbers $s_1, \ldots, s_k$ in $\{1, \ldots, n-1\}^k$ and computes $v_i = s_i^2 \bmod n$, $1 \le i \le k$. Her public key is $(n, v_1, \ldots, v_k)$. Her secret key is $(s_1, \ldots, s_k)$. To convince Bob of her identity, she chooses a random number $r \in \{1, \ldots, n-1\}$, computes the commitment $x = r^2 \bmod n$, and sends it to Bob. Bob chooses a random challenge $(e_1, \ldots, e_k) \in \{0, 1\}^k$ and sends it to Alice. Alice sends the response $y = r \prod_{i=1}^{k} s_i^{e_i}$ to Bob. Bob verifies that $y^2 \equiv x \prod_{i=1}^{k} v_i^{e_i} \bmod p$. Determine the probability of success for a cheating verifier in one round.

Exercise 14.4.4
Modify the scheme from Exercise 14.4.3 such that its security is based on computing discrete logarithms.

Exercise 14.4.5 (Signatures from identification)
Find a signature scheme based on the protocol from Exercise 14.4.3. The idea is to replace the challenge by the hash value $h(x \circ m)$, where m is the message to be signed and x is the commitment.

15 Secret Sharing

CHAPTER

In public-key infrastructures it is frequently useful to be able to reconstruct private keys. For example, if a user has lost his smartcard that contains his private decryption key, then he cannot decrypt any encrypted file on his computer anymore. So those encrypted files are then inaccessible for the user unless it is possible to reconstruct the decryption key. However, for security reasons it may be important that the key cannot be reconstructed by a single person. That person could abuse the knowledge of the private key. It is more secure if a group of people has to be involved in the reconstruction. In this chapter we describe *secret sharing*, a protocol that can be used to solve this problem.

15.1 The Principle

We explain what secret sharing does. Let n and t be positive integers. In an (n, t) secret sharing protocol the secret is distributed among n shareholders. Each of them has his share of the secret. If t of the shareholders collaborate, then they can reconstruct the se-

cret. However, fewer than t shareholders cannot obtain any relevant information about the key.

15.2 The Shamir Secret Sharing Protocol

Let $n, t \in \mathbb{N}$, $t \leq n$. We describe the (n, t) secret sharing protocol of Shamir [65]. It uses a prime number p and is based on the following lemma.

Lemma 15.2.1
Let $\ell, t \in \mathbb{N}$, $\ell \leq t$. Also, let $x_i, y_i \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq \ell$, where the x_i are pairwise distinct. Then there are exactly $p^{t-\ell}$ polynomials $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ of degree $\leq t-1$ with $b(x_i) = y_i$, $1 \leq i \leq \ell$.

Proof. The Lagrange interpolation formula yields the polynomial

$$b(X) = \sum_{i=1}^{\ell} y_i \prod_{j=1, j\neq i}^{\ell} \frac{x_j - X}{x_j - x_i}. \tag{15.1}$$

It satisfies $b(x_i) = y_i$, $1 \leq i \leq \ell$. This shows that at least one polynomial exists with the asserted properties. Now we determine the number of such polynomials.

Let $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ be such a polynomial. Write

$$b(X) = \sum_{j=0}^{t-1} b_j X^j, \quad b_j \in \mathbb{Z}/p\mathbb{Z}, 0 \leq j \leq t-1.$$

From $b(x_i) = y_i$, $1 \leq i \leq \ell$ we obtain the linear system

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_\ell & x_\ell^2 & \cdots & x_\ell^{t-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_\ell \end{pmatrix}. \tag{15.2}$$

The coefficient matrix

$$U = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{\ell-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{\ell-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_\ell & x_\ell^2 & \cdots & x_\ell^{\ell-1} \end{pmatrix}$$

is a *Vandermonde matrix*. Its determinant is

$$\det U = \prod_{1 \leq i < j \leq \ell} (x_i - x_j).$$

Since the x_i are distinct by assumption, that determinant is nonzero. So the rank of U is ℓ. This implies that the kernel of the coefficient matrix (15.2) has rank $t - \ell$ and the number of solutions of our linear system is $p^{t-\ell}$. □

Now we are able to describe the protocol.

15.2.1 Initialization

The dealer chooses a prime number p, $p \geq n+1$ nonzero elements $x_i \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq n$, which are pairwise distinct. Those elements in $\mathbb{Z}/p\mathbb{Z}$ can, for example, be represented by their least nonnegative representative. The dealer publishes the x_i.

15.2.2 The shares

Let $s \in \mathbb{Z}/p\mathbb{Z}$ be the secret.

1. The dealer secretly chooses elements $a_j \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq j \leq t-1$ and constructs the polynomial

$$a(X) = s + \sum_{j=1}^{t-1} a_j X^j. \tag{15.3}$$

   It is of degree $\leq t-1$.
2. The dealer computes the shares $y_i = a(x_i)$, $1 \leq i \leq n$.
3. The dealer sends share y_i to the ith shareholder $1 \leq i \leq n$.

So the secret is value $a(0)$ of the polynomial $a(X)$.

Example 15.2.2
Let $n = 5$, $t = 3$. The dealer chooses $p = 17$, $x_i = i$, $1 \le i \le 5$.

Let the secret be $s = 3$. The dealer chooses the secret coefficients $a_i = p - i$, $1 \le i \le 2$. Then

$$a(X) = 15X^2 + 14X + 3. \tag{15.4}$$

So the shares are $y_1 = a(1) = 15$, $y_2 = a(2) = 6$, $y_3 = a(3) = 10$, $y_4 = a(4) = 10$, $y_5 = a(5) = 6$.

15.2.3 Reconstruction of the secret

Suppose that t shareholders collaborate. Without loss of generality assume that the shares are numbered such that $y_i = a(x_i)$, $1 \le i \le t$ with the polynomial $a(X)$ from (15.3). Now we have

$$a(X) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j - X}{x_j - x_i}. \tag{15.5}$$

In fact, this polynomial satisfies $a(x_i) = y_i$, $1 \le i \le t$ and by Lemma 15.2.1 there is exactly one such polynomial of degree $\le t-1$. Therefore, the shareholders can reconstruct the secret as

$$s = a(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i}. \tag{15.6}$$

Example 15.2.3
We continue Example 15.2.2.

The first two shareholders reconstruct the secret. The Lagrange interpolation formula yields

$$a(0) = 15\frac{6}{2} + 6\frac{3}{-1} + 10\frac{2}{2} \bmod 17 = 3. \tag{15.7}$$

15.2.4 Security

Suppose that m shareholders want to reconstruct the secret where $m < t$. Without loss of generality assume that their shares are y_i,

$1 \le i \le m$. The shareholders know that the share is the constant term $a(0)$ of a polynomial $a \in \mathbb{Z}_p[X]$ of degree $\le t-1$ that satisfies $a(x_i) = y_i$, $1 \le i \le m$. From Lemma 15.2.1 we obtain the following result.

Lemma 15.2.4
For any $s' \in \mathbb{Z}/p\mathbb{Z}$ there are exactly p^{t-m-1} polynomials $a'(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ of degree $\le t-1$ with $a'(0) = s'$ and $a'(x_i) = y_i$, $1 \le i \le m$.

Proof. Since the x_i are pairwise distinct and nonzero, the assertion follows from Lemma 15.2.1 with $\ell = m + 1$. □

Lemma 15.2.4 shows that the m shareholders obtain no information about the secret since all possible constant terms $a(0)$ are equally likely.

15.3 Exercises

Exercise 15.3.1
Reconstruct the secret in Example 15.2.2 from the last three shares.

Exercise 15.3.2
Let $n = 4$, $t = 2$, $p = 11$, $s = 3$, $a_1 = 2$. Construct $a(X)$ and the shares y_i, $1 \le i \le 4$.