CSCI 1515 Applied Cryptography

This Lecture:

- Case Study: Group Chat (Continued)
- Single Sign-On (SSO) Authentication
- Zero-Knowledge Proof
- Example: Diffie-Hellman Tuple
Secure Messaging

\[ AE_{k_{bs}}(AE_{gab}(m)) \]

Server

\[(V_{k_{s}}, S_{k_{s}}) \leftarrow \text{Gen}(1^n)\]

Public (X.509 certificate)

End-to-end encryption

Alice

Bob

\[ g_{ab} \]

\[ g_{ab} \]
Group Chat?

Server

(public (X.509 certificate) → (VKs, SKs) ← Gen(1^))

- m revealed to server?
- group structure revealed to server?
- same key / different keys?

Alice

Signup → Login

Bob

Charlie

How would you design it?
Figure 5. Schematic depiction of traffic, generated for a message $m$ from sender $A$ to receivers $B, C$ in group $gr$ with $\mathcal{G}_{gr} = \{A, B, C\}$ in WhatsApp.
Figure 3. Schematic depiction of Signal’s traffic, generated for a message $m$ from sender $A$ to receivers $B$ and $C$ in group $gr$ with $\mathcal{G}_{gr} = \{A, B, C\}$. Transport layer protection is not in the analysis scope (gray).
Single Sign-On (SSO) Authentication

User

Password-Based Authentication

Server

Request "token"

"token" (Signature / MAC)

MAC

Signature

Service Provider

"token"

OAuth/OpenID: Sign-in with Google/Apple/...

Kerberos: enterprises
Zero-Knowledge Proofs

Prover

Verifier

Coca-Cola & Pepsi taste differently

There is a bug in your code

I have the secret key for this ciphertext

What is a proof?

What does zero-knowledge mean?
What is a "proof system"?

Statement:  

proof:  

- Completeness: If statement is true, then $\exists$ proof that proves it's true.
- Soundness: If statement is false, then $\forall$ proof can't prove it's true.
NP as a Proof System

Ex: Graph 3-coloring

NP language \( L = \{ G : G \text{ has 3-coloring} \} \)

NP relation \( R_L = \{ (G, 3\text{COL}) \} \)

Statement: graph \( G \)

Proof: 3-coloring of \( G \): \( 3\text{COL} \)

\((G, 3\text{COL}) \in R_L\)
NP as a Proof System

A language $L$ is in NP if $\exists$ poly-time $V$ s.t.

- **Completeness:** $\forall x \in L$, $\exists w$ s.t. $V(x, w) = 1$

- **Soundness:** $\forall x \notin L$, $\forall w^*$, $V(x, w^*) = 0$

Diagram:

```
Prover  Verifier
\( (x, w) \)  \( w \)  \( x \)
```
Zero-Knowledge Proof (ZKP)

Let \( (P, V) \) be a pair of probabilistic poly-time (PPT) interactive machines. \( (P, V) \) is a zero-knowledge proof system for a language \( L \) with associated relation \( R_L \) if

- **Completeness**: \( \forall (x, w) \in R_L, \ \Pr [ P(x, w) \leftrightarrow V(x) \text{ outputs 1}] = 1 \).  
- **Soundness**: \( \forall x \in L, \forall (PPT) P^*, \ \Pr [ P^*(x) \leftrightarrow V(x) \text{ outputs 1}] \approx 0 \).

**Zero-Knowledge?**

*argument*
Zero-Knowledge Proof (ZKP)

Simulator

Verifier*

Zero-knowledge: \[ \forall PPT V^*, \exists PPT S \text{ s.t. } \forall (x,w) \in R_L, \]
\[ \text{Output}_{x}[P(x,w) \leftrightarrow V^*(x)] \approx S(x) \]
Example: Diffie-Hellman Tuple

Input: Cyclic group $G$ of order $q$, generator $g$, $h$, $u$, $v$

Witness: $b$

Statement: $\exists b \in \mathbb{Z}_q$ s.t. $u = g^b$ \& $v = h^b$

Prover

$r \leftarrow \mathbb{Z}_q$

$A := g^r$, $B := h^r$

$S := 6 \cdot b + r \pmod{q}$

Completeness? $6 \leftarrow \{0, 1\}$

Verifier

If $6 = 0 \Rightarrow S = r \Rightarrow$ Verify $A = g^S$, $B = h^S$

If $6 = 1 \Rightarrow S = b + r \Rightarrow u \cdot A = g^S$, $v \cdot B = h^S$
Soundness? \((g, h, u, v) \& L\)

\[
g^a \quad g^b \quad g^c
g^a \quad g^b \quad g^c
\]

\(\forall x \in L, \forall P^*, \Pr[P^*(x) \leftrightarrow V(x) \text{ outputs } 1] \approx 0\).

\[\forall x \in L, \forall P^*, \Pr[P^*(x) \leftrightarrow V(x) \text{ outputs } 1] \approx 0.\]

Prover*

\[r \in \mathbb{Z}_q\]

\[A := g^r, B := h^r\]

\[S := b \cdot r \pmod{q}\]

Verifier

\[\sigma \in \{0, 1\}\]

\[\lambda \text{ times}\]

\[\text{If } \sigma = 0 \Rightarrow S = r \Rightarrow \text{Verify } A = g^S, B = h^S\]

\[\text{If } \sigma = 1 \Rightarrow S = b + r \Rightarrow u \cdot A = g^S, v \cdot B = h^S\]

1. \(A = g^r, B = h^r\) valid

   \(\text{If } \sigma = 1 \Rightarrow \text{caught}\)

   \(s \text{ s.t. } u \cdot g^r = g^s\)

   \(v \cdot h^r = h^s\)

   \(u = g^{s-r}\)

   \(v = h^{s-r}\)

   \(b = s - r\)

   **Does Not Exist!**

2. \(A = g^{r_1}, B = h^{r_2}\) invalid

   \(r_1 \neq r_2\)

   \(\text{If } \sigma = 0 \Rightarrow \text{caught}\)
Zero-Knowledge?

\[ \forall \text{PPT } V^*, \exists \text{PPT } S \text{ s.t. } A(x,w) \in \mathbb{R}_L, \]

\[ \text{Output}_{V^*}[P(x,w) \leftrightarrow V^*(x)] \approx S(x) \]

**Simulator**

- \( r \leftarrow \mathbb{Z}_q \)
- **Prepare** \( A, B \)
  \[ A := g^r, \quad B := h^r \]
- **Rewind**

**Verifier**

- \( \delta \leftarrow \{0, 1\} \)
- If \( \delta = 0 \):
  - Proceed
- If \( \delta = 1 \):
  - \( S := \delta \cdot b + r \mod q \)

**Parallel Repetition**

\( \delta_1, \ldots, \delta_{2^\lambda} \)

\[ \Pr[\delta_1 = \delta_1', \ldots, \delta_{2^\lambda} = \delta_{2^\lambda}'] = (\frac{1}{2})^{2^\lambda} \]

**NOT ZK!**