CS 120/ E-177: Introduction to Cryptography

Salil Vadhan and Alon Rosen Dec. 12, 2006

Lecture Notes 20:

Zero-Knowledge Proofs

Recommended Reading.

- Vadhan, *Interactive & Zero-Knowledge Proofs*, from IAS/PCMI Summer School on Computational Complexity, Secs 1.1, 1.2, 2.1, 2.2.
- Goldreich, Chapter 4 (up to 4.4)

1 Interactive Proofs

Motivation: transforming protocols secure against honest-but-curious adversaries into ones secure against malicious adversaries.

- Have parties 'prove' that they are following the protocol.
- How can this be done without leaking information (e.g. their input)?

1.1 "Classical" Proofs

Definition 1 *An* **NP** proof system *for membership in a language L is an algorithm V such that*

1. *(Completeness) If $x \in L$, then there exists proof s.t. $V(x, \mathit{proof}) =$* `accept`.
2. *(Soundness) If $x \notin L$, then for all proof*, $V(x, \mathit{proof}^*) =$* `reject`.
3. *(Efficiency) $V(x, \mathit{proof})$ runs in time* $\mathrm{poly}(\|x\|)$.

- **NP** proofs inherently provide more knowledge than $x \in L$.

1.2 Interactive Proofs

- Two new ingredients: interaction and randomization. Instead of having the proof be a "static" object, we have a dynamic prover who interacts with the verifier. The verifier V is probabilistic and is allowed to make a small error probability.
- Interactive (2-party) protocol: A pair of algorithms (A, B) taking input, history, and coin tosses to next message, e.g. $m_1 = A(x; r_A)$, $m_2 = B(x, m_1; r_B)$, $m_3 = A(x, m_1, m_2; r_A)$, ...

Definition 2 *An* interactive proof *for a language L is an interactive protocol (P, V) such that*

1. *(Completeness) If $x \in L$, then V accepts in $(P, V)(x)$ with probability at least* $2/3$.
2. *(Soundness) If $x \notin L$, then for all P^*, V accepts in $(P^*, V)(x)$ with probability at most* $1/3$.

3. *(Efficiency) The total computation time of V and total communication in $(P,V)(x)$ is at most* $\mathrm{poly}(\|x\|)$.

- Efficiency of honest prover P
  - Complexity theory: allow P to be computationally unbounded, and study the power of interactive proofs (**IP**) as compared to classical proofs (**NP**).
  - Cryptography: restrict to $L \in \mathbf{NP}$, require P to be polynomial time given an **NP** proof, and hope for additional properties not possible with **NP** proofs (namely, zero knowledge)
- Error probabilities can be made exponentially small by repetition as usual.

1.3 Quadratic Residuosity

- $L = \{(N, x) : x \in \mathrm{QR}(N)\}$.
- How can we prove that $x \in \mathrm{QR}(N)$ without revealing a square root of x?
- **Idea:** cut and choose
  - $x \in \mathrm{QR}(N) \Leftrightarrow \exists y \; y \in \mathrm{QR}(N) \wedge xy \in \mathrm{QR}(N)$
  - Prover 'cuts' by choosing random y, verifier 'chooses' which of the two statements should be proven.

Proof system for Quadratic Residuosity**, on common input** (N, x)**:**

1. P: Let q be such that $x = q^2 \bmod N$.
2. P: Choose $r \stackrel{\mathrm{R}}{\leftarrow} \mathbb{Z}_N^*$.
   Send $y = r^2 \bmod N$.
3. V: Choose and send $b \stackrel{\mathrm{R}}{\leftarrow} \{0, 1\}$.
4. P: If $b = 0$, let $s = r$.
   If $b = 1$, let $s = qr \bmod N$.
   Send s to V.
5. V: If $b = 0$, accept if $s^2 \equiv y \pmod N$.
   If $b = 1$, accept if $s^2 \equiv xy \pmod N$.

Proposition 3 *Above is an interactive proof for* Quadratic Residuosity.

Proof:

2 Zero-Knowledge Proofs

- Intuitively, verifier "learns nothing" in QR protocol: all verifier sees is s, a random string in $\mathbb{Z}_n^*$ and either $y = s^2$ or $y = s^2/x$.
- *Simulation paradigm*: verifier learns nothing if it can generate everything it sees on its own, without interacting with prover.

Definition 4 (P, V) *is* zero knowledge *if for every PPT V^*, there is a PPT S such that $S(x)$ is computationally indistinguishable from* $\mathsf{View}_{V^*}^{(P,V^*)}(x)$ *when $x \in L$.*

That is, for every PPT D, there is a negligible function ε such that for all $x \in L$,

$$|\Pr\left[D(\mathsf{View}_{V^*}^{(P,V^*)}(x)) = 1\right] - \Pr\left[D(S(x)) = 1\right]| \leq \varepsilon(\|x\|).$$

Theorem 5 *Above proof system for* Quadratic Residuosity *is (perfect) zero knowledge.*

Proof: $S(N, x)$:

1. Choose $s \xleftarrow{\text{R}} \mathbb{Z}_N^*$.
2. Choose $b \xleftarrow{\text{R}} \{0, 1\}$.
3. If $b = 0$, let $y = s^2 \bmod N$. If $b = 1$, let $y = s^2 \cdot x^{-1} \bmod N$.
4. If $V^*((N, x), y) \neq b$, try again (goto Step 1).
5. Else output (y, b, s).

■

Technical comment: in the definition of zero knowledge, we should also account for additional information about x possessed by the verifier (e.g. from a prior execution of the zero-knowledge proof or from a higher-level protocol in which the zero-knowledge proof is being used). This is done by giving an auxiliary input z to both V^* and S, and quantifying over all $x \in L$ and all z.