Institut for Matematik og Datalogi
Syddansk Universitet

May 9, 2013
JFB

Cryptology – F13 – Week 11

Lecture, May 2

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

May 9 is a holiday.

Lecture, May 10

We will finish chapter 9 in the textbook and begin on chapter 10.

Problem session May 6

1. Do the last problem from April 29.
2. Do problem 8.7.
3. Do problem 9.1.
4. Do problem 9.2.
5. Do problem 9.6.
6. Do problem 9.7.
7. Do problem 9.8a.
8. Do problem 9.13.

Assignment due Thursday, May 30, 10:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two or three. Submit it through Blackboard.

1. Give a zero-knowledge proof for Independent Set. Thus, your input is a graph, G, and a positive integer k, where G has an independent set of size at least k. Assume that the Prover knows such an independent set. (Hint: Consider the proof given in Damgård's notes for Hamiltonian Circuit.) Note that you should do a direct proof, rather than a reduction to another NP-Complete problem and then doing the zero-knowledge proof for the other problem. Prove that your protocol has the following properties:

   - Completeness
   - Soundness
   - Zero-knowledge

2. Let p be a large prime, and let α, β, and γ be elements of Z_p^*. Assume the Prover knows positive integers s and t such that $\gamma \equiv \alpha^s \beta^t \pmod{p}$. The Prover convinces the Verifier that γ is in the subgroup $< \alpha, \beta >$ generated by α and γ by repeating the following protocol $\lceil \log_2 p \rceil$ times:

Prover		Verifier
Choose random $i, j \in \mathbb{Z}_{p-1}$. Let $x \equiv \alpha^i \beta^j \pmod{p}$.		
	$\xrightarrow{x}$	
		Choose a random $b \in \{0, 1\}$.
	$\xleftarrow{b}$	
If $b = 0$, let $s' = i,\ t' = j$. If $b = 1$, let $s' \equiv s - i \pmod{p-1},\ t' \equiv t - j \pmod{p-1}$.		
	$\xrightarrow{s', t'}$	
		If $b = 0$, check that $x \equiv \alpha^{s'} \beta^{t'} \pmod{p}$. If $b = 1$, check that $\gamma \equiv x \alpha^{s'} \beta^{t'} \pmod{p}$. If so, accept. Otherwise, reject.

- Prove completeness for the above protocol, showing that (assuming that both the Prover and Verifier follow the protocol) the Verifier will accept if $\gamma \in < \alpha, \beta >$.
- Prove soundness for the above protocol.
- Prove that the above protocol is perfect zero-knowledge.