Institut for Matematik og Datalogi
Syddansk Universitet

May 11, 2005
JFB

Cryptology – F05 – Lecture 13

Lecture, May 6

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

Lecture, May 13

We will continue with zero-knowledge, giving some more examples, including proofs of knowledge.

Lecture, May 20

We will cover bit commitments which are computationally binding and unconditionally concealing. Then, we will cover secret sharing and oblivious transfer from the notes by Goldwasswer and Bellare, and introduce secure pseudorandom number generators.

Recall that the exam will be June 1.

The pensum is all subjects covered in the lectures and discussion sections. The relevant sections in the textbook and handouts are all mentioned in the weekly notes.

Problem session May 18

1. (From the last note:) 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. The Subgroup Membership Problem is as follows: Given a positive integer n and two distinct elements α, $\beta \in \mathbb{Z}_n^*$, 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.

---

   e (From the last note:) 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?

3. Give a zero-knowledge interactive proof system for the Subgroup Non-membership Problem (showing that β is not in the subgroup generated by α). Prove the your protocol is an interative proof system. Prove that it is zero-knowledge.

4. Let $p = 4k + 3$ be a prime, and let g and h be quadratic residues modulo p. Assume that h is in the subgroup generated by g and that the Prover knows an x such that $g^x = h \pmod{p}$. Suppose that p, g, and h are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated $\log_2 p$ times:

Prover		Verifier
Choose a random $k \in \{1, ..., \frac{p-1}{2}\}$. Let $z = h \cdot g^{2k} \pmod p$.	$\xrightarrow{z}$	
		Choose a random $b \in \{0, 1\}$.
	$\xleftarrow{b}$	
Let $r = 2k + b \cdot x \pmod{p-1}$.	$\xrightarrow{r}$	
		Check that r is even, $z = g^r h^{1-b} \pmod p$, $p \pmod 4 = 3$, and $g^{\frac{p-1}{2}} = 1 \pmod p$. If not, reject and halt.

(Actually, the last two checks only need to be done once and could be done before the first round of the protocol. Don't let their placement here confuse you.)

a. Prove that the above protocol is an interactive proof system showing that $h = g^{2y} \pmod p$ for some integer y.

b. Suppose that $h = g^{2y} \pmod p$ for some integer y. What is the probability distribution of the values (z, r) sent by a Prover following the protocol?

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

d. Suppose $p = 4k + 3$. Note that any quadratic residue g modulo p has odd order. Use this fact to show that if h is in the subgroup generated by a quadratic residue g, then it is always possible to write h as $h = g^{2y} \pmod p$ for some integer y. (Thus, the above protocol is an alternative zero-knowledge proof of subgroup membership for this special case.)

e. Suppose $p = 4k + 3$, $g \neq 1$ is a quadratic residue modulo p, and $q =$

$\frac{p-1}{2} = 2k+1$ is a prime. Then, there is a more efficient secure way, than using the above protocol, to convince the Verifier that $h = g^y \pmod{p}$ for some integer y. What is it? (Hint: no Prover is necessary.)