Institut for Matematik og Datalogi
Syddansk Universitet

May 4, 2005
JFB

Cryptology – F05 – Lecture 12

Lecture, April 29

We covered undeniable signatures following that handout given in class and begin on protocols (from the handout). We covered sections 11.1.3 and 11.1.4 in Goldwasser and Bellare's lecture notes.

Lecture, May 6

We will begin on zero-knowledge (from the handout), covering the the first four subsections of section 11.2 in the lecture notes by Goldwasser and Bellare.

Lecture, May 13

We will continue with zero-knowledge, covering section 11.2.5 from the lecture notes by Goldwasser and Bellare, and giving some more examples.

Problem session May 11

1. Let n be an integer with unknown factorization $n = pq$, where p and q are prime, and let $x_0, x_1 \in \mathbb{Z}_n^*$ be such that at least one of x_0 and x_1 is a quadratic residue modulo n. Assume that both x_0 and x_1 have Jacobi symbol $+1$ modulo n. (Assume that it is x_b and $u^2 \equiv x_b \pmod{n}$). Suppose that x_0, x_1, and n are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated $\log_2 n$ times:

Prover		Verifier
Choose random $i \in \{0,1\}$ and random $v_b, v_{1-b} \in \mathbb{Z}_n^*$. Compute $y_b = v_b^2 \pmod{n}$ and $y_{1-b} = v_{1-b}^2 (x_{1-b}^i)^{-1} \pmod{n}$.	$\xrightarrow{y_0, y_1}$	
		Choose a random $c \in \{1,0\}$.
	$\xleftarrow{c}$	
Compute $z_b = u^{i \oplus c} v_b \pmod{n}$, $z_{1-b} = v_{1-b}$.	$\xrightarrow{z_0, z_1}$	
		Check that either ($z_0^2 \equiv y_0 \pmod{n}$ and $z_1^2 \equiv x_1^c y_1 \pmod{n}$) or ($z_0^2 \equiv x_0 y_0 \pmod{n}$ and $z_1^2 \equiv (x_1)^{1-c} y_1 \pmod{n}$). If not, reject and halt.

Note that $\oplus$ is addition modulo 2.

a. Prove that the above protocol is an interactive proof system showing that at least one of x_0 and x_1 is a quadratic residue modulo n.

b. Suppose that x_{1-b} is also a quadratic residue. What is the distribution of the values y_0, y_1, z_0, z_1 sent by a Prover following the protocol?

c. Suppose that x_{1-b} is a quadratic nonresidue. What is the distribution of the values y_0, y_1, z_0, z_1 sent by a Prover following the protocol?

d. Prove that the above protocol is perfect zero-knowledge.

2. Throughout this problem, suppose it is known that $n = p \cdot q$, where p and q are distinct primes, though the factorization of n is unknown to the Verifier. Let $x, y \in \mathbb{Z}_n^*$ both have Jacobi symbol $+1$.

   a. Prove that $x \cdot y \pmod{n}$ is a quadratic residue modulo n if and only if either

   (a) x and y are both quadratic residues, or

(b) x and y are both quadratic nonresidues.

b. Prove that $x^3 \cdot y^5 \pmod{n}$ is a quadratic residue modulo n if and only if either

(a) x and y are both quadratic residues, or

(b) x and y are both quadratic nonresidues.

c. Give a perfect zero-knowledge proof showing that x and y satisfy one of the following two conditions modulo n:

(a) x and y are both quadratic residues, or

(b) x and y are both quadratic nonresidues.

3. This is similar to a problem from the first edition of Stinson's textbook. Suppose $n = pq$, where p and q are two (secret) distinct large primes. Suppose that α is an element with large order in $\mathbb{Z}_n^*$. Define a hash function $h : \{1, .., n^2\} \to \mathbb{Z}_n^*$ by $h(x) = \alpha^x \pmod{n}$. Suppose $n = 603241$ and $\alpha = 11$, and suppose that we are given three collisions for h: $h(1294755) = h(80115359) = h(52738737)$. Use this information to factor n:

   (a) How do you find an exponent y such that $\alpha^y = 1 \pmod{n}$? What exponent do you find in this case?

   (b) How do you find the four square roots of 1 modulo n? (Hint: Recall the Rabin-Miller algorithm for primality testing.) What are they in this case?

   (c) Now, how do you factor n?

4. The Subgroup Membership Problem is as follows: Given a positive integer n and two distinct elements $\alpha, \beta \in \mathbb{Z}_n^*$, where the order of α is l and is publicly know, determine if β is in the subgroup generated by α.

   Suppose that α, β, l, and n are given as input to a Prover and Verifier, and that the Prover is also given k such that $\alpha^k = \beta \pmod{n}$. Consider the interactive protocol in which the following is repeated $\log_2 n$ times:

Prover		Verifier
Choose random $0 \leq j \leq l-1\}$. Compute $\gamma = \alpha^j \pmod{n}$.	$\xrightarrow{\gamma}$	
		Choose a random $c \in \{0, 1\}$.
	$\xleftarrow{c}$	
Compute $h = j + ck \pmod{l}$.		
	$\xrightarrow{h}$	
		Check that $\alpha^h \equiv \beta^c \gamma \pmod{n}$. If not, reject and halt.

(a) Prove that the above protocol is an interactive proof system for Subgroup Membership.

(b) Suppose that β is in the subgroup generated by α. Show that the number of triples (γ, c, h) which the Verifier would accept is $2l$ and that each such triple is generated with equal probability if both the Prover and Verifier follow the protocol.

(c) Suppose that β is in the subgroup generated by α. What is the distribution of the values γ, h sent by a Prover following the protocol?

(d) Prove that the above protocol is perfect zero-knowledge.

(e) If n is a prime, what value can you use for l? If n is not prime, is it reasonable to make this value l known?