CRYPTOGRAPHIC PROTOCOLS
2016, LECTURE 3

Key Exchange, CDH, DDH

Helger Lipmaa
University of Tartu, Estonia
UP TO NOW

- Basic intro
- Basic algebra
- Exponentiation
- Assumptions
- Algebra + assumptions: DL
- How to define assumptions (DL)
WHAT CAN BE DONE WITH DL?

- First idea:
  - let $s \leftarrow \mathbb{Z}_q$ be secret key and $h \leftarrow g^s$ be public key
  - computation of $s$ from $h$ is infeasible
  
- Use the keys to "encrypt", "sign", etc

- This lecture: more details
I want to send secret information to Bob, but he is in Jamaica.

Let us agree on a joint secret key for further communication.
KEY EXCHANGE

Asymmetric, public key

Asymmetric, public key

\[ \text{sk}_a, \text{pk}_a \]

\[ \text{sk}_b, \text{pk}_b \]

\[ \text{pk}_a \]

\[ \text{pk}_b \]

\[ \text{sk} \leftarrow \text{SK}(\text{sk}_a, \text{pk}_b) \]

\[ \text{sk} \leftarrow \text{SK}(\text{sk}_b, \text{pk}_a) \]

\[ \text{sk} \]

Symmetric, shared key
KEY EXCHANGE WITH DL

\[ s, h_A \leftarrow g^s \]

\[ t, h_B \leftarrow g^t \]

\[ h_A \]

\[ h_B \]

\[ sk \leftarrow SK(s, h_B) \]

\[ = \]

\[ sk \leftarrow SK(t, h_A) \]
Quiz

- $SK(t, g^s) = sk = SK(s, g^t)$
- What could $SK$ be?
- **Hint:** we are working in a group
  - Use commutativity + efficient operations
- **Answer:** $SK(s, h) = h^s$
  - $SK(t, g^s) = g^{st} = g^{ts} = SK(s, g^t)$
DIFFIE-HELLMAN KEY EXCHANGE

$s, h_A \leftarrow g^s$

$h_A$

$h_B \leftarrow g^t$

$sk = g^{st}$

$sk = g^{st}$
**DHKE: FORMALLY**

### DHKE.Setup ($\kappa$):
1. Choose a group $G$ of order $q$ where breaking DL has complexity $2^\kappa$
2. Choose a generator $g$ of $G$
3. Return $g^k \leftarrow \text{desc} (G) = (... , q, g)$

### DHKE.Keygen ($g^k$):
1. $sk = s \leftarrow \mathbb{Z}_q$
2. $pk \leftarrow g^s$
3. Return $(sk, pk)$

### DHKE.SK ($g^k, s, h$):
1. Return $h^s$
QUIZ: IS DHKE SECURE?

✧ Correct question:

✧ is DHKE what-secure under X assumption?

✧ Three tasks:

1. Formulate security of KE
2. Decide on X
3. Provide a proof by reduction (X holds => DHKE what-secure)
We already saw some issues in the last lecture

...so we won't concentrate on the same issues

Random key, probabilistic algorithms, ...
DHKE: INTUITIVE SECURITY

\[ s, h_A \leftarrow g^s \]

\[ t, h_B \leftarrow g^t \]

\[ sk = g^{st} \]

\[ sk = g^{st} \]
KEY RECOVERY SECURITY

- Three algorithms $KE = (\text{Setup}, \text{Keygen}, \text{SK})$


- $\mathcal{A}$ $\varepsilon$-breaks KR (key recovery) security of $KE$ iff $\text{Adv}[KR] \geq \varepsilon$

- $KE$ is $(\tau, \varepsilon)$-KR secure iff no adversary $\varepsilon$-breaks KR security of $KE$ in time $\leq \tau$

- $KE$ is KR secure iff it is $(\text{poly}(\kappa), \text{negl}(\kappa))$-KR secure

Game $KR(1^\kappa, KE, \mathcal{A})$

\begin{align*}
gk &\leftarrow \text{Setup}(1^\kappa) \\
(sk_a, pk_a) &\leftarrow \text{Keygen}(gk) \\
(sk_b, pk_b) &\leftarrow \text{Keygen}(gk) \\
\mathcal{A} &\leftarrow (gk, pk_a, pk_b) \\
\text{sk}^* &\leftarrow \mathcal{A}(gk, pk_a, pk_b) \\
\text{If } \text{sk}^* = \text{SK}(gk, sk_a, pk_b) \\text{ return } 1 \\
\text{else } \\
\text{return } 0
\end{align*}
security reduction?

- We would like to prove that DHKE is KR secure
- by reducing KR-security to DL assumption
- Unfortunately not known how to do it
NEW ASSUMPTION: CDH

- DHKE was proposed together with the idea of public-key cryptography by Diffie and Hellman in 1976
- No success in breaking it in *any reasonable* group where DL is hard
- Seems logical: introduce a tautological assumption
  - CDH: Computational Diffie-Hellman
  - "key recovery attack against DHKE is hard"
DEF: CDH ASSUMPTION

- Use (DHKE.Setup, DHKE.Keygen, DHKE.SK)
- \( \text{Adv}[\text{CDH}] := | \Pr[\text{CDH} = 1] - 1 / q | \)
- \( \forall \varepsilon\)-breaks CDH in group \( G \) iff \( \text{Adv}[\text{CDH}] \geq \varepsilon \)
- \( G \) is \((\tau,\varepsilon)\)-CDH group iff no adversary \( \varepsilon \)-breaks CDH in \( G \) in time \( \leq \tau \)
- \( G \) is CDH group iff it is \((\text{poly}(\kappa),\text{negl}(\kappa))\)-CDH group

Game CDH\((1^{\kappa}, KE, A)\)

\( gk \leftarrow \text{Setup}(1^{\kappa}) \)
(\( sk_a, pk_a \)←Keygen (gk)
(\( sk_b, pk_b \)←Keygen (gk)
\( sk^* \leftarrow A (gk, pk_a, pk_b) \)
If \( sk^* = \text{SK} (gk, sk_a, pk_b) \)
\quad return 1
else
\quad return 0
Remarks

- Clearly, CDH is secure in a group iff DHKE is KR secure in the same group.
- \( \tau = \tau(\kappa) \) and \( \epsilon = \epsilon(\kappa) \) are functions of \( \kappa \).
QUIZ: CDH VS DL
QUIZ: CDH VS DL

CDH hard

Answer: yes

DL hard

some contrived groups where DL holds but not CDH, ...

Answer: depends
PROOF: CDH => DL

**Theorem.** If $G$ is a $(\tau + \text{small}, (1 - 1/q) \varepsilon + (1 - 1/q)/q)$-CDH group, then it is also a $(\tau, \varepsilon)$-DL group.

**Proof idea.** Reduction to absurd: we show that if DL is easy in $G$, then CDH must also be easy in $G$.

- DL is easy => there exists an adversary $D$ that breaks DL

- We show CDH is easy by constructing an adversary $C$ that breaks CDH

- $C$ can use help from adversary $D$, by sending inputs to $D$ and receiving outputs

Typical reduction
INTUITIVE PROOF

- Assume \( \mathcal{D} \) can break DL
  - given \( g^s \), outputs \( s \) with probability \( \varepsilon \)
- Construct adversary \( \mathcal{C} \) that breaks CDH
  - given \( g^s, g^t \), call \( \mathcal{D} \) to compute \( s \leftarrow \mathcal{D}(g^s) \)
  - return \( (g^t)^s = g^{st} \)
SECURITY GAMES

CDH game: need to construct $C$

A challenger generates values from some fixed "valid" distributions and sends them to the adversary $C$

Depending on the input and the output, the challenger declares $C$ to be either successful or not

After some computation, $C$ returns some value to the challenger

DL game: $D$ is given

A challenger generates values from some fixed "valid" distributions and sends them to the adversary $D$

After some computation, $D$ returns some value to the challenger

Depending on the input and the output, the challenger declares $D$ to be either successful or not

This is the only thing we know...
SECURITY REDUCTION

CDH game: need to construct $C$

A challenger generates values from some fixed "valid" distributions and sends them to the adversary $C$.

Depending on the input and the output, the challenger declares $C$ to be either successful or not.

After some computation, $C$ returns some value to the challenger.

DL game: $D$ is given

$C$ or generates values from some fixed "valid" distributions and sends them to the adversary $D$.

After some computation, $D$ returns some value to the challenger $C$. 

$C$
REDUCTION: CDH => DL

\[ s, t \leftarrow \mathbb{Z}_q; h_A \leftarrow g^s; h_B \leftarrow g^t \]

\((\text{desc}(G), h_A, h_B)\) remove 1 elem.

\((\text{desc}(G), h_A)\)

\(*;/* compute m */*

if \(h_A = g^m\)

return \(sk^* \leftarrow f^m\)

else

return \(sk^* \leftarrow \mathbb{Z}_q\)

if \(sk^* = g^{st}\)

return 1

else

return 0

Challenger

 Exists

 Need to construct

 Exists

\(\mathbb{G}\)

\(D\)
ABOUT SUCCESS PROBABILITY

- Weird expression due to “else return sk* ← ℤ_q”
- Will not analyse (see slides of 2015 if interested)
**QUIZ: ARE WE DONE?**

- If not, why not?
- Is the achieved security sufficient?

**Answer:**

- The fact that $sk$ is unknown is not sufficient
- Adversary should have **no** information about $sk$
DHKE IN WILD WORLD

One-time pad

\[ s, h_A \leftarrow g^s \]

\[ t, h_B \leftarrow g^t \]

\[ sk = g^{st} \]

\[ m \xrightarrow{\text{XOR}} c \]

Any information about \( sk \) leaks information about \( m \)
DHKE: IND SECURITY

Intuition: if Eve has any information about sk, she should be able to distinguish real sk from random.

\[ s, h_A \leftarrow g^s \]

\[ t, h_B \leftarrow g^t \]

\[ s, h_A \leftarrow g^s \]

\[ t, h_B \leftarrow g^t \]

\[ s, h_A \leftarrow g^s \]

\[ t, h_B \leftarrow g^t \]

is it sk or garbage?

\[ sk = g^{st} \]

\[ = sk \]

\[ sk = g^{st} \]
\[ KE = (\text{Setup}, \text{Keygen}, \text{SK}) \]

\[ \text{Adv}[\text{IND}] := 2 \cdot | \Pr[\text{IND} = 1] - \frac{1}{2} | \]

\[ \forall \varepsilon \text{-breaks IND security of } KE \text{ iff } \text{Adv}[\text{IND}] \geq \varepsilon \]

\[ KE \text{ is } (\tau,\varepsilon)\text{-IND secure} \text{ iff no adversary } \varepsilon \text{-breaks IND security of } KE \text{ in time } \leq \tau \]

\[ KE \text{ is IND secure} \text{ iff it is } (\text{poly}(\kappa),\negl(\kappa))\text{-IND secure} \]
SECURITY REDUCTION?

- We would like to prove that DHKE is IND secure
  - by reducing IND security to CDH assumption
- Not possible
  - well-known groups where CDH holds but DHKE is not IND secure
We introduce again a tautological assumption, **DDH**

- **Decisional Diffie-Hellman**, known since 70s => good
- ...in many groups

- DDH is extremely useful in many protocols

- Well-known groups where DDH does not hold

- **pairing-based groups**: CDH conjectured to be hard, but DDH trivially breakable

- Interestingly, pairing-based groups are also extremely useful
DEF: DDH SECURITY

- Use (DHKE.Setup, DHKE.Keygen, DHKE.SK)
- Assume that for any $\kappa$, Setup picks exactly one group $G = G(\kappa)$
- $\text{Adv}[\text{DDH}] := 2 \cdot | \Pr[\text{DDH} = 1] - 1/2 |$
- $\mathcal{A}$ $\epsilon$-breaks DDH in $G$ iff $\text{Adv}[\text{DDH}] \geq \epsilon$
- $G$ is a $(\tau, \epsilon)$-DDH group iff no PPT adversary $\mathcal{A}$ $\epsilon$-breaks DDH in $G$ in time $\leq \tau$
- $G$ is a DDH group iff it is $(\text{poly}(\kappa), \text{negl}(\kappa))$-DDH group

Game DDH$(\mathbb{G}_\kappa, G, \mathcal{A})$

- $g_k \leftarrow \text{Setup}(\mathbb{G}_\kappa)$
- $(sk_a, pk_a) \leftarrow \text{Keygen}(g_k)$
- $(sk_b, pk_b) \leftarrow \text{Keygen}(g_k)$
- $sk_0 \leftarrow \text{SK}(g_k, sk_a, pk_b)$
- $sk_1 \leftarrow G$
- $\beta \leftarrow \{0, 1\}$
- $\beta^* \leftarrow \mathcal{A}(g_k, pk_a, pk_b, sk_\beta)$
- Return $\beta = \beta^* ? 1 : 0$
DDH: SHORT FORM

- Fix a cyclic group $G$ and its generator $g$
- Adversary has to distinguish between
  - $(g, g^s, g^t, g^{st})$ -- DDH tuple
  - $(g, g^s, g^t, g^m)$ -- random tuple
- where $s, t, m$ are random
DDH VS IND SECURITY

- Clearly, $G$ is a DDH group iff DHKE is IND secure in $G$

- (tautology)
THEOREM. If $G$ is a $(\approx \tau, \approx \varepsilon)$-DDH group, then it is also a $(\tau, \varepsilon)$-CDH group.

PROOF IDEA. Reduction to absurd: we show that if CDH is easy in $G$, then DDH must also be easy in $G$.

- CDH is easy $\Rightarrow$ there exists an adversary $D$ that breaks CDH

- We show DDH is easy by constructing an adversary $C$ that breaks DDH

- $C$ can use help from adversary $D$, by sending inputs to $D$ and receiving outputs

HOME EXERCISE: Very similar to previous proof. Finish! Find parameters
BEYOND IND: SEMIHONEST VS MALICIOUS

- Actual security requirements even more stringent
  - KR, IND security only demonstrate basic concepts
- We assumed Eve is semihonest
  - Eavesdrops but does not change messages
- Malicious Eve: can change, inject, delete messages
- Alice and Bob need to authenticate each other
- "Authenticated Diffie-Hellman"

Crucial notions

Security of various protocols against malicious adversaries: second half of the course
WHAT NEXT?

- DDH is a very versatile assumption
- One can construct many useful protocols from it
WHAT NEXT?

- Since many protocols are based on homomorphic encryption, the next lecture is about homomorphic encryption.

- More precisely: Elgamal encryption.
STUDY OUTCOMES

- Key exchange
- DHKE in particular
- KR security and CDH
- IND security and DDH
- Reductions: how to do