Institut for Matematik og Datalogi
Syddansk Universitet

May 5, 2003
JFB

Cryptology – F03 – Note 12

Lecture, April 29

We finished undeniable signatures, covering the denial protocol, and began on protocols. There are handouts for this; it is not in the textbook. We covered sections 11.1.3 and 11.1.4 in Goldwasser and Bellare's lecture notes and up through subsection 11.2.4 of section 11.2.

Lecture, May 6

We will continue with zero-knowledge from the notes by Goldwasser and Bellare, covering section 11.2.5, plus some details missed earlier in section 11.2.

Lecture, May 13

We will cover section 11.3.1 of the notes from Goldwasswer and Bellare, and begin on pseudorandom number generators.

Problems for Thursday, May 15

1. This is similar to a problem from the first edition of Stinson's textbook. Suppose $n = pq$, where p and q are two (secret) distinct large primes. Suppose that α is an element with large order in $\mathbb{Z}_n^*$. Define a hash function $h : \{1, .., n^2\} \rightarrow \mathbb{Z}_n^*$ by $h(x) = \alpha^x \pmod{n}$. Suppose $n = 603241$ and $\alpha = 11$, and suppose that we are given three collisions for h: $h(1294755) = h(80115359) = h(52738737)$. Use this information to factor n:

   (a) How do you find an exponent y such that $\alpha^y = 1 \pmod{n}$? What exponent do you find in this case?

(b) How do you find the four square roots of 1 modulo n? (Hint: Recall the Rabin-Miller algorithm for primality testing.) What are they in this case?

(c) Now, how do you factor n?

2. 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 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 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.