Constant-Round Authenticated Group Key Exchange for Dynamic Groups

Hyun-Jeong Kim, Su-Mi Lee, Dong Hoon Lee

Center for Information Security Technologies,

Korea University

Outline

- Introduction
- Related Work
- Our Constant-Round AGKE Protocol
- Security
- Efficiency
- Contribution
- Further Research

Introduction

- Secure and efficient AGKE protocols for the group communication in a wireless network
  - The limitation on the bandwidth of the wireless network
  - The limitation on the computing power and speed
  - The limitation on the storage
  - The dynamic network topology
  - The absence of the third party (in an ad-hoc network)

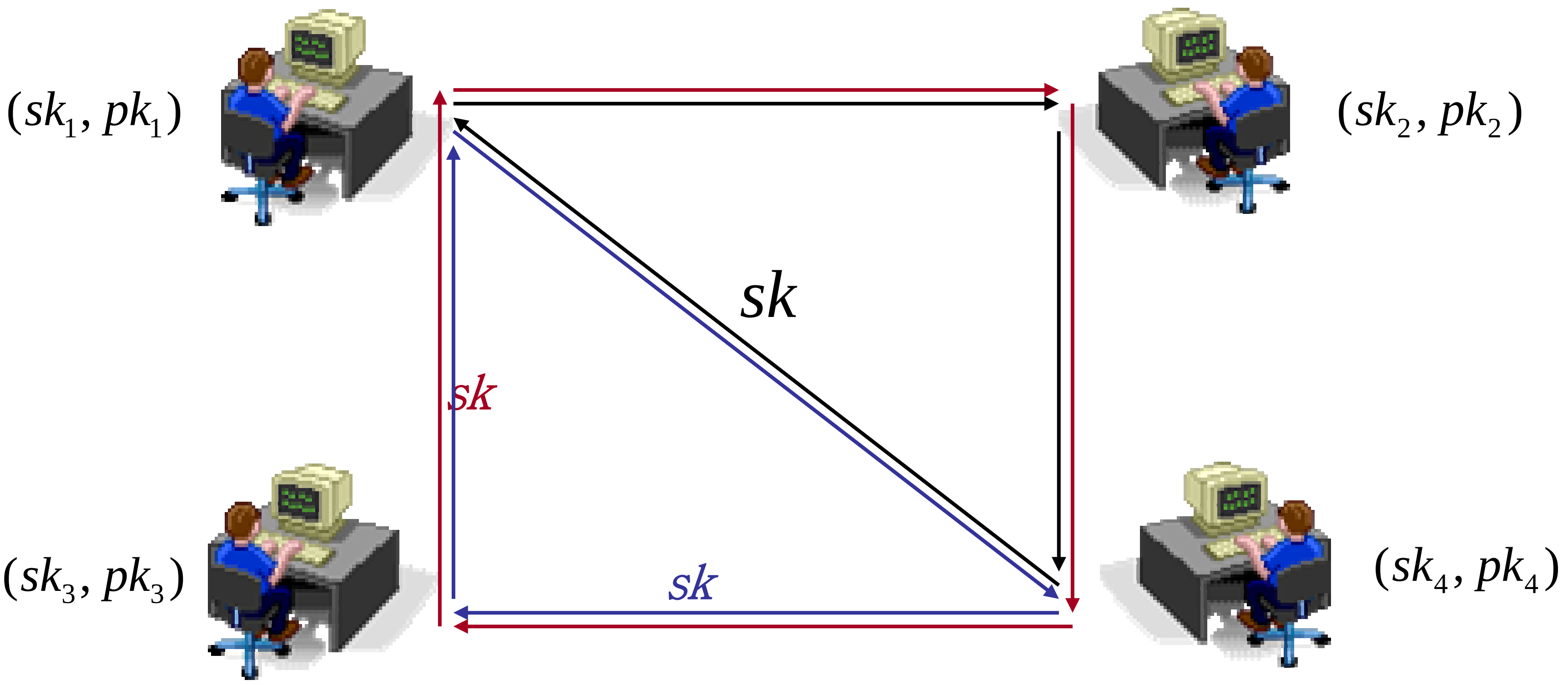
⇨ Constant-round AGKE protocols for dynamic groups

Related Work

- Static GKE protocols with constant rounds
  - Burmester and Desmedt [BD94]
- Static AGKE protocols with constant rounds
  - Tzeng and Tzeng [TT00]
  - Boyd and Nieto [BN03]
  - Katz and Yung [KY03]
  - Bresson and Catalano [BC04]
- Dynamic AGKE protocols with constant rounds
  - Bresson et al. [Bre03]

Our AGKE Protocol-Model

Key Generation	Setup	Join	Leave



Setup

- Parameters and Notations

  $\mathbf{G} = \langle g \rangle$: a cyclic group of prime order p

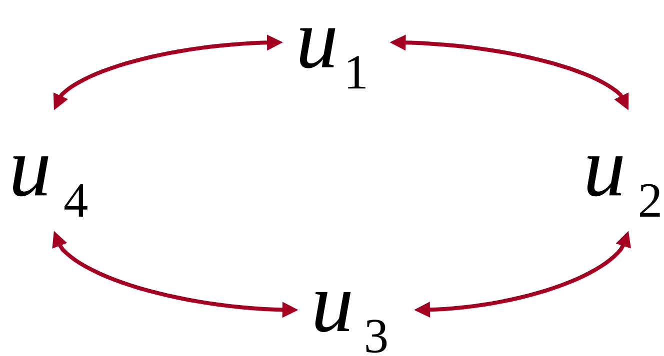
  $H : \{0,1\}^* \rightarrow \{0,1\}^{\ell}$: a one-way hash function

  $\Sigma = (K, S, V)$: a secure signature scheme

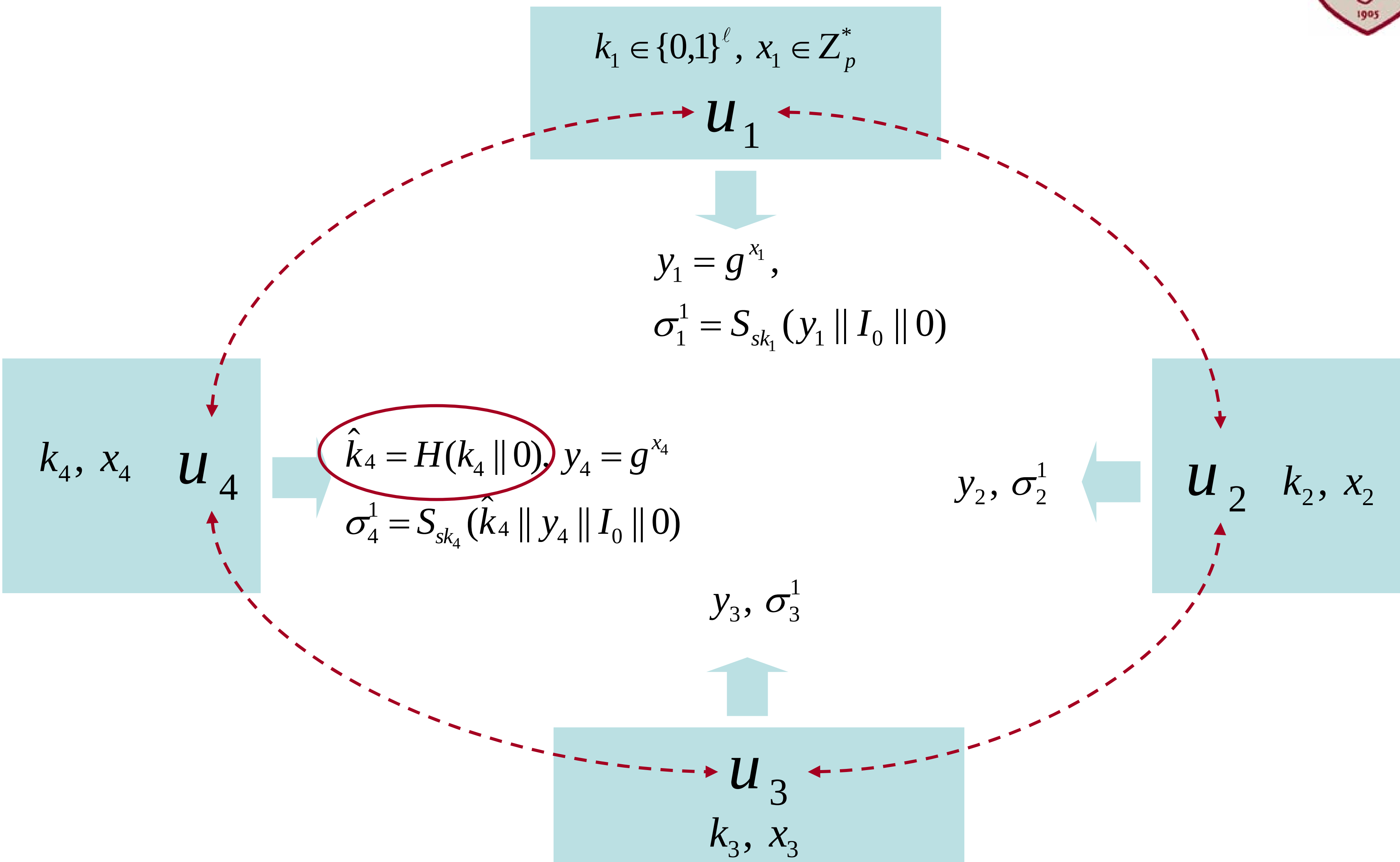
  $G_0 = \{u_1, u_2, u_3, u_4\}$: an initial group of members

  $I_0 = ID_{u_1} \| ID_{u_2} \| ID_{u_3} \| ID_{u_4}$

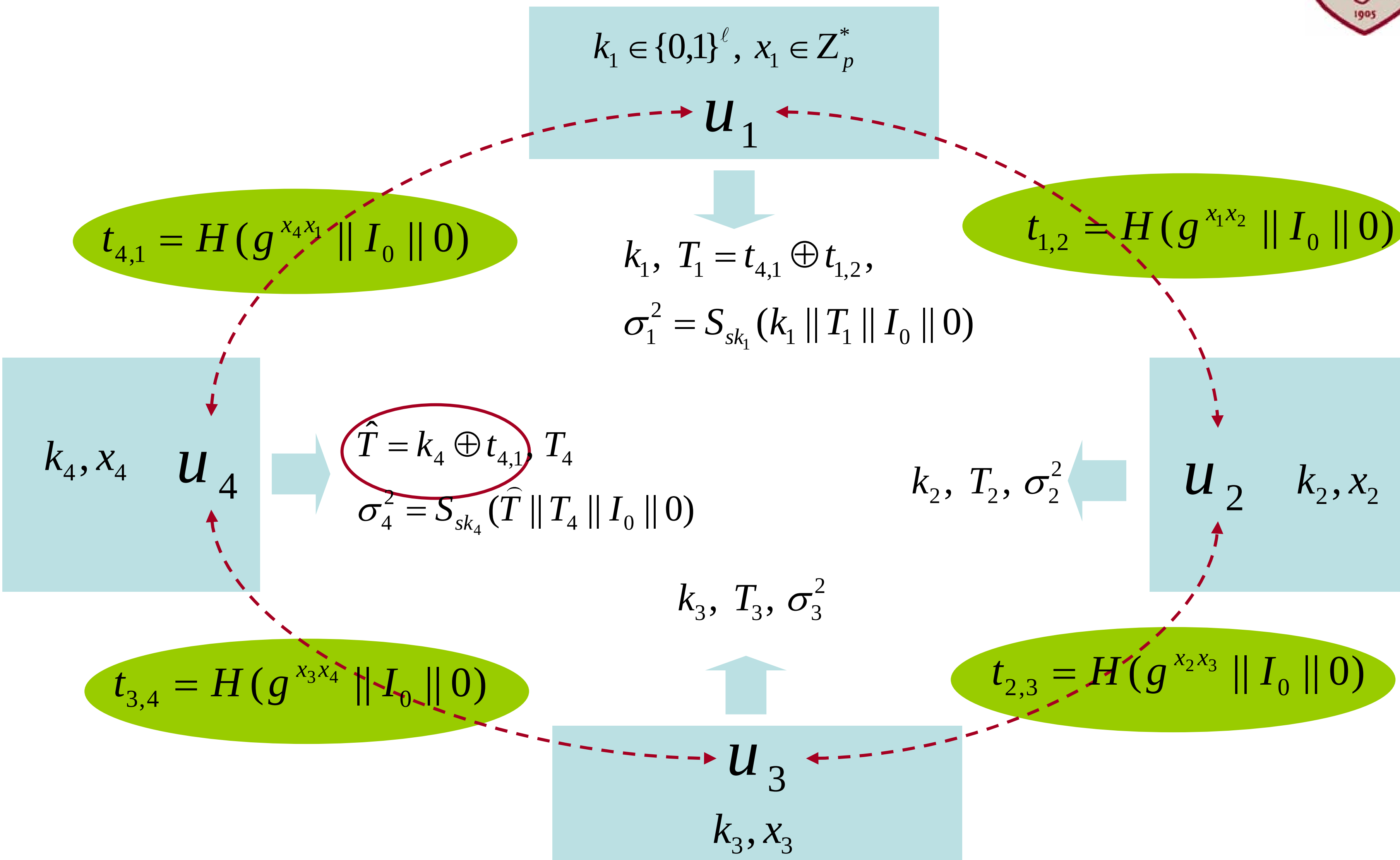
- A ring structure between members



Setup (Round1)



Setup (Round2)



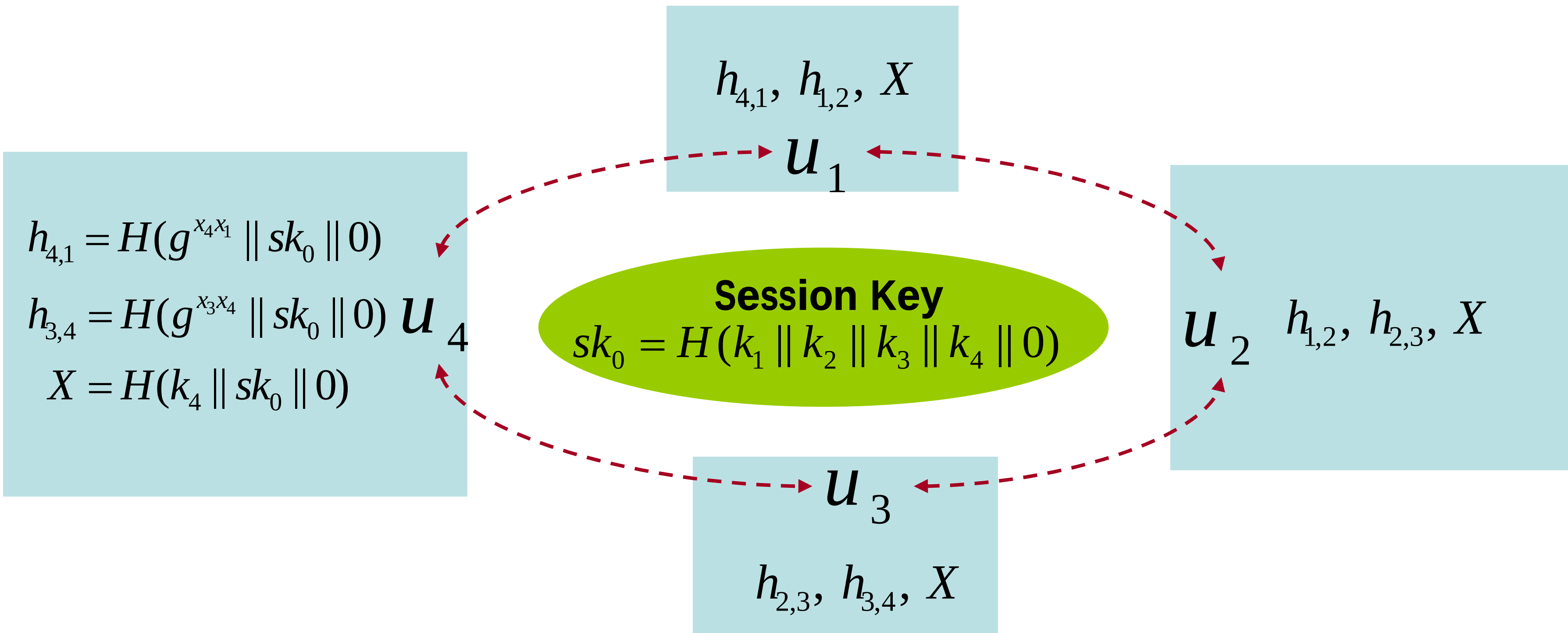
Setup(Post-Computation)

- Message Validity Check

  For the member u_2,

  $$1.\ (T_1 \oplus T_3 \oplus T_4) \oplus t_{2,3} \stackrel{?}{=} t_{1,2}$$

  $$2.\ H(\{(T_3 \oplus T_4) \oplus t_{2,3}\} \oplus \hat{T} \,\|\, 0) \stackrel{?}{=} \hat{k}_4$$

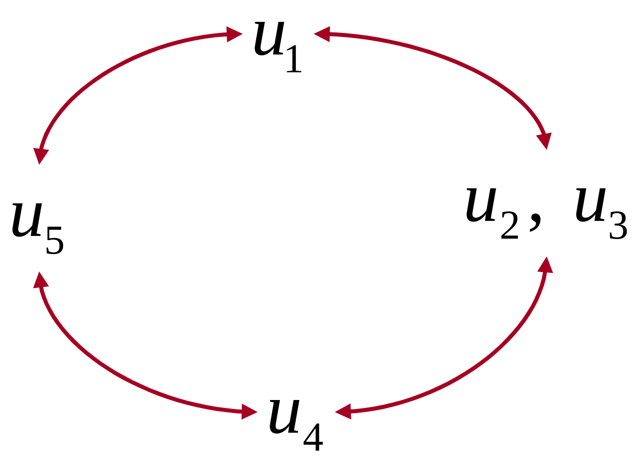


Join

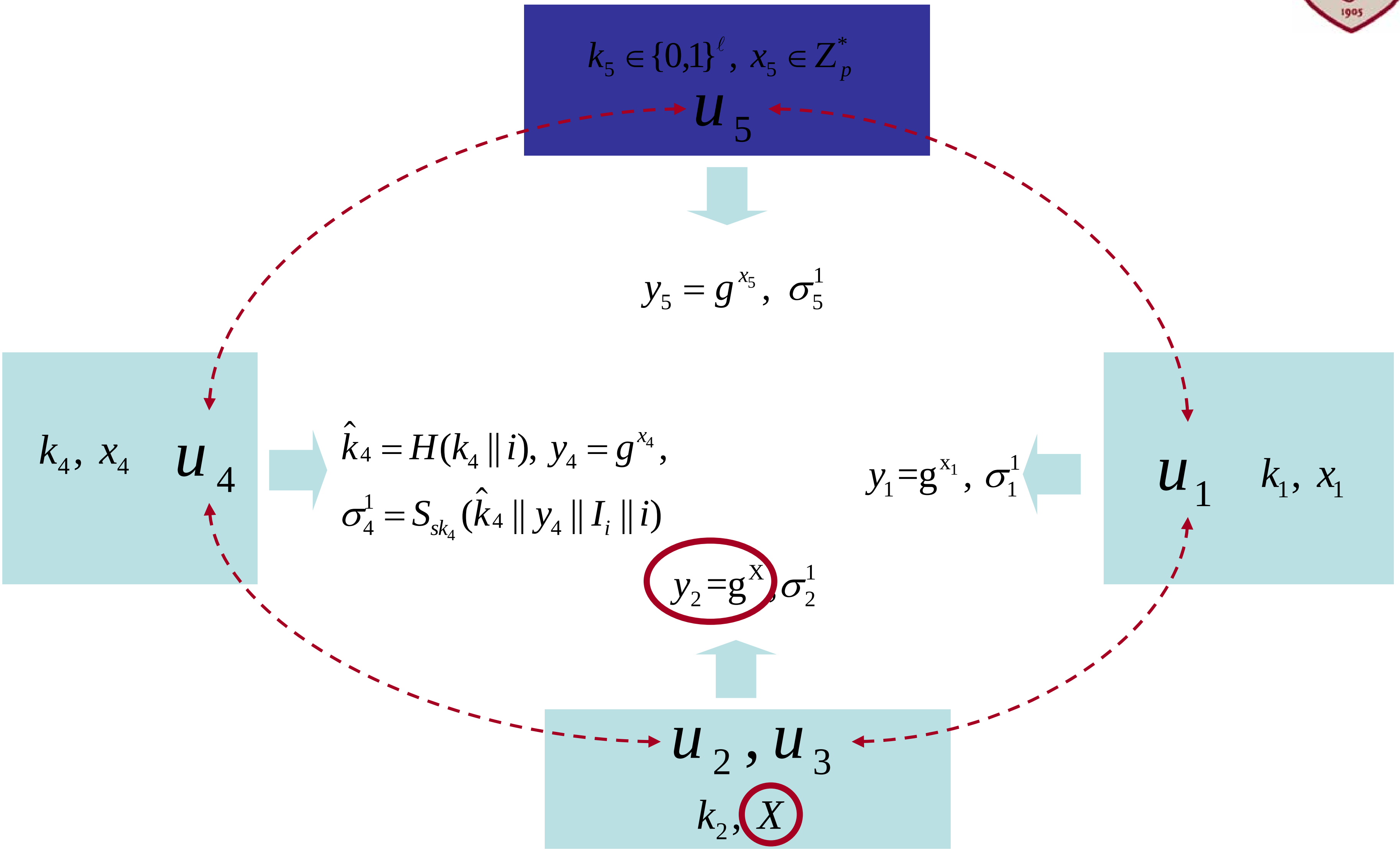
$G_{i-1} = \{ u_1, u_2, u_3, u_4 \}$ - a current group, u_5 - a new member

$\Rightarrow$ $G_i = \{ u_1, u_2, u_3, u_4, u_5 \}$ $\quad I_i = ID_{u_1} \| ID_{u_2} \| ID_{u_3} \| ID_{u_4} \| ID_{u_5}$

- A ring structure between members

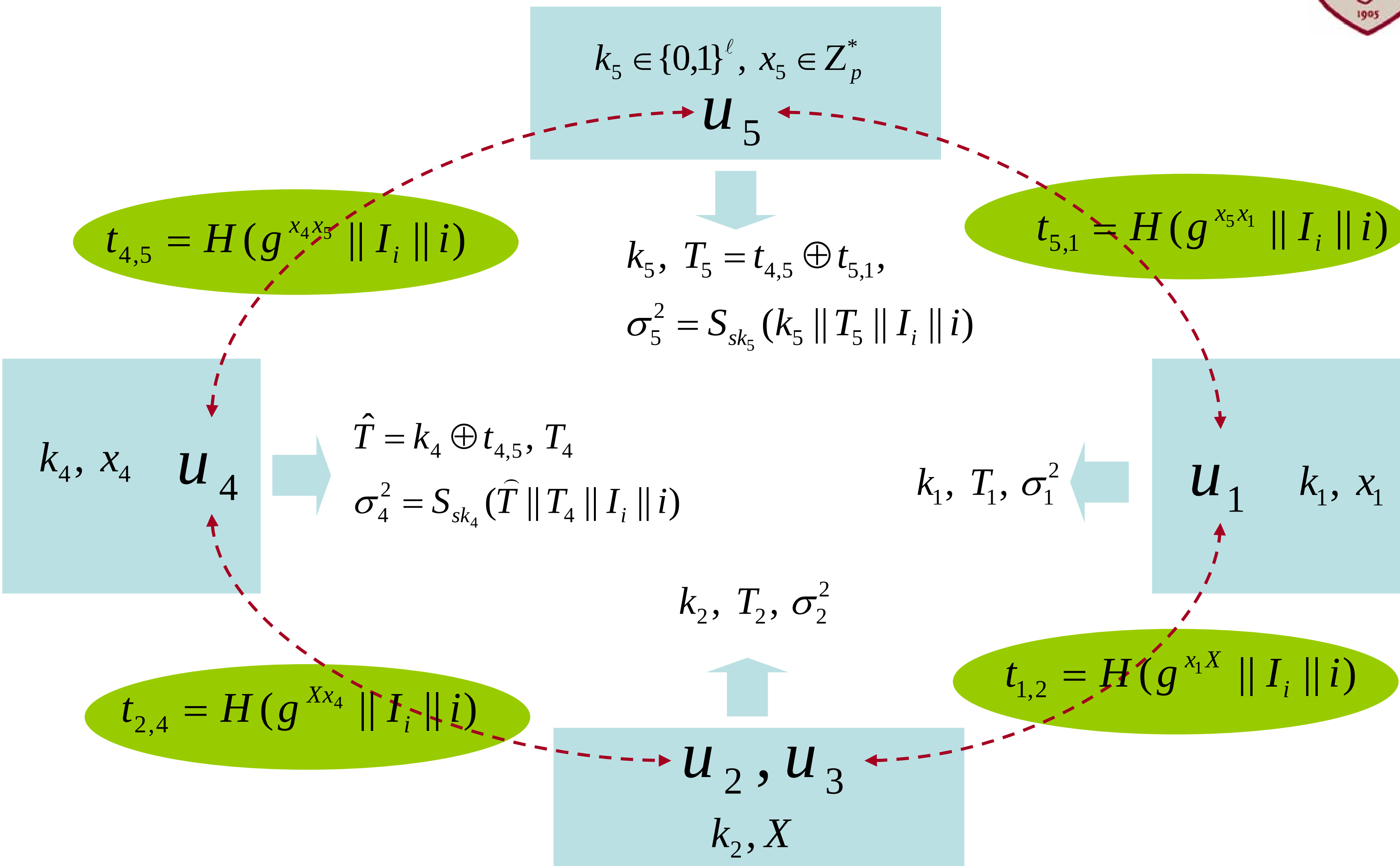


Join(Round1)



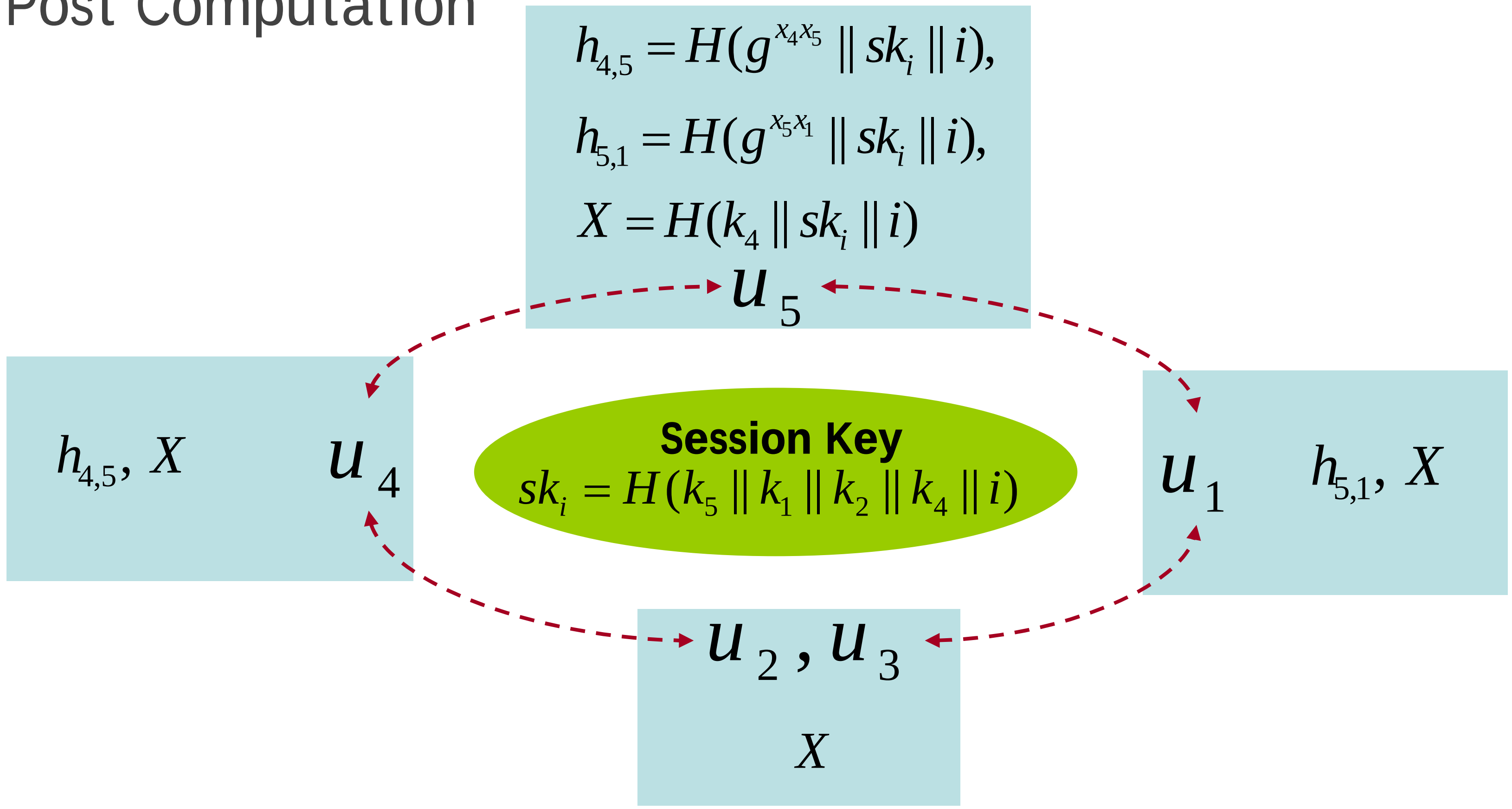
$k_5 \in \{0,1\}^{\ell}, x_5 \in Z_p^*$
u_5
$y_5 = g^{x_5}, \sigma_5^1$
k_4, x_4
u_4
$\hat{k}_4 = H(k_4 \| i), y_4 = g^{x_4},$
$\sigma_4^1 = S_{sk_4}(\hat{k}_4 \| y_4 \| I_i \| i)$
$y_1 = g^{x_1}, \sigma_1^1$
u_1
k_1, x_1
$y_2 = g^X, \sigma_2^1$
u_2, u_3
k_2, X

Join(Round2)


$k_5 \in \{0,1\}^{\ell}, \ x_5 \in Z_p^*$
u_5
$t_{4,5} = H(g^{x_4 x_5} \parallel I_i \parallel i)$
$t_{5,1} = H(g^{x_5 x_1} \parallel I_i \parallel i)$
$k_5, \ T_5 = t_{4,5} \oplus t_{5,1},$
$\sigma_5^2 = S_{sk_5}(k_5 \parallel T_5 \parallel I_i \parallel i)$
$k_4, \ x_4$
u_4
$\hat{T} = k_4 \oplus t_{4,5}, \ T_4$
$\sigma_4^2 = S_{sk_4}(\hat{T} \parallel T_4 \parallel I_i \parallel i)$
$k_1, \ T_1, \ \sigma_1^2$
u_1
$k_1, \ x_1$
$k_2, \ T_2, \ \sigma_2^2$
$t_{1,2} = H(g^{x_1 X} \parallel I_i \parallel i)$
$t_{2,4} = H(g^{X x_4} \parallel I_i \parallel i)$
u_2, u_3
k_2, X

Join(Post-Computation)

- Message Validity Check
- Post Computation

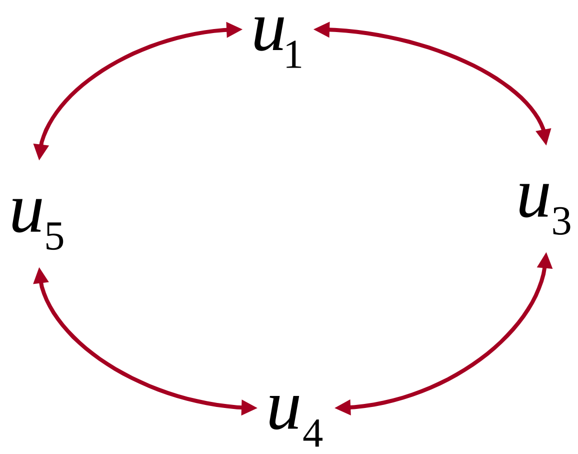


Leave

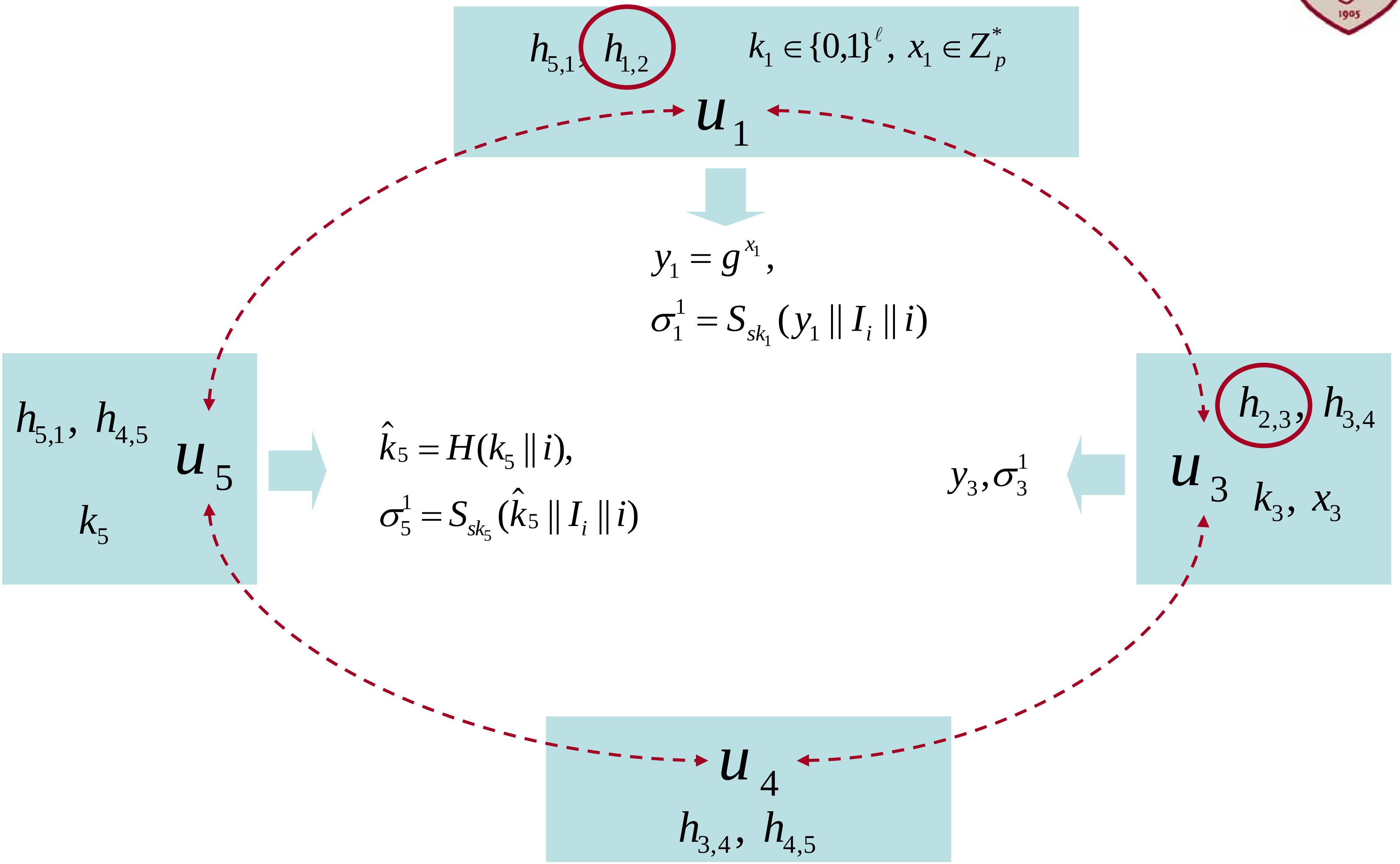
$G_{i-1} = \{ u_1, u_2, u_3, u_4, u_5 \}$ - a current group, u_2 - a leaving member

→ $G_i = \{ u_1, u_3, u_4, u_5 \}$ $I_i = ID_{u_1} \| ID_{u_3} \| ID_{u_4} \| ID_{u_5}$

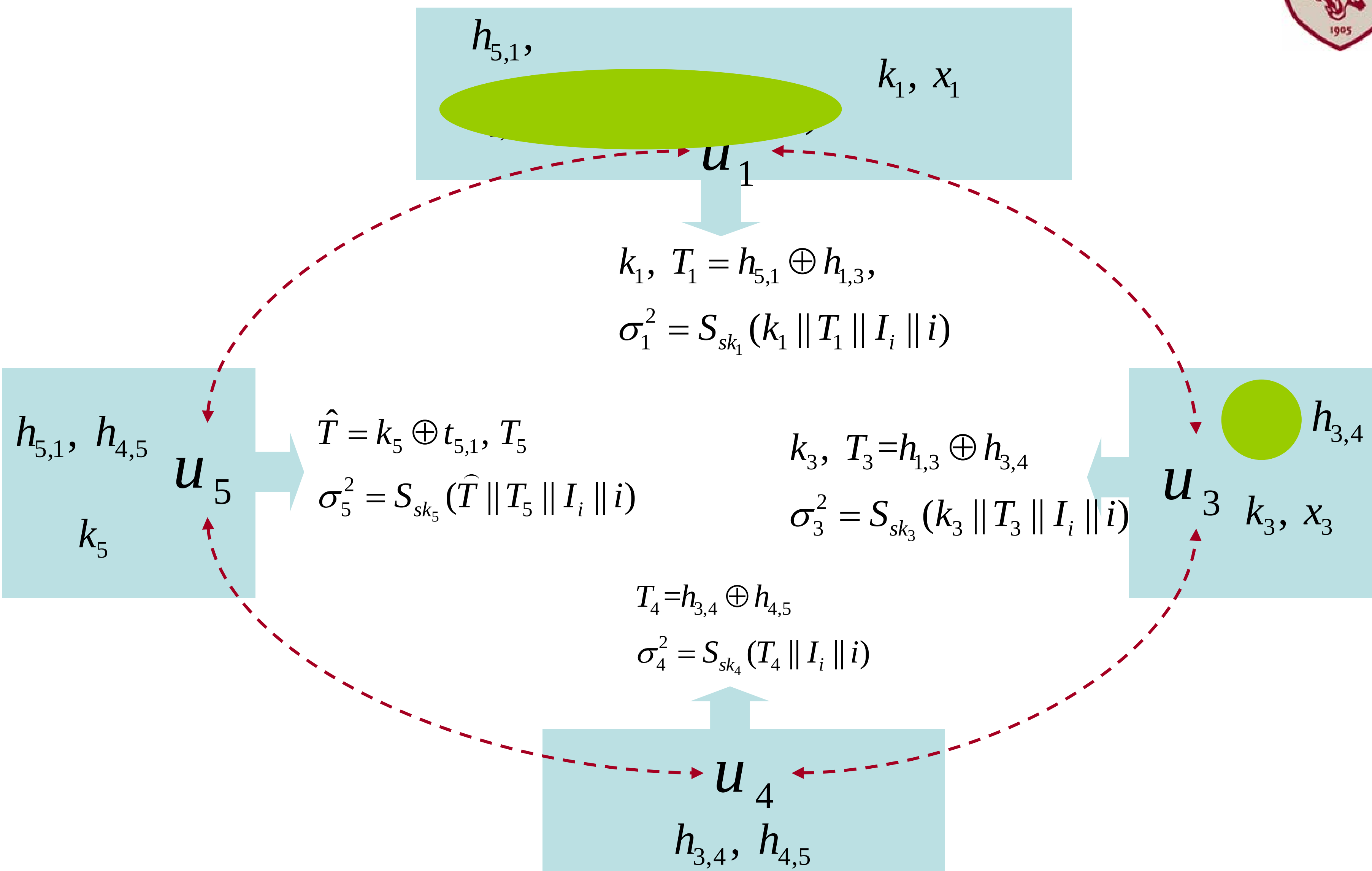
- A ring structure between members



Leave(Round1)

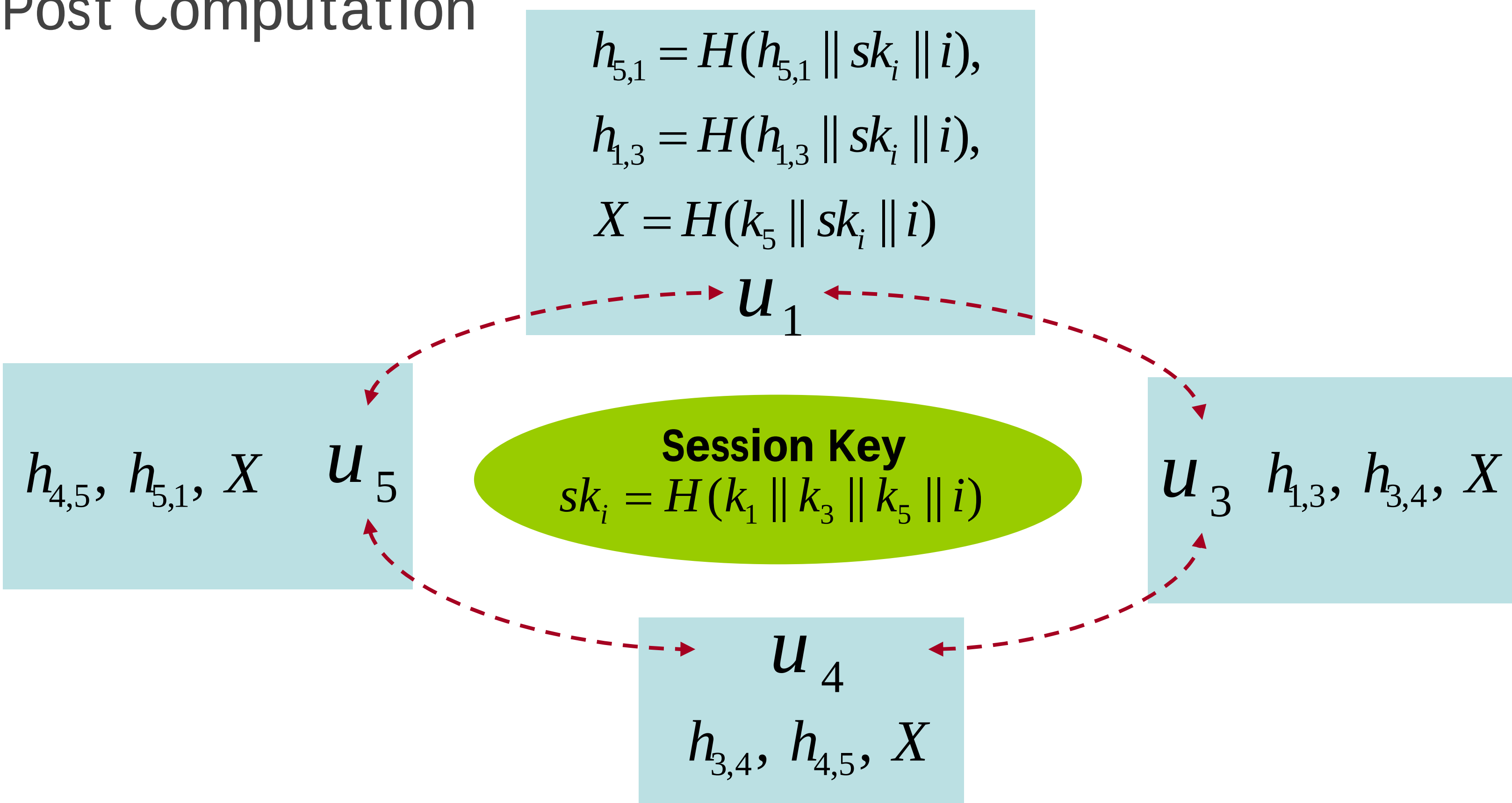


Leave(Round2)



Leave(Post-Computation)

- Message Validity Check
- Post Computation



Security and Efficiency

- The security of our protocol is based on the followings
  - It is not easy to solve the Computational Diffie-Hellman Problem.
  - It is not easy to existentially forge a signature scheme secure against chosen message attacks.
- Our scheme is more efficient than the existing dynamic authenticated group key exchange protocols.

Contribution

- Our 2-round AGKE protocol is a dynamic group key exchange protocol.
- No trustee is needed.
- Every honest member can check if transmitted messages are valid.
- A member's computation rate is low, since the operation dependent on the number of members is the XOR operation.

Further Research

- In our protocol, every member can check if transmitted messages are valid, but it is not easy to detect illegal members directly.
  - Fault tolerance
- In our protocol, the number of operations for signature verification is dependent on the number of members
  - Efficient authentication methods
- A symmetric structure (Ring structure)
  - An asymmetric structure

Thank you.