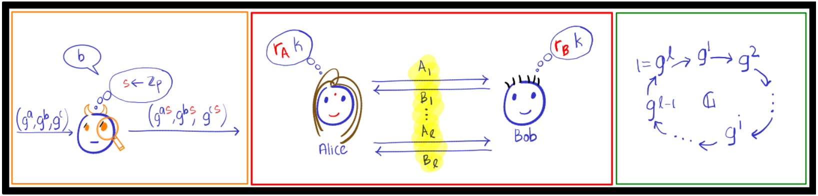
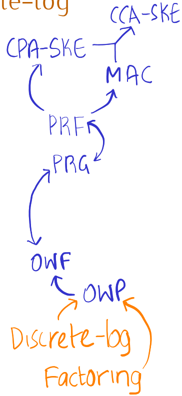


CS783: Theoretical Foundations of Cryptography

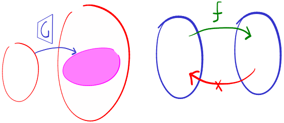
Lecture 8 (23/Aug/24)

Instructor: Chethan Kamath

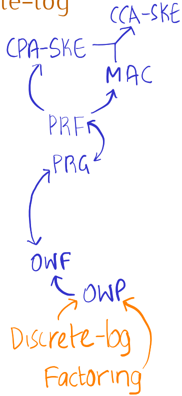
- We learnt: secure communication in the shared-key setting
- Primitives encountered: PRG, PRF, OWF, OWP, PI hash, MAC
- Computational hardness assumptions: factoring, discrete-log



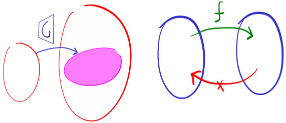
- We learnt: secure communication in the shared-key setting
- Primitives encountered: PRG, PRF, OWF, OWP, PI hash, MAC
- Computational hardness assumptions: factoring, discrete-log
- Key conceptual takeaways:
  - Computational security
  - Pseudo-randomness ↔ hardness ↔ unpredictability



$$x \to x^2 \to x^{2^2} \to x^{2^3} \to \cdots$$
$$b_1 \quad b_2 \quad b_3$$



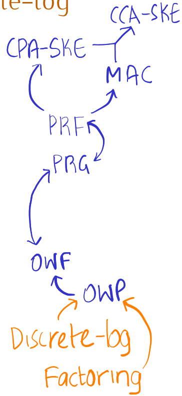
- We learnt: secure communication in the shared-key setting
- Primitives encountered: PRG, PRF, OWF, OWP, PI hash, MAC
- Computational hardness assumptions: factoring, discrete-log
- Key conceptual takeaways:
  - Computational security
  - Pseudo-randomness ↔ hardness ↔ unpredictability



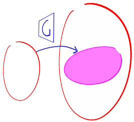
$x \to x^2 \to x^{2^2} \to x^{2^3} \to \cdots$

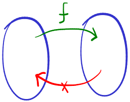
$b_1 \quad b_2 \quad b_3$

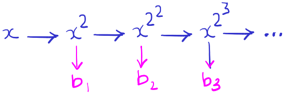
- Key tools: security reduction, hybrid argument

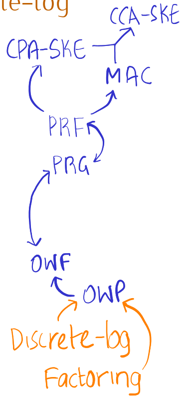


- We learnt: secure communication in the shared-key setting
- Primitives encountered: PRG, PRF, OWF, OWP, PI hash, MAC
- Computational hardness assumptions: factoring, discrete-log
- Key conceptual takeaways:
    - Computational security
    - Pseudo-randomness $\leftrightarrow$ hardness $\leftrightarrow$ unpredictability

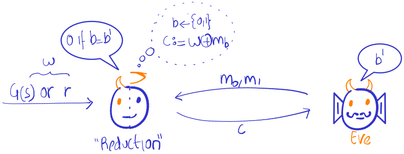


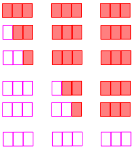






- Key tools: security reduction, hybrid argument

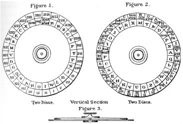


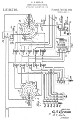


MODULE I

(Shared keys)

For a large part of history



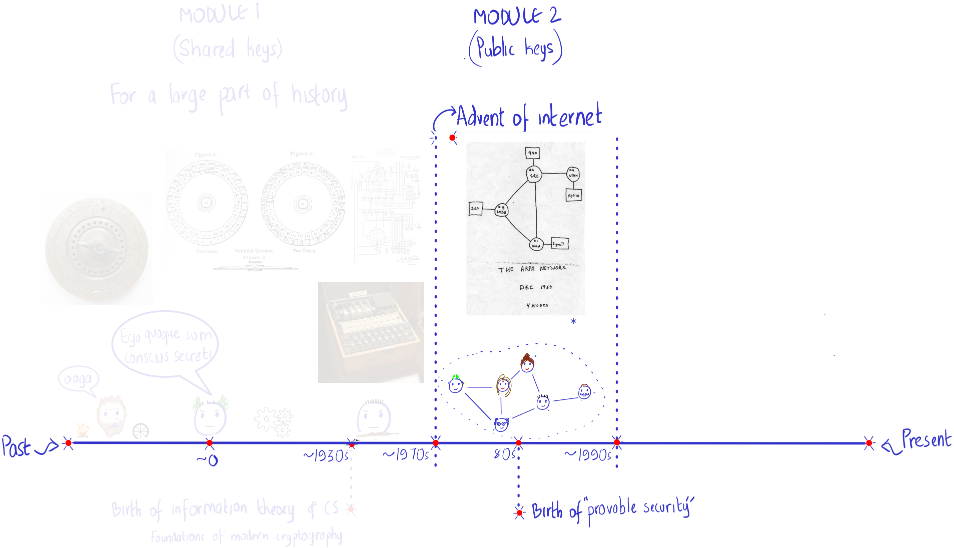


Birth of information theory & CS

Foundations of modern cryptography

Credit for images: Wikipedia (*User:DARPA)

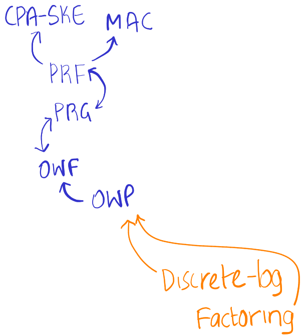
This Module...



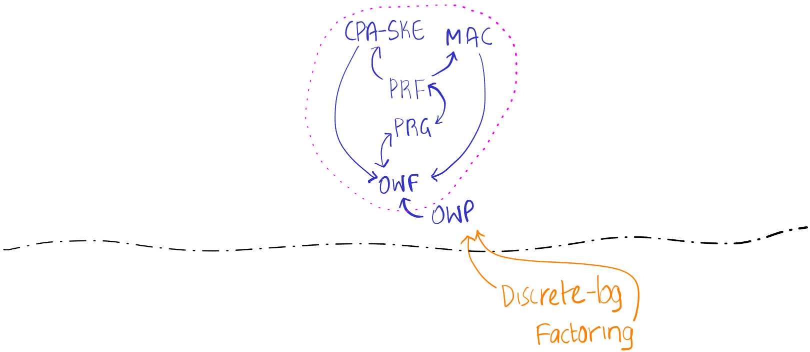
Credit for images: Wikipedia (*User:DARPA)

This Module...

- Minicrypt to Cryptomania

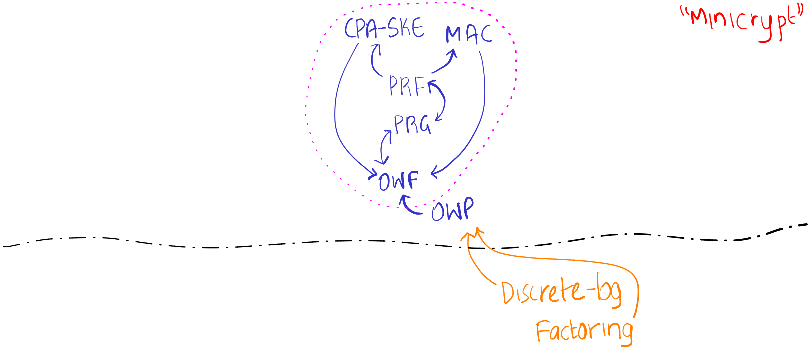


- Minicrypt to Cryptomania



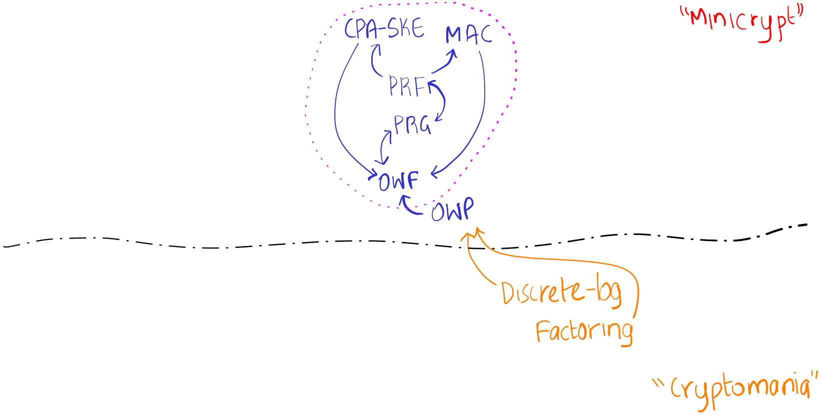
This Module...

- Minicrypt to Cryptomania

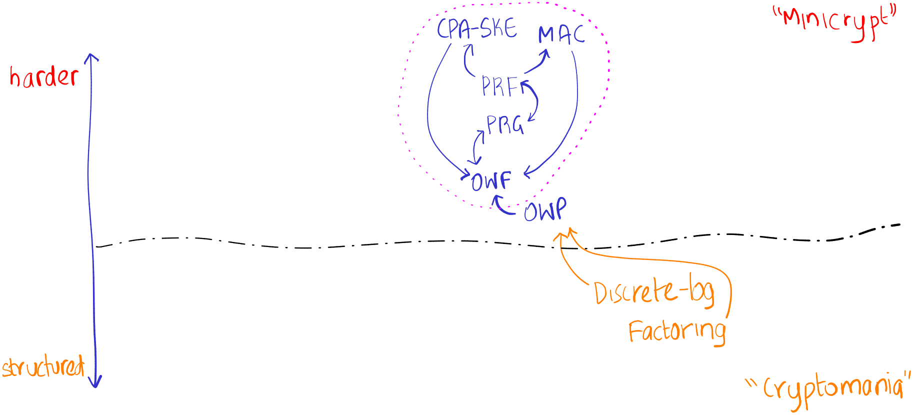


This Module...

- Minicrypt to Cryptomania

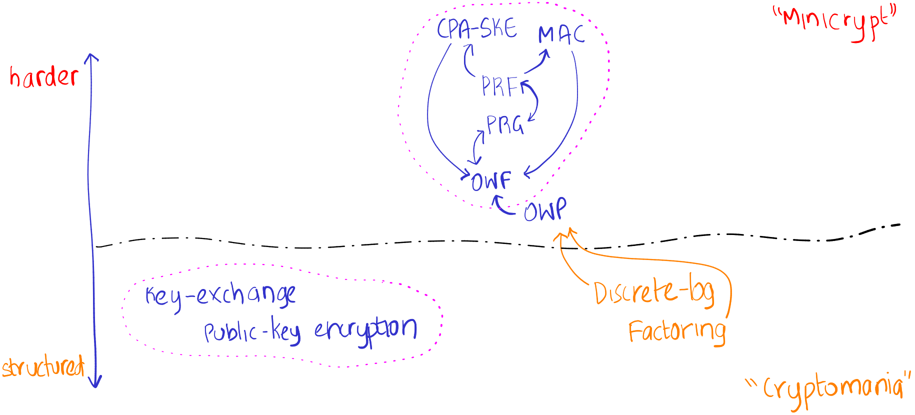


- Minicrypt to Cryptomania

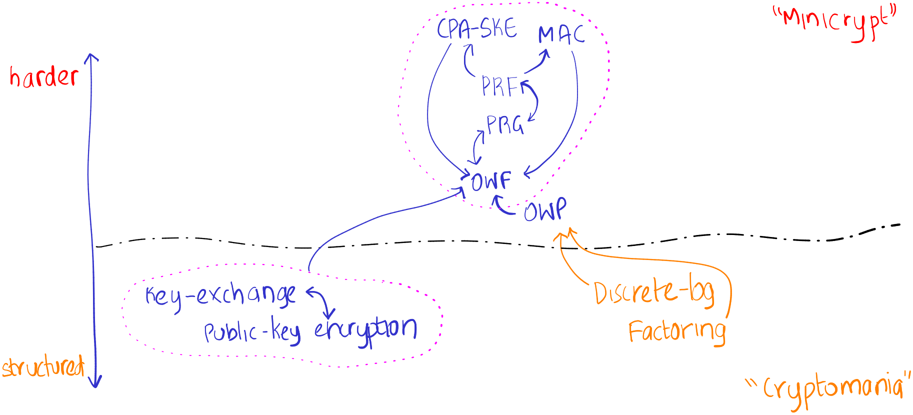


This Module...

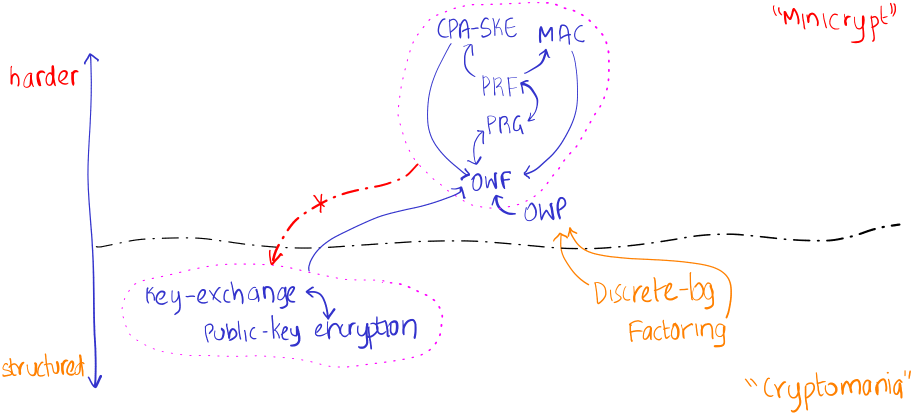
- Minicrypt to Cryptomania



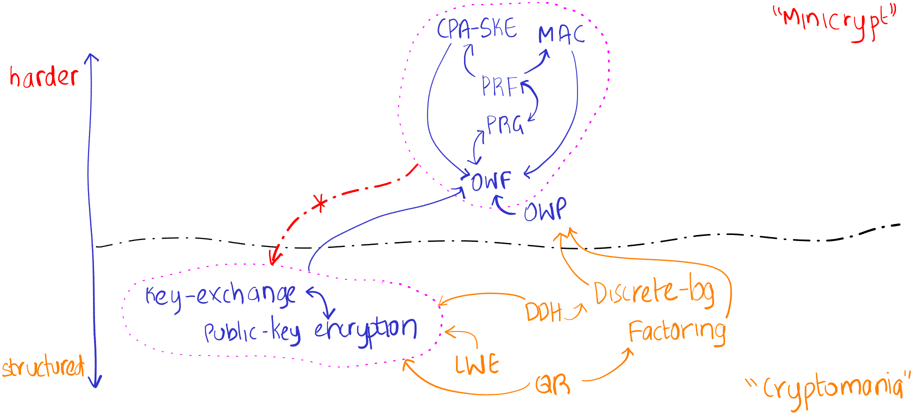
- Minicrypt to Cryptomania



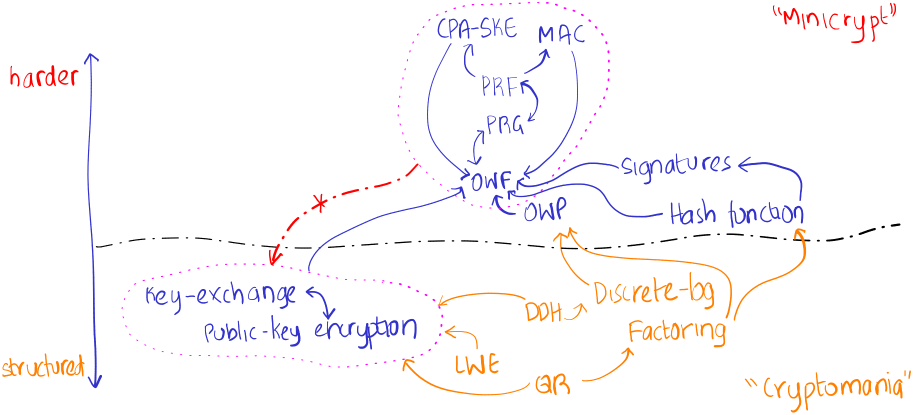
- Minicrypt to Cryptomania



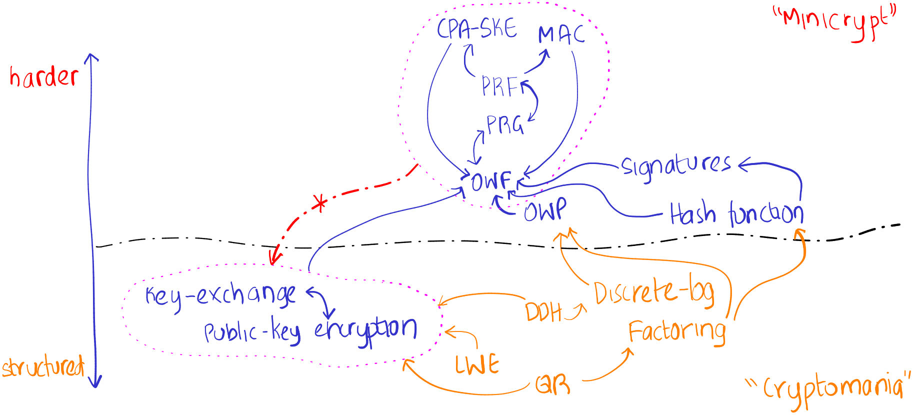
- Minicrypt to Cryptomania



- Minicrypt to Cryptomania

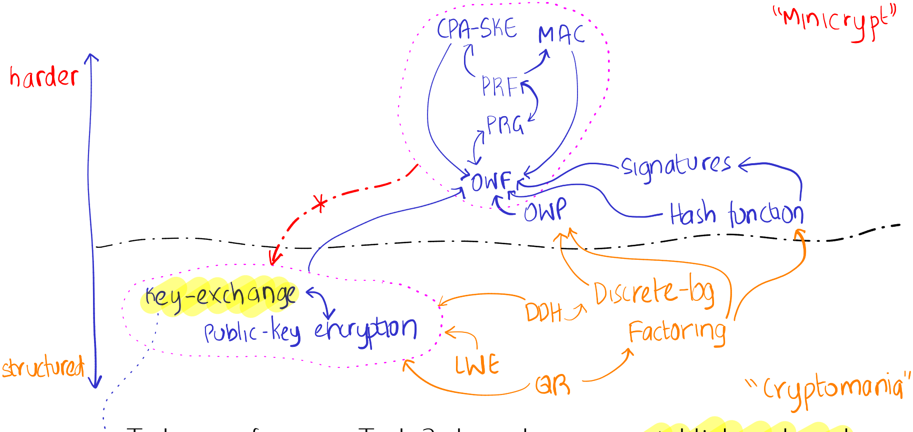


- Minicrypt to Cryptomania



- Today we focus on Task 3: how does one establish a shared key in the first place?

- Minicrypt to Cryptomania



- Today we focus on Task 3: how does one establish a shared key in the first place?

Plan for This Lecture...

General *template*:

1. Identify the task

Key exchange

2. Come up with precise threat model M (a.k.a security model)
   - Adversary/Attack: What are the adversary's capabilities?
   - Security Goal: What does it mean to be secure?
3. Construct a scheme Π
4. Formally prove that Π in secure in model M

computational secrecy

General *template*: Key exchange

Eavesdroppers

1. Identify the task
2. Come up with precise threat model M (a.k.a security model)
   - Adversary/Attack: What are the adversary's capabilities?
   - Security Goal: What does it mean to be secure?
3. Construct a scheme Π
4. Formally prove that Π in secure in model M

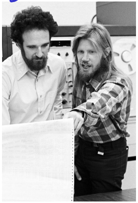
computational secrecy

General *template*:

Key exchange

Eavesdroppers

1. Identify the task
2. Come up with precise threat model M (a.k.a security model)
   - Adversary/Attack: What are the adversary's capabilities?
   - Security Goal: What does it mean to be secure?
3. Construct a scheme Π → Diffie-Hellman key exchange
4. Formally prove that Π in secure in model M



Credit for image: icour.fr

computational secrecy

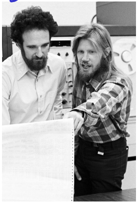
General *template*:

Key exchange

Eavesdroppers

1. Identify the task
2. Come up with precise threat model M (a.k.a security model)
   - Adversary/Attack: What are the adversary's capabilities?
   - Security Goal: What does it mean to be secure?
3. Construct a scheme Π → Diffie-Hellman key exchange
4. Formally prove that Π in secure in model M

↳ Assumption = proof!



Credit for image: icour.fr

Plan for This Lecture...

1. Key Exchange Protocol
2. Diffie-Hellman Key-Exchange Protocol
3. Exchanging Multiple Keys

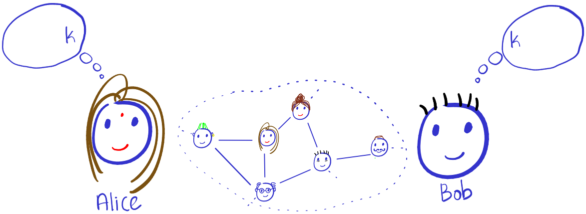
Plan for This Lecture...

1. Key Exchange Protocol

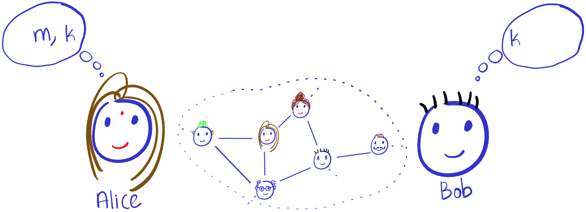
2. Diffie-Hellman Key-Exchange Protocol

3. Exchanging Multiple Keys

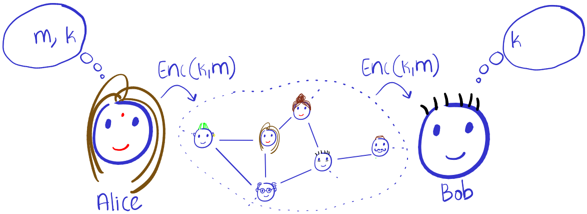
How To Establish a Shared Key in the First Place?



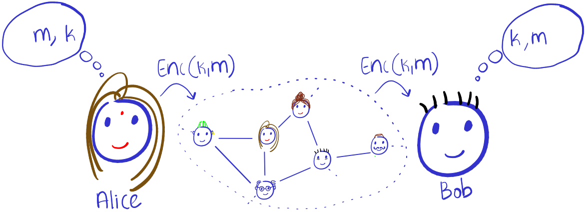
How To Establish a Shared Key in the First Place?



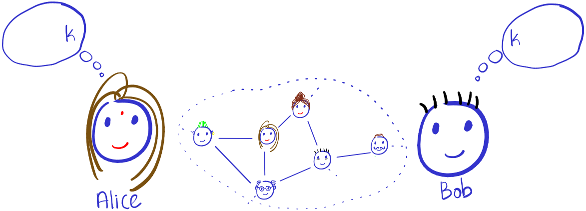
How To Establish a Shared Key in the First Place?



How To Establish a Shared Key in the First Place?

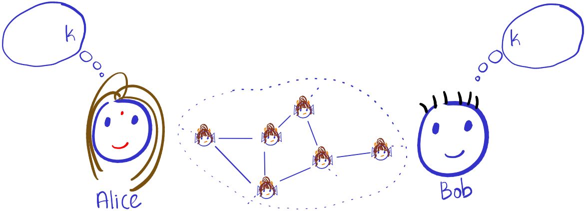


How To Establish a Shared Key in the First Place?



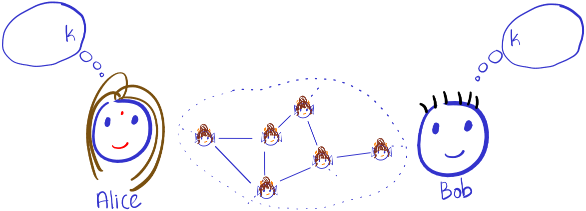
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$

How To Establish a Shared Key in the First Place?



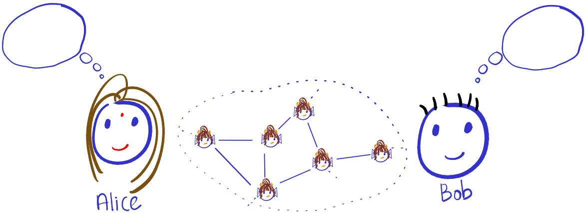
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve

How To Establish a Shared Key in the First Place?



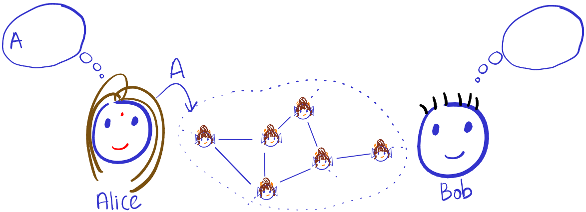
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve 
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)

How To Establish a Shared Key in the First Place?



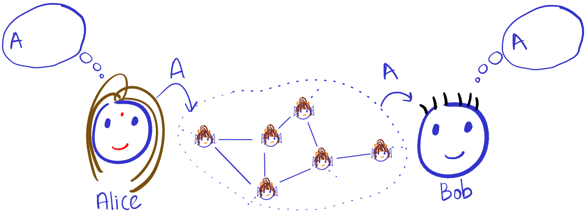
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key

How To Establish a Shared Key in the First Place?



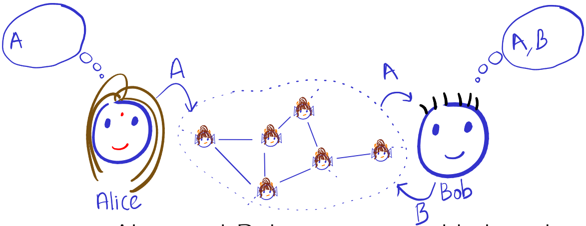
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key

How To Establish a Shared Key in the First Place?



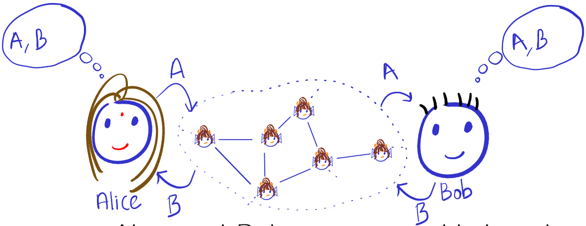
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key

How To Establish a Shared Key in the First Place?



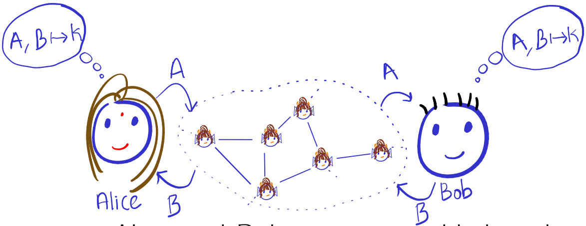
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key

How To Establish a Shared Key in the First Place?



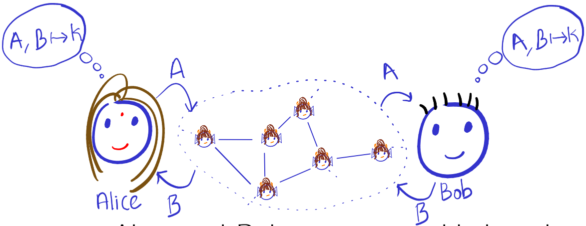
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key

How To Establish a Shared Key in the First Place?



- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve
  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key

How To Establish a Shared Key in the First Place?



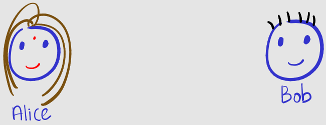
- The setting: Alice and Bob want to establish a shared key $k \in \{0,1\}^n$ in presence of an *eavesdropper* Eve

  - Why not rely on a key-distribution centre?
    - E.g.: Needham-Schroeder protocol (used in Kerberos)
    - Problems: single point of failure; doesn't scale
  - Ideally: Alice and Bob execute a *protocol*, at the end of which they will have established a key
- Key Exchange IRL: HTTPs, TLS, SSH

Syntax of Key Exchange Protocol

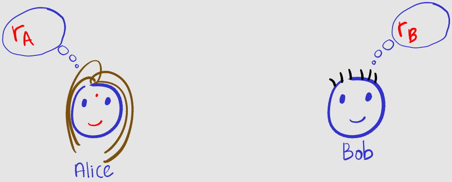
Defintion 1 (Key Exchange Protocol)

A (two-party) key-exchange protocol Π *is a probabilistic protocol between two parties* A *and* B *at the end of which party* A *locally outputs* $k_A \in \{0,1\}^n$ *and party* B *locally outputs* $k_B \in \{0,1\}^n$.



Defintion 1 (Key Exchange Protocol)

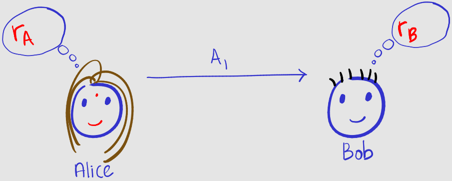
A (two-party) key-exchange protocol Π *is a probabilistic protocol between two parties* A *and* B *at the end of which party* A *locally outputs* $k_A \in \{0,1\}^n$ *and party* B *locally outputs* $k_B \in \{0,1\}^n$.



Syntax of Key Exchange Protocol

Defintion 1 (Key Exchange Protocol)

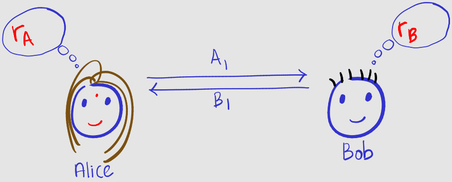
A (two-party) key-exchange protocol Π *is a probabilistic protocol between two parties* A *and* B *at the end of which party* A *locally outputs* $k_A \in \{0,1\}^n$ *and party* B *locally outputs* $k_B \in \{0,1\}^n$.



Syntax of Key Exchange Protocol

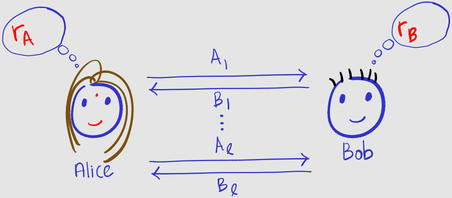
Defintion 1 (Key Exchange Protocol)

A (two-party) key-exchange protocol Π is a probabilistic protocol between two parties A and B at the end of which party A locally outputs $k_A \in \{0,1\}^n$ and party B locally outputs $k_B \in \{0,1\}^n$.



Defintion 1 (Key Exchange Protocol)

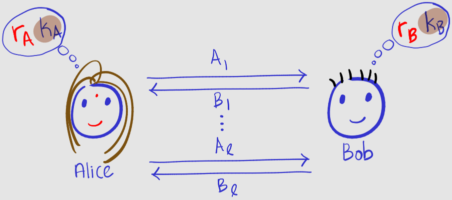
A (two-party) key-exchange protocol Π *is a probabilistic protocol between two parties* A *and* B *at the end of which party* A *locally outputs* $k_A \in \{0,1\}^n$ *and party* B *locally outputs* $k_B \in \{0,1\}^n$.



Syntax of Key Exchange Protocol

Defintion 1 (Key Exchange Protocol)

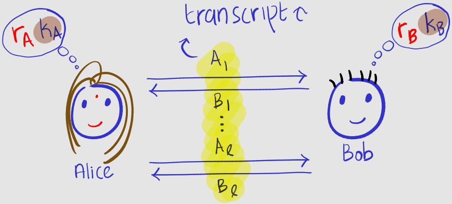
A (two-party) key-exchange protocol Π *is a probabilistic protocol between two parties* A *and* B *at the end of which party* A *locally outputs* $k_A \in \{0,1\}^n$ *and party* B *locally outputs* $k_B \in \{0,1\}^n$.



Syntax of Key Exchange Protocol

Defintion 1 (Key Exchange Protocol)

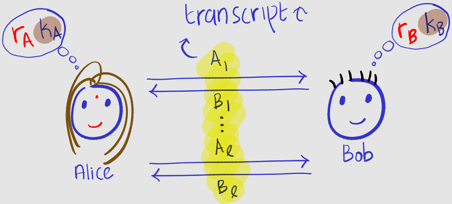
A (two-party) key-exchange protocol Π is a probabilistic protocol between two parties A and B at the end of which party A locally outputs $k_A \in \{0,1\}^n$ and party B locally outputs $k_B \in \{0,1\}^n$.



Syntax of Key Exchange Protocol

Defintion 1 (Key Exchange Protocol)

A (two-party) key-exchange protocol Π is a probabilistic protocol between two parties A and B at the end of which party A locally outputs $k_A \in \{0,1\}^n$ and party B locally outputs $k_B \in \{0,1\}^n$.



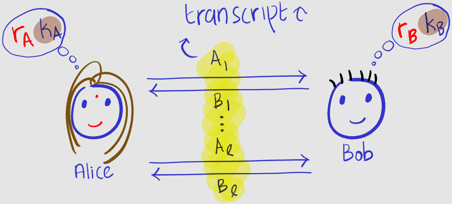
- *Correctness of key exchange: for every $n \in \mathbb{N}$*

$$\Pr_{(k_A, k_B, \tau) \leftarrow \Pi(1^n)}[k_A = k_B] = 1$$

Syntax of Key Exchange Protocol

Defintion 1 (Key Exchange Protocol)

A (two-party) key-exchange protocol Π is a probabilistic protocol between two parties A and B at the end of which party A locally outputs $k_A \in \{0,1\}^n$ and party B locally outputs $k_B \in \{0,1\}^n$.

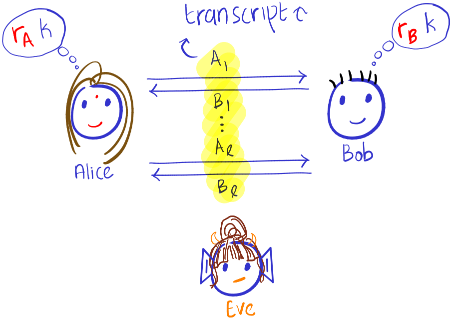


- *Correctness of key exchange: for every $n \in \mathbb{N}$*

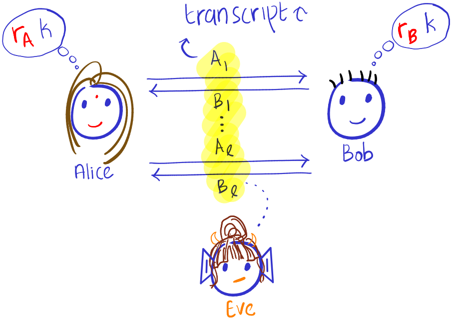
$$\Pr_{(\underset{k}{\cancel{k_A, k_B}}, \tau) \leftarrow \Pi(1^n)} [k_A = k_B] = 1$$

How to Define Security?...

- Intuitively, what is the security requirement?



- Intuitively, what is the security requirement?
  - Key k should be "hidden" given the *transcript* τ of the protocol



How to Define Security?...

- Intuitively, what is the security requirement?
  - Key k should be "hidden" given the *transcript* τ of the protocol

Defintion 2 (Secrecy Against Eavesdroppers)

A key-exchange protocol Π is secret against eavesdroppers if for every PPT eavesdropper Eve the following is negligible.

$$\delta(n) := \left| \Pr_{(k,\tau)\leftarrow\Pi(1^n)}[\mathsf{Eve}(\tau, k) = 0] - \Pr_{\substack{(k,\tau)\leftarrow\Pi(1^n)\\ r\leftarrow\{0,1\}^n}}[\mathsf{Eve}(\tau, r) = 0] \right|$$

How to Define Security?...

- Intuitively, what is the security requirement?
  - Key k should be "hidden" given the *transcript* τ of the protocol

Defintion 2 (Secrecy Against Eavesdroppers)

A key-exchange protocol Π is secret against eavesdroppers if for every PPT eavesdropper Eve the following is negligible.

$$\delta(n) := \left| \Pr_{(k,\tau)\leftarrow\Pi(1^n)}[\mathsf{Eve}(\tau, k) = 0] - \Pr_{\substack{(k,\tau)\leftarrow\Pi(1^n)\\ r\leftarrow\{0,1\}^n}}[\mathsf{Eve}(\tau, r) = 0] \right|$$

"Real world"

"Random world"

- Intuitively, what is the security requirement?
  - Key k should be "hidden" given the *transcript* τ of the protocol

Defintion 2 (Secrecy Against Eavesdroppers)

A key-exchange protocol Π is secret against eavesdroppers if for every PPT eavesdropper Eve the following is negligible.

$$\delta(n) := \left| \Pr_{(k,\tau)\leftarrow\Pi(1^n)}[\mathsf{Eve}(\tau, k) = 0] - \Pr_{\substack{(k,\tau)\leftarrow\Pi(1^n)\\ r\leftarrow\{0,1\}^n}}[\mathsf{Eve}(\tau, r) = 0] \right|$$

"Real world" "Random world"

Exercise 1

How can an unbounded eavesdropper Eve break secrecy?

Plan for this Lecture

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse.

But First Some Group Theory...

❓ What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms) $\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 \in \mathcal{G}$

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse.

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 \in \mathcal{G}$

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse.

$\forall g_1, g_2, g_3 \in \mathcal{G} : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

But First Some Group Theory...

? What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 \in \mathcal{G}$

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse.

$\exists 1 \in \mathcal{G}\ \forall g \in \mathcal{G} : 1 \cdot g = g \cdot 1 = g$

$\forall g_1, g_2, g_3 \in \mathcal{G} : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 \in \mathcal{G}$

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse.

$\exists 1 \in \mathcal{G}\ \forall g \in \mathcal{G} : 1 \cdot g = g \cdot 1 = g$

$\forall g \exists g^{-1} : g \cdot g^{-1} = 1$

$\forall g_1, g_2, g_3 \in \mathcal{G} : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 \in \mathcal{G}$

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

$\exists 1 \in \mathcal{G}\ \forall g \in \mathcal{G} : 1 \cdot g = g \cdot 1 = g$

$\forall g \exists g^{-1} : g \cdot g^{-1} = 1$

$\forall g_1, g_2, g_3 \in \mathcal{G} : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 = g_2 \cdot g_1$

? What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 \in \mathcal{G}$

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

$\exists 1 \in \mathcal{G}\ \forall g \in \mathcal{G} : 1 \cdot g = g \cdot 1 = g$

$\forall g \exists g^{-1} : g \cdot g^{-1} = 1$

$\forall g_1, g_2, g_3 \in \mathcal{G} : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

$\forall g_1, g_2 \in \mathcal{G} : g_1 \cdot g_2 = g_2 \cdot g_1$

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order*

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order*
- *Order of an element g: smallest ℓ such that $g^\ell := g \cdot \ldots \cdot g = 1$*

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order* ℓ
- *Order of an element g: smallest ℓ such that $g^\ell := g \cdot \ldots \cdot g = 1$*

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order* ℓ
- *Order of an element g: smallest ℓ such that $g^\ell := g \cdot \ldots \cdot g = 1$*
- *Cyclic group: there exists a "generator" $g \in \mathcal{G}$ with order $\ell = |\mathcal{G}|$*
    - *That is $\{g^1 = g, g^2, \ldots, g^{\ell-1}, g^\ell = 1\} = \mathcal{G}$*

But First Some Group Theory...

❓ What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

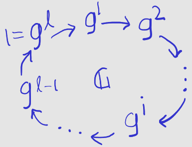
- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order.* ℓ
- *Order of an element $\mathbf{g}$: smallest ℓ such that $\mathbf{g}^\ell := \mathbf{g} \cdot \ldots \cdot \mathbf{g} = 1$*
- *Cyclic group: there exists a "generator" $\mathbf{g} \in \mathcal{G}$ with order $\ell = |\mathcal{G}|$*
    - *That is* $\{\mathbf{g}^1 = \mathbf{g}, \mathbf{g}^2, \ldots, \mathbf{g}^{\ell-1}, \mathbf{g}^\ell = 1\} = \mathcal{G}$



But First Some Group Theory...

? What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

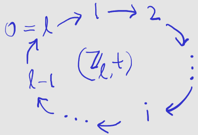
- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

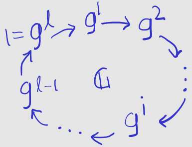
Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order* ℓ
- *Order of an element g: smallest ℓ such that $g^\ell := g \cdot \ldots \cdot g = 1$*
- *Cyclic group: there exists a "generator" $g \in \mathcal{G}$ with order $\ell = |\mathcal{G}|$*
  - *That is $\{g^1 = g, g^2, \ldots, g^{\ell-1}, g^\ell = 1\} = \mathcal{G}$*





  - *"Isomorphism" between $(\mathbb{Z}_\ell, +)$ and $\mathbb{G}$*

But First Some Group Theory...

What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

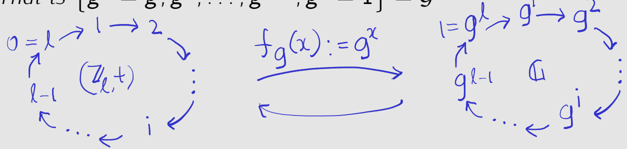
- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order* ℓ
- *Order of an element $\boldsymbol{g}$: smallest ℓ such that $\boldsymbol{g}^{\ell} := \boldsymbol{g} \cdot \ldots \cdot \boldsymbol{g} = 1$*
- *Cyclic group: there exists a "generator" $\boldsymbol{g} \in \mathcal{G}$ with order $\ell = |\mathcal{G}|$*
  - *That is $\{\boldsymbol{g}^1 = \boldsymbol{g}, \boldsymbol{g}^2, \ldots, \boldsymbol{g}^{\ell-1}, \boldsymbol{g}^{\ell} = 1\} = \mathcal{G}$*



  - *"Isomorphism" between $(\mathbb{Z}_\ell, +)$ and $\mathbb{G}$*

But First Some Group Theory...

? What are some properties of $(\{0,1\}^n, \oplus)$ we have exploited?

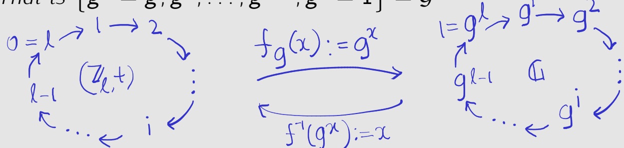
- Closure of $\oplus$, self-inverse ($k \oplus k = 0^n$), associativity?

Defintion 3 (Group axioms)

A group $\mathbb{G}$ is a set $\mathcal{G}$ with a binary operation $\cdot$ satisfying: 1) closure 2) associativity, 3) existence of identity and 4) existence of inverse. $\mathbb{G}$ Abelian if it additionally satisfies 5) commutativity.

Defintion 4 (Group terminology)

- *Order of the group, $|\mathcal{G}|$. We're interested in groups of finite order* ℓ
- *Order of an element $\mathbf{g}$: smallest ℓ such that $\mathbf{g}^\ell := \mathbf{g} \cdot \ldots \cdot \mathbf{g} = 1$*
- *Cyclic group: there exists a "generator" $\mathbf{g} \in \mathcal{G}$ with order $\ell = |\mathcal{G}|$*
  - *That is* $\{\mathbf{g}^1 = \mathbf{g}, \mathbf{g}^2, \ldots, \mathbf{g}^{\ell-1}, \mathbf{g}^\ell = 1\} = \mathcal{G}$



  - *"Isomorphism" between $(\mathbb{Z}_\ell, +)$ and $\mathbb{G}$*

But First Some Group Theory...

Exercise 2 (Lagrange's theorem)

Prove that the order of an element divides order of the (finite) group.

Exercise 3

For a group $\mathbb{G}$ *of order* ℓ *with generator* g*, show using group axioms that for all* $a, b \in \mathbb{Z}_\ell$*,* $(g^a)^b = g^{ab} = (g^b)^a$

Exercise 4

Prove that a prime-order group is cyclic. Are all cyclic groups of prime order?

Addition modulo prime p

$(\mathbb{Z}_p, +)$

$\{0, \cdots p-1\}$ $\quad$ $g_1 + g_2 := g_1 + g_2 \pmod{p}$

Some Examples of Groups

Addition modulo prime p

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $g_1 + g_2 := g_1 + g_2 \pmod{p}$

- order p
- cyclic

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0 = p$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$ $\quad$ $g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Some Examples of Groups

Addition modulo prime p

$$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0 = p$$

$$(\mathbb{Z}_p, +)$$

$\{0, \dots, p-1\}$ $\quad$ $g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

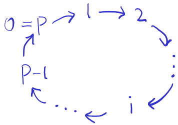
Multiplication modulo prime p

$$(\mathbb{Z}_p^\times, \cdot)$$

$\{1, \dots, p-1\}$ $\quad$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

Some Examples of Groups

Addition modulo prime *p*



$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $\quad$ $g_1 + g_2 := g_1 + g_2 \pmod{p}$

◆ order p ◆ cyclic

Multiplication modulo prime *p*

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$ $\quad$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{p}$

◆ order p-1 ◆ cyclic

Some Examples of Groups

Addition modulo prime p

$$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0 = p$$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$ $\quad$ $g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1 = g^{p-1} \bmod p$$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots, p-1\}$ $\quad$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Some Examples of Groups

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0 = p$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$ $\quad g_1 + g_2 := g_1 + g_2 \pmod{p}$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1 = g^{p-1} \bmod p$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots, p-1\}$ $\quad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{p}$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

Some Examples of Groups

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

Some Examples of Groups

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots, p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots, p-1,$
$p+1, \dots, 2p-1,$
$\dots, pq-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Some Examples of Groups

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0 = p$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1 = g^{p-1} \bmod p$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots, p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

"RSA group"

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots, p-1,$
$p+1, \dots, 2p-1,$
$\dots, pq-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Finding order as hard as factoring N

Some Examples of Groups

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod{p}$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots, p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{p}$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots, p-1, p+1, \dots, 2p-1, \dots, pq-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{N}$

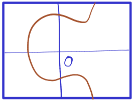
- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E_p, +)$ "curve points addition"

solutions to

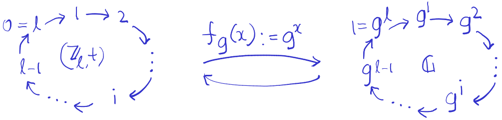
$y^2 = x^3 + Ax + B \pmod{p}$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

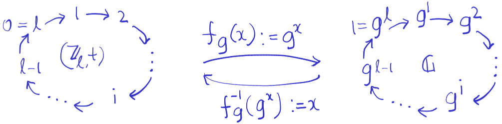
A Hard(?) Computational Problem Over Cyclic Groups...

- Recall our exp. map

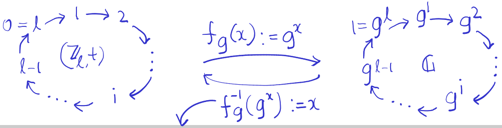


A Hard(?) Computational Problem Over Cyclic Groups...

- Recall our exp. map



- Recall our exp. map

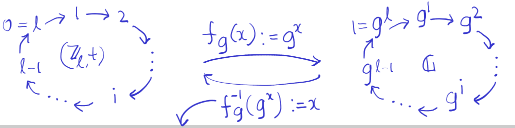


Defintion 5 (Discrete logarithm (DLog) problem in $\mathbb{G}$ w.r.to S)

- *Input:*
  1. $(\mathbb{G}, \ell, g)$ *sampled by a group sampler* $\mathsf{S}(1^n)$
  2. $h := g^a$ *for* $a \leftarrow \mathbb{Z}_\ell$
- *Solution:* a

A Hard(?) Computational Problem Over Cyclic Groups...

- Recall our exp. map



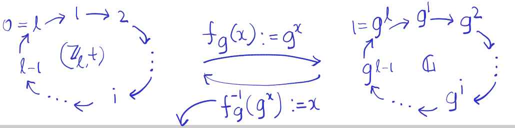
Defintion 5 (Discrete logarithm (DLog) problem in $\mathbb{G}$ w.r.to S)

- *Input:*
  1. $(\mathbb{G}, \ell, g)$ *sampled by a group sampler* $\mathsf{S}(1^n)$
  2. $h := g^a$ *for* $a \leftarrow \mathbb{Z}_\ell$
- *Solution:* a

E.g. for group $(\mathbb{Z}_p^\times, \cdot)$ S outputs prime of "size" n

A Hard(?) Computational Problem Over Cyclic Groups...

- Recall our exp. map



Defintion 5 (Discrete logarithm (DLog) problem in $\mathbb{G}$ w.r.to S)

- *Input:*
  1. $(\mathbb{G}, \ell, g)$ *sampled by a group sampler* $\mathsf{S}(1^n)$
  2. $h := g^a$ *for* $a \leftarrow \mathbb{Z}_\ell$
- *Solution:* a

E.g. for group $(\mathbb{Z}_p^\times, \cdot)$ S outputs prime of "size" n

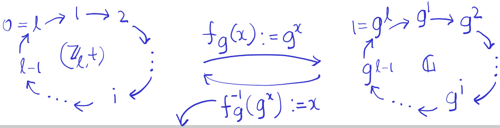
Assumption 1 (DLog assumption in $\mathbb{G}$ w.r.to S)

The DLog assumption in $\mathbb{G}$ w.r.to S holds if solving the DLog problem in $\mathbb{G}$ w.r.to S is hard for all PPT inverters Inv. That is, for all Inv, the following is negligible:

$$\delta(n) := \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a\leftarrow\mathbb{Z}_\ell}}\left[\mathsf{Inv}((\mathbb{G},\ell,g),g^a) = a\right]$$

A Hard(?) Computational Problem Over Cyclic Groups...

- Recall our exp. map



Defintion 5 (Discrete logarithm (DLog) problem in $\mathbb{G}$ w.r.to S)

- *Input:*
  1. $(\mathbb{G}, \ell, g)$ *sampled by a group sampler* $\mathsf{S}(1^n)$ E.g. for group $(\mathbb{Z}_p^\times, \cdot)$ S outputs prime of "size" n
  2. $h := g^a$ *for* $a \leftarrow \mathbb{Z}_\ell$
- *Solution:* a

Assumption 1 (DLog assumption in $\mathbb{G}$ w.r.to S)

The DLog assumption in $\mathbb{G}$ *w.r.to* S *holds if solving the DLog problem in* $\mathbb{G}$ *w.r.to* S *is hard for all PPT inverters* Inv. *That is, for all* Inv, *the following is negligible:*

$$\delta(n) := \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow \mathsf{S}(1^n) \\ a \leftarrow \mathbb{Z}_\ell}} [\mathsf{Inv}((\cancel{\mathbb{G}, \ell, g}), g^a) = a]$$

A Hard(?) Computational Problem Over Cyclic Groups...

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $\quad g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$ $\quad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$

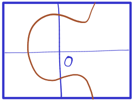
$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to
$y^2 = x^3 + Ax + B \pmod p$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

A Hard(?) Computational Problem Over Cyclic Groups...

? Easy! Division modulo p

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $\quad$ $g_1 + g_2 := g_1 + g_2 \pmod p$

◆ order p ◆ cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$ $\quad$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

◆ order $p-1$ ◆ cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

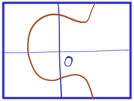
$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$ $\quad$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

◆ order $(p-1)(q-1)$ ◆ not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to
$y^2 = x^3 + Ax + B \pmod p$



◆ $|p+1 - \text{order}| \leq 2\sqrt{p}$ ◆ cyclic

A Hard(?) Computational Problem Over Cyclic Groups...

Easy! Division modulo p

Addition modulo prime p

$0=p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0=p$

$(\mathbb{Z}_p, +)$

$\{0,\dots,p-1\}$ $\quad g_1+g_2 := g_1+g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1=g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1=g^{p-1} \bmod p$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1,\dots,p-1\}$ $\quad g_1\cdot g_2 := g_1\cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1,\dots,p-1,$
$p+1,\dots,2p-1,$
$\dots pq-1\}$

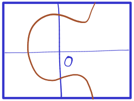
$g_1\cdot g_2 := g_1\cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to
$y^2=x^3+Ax+B \pmod p$



- $|p+1-\text{order}| \le 2\sqrt{p}$
- cyclic

A Hard(?) Computational Problem Over Cyclic Groups...

? Easy! Division modulo p

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots, p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

◆ order p ◆ cyclic

? Believed hard; $\exists$ sub-exponential algos

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots, p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

◆ order $p-1$ ◆ cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots, p-1,$
$p+1, \dots, 2p-1,$
$\dots, pq-1\}$

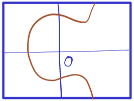
$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

◆ order $(p-1)(q-1)$ ◆ not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to $y^2 = x^3 + Ax + B \pmod p$



◆ $|p+1 - \text{order}| \leq 2\sqrt{p}$ ◆ cyclic

A Hard(?) Computational Problem Over Cyclic Groups...

? Easy! Division modulo p

Addition modulo prime p

$$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $\qquad g_1 + g_2 := g_1 + g_2 \pmod p$

◆ order p ◆ cyclic

? Believed hard; $\exists$ sub-exponential algos

Multiplication modulo prime p

$$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$ $\qquad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

◆ order $p-1$ ◆ cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

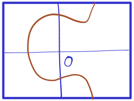
$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$ $\qquad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

◆ order $(p-1)(q-1)$ ◆ not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to
$y^2 = x^3 + Ax + B \pmod p$



◆ $|p+1 - \text{order}| \leq 2\sqrt{p}$ ◆ cyclic

A Hard(?) Computational Problem Over Cyclic Groups...

? Easy! Division modulo p

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod{p}$

- order p
- cyclic

? Believed hard; ∃ sub-exponential algos

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{p}$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{N}$

- order $(p-1)(q-1)$
- not cyclic

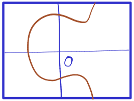
Hard in its cyclic subgroup

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to

$y^2 = x^3 + Ax + B \pmod{p}$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

A Hard(?) Computational Problem Over Cyclic Groups...

? Easy! Division modulo p

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \ldots, p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

◆ order p ◆ cyclic

? Believed hard; ∃ sub-exponential algos

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \ldots, p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

◆ order $p-1$ ◆ cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \ldots, p-1, p+1, \ldots, 2p-1, \ldots, pq-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

◆ order $(p-1)(q-1)$ ◆ not cyclic

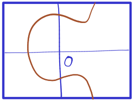
Hard in its cyclic subgroup

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to

$y^2 = x^3 + Ax + B \pmod p$



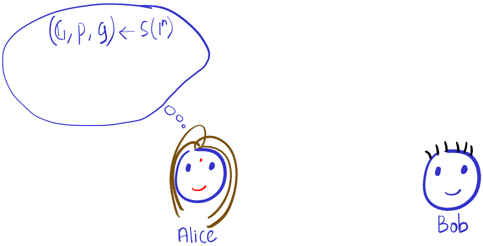
◆ $|p+1 - \text{order}| \le 2\sqrt{p}$ ◆ cyclic

Believed hard; no known sub-exponential algos!

Diffie-Hellman Key-Exchange Protocol

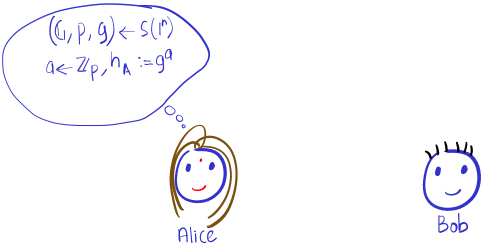
- The protocol:

Diffie-Hellman Key-Exchange Protocol



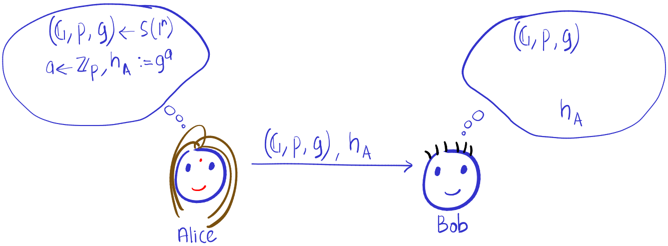
- The protocol:

Diffie-Hellman Key-Exchange Protocol

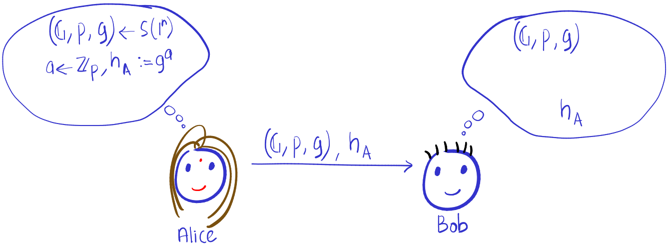


- The protocol:

Diffie-Hellman Key-Exchange Protocol

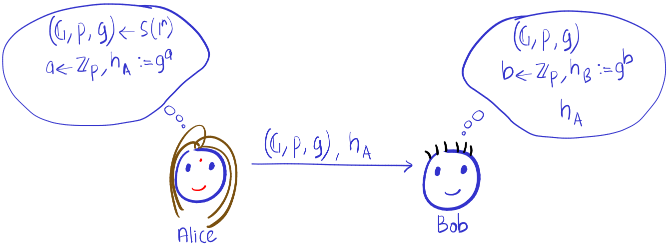


- The protocol:



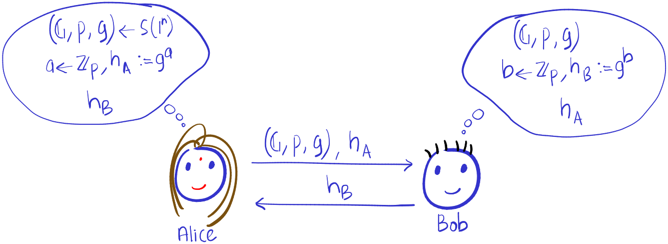
- The protocol:
  1. Alice→Bob: Send $((\mathbb{G}, p, g), h_A := g^a)$, where $(\mathbb{G}, p, g) \leftarrow \mathsf{S}(1^n)$ and $a \leftarrow \mathbb{Z}_p$

Diffie-Hellman Key-Exchange Protocol



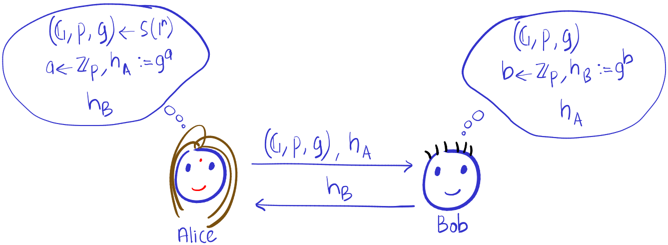
- The protocol:
  1. Alice→Bob: Send $((\mathbb{G}, p, g), h_A := g^a)$, where $(\mathbb{G}, p, g) \leftarrow \mathsf{S}(1^n)$ and $a \leftarrow \mathbb{Z}_p$

Diffie-Hellman Key-Exchange Protocol



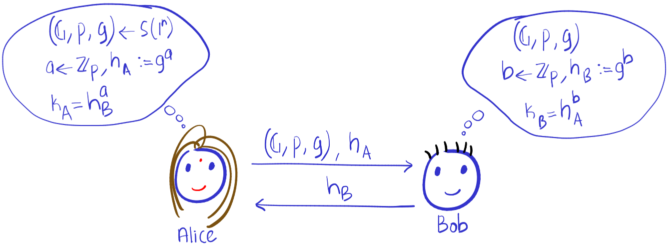
- The protocol:
  1. Alice→Bob: Send $((\mathbb{G}, p, g), h_A := g^a)$, where $(\mathbb{G}, p, g) \leftarrow \mathsf{S}(1^n)$ and $a \leftarrow \mathbb{Z}_p$

Diffie-Hellman Key-Exchange Protocol



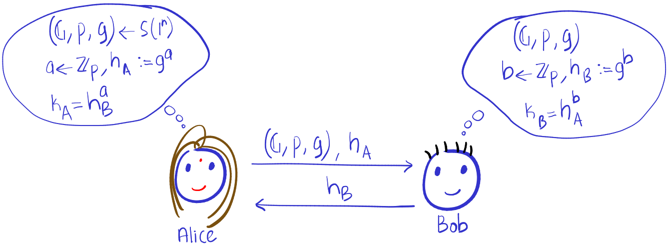
- The protocol:
  1. Alice→Bob: Send $((\mathbb{G}, p, g), h_A := g^a)$, where $(\mathbb{G}, p, g) \leftarrow \mathsf{S}(1^n)$ and $a \leftarrow \mathbb{Z}_p$
  2. Alice←Bob: Send $h_B := g^b$ for $b \leftarrow \mathbb{Z}_p$

Diffie-Hellman Key-Exchange Protocol



- The protocol:
  1. Alice$\rightarrow$Bob: Send $((\mathbb{G}, p, g), h_A := g^a)$, where $(\mathbb{G}, p, g) \leftarrow \mathsf{S}(1^n)$ and $a \leftarrow \mathbb{Z}_p$
  2. Alice$\leftarrow$Bob: Send $h_B := g^b$ for $b \leftarrow \mathbb{Z}_p$

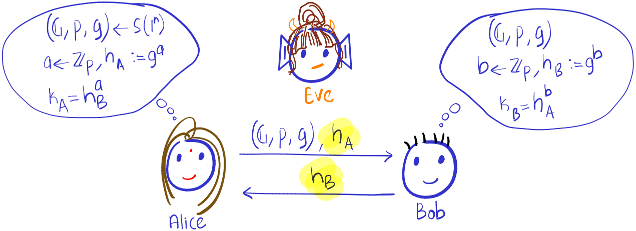
Diffie-Hellman Key-Exchange Protocol



- The protocol:
  1. Alice→Bob: Send $((\mathbb{G}, p, g), h_A := g^a)$, where $(\mathbb{G}, p, g) \leftarrow \mathsf{S}(1^n)$ and $a \leftarrow \mathbb{Z}_p$
  2. Alice←Bob: Send $h_B := g^b$ for $b \leftarrow \mathbb{Z}_p$
  3. Alice outputs $k_A := (h_B)^a$; Bob outputs $k_B := (h_A)^b$
- Correctness of key generation:

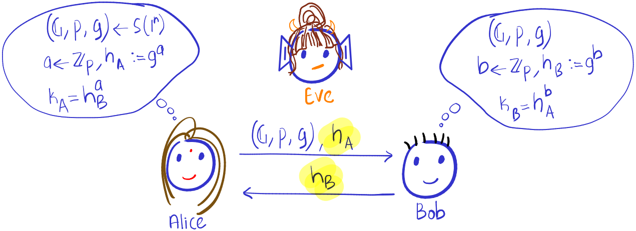
$$k_A = h_B^a = (g^b)^a = g^{ab} = (g^a)^b = h_A^b = k_B$$

When is it Secret Against Eavesdroppers?...



- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$

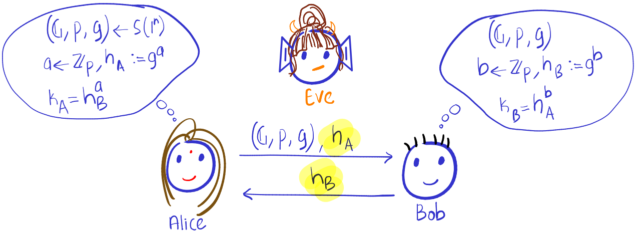
When is it Secret Against Eavesdroppers?...



- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$

? What if DLog problem is easy over $\mathbb{G}$?

When is it Secret Against Eavesdroppers?...

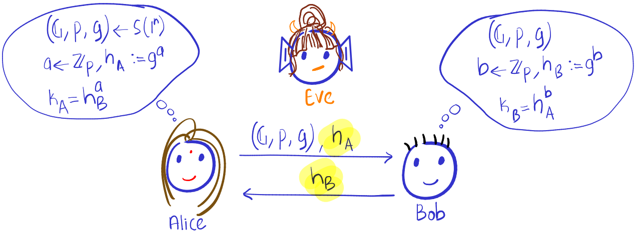


- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$

What if DLog problem is easy over $\mathbb{G}$?

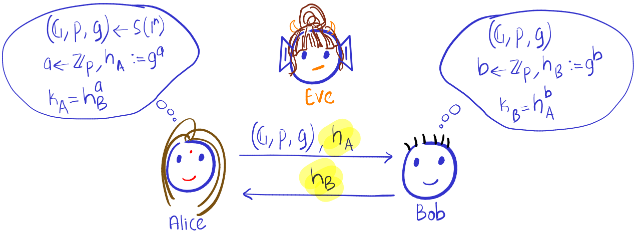
Then Eve can invert h_A to get a and compute $k = h_B^a$

When is it Secret Against Eavesdroppers?...



- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$
- What if DLog problem is easy over $\mathbb{G}$?
  - Then Eve can invert h_A to get a and compute $k = h_B^a$
- Is DLog problem being hard sufficient?

When is it Secret Against Eavesdroppers?...



- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$

What if DLog problem is easy over $\mathbb{G}$?

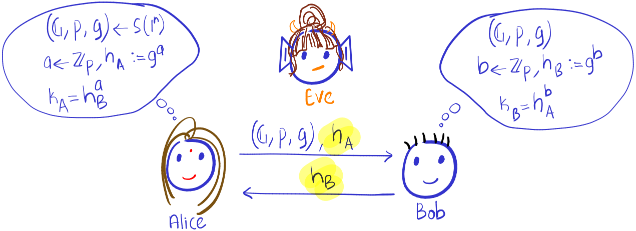
Then Eve can invert h_A to get a and compute $k = h_B^a$

Is DLog problem being hard sufficient?

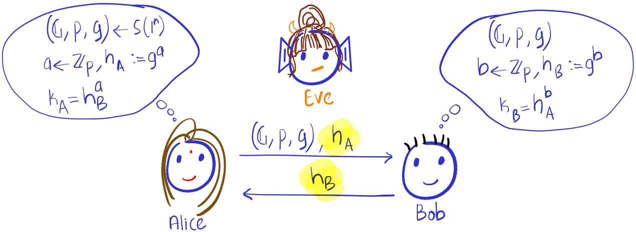
No, what if Eve can compute g^{ab} given g^a and g^b?

- This is the "computational Diffie-Hellman" (CDH) problem

When is it Secret Against Eavesdroppers?...



- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$
- What if DLog problem is easy over $\mathbb{G}$?
  - Then Eve can invert h_A to get a and compute $k = h_B^a$
- Is DLog problem being hard sufficient?
  - No, what if Eve can compute g^{ab} given g^a and g^b?
    - This is the "computational Diffie-Hellman" (CDH) problem
- Is CDH problem being hard sufficient?



- What does Eve see? The transcript is $(h_A := g^a, h_B := g^b)$

What if DLog problem is easy over $\mathbb{G}$?

Then Eve can invert h_A to get a and compute $k = h_B^a$

Is DLog problem being hard sufficient?

No, what if Eve can compute g^{ab} given g^a and g^b?

- This is the "computational Diffie-Hellman" (CDH) problem

Is CDH problem being hard sufficient?

What if Eve can distinguish g^{ab} from random group elements?

- There exist such groups!

When is it Secret Against Eavesdroppers?...

Assumption 2 (Decisional DH (DDH) assumption in in $\mathbb{G}$ w.r.to S)

The DDH assumption holds in $\mathbb{G}$ w.r.to S if for all PPT distinguishers D, the following is negligible:

$$\left| \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow \mathsf{S}(1^n)\\ a,b\leftarrow \mathbb{Z}_\ell}}[\mathsf{D}(g^a, g^b, g^{ab}) = 0] - \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow \mathsf{S}(1^n)\\ a,b,r\leftarrow \mathbb{Z}_\ell}}[\mathsf{D}(g^a, g^b, g^{r}) = 0] \right|$$

When is it Secret Against Eavesdroppers?...

Assumption 2 (Decisional DH (DDH) assumption in in $\mathbb{G}$ w.r.to S)

The DDH assumption holds in $\mathbb{G}$ w.r.to S if for all PPT distinguishers D, the following is negligible:

$$\left| \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a,b\leftarrow\mathbb{Z}_\ell}}[\mathsf{D}(g^a,g^b,g^{ab})=0] - \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a,b,r\leftarrow\mathbb{Z}_\ell}}[\mathsf{D}(g^a,g^b,g^{r})=0] \right|$$

"Real world" "Random world"

When is it Secret Against Eavesdroppers?...

Assumption 2 (Decisional DH (DDH) assumption in in $\mathbb{G}$ w.r.to S)

The DDH assumption holds in $\mathbb{G}$ w.r.to S if for all PPT distinguishers D, the following is negligible:

$$\left| \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a,b\leftarrow\mathbb{Z}_\ell}}[\mathsf{D}(g^a, g^b, g^{ab}) = 0] - \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a,b,r\leftarrow\mathbb{Z}_\ell}}[\mathsf{D}(g^a, g^b, g^{r}) = 0] \right|$$

"Real world" "Random world"

Theorem 1

Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof.

Secrecy requirement is same as the assumption! □

When is it Secret Against Eavesdroppers?...

Assumption 2 (Decisional DH (DDH) assumption in in $\mathbb{G}$ w.r.to S)

The DDH assumption holds in $\mathbb{G}$ w.r.to S if for all PPT distinguishers D, the following is negligible:

$$\left| \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow \mathsf{S}(1^n)\\ a,b\leftarrow \mathbb{Z}_\ell}}[\mathsf{D}(g^a,g^b,g^{ab})=0] - \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow \mathsf{S}(1^n)\\ a,b,r\leftarrow \mathbb{Z}_\ell}}[\mathsf{D}(g^a,g^b,g^{r})=0] \right|$$

"Real world" "Random world"

Theorem 1

Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof.

Secrecy requirement is same as the assumption! □

Exercise 5

But I did slightly cheat! Figure out where.

Where is DDH Assumption Known to Hold?

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \ldots, p-1\}$ $\quad g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \ldots, p-1\}$ $\quad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

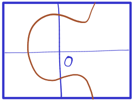
$\{1, \ldots, p-1, p+1, \ldots, 2p-1, \ldots, pq-1\}$ $\quad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to $y^2 = x^3 + Ax + B \pmod p$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

Where is DDH Assumption Known to Hold?

? Easy! Since DLog is easy

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$

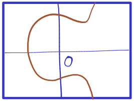
$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to
$y^2 = x^3 + Ax + B \pmod p$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

Where is DDH Assumption Known to Hold?

? Easy! Since DLog is easy

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod{p}$

- order p
- cyclic

?

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{p}$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1,$
$p+1, \dots, 2p-1,$
$\dots pq-1\}$

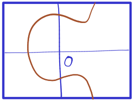
$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod{N}$

- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to
$y^2 = x^3 + Ax + B \pmod{p}$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

Where is DDH Assumption Known to Hold?

? Easy! Since DLog is easy

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$

$g_1 + g_2 := g_1 + g_2 \pmod p$

- order p
- cyclic

? Easy! Maybe Assignment 3

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$

$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

- order $p-1$
- cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1, p+1, \dots, 2p-1, \dots pq-1\}$

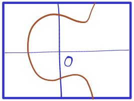
$g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

- order $(p-1)(q-1)$
- not cyclic

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to $y^2 = x^3 + Ax + B \pmod p$



- $|p+1 - \text{order}| \leq 2\sqrt{p}$
- cyclic

Where is DDH Assumption Known to Hold?

? Easy! Since DLog is easy

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0 = p$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $g_1 + g_2 := g_1 + g_2 \pmod p$

◆ order p ◆ cyclic

? Easy! Maybe Assignment 3

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

◆ order $p-1$ ◆ cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1, p+1, \dots, 2p-1, \dots pq-1\}$ $g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

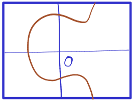
◆ order $(p-1)(q-1)$ ◆ not cyclic

Hard in its cyclic subgroup

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to $y^2 = x^3 + Ax + B \pmod p$



◆ $|p+1 - \text{order}| \le 2\sqrt{p}$ ◆ cyclic

Where is DDH Assumption Known to Hold?

? Easy! Since DLog is easy

Addition modulo prime p

$0 = p \to 1 \to 2 \to \cdots \to i \to \cdots \to p-1 \to 0$

$(\mathbb{Z}_p, +)$

$\{0, \dots p-1\}$ $\quad g_1 + g_2 := g_1 + g_2 \pmod p$

◆ order p ◆ cyclic

? Easy! Maybe Assignment 3

Multiplication modulo prime p

$1 = g^{p-1} \bmod p \to g^1 \bmod p \to \cdots \to g^i \bmod p \to \cdots \to 1$

$(\mathbb{Z}_p^\times, \cdot)$

$\{1, \dots p-1\}$ $\quad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod p$

◆ order $p-1$ ◆ cyclic

Multiplication modulo $N = pq$

primes

$(\mathbb{Z}_N^\times, \cdot)$

$\{1, \dots p-1, p+1, \dots, 2p-1, \dots pq-1\}$ $\quad g_1 \cdot g_2 := g_1 \cdot g_2 \pmod N$

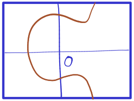
◆ order $(p-1)(q-1)$ ◆ not cyclic

Hard in its cyclic subgroup

Elliptic curves modulo prime p

$(E, +)$ "curve points addition"

solutions to $y^2 = x^3 + Ax + B \pmod p$

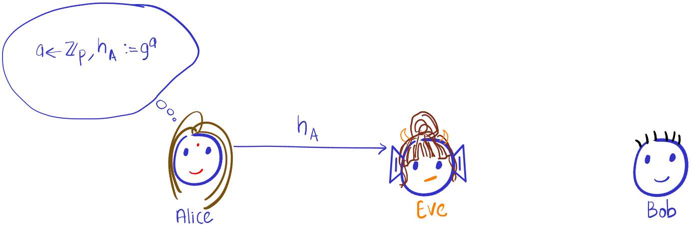


◆ $|p+1 - \text{order}| \leq 2\sqrt{p}$ ◆ cyclic

Believed hard

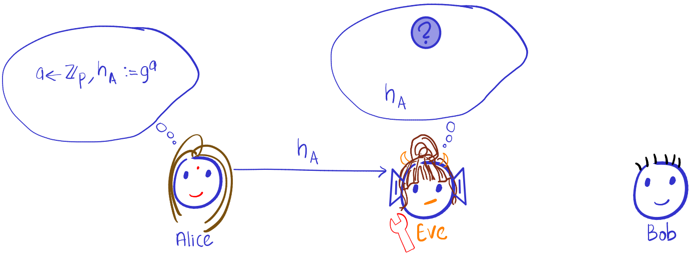
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages

What About Secrecy Against Active Eve?



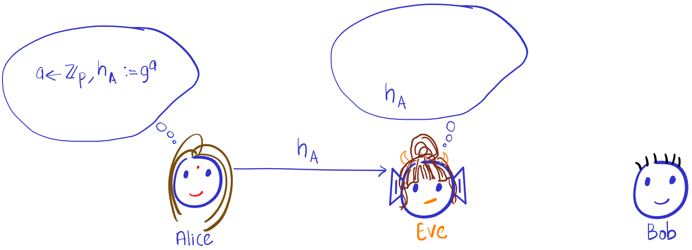
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages

What About Secrecy Against Active Eve?



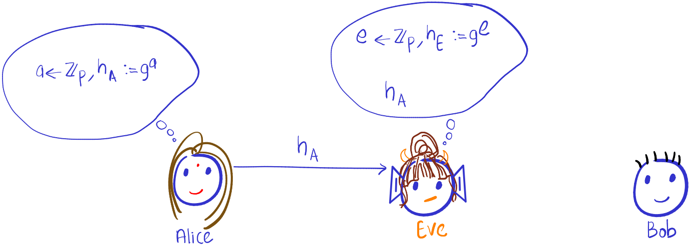
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages

What About Secrecy Against Active Eve?



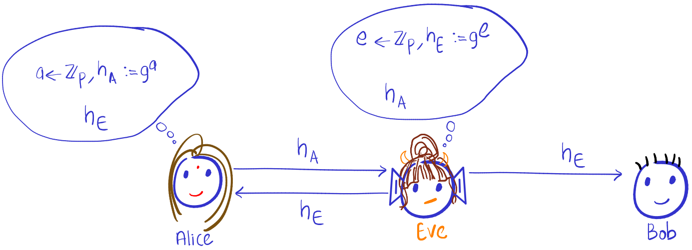
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



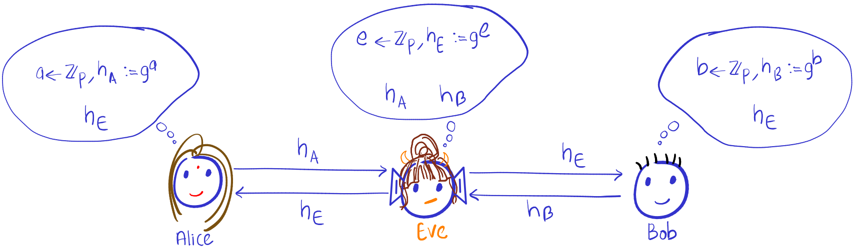
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



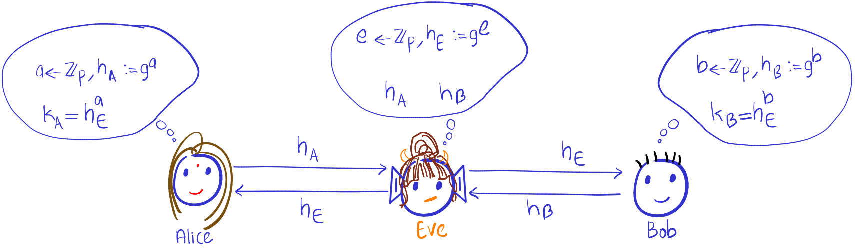
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



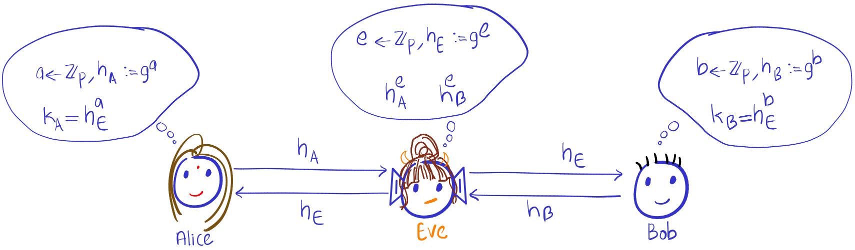
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



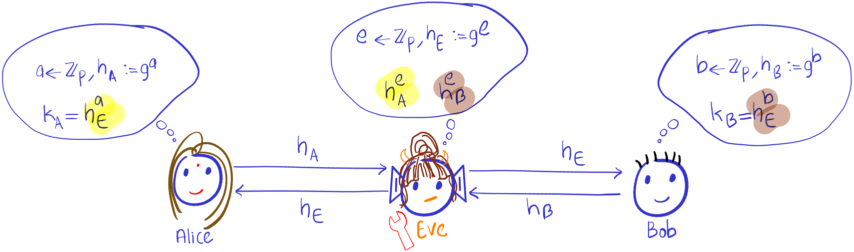
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



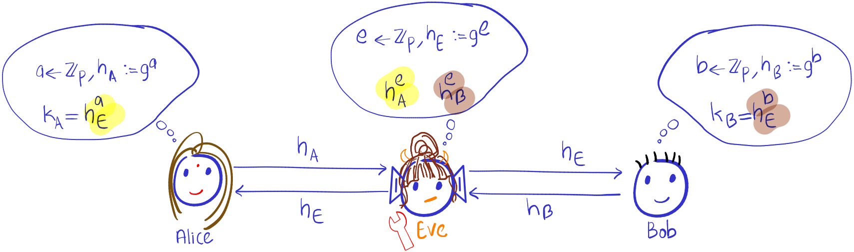
- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

What About Secrecy Against Active Eve?



- What if Eve is an active adversary?
  - Recall that active Eve can intercept/tamper messages
- There is a person-in-the-middle attack!
  - Pretends to be Alice to Bob and Bob to Alice
  - Eve sets up two separate key exchanges with Alice and Bob

⚠ Insecure against active adversary

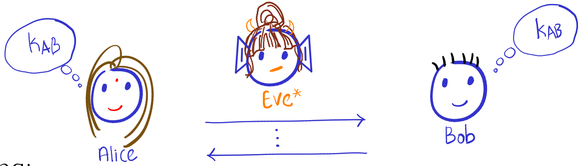
Plan for this Lecture

1 Key Exchange Protocol

2 Diffie-Hellman Key-Exchange Protocol

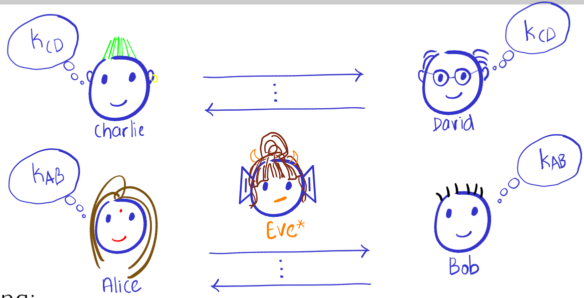
3 Exchanging Multiple Keys

Let's Try Exchanging Multiple Keys



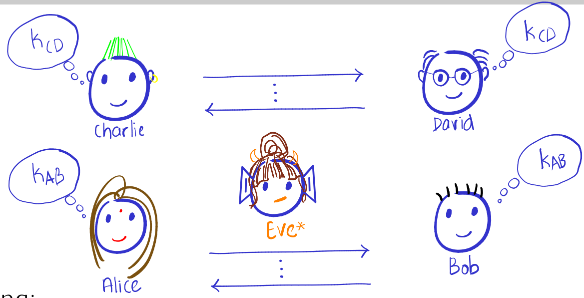
- The setting:
  - Alice and Bob want to establish a shared key $k_{AB} \in \{0,1\}^n$ in presence of an *eavesdropper* Eve*

Let's Try Exchanging Multiple Keys



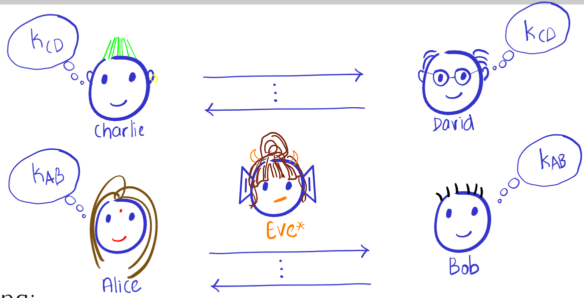
- The setting:
  - Alice and Bob want to establish a shared key $k_{AB} \in \{0,1\}^n$ in presence of an *eavesdropper* Eve*
  - Charlie and David want to do the same

Let's Try Exchanging Multiple Keys



- The setting:
  - Alice and Bob want to establish a shared key $k_{AB} \in \{0,1\}^n$ in presence of an *eavesdropper* Eve*
  - Charlie and David want to do the same
- In general: t pairs of parties, t pairwise shared keys
- Secrecy: the t shared keys should be indistinguishable to Eve* from t random keys (given all transcripts)

Let's Try Exchanging Multiple Keys



- The setting:
  - Alice and Bob want to establish a shared key $k_{AB} \in \{0,1\}^n$ in presence of an *eavesdropper* Eve*
  - Charlie and David want to do the same
- In general: t pairs of parties, t pairwise shared keys
- Secrecy: the t shared keys should be indistinguishable to Eve* from t random keys (given all transcripts)
- Solution: run t instances of DH key-exchange protocol
  - Can use same $(\mathbb{G}, p, g)$ across instances

Why is it Secret?

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

Real world $(\mathbb{G}, p, g)$ (g^a, g^b, g^{ab})

Random world $(\mathbb{G}, p, g)$ (g^a, g^b, g^r)

Why is it Secret?

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

Real world $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$

Random world $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$

Why is it Secret?

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

Real world $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_1 $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

DDH real vs random

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_1 $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

DDH real vs random

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})(g^{a_2}, g^{b_2}, g^{a_2 b_2}) \cdots (g^{a_i}, g^{b_i}, g^{a_i b_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_1 $(\mathbb{G}, p, g)$ $(g^{a}, g^{b}, g^{r_1})(g^{a_2}, g^{b_2}, g^{a_2 b_2}) \cdots (g^{a_i}, g^{b_i}, g^{a_i b_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_2 $(\mathbb{G}, p, g)$ $(g^{a}, g^{b}, g^{r_1})(g^{a_2}, g^{b_2}, g^{r_2}) \cdots (g^{a_i}, g^{b_i}, g^{a_i b_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})(g^{a_2}, g^{b_2}, g^{r_2}) \cdots (g^{a_i}, g^{b_i}, g^{r_i}) \cdots (g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

DDH real vs random

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_1 $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_2 $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

DDH real vs random

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})(g^{a_2}, g^{b_2}, g^{a_2 b_2}) \cdots (g^{a_i}, g^{b_i}, g^{a_i b_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_1 $(\mathbb{G}, p, g)$ $(g^{a}, g^{b}, g^{r_1})(g^{a_2}, g^{b_2}, g^{a_2 b_2}) \cdots (g^{a_i}, g^{b_i}, g^{a_i b_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_2 $(\mathbb{G}, p, g)$ $(g^{a}, g^{b}, g^{r_1})(g^{a_2}, g^{b_2}, g^{r_2}) \cdots (g^{a_i}, g^{b_i}, g^{a_i b_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

$\vdots$

Hybrid H_i $(\mathbb{G}, p, g)$ $(g^{a}, g^{b}, g^{r_1})(g^{a_2}, g^{b_2}, g^{r_2}) \cdots (g^{a_i}, g^{b_i}, g^{r_i}) \cdots (g^{a_t}, g^{b_t}, g^{a_t b_t})$

$\vdots$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})(g^{a_2}, g^{b_2}, g^{r_2}) \cdots (g^{a_i}, g^{b_i}, g^{r_i}) \cdots (g^{a_t}, g^{b_t}, g^{r_t})$

Why is it Secret? HYBRID ARGUMENT, OF COURSE!

Theorem 2

Multiple instances of Diffie–Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

DDH real vs random

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_1 $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Hybrid H_2 $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

$\vdots$

Hybrid H_i $(\mathbb{G}, p, g)$ (g^{a}, g^{b}, g^{r_1}) $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

$\vdots$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

- Hybrid argument with $t+1$ hybrids $H_0, \ldots, H_t$:
  - All keys real in H_0; all keys random in H_t
  - In hybrid world H_i, the first i keys are random and the rest real
  - Hybrids H_i and H_{i+1} indistinguishable by DDH assumption $\square$

Theorem 2 ← Loss in distinguishing advantage: $1/t$!

Multiple instances of Diffie–Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof sketch.

DDH real vs random

Real world H_0	$(\mathbb{G}, p, g)$	$(g^{a_1}, g^{b_1}, g^{a_1 b_1})$	$(g^{a_2}, g^{b_2}, g^{a_2 b_2})$	$\cdots$	$(g^{a_i}, g^{b_i}, g^{a_i b_i})$	$\cdots$	$(g^{a_t}, g^{b_t}, g^{a_t b_t})$
Hybrid H_1	$(\mathbb{G}, p, g)$	(g^{a}, g^{b}, g^{r_1})	$(g^{a_2}, g^{b_2}, g^{a_2 b_2})$	$\cdots$	$(g^{a_i}, g^{b_i}, g^{a_i b_i})$	$\cdots$	$(g^{a_t}, g^{b_t}, g^{a_t b_t})$
Hybrid H_2	$(\mathbb{G}, p, g)$	(g^{a}, g^{b}, g^{r_1})	$(g^{a_2}, g^{b_2}, g^{r_2})$	$\cdots$	$(g^{a_i}, g^{b_i}, g^{a_i b_i})$	$\cdots$	$(g^{a_t}, g^{b_t}, g^{a_t b_t})$
$\vdots$					$\vdots$		
Hybrid H_i	$(\mathbb{G}, p, g)$	(g^{a}, g^{b}, g^{r_1})	$(g^{a_2}, g^{b_2}, g^{r_2})$	$\cdots$	$(g^{a_i}, g^{b_i}, g^{r_i})$	$\cdots$	$(g^{a_t}, g^{b_t}, g^{a_t b_t})$
$\vdots$					$\vdots$		
Random world H_t	$(\mathbb{G}, p, g)$	$(g^{a_1}, g^{b_1}, g^{r_1})$	$(g^{a_2}, g^{b_2}, g^{r_2})$	$\cdots$	$(g^{a_i}, g^{b_i}, g^{r_i})$	$\cdots$	$(g^{a_t}, g^{b_t}, g^{r_t})$

- Hybrid argument with $t+1$ hybrids $H_0, \ldots, H_t$:
  - All keys real in H_0; all keys random in H_t
  - In hybrid world H_i, the first i keys are random and the rest real
  - Hybrids H_i and H_{i+1} indistinguishable by DDH assumption □

But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.

$\square$

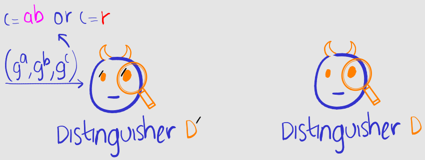
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



$\square$

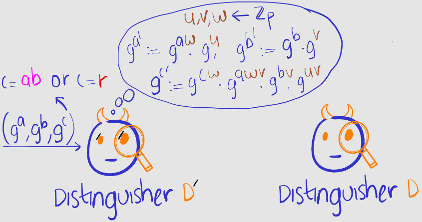
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



$\square$

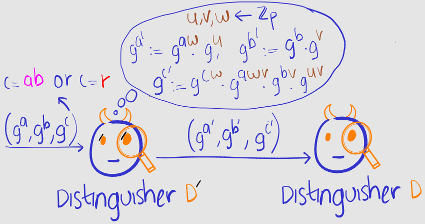
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow \exists D$ against random instance.



$\square$

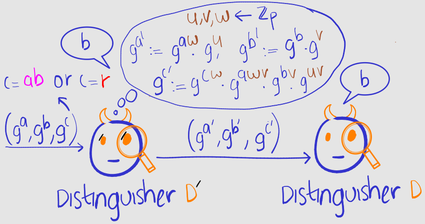
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



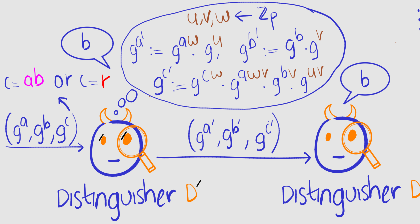
$\square$

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



Analysis

- case 1) $c = ab$ (real DDH) $\Rightarrow$
  $c' = abw + awv + bv + uv = (aw+u)(b+v) = a'b'$

$\square$

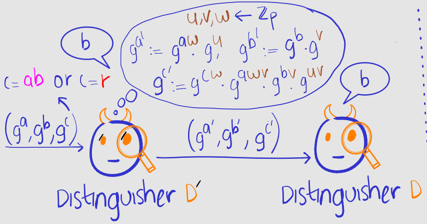
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists$D$'$ against given instance $\Leftarrow$ $\exists$D against random instance.



Analysis

- case 1) $c = ab$ (real DDH) $\Rightarrow$ real DDH $\Uparrow$

  $c' = abw + awv + bv + uv = (aw+u)(b+v) = a'b'$

$\square$

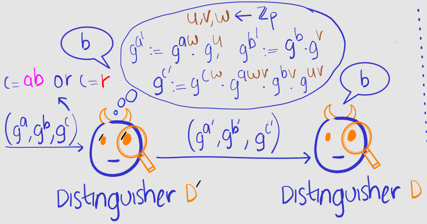
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



Analysis

real DDH $\Uparrow$

- case I) $c = ab$ (real DDH) $\Rightarrow$

  $c' = abw + awv + bv + uv = (aw+u)(b+v) = a'b'$

- case II) $c = r$ (random DDH) $\Rightarrow$

  $c' = rw + awv + bv + uv$

$\square$

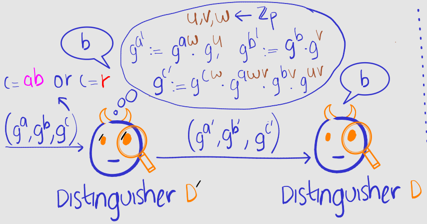
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



Analysis

real DDH
$\Uparrow$

- Case I) $c = ab$ (real DDH) $\Rightarrow$

  $c' = abw + awv + bv + uv = (aw+u)(b+v) = a'b'$

- Case II) $c = r$ (random DDH) $\Rightarrow$

  $c' = rw + awv + bv + uv$ $\Rightarrow$ random DDH

$\square$

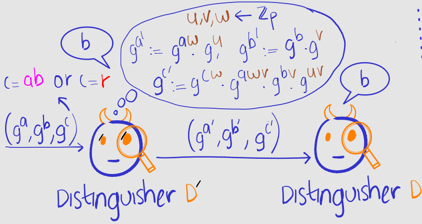
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow \exists D$ against random instance.



Analysis

- case I) $c = ab$ (real DDH) $\Rightarrow$ real DDH $\Uparrow$
  $c' = abw + awv + bv + uv = (aw+u)(b+v) = a'b'$
- case II) $c = r$ (random DDH) $\Rightarrow$
  $c' = rw + awv + bv + uv \Rightarrow$ random DDH
- Since D' mimics D, it distinguishes with same probability as D

$\square$

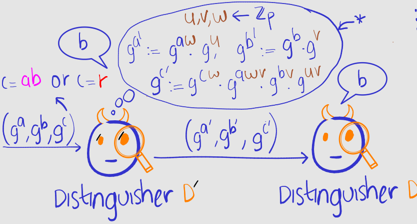
But We Can Do Better! Random Self-Reducibility...

- Random self-reducibility for DDH over $(\mathbb{G}, p, g)$:
  1. Given instance of DDH $\mapsto$ random instance of DDH
  2. Solve given instance of DDH $\Leftarrow$ solve random instance of DDH

Claim 1

The DDH problem over $\mathbb{G}$ is random self-reducible

Proof. $\exists D'$ against given instance $\Leftarrow$ $\exists D$ against random instance.



Analysis

- case I) $c = ab$ (real DDH) $\Rightarrow$ real DDH $\Uparrow$
  $c' = abw + awv + bv + uv = (aw+u)(b+v) = a'b'$
- case II) $c = r$ (random DDH) $\Rightarrow$
  $c' = rw + awv + bv + uv$ $\Rightarrow$ random DDH
- Since D' mimics D, it distinguishes with same probability as D

$\square$

Exercise 6

Is the DLog problem random self-reducible? What about CDH?

But We Can Do Better! Random Self-Reducibility...

Theorem 3 ← no loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

$\square$

Theorem 3 ← no Loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

□

But We Can Do Better! Random Self-Reducibility...

Theorem 3 ← no Loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

DDH

Key exchange

Distinguisher D'

Eve*

$\square$

But We Can Do Better! Random Self-Reducibility...

Theorem 3 ← no loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

DDH

Key exchange

$c = ab$ or $c = r$

$(g^a, g^b, g^c) \longrightarrow$

Distinguisher D'

Eve*

$\square$

But We Can Do Better! Random Self-Reducibility...

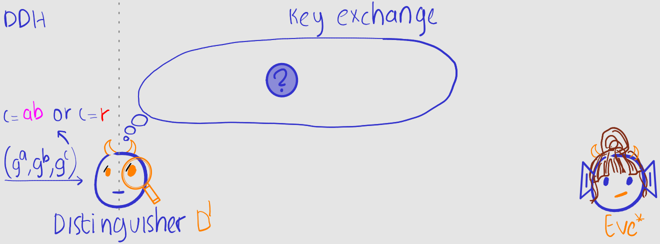
Theorem 3 ← no loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$



□

Theorem 3 ← no Loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$

DDH

Key exchange

$\{u_i, v_i, w_i\}_{i\in[1,t]} \leftarrow \mathbb{Z}_p$

$(g^a, g^b, g^c) \xrightarrow[*]{u_i, v_i, w_i} (g^{a_i'}, g^{b_i'}, g^{c_i'})$

$c = ab$ or $c = r$

(g^a, g^b, g^c)

Distinguisher D'

Eve*

□

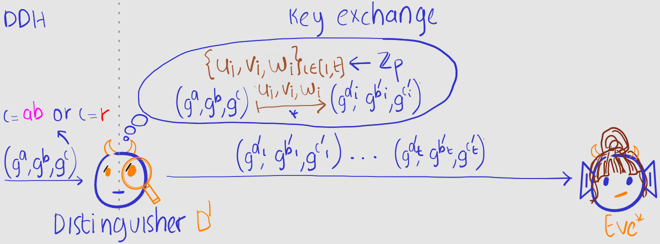
Theorem 3 ← no Loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$



□

But We Can Do Better! Random Self-Reducibility...

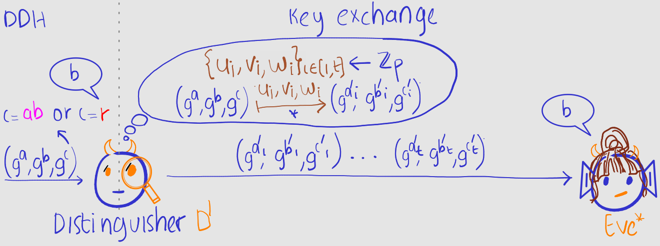
Theorem 3 ← no Loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$



$\square$

But We Can Do Better! Random Self-Reducibility...

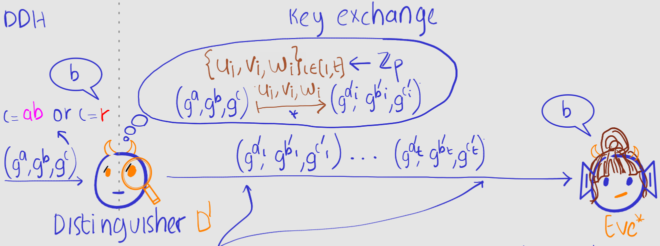
Theorem 3 ← no Loss in distinguishing advantage!

Multiple instances of Diffie-Hellman key-exchange is secret against eavesdroppers under the DDH assumption in $\mathbb{G}$ w.r.to S.

Proof, using random self-reducibility.

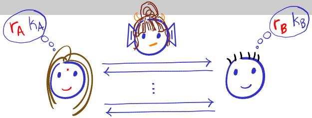
Real world H_0 $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{a_1 b_1})$ $(g^{a_2}, g^{b_2}, g^{a_2 b_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{a_i b_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{a_t b_t})$

Random world H_t $(\mathbb{G}, p, g)$ $(g^{a_1}, g^{b_1}, g^{r_1})$ $(g^{a_2}, g^{b_2}, g^{r_2})$ $\cdots$ $(g^{a_i}, g^{b_i}, g^{r_i})$ $\cdots$ $(g^{a_t}, g^{b_t}, g^{r_t})$



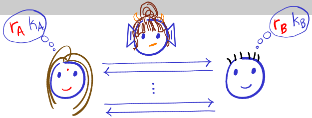
Analysis: If $c=ab$, then all t instances real; If $c=r$, then all t instances random □

To Recap Today's Lecture

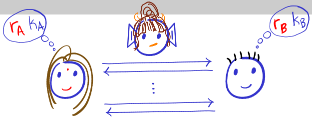


- Task 3: sharing key in presence of eavesdropper
  - Modelled key exchange setting and security

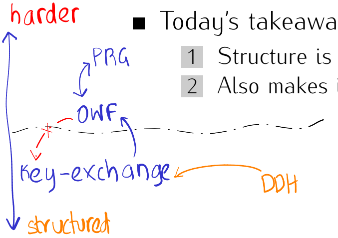
To Recap Today's Lecture



- Task 3: sharing key in presence of eavesdropper
  - Modelled key exchange setting and security
  - Diffie-Hellman key exchange protocol
    - Based security on the DDH assumption
  - Studied multi-instance Diffie-Hellman key exchange
    - First proof using hybrid argument
    - Second proof beats hybrid argument via random self-reducibility



- Task 3: sharing key in presence of eavesdropper
  - Modelled key exchange setting and security
  - Diffie-Hellman key exchange protocol
    - Based security on the DDH assumption
  - Studied multi-instance Diffie-Hellman key exchange
    - First proof using hybrid argument
    - Second proof beats hybrid argument via random self-reducibility



- Today's takeaway: structure vs hardness
  1. Structure is useful for protocol design and proofs
  2. Also makes it susceptible to algorithms

Next Lecture

- Task 4: public-key encryption (PKE)
  - Syntax and security
  - Relationship with key-exchange
  - Basic number theory
  - Goldwasser-Micali PKE

References

1. [KL14, Chapter 11] for details on this lecture.
2. Read the seminal paper by Diffie and Hellman [DH76] for a description of the namesake key-exchange.
3. Boneh's survey [Bon98] is an excellent source on the DDH problem.
4. Random self-reducibility was first studied in [BM84]. Refer to [FF93] to read more. RSR of the DDH problem were studied in [Sta96, NR04].

Manuel Blum and Silvio Micali.
How to generate cryptographically strong sequences of pseudo-random bits.
SIAM J. Comput., 13(4):850–864, 1984.

Dan Boneh.
The decision diffie-hellman problem.
In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer, 1998.

Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Trans. Inf. Theory, 22(6):644–654, 1976.

Joan Feigenbaum and Lance Fortnow.
Random-self-reducibility of complete sets.
SIAM J. Comput., 22(5):994–1005, 1993.

Jonathan Katz and Yehuda Lindell.
Introduction to Modern Cryptography (3rd ed.).
Chapman and Hall/CRC, 2014.

Moni Naor and Omer Reingold.
Number-theoretic constructions of efficient pseudo-random functions.
J. ACM, 51(2):231–262, 2004.