Diffie–Hellman Key Exchange from Commutativity to Group Laws

Dung Hoang Duong

UNIVERSITY OF WOLLONGONG AUSTRALIA

Youming Qiao

UNIVERSITY OF TECHNOLOGY SYDNEY

Chuanqi Zhang

UNIVERSITY OF TECHNOLOGY SYDNEY

This work has been accepted to ITCS 2026. For more details, please refer to our preprint at https://eprint.iacr.org/2025/1677.pdf

Outline

- Review the classical Diffie–Hellman key exchange.

Outline

- Review the classical Diffie–Hellman key exchange.
- Propose our group action-based key exchange framework.

Outline

- Review the classical Diffie–Hellman key exchange.
- Propose our group action-based key exchange framework.
- Instantiate the framework by linear code equivalence problems.

What is key exchange?

- Key exchange: a public-key protocol allowing two parties to establish a shared secret over an insecure channel.

What is key exchange?

- Key exchange: a public-key protocol allowing two parties to establish a shared secret over an insecure channel.
    - The shared secret is computed from the combination of a public key and one's private key.

What is key exchange?

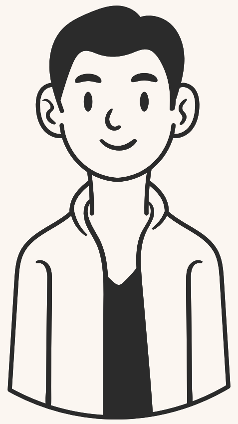
- Key exchange: a public-key protocol allowing two parties to establish a shared secret over an insecure channel.
    - The shared secret is computed from the combination of a public key and one's private key.
    - An adversary can eavesdrop on all transmitted messages.

What is key exchange?

- Key exchange: a public-key protocol allowing two parties to establish a shared secret over an insecure channel.
  - The shared secret is computed from the combination of a public key and one's private key.
  - An adversary can eavesdrop on all transmitted messages.
- Application: HTTPS, VPN, and messaging services.

Diffie–Hellman key exchange protocol

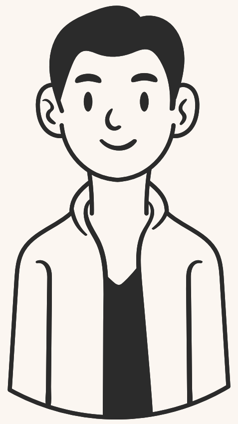
Alice



Bob

Diffie–Hellman key exchange protocol

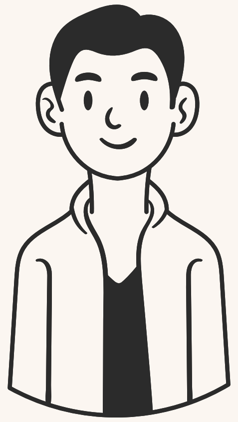
pk : prime p and generator γ of a cyclic group C_p



Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p

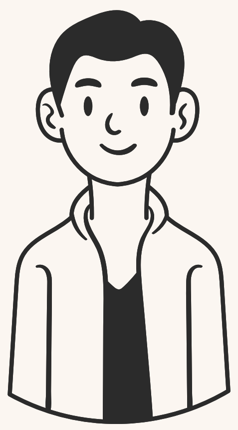


Bob

$a \xleftarrow{\$} \mathbb{Z}_p^*$

Diffie–Hellman key exchange protocol

pk : prime p and generator γ of a cyclic group C_p



Alice

Bob

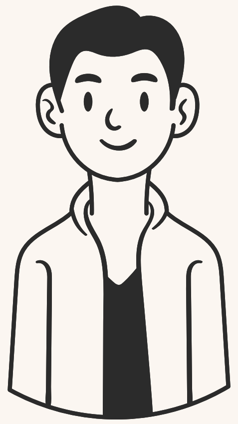
$a \xleftarrow{\$} \mathbb{Z}_p^*$

$A = \gamma^a$

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p

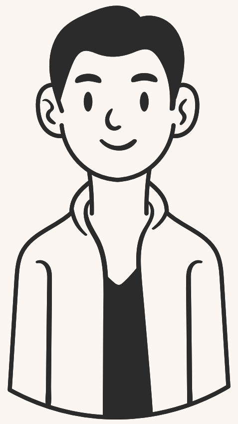


Bob

Alice	Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$	$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$	$B = \gamma^b$

Diffie–Hellman key exchange protocol

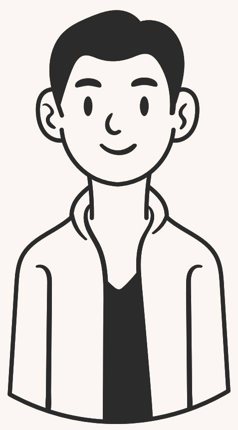
pk : prime p and generator γ of a cyclic group C_p



Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$	$\xrightarrow{\quad A \quad}$	$B = \gamma^b$

Diffie–Hellman key exchange protocol

pk : prime p and generator γ of a cyclic group C_p

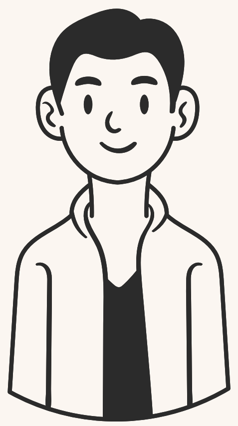


Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$		$B = \gamma^b$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

$a \xleftarrow{\$} \mathbb{Z}_p^*$

$A = \gamma^a$

$b \xleftarrow{\$} \mathbb{Z}_p^*$

$B = \gamma^b$

$$\xrightarrow{\quad A \quad}$$

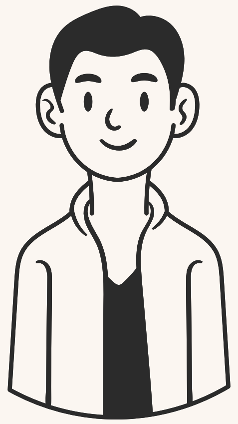
$$\xleftarrow{\quad B \quad}$$

$\mathbf{key} = B^a$

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



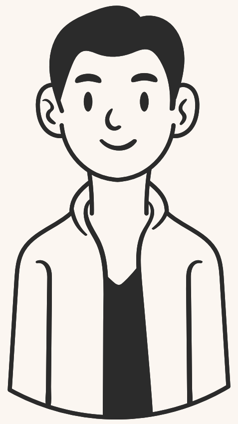
Bob

Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$		$B = \gamma^b$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B^a$		$\mathbf{key} = A^b$

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

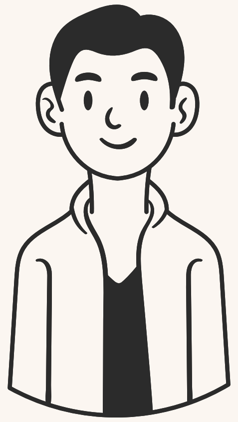
Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$	$\xrightarrow{\quad A \quad}$	$B = \gamma^b$
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B^a$		$\mathbf{key} = A^b$

Correctness: $A^b = \gamma^{ab} = \gamma^{ba} = B^a$.

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

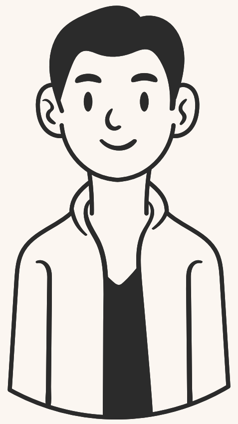
Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$	$\xrightarrow{\quad A \quad}$	$B = \gamma^b$
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B^a$		$\mathbf{key} = A^b$

Correctness: $A^b = \gamma^{ab} = \gamma^{ba} = B^a$.

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

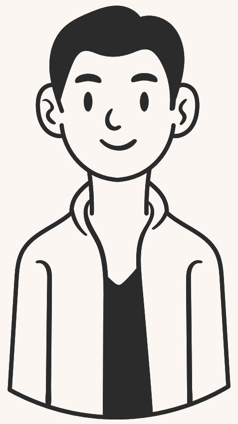
Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$	$\xrightarrow{\quad A \quad}$	$B = \gamma^b$
$\mathbf{key} = B^a$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A^b$

Correctness: $A^b = \gamma^{ab} = \gamma^{ba} = B^a$.

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

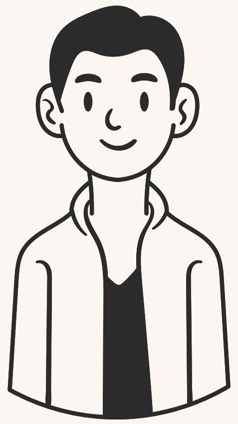
Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$		$B = \gamma^b$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	
$\textbf{key} = B^a$		$\textbf{key} = A^b$

Correctness: $A^b = \gamma^{ab} = \gamma^{ba} = B^a$.

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

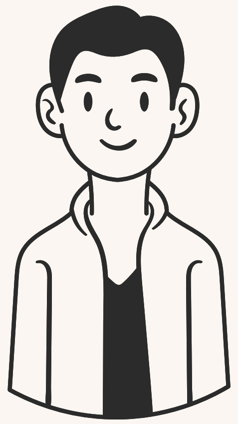
Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$	Given γ, γ^a, it's hard to solve a!	$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$	$\xrightarrow{\quad A \quad}$	$B = \gamma^b$
$\mathbf{key} = B^a$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A^b$

Correctness: $A^b = \gamma^{ab} = \gamma^{ba} = B^a$.

Diffie–Hellman key exchange protocol

Alice

pk : prime p and generator γ of a cyclic group C_p



Bob

Discrete Log Assumption

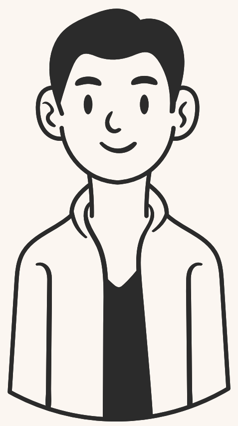
Given γ, γ^a, it's hard to solve a!

Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}_p^*$		$b \xleftarrow{\$} \mathbb{Z}_p^*$
$A = \gamma^a$		$B = \gamma^b$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	
$\textbf{key} = B^a$		$\textbf{key} = A^b$

Correctness: $A^b = \gamma^{ab} = \gamma^{ba} = B^a$.

Diffie–Hellman key exchange protocol from group action view

Alice

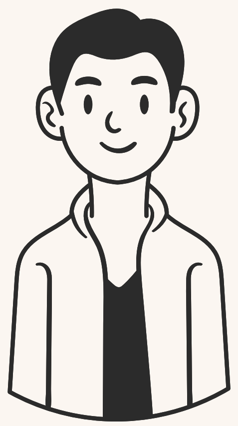


Bob

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$

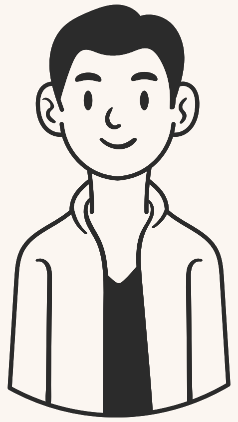


Bob

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

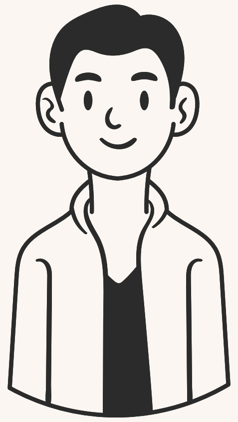
$g \xleftarrow{\$} G$

$A = s * g$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



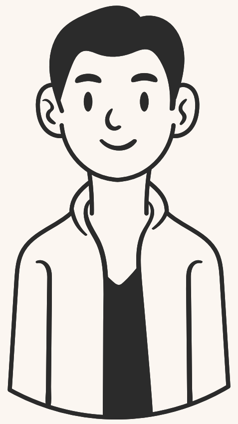
Bob

Alice	Bob
$g \xleftarrow{\$} G$	$h \xleftarrow{\$} G$
$A = s * g$	$B = s * h$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

$g \overset{\$}{\leftarrow} G$

$A = s * g$

$h \overset{\$}{\leftarrow} G$

$B = s * h$

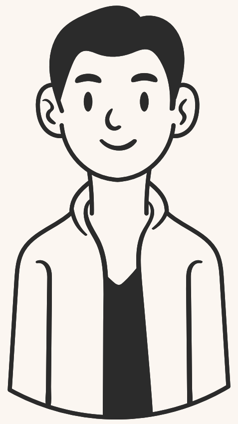
$$\xrightarrow{\quad A \quad}$$

$$\xleftarrow{\quad B \quad}$$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



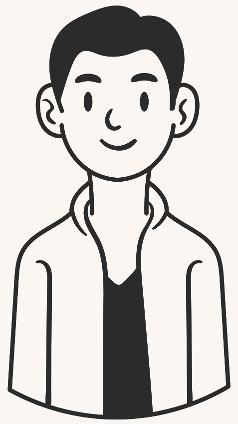
Bob

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\mathbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A * h$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

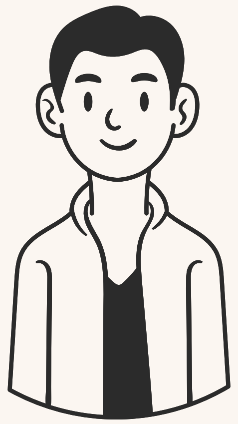
Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\mathbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A * h$

Correctness: $B * g = s * hg = s * gh = A * h.$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

$g \xleftarrow{\$} G$ $\qquad\qquad\qquad$ $h \xleftarrow{\$} G$

$A = s * g$ $\qquad\qquad\qquad$ $B = s * h$

$$\xrightarrow{\quad A \quad}$$

$$\xleftarrow{\quad B \quad}$$

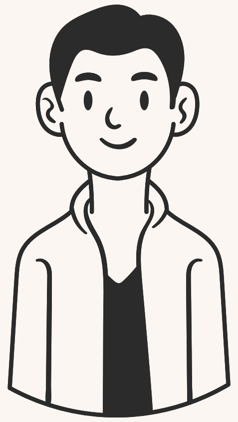
$\mathbf{key} = B * g$ $\qquad\qquad\qquad$ $\mathbf{key} = A * h$

Correctness: $B * g = s * \color{red}{hg} = s * \color{red}{gh} = A * h.$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

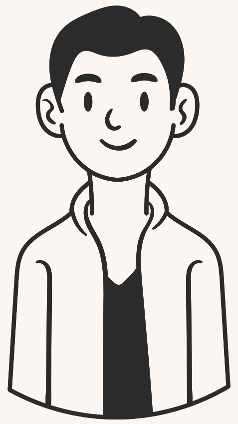
Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B * g$		$\mathbf{key} = A * h$

Correctness: $B * g = s * hg = s * gh = A * h.$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

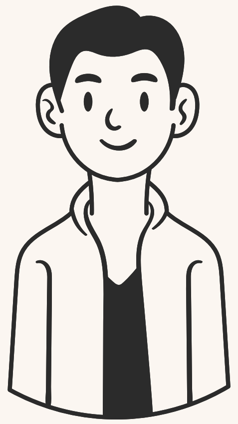
Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\textbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\textbf{key} = A * h$

Correctness: $B * g = s * hg = s * gh = A * h$.

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

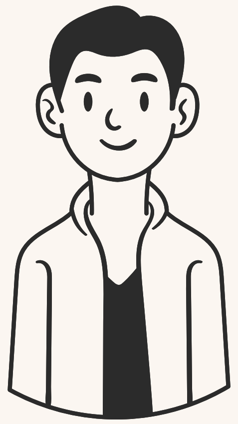
Alice		Bob
$g \xleftarrow{\$} G$	Given s, $s * g$ it's hard to solve g!	$h \xleftarrow{\$} G$
$A = s * g$		$B = s * h$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B * g$		$\mathbf{key} = A * h$

Correctness: $B * g = s * hg = s * gh = A * h$.

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

One-way Hardness Assumption[1]

Given s, $s * g$ it's hard to solve g!

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$		$B = s * h$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B * g$		$\mathbf{key} = A * h$

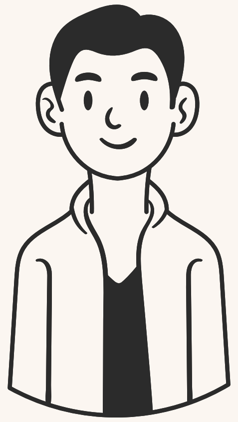
Correctness: $B * g = s * hg = s * gh = A * h.$

[1] [Brassard-Yung, *Crypto*, 90]

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

One-way Hardness Assumption[1]
Given $s, s * g$ it's hard to solve g!

$g \xleftarrow{\$} G$

$A = s * g$

$h \xleftarrow{\$} G$

$B = s * h$

$\xrightarrow{\quad A \quad}$

$\xleftarrow{\quad B \quad}$

$\mathbf{key} = B * g$

$\mathbf{key} = A * h$

Good candidate for instantiation

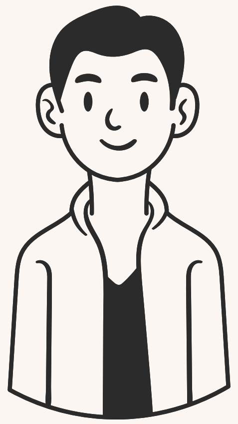
Correctness: $B * g = s * hg = s * gh = A * h.$

[1] [Brassard-Yung, *Crypto*, 90]

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

One-way Hardness Assumption[1]
Given $s, s * g$ it's hard to solve g!

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\mathbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A * h$

Correctness: $B * g = s * hg = s * gh = A * h.$

Good candidate for instantiation

$S = C_p \setminus \mathrm{id}$

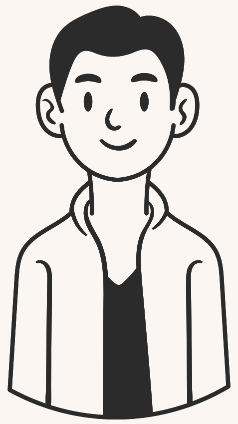
$G = \mathrm{Aut}(C_p)$

[1] [Brassard-Yung, *Crypto*, 90]

Diffie–Hellman key exchange protocol from group action view

$\mathsf{pk} : s \in S$

Alice



Bob

One-way Hardness Assumption[1]
Given s, $s * g$ it's hard to solve g!

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\textbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\textbf{key} = A * h$

Correctness: $B * g = s * hg = s * gh = A * h$.

Good candidate for instantiation

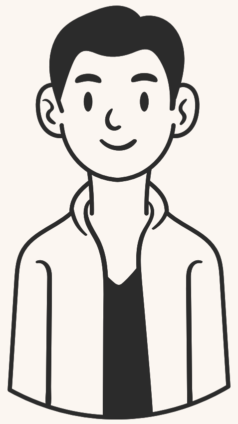
$$S = C_p \setminus \mathrm{id}$$

$$G = \mathrm{Aut}(C_p)$$

[1] [Brassard-Yung, *Crypto*, 90]

Diffie–Hellman key exchange protocol from group action view

Alice



Bob

$\mathsf{pk} : s \in S$

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$		$B = s * h$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow{\quad B \quad}$	
$\mathbf{key} = B * g$		$\mathbf{key} = A * h$

One-way Hardness Assumption[1]
Given s, $s * g$ it's hard to solve g!

Correctness: $B * g = s * hg = s * gh = A * h.$

Good candidate for instantiation

$$S = C_p \setminus \mathrm{id}$$

$$G = \mathrm{Aut}(C_p)$$

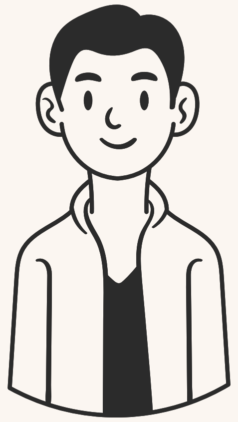
$\boxed{\mathrm{Aut}(C_p) \cong \mathbb{Z}_p^*}$

[1] [Brassard-Yung, *Crypto*, 90]

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

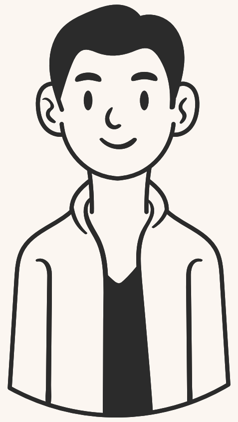
Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\textbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\textbf{key} = A * h$

Correctness: $B * g = s * {\color{red}hg} = s * {\color{red}gh} = A * h.$

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\mathbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A * h$

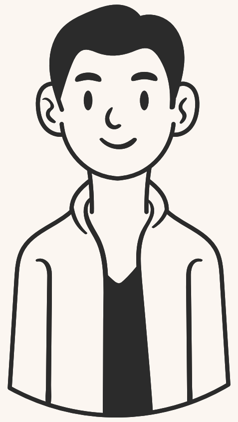
Correctness: $B * g = s * hg = s * gh = A * h.$

Beyond commutativity?

Diffie–Hellman key exchange protocol from group action view

Alice

$\mathsf{pk} : s \in S$



Bob

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
$A = s * g$	$\xrightarrow{\quad A \quad}$	$B = s * h$
$\mathbf{key} = B * g$	$\xleftarrow{\quad B \quad}$	$\mathbf{key} = A * h$

Correctness: $B * g = s * {\color{red}hg} = s * {\color{red}gh} = A * h.$

Idea: treating this as a law in a group!

Law in a group

Law in a group

A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

Law in a group

A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

- $ab = ba$ is a law in an abelian group.

Law in a group

A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

- $ab = ba$ is a law in an abelian group.

- $aba^{-1}b^{-1}cdc^{-1}d^{-1} = cdc^{-1}d^{-1}aba^{-1}b^{-1}$ is a law in a metabelian group.

Law in a group

A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

- $ab = ba$ is a law in an abelian group.

- $aba^{-1}b^{-1}cdc^{-1}d^{-1} = cdc^{-1}d^{-1}aba^{-1}b^{-1}$ is a law in a metabelian group.
  $[a, b], [c, d] = [c, d][a, b]$

Law in a group

A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

- $ab = ba$ is a law in an abelian group.

- $aba^{-1}b^{-1}cdc^{-1}d^{-1} = cdc^{-1}d^{-1}aba^{-1}b^{-1}$ is a law in a metabelian group.

- $u(a, b, c, \ldots) = v(a, b, c, \ldots)$ is a law in a group.

Law in a group

A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

- $ab = ba$ is a law in an abelian group.

- $aba^{-1}b^{-1}cdc^{-1}d^{-1} = cdc^{-1}d^{-1}aba^{-1}b^{-1}$ is a law in a metabelian group.

- $\underset{\substack{\downarrow \\ \text{word}}}{u}(a, b, c, \ldots) = v(a, b, c, \ldots)$ is a law in a group.

Law in a group

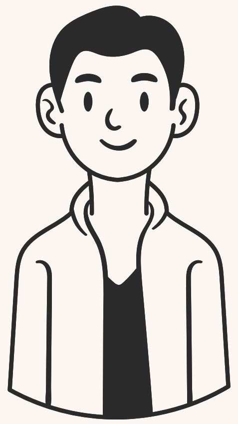
A *law* in a group G is an equation that is satisfied by any assignments of variables by group elements in G.

- $ab = ba$ is a law in an abelian group.
- $aba^{-1}b^{-1}cdc^{-1}d^{-1} = cdc^{-1}d^{-1}aba^{-1}b^{-1}$ is a law in a metabelian group.
- $u(a, b, c, \ldots) = v(a, b, c, \ldots)$ is a law in a group.

word: e.g., $a^2b^3a^{-5}c^2b^7$

Key exchange protocol for actions of groups with laws

Alice

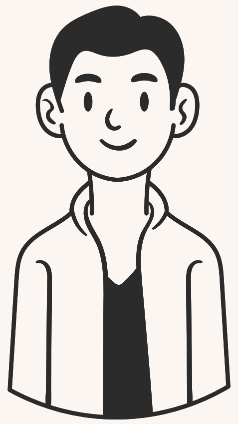


Bob

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$

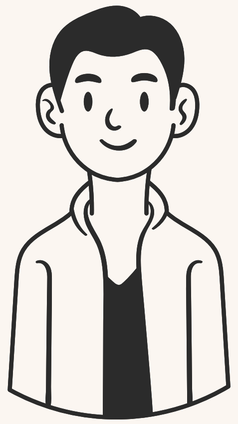


Bob

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

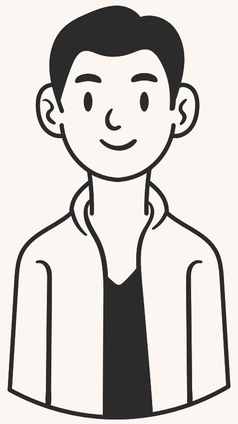
$$y^{b_1} x^{a_1} \ldots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \ldots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

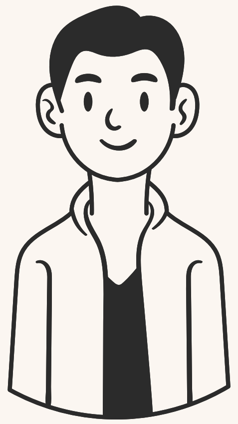
$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \ldots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \ldots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$g \xleftarrow{\$} G$

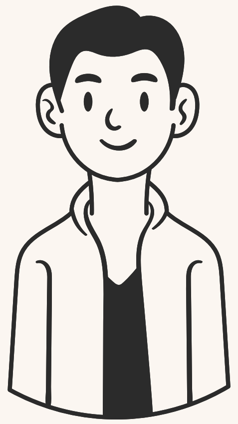
$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$g \xleftarrow{\$} G$

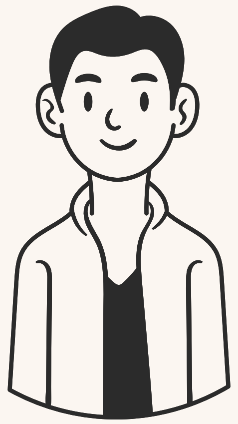
$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

$\xleftarrow{\quad t_1 \quad}$

Key exchange protocol for actions of groups with laws

Alice



Bob

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

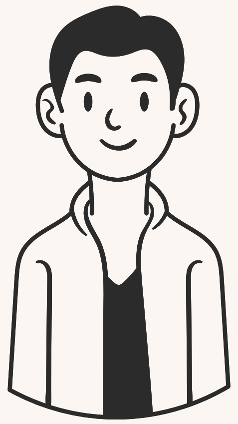
$\xleftarrow{\quad t_1 \quad}$

$s_1 = t_1 * g^{a_1}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \ldots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \ldots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

$\xleftarrow{\quad t_1 \quad}$

$s_1 = t_1 * g^{a_1}$

$\xrightarrow{\quad s_1 \quad}$

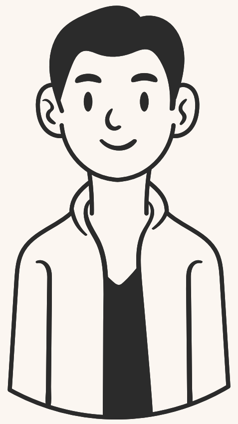
Key exchange protocol for actions of groups with laws

Alice

$$\mathsf{pk} : s_0 \in S$$

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$



Bob

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

$$\xleftarrow{\quad t_1 \quad}$$

$s_1 = t_1 * g^{a_1}$

$$\xrightarrow{\quad s_1 \quad}$$

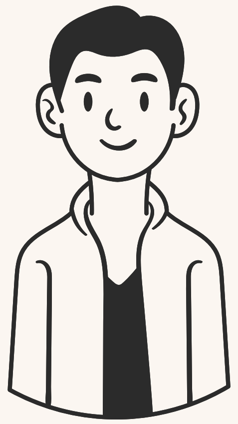
$t_2 = s_1 * h^{b_2}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

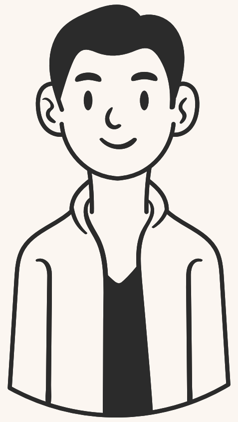


Bob

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
	$\xleftarrow{\quad t_1 \quad}$	$t_1 = s_0 * h^{b_1}$
$s_1 = t_1 * g^{a_1}$	$\xrightarrow{\quad s_1 \quad}$	
	$\xleftarrow{\quad t_2 \quad}$	$t_2 = s_1 * h^{b_2}$

Key exchange protocol for actions of groups with laws

Alice



Bob

$\mathsf{pk} : s_0 \in S$

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

Alice: $g \xleftarrow{\$} G$

Bob: $h \xleftarrow{\$} G$

Bob: $t_1 = s_0 * h^{b_1}$

$\xleftarrow{\quad t_1 \quad}$

Alice: $s_1 = t_1 * g^{a_1}$

$\xrightarrow{\quad s_1 \quad}$

Bob: $t_2 = s_1 * h^{b_2}$

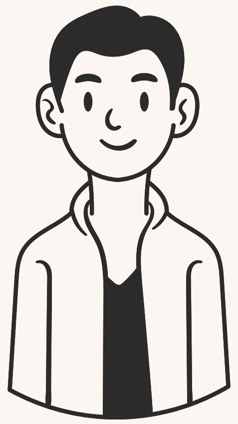
$\xleftarrow{\quad t_2 \quad}$

Alice: $s_2 = t_2 * g^{a_2}$

Key exchange protocol for actions of groups with laws

$\mathsf{pk} : s_0 \in S$

Alice



Bob

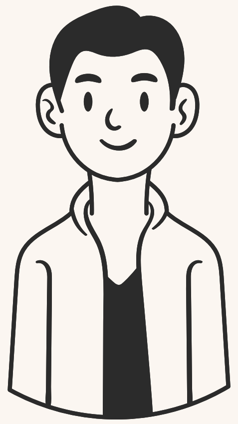
$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
	$\xleftarrow{t_1}$	$t_1 = s_0 * h^{b_1}$
$s_1 = t_1 * g^{a_1}$	$\xrightarrow{s_1}$	
	$\xleftarrow{t_2}$	$t_2 = s_1 * h^{b_2}$
$s_2 = t_2 * g^{a_2}$		
	$\vdots$	

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

$\xleftarrow{\quad t_1 \quad}$

$s_1 = t_1 * g^{a_1}$

$\xrightarrow{\quad s_1 \quad}$

$t_2 = s_1 * h^{b_2}$

$\xleftarrow{\quad t_2 \quad}$

$s_2 = t_2 * g^{a_2}$

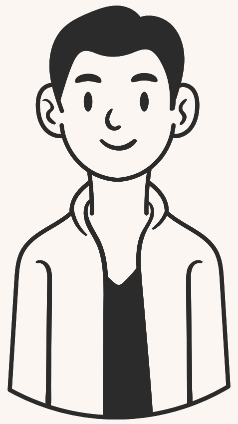
$\vdots$

$t_k = s_{k-1} * h^{b_k}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

$\xleftarrow{\quad t_1 \quad}$

$s_1 = t_1 * g^{a_1}$

$\xrightarrow{\quad s_1 \quad}$

$t_2 = s_1 * h^{b_2}$

$\xleftarrow{\quad t_2 \quad}$

$s_2 = t_2 * g^{a_2}$

$\vdots$

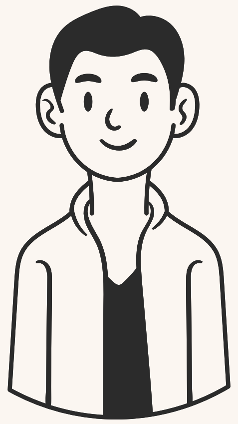
$t_k = s_{k-1} * h^{b_k}$

$\xleftarrow{\quad t_k \quad}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \ldots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \ldots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

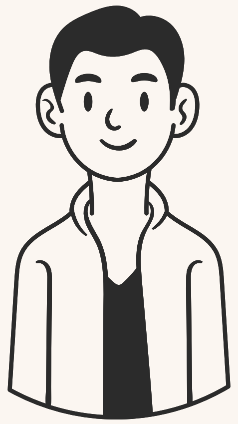
Alice		Bob
$g \xleftarrow{\$} G$		$h \xleftarrow{\$} G$
	$\xleftarrow{\quad t_1 \quad}$	$t_1 = s_0 * h^{b_1}$
$s_1 = t_1 * g^{a_1}$	$\xrightarrow{\quad s_1 \quad}$	
	$\xleftarrow{\quad t_2 \quad}$	$t_2 = s_1 * h^{b_2}$
$s_2 = t_2 * g^{a_2}$		
	$\vdots$	
	$\xleftarrow{\quad t_k \quad}$	$t_k = s_{k-1} * h^{b_k}$

key : $s_k = t_k * g^{a_k}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$t_1 = s_0 * h^{b_1}$

$\xleftarrow{\quad t_1 \quad}$

$s_1 = t_1 * g^{a_1}$

$\xrightarrow{\quad s_1 \quad}$

$t_2 = s_1 * h^{b_2}$

$\xleftarrow{\quad t_2 \quad}$

$s_2 = t_2 * g^{a_2}$

$\vdots$

$t_k = s_{k-1} * h^{b_k}$

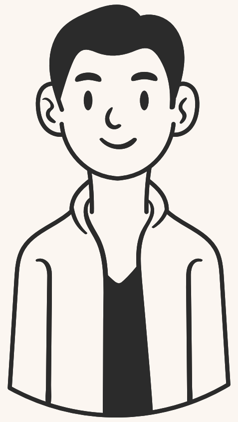
$\xleftarrow{\quad t_k \quad}$

key : $s_k = t_k * g^{a_k} = s_0 * h^{b_1}g^{a_1}\dots h^{b_k}g^{a_k}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

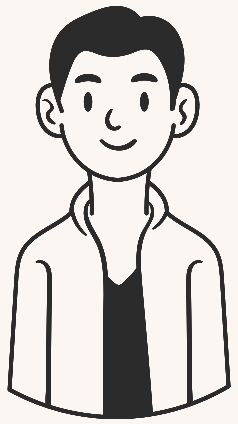
for any $x, y \in G$

$s_1' = s_0 * g^{c_1}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

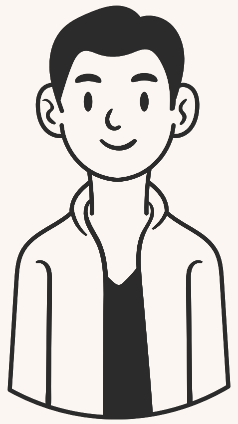
for any $x, y \in G$

$s_1' = s_0 * g^{c_1}$

$\xrightarrow{s_1'}$

Key exchange protocol for actions of groups with laws

Alice



Bob

$\mathsf{pk}: s_0 \in S$

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

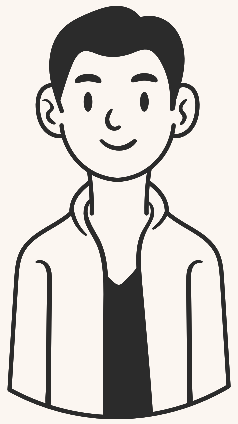
$s_1' = s_0 * g^{c_1}$

$\xrightarrow{\;s_1'\;}$

$t_1' = s_1' * h^{d_1}$

Key exchange protocol for actions of groups with laws

Alice



Bob

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$s'_1 = s_0 * g^{c_1}$

$$\xrightarrow{\quad s'_1 \quad}$$

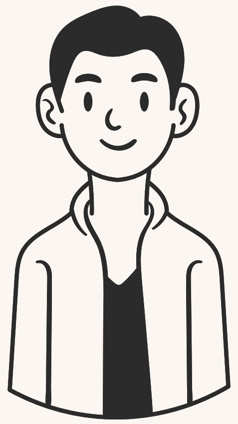
$$\xleftarrow{\quad t'_1 \quad}$$

$t'_1 = s'_1 * h^{d_1}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$s_1' = s_0 * g^{c_1}$

$\xrightarrow{\quad s_1' \quad}$

$t_1' = s_1' * h^{d_1}$

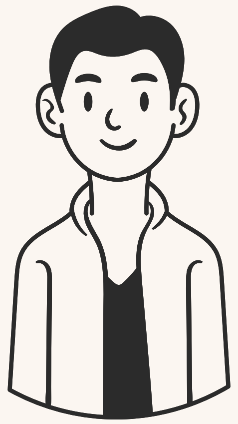
$\xleftarrow{\quad t_1' \quad}$

$s_2' = t_1' * g^{c_2}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

$s_1' = s_0 * g^{c_1}$

$\xrightarrow{s_1'}$

$\xleftarrow{t_1'}$

$t_1' = s_1' * h^{d_1}$

$s_2' = t_1' * g^{c_2}$

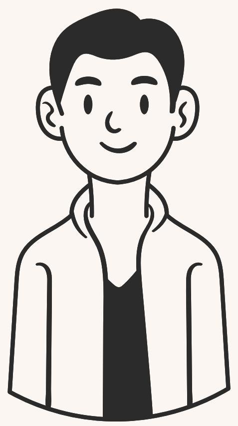
$\xrightarrow{s_2'}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$



Bob

$s_1' = s_0 * g^{c_1}$

$$\xrightarrow{\quad s_1' \quad}$$

$t_1' = s_1' * h^{d_1}$

$$\xleftarrow{\quad t_1' \quad}$$

$s_2' = t_1' * g^{c_2}$

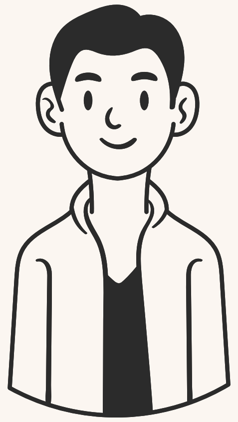
$$\xrightarrow{\quad s_2' \quad}$$

$t_2' = s_2' * h^{d_2}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$s'_1 = s_0 * g^{c_1}$

$$\xrightarrow{\quad s'_1 \quad}$$

$t'_1 = s'_1 * h^{d_1}$

$$\xleftarrow{\quad t'_1 \quad}$$

$s'_2 = t'_1 * g^{c_2}$

$$\xrightarrow{\quad s'_2 \quad}$$

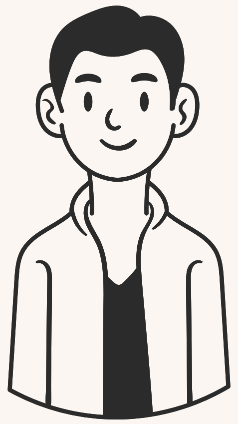
$t'_2 = s'_2 * h^{d_2}$

$$\vdots$$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

$s'_1 = s_0 * g^{c_1}$

$\xrightarrow{\quad s'_1 \quad}$

$t'_1 = s'_1 * h^{d_1}$

$\xleftarrow{\quad t'_1 \quad}$

$s'_2 = t'_1 * g^{c_2}$

$\xrightarrow{\quad s'_2 \quad}$

$t'_2 = s'_2 * h^{d_2}$

$\vdots$

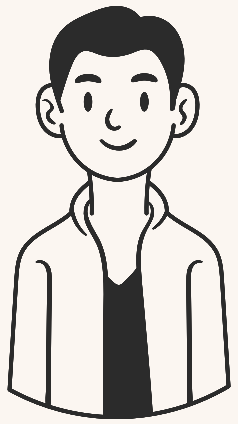
$s'_\ell = t'_{\ell-1} * g^{d_\ell}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$



Bob

$s_1' = s_0 * g^{c_1}$ $\xrightarrow{s_1'}$

$\xleftarrow{t_1'}$ $t_1' = s_1' * h^{d_1}$

$s_2' = t_1' * g^{c_2}$ $\xrightarrow{s_2'}$

$t_2' = s_2' * h^{d_2}$

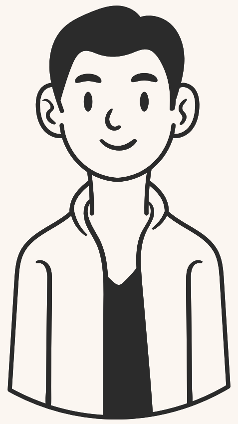
$\vdots$

$s_\ell' = t_{\ell-1}' * g^{d_\ell}$ $\xrightarrow{s_\ell'}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

$s_1' = s_0 * g^{c_1}$

$$\xrightarrow{\quad s_1' \quad}$$

$t_1' = s_1' * h^{d_1}$

$$\xleftarrow{\quad t_1' \quad}$$

$s_2' = t_1' * g^{c_2}$

$$\xrightarrow{\quad s_2' \quad}$$

$t_2' = s_2' * h^{d_2}$

$\vdots$

$s_\ell' = t_{\ell-1}' * g^{d_\ell}$

$$\xrightarrow{\quad s_\ell' \quad}$$

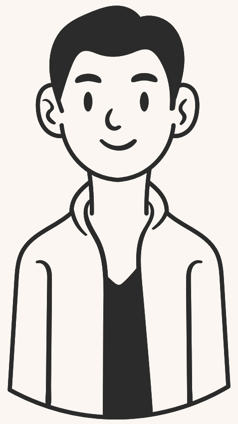
key : $t_\ell' = s_\ell' * h^{d_\ell}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = {\color{red}x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}}$$
for any $x, y \in G$



Bob

$s_1' = s_0 * g^{c_1}$

$\xrightarrow{\quad s_1' \quad}$

$t_1' = s_1' * h^{d_1}$

$\xleftarrow{\quad t_1' \quad}$

$s_2' = t_1' * g^{c_2}$

$\xrightarrow{\quad s_2' \quad}$

$t_2' = s_2' * h^{d_2}$

$\vdots$

$s_\ell' = t_{\ell-1}' * g^{d_\ell}$

$\xrightarrow{\quad s_\ell' \quad}$

$\mathbf{key} : t_\ell' = s_\ell' * h^{d_\ell} = s_0 * {\color{red}g^{c_1}h^{d_1}\dots g^{c_\ell}h^{d_\ell}}$

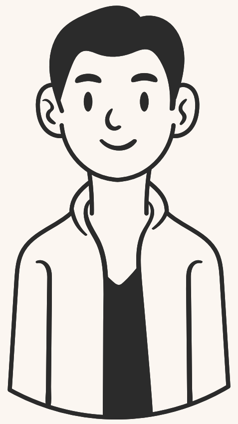
Key exchange protocol for actions of groups with laws

Alice

$g \xleftarrow{\$} G$

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$



Bob

$h \xleftarrow{\$} G$

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

$\vdots$

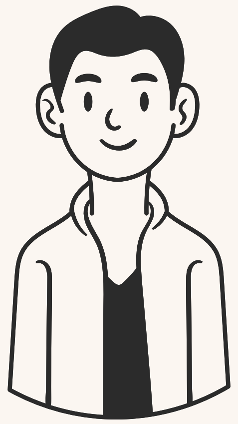
$\vdots$

key : $s_k = t_k * g^{a_k} = s_0 * h^{b_1} g^{a_1} \dots h^{b_k} g^{a_k}$

key : $t'_\ell = s'_\ell * h^{d_\ell} = s_0 * g^{c_1} h^{d_1} \dots g^{c_\ell} h^{d_\ell}$

Key exchange protocol for actions of groups with laws

$\mathsf{pk} : s_0 \in S$



$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

$\vdots$

$\vdots$

This can be generalised to the multi-variable case!

key : $s_k = t_k * g^{a_k} = s_0 * h^{b_1} g^{a_1} \dots h^{b_k} g^{a_k}$

key : $t'_\ell = s'_\ell * h^{d_\ell} = s_0 * g^{c_1} h^{d_1} \dots g^{c_\ell} h^{d_\ell}$

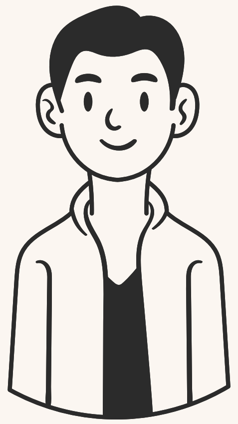
Key exchange protocol for actions of groups with laws

Alice

$g \xleftarrow{\$} G$

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$



Bob

$h \xleftarrow{\$} G$

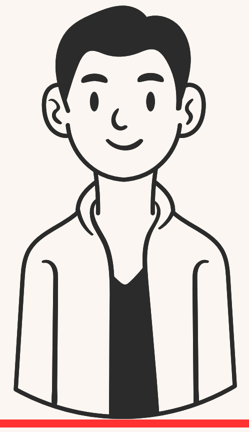
$$\longrightarrow$$
$$\longleftarrow$$
$$\longrightarrow$$
$$\vdots$$
$$\vdots$$

key : $s_k = t_k * g^{a_k} = s_0 * h^{b_1} g^{a_1} \dots h^{b_k} g^{a_k}$

key : $t'_\ell = s'_\ell * h^{d_\ell} = s_0 * g^{c_1} h^{d_1} \dots g^{c_\ell} h^{d_\ell}$

Key exchange protocol for actions of groups with laws

Alice



Bob

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

$\vdots$

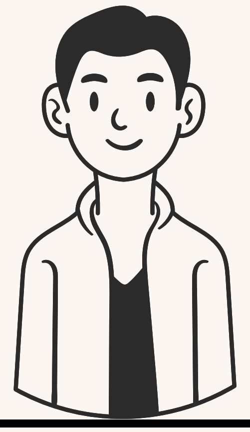
$\vdots$

key : $s_k = t_k * g^{a_k} = s_0 * h^{b_1} g^{a_1} \dots h^{b_k} g^{a_k}$

key : $t'_\ell = s'_\ell * h^{d_\ell} = s_0 * g^{c_1} h^{d_1} \dots g^{c_\ell} h^{d_\ell}$

Key exchange protocol for actions of groups with laws

Alice



Bob

$\mathsf{pk} : s_0 \in S$

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$
for any $x, y \in G$

length of a law $\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$

$g \xleftarrow{\$} G$

$h \xleftarrow{\$} G$

Multi-variable laws can be turned into 2-variable laws by a polynomial blow-up in length [Bradford-Thom, *TAMS*, 19]

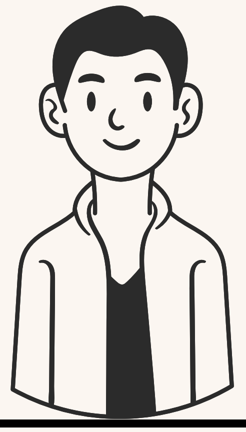
key : $s_k = t_k * g^{a_k} = s_0 * h^{b_1} g^{a_1} \dots h^{b_k} g^{a_k}$

key : $t'_\ell = s'_\ell * h^{d_\ell} = s_0 * g^{c_1} h^{d_1} \dots g^{c_\ell} h^{d_\ell}$

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

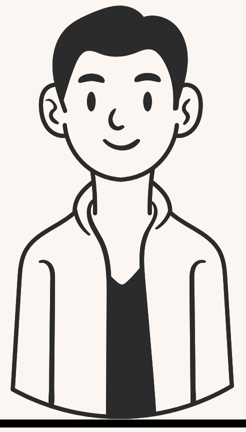
$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

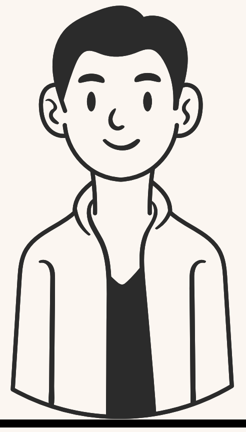
What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\ldots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\ldots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\longrightarrow \sum_{i=1}^{k}(a_i+b_i)+\sum_{i=1}^{\ell}(c_i+d_i)$$

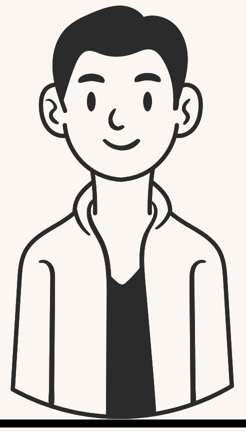
What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$

length of a law
$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

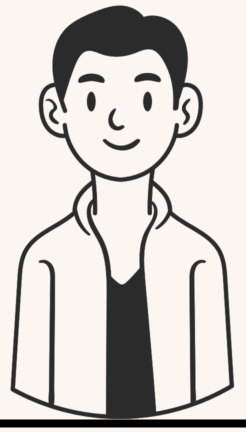
What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Key exchange protocol for actions of groups with laws


Alice

pk : $s_0 \in S$


Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

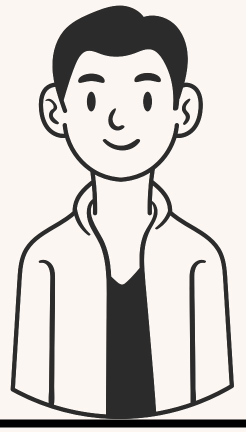
1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Metabelian groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i+b_i) + \sum_{i=1}^{\ell}(c_i+d_i)$$

What kind of (non-abelian) Group should we choose?

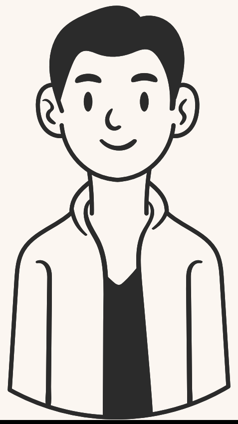
1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Metabelian groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i+b_i)+\sum_{i=1}^{\ell}(c_i+d_i)$$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)

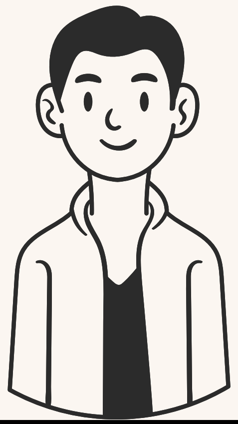
2. With a law whose length is as short as possible

Metabelian groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\ldots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\ldots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$

length of a law
$$\sum_{i=1}^{k}(a_i+b_i)+\sum_{i=1}^{\ell}(c_i+d_i)$$

What kind of (non-abelian) Group should we choose?

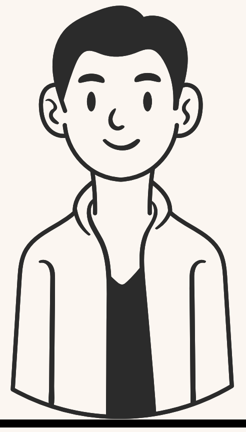
1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Metabelian groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\ldots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\ldots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

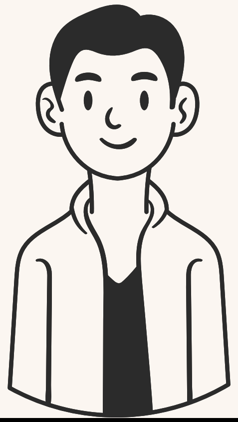
1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Highly non-abelian groups,
e.g., general linear groups

Key exchange protocol for actions of groups with laws

Alice

$\mathsf{pk} : s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i+b_i)+\sum_{i=1}^{\ell}(c_i+d_i)$$

What kind of (non-abelian) Group should we choose?

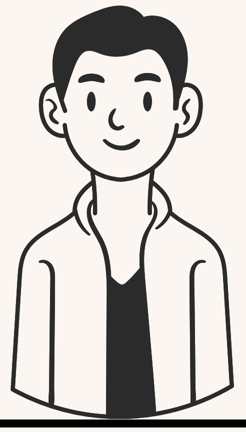
1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Highly non-abelian groups,
e.g., general linear groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1} x^{a_1} \dots y^{b_k} x^{a_k} = x^{c_1} y^{d_1} \dots x^{c_\ell} y^{d_\ell}$$

for any $x, y \in G$

length of a law $\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

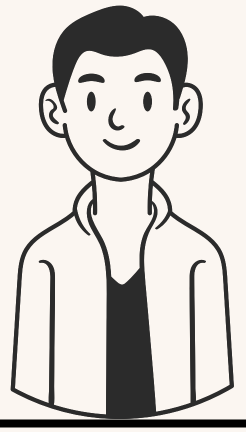
Highly non-abelian groups,

e.g., general linear groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

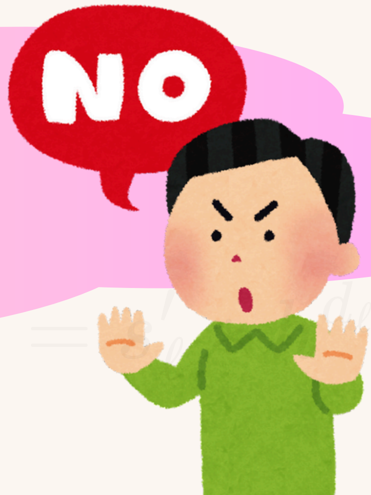
length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Highly non-abelian groups,
e.g., general linear groups

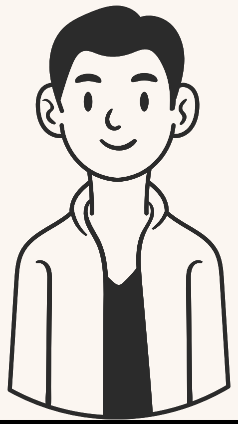


[Bradford-Thom, *JEMS*, 24]
The length could be exponentially long!

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

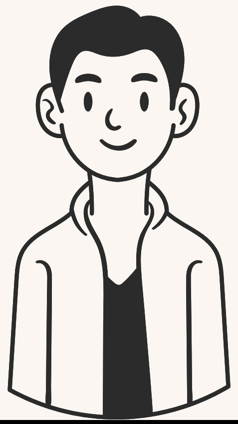
1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

Highly non-abelian groups,
e.g., symmetric groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

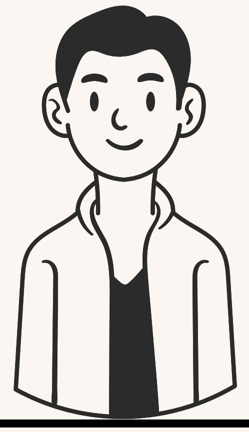
1. One-way hardness (with multiple copies) ✔
2. With a law whose length is as short as possible

Highly non-abelian groups,
e.g., symmetric groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. With a law whose length is as short as possible

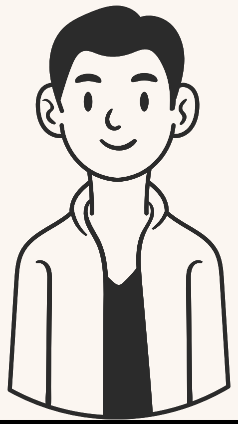
Highly non-abelian groups,

e.g., symmetric groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\ldots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\ldots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

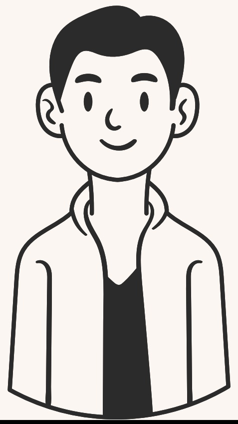
1. One-way hardness (with multiple copies)
2. There is a short law with high probability

Highly non-abelian groups,
e.g., symmetric groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i + b_i) + \sum_{i=1}^{\ell}(c_i + d_i)$$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. There is a short law with high probability

$$(xy)^{\lceil n/2 \rceil} = (y^{-1}x^{-1})^{\lfloor n/2 \rfloor}$$

i.e., $(xy)^n = \mathrm{id}$

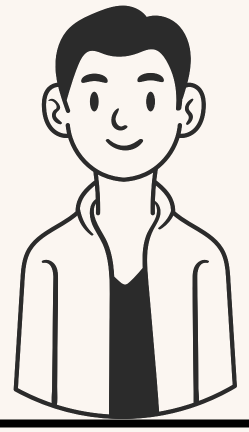
Highly non-abelian groups,

e.g., symmetric groups

Key exchange protocol for actions of groups with laws


Alice

pk : $s_0 \in S$


Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$
for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i+b_i)+\sum_{i=1}^{\ell}(c_i+d_i)$$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. There is a short law with high probability

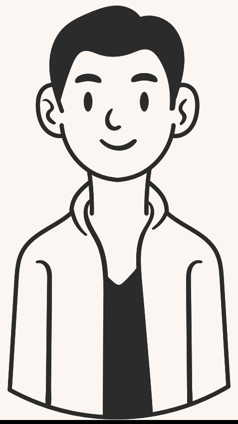
$(xy)^{\lceil n/2 \rceil} = (y^{-1}x^{-1})^{\lfloor n/2 \rfloor}$
i.e., $(xy)^n = \mathrm{id}$

Highly non-abelian groups,
e.g., symmetric groups

Key exchange protocol for actions of groups with laws

Alice

pk : $s_0 \in S$



Bob

$$y^{b_1}x^{a_1}\dots y^{b_k}x^{a_k} = x^{c_1}y^{d_1}\dots x^{c_\ell}y^{d_\ell}$$

for any $x, y \in G$

length of a law

$$\sum_{i=1}^{k}(a_i+b_i)+\sum_{i=1}^{\ell}(c_i+d_i)$$

What kind of (non-abelian) Group should we choose?

1. One-way hardness (with multiple copies)
2. There is a short law with high probability

$(xy)^{\lceil n/2 \rceil} = (y^{-1}x^{-1})^{\lfloor n/2 \rfloor}$

i.e., $(xy)^n = \mathrm{id}$

with probability $1/n$

Highly non-abelian groups,

e.g., symmetric groups

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{M}(k \times n, \mathbb{F})$: the set of all $k \times n$ matrices over $\mathbb{F}$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{M}(k, \mathbb{F})$: the set of all $k \times k$ matrices over $\mathbb{F}$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- How do we understand the action of A and M?

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- How do we understand the action of A and M?
- View 1 : $\mathrm{GL}(k, \mathbb{F}_q) \times \mathrm{Mon}(n, \mathbb{F}_q)$ acts on the set of all generator matrices in $\mathrm{M}(k \times n, \mathbb{F}_q)$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- How do we understand the action of A and M?
- View 1 : $\mathrm{GL}(k, \mathbb{F}_q) \times \mathrm{Mon}(n, \mathbb{F}_q)$ acts on the set of all generator matrices in $\mathrm{M}(k \times n, \mathbb{F}_q)$.
- View 2 : $\mathrm{Mon}(n, \mathbb{F}_q)$ acts on the set of all k-dimensional codes in $\mathbb{F}_q^n$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- Note that $M = DP$, where $D \in \mathrm{D}(n, \mathbb{F}_q)$ and $P \in \mathrm{S}_n$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- Note that $M = DP$, where $D \in \mathrm{D}(n, \mathbb{F}_q)$ and $P \in \mathrm{S}_n$, then $AC_2M = AC_2DP$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- Note that $M = DP$, where $D \in \mathrm{D}(n, \mathbb{F}_q)$ and $P \in \mathrm{S}_n$, then $AC_2M = AC_2DP$.
- Our view : S_n acts on the set of equivalence classes $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$, for every $C \in \mathrm{M}(k \times n, \mathbb{F}_q)$.

Instantiation by Linear Code Equivalence

Notation:

- $\mathrm{GL}(k, \mathbb{F})$: the general linear group of all $k \times k$ invertible matrices over $\mathbb{F}$.
- $\mathrm{D}(n, \mathbb{F})$: the diagonal group of all $n \times n$ invertible diagonal matrices over $\mathbb{F}$.
- $\mathrm{Mon}(n, \mathbb{F})$: the monomial group of all $n \times n$ monomial matrices over $\mathbb{F}$.
- S_n : the symmetric group of degree n.

Problem (Linear Code Equivalence)
For two generator matrices $C_1, C_2 \in \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there is $A \in \mathrm{GL}(k, \mathbb{F}_q)$ and $M \in \mathrm{Mon}(n, \mathbb{F}_q)$ such that $C_1 = AC_2M$.

- Note that $M = DP$, where $D \in \mathrm{D}(n, \mathbb{F}_q)$ and $P \in \mathrm{S}_n$, then $AC_2M = AC_2DP$.
- Our view : S_n acts on the set of equivalence classes $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$, for every $C \in \mathrm{M}(k \times n, \mathbb{F}_q)$.
- Key properties : $[C]_\sim P = [CP]_\sim$ for any $P \in \mathrm{S}_n$.

Instantiation by Linear Code Equivalence

- $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}.$

Instantiation by Linear Code Equivalence

- $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$.
- Alice and Bob send matrices in $[C]_\sim$, with randomly sampled A and D in each round.

Instantiation by Linear Code Equivalence

- $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$.
- Alice and Bob send matrices in $[C]_\sim$, with randomly sampled A and D in each round.
- We give a canonical form algorithm to efficiently compute a representative in $[C]_\sim$.

Instantiation by Linear Code Equivalence

- $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$.
- Alice and Bob send matrices in $[C]_\sim$, with randomly sampled A and D in each round.
- We give a canonical form algorithm to efficiently compute a representative in $[C]_\sim$.

- We propose the following new hardness assumption:

Instantiation by Linear Code Equivalence

- $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$.
- Alice and Bob send matrices in $[C]_\sim$, with randomly sampled A and D in each round.
- We give a canonical form algorithm to efficiently compute a representative in $[C]_\sim$.

- We propose the following new hardness assumption:

Problem (Diagonal-masked Linear Code Equivalence)
For generator matrices $\{C_i : i \in [n]\} \subseteq \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there exist $\{A_i : i \in [n-1]\} \subseteq \mathrm{GL}(k, \mathbb{F}_q)$, $\{D_i : i \in [n-1]\} \subseteq \mathrm{D}(n, \mathbb{F}_q)$ and $P \in \mathrm{S}_n$ such $A_i C_i D_i P = C_{i+1}$ for all $i \in [n-1]$. If yes, compute such a permutation P.

Instantiation by Linear Code Equivalence

- $[C]_\sim := \{ACD : A \in \mathrm{GL}(k, \mathbb{F}_q), D \in \mathrm{D}(n, \mathbb{F}_q)\}$.
- Alice and Bob send matrices in $[C]_\sim$, with randomly sampled A and D in each round.
- We give a canonical form algorithm to efficiently compute a representative in $[C]_\sim$.

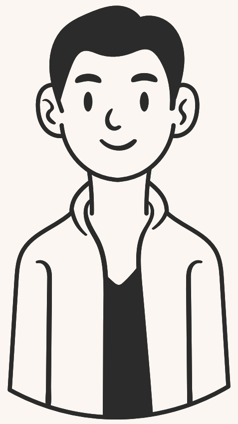
- We propose the following new hardness assumption:

Problem (Diagonal-masked Linear Code Equivalence)
For generator matrices $\{C_i : i \in [n]\} \subseteq \mathrm{M}(k \times n, \mathbb{F}_q)$, determine if there exist $\{A_i : i \in [n-1]\} \subseteq \mathrm{GL}(k, \mathbb{F}_q)$, $\{D_i : i \in [n-1]\} \subseteq \mathrm{D}(n, \mathbb{F}_q)$ and $P \in \mathrm{S}_n$ such $A_i C_i D_i P = C_{i+1}$ for all $i \in [n-1]$. If yes, compute such a permutation P.

- We also carry out Magma experiments to support the hardness.

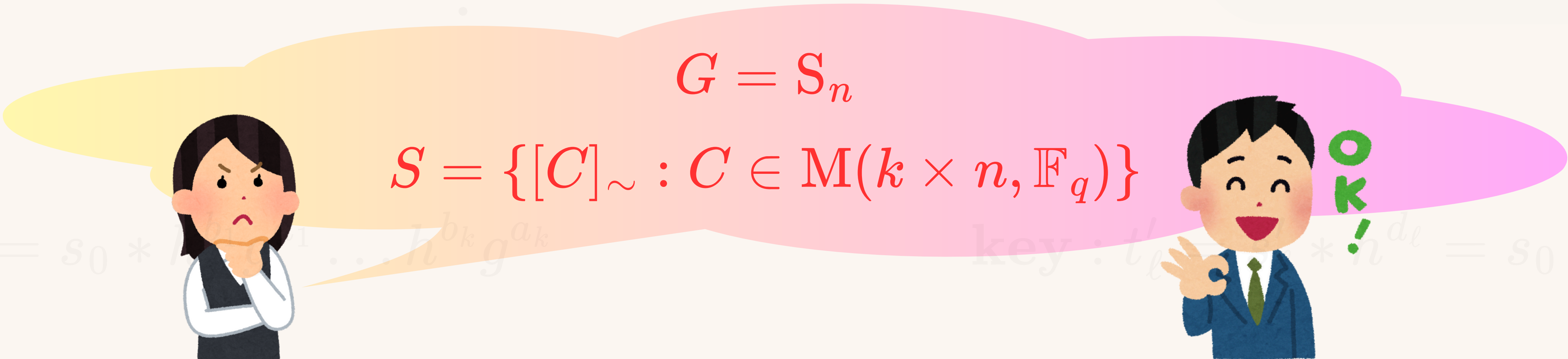
Instantiation Summary

Alice



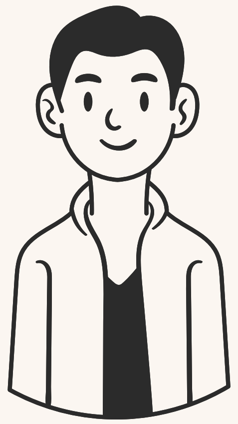
Bob

What kind of Group and Set did we choose?



Instantiation Summary

Alice



Bob

$$(xy)^{\lceil n/2 \rceil} = (y^{-1}x^{-1})^{\lfloor n/2 \rfloor}$$

for a large proportion of $x, y \in G$

What kind of Group and Set did we choose?

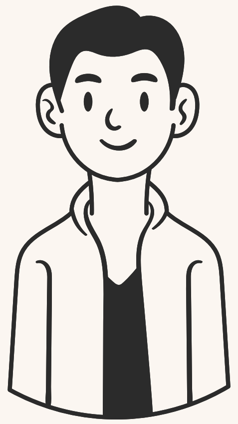
1. One-way hardness (with multiple copies)
2. There is a short law with high probability

$$G = \mathrm{S}_n$$

$$S = \{[C]_\sim : C \in \mathrm{M}(k \times n, \mathbb{F}_q)\}$$

Instantiation Summary

Alice



Bob

$$(xy)^{\lceil n/2 \rceil} = (y^{-1}x^{-1})^{\lfloor n/2 \rfloor}$$

for a large proportion of $x, y \in G$

What kind of Group and Set did we choose?

1. One-way hardness (with multiple copies)
2. There is a short law with high probability

$$G = \mathrm{S}_n$$

$$S = \{[C]_\sim : C \in \mathrm{M}(k \times n, \mathbb{F}_q)\}$$

Instantiation Summary

Alice

Bob

$$(xy)^{\lceil n/2 \rceil} = (y^{-1}x^{-1})^{\lfloor n/2 \rfloor}$$

for a large proportion of $x, y \in G$

What kind of Group and Set did we choose?

1. One-way hardness (with multiple copies) ?

2. There is a short law with high probability

$$G = \mathrm{S}_n$$

$$S = \{[C]_\sim : C \in \mathrm{M}(k \times n, \mathbb{F}_q)\}$$

Question and Answer

Thank you so much!