Institut for Matematik og Datalogi
Syddansk Universitet

April 19, 2013
JFB

Cryptology – F13 – Week 9

Lecture, April 17

We finished section 8.4 and covered undeniable signatures from section 7.6 using notes. I gave am introduction to protocols, starting on the slides.

Lecture, April 22

We will begin 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). There are copies of the slides with some course notes.

Lecture, April 25, in U49D

We will continue 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.

Problem session April 25, 8:15 in U142

1. Do exercises 1, 3, 4, and 6 in the notes by Damgård and Nielsen.

2. Do exercises 4 and 5 in the notes by Damgård.

3. Let p be a large prime and let $x, y \in Z_p^*$. Suppose that $x = g^k \pmod p$ and $y = h^k \pmod p$. Assume the Prover knows the value k and that both the Prover and the Verifier are given the values p, g, h, x, and y. To show that the discrete logarithm of x with respect to g is equal to the discrete logarithm of y with respect to h, one can execute the following protocol:

Prover		Verifier
Choose random $s \in Z_{p-1}$. Let $u \equiv g^s \pmod{p}$ $v \equiv h^s \pmod{p}$.	$\xrightarrow{u, v}$	
		Choose a random $c \in Z_{p-1}$.
	$\xleftarrow{c}$	
Let $e \equiv c \cdot k + s \pmod{p-1}$.		
	$\xrightarrow{e}$	
		Check that $g^e \equiv x^c \cdot u \pmod{p}$ and $h^e \equiv y^c \cdot v \pmod{p}$. If so, accept. Otherwise, reject.

a. Prove completeness for the above protocol, showing that (assuming that both the Prover and Verifier follow the protocol) the Verifier will accept if the discrete logarithm of x with respect to g is equal to the discrete logarithm of y with respect to h.

b. Prove soundness for the above protocol. Assume that the discrete logarithm of x with respect to g is not equal to the discrete logarithm of y with respect to h. (Hint: after assuming that the Prover can give acceptable answers for two different values of c, show how a transcript containing both executions could be used to find the discrete logarithm of x with respect to g and the discrete logarithm of y with respect to h.)

c. Prove that the above protocol is honest verifier zero-knowledge, i.e., show that one can efficiently generate conversations $((u, v), c, e)$ with the same distribution as produced by the honest Prover and Verifier, without knowing k.