# Tighter Security for Group Key Agreement in the ROM

Andreas Ellison
Supervisor: Karen Klein

# Overview

1. Big picture
2. CGKA schemes
3. The TreeKEM protocol
4. Proof in [ACC+19]
5. Proof in my thesis

# Overview

1. Big picture
2. CGKA schemes
3. The TreeKEM protocol
4. Proof in [ACC+19]
5. Proof in my thesis

context

# Big picture

## RFC 9420
## The Messaging Layer Security (MLS) Protocol


### Abstract

Messaging applications are increasingly making use of end-to-end security mechanisms to ensure that messages are only accessible to the communicating endpoints, and not to any servers involved in delivering messages. Establishing keys to provide such protections is challenging for group chat settings, in which more than two clients need to agree on a key but may not be online at the same time. In this document, we specify a key establishment protocol that provides efficient asynchronous group key establishment with forward secrecy (FS) and post-compromise security (PCS) for groups in size ranging from two to thousands.


### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9420.

# Big picture

## RFC 9420
## The Messaging Layer Security (MLS) Protocol

### Abstract

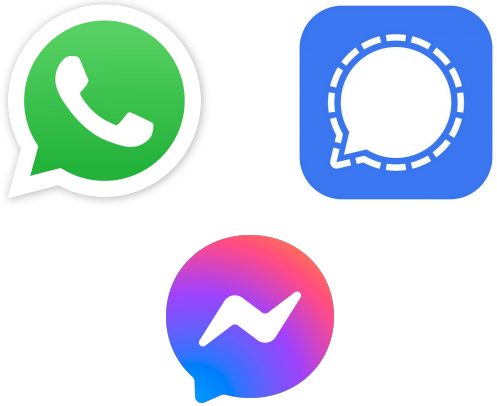
Messaging applications are increasingly making use of end-to-end security mechanisms to ensure that messages are only accessible to the communicating endpoints, and not to any servers involved in delivering messages. Establishing keys to provide such protections is challenging for group chat settings, in which more than two clients need to agree on a key but may not be online at the same time. In this document, we specify a key establishment protocol that provides efficient asynchronous group key establishment with forward secrecy (FS) and post-compromise security (PCS) for groups in size ranging from two to thousands.

### Status of This Memo

This is an Internet Standards Track document.

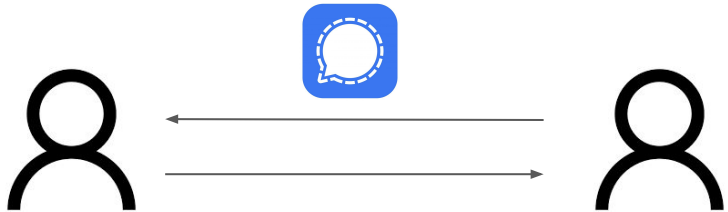
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9420.



# Why MLS?

# Why MLS?



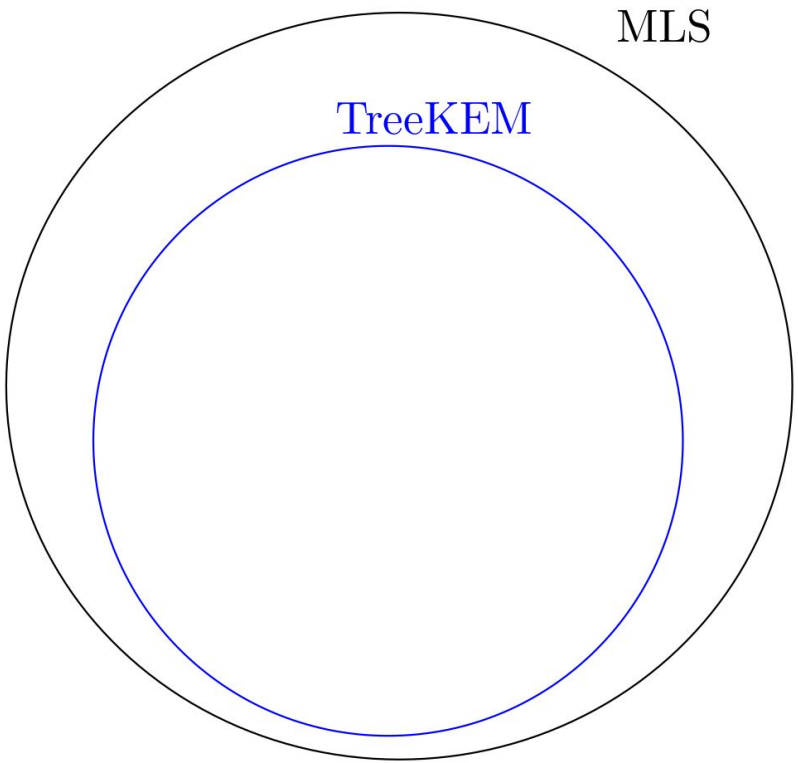
# Why MLS?

1. Scale to large groups

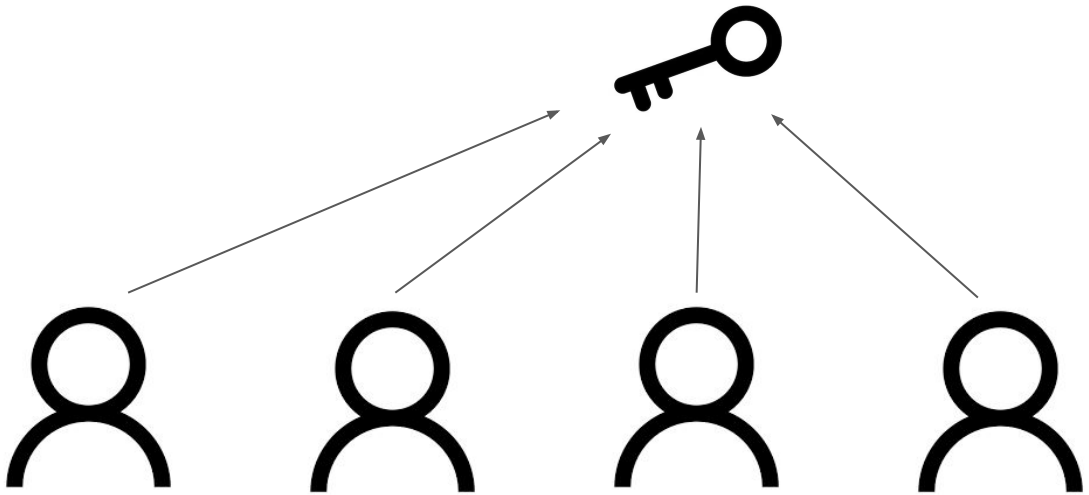
# Why MLS?

1. Scale to large groups
2. Standardized protocol

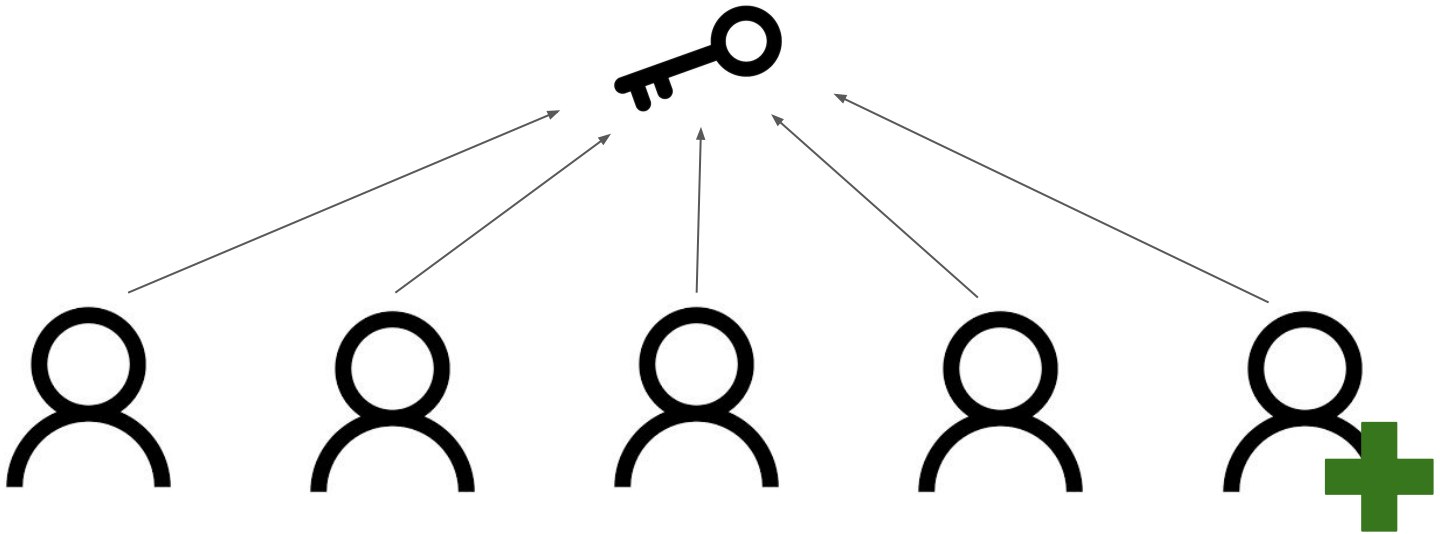
# Continuous Group Key Agreement (CGKA)



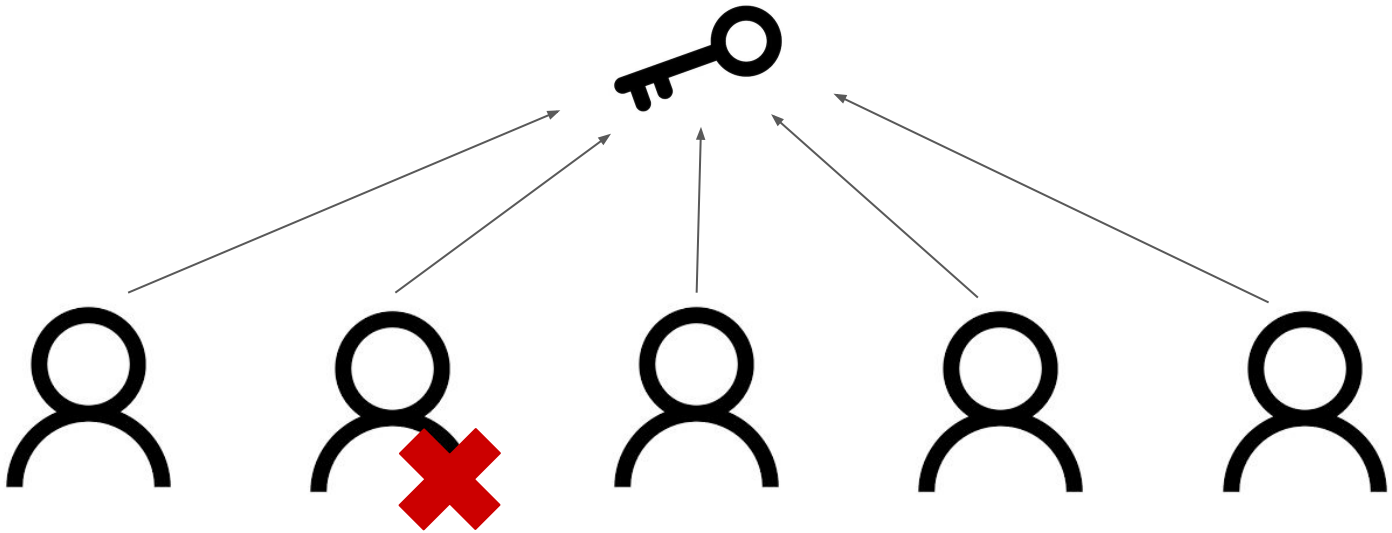
# CGKA – Key agreement



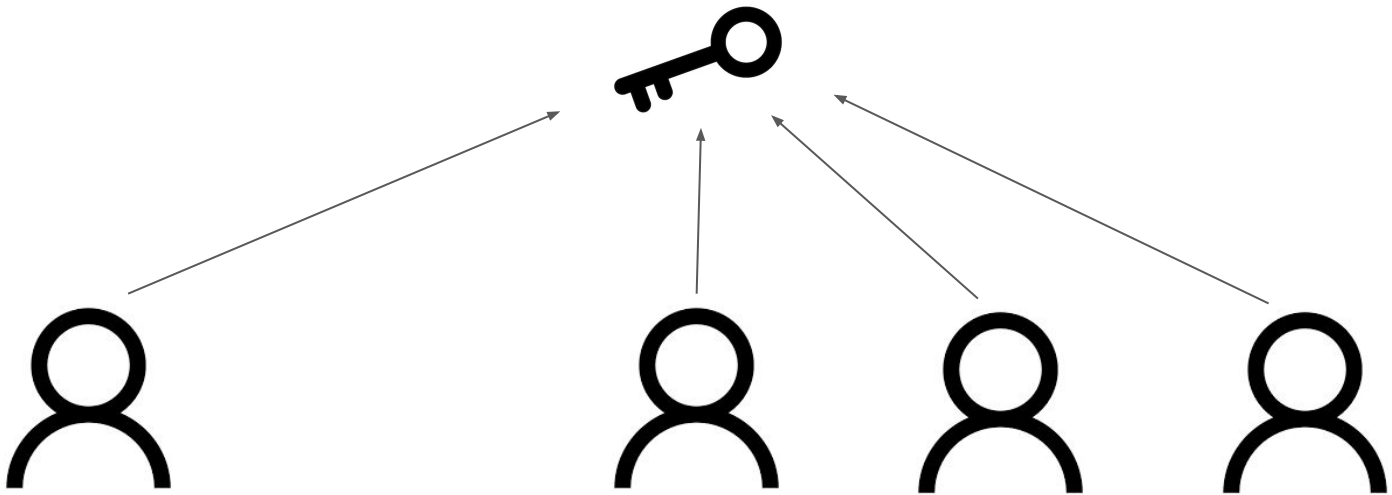
# CGKA – Add user



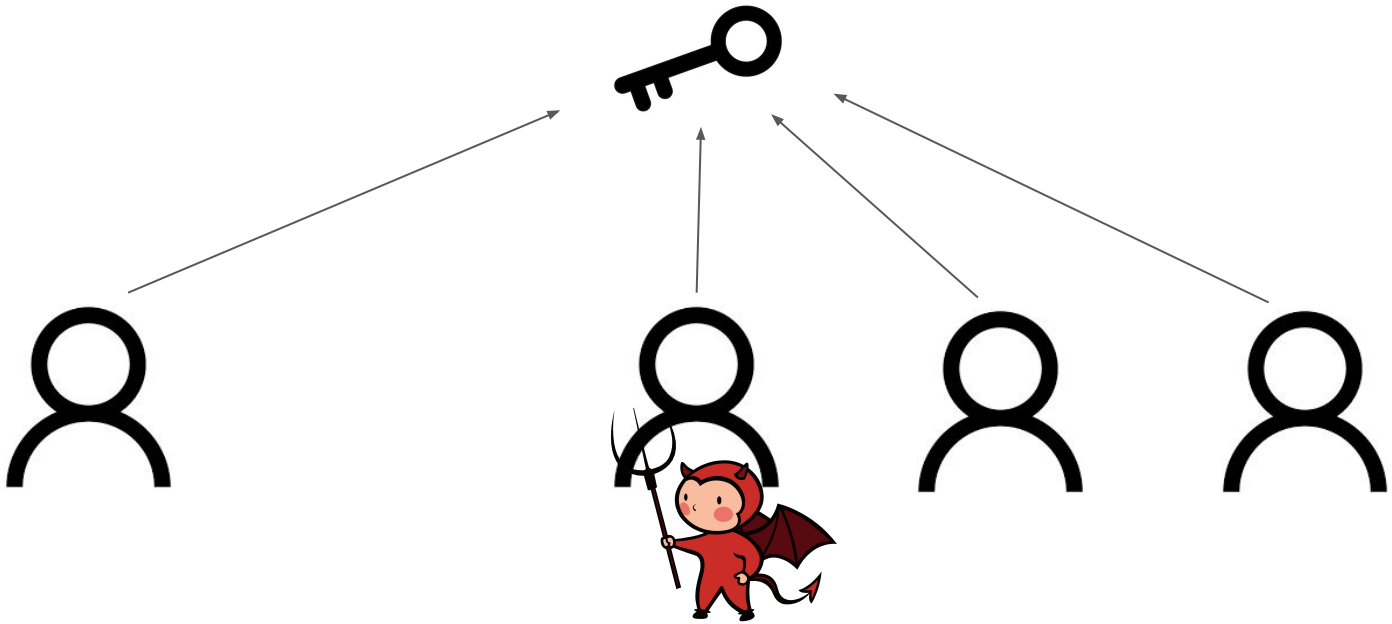
# CGKA – Remove user



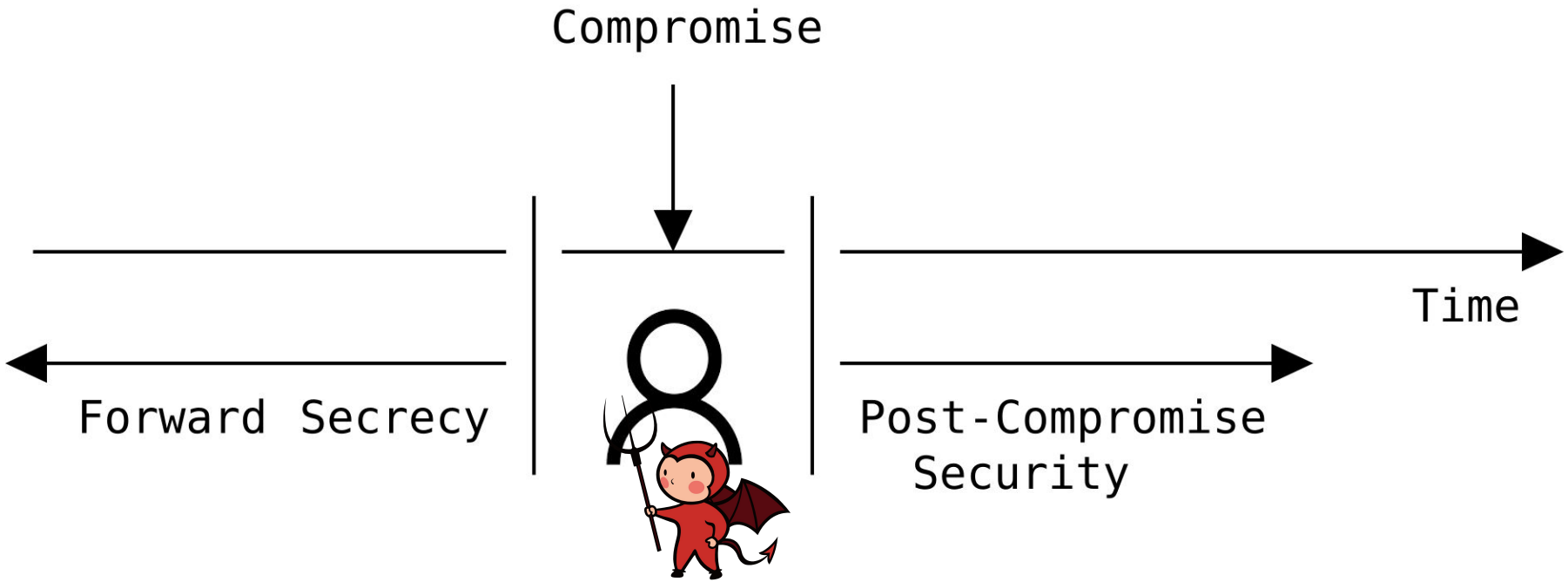
# CGKA



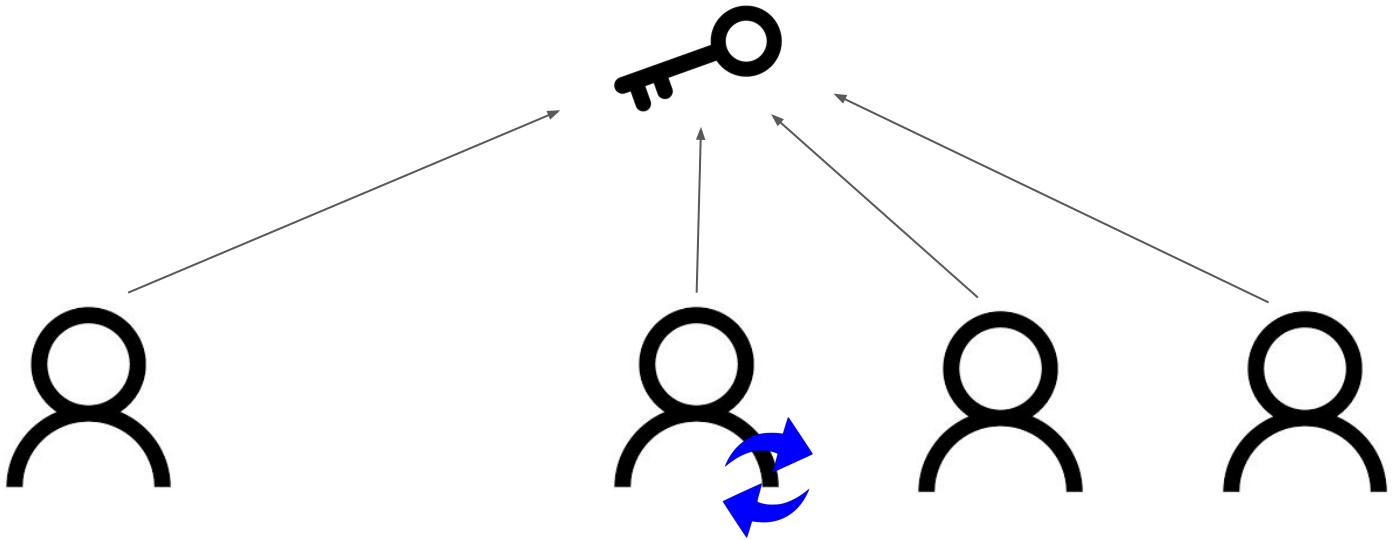
# CGKA – Dealing with compromise



# CGKA – Dealing with compromise

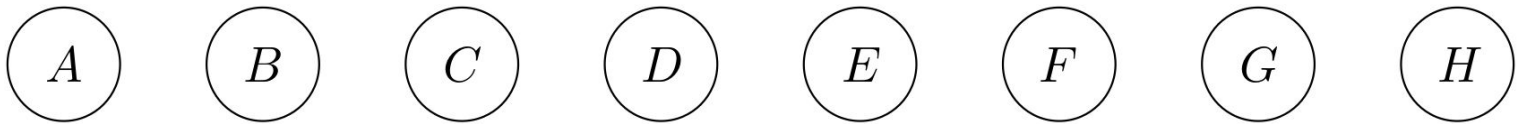


# CGKA – Update

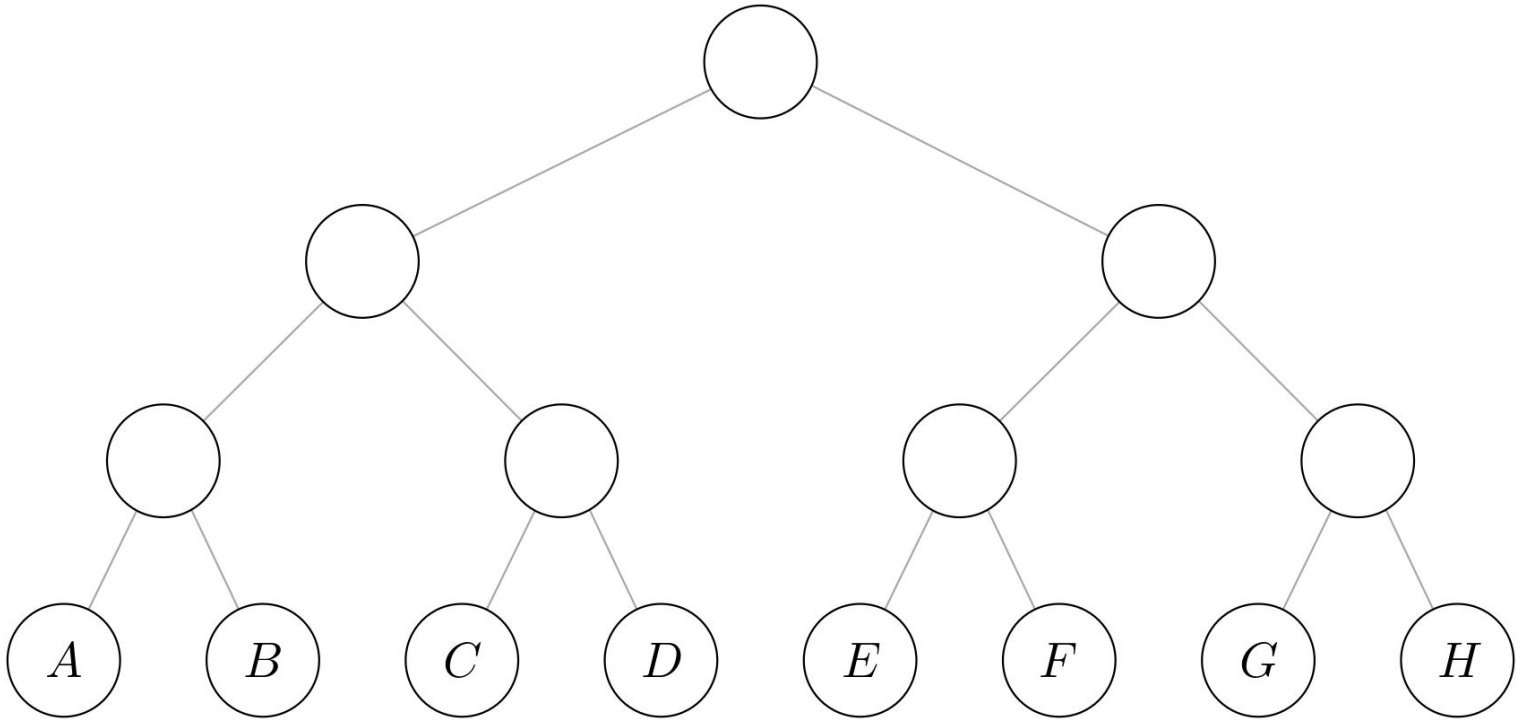


# TreeKEM

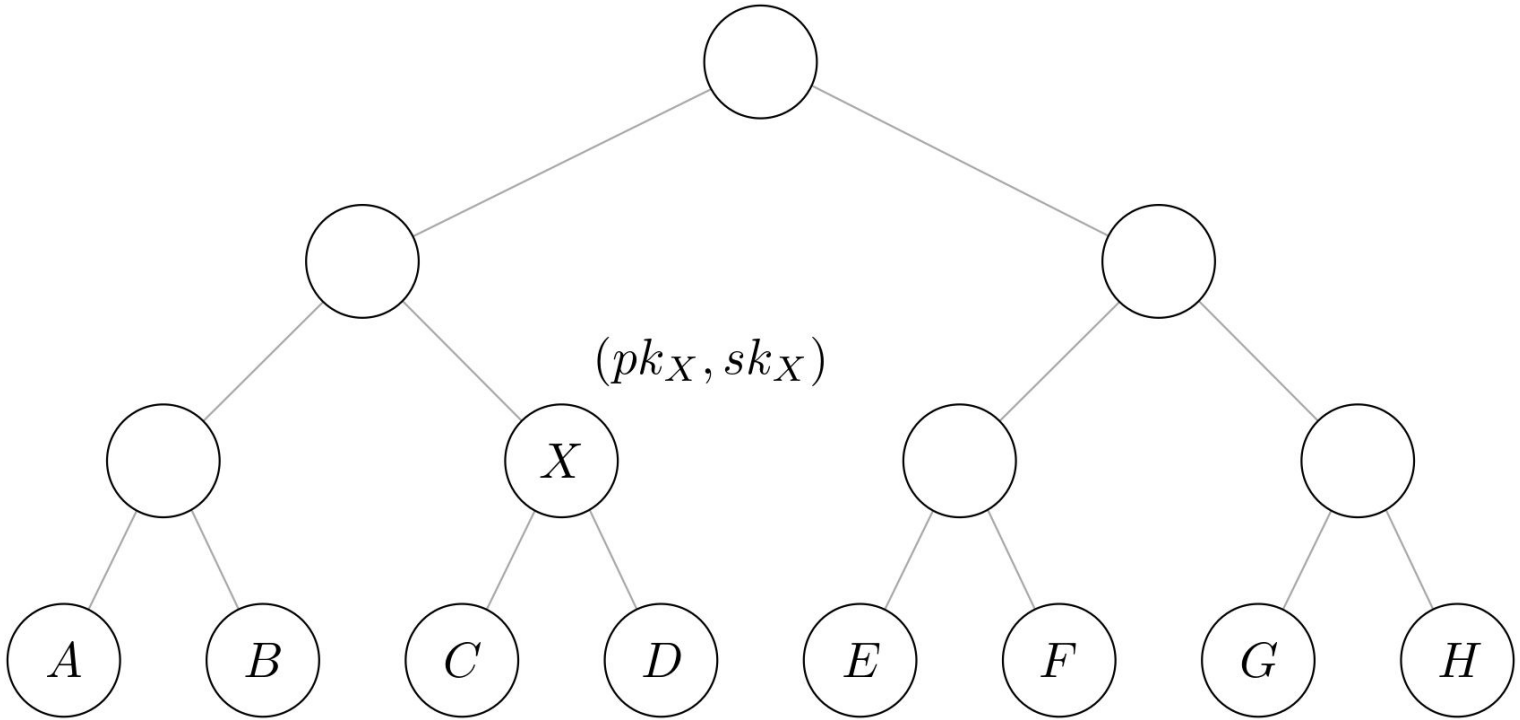
# TreeKEM



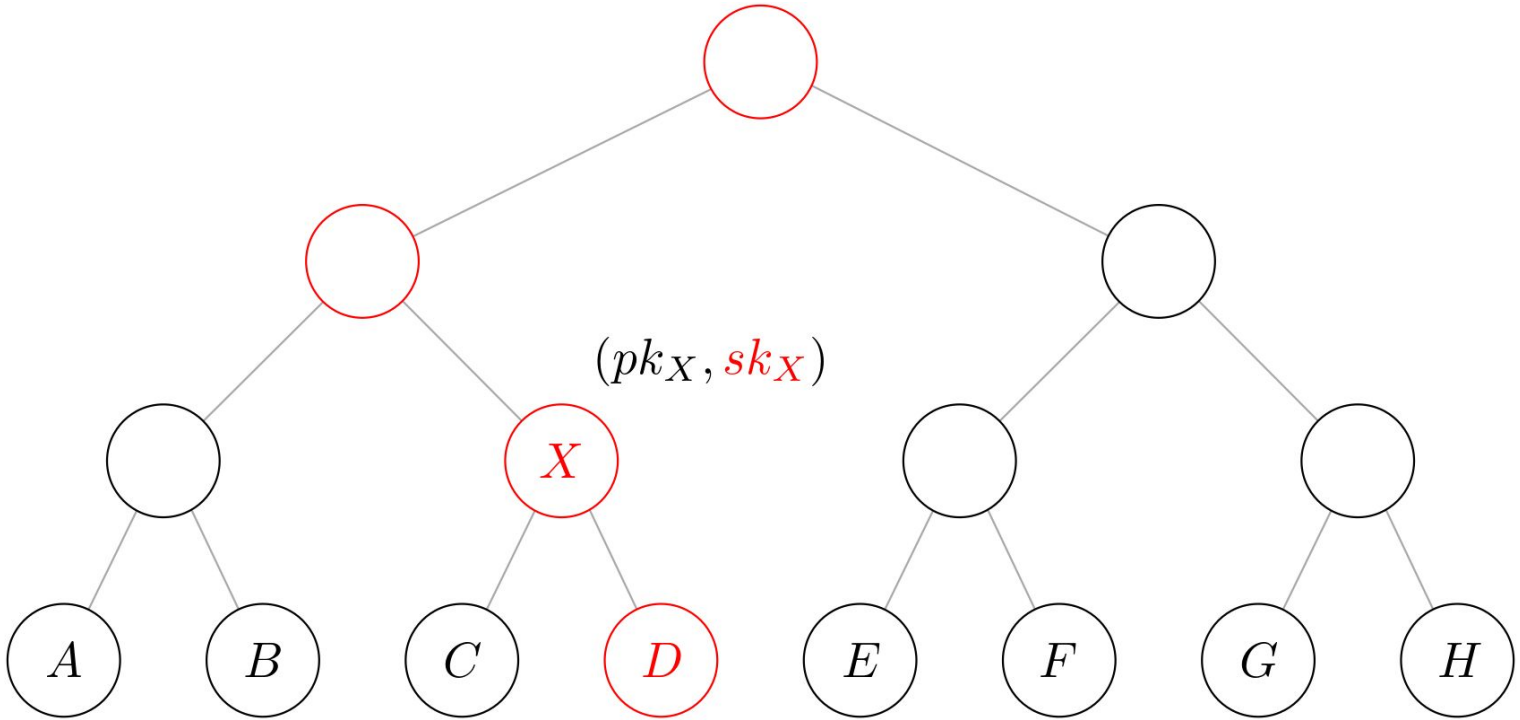
# TreeKEM



# TreeKEM

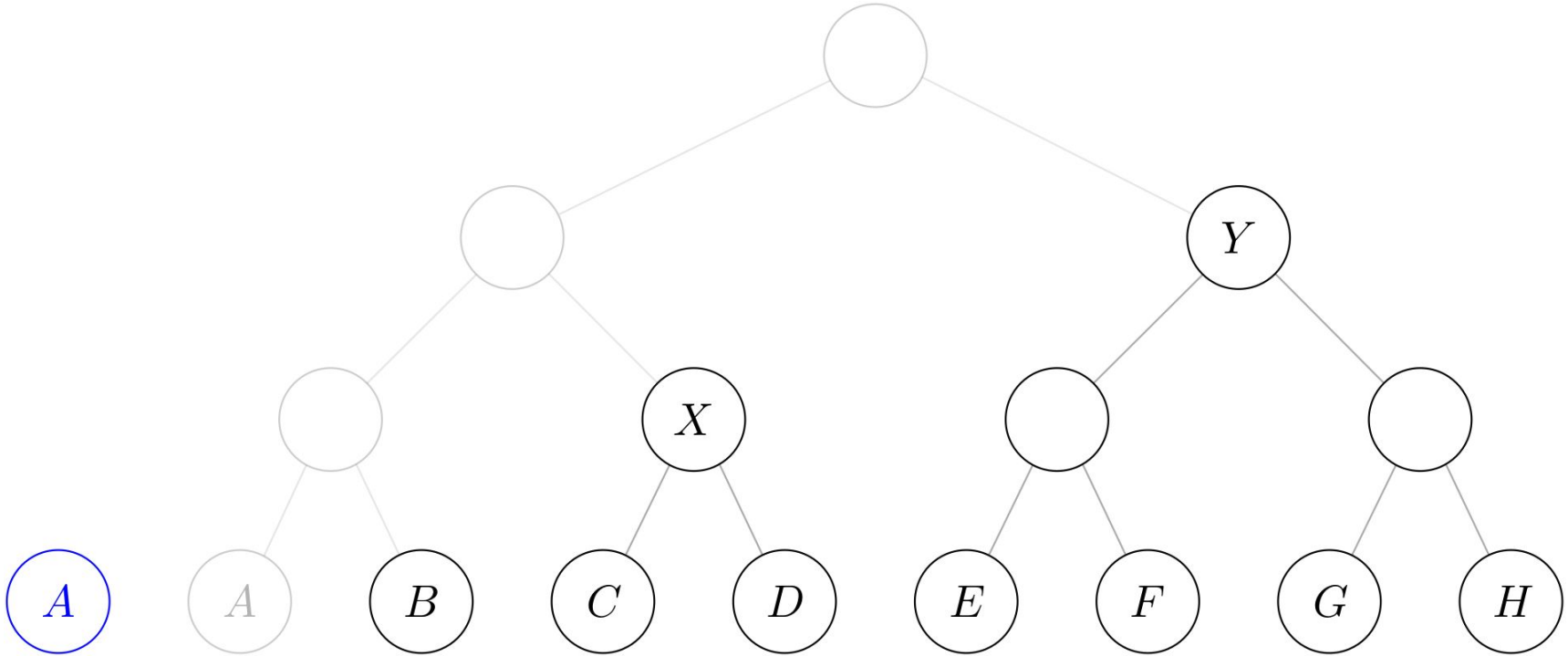


# TreeKEM



# TreeKEM commit

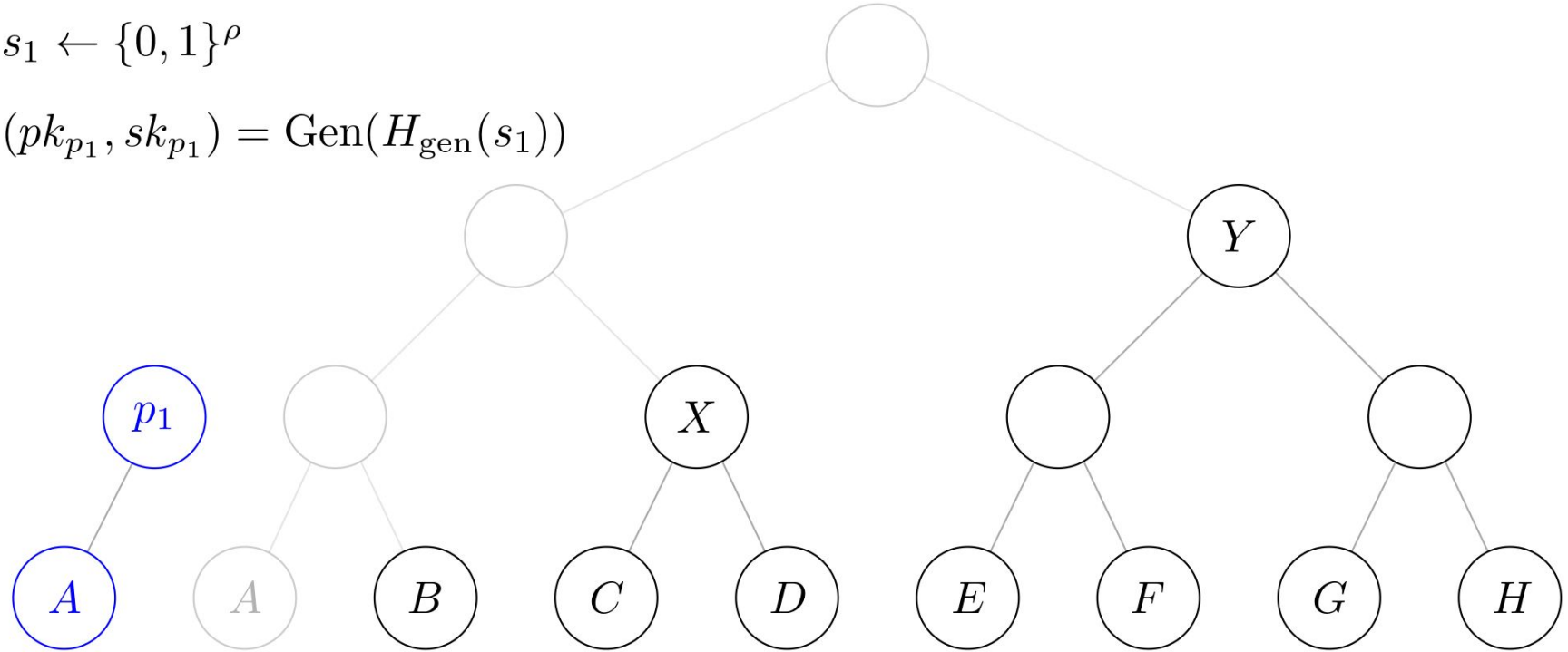
# TreeKEM commit



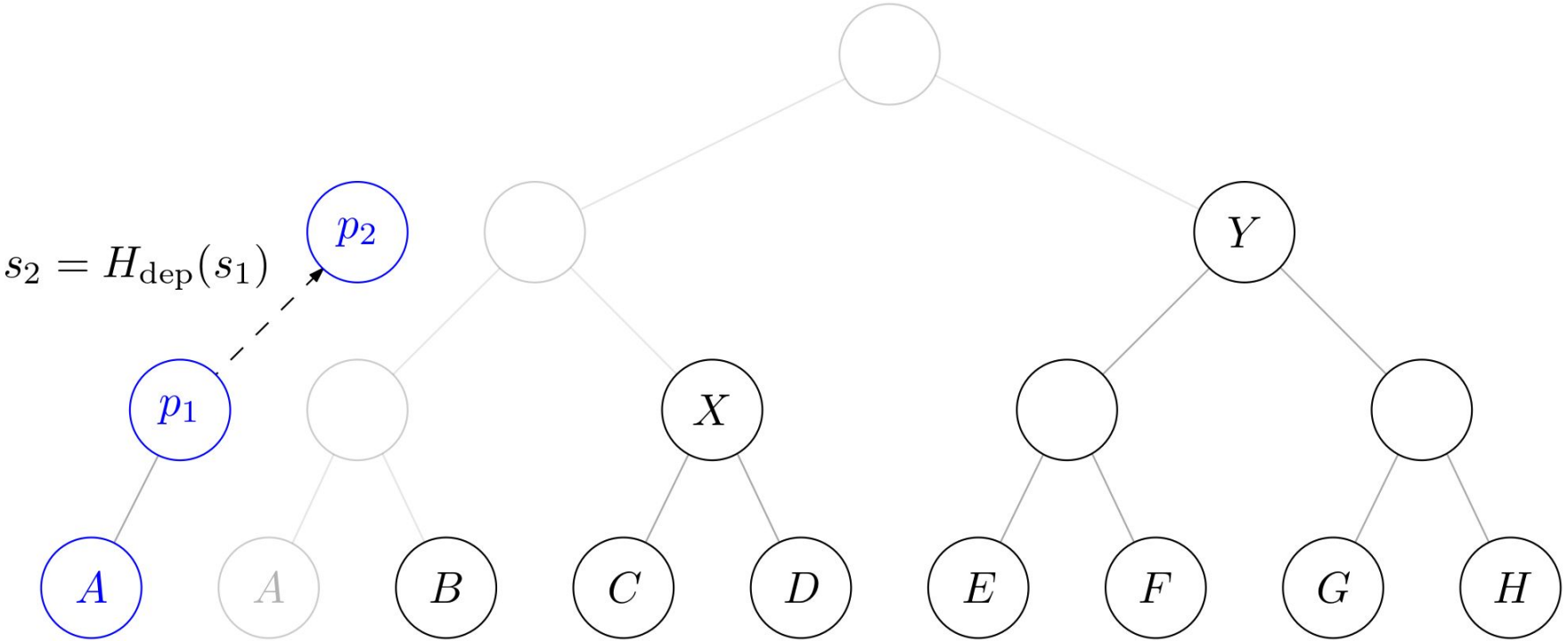
# TreeKEM commit

$s_1 \leftarrow \{0,1\}^\rho$

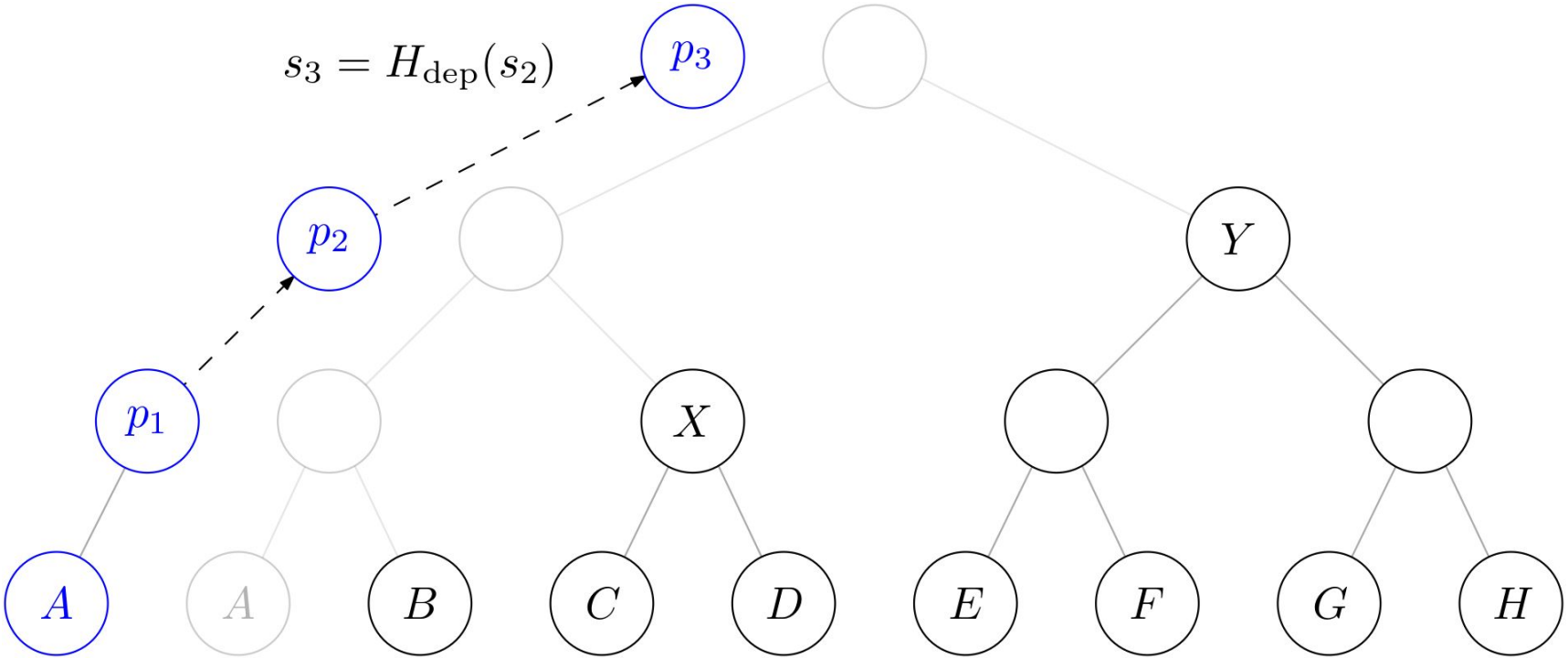
$(pk_{p_1}, sk_{p_1}) = \mathrm{Gen}(H_{\mathrm{gen}}(s_1))$



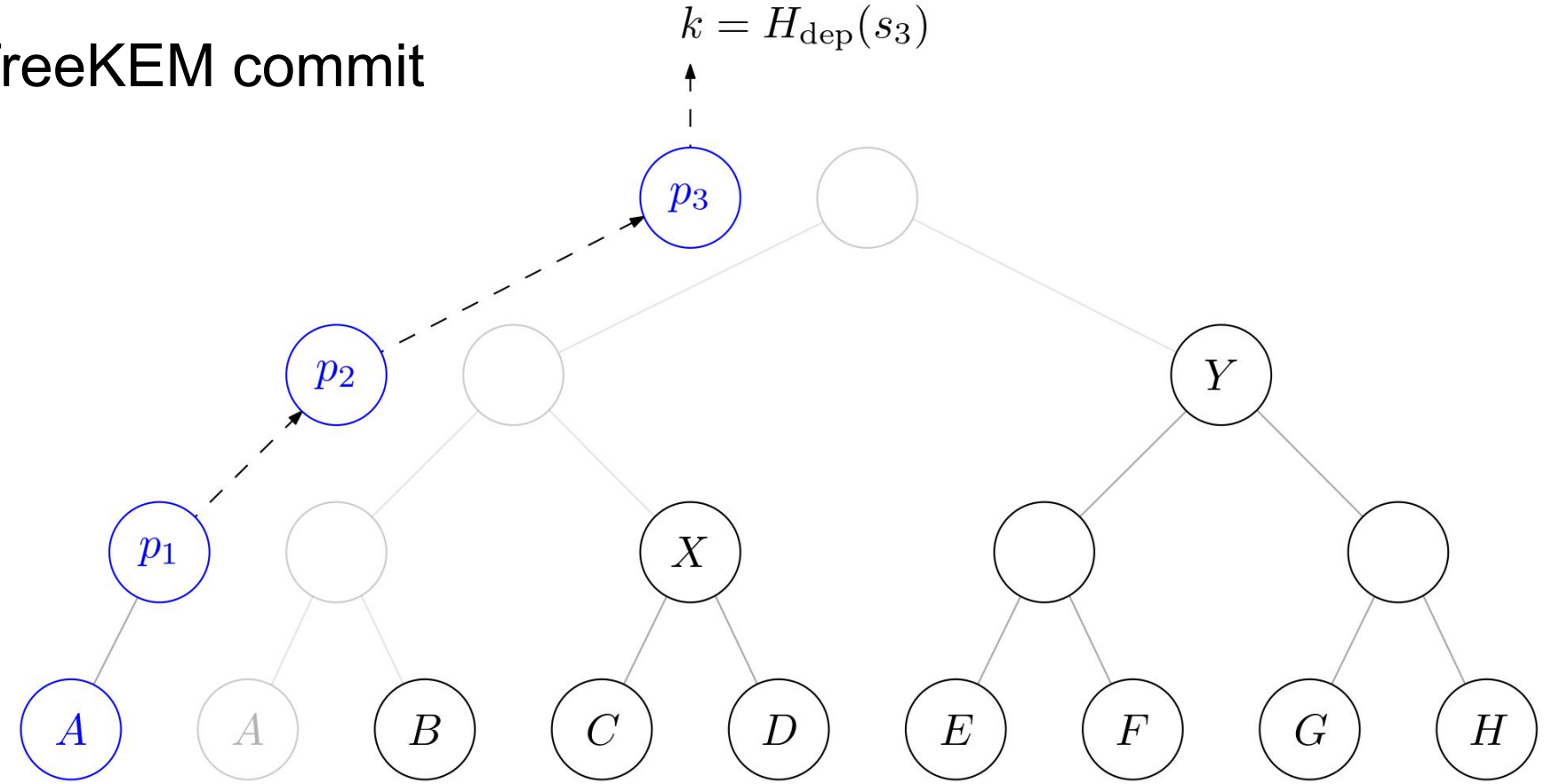
# TreeKEM commit



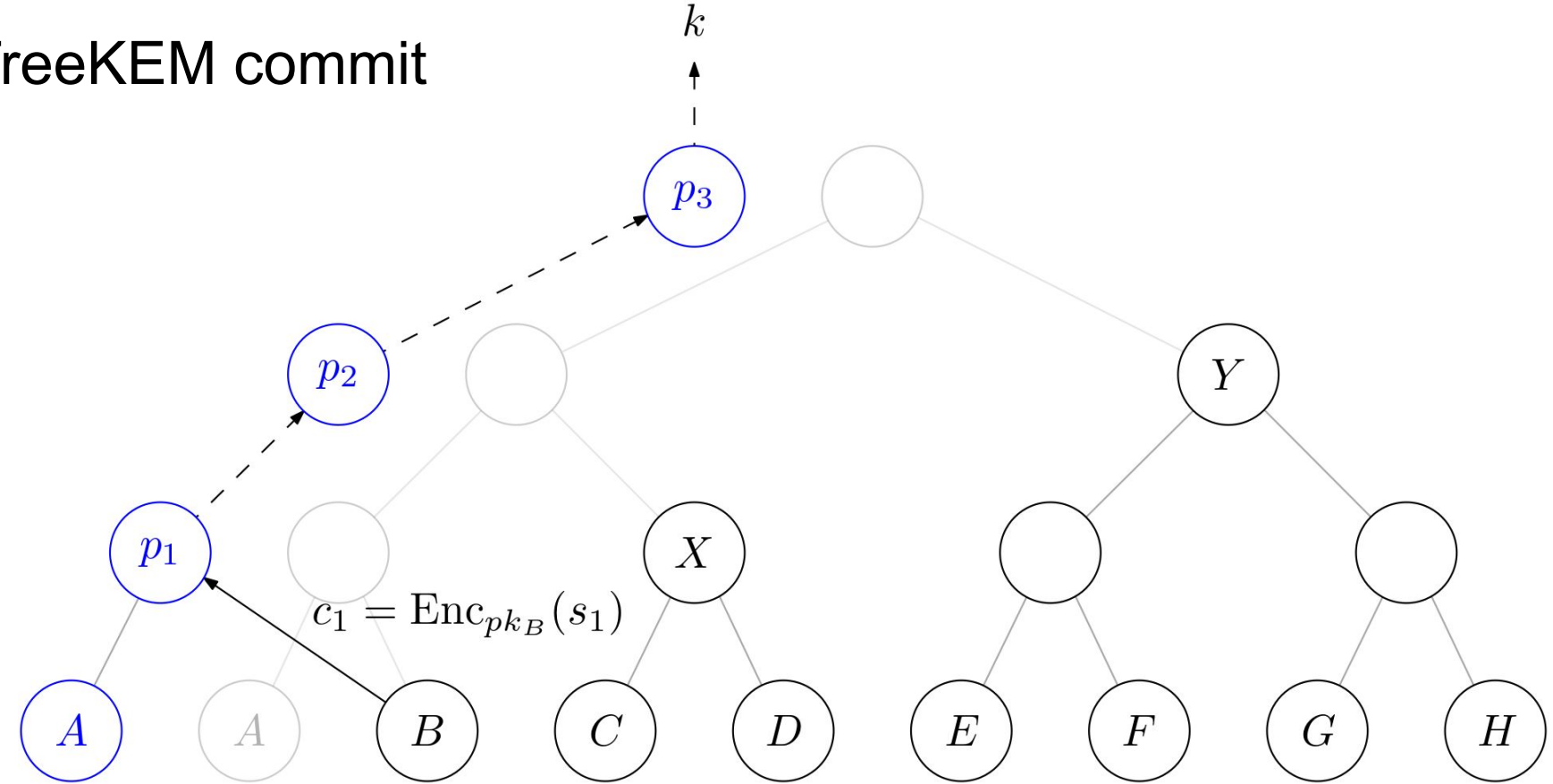
# TreeKEM commit



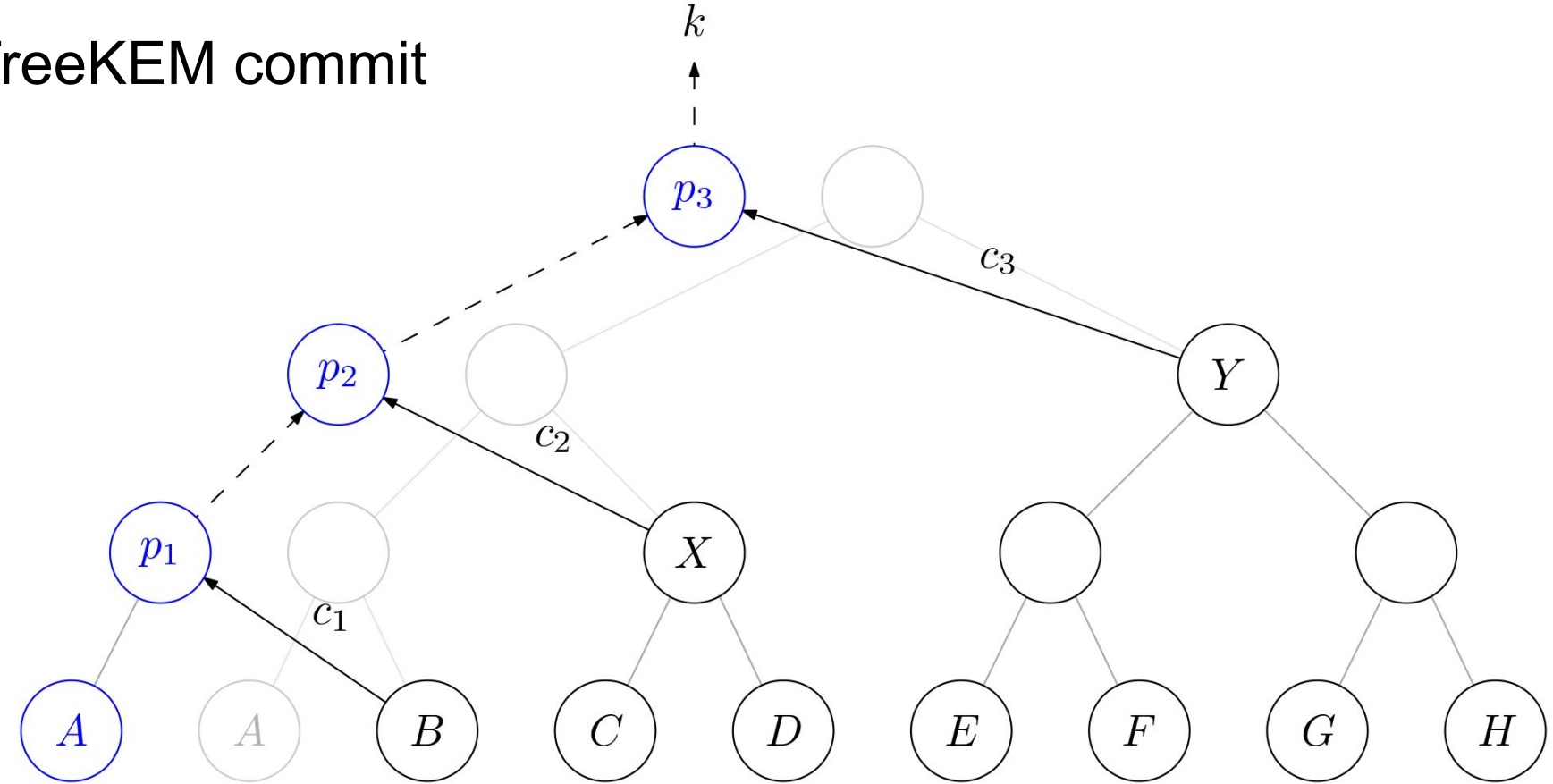
# TreeKEM commit



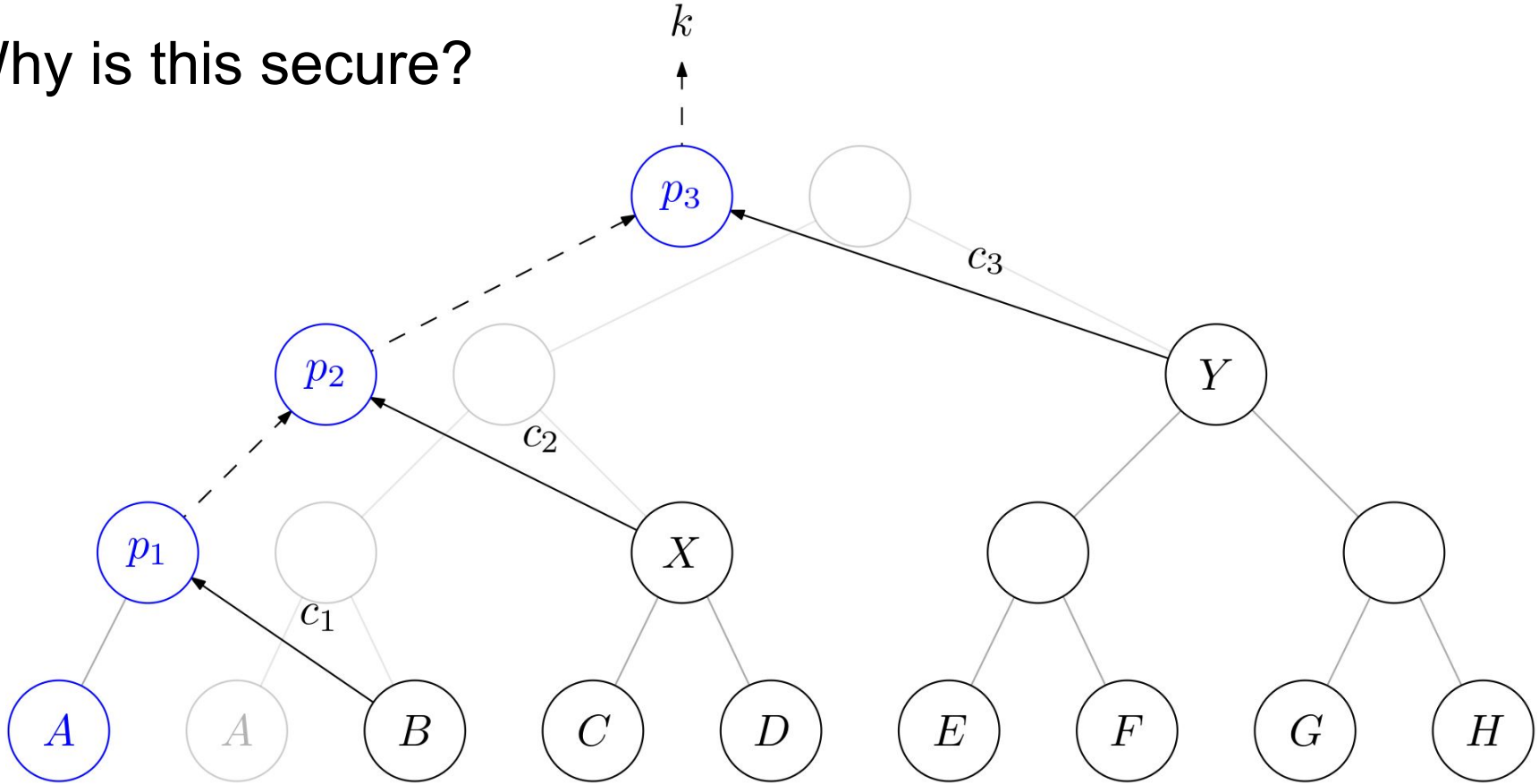
# TreeKEM commit



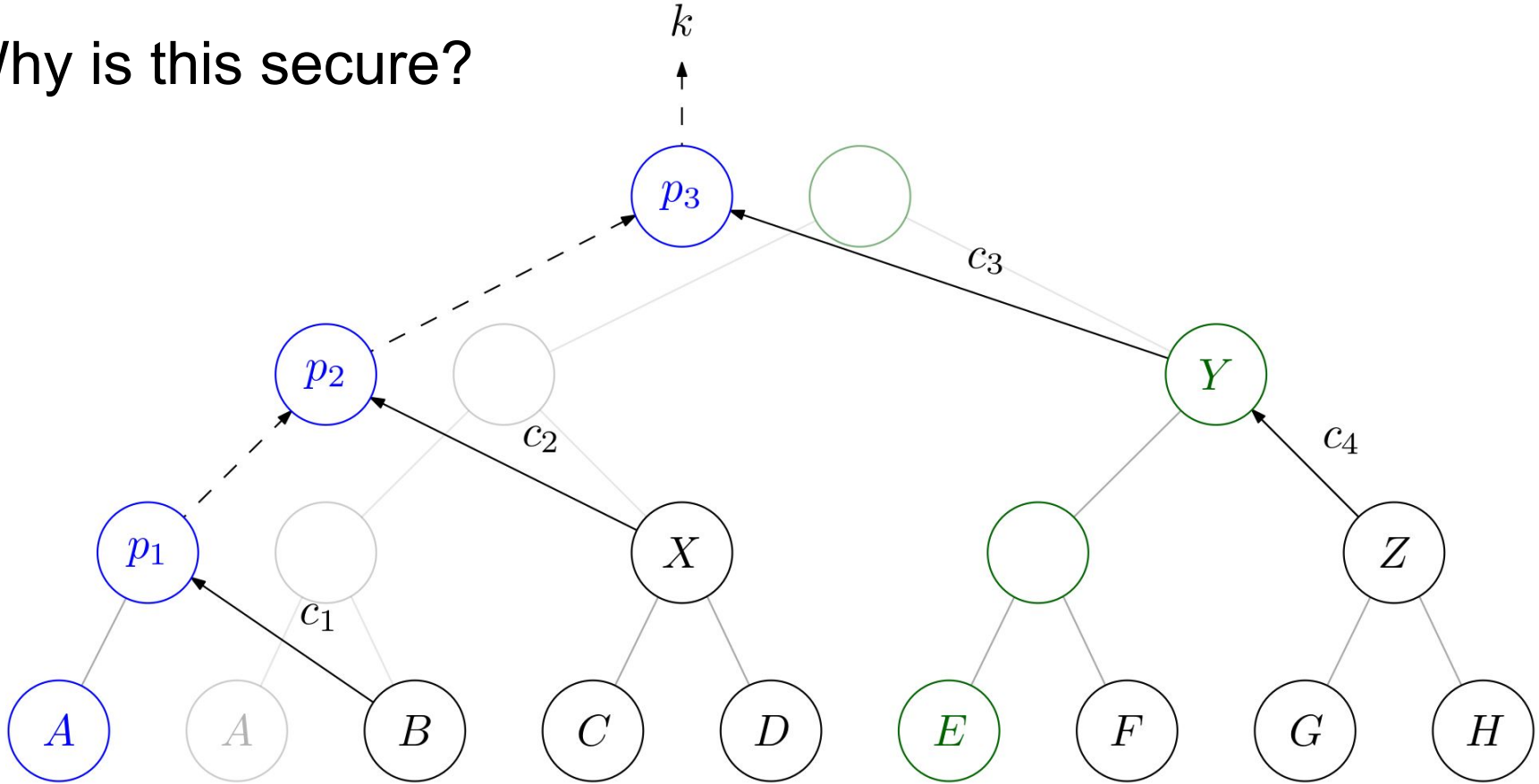
# TreeKEM commit



# Why is this secure?



# Why is this secure?



# CGKA game

$\mathcal{C}$

$\text{commit}(\cdot)$

$c_1$

$\vdots$

$\text{commit}(\cdot)$

$c_n$

$\text{challenge}(c_i)$

$\tilde{k}$

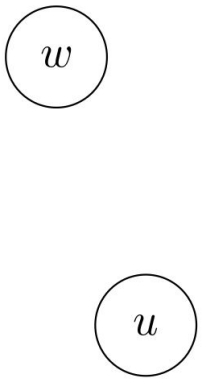
# GSD [Pan07]

# SD-GSD

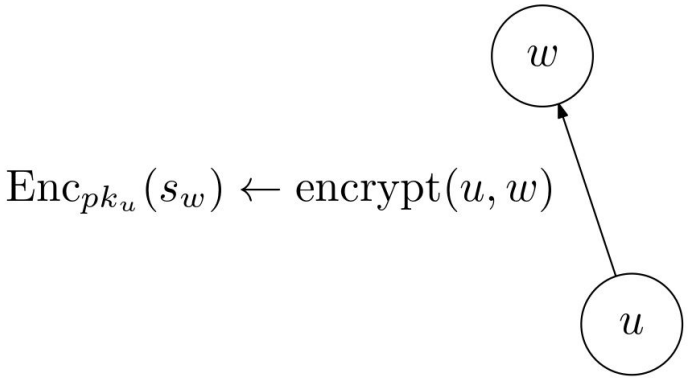
$$s_u \leftarrow \{0,1\}^\rho$$

$$(pk_u, sk_u) = \mathrm{Gen}(H_{\mathrm{gen}}(s_u))$$

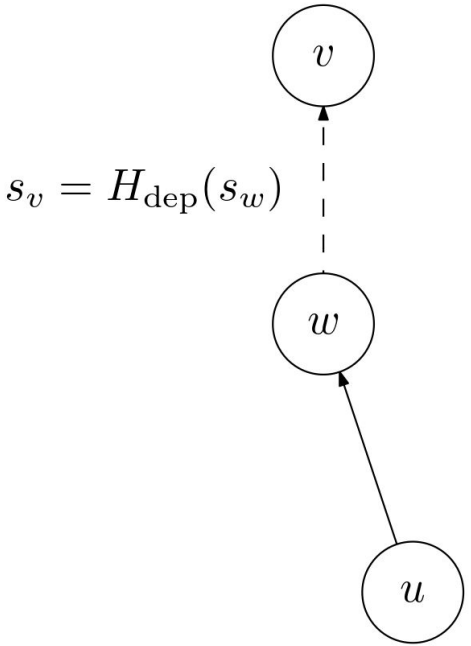
# SD-GSD



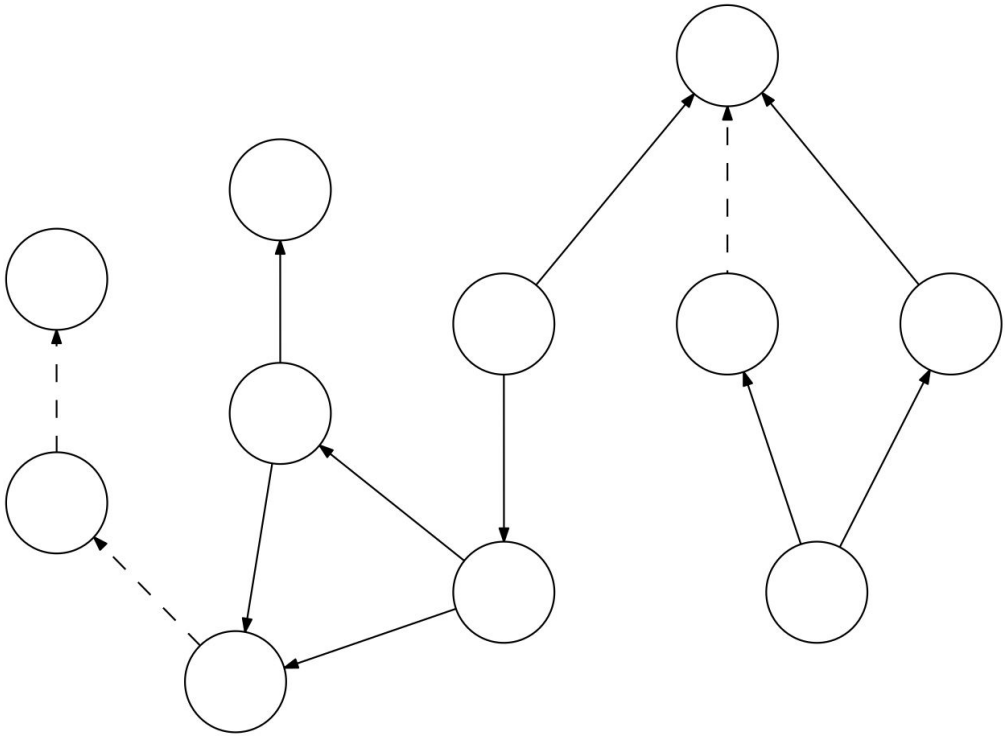
# SD-GSD



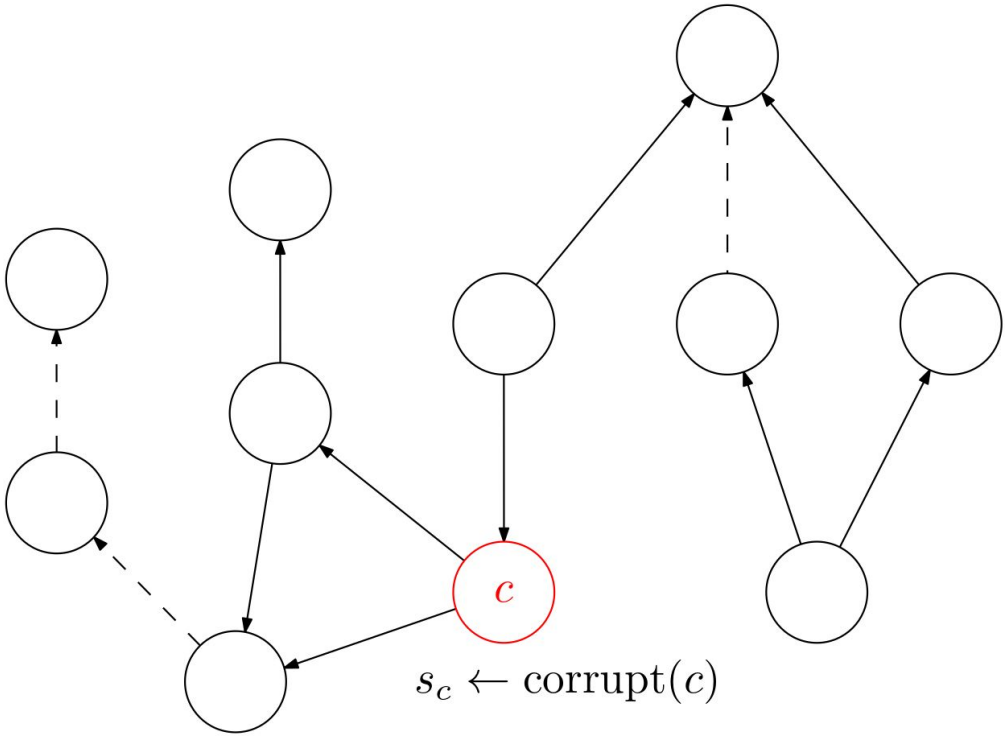
# SD-GSD



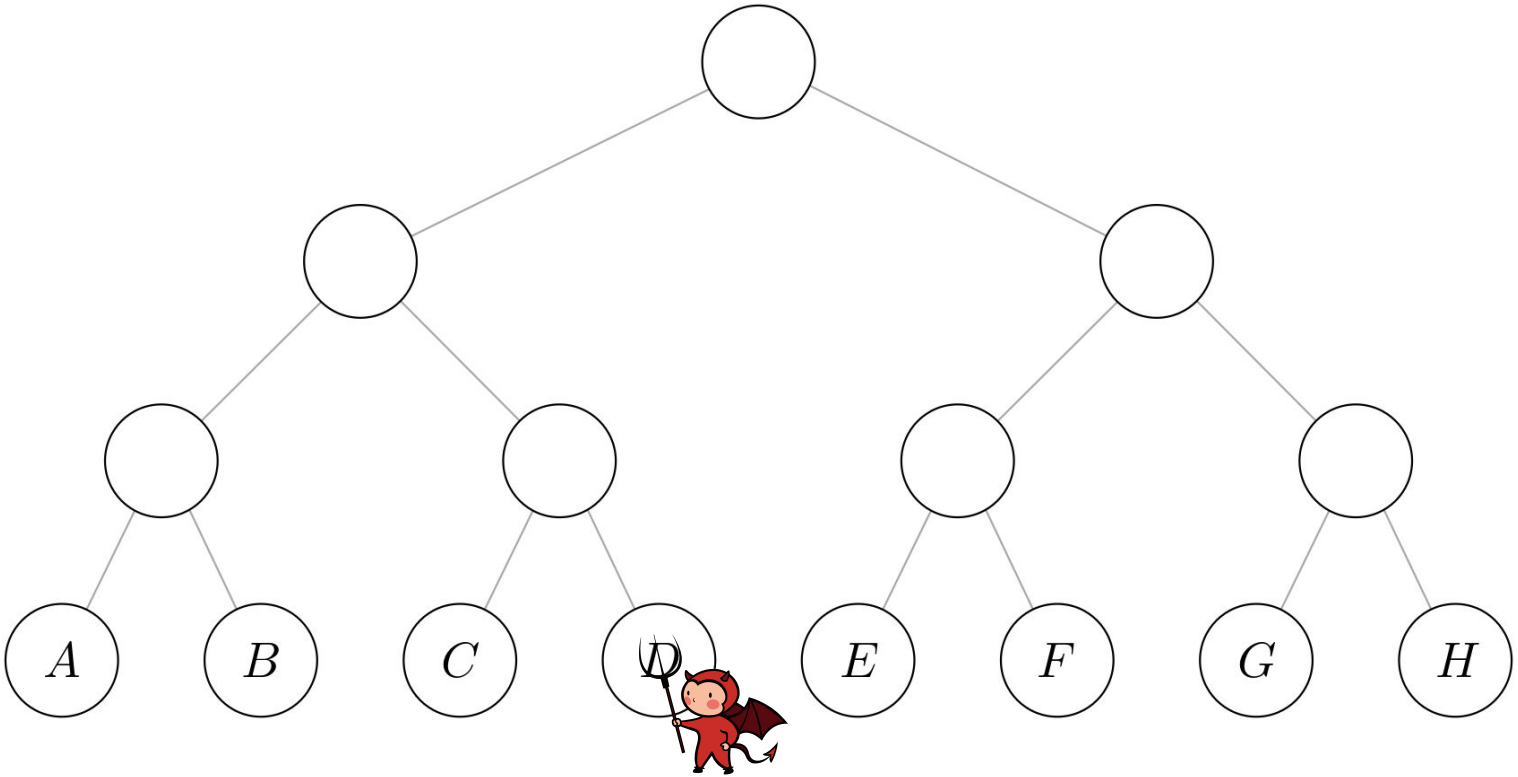
# SD-GSD



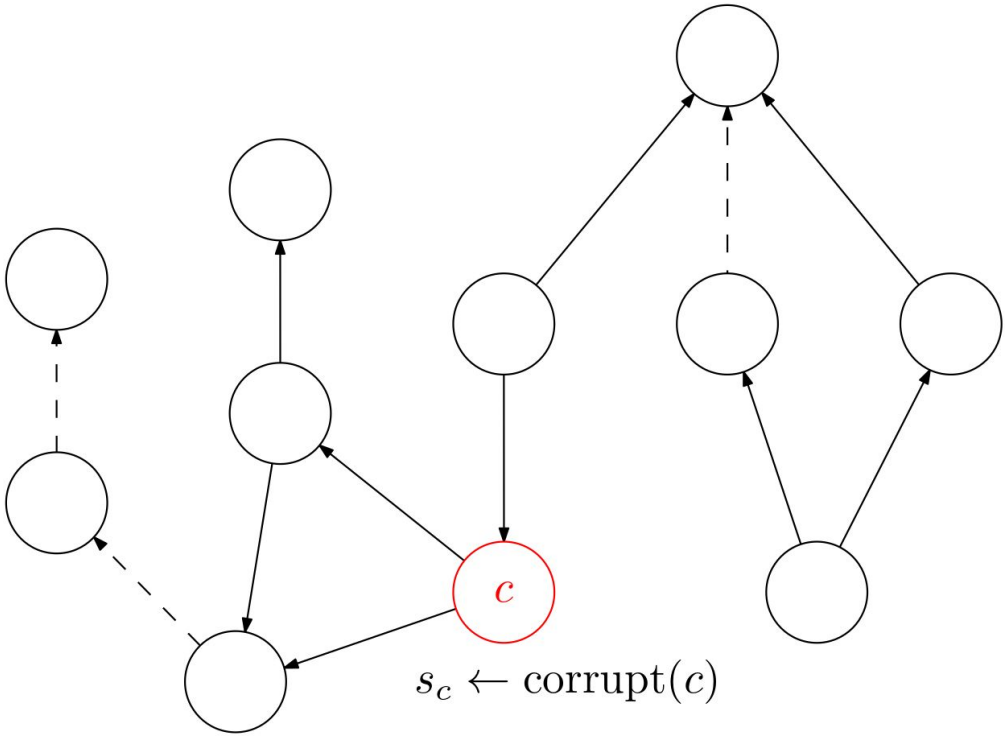
# SD-GSD



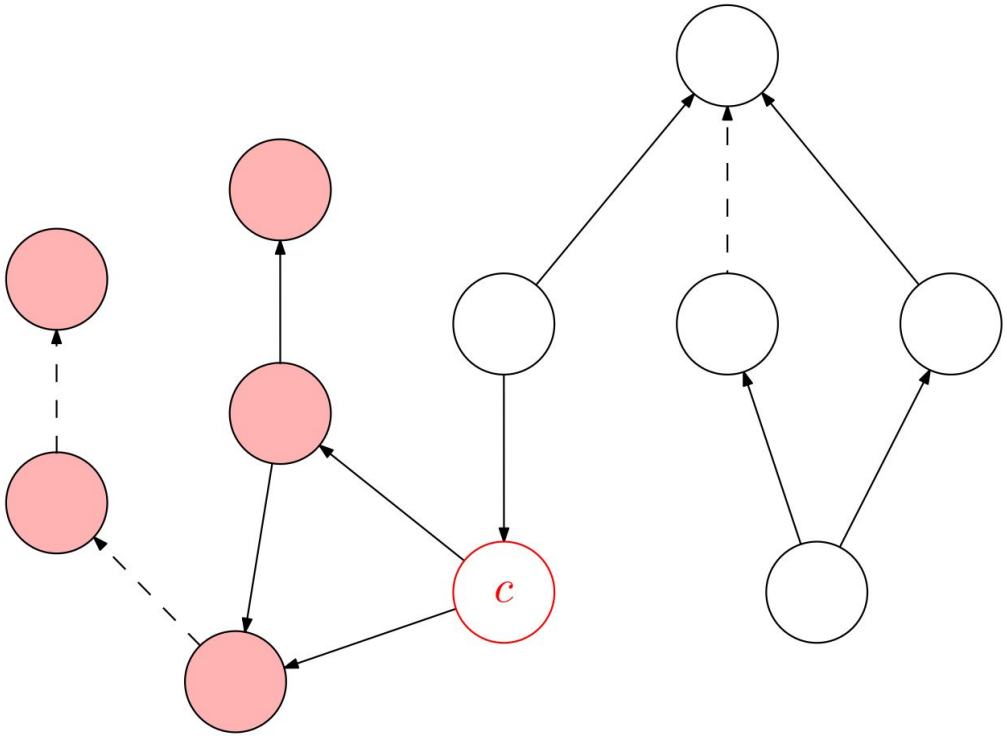
# Corruptions in CGKA game



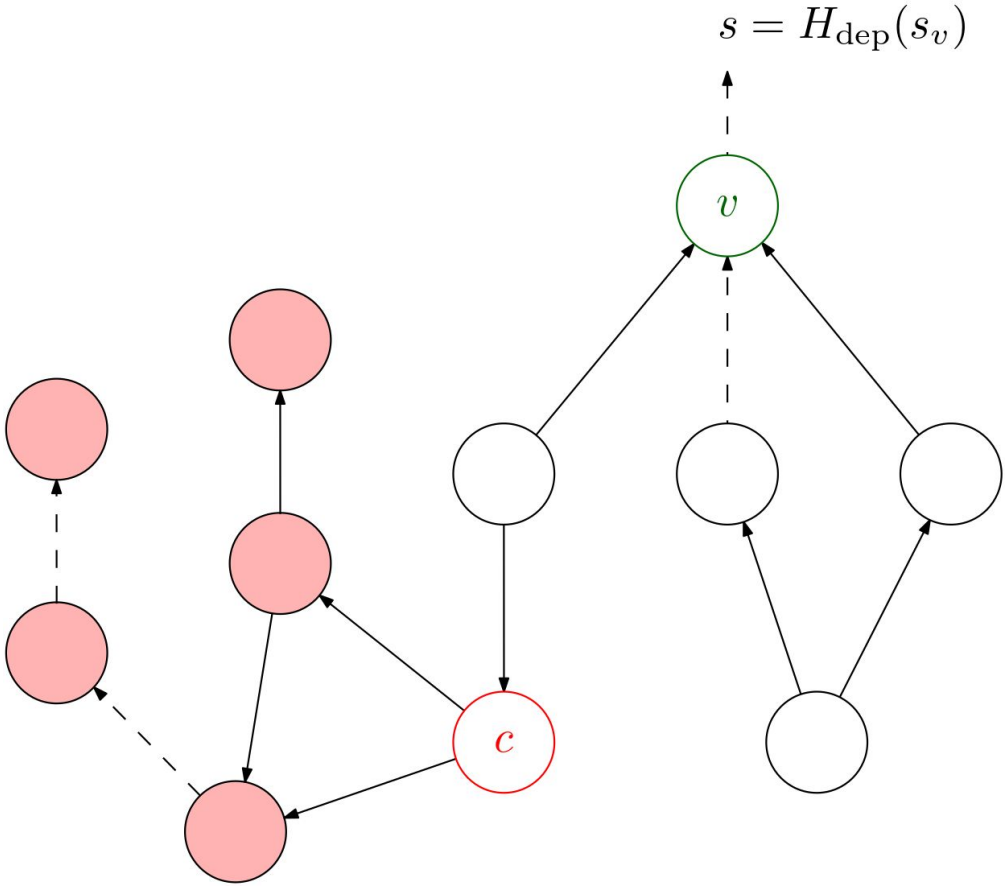
# SD-GSD



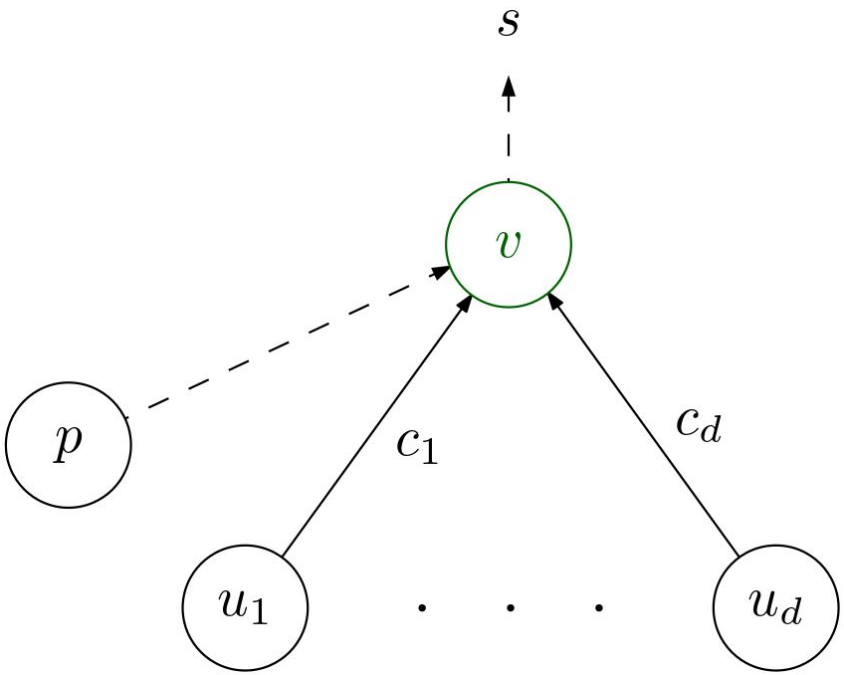
# SD-GSD



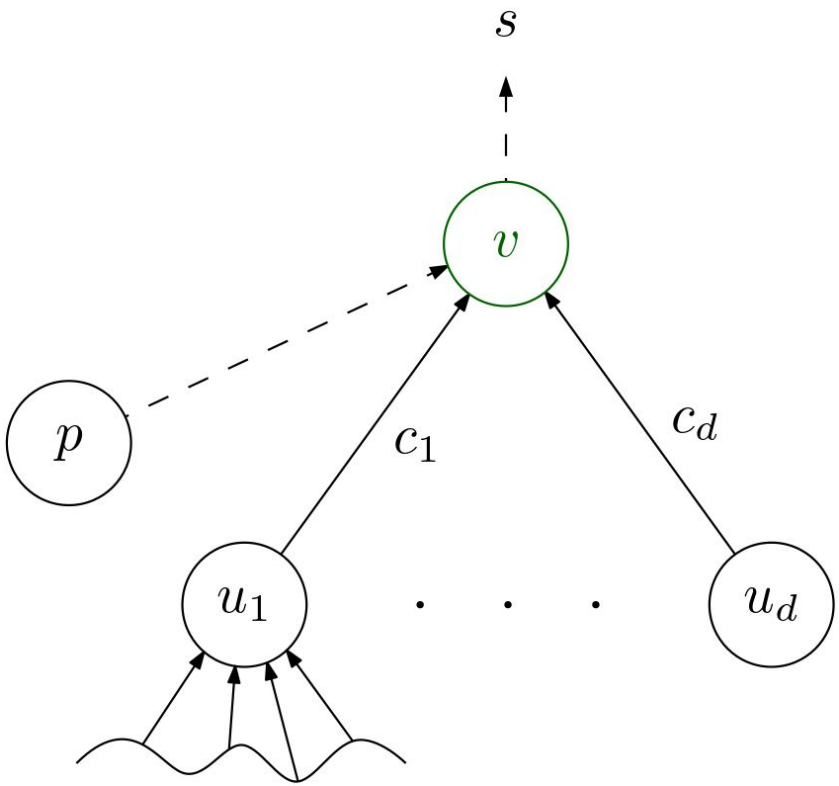
# SD-GSD



# How do ROs help?

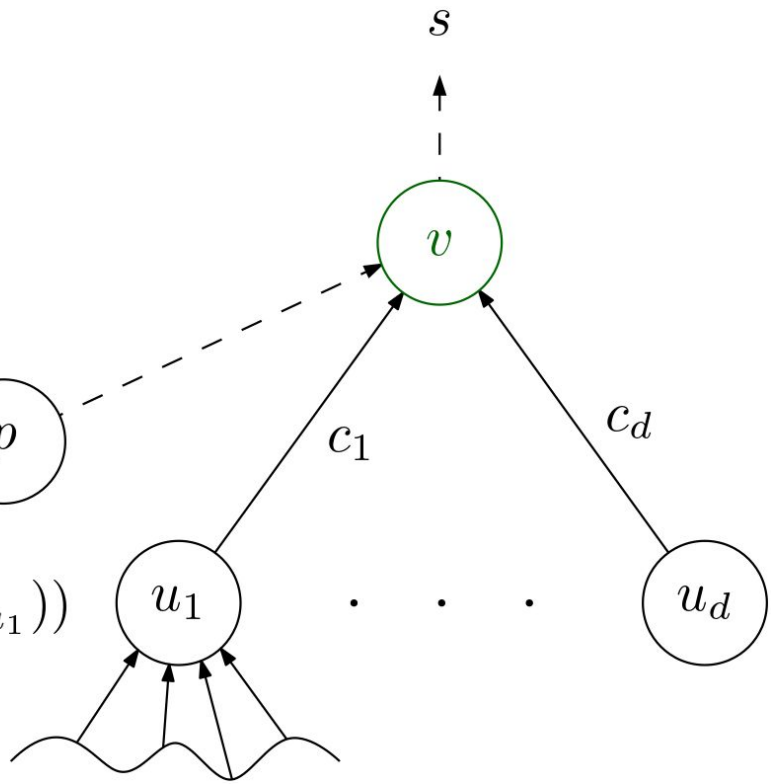


# How do ROs help?

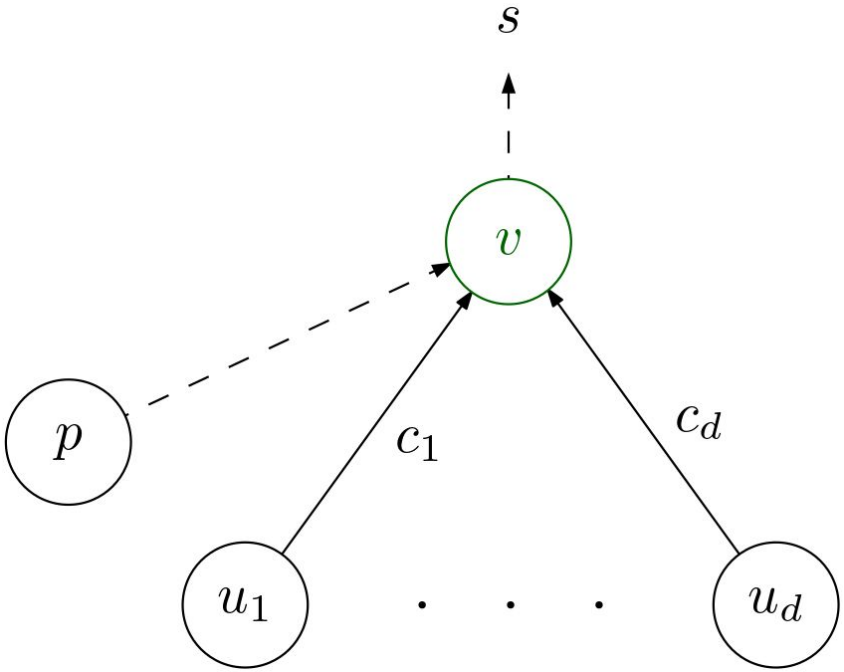


# How do ROs help?

$$(pk_{u_1}, sk_{u_1}) = \mathrm{Gen}(H_{\mathrm{gen}}(s_{u_1}))$$

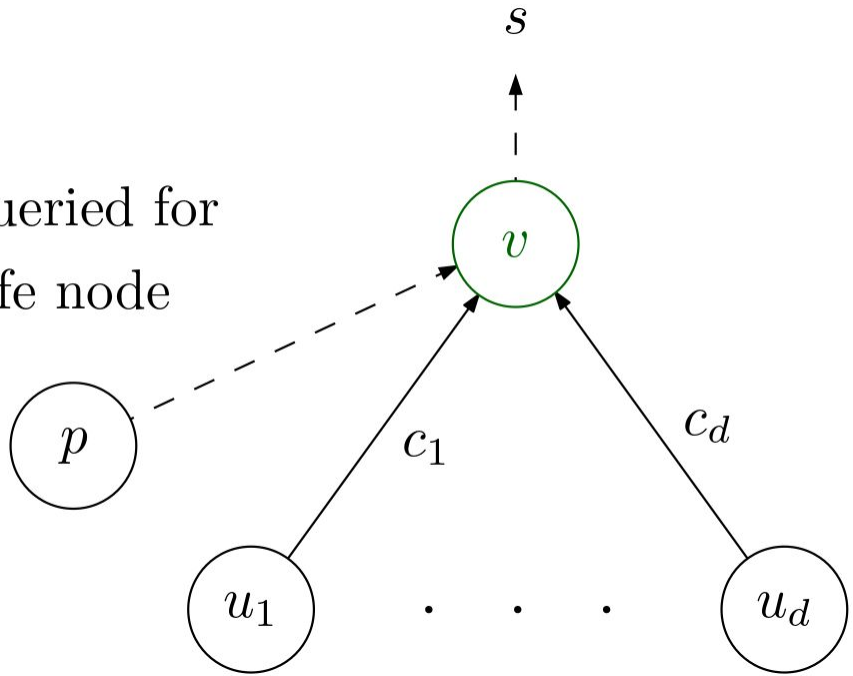


# Proving security in the ROM

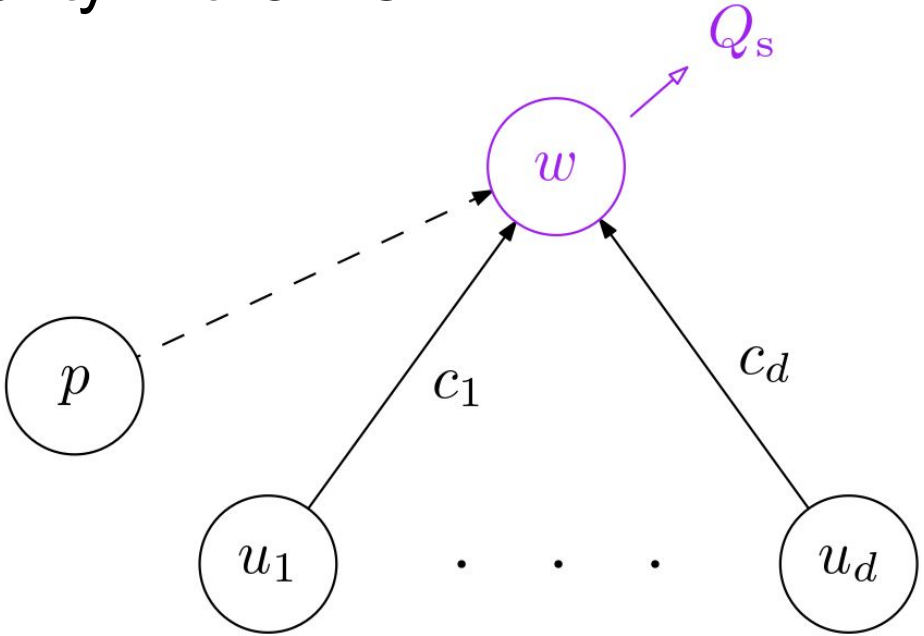


# Proving security in the ROM

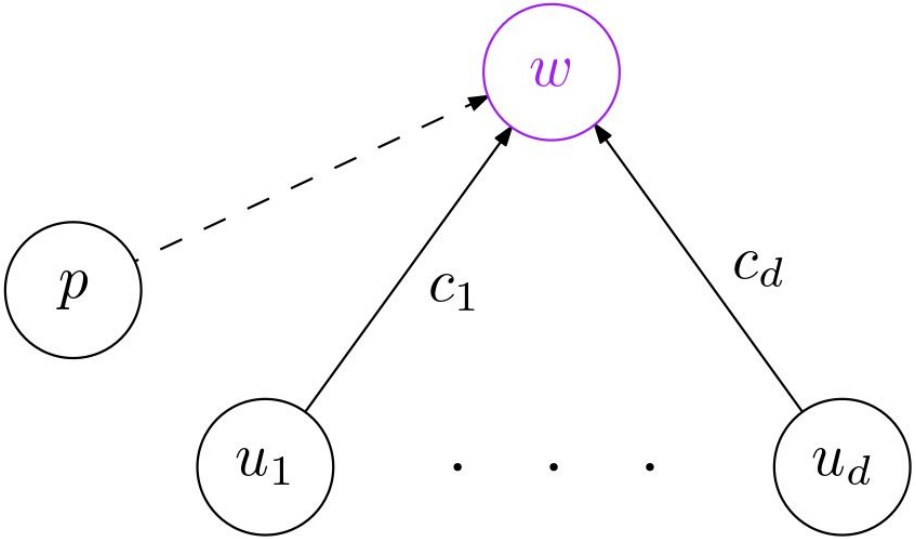
$Q_{\mathrm{s}} := H_{\mathrm{gen}}$ or $H_{\mathrm{dep}}$ queried for the seed of a safe node



# Proving security in the ROM

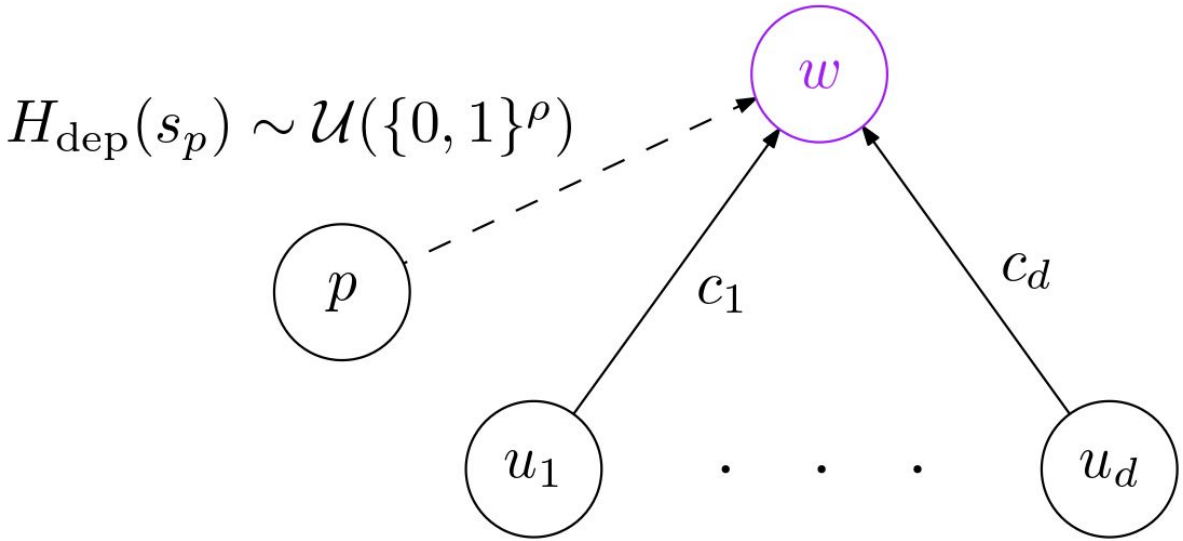


# Proving security in the ROM

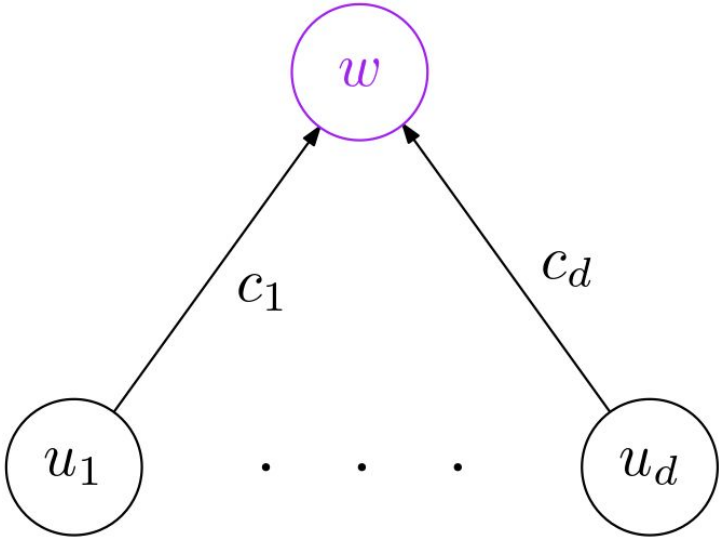



$$H_{\text{gen}}(s_{u_i}) \sim \mathcal{U}(\{0,1\}^{\rho})$$
$$\Downarrow$$
$$(pk_{u_i}, sk_{u_i}) \sim \text{Gen}$$

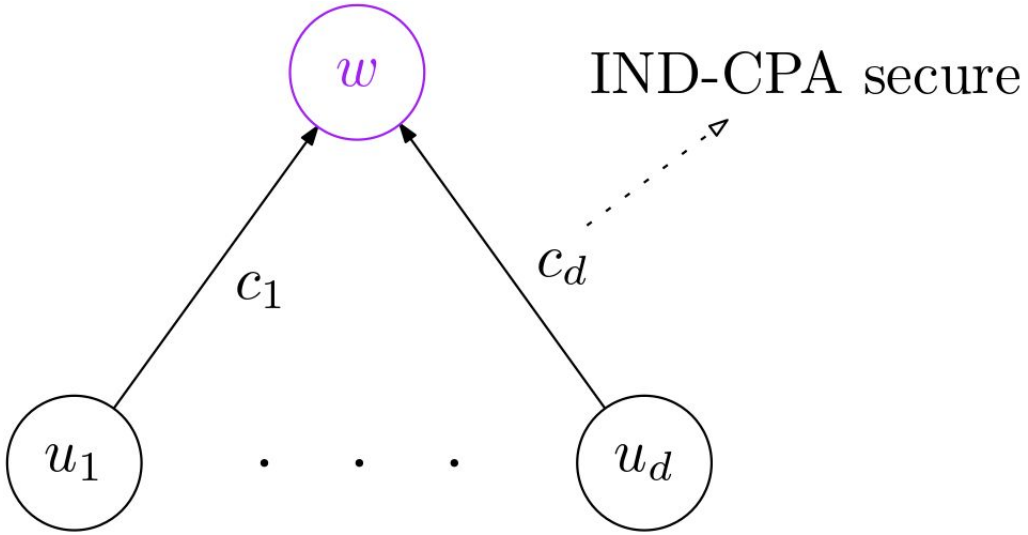
# Proving security in the ROM



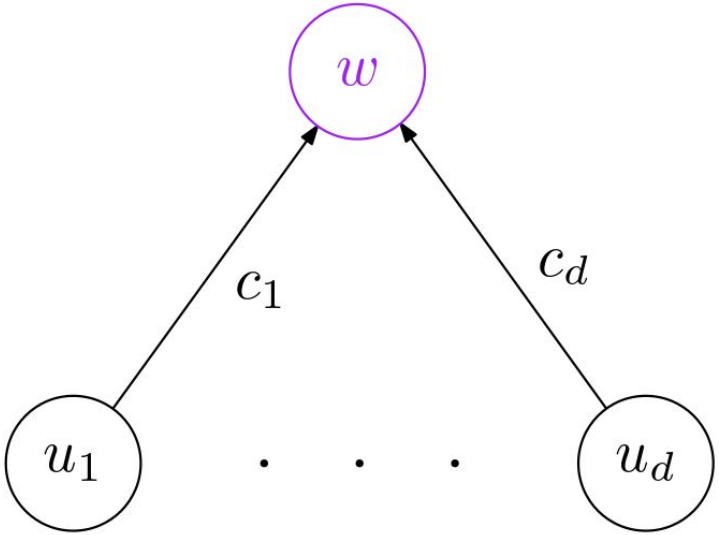
# Proof in [ACC+19]



# Proof in [ACC+19]



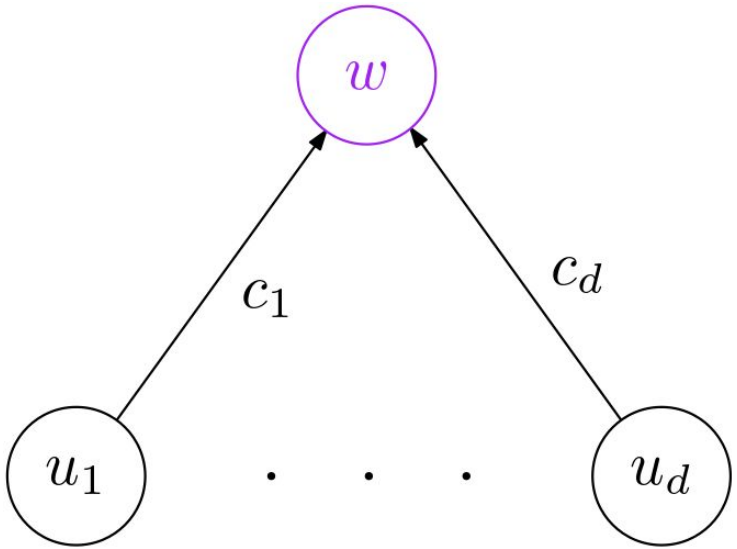
# Proof in [ACC+19]



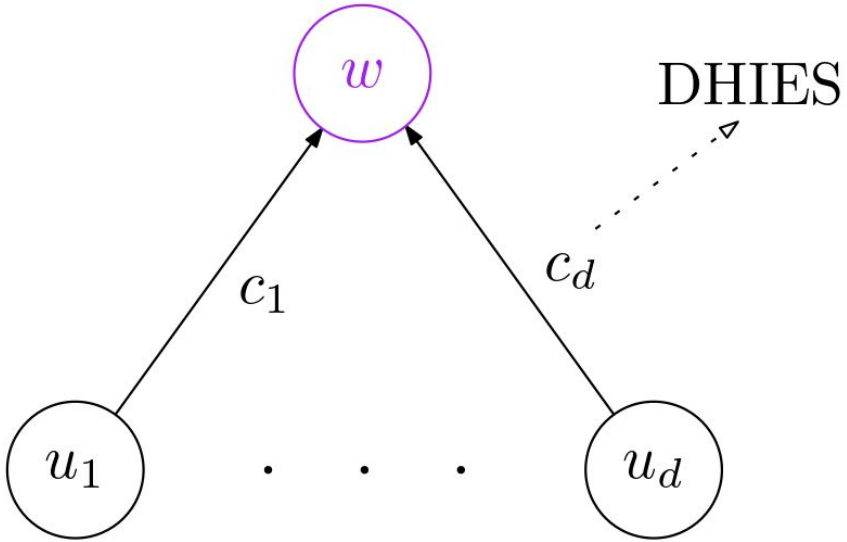

$$\Pr[Q_{\mathrm{s}}] \leq N^2 \cdot \varepsilon_{\text{IND-CPA}} + \mathrm{negl}$$

where $N := \#\text{nodes}$

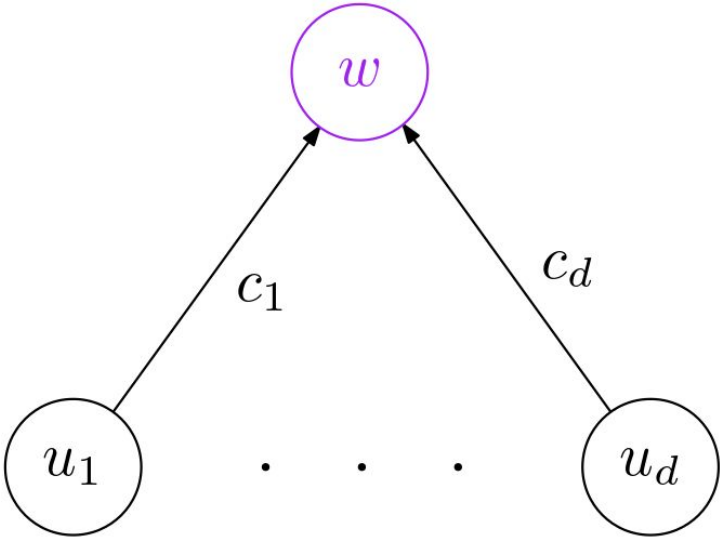
# Our approach



# Our approach



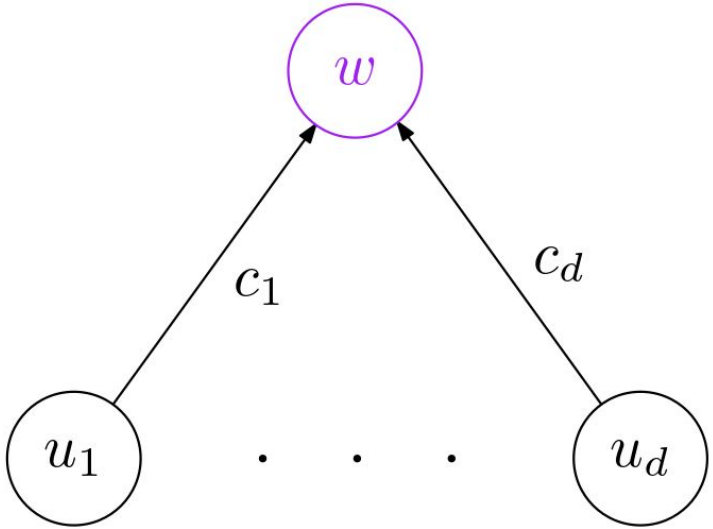
# Our approach




$$(pk_{u_i}, sk_{u_i}) = (g^{x_i}, x_i)$$

where $x_i \leftarrow [|\mathbb{G}|]$

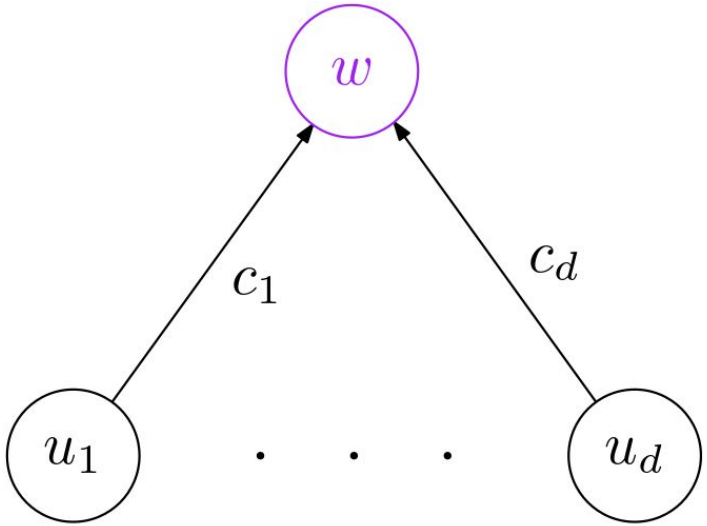
# Our approach




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$$

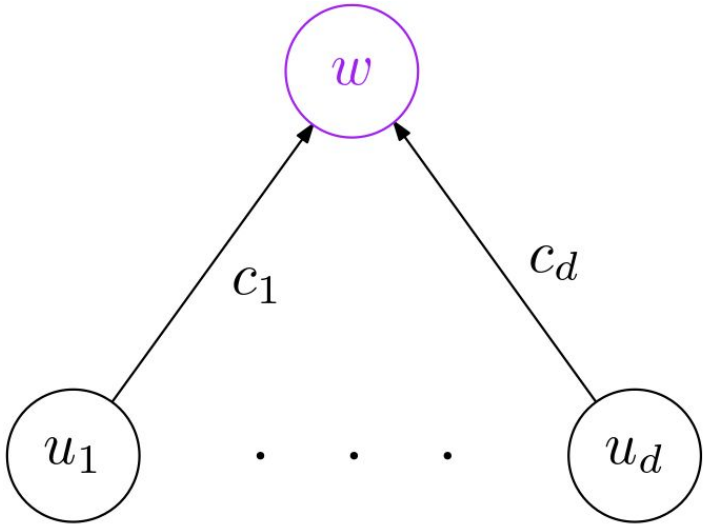
# Our approach




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$$

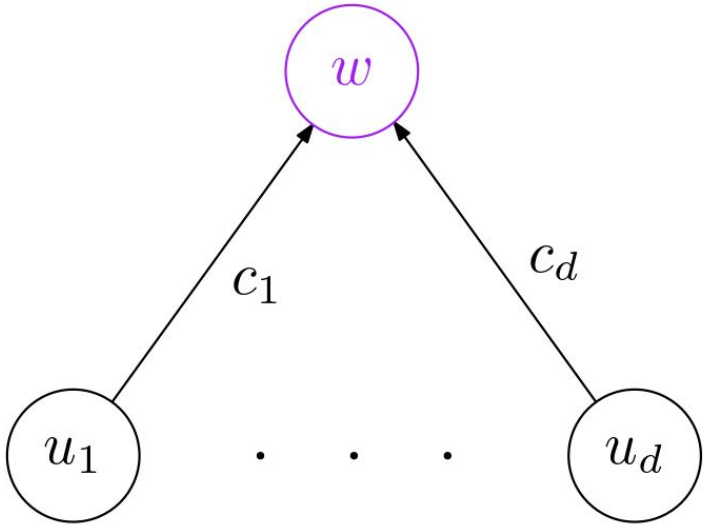
# Our approach




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$$

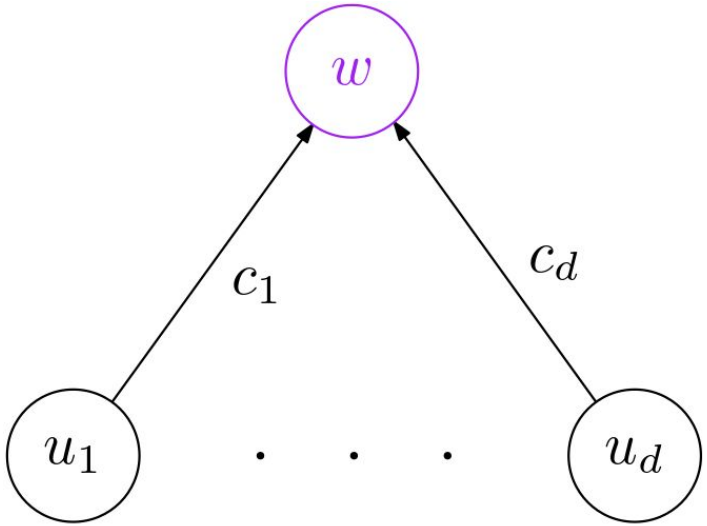
# Our approach




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$$

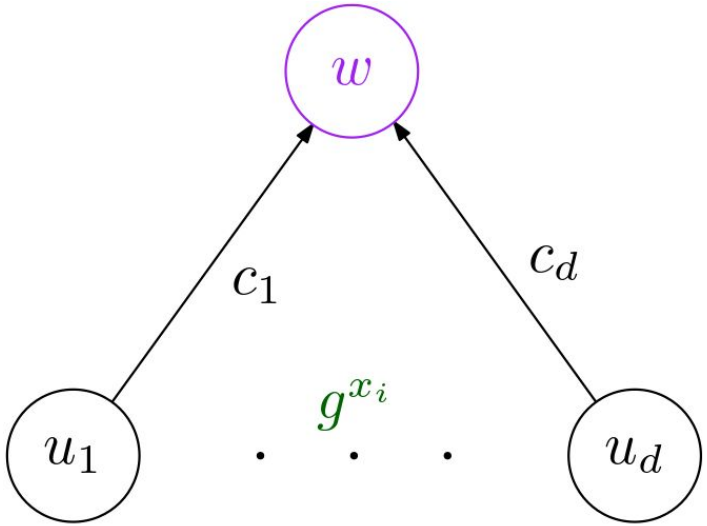
# Our approach




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$$

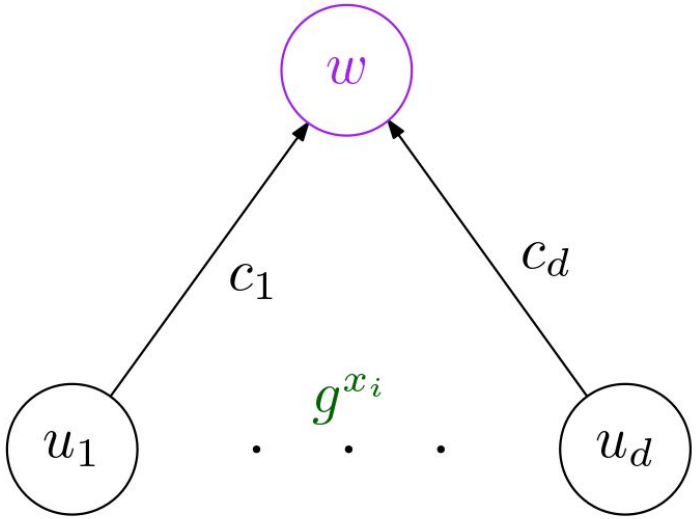
# Our approach




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$$

# Our approach

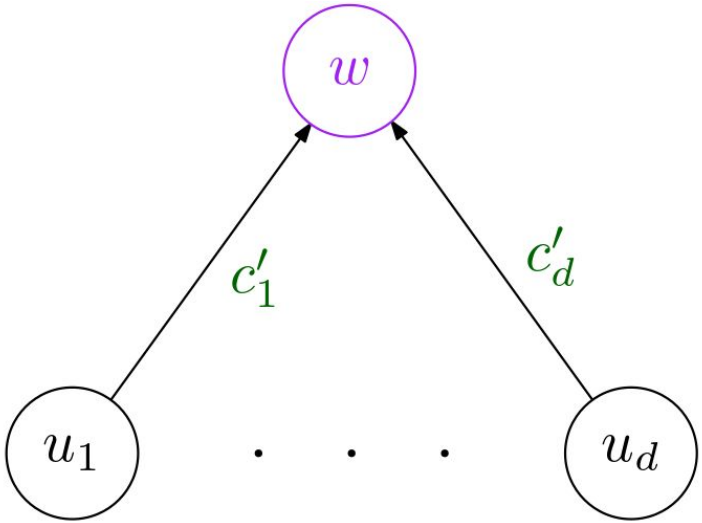



$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_w) \rangle$$

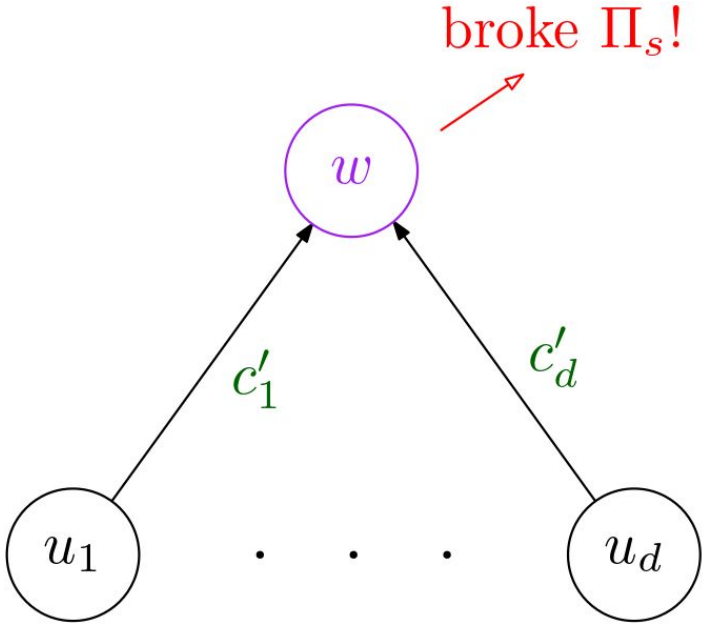
where $y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_i \cdot y_i})$

solved CDH!

# Our approach

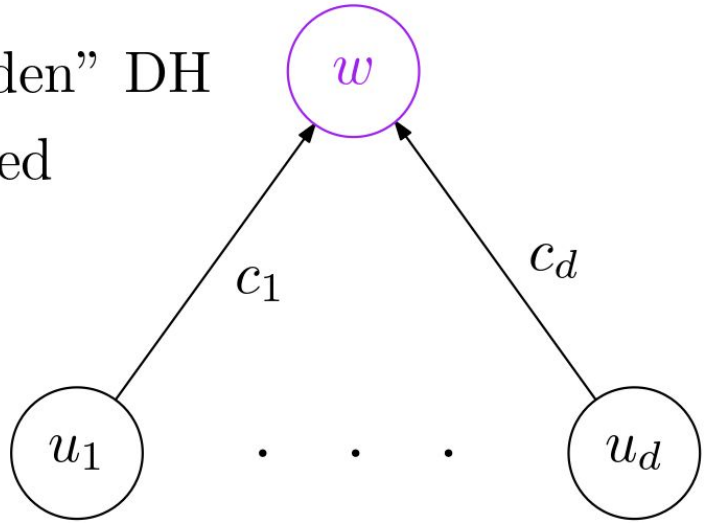


# Our approach



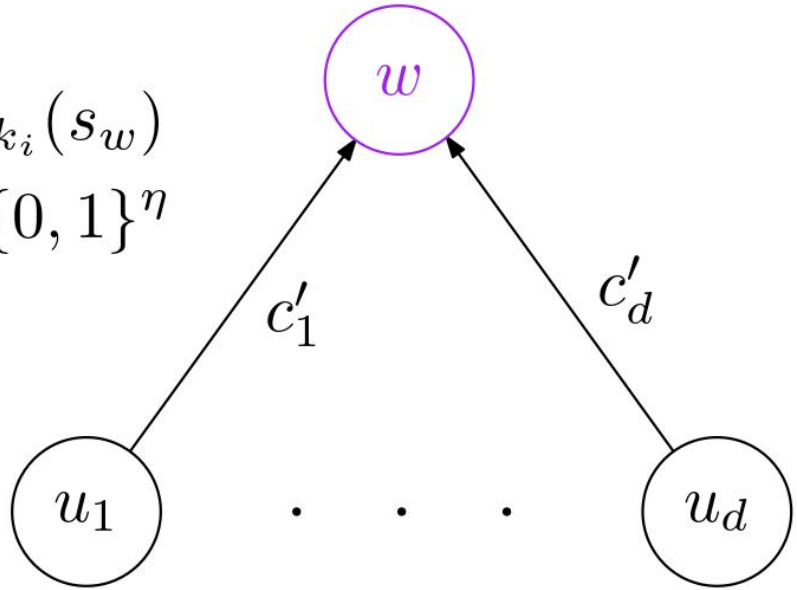
# The proof

$F_{\mathrm{DH}} := H_{\mathrm{DH}}$ queried for "hidden" DH key *before* $Q_s$ triggered



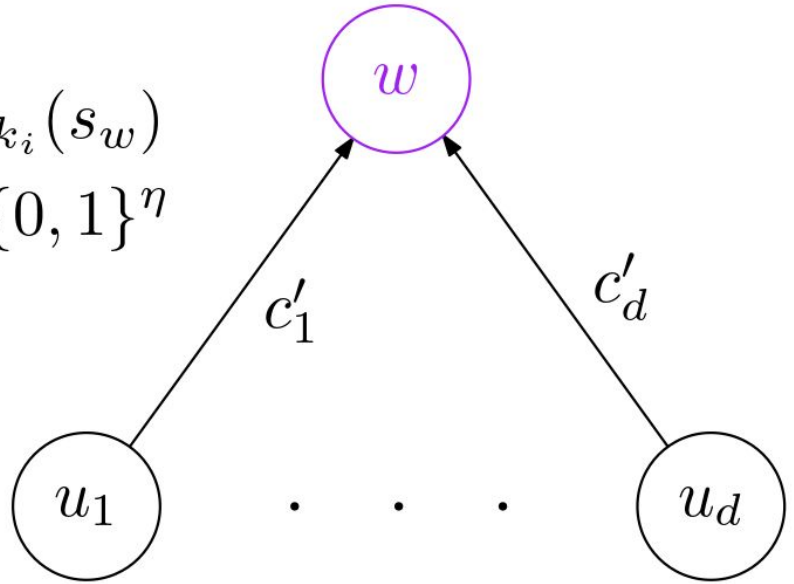
# Reducing to EAV security: $Q_{\mathrm{s}} \wedge \overline{F_{\mathrm{DH}}}$

$$c'_i \leftarrow \Pi_s.\mathrm{Enc}_{k_i}(s_w)$$
$$\text{where } k_i \leftarrow \{0,1\}^\eta$$



# Reducing to EAV security: $Q_{\mathrm{s}} \wedge \overline{F_{\mathrm{DH}}}$

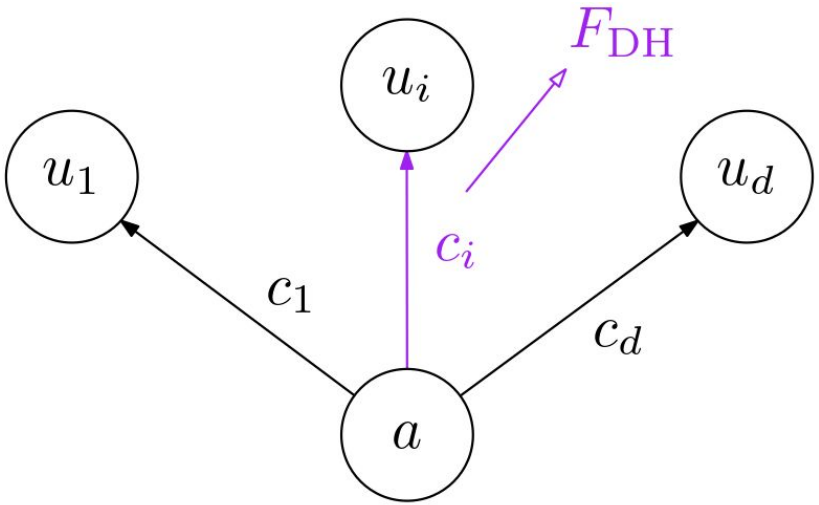
$$c'_i \leftarrow \Pi_s.\mathrm{Enc}_{k_i}(s_w)$$
$$\text{where } k_i \leftarrow \{0,1\}^{\eta}$$




$$\Pr\left[Q_{\mathrm{s}} \wedge \overline{F_{\mathrm{DH}}}\right] \leq \delta \cdot N \cdot \epsilon_{\mathrm{EAV}} + \mathrm{negl}$$

# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$

# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$

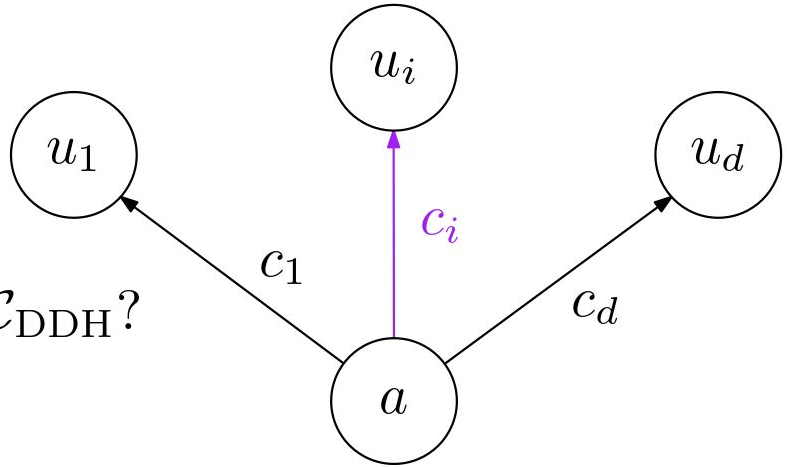



$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_{u_i}) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_a \cdot y_i})$$

# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$

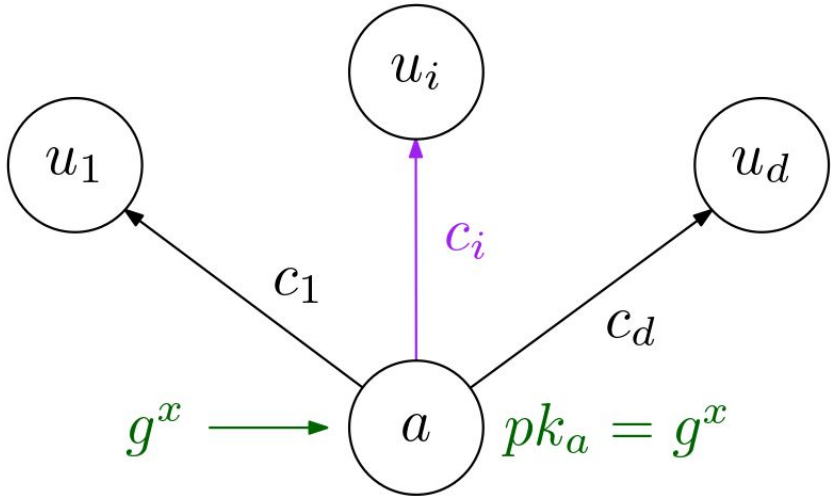
Where to embed $(g^x, g^y) \leftarrow \mathcal{C}_{\mathrm{DDH}}$?




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_{u_i}) \rangle$$

where $y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x_a \cdot y_i})$

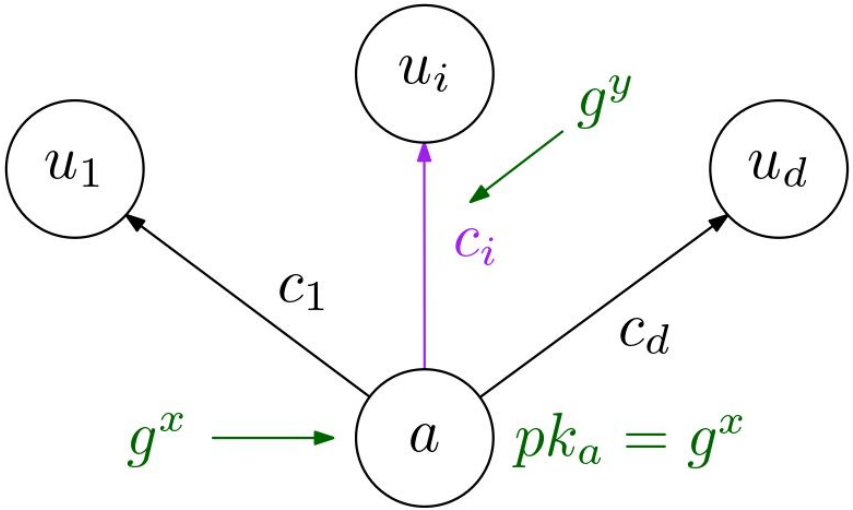
# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_{u_i}) \rangle$$

$$\text{where } y_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x \cdot y_i})$$

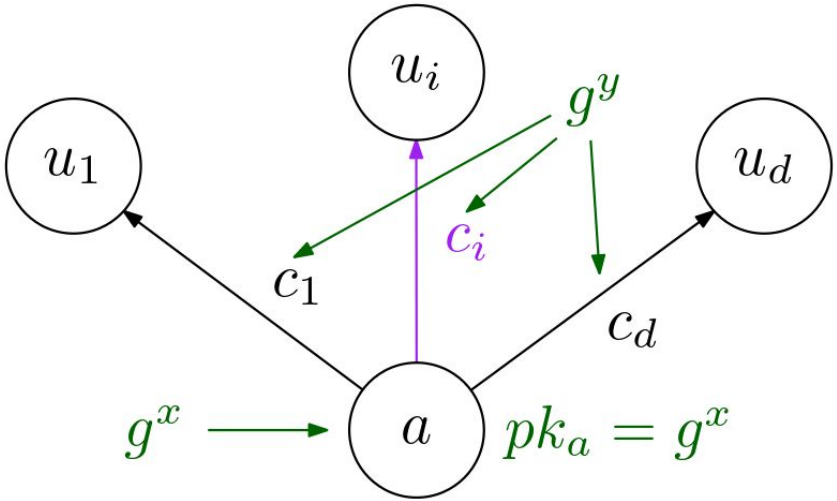
# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_{u_i}) \rangle$$

$$\text{where } y_i = y, k_i = H_{\mathrm{DH}}(g^{x \cdot y})$$

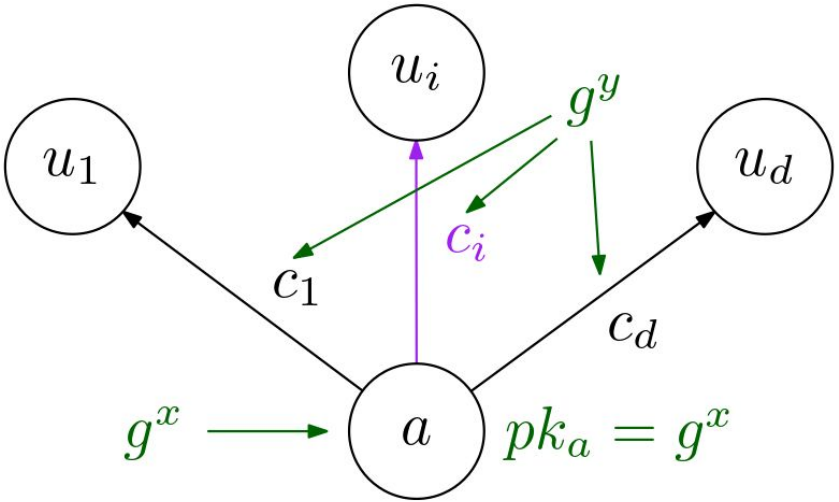
# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$




$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_{u_i}) \rangle$$

$$\text{where } y_i = y + r_i, r_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x \cdot y_i})$$

# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$

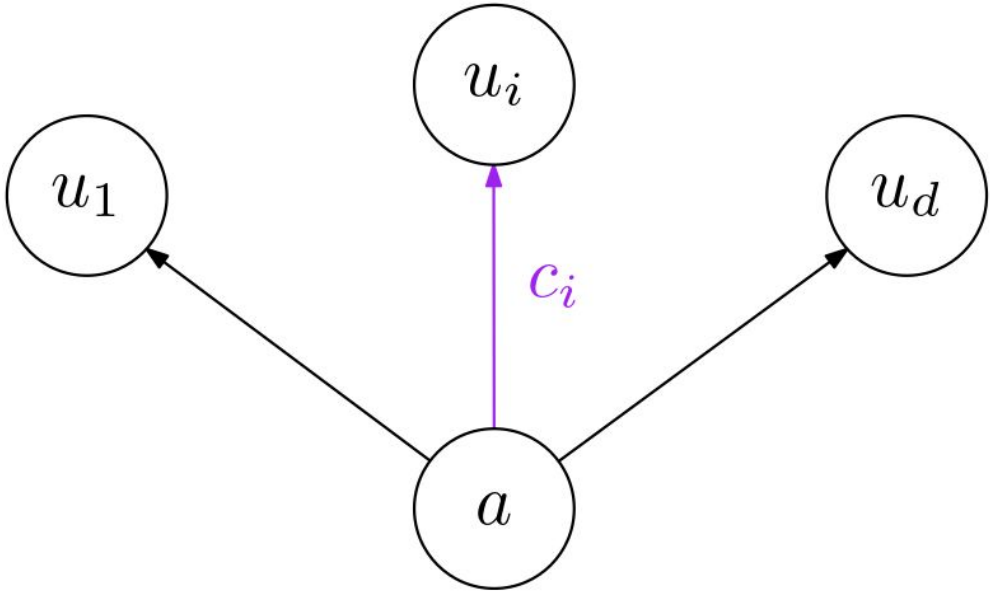



$g^{x \cdot y}$

$$c_i = \langle g^{y_i}, \Pi_s.\mathrm{Enc}_{k_i}(s_{u_i}) \rangle$$

$$\text{where } y_i = y + r_i, r_i \leftarrow [|\mathbb{G}|], k_i = H_{\mathrm{DH}}(g^{x \cdot y_i})$$

# Reducing to the DDH problem: $Q_{\mathrm{s}} \wedge F_{\mathrm{DH}} \subseteq F_{\mathrm{DH}}$




$$\Pr[F_{\mathrm{DH}}] \leq N \cdot \epsilon_{\mathrm{DDH}} + \mathrm{negl}$$

# Overall

$$\Pr[Q_{\mathrm{s}}] \leq \delta \cdot N \cdot \epsilon_{\mathrm{EAV}} + N \cdot \epsilon_{\mathrm{DDH}} + \mathrm{negl}$$

# Overall

$$\Pr[Q_{\mathrm{s}}] \leq \delta \cdot N \cdot \epsilon_{\mathrm{EAV}} + N \cdot \epsilon_{\mathrm{DDH}} + \mathrm{negl}$$

vs.

$$\Pr[Q_{\mathrm{s}}] \leq N^2 \cdot \epsilon_{\text{IND-CPA}} + \mathrm{negl}$$

# Overall

#commits #users

$$\delta \cdot N = \mathcal{O}(c \cdot u \cdot \log u)$$

vs.

$$N = \mathcal{O}((c \cdot \log u)^2)$$