This Lecture:

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

$AE_{k_{bs}}(AE_{gab}(m))$

Server

$\text{public (X.509 certificate)}$

$(V_{K_{s}}, S_{K_{s}}) \leftarrow \text{Gen}(1^\lambda)$

$AE_{gab}(m)$

$AE_{k_{bs}}(AE_{gab}(m))$

$AE_{k_{bs}}(g^{a})$

$AE_{k_{bs}}(g^{b})$

$g^{ab}$

Alice

Bob

End-to-end encryption
Group Chat?

Server

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

VKs, SKs ← Gen(1^n)

public (X.509 certificate)

Alice

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 $G_{gr} = \{A, B, C\}$ 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)

Service Provider

- 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: 

[Blank]
NP as a Proof System

Ex: Graph 3-coloring

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

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

Statement: graph \( G \)

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

\((G, \text{3CO}_L) \in R_L\)
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. $V(x, w) = 1$ (Witness)

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

Prover $\rightarrow$ Verifier

$(x, w)$
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**: \(\forall x \notin L, \forall (PPT) \: P^*, \Pr [P^*(x) \leftrightarrow V(x) \text{ outputs } 1] \approx 0\).

**Zero-Knowledge?**
**Zero-Knowledge Proof (ZKP)**

Zero-Knowledge: \[
\forall \text{PPPT } V^*, \exists \text{PPPT } S \text{ s.t. } \forall (x, w) \in R_L, \]

\[
\text{Output}_{S}[P(x, w) \rightarrow V^*(x)] \approx S(x)
\]
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. $u = g^b \land v = h^b$

<table>
<thead>
<tr>
<th>Prover</th>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r \in \mathbb{Z}_q$</td>
<td>$r \in {0, 1}$</td>
</tr>
<tr>
<td>$A := g^r$, $B := h^r$</td>
<td></td>
</tr>
<tr>
<td>$s := 6 \cdot b + r \pmod{q}$</td>
<td></td>
</tr>
</tbody>
</table>

If $6 = 0 \Rightarrow s = r \Rightarrow$

If $6 = 1 \Rightarrow s = b + r \Rightarrow$
Soundness? \((g, h, u, v) \& L\)

\[
\begin{align*}
&\forall x \& L, \forall p^*, \Pr[p^*(x) \leftrightarrow V(x) \text{ outputs 1}] \approx 0.
\end{align*}
\]

**Prover**

- \(r \leftarrow \$ Z_q\)
- \(A := g^r, B := h^r\)
- \(S := 6 \cdot b + r \mod q\)

**Verifier**

- \(c \leftarrow \$ \{0, 1\}\)
Zero-Knowledge?

\[ \forall \text{PPT } V^*, \exists \text{PPT } S \text{ s.t. } A(x,w) \in R_l, \]
\[ \text{Output}_{V^*}[P(x,w) \leftrightarrow V^*(x)] \approx S(x) \]

<table>
<thead>
<tr>
<th>Simulator</th>
<th>Verifier*</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r \in \mathbb{Z}_q )</td>
<td>( A := g^r, \ B := h^r )</td>
</tr>
<tr>
<td></td>
<td>( 6 \in \mathbb{Z}_q )</td>
</tr>
<tr>
<td></td>
<td>( S := 6 \cdot b + r \mod q )</td>
</tr>
</tbody>
</table>
Proof of Knowledge (Pok)

\[ \text{Prover} \quad \begin{array}{c}
\text{Verifier} \\
\bigcirc \\
\begin{array}{c} \text{A} \\
(\text{x, w}) \\
\end{array} \\
\end{array} \]

Soundness: \forall x \in \mathbb{L}, \forall (\text{ppt}) p^*, \Pr [ p^*(x) \xrightarrow{\text{x}} V(x) \text{ outputs 1} ] \approx 0.

\[ R = \{(h=g^x, x)\} \]

\[ \forall x, x \in \mathbb{L} \]
Proof of Knowledge (Pok)

\[ \text{Proof of Knowledge: } \exists \text{PPTE } E \text{ s.t. } \forall \text{PPTE } p^*, \forall x \in L, \]
\[ \Pr[E^{p^*}(x) \text{ outputs } w \text{ s.t. } (x,w) \in L] \approx \Pr[p^* \leftrightarrow V(x) \text{ outputs 1}] . \]
Proof of Knowledge? \((g, h, u, v) \in L\)