Institut for Matematik og Datalogi December 2, 2019
Syddansk Universitet JFB

Cryptology – 2019 – Lecture 17

Announcement

I have moved the remaining lectures on Thursdays to Mondays and Tuesdays in December.

Lecture, November 18 and 19

We covered sections 4.1, 4.2, 4.3, and 4.5 fairly quickly (from the slides), with emphasis on curves of characteristic $p > 3$. We will continue with chapter 16, covering up through section 16.5.3, covering after section 6.1 fairly quickly. We also covered sections 19.1, 19.2.1, and 19.4 from chapter 19. My presentation of Shamir's threshold secret sharing scheme did not directly use Reed-Solomon codes; it was more similar to what you can read here: https://www.eit.lth.se/fileadmin/eit/courses/edi051/lecture_notes/LN8.pdf

Lecture, November 25

We will begin on protocols and zero-knowledge from the slides, Interactive proof systems are defined in section 21.1 of the textbook and zero-knowledge in section 21.2. Bit commitment from chapter 20 will also be discussed.

Lecture, December 2

We will finish protocols from the slides.

Problem session December 3

We will finish those problems not finished on November 26.

1. In an undirected graph $G = (V, E)$ where $|V| = n$, an ordered sequence of the vertices, $C = \langle v_{i_1}, v_{i_2}, \cdots, v_{i_n}, v_{i_{n+1}} \rangle$, is a Hamiltonian circuit if $v_{i_1} = v_{i_{n+1}}$, no other vertex in the sequence is the same as any other, and there is an edge $e = (v_{i_j}, v_{i_{j+1}}) \in E$ for $1 \leq j \leq n$. Thus, it is a cycle containing all vertices in the graph exactly once, and it is not necessary to list $v_{i_{n+1}}$, since it is always the first vertex. The Hamiltonian Circuit problem is to determine for a given graph if it has a Hamiltonian circuit. (This problem is NP-Complete.)

   Give a zero-knowledge proof for Hamiltonian Circuit. Thus, your input is an undirected graph, $G = (V, E)$, containing a Hamiltonian circuit, and the Prover should prove that G contains a Hamiltonian circuit. Assume that the Prover knows such a Hamiltonian circuit. Assume that the graph is given as an incidence matrix (the rows and columns are indexed by the vertices and there is 1 in the cell if the two vertices indexing that cell have an edge between them and 0 if not).

   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. Use Goldwasser-Micali bit commitments.

   Prove that your protocol has the following properties:

   - Completeness
   - Soundness
   - Zero-knowledge

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 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?

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. (Assume that you know a multiple of the order of α.)

4. 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.)