Dynamic Group Key Exchange

Dr Tan Chik How

Temasek Laboratories

National University of Singapore

Aims

- Introduction
- Group key exchange
- Analysis of (dynamic) group key exchange protocols
- A new dynamic group key exchange protocol
- Conclusion

Group Key Exchange Protocols (1/2)

- Group key exchange protocols : allow a group of users communicating over an insecure network to establish a shared secret key
- Application of Group Communication:
  - Telecommunication
  - Collaborative distributive computing
  - Information broadcasting
  - Ad hoc network
  - etc

Group Key Exchange Protocols (2/2)

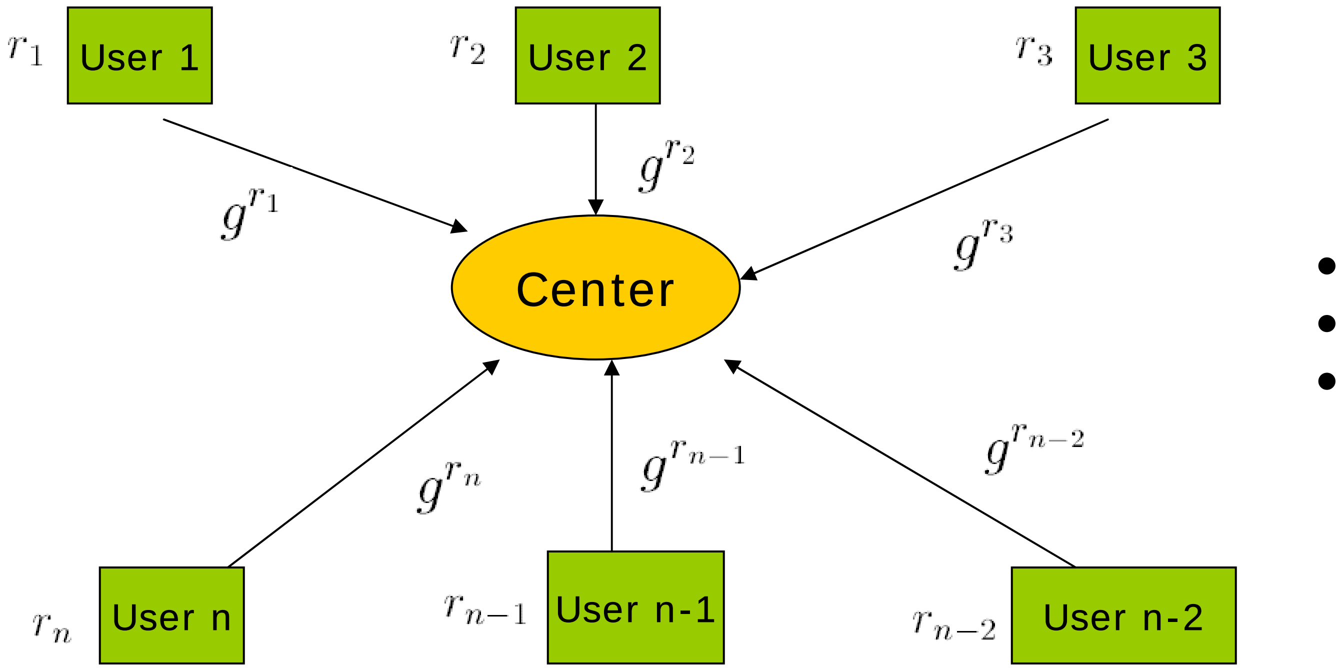
- Security Goals:
  - Session Key Security: no information, not even a single bit, of the session key is leaked to any passive or active adversary on the network
  - Entity Authentication: in a successful protocol execution, all legitimate group members and only them have actually participated in the protocol and generated the common session key
  - Contributiveness: all participants equally contribute to the computation of the agreed session key
- Insider security:
  - Entity Authentication: even a group of colluding insiders cannot impersonate another honest party
  - Contributiveness: the session key cannot be controlled by any subset of group members (i.e. secure against key control attacks)

Group key exchange

- Different Structures
  - Star-based GKE
  - Tree-based GKE
  - Link-based GKE
  - Ring-based GKE
- Different types
  - Static : users in the group is fixed
  - Dynamic : any user can join and leave the group

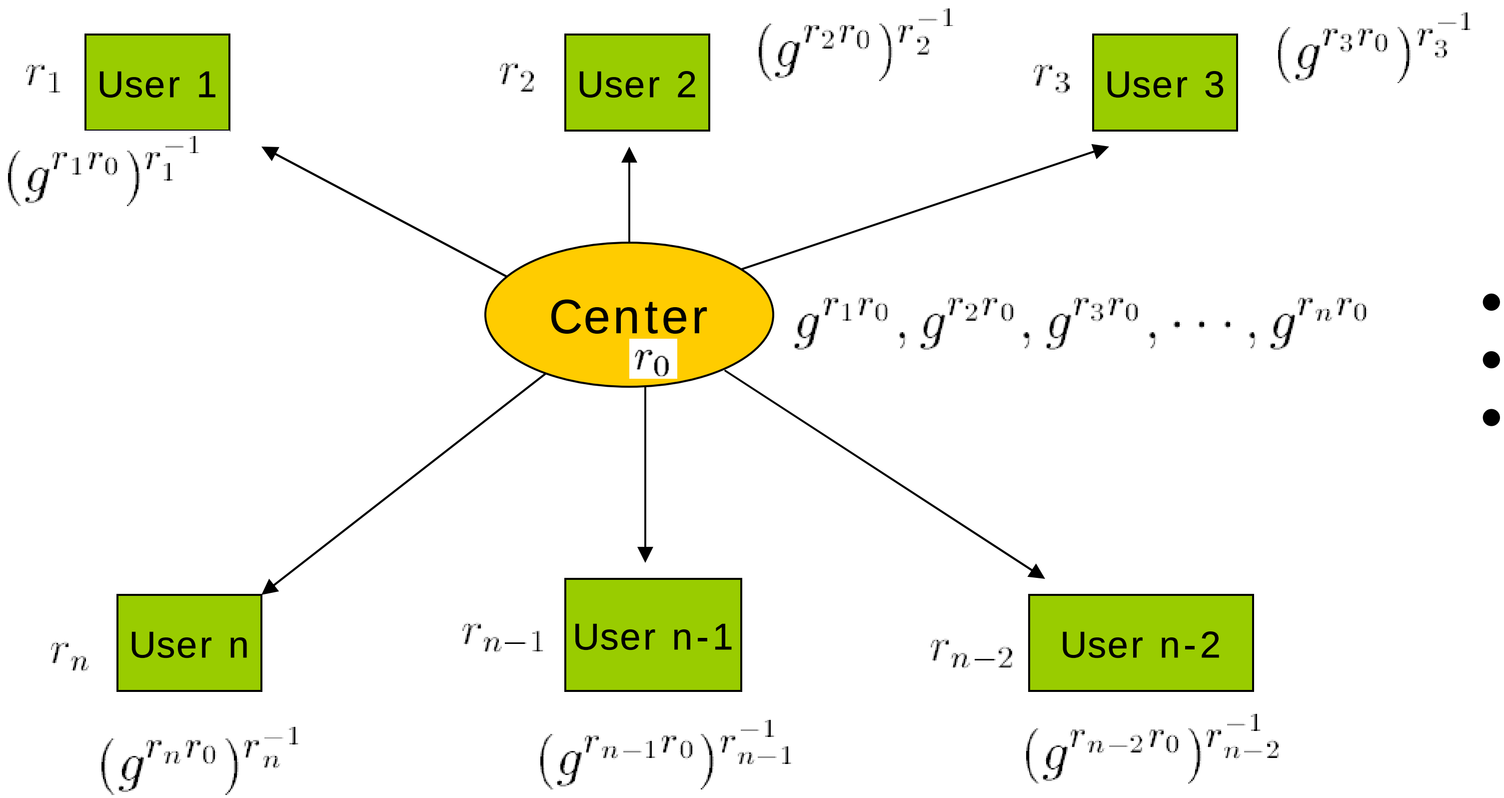
Star-based GKE (1/2)

A group $G = < g >$ and $|G| = q$



Daniel Augot, Raghav Bhaskar, Valerie Issarny, and Daniele Sacchetti. An efficient group key agreement protocol for ad hoc networks. In International Conference on a World of Wireless, Mobile and Multimedia Networks, pp. 576-580, 2005.

Star-based GKE (2/2)

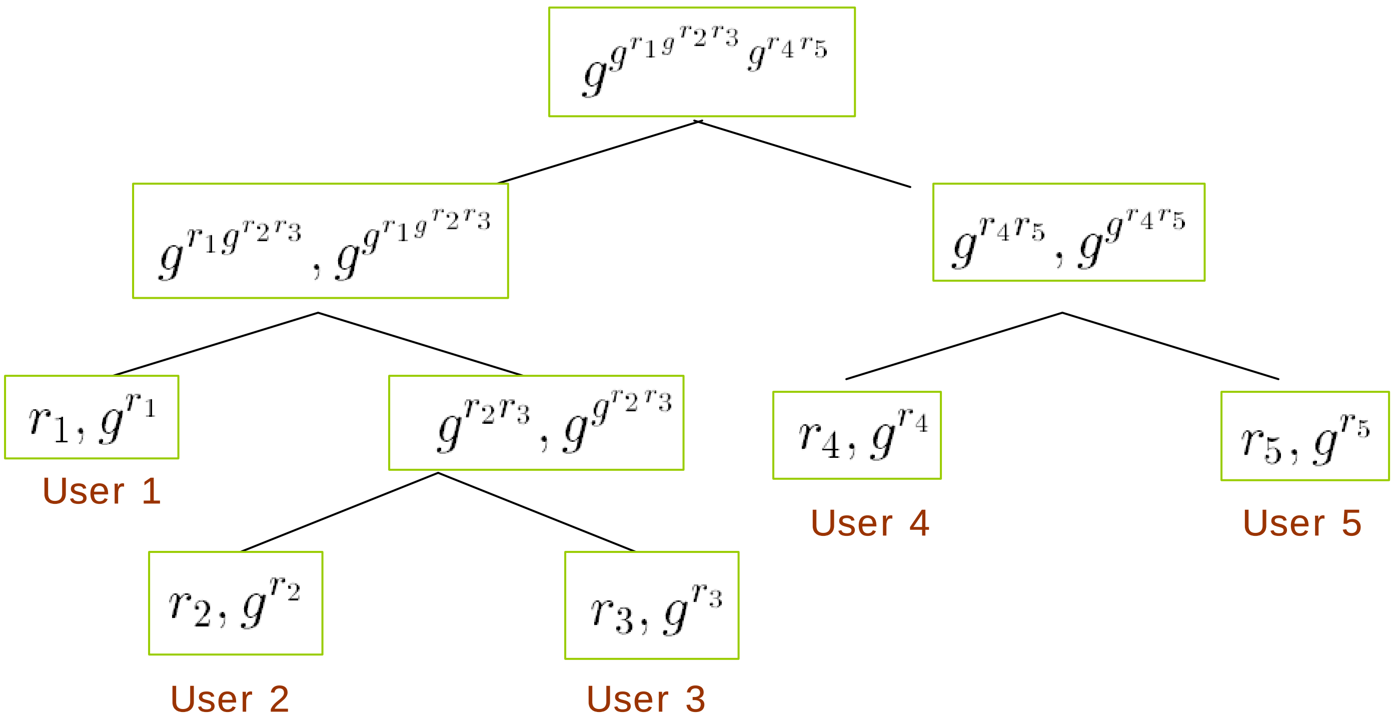


$$K = g^{r_0 + r_0 r_1 + r_0 r_2 + r_0 r_3 + \cdots + r_0 r_n}$$

Daniel Augot, Raghav Bhaskar, Valerie Issarny, and Daniele Sacchetti. An efficient group key agreement protocol for ad hoc networks. In International Conference on a World of Wireless, Mobile and Multimedia Networks, pp. 576-580, 2005.

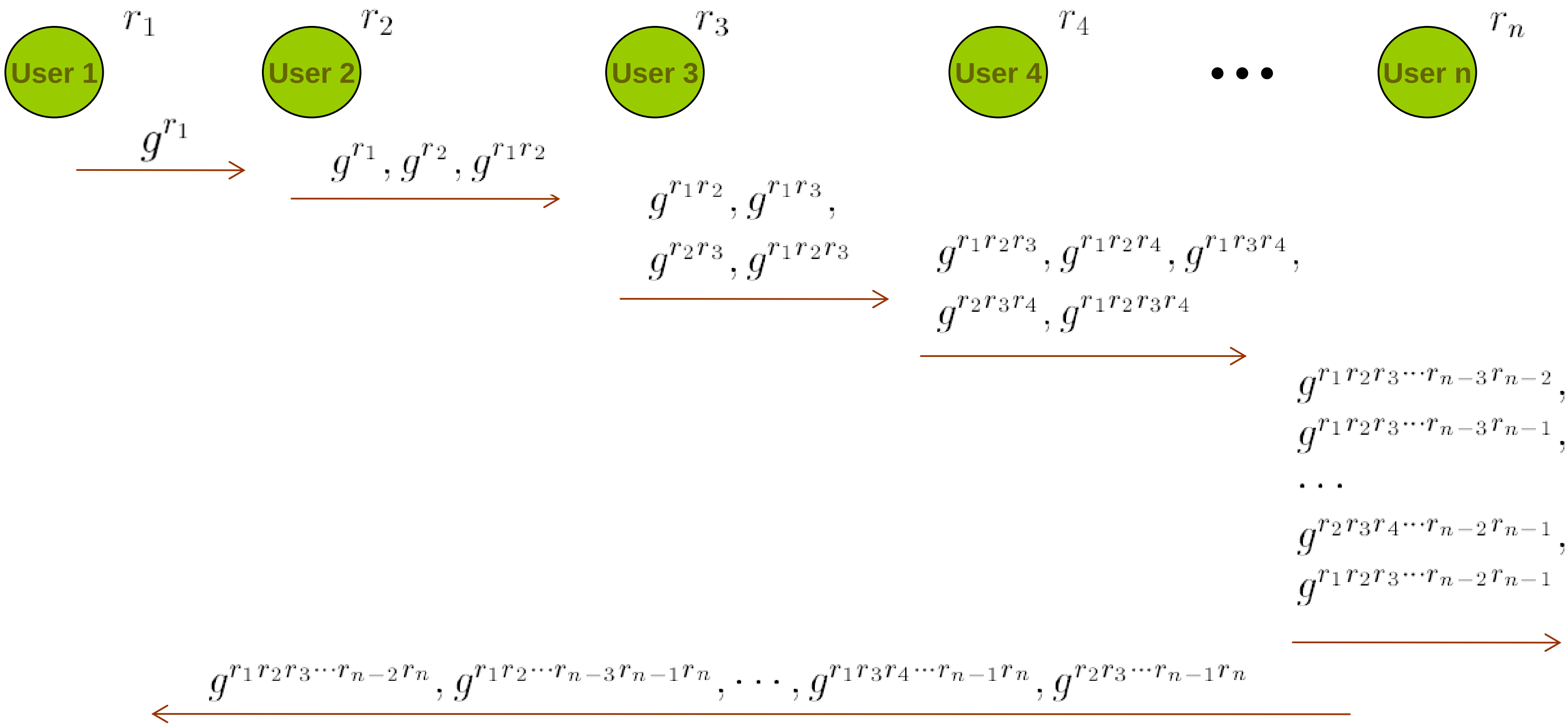
Tree-based GKE

A group $G =< g >$ and $|G| = q$



Yongdae Kim, Adrian Perrig, Gene Tsudik: Tree-based group key agreement. ACM Trans. Inf. Syst. Secur, 2004.

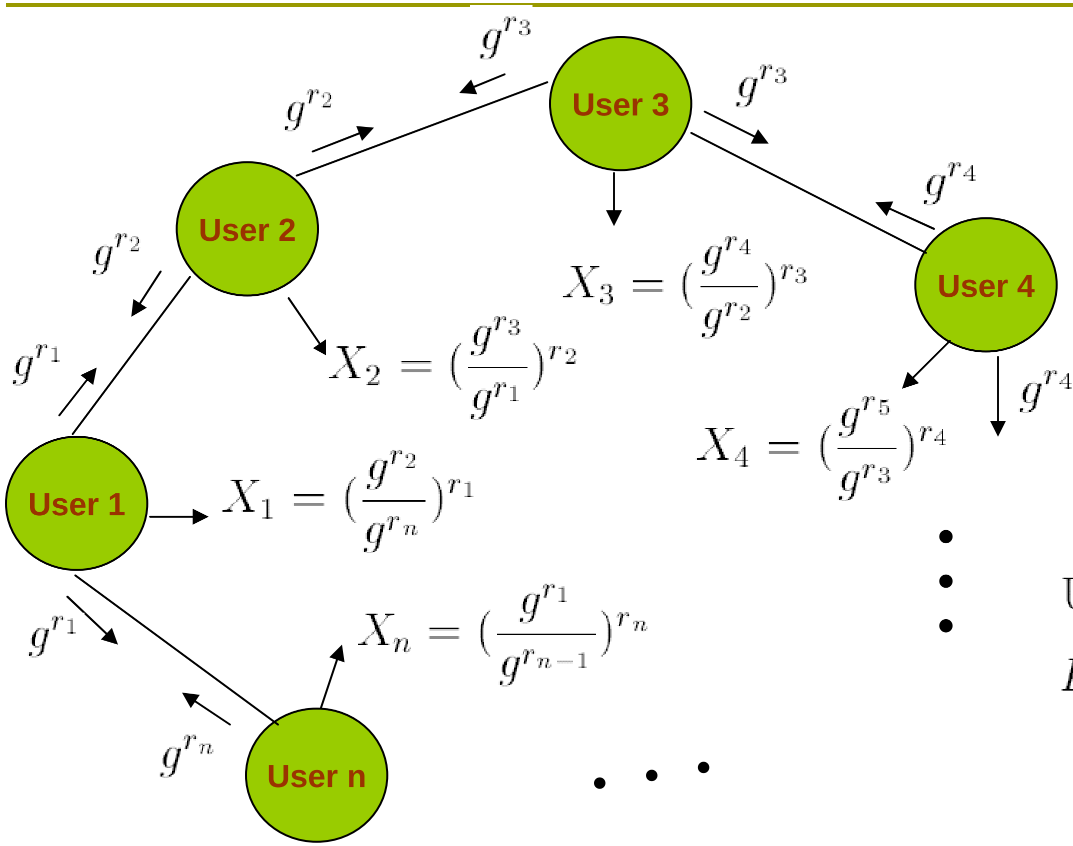
Link-based GKE



$$K = g^{r_1 r_2 r_3 \cdots r_{n-1} r_n}$$

Emmanuel Bresson, Olivier Chevassut, David Pointcheval: Provably secure authenticated group Diffie-Hellman key exchange. ACM Trans. Inf. Syst. Secur, 2007.

Ring-based GKE



User i :

$$K = (g^{r_{i-1} r_i})^n X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i+n-2}$$

$$= g^{r_1 r_2 + r_2 r_3 + \cdots + r_{n-1} r_n + r_n r_1}$$

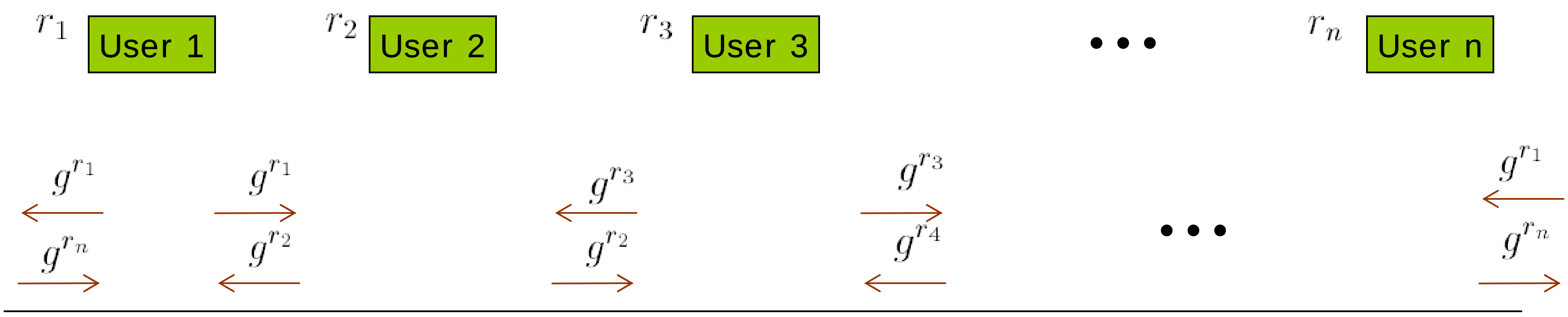
Mike Burmester and Yvo Desmedt. A secure and efficient conference key distribution system (extended abstract). In *Advances in Cryptology - Eurocrypt '94.*
Jonathan Katz and Moti Yung, Scalable Protocols for Authenticated Group Key Exchange. In Advances in Cryptology – Crypto’03

DB's Dynamic Group key exchange

- Dutta and Barua proposed a dynamic group key exchange in 2005 and 2008
- The static group key exchange is same as that of Burmester-Desmedt group key exchange
- The dynamic group key exchange security model follows the Bresson et al's security model, they proved that their dynamic group key exchange was secured in forward security and backward security

$$\text{A group } G = < g > \text{ and } |G| = q$$

DB's Group Key Exchange



$$K_i^{\mathrm{R}} = (g^{r_{i+1}})^{r_i}, \quad K_i^{\mathrm{L}} = (g^{r_{i-1}})^{r_i}$$

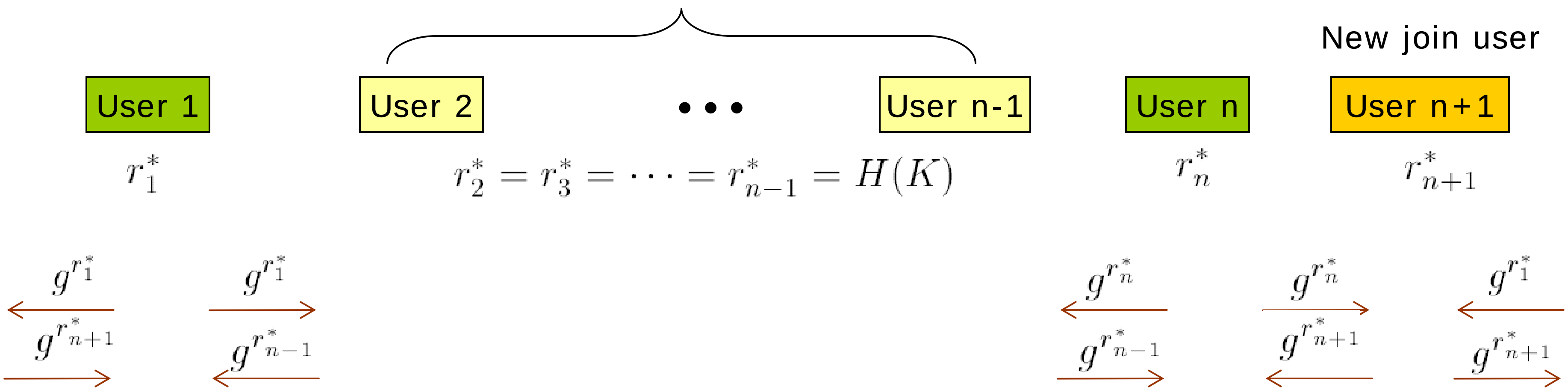
$$X_i = K_i^{\mathrm{R}} / K_i^{\mathrm{L}}$$

$$K_{i+1}^{\mathrm{R}} = K_i^{\mathrm{R}} X_{i+1}$$

$$K = K_1^{\mathrm{R}} K_2^{\mathrm{R}} \cdots K_{n-1}^{\mathrm{R}} K_n^{\mathrm{R}}$$

Ratna Dutta and Rana Barua. Constant round dynamic group key agreement. Proc. *ISC 2005, LNCS. vol. 3650, 74-88, Springer, 2005.*
Ratna Dutta and Rana Barua. Provably secure constant round contributory group key agreement in dynamic setting. *IEEE Trans. Inf. Theory, 54(5):2007-2025, 2008.*

DB's Dynamic Group Key Exchange : Join



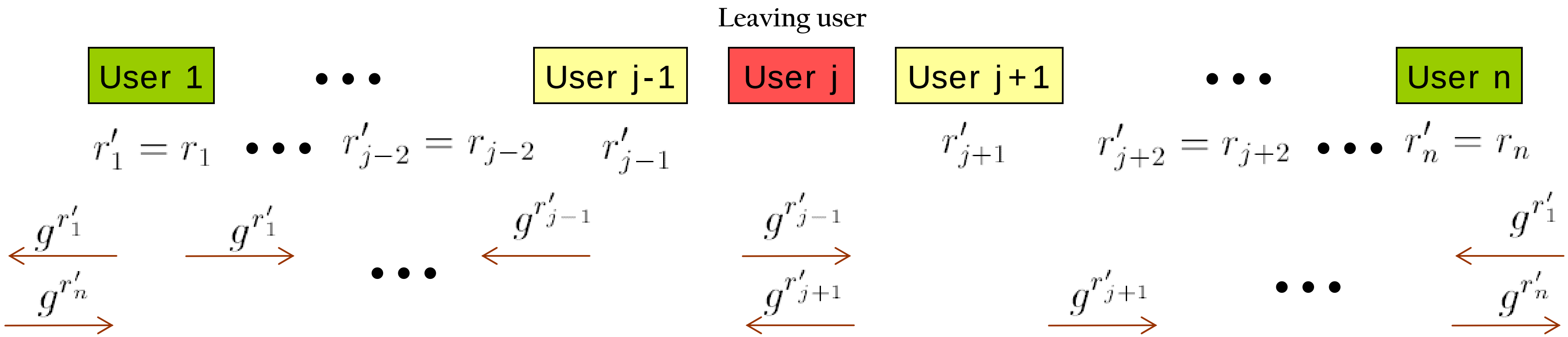
$$\text{For } i = 1, n-1, n, n+1, \quad K_i^{*\mathrm{R}} = (g^{r_{i+1}^*})^{r_i^*}, \quad K_i^{*\mathrm{L}} = (g^{r_{i-1}^*})^{r_i^*}$$

$$X_i^* = K_i^{*\mathrm{R}} / K_i^{*\mathrm{L}}$$

$$K_{i+1}^{*\mathrm{R}} = K_i^{*\mathrm{R}} X_{i+1}^*$$

$$K^* = K_1^{*\mathrm{R}} K_{n-1}^{*\mathrm{R}} K_n^{*\mathrm{R}} K_{n+1}^{*\mathrm{R}}$$

DB's Dynamic Group Key Exchange : Leave



$$r'_1 = r_1 \quad \cdots \quad r'_{j-2} = r_{j-2} \quad r'_{j-1} \quad r'_{j+1} \quad r'_{j+2} = r_{j+2} \quad \cdots \quad r'_n = r_n$$

$$g^{r'_1} \quad g^{r'_n} \quad g^{r'_1} \quad \cdots \quad g^{r'_{j-1}} \quad g^{r'_{j-1}} \quad g^{r'_{j+1}} \quad g^{r'_{j+1}} \quad \cdots \quad g^{r'_1} \quad g^{r'_n}$$

$$\text{For } i \neq j-1, j, j+1, \quad K'^{\mathrm{R}}_i = (g^{r'_{i+1}})^{r'_i}, \quad K'^{\mathrm{L}}_i = (g^{r'_{i-1}})^{r'_i}$$

$$K'^{\mathrm{R}}_{j-1} = (g^{r'_{j+1}})^{r'_{j-1}}, \quad K'^{\mathrm{L}}_{j-1} = (g^{r'_{j-2}})^{r'_{j-1}}$$

$$K'^{\mathrm{R}}_{j+1} = (g^{r'_{j+2}})^{r'_{j+1}}, \quad K'^{\mathrm{L}}_{j+1} = (g^{r'_{j-1}})^{r'_{j+1}}$$

$$X'_i = K'^{\mathrm{R}}_i / K'^{\mathrm{L}}_i$$

$$K'^{\mathrm{R}}_{i+1} = K'^{\mathrm{R}}_i X'_{i+1}$$

$$K' = K'^{\mathrm{R}}_1 \cdots K'^{\mathrm{R}}_{j-1} K'^{\mathrm{R}}_{j+1} \cdots K'^{\mathrm{R}}_n = g^{r'_1 r'_2 + \cdots + r'_{j-2} r'_{j-1} + r'_{j-1} r'_{j+1} + \cdots + r'_n r'_1}$$

DB Not Backward Security

- The leaving user j can compute the new group key K' established by among user i for i ≠ j
- Now, user j-1 and user j+1 are neighbour

Since $r'_i = r_i$ for $i \neq j-1, j+1$, therefore $K'^{R}_i = K^{R}_i$ for $i \neq j-2, j-1, j+1$.

The user j knows K'^{R}_i for $i \neq j-2, j-1, j+1$. Compute

$$
\begin{aligned}
K'^{R}_{j-2} &= X'_{j-2} K'^{R}_{j-3} = \frac{g^{r'_{j-2} r'_{j-1}}}{g^{r'_{j-2} r'_{j-3}}} \cdot g^{r'_{j-2} r'_{j-3}} \\
K'^{L}_{j-1} &= K'^{R}_{j-2} = g^{r'_{j-2} r'_{j-1}} \\
K'^{R}_{j-1} &= X'_{j-1} K'^{L}_{j-1} = \frac{g^{r'_{j+1} r'_{j-1}}}{g^{r'_{j-2} r'_{j-1}}} \cdot g^{r'_{j-2} r'_{j-1}} \\
K'^{R}_{j+1} &= X'_{j+1} K'^{R}_{j-1} = \frac{g^{r'_{j+2} r'_{j+1}}}{g^{r'_{j+1} r'_{j-1}}} \cdot g^{r'_{j+1} r'_{j-1}}
\end{aligned}
$$

$$K' = K'^{R}_1 \cdots K'^{R}_{j-1} K'^{R}_{j+1} \cdots K'^{R}_n$$

Joseph Chee Ming Teo, Chik How Tan, and Jim Mee Ng. Security analysis of provably secure constant round dynamic group key agreement. *IEICE Transactions, 89-A(11)*:3348-3350, 2005.

DB's Adversary Model for Security Proof

- In the adversarial model, an adversary $\mathcal{A}$ could make the following queries
  - Send queries : to activate send message to users
  - Execute queries : to execute the basic group key agreement protocol
  - Join queries : to get transcripts of honest execution of Join protocol
  - Leave queries : to get transcripts of honest execution of Leave protocol
  - Corrupt queries : $\mathcal{A}$ allows to learn the long term secret key of the party
  - Reveal query : $\mathcal{A}$ allows to learn the agreed group key of the session
  - Test queries : an unbiased coin is tossed, if b=0, then a random key is returned to the adversary A, otherwise, the real group key generated in session is returned

Ratna Dutta and Rana Barua. Provably secure constant round contributory group key agreement in dynamic setting. *IEEE Trans. Inf. Theory, 54(5):2007-2025, 2008.*

DB Not Forward Security

- In the adversary model, the adversary $\mathcal{A}$ works as follows:
  - The adversary $\mathcal{A}$ asks an Execute query to form a group of users with group key
  - $\mathcal{A}$ issues a Test query and obtains a response K which is either real group key or random key
  - $\mathcal{A}$ also issues a Join query to add a new user into the group, and obtains the transcript of the join protocol
  - $\mathcal{A}$ then computes $r^*_{n-1} = H(K)$ and $g^{r^*_{n-1}}$
    - If $g^{r^*_{n-1}}$ = $g^{\bar{r}_{n-1}}$ in the transcript, then b=1, otherwise b=0

Chik How Tan and Guomin Yang. Comment on “Provably secure constant round contributory group key agreement in dynamic setting”. *IEEE Trans. Inf. Theory, 56(11):5887-5888, 2010.*

Authenticated Group Key Exchange

A group of users $U = \{U_1, U_2, \cdots, U_n\}$

User 1 | User 2 | User 3 | $\cdots$ | User n

$i = 1, \cdots, n-1$

$k_i \in \{0,1\}^k$

$r_i \in [1, q-1]$

$\sigma_i = \text{Sign}(LK_i, g^{r_i}, U)$

$\cdots$

$k_n \in \{0,1\}^k$

$r_n \in [1, q-1]$

$\sigma_n = \text{Sign}(LK_n, H(k_n), g^{r_n}, U)$

g^{r_1}, σ_1 $\quad g^{r_2}, \sigma_2$ $\quad \cdots \quad$ $H(k_n), g^{r_n}, \sigma_n$

$i = 1, \cdots, n-1$

$K_i^{\text{L}} = H(g^{r_{i-1} r_i}, U)$

$K_i^{\text{R}} = H(g^{r_{i+1} r_i}, U)$

$T_i = K_i^{\text{L}} \oplus K_i^{\text{R}}$

$\sigma_i' = \text{Sign}(LK_i, k_i, T_i, U)$

$K_n^{\text{L}} = H(g^{r_{n-1} r_n}, U)$

$K_n^{\text{R}} = H(g^{r_1 r_n}, U)$

$T_n = K_n^{\text{L}} \oplus K_n^{\text{R}}$

$T' = k_n \oplus K_n^{\text{R}}$

$\sigma_n' = \text{Sign}(LK_n, T', T_n, U)$

k_1, T_1, σ_1' $\quad k_2, T_2, \sigma_2'$ $\quad \cdots \quad$ T', T_n, σ_n'

$$K_{i+1}^{\text{R}} = T_{i+1} \oplus K_i^{\text{R}}$$

$$K = H(k_1, k_2, \cdots, k_n)$$

Hyun-Jeong Kim, Su-Mi Lee, and Dong Hoon Lee. Constant-round authenticated group key exchange for dynamic groups. In *Advances in Cryptology - ASIACRYPT 2004, pages 245-259.*

Collusion in Authenticated Group Key Exchange

Assume user 3 & 1 collude user 2 in the group $U = \{U_1, U_2, \cdots, U_n\}$

User 1	User 2	User 3	• • •	User n
$i = 1, 3$ $k_i \in \{0,1\}^k$ $r_i \in [1, q-1]$ $\sigma_i = \text{Sign}(LK_i, g^{r_i}, U)$		$i = 4, \cdots, n-1$ $k_i^* \in \{0,1\}^k$ $r_i^* \in [1, q-1]$ $\sigma_i = \text{Sign}(LK_i, g^{r_i}, U)$	• • •	$k_n^* \in \{0,1\}^k$ $r_n^* \in [1, q-1]$ $\sigma_n = \text{Sign}(LK_n, H(k_n^*), g^{r_n^*}, U)$
g^{r_1}, σ_1	g^{r_2}, σ_2	g^{r_3}, σ_3 $g^{r_i^*}, \sigma_i$	• • •	$H(k_n^*), g^{r_n^*}, \sigma_n$
$K_1^{*L} = H(g^{r_n^* r_1}, U)$ $K_i^R = H(g^{r_2 r_i}, U)$ $T_1^* = K_1^{*L} \oplus K_1^R$ $\sigma_1' = \text{Sign}(LK_1, k_1^*, T_1^*, U)$		$i = 3, \cdots, n-2$ $K_i^L = H(g^{r_{i-1} r_i}, U)$ $K_i^R = H(g^{r_{i+1} r_i}, U)$ $T_i = K_i^L \oplus K_i^R$ $\sigma_i' = \text{Sign}(LK_i, k_i^*, T_i, U)$	• • • $K_{n-1}^L = H(g^{r_{n-2} r_{n-1}}, U)$ $K_{n-1}^{*R} = H(g^{r_n^* r_{n-1}}, U)$ $T_{n-1}^* = K_{n-1}^L \oplus K_{n-1}^{*R}$ $\sigma_{n-1}' = \text{Sign}(LK_{n-1}, k_{n-1}^*, T_{n-1}^*, U)$	$K_n^{*L} = H(g^{r_{n-1} r_n^*}, U)$ $K_n^{*R} = H(g^{r_1 r_n^*}, U)$ $T_n^* = K_n^{*L} \oplus K_n^{*R}$ $T' = k_n^* \oplus K_n^{*R}$ $\sigma_n' = \text{Sign}(LK_n, T', T_n^*, U)$
k_1^*, T_1^*, σ_1'	k_2, T_2, σ_2'	k_i^*, T_i^*, σ_i^*	• • • $k_{n-1}^*, T_{n-1}^*, \sigma_{n-1}'$	T', T_n^*, σ_n'

$$K_{i+1}^R = T_{i+1} \oplus K_i^R$$

$$K = H(k_1^*, k_2^*, \cdots, k_n^*)$$

Summary

- Burmester-Desmedt's group key exchange is secured
- Dutta-Barua's dynamic group key exchange is
  - not forward secure
  - not backward secure
- Kim et al.'s authenticated group key exchange, which is similar to Burmester-Desmedt's protocol, is
  - not insider secure
  - not contributiveness

Security of Dynamic Group Key Exchange

- Session Key Security: no information, not even a single bit, of the session key is leaked to any passive or active adversary on the network
- Entity Authentication: in a successful protocol execution, all legitimate group members and only them have actually participated in the protocol and generated the common session key
- Contributiveness: all participants equally contribute to the computation of the agreed session key
- Forward Security: previous session keys are protected from joining members
- Backward Security: subsequent sessions key are protected from leaving members

New Authenticated Dynamic Group Key Exchange (1/3)

- Commitment scheme
  - CMT: take a message M to be committed as input and returns a commitment C and an opening key ϑ
  - CVF: take C, M, ϑ as input and returns either 0 or 1
  - Perfectly Hiding: Given C, no information about the committed message M is leaked
  - Computationally Binding: it is computationally infeasible to come up with a tuple $(C, (M_0, \vartheta_0), (M_1, \vartheta_1))$ such that $M_0 \neq M_1$ & $CVF(C, M_0, \vartheta_0) = 1$ & $CVF(C, M_1, \vartheta_1) = 1$
  - Uniformly Distributed: for any message M, an honest execution of CMT(M) generates a commitment C that is uniformly distributed in the range of $CMT(\cdot)$
- Pseudo random function
  - $F_K(m)$: takes a secret key $K \in KeySpace_F$, a message $m \in Domain_F$ as input and generates an output in a specific range $Range_F$
  - Security requirement: F_K works just "like" a truly random function
- Digital signature scheme

New Authenticated Dynamic Group Key Exchange (2/3)

A group of users $U = \{U_1, U_2, \cdots, U_n\}$

User 1 | User 2 | User 3 | • • • | User n

$i = 1, \cdots, n$

$k_i \in \{0,1\}^k$

$r_i \in [1, q-1]$

$(c_i, o_i) = \mathrm{CMT}(k_i)$

g^{r_i}, c_i ⟷

$\mathrm{sid} = c_1 || c_2 || \cdots || c_n$

$i = 1, \cdots, n-1$

$K_i^{\mathrm{L}} = F_{g^{r_{i-1} r_i}}(1)$

$K_i^{\mathrm{R}} = F_{g^{r_{i+1} r_i}}(1)$

$T_i = K_i^{\mathrm{L}} \oplus K_i^{\mathrm{R}}$

$\sigma_i = \mathrm{Sign}(LK_i, g^{r_i}, c_i, k_i, o_i, T_i, U, \mathrm{sid})$

$K_n^{\mathrm{L}} = F_{g^{r_{n-1} r_n}}(1)$

$K_n^{\mathrm{R}} = F_{g^{r_1 r_n}}(1)$

$T_n = K_n^{\mathrm{L}} \oplus K_n^{\mathrm{R}}$

$T' = (k_n || o_n) \oplus K_n^{\mathrm{R}}$

$\sigma_n = \mathrm{Sign}(LK_n, g^{r_n}, c_n, T', T_n, U, \mathrm{sid})$

k_1, o_1, T_1, σ_1 $\quad k_2, o_2, T_2, \sigma_2$ $\quad \cdots$ $\quad T', T_n, \sigma_n$ ⟷

Guomin Yang and Chik How Tan, "Dynamic Group Key Exchange Revisited", The 9th International Conference on Cryptology And Network Security (CANS'2010), LNCS 6467, pp. 261-277, Springer, 2010.

New Authenticated Dynamic Group Key Exchange (3/3)

A group of users $U = \{U_1, U_2, \cdots, U_n\}$

User 1 | User 2 | User 3 | • • • | User n

$$i = 1, \cdots, n$$

$$K^{\mathrm{R}}_{i+1} = T_{i+1} \oplus K^{\mathrm{R}}_i$$

$$k_n || o_n = T' \oplus K^{\mathrm{R}}_n$$

$$K = F'_{k_1 \oplus k_2 \oplus \cdots \oplus k_n}(1)$$

$$H^{\mathrm{L}}_i = F_{g^{r_{i-1} r_i}}(0)$$

$$H^{\mathrm{R}}_i = F_{g^{r_{i+1} r_i}}(0)$$

$$r = F'_{k_1 \oplus k_2 \oplus \cdots \oplus k_n}(0)$$

New Authenticated Dynamic Group Key Exchange : Join (1/3)

A new group of users $U^* = \{U_1, U_2, \cdots, U_n, U_{n+1}\}$

New User

User 1	User 2	User 3	• • •	User n	User n+1
$H_1^{\mathrm{L}}, H_1^{\mathrm{R}}, r$ $k_1^* \in \{0,1\}^k$ $r_1^* \in [1, q-1]$ $(c_1^*, o_1^*) = \mathrm{CMT}(k_1)$	$H_2^{\mathrm{L}}, H_2^{\mathrm{R}}, r$ $k_2^* \in \{0,1\}^k$ $r_2^* = r$ $(c_2^*, o_2^*) = \mathrm{CMT}(k_2)$	$i = 3, \cdots, n-1$ $H_i^{\mathrm{L}}, H_i^{\mathrm{R}}, r$ $k_i^* \in \{0,1\}^k$ $(c_i^*, o_i^*) = \mathrm{CMT}(k_i^*)$		$H_n^{\mathrm{L}}, H_n^{\mathrm{R}}, r$ $k_n^* \in \{0,1\}^k$ $r_n^* \in [1, q-1]$ $(c_n^*, o_n^*) = \mathrm{CMT}(k_n)$	$k_{n+1}^* \in \{0,1\}^k$ $r_{n+1}^* \in [1, q-1]$ $(c_{n+1}^*, o_{n+1}^*) = \mathrm{CMT}(k_{n+1})$

Broadcast (↔):

$g^{r_1^*}, c_1^*$ — $g^{r_2^*}, c_2^*$ — $i = 3, \cdots, n-1$: c_i^* — $g^{r_n^*}, c_n^*$ — $g^{r_{n+1}^*}, c_{n+1}^*$

New Authenticated Dynamic Group Key Exchange : Join (2/3)

A new group of users $U^* = \{U_1, U_2, \cdots, U_n, U_{n+1}\}$

New User

User 1 | User 2 | User 3 | • • • | User n | User n+1

$$\mathrm{sid}^* = c_1^* || c_2^* || \cdots || c_{n+1}^*$$

$$i = 1, 2, n+1$$
$$K_i^{*\mathrm{L}} = F_{g^{r_{i-1}^* r_i^*}}(1)$$
$$K_i^{*\mathrm{R}} = F_{g^{r_{i+1} r_i^*}}(1)$$
$$T_i^* = K_i^{*\mathrm{L}} \oplus K_i^{*\mathrm{R}}$$
$$\sigma_i^* = \mathrm{Sign}(LK_i, g^{r_i^*}, c_i^*, k_i^*, o_i^*, T_i^*, U^*, \mathrm{sid}^*)$$

$$K_n^{*\mathrm{L}} = F_{g^{r_2^* r_n^*}}(1)$$
$$K_n^{*\mathrm{R}} = F_{g^{r_{n+1}^* r_n}}(1)$$
$$T_n^* = K_n^{*\mathrm{L}} \oplus K_n^{*\mathrm{R}}$$
$$T' = (k_n^* || o_n^*) \oplus K_n^{*\mathrm{R}}$$
$$\sigma_n^* = \mathrm{Sign}(LK_n, g^{r_n^*}, c_n^*, \bar{T}', T_n^*, U^*, \mathrm{sid}^*)$$

$$i = 3, \cdots, n-1$$
$$\sigma_i^* = \mathrm{Sign}(LK_i, c_i^*, k_i^*, o_i^*, U^*, \mathrm{sid}^*)$$

$k_1^*, o_1^*, T_1^*, \sigma_1^*$ | $k_2^*, o_2^*, T_2^*, \sigma_2^*$ | k_i^*, o_i^*, σ_i^* | • • • | $\bar{T}', T_n^*, \sigma_n^*$ | $k_{n+1}^*, o_{n+1}^*, T_{n+1}^*, \sigma_{n+1}^*$

New Authenticated Dynamic Group Key Exchange : Join (3/3)

A group of users $U^* = \{U_1, U_2, \cdots, U_n, U_{n+1}\}$

New User

User 1 | User 2 | User 3 | • • • | User n | User n+1

$$K_{i+1}^{*R} = T_{i+1}^* \oplus K_i^{*R}$$
$$k_n^* || o_n^* = T' \oplus K_n^{*R}$$
$$K = F'_{k_1^* \oplus k_2^* \oplus \cdots \oplus k_{n+1}^*}(1)$$
$$r^* = F'_{k_1^* \oplus k_2^* \oplus \cdots \oplus k_{n+1}^*}(0)$$

$$i = 2, \cdots, n-1$$

$$H_1^{*L} = F_{g^{r^*_{n+1} r_1}}(0)$$
$$H_1^R$$

$$H_i^L$$
$$H_i^R$$

$$H_n^L$$
$$H_n^{*R} = F_{g^{r^*_{n+1} r^*_n}}(0)$$

$$H_{n+1}^{*L} = F_{g^{r^*_{n+1} r^*_n}}(0)$$
$$H_{n+1}^{*R} = F_{g^{r^*_{n+1} r_1}}(0)$$

New Authenticated Dynamic Group Key Exchange : Leave (1/3)

A new group of users $U^* = \{U_1, \cdots, U_{j-1}, U_{j+1}, \cdots, U_n\}$

Leaving user

User 1 • • • User j-1 | User j | User j+1 • • • User n

$i = 1, \cdots, j-2, j+2, \cdots, n$

$H_i^{\mathrm{L}}, H_i^{\mathrm{R}}, r$

$k_i^* \in \{0,1\}^k$

$(c_i^*, o_i^*) = \mathrm{CMT}(k_i^*)$

$i = j-1, j+1$

$H_i^{\mathrm{L}}, H_i^{\mathrm{R}}, r$

$k_i^* \in \{0,1\}^k$

$r_i^* \in [1, q-1]$

$(c_i^*, o_i^*) = \mathrm{CMT}(k_i)$

c_i^* • • • $g^{r_{j-1}^*}, c_{j-1}^*$ $g^{r_{j+1}^*}, c_{j+1}^*$ • • • c_i^* • • • $g^{r_n^*}, c_n^*$

New Authenticated Dynamic Group Key Exchange : Leave (2/3)

A new group of users $U^* = \{U_1, \cdots, U_{j-1}, U_{j+1}, \cdots, U_n\}$

Leaving user

User 1 • • • User j-1 | User j | User j+1 • • • User n

$$\text{sid}^* = c_1^* || \cdots || c_{j-1}^* || c_{j+1}^* || \cdots || c_n^*$$

$i = 1, \cdots, j-2, j+2, \cdots, n$

$$K_i^{*\mathrm{L}} = F_{H_i^{\mathrm{L}}}(1)$$
$$K_i^{*\mathrm{R}} = F_{H_i^{\mathrm{R}}}(1)$$
$$T_i^* = K_i^{*\mathrm{L}} \oplus K_i^{*\mathrm{R}}$$
$$\sigma_i^* = \text{Sign}(LK_i, c_i^*, k_i^*, o_i^*, T_i^*, U^*, \text{sid}^*)$$

$$K_{j-1}^{*\mathrm{L}} = F_{H_{j-1}^{\mathrm{L}}}(1)$$
$$K_{j-1}^{*\mathrm{R}} = F_{g^{r_{j-1}^* r_{j+1}^*}}(0)$$
$$T_{j-1}^* = K_{j-1}^{*\mathrm{L}} \oplus K_{j-1}^{*\mathrm{R}}$$
$$\sigma_{j-1}^* = \text{Sign}(LK_i, g^{r_{j-1}^*}, c_{j-1}^*, k_{j-1}^*, o_{j-1}^*, T_{j-1}^*, U^*, \text{sid}^*)$$

$$K_{j+1}^{*\mathrm{R}} = F_{H_{j+1}^{\mathrm{R}}}(1)$$
$$K_{j+1}^{*\mathrm{L}} = F_{g^{r_{j-1}^* r_{j+1}^*}}(0)$$
$$T_{j+1}^* = K_{j+1}^{*\mathrm{L}} \oplus K_{j+1}^{*\mathrm{R}}$$
$$\sigma_{j+1}^* = \text{Sign}(LK_i, g^{r_{j+1}^*}, c_{j+1}^*, k_{j+1}^*, o_{j+1}^*, T_{j+1}^*, U^*, \text{sid}^*)$$

$$T' = (k_n^* || o_n^*) \oplus K_n^{*\mathrm{R}}$$

$i \neq j, n$ $\quad k_i^*, o_i^*, T_i^*, \sigma_i^*$ $\qquad \bar{T}', T_n^*, \sigma_n^*$

New Authenticated Dynamic Group Key Exchange : Leave (3/3)

A new group of users $U^* = \{U_1, \cdots, U_{j-1}, U_{j+1}, \cdots, U_n\}$

Leaving user

User 1 • • • User j-1 | User j | User j+1 • • • User n

$i \neq j$

$$K_{i+1}^{*\mathrm{R}} = T_{i+1}^* \oplus K_i^{*\mathrm{R}}$$
$$k_n^* || o_n^* = T' \oplus K_n^{*\mathrm{R}}$$
$$K = F'_{k_1^* \oplus \cdots \oplus k_{j-1}^* \oplus k_{j+1}^* \oplus \cdots \oplus k_n^*}(1)$$
$$r^* = F'_{k_1^* \oplus \cdots \oplus k_{j-1}^* \oplus k_{j+1}^* \oplus \cdots \oplus k_n^*}(0)$$

$$H_i^{\prime\mathrm{L}} = F_{H_i^{*\mathrm{L}}}(0)$$
$$H_i^{\prime\mathrm{R}} = F_{H_i^{*\mathrm{R}}}(0)$$

Conclusion

- The new authenticated dynamic group key protocol is provably secure in
  - Session key
  - Entity authentication
  - Forward security
  - Backward security
  - Contributiveness