Institut for Matematik og Datalogi
Syddansk Universitet

May 4, 2011
JFB

Cryptology – F11 – Week 12

Lecture, May 4

We continued with zero-knowledge, from the notes and slides, and began on chapter 9 in the textbook.

Lecture, May 11

We will finish chapter 9 in the textbook and begin on chapter 10.

Lecture, May 16

We will cover sections 10.1, 10.2, and 10.5.4 of chapter 10, section 11.2 of chapter 11, and section 13.1 of chapter 13.

Problem sessions May 12 and May 18.

1. 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. (Assume that you know a multiple of the order of α.

2. 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.)

3. Do problem 8.7.

4. Do problem 9.1.

5. Do problem 9.2.

6. Do problem 9.6.

7. Do problem 9.7.

8. Do problem 9.8a.

9. Do problem 9.13.