Cryptographic Protocols

Spring 2017

Lecture 1: Introduction, Interactive Proofs

Cryptographic Protocols

1. Interactive Proofs and Zero-Knowledge Protocols
   Proving without Showing
2. Secure Multi-Party Computation
   Computing without Knowing
3. Broadcast
   Agreeing without Trusting
4. Secure E-Voting
   no buzzword here . . .

Formal and Non-Formal Proofs

Non-Formal Proof

- Lemma: $\forall n, d \in \mathbb{N} : \exists a : a, a + d, \ldots, a + (n-1)d$ are prime
- Proof: Consider the hyperbolic plane ρ with zero-free points α . . .
- Verification: **???**

Formal Proof

- Class of statements: For given n, d: $\exists a : a, .., a+(n-1)d$ are prime
- Statement: (n, d), e.g. $(3, 12)$
  Read: For $n = 3$ and $d = 12$, there exists an a such that . . .
- Proof: a, e.g. 5
  Read: For $a = 5$, the numbers $a, .., a+(n-1)d$ are prime
- Verification: Given (n, d) and a, check that $a, .., a+(n-1)d$ are prime
  Read: Check that $5, 17, 29$ are prime

A Formal Proof System

Proof System for a Class of Statements

- A statement (from the class) is a string (over a finite alphabet).
- A semantics that defines which statements are true.
- A proof is a string.
- Verification algorithm: (statement, proof) $\rightarrow$ {accept, reject}.

Example: n is Non-Prime

- Statement: a number n (sequence of digits), e.g. „399800021".
- Proof: a factor f, e.g. „19997".
- Verification: Check whether f divides n.

Requirements for a Proof System

- **Soundness:** Only true statements have proofs.
- **Completeness:** Every true statement has a proof.
- ____

Proof System: Sudoku has Solution

Good Proof System

- Statement: 9-by-9 Matrix $\mathcal{Z}$ over $\{1, \ldots, 9, \perp\}$.
- Proof: 9-by-9 Matrix $\mathcal{X}$ over $\{1, \ldots, 9\}$.
- Verification:
  1) ______________________________
  2) ______________________________

						4		
2					1		5	
4	3		7	5		1		2
				7			6	
	5	3				2	4	
	4			1				
3		1		8	2		7	4
	2		9					5
		8						

Stupid Proof System

- Statement: 9-by-9 Matrix $\mathcal{Z}$ over $\{1, \ldots, 9, \perp\}$.
- Proof: "" (empty string)
- Verification: Travel through possible $\mathcal{X}$, check if $\mathcal{X}$ is solution for $\mathcal{Z}$.

$\rightarrow$ **This is not a proof!**

Two Types of Proofs

Proofs of Statements:

- Sudoku $\mathcal{Z}$ has a solution $\mathcal{X}$.
- z is a square modulo m, i.e. $\exists x : z = x^2 \pmod{m}$.
- The graphs $\mathcal{G}_0$ and $\mathcal{G}_1$ are isomorphic.
- The graphs $\mathcal{G}_0$ and $\mathcal{G}_1$ are non-isomorphic.

Proofs of Knowledge:

- I know a solution $\mathcal{X}$ of Sudoku $\mathcal{Z}$.
- I know a value x such that $z = x^2 \pmod{m}$.
- I know an isomorphism π from $\mathcal{G}_0$ to $\mathcal{G}_1$.
- I know a anti-isomorphism between $\mathcal{G}_0$ and $\mathcal{G}_1$????

Often: Proof of knowledge $\rightarrow$ Proof of statement (knowledge exists)

Static Proofs vs. Interactive Proofs

Static Proof

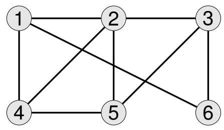
Prover P		**Verifier V**
knows statement s, proof p	$\xrightarrow{p}$	knows statement s $(s, p) \rightarrow$ {accept, reject}

Interactive Proof

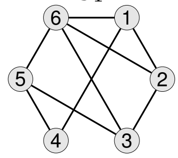
Prover P		**Verifier V**
knows statement s, proof p		knows statement s
	$\xrightarrow{m_1}$	
	$\xleftarrow{m_2}$	
	$\dots$	
	$\xrightarrow{m_\ell}$	$(s, m_1, \dots, m_\ell) \rightarrow$ {accept, reject}

The Graph Isomorphism (GI) Problem

$\mathcal{G}_0$



$\mathcal{G}_1$



$$\begin{bmatrix} 0&1&0&1&0&1\\ 1&0&1&1&1&0\\ 0&1&0&0&1&1\\ 1&1&0&0&1&0\\ 0&1&1&1&0&0\\ 1&0&1&0&0&0 \end{bmatrix} \qquad \begin{bmatrix} 0&1&0&1&0&1\\ 1&0&1&0&0&1\\ 0&1&0&0&1&1\\ 1&0&0&0&1&0\\ 0&0&1&1&0&1\\ 1&1&1&0&1&0 \end{bmatrix}$$

Graph Isomorphism – One Round of the Protocol

Setting: Given two graphs $\mathcal{G}_0$ and $\mathcal{G}_1$.
Goal: Prove that $\mathcal{G}_0$ and $\mathcal{G}_1$ are isomorphic.

Peggy		**Vic**
knows $\mathcal{G}_0$, $\mathcal{G}_1$, σ s.t. $\mathcal{G}_1 = \sigma\mathcal{G}_0\sigma^{-1}$		knows $\mathcal{G}_0$ and $\mathcal{G}_1$
pick random permutation π $\mathcal{T} = \pi\mathcal{G}_0\pi^{-1}$	$\xrightarrow{\mathcal{T}}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1\}$
$c = 0 : \rho = \pi$ $c = 1 : \rho = \pi\sigma^{-1}$	$\xrightarrow{\rho}$	$c = 0 : \mathcal{T} \stackrel{?}{=} \rho\mathcal{G}_0\rho^{-1}$ $c = 1 : \mathcal{T} \stackrel{?}{=} \rho\mathcal{G}_1\rho^{-1}$

Interactive Proofs: Requirements

- **Completeness:** If the statement is true [resp., the prover knows the claimed information], then the correct verifier will always accept the proof by the correct prover.
- **Soundness:** If the statement is false [resp., the prover does not know the claimed information], then the correct verifier will accept the proof only with negligible probability, independent of the prover's strategy.

Desired Property:

- **Zero-Knowledge:** As long as the prover follows the protocol, the verifier learns nothing but the fact that the statement is true [resp., that the prover knows the claimed information].

Graph-NON-Isomorphism – One Round of the Protocol

Setting: Given two graphs $\mathcal{G}_0$ and $\mathcal{G}_1$.
Goal: Prove that $\mathcal{G}_0$ and $\mathcal{G}_1$ are *not* isomorphic.

Peggy		**Vic**
knows $\mathcal{G}_0$ and $\mathcal{G}_1$		knows $\mathcal{G}_0$ and $\mathcal{G}_1$
	$\xleftarrow{\mathcal{T}}$	$b \in_R \{0, 1\}$, π at random $\mathcal{T} = \pi\mathcal{G}_b\pi^{-1}$
if $\mathcal{T} \sim \mathcal{G}_0$: $c = 0$, if $\mathcal{T} \sim \mathcal{G}_1$: $c = 1$	$\xrightarrow{c}$	$c \stackrel{?}{=} b$

Fiat-Shamir – One Round of the Protocol

Setting: m is an RSA-Modulus.
Goal: Prove knowledge of a square root of a given $z \in \mathbb{Z}_m^*$.

Peggy		**Vic**
knows x s.t. $x^2 = z \pmod m$		knows $z \in \mathbb{Z}_m^*$
$k \in_R \mathbb{Z}_m^*$, $t = k^2$	$\xrightarrow{t}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1\}$
$r = k \cdot x^c$	$\xrightarrow{r}$	$r^2 \stackrel{?}{=} t \cdot z^c$