Cryptographic Protocols

Spring 2020

Part 1

1. Interactive Proofs and Zero-Knowledge Protocols
2. Secure Multi-Party Computation
3. Broadcast
4. Blockchain

Broadcast / Byzantine Agreement

Theorem [LSP80]: Among n players, broadcast is achievable if and only if \( t < n/3 \) players are corrupted.

Secure Multi-Party Computation

Formal Proofs (Conventional)

Proof system for a class of statements
- A statement (from the class) is a string (over a finite alphabet).
- The semantics defines which statements are true.
- A proof is a string.
- Verification function \( \varphi \) : (statement, proof) \( \mapsto \) \{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.
- Efficient verifier: \( \varphi \) is efficiently computable.
### Two Types of Proofs

**Proofs of Statements:**
- Sudoku $Z$ has a solution $X$.
- $z$ is a square modulo $m$, i.e., $\exists x : x^2 \equiv z \pmod{m}$.
- The graphs $G_0$ and $G_1$ are isomorphic.
- The graphs $G_0$ and $G_1$ are non-isomorphic.
- $P = \text{NP}$

**Proofs of Knowledge:**
- I know a solution $X$ of Sudoku $Z$.
- I know a value $x$ such that $z = x^2 \pmod{m}$.
- I know an isomorphism $\pi$ from $G_0$ to $G_1$.
- I know a non-isomorphism between $G_0$ and $G_1$? ? ? ?
- I know a proof for either $P = \text{NP}$ or $P \neq \text{NP}$.
- I know $x$ such that $z = x^2$.

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

### Static Proofs vs. Interactive Proofs

**Static Proof**

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

**Interactive Proof**

- **Prover P** knows statement $s$.
- **Verifier V** knows statement $s$.
- **proof** $m_1, m_2, \ldots, m_l$ $\rightarrow$ $(s, m_1, \ldots, m_l) \rightarrow \{\text{accept}, \text{reject}\}$

**Motivation for IP’s:**
1. zero knowledge
2. more powerful
3. applications

### Interactive Proofs: Requirements (Informal)

- **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.

### The Graph Isomorphism (GI) Problem

**$G_0$**

```
0 1 0 1 0 1
1 0 1 1 0 1
1 1 0 0 1 1
0 1 1 1 1 0
1 0 1 0 0 1
1 0 0 1 0 1
```

**$G_1$**

```
0 1 0 1 0 1
1 0 1 0 0 1
0 1 0 0 1 0
0 1 1 1 0 1
1 1 1 0 1 0
```

**$G_1$** is isomorphic to $G_0$.
Graph Isomorphism – One Round of the Protocol

**Setting:** Given two graphs $G_0$ and $G_1$.

**Goal:** Prove that $G_0$ and $G_1$ are isomorphic.

**Peggy**

knows $G_0$, $G_1$, $\sigma$ s.t. $G_1 = \sigma G_0 \sigma^{-1}$

**Vic**

knows $G_0$ and $G_1$

pick random permutation $\pi$

$T = \pi G_0 \pi^{-1}$

$c \in \mathbb{R} \{0,1\}$

$c = 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$c = 0 : \mathcal{T} \equiv \rho G_0 \rho^{-1}$

c = 1 : $\mathcal{T} \equiv \rho \pi \sigma^{-1}$

Graph Isomorphism – One Round of the Protocol

**Setting:** Given two graphs $G_0$ and $G_1$.

**Goal:** Prove that $G_0$ and $G_1$ are isomorphic.

**Peggy**

knows $G_0$, $G_1$, $\sigma$ s.t. $G_1 = \sigma G_0 \sigma^{-1}$

**Vic**

knows $G_0$ and $G_1$

pick random permutation $\pi$

$T = \pi G_0 \pi^{-1}$

$c \in \mathbb{R} \{0,1\}$

$c = 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$c = 0 : \mathcal{T} \equiv \rho G_0 \rho^{-1}$

c = 1 : $\mathcal{T} \equiv \rho \pi \sigma^{-1}$

Graph-NON-Isomorphism – One Round of the Protocol

**Setting:** Given two graphs $G_0$ and $G_1$.

**Goal:** Prove that $G_0$ and $G_1$ are not isomorphic.

**Peggy**

knows $G_0$ and $G_1$

knows $G_0$ and $G_1$

pick random permutation $\pi$

$T = \pi G_b \pi^{-1}$

$c \in \mathbb{R} \{0,1\}$

$c = 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$c = 0 : \mathcal{T} \equiv \rho G_0 \rho^{-1}$

c = 1 : $\mathcal{T} \equiv \rho \pi \sigma^{-1}$

Fiat-Shamir – One Round of the Protocol

**Setting:** $m$ is an RSA-Modulus.

**Goal:** Prove knowledge of a square root $x$ of a given $z \in \mathbb{Z}_m^*$.

**Peggy**

knows $x$ s.t. $x^2 = z$ (mod $m$)

**Vic**

knows $z$

$k \in \mathbb{R} \mathbb{Z}_m^*$,

t = $k^2$

$c \in \mathbb{R} \{0,1\}$

$r = k \cdot x^c$

$c \neq 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$r \frac{1}{2} \rho \equiv t \cdot z^c$

Fiat-Shamir – One Round of the Protocol

**Setting:** $m$ is an RSA-Modulus.

**Goal:** Prove knowledge of a square root $x$ of a given $z \in \mathbb{Z}_m^*$.

**Peggy**

knows $x$ s.t. $x^2 = z$ (mod $m$)

**Vic**

knows $z$

$k \in \mathbb{R} \mathbb{Z}_m^*$,

t = $k^2$

$c \in \mathbb{R} \{0,1\}$

$r = k \cdot x^c$

$c \neq 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$r \frac{1}{2} \rho \equiv t \cdot z^c$

Guillou-Quisquater – One Round of the Protocol

**Setting:** $m$ is an RSA-Modulus.

**Goal:** Prove knowledge of an $e$-th root $x$ of a given $z \in \mathbb{Z}_m^*$.

**Peggy**

knows $x$ s.t. $x^e = z$ (mod $m$)

**Vic**

knows $z$

$k \in \mathbb{R} \mathbb{Z}_m^*$,

t = $k^e$

$c \in \mathbb{R} \{0,1\}$

$r = k \cdot x^c$

$c \neq 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$r \neq 0 : t^2 \equiv t \cdot z^c$

Guillou-Quisquater – One Round of the Protocol

**Setting:** $m$ is an RSA-Modulus.

**Goal:** Prove knowledge of an $e$-th root $x$ of a given $z \in \mathbb{Z}_m^*$.

**Peggy**

knows $x$ s.t. $x^e = z$ (mod $m$)

**Vic**

knows $z$

$k \in \mathbb{R} \mathbb{Z}_m^*$,

t = $k^e$

$c \in \mathbb{R} \{0,1\}$

$r = k \cdot x^c$

$c \neq 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$r \neq 0 : t^2 \equiv t \cdot z^c$

Schnorr – One Round of the Protocol

**Setting:** Cyclic group $H = \langle h \rangle$, $|H|$ = prime.

**Goal:** Prove knowledge of the discrete logarithm $x$ of a given $z \in H$.

**Peggy**

knows $x \in \mathbb{Z}_q$ s.t. $h^x = z$

**Vic**

knows $z$

$k \in \mathbb{R} \mathbb{Z}_q$,

t = $h^k$

$c \in \mathbb{R} C \subseteq \mathbb{Z}_q$

$r = k + xc$

$c \neq 0 : \rho = \pi$

c = 1 : $\rho = \pi \sigma^{-1}$

$r \neq 0 : h^r \equiv t \cdot z^c$

Schnorr – One Round of the Protocol

**Setting:** Cyclic group $H = \langle h \rangle$, $|H|$ = prime.

**Goal:** Prove knowledge of the discrete logarithm $x$ of a given $z \in H$.