Institut for Matematik og Datalogi
Syddansk Universitet

April 25, 2013
JFB

Cryptology – F13 – Week 10

Lecture, April 22

We began on zero-knowledge (from the notes on commitment schemes and zero-knowledge by Ivan Damgård and Jesper Buus Nielsen, available through the course's homepage). We covered basic definitions, and zero-knowledge proofs for quadratic residuosity and graph 3-colorability. We also covered a definition for a proof of knowledge.

Lecture, April 25, in U49D

We continued with zero-knowledge from the notes and slides. Note that there are more notes on the course's homepage: Ivan Damgård has notes on graph nonisomorphism and zero-knowledge for NP.

Lecture, May 2

We will finish with zero-knowledge, from the notes, and begin on chapter 9 in the textbook.

All classes after 10:00 on May 3 at SDU are cancelled.

Problem session April 29

1. Do the last problem from April 25.

2. The Subgroup Membership Problem is as follows: Given a positive integer n and two distinct elements α, $\beta \in Z_n^*$, 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?

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

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.)