Institut for Matematik og Datalogi
Syddansk Universitet

December 12, 2016
JFB

Cryptology – E16 – Lecture 17

Lecture, November 28

We continued with chapter 21 from the slides, covering up through the proof that all problems in NP have zero-knowledge proofs, using the Graph 3-Colorability problem. Commitment schemes from chapter 20 were also discussed, using the Goldwasser-Micali encryption scheme for bit commitment as an example.

Lecture, December 5

We will continue with chapter 21.

Lecture, December 12

We will continue with chapter 21.

Problem session November 29

Last time we did not get to the last problem from some notes by Ivan Damgård, entitled "CPT Notes, Graph Non Zero-Knowledge for NP and Exercises". We will do it this time. I am also repeating the second to last problem for reference.

1. Consider the Pedersen commitment scheme $B_a(x) = h^x \cdot g^a$ where the commitments are only to bits, so $x \in \{0, 1\}$. Suppose a prover P has committed to bits b_1, b_2 using commitments c_1, c_2, where $b_1 \neq b_2$. Now P wants to convince the verifier V that the bits are different. We claim he can do this by sending to V a number $s \in \mathbb{Z}_{p-1}$ such that $c_1 c_2 = hg^s$.

- Show how an honest P can compute the required s, and argue that the distribution of s is the same when $(b_1, b_2) = (0, 1)$ as when $(b_1, b_2) = (1, 0)$. This means that V learns nothing except that $b_1 \neq b_2$.
- Argue that if P has in fact committed in c_1, c_2 to $(0, 0)$ or $(1, 1)$, he cannot efficiently find s as above unless he can compute the discrete logarithm of h.
- Argue in a similar way that P can convince V that she has committed to two bits that are equal by revealing s such that $c_1 c_2^{-1} = g^s$.

2. Assume P commits to two string $b_1, ..., b_t, b'_1, ..., b'_t$ using commitments $c_1, ..., c_t, c'_1, ..., c'_t$ as in the previous exercise. She claims that the strings are different and wants to convince V that this is the case while revealing no extra information. Note that he cannot point to an index j where $b_j \neq b'_j$ and use the above method on c_j, c'_j. This would reveal where the strings are different. Instead consider the following protocol:

   (a) P chooses a random permutation π on the set of indices $\{1, ..., t\}$. She computes, for $i = 1, ..., t$ a commitment $d_i = C(b_{\pi(i)}, r_i)$ and $d_i = C(b'_{\pi(i)}, r'_i)$. In other words, permute both strings randomly with the same permutation and commit bit by bit to the resulting strings. Send $d_1, ..., d_t, d'_1, ..., d'_t$ to V.

   (b) V chooses a random bit b and sends it to P.

   (c) If $b = 1$, P reveals π and uses the above method to convince V for all i that $c_{\pi(i)}$ contains the same bit as d_i. Similarly for $c'_{\pi(i)}$ and d'_i. If $b = 1$, P finds a position i where $b_\pi(i) \neq b'_{\pi(i)}$ and uses the above method to convince V that d_i, d'_i contain different bits.

   - Completeness: Argue that an honest prover always convinces the verifier.
   - Soundness: Show that if P can, for some set of commitments $d_1, ..., d_t, d'_1, ..., d'_r$ answer V correctly for both $b = 0$ and $b = 1$, then there is at least one j, where P can open c_j, c'_j to reveal different bits. Note that we assume she knows how to open the commitments $c_1, ..., c_t, c'_1, ..., c'_t$. The protocol in this exercise does not verify that P knows this — if one wants to check this, there are other protocols one can use.

- Zero-knowledge: Sketch a simulator for this protocol. Hint: given commitment c, if you set $d = cg^{-s} \pmod{p}$, then $cd^{-1} = g^s \pmod{p}$. This means that even if the simulator does not know how to open c, it can create d and fake a proof that d contains the same bit as c. You do not have to formally prove that your simulator works.

These are the new problems:

1. 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 known, 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?

2. Give a zero-knowledge interactive proof system for the Subgroup Nonmembership 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.)

3. 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.)