Institut for Matematik og Datalogi
Syddansk Universitet

May 19, 2005
JFB

Cryptology – F05 – Lecture 14

Lecture, May 13

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

Lecture, May 20

We will finish the zero-knowledge proof of graph nonisomorphism. Then, we will cover bit commitments which are computationally binding and unconditionally concealing. Finally, we will cover secret sharing and oblivious transfer from the notes by Goldwasswer and Bellare, and introduce secure pseudorandom number generators.

Lecture, May 27

We will continue with pseudorandom number generators and oblivious transfer.

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.

Announcement

IMADA
orienteringsmøde
for alle studerende
i datalogi og matematik
torsdag d. 26. maj kl. 16.15 i lokale U49

Program

16:15. Generel information om speciale-/bachelorstudiet. Desuden orientering om den forestående studiereform; specielt mhp. instruktor-ansættelser.

16:45. Orientering om planlagte valgfri kurser i matematik og datalogi samt om mulige speciale- og bachelorprojekter. Endvidere eventuelle "ønsker" fra de studerende

18:00. Gratis forfriskning: Pizza, øl og sodavand.

Problem session May 25

1. (From the last note:) 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 $r = 2k + b \cdot x \pmod{p-1}$.

$$\xrightarrow{\quad r \quad}$$

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.)

2. In class, we looked at a bit commitment scheme which had its security based on the Quadratic Residuosity Assumption. User A has a public key pair (N, y), where N is the product of two large primes and y is a quadratic nonresidue with Jacobi symbol $+1$. To commit to a bit b, user A chooses a random $r \in \mathbb{Z}_N^*$ and produces the blob $y^b r^2 \pmod{N}$. Suppose that user A has committed to two bits b_1 and b_2, producing blobs B_1 and B_2. Show how A can use the blobs B_1 and B_2 to reveal

c such that $c = b_1$ XOR b_2, and to prove to another user B that $c = b_1$ XOR b_2, without revealing b_1 or b_2. (The fact that this can be done means that this system for producing blobs has what is called the *equality property*, because it can be used to show that two blobs are commitments to equal bits, showing that the XOR is zero.)

3. Consider MAJORITY gates with fan-in n, where $n = 2m + 1$. The output should be one if at least $m+1$ of the inputs are one, and zero if at least $m + 1$ of the inputs are zero. Suppose that user A has committed to n input bits, $b_1, b_2, ..., b_n$, and one output bit b_{n+1}, and produced blobs (bit commitments) $B_1, B_2, ..., B_n, B_{n+1}$, using the scheme based on the quadratic residuosity. If user A wishes to prove to user B that $B_1, B_2, ..., B_n$, are commitments to the inputs to a MAJORITY gate and B_{n+1} is a commitment to the output of that same MAJORITY gate, user A only need show that there are $m + 1$ inputs which are equal to the output. In order to hide which of the inputs are the same as the output, user A will produce n more blobs corresponding to the original input blobs for that gate. These additional n blobs will be commitments to the same bits as the input blobs, but user A will send them to user B in random order, so user B will be unable to determine the correspondence. Now, user B will send user A a challenge $c \in \{0, 1\}$. If $c = 0$, user A will show user B the correspondence between the input blobs and the n additional blobs, telling user B which additional blob corresponds to which original input blob and proving it using the equality property If $c = 1$, user A will show that $m+1$ of the additional blobs are commitments to the same bit as B_{n+1} is, again using the equality property. Thus, the protocol is as follows ("random" means independently, from a uniform distribution):

Repeat the following $k(n + 1)$ times, where k is the length of the blobs produced:
User A: Choose random $r_1, r_2, ..., r_n \in \mathbb{Z}_N^*$.
Create $C_i = y^{b_i} r_i^2 \pmod{N}$, for $1 \leq i \leq n$.
Choose a random permutation σ of the numbers $1, 2, ..., n$.
Send user B the blobs $(D_1, D_2, ..., D_n) = (C_{\sigma(1)}, C_{\sigma(2)}, ..., C_{\sigma(n)})$.
User B: Choose random $e \in \{0, 1\}$.
Send e to user A.
User A: Case $e = 0$: Send σ to user A.
Use the equality property to show that $B_{\sigma(i)}$ and D_i

are commitments to the same bit, for $1 \leq i \leq n$.

Case $e = 1$: Choose a subset $\{D_{i_1}, D_{i_2}, ..., D_{i_{m+1}}\}$ of the D_is of size $m + 1$, such that those D_i's are commitments to the same bit as the output blob B_{n+1}. (If there are more than $m + 1$ satisfying this, choose among them randomly.) Use the equality property to show that D_{i_j} and B_{n+1} are commitments to the same bit, for $1 \leq j \leq m + 1$.

User B accepts if user A has correctly answered all challenges and rejects otherwise.

a Show that the protocol described above is an interactive proof system proving that $B_1, B_2, ..., B_n$, are commitments to the inputs to a MAJORITY gate and B_{n+1} is a commitment to the output of that same MAJORITY gate.

b Show that the protocol described above is computational zero-knowledge, assuming the Quadratic Residuosity Assumption.

4. Use problem 4 to design a computational zero-knowledge interactive proof system proving that B_1 and B_2 are commitments to the inputs to an OR gate and B_3 is a commitment to the output to that same OR gate. (Hint: note that an OR gate has an even number of inputs, but the MAJORITY gate described above has an odd number of inputs. Try adding a special extra input to the OR gate.)