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 $|G| = q$

Star-based GKE (2/2)

Tree-based GKE

A group $G = \langle g \rangle$ and $|G| = q$

Link-based GKE

\[ \begin{array}{c}
\text{User 1} \rightarrow g^{r_1} \\
\text{User 2} \rightarrow g^{r_2}, g^{r_1r_2} \\
\text{User 3} \rightarrow g^{r_1r_2}, g^{r_1r_3}, g^{r_2r_3}, g^{r_1r_2r_3} \\
\text{User 4} \rightarrow g^{r_1r_2r_3}, g^{r_1r_2r_4}, g^{r_1r_3r_4}, g^{r_2r_3r_4}, g^{r_1r_2r_3r_4} \\
\cdots \\
\text{User n} \rightarrow g^{r_1r_2r_3 \cdots r_{n-3}r_{n-2}}, g^{r_1r_2r_3 \cdots r_{n-3}r_{n-1}}, \ldots, g^{r_1r_2r_3 \cdots r_{n-3}r_{n-1}}, g^{r_2r_3r_4 \cdots r_{n-2}r_{n-1}}, g^{r_1r_2r_3 \cdots r_{n-2}r_{n-1}} \\
\end{array} \]

\[ K = g^{r_1r_2r_3 \cdots r_{n-1}r_n} \]

Ring-based GKE

\[ X_1 = \left( \frac{g^{r_2}}{g^{r_n}} \right)^{r_1} \]
\[ X_2 = \left( \frac{g^{r_3}}{g^{r_2}} \right)^{r_2} \]
\[ X_3 = \left( \frac{g^{r_4}}{g^{r_2}} \right)^{r_3} \]
\[ X_4 = \left( \frac{g^{r_5}}{g^{r_3}} \right)^{r_4} \]

\[ K = \left( g^{r_{i-1}r_i} \right)^n X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i+n-2}^{n-2} \]
\[ = g^{r_{i+1}r_{i+2} + r_{i+2}r_{i+3} + \cdots + r_{n-1}r_n + r_n r_1} \]

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

A group $G = \langle g \rangle$ and $|G| = q$
DB’s Group Key Exchange

\[ g_1^{r_1} \xleftrightarrow{r_2} g_2^{r_2} \xleftrightarrow{r_3} g_3^{r_3} \cdots \xleftrightarrow{r_n} g_n^{r_n} \]

\[
K_i^R = (g_i^{r_{i+1}})^{r_i}, \quad K_i^L = (g_i^{r_{i-1}})^{r_i} \\
X_i = K_i^R / K_i^L \\
K_{i+1}^R = K_i^R X_i + 1 \\
K = K_2^R K_3^R \cdots K_{n-1}^R K_n^R
\]

DB’s Dynamic Group Key Exchange: Join

For $i = 1, n-1, n, n+1$, $K_{i}^{*R} = (g_{i+1}^{r_{i}})^{r_{i}}$, $K_{i}^{*L} = (g_{i-1}^{r_{i}})^{r_{i}}$

$$X_{i}^{*} = K_{i}^{*R} / K_{i}^{*L}$$

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

$$K^{*} = K_{1}^{*R} K_{n-1}^{*R} K_{n}^{*R} K_{n+1}^{*R}$$
DB’s Dynamic Group Key Exchange: Leave

\[ r'_1 = r_1 \quad \cdots \quad r'_{j-2} = r_{j-2} \quad r'_{j-1} \]

\[ r'_j = \text{Leaving user} \quad r'_{j+1} \quad \cdots \quad r'_n = r_n \]

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

For \( i \neq j-1, j, j+1 \),

\[ K'_i = (g^{r'_{i+1}})^{r'_i}, \quad K'_i = (g^{r'_{i-1}})^{r'_i} \]

\[ K'_{j-1} = (g^{r'_{j+1}})^{r'_{j-1}}, \quad K'_{j-1} = (g^{r'_{j-2}})^{r'_{j-1}} \]

\[ K'_{j+1} = (g^{r'_{j+2}})^{r'_{j+1}}, \quad K'_{j+1} = (g^{r'_{j-1}})^{r'_{j+1}} \]

\[ X'_i = K'_i / K'_i \]

\[ K'_{i+1} = K'_i X'_{i+1} \]

\[ K' = K'_1 \cdots K'_{j-1} K'_{j+1} \cdots K'_n = g^{r'_{1}r'_{2} + \cdots + r'_{j-2}r'_{j-1} + r'_{j-1}r'_{j+1} + \cdots + r'_{n}r'_{1}} \]
DB Not Backward Security

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

Since $r_i' = r_i$ for $i \neq j-1, j+1$, therefore $K_i'^R = K_i^R$ for $i \neq j-2, j-1, j+1$.

The user $j$ knows $K_i'^R$ for $i \neq j-2, j-1, j+1$. Compute

\[
K_{j-2}' = X_{j-2}'K_{j-3}' = \frac{g_{j-2}'r_{j-1}'}{g_{j-2}'r_{j-3}'} \cdot g_{j-2}'r_{j-3}'
\]

\[
K_{j-1}' = K_{j-2}' = g_{j-2}'r_{j-1}'
\]

\[
K_{j-1}' = X_{j-1}'K_{j-1}' = \frac{g_{j-1}'r_{j-1}'}{g_{j-2}'r_{j-1}'} \cdot g_{j-2}'r_{j-1}'
\]

\[
K_{j+1}' = X_{j+1}'K_{j-1}' = \frac{g_{j+2}'r_{j+1}'}{g_{j+1}'r_{j+1}'} \cdot g_{j+1}'r_{j+1}'
\]

DB’s Adversary Model for Security Proof

- In the adversarial model, an adversary $A$ 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**: $A$ allows to learn the long term secret key of the party
  - **Reveal query**: $A$ 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

DB Not Forward Security

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

Authenticated Group Key Exchange

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

\[
\begin{align*}
\text{User 1} & \quad g^{r_1}, \sigma_1 \\
\text{User 2} & \quad g^{r_2}, \sigma_2 \\
\text{User 3} & \quad \cdots \\
\text{User n} & \quad \cdots \\
\end{align*}
\]

\[
\begin{align*}
i & = 1, \cdots, n-1 \quad k_i \in \{0, 1\}^k \\
r_i & \in [1, q-1] \\
\sigma_i & = \text{Sign}(LK_i, g^{r_i}, U) \quad \cdots \\
\end{align*}
\]

\[
\begin{align*}
K_{i}^L & = H(g^{r_{i-1}r_i}, U) \\
K_{i}^R & = H(g^{r_{i+1}r_i}, U) \\
T_i & = K_i^L \oplus K_i^R \\
\sigma_i' & = \text{Sign}(LK_i, k_i, T_i, U) \quad \cdots \\
\end{align*}
\]

\[
\begin{align*}
k_{1}, T_1, \sigma_1' & \quad k_{2}, T_2, \sigma_2' \\
\cdots & \quad \cdots \\
T', T_n, \sigma_n' & \quad \cdots \\
\end{align*}
\]

\[
\begin{align*}
K_{i+1}^R & = T_{i+1} \oplus K_i^R \\
K & = H(k_1, k_2, \cdots, k_n)
\end{align*}
\]

Collusion in Authenticated Group Key Exchange

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

<table>
<thead>
<tr>
<th>User 1</th>
<th>User 2</th>
<th>User 3</th>
<th>...</th>
<th>User n</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i = 1, 3$</td>
<td>$i = 4, \cdots, n - 1$</td>
<td>$k_i^r \in {0, 1}^k$</td>
<td>$r_i^r \in [1, q - 1]$</td>
<td>$\sigma_i = \text{Sign}(LK_i, g^{r_i}, U)$</td>
</tr>
<tr>
<td>$g^{r_1}, \sigma_1$</td>
<td>$g^{r_2}, \sigma_2$</td>
<td>$g^{r_3}, \sigma_3$</td>
<td>$g^{r_i}, \sigma_i$</td>
<td>$H(k_n^*, g^{r_n}, \sigma_n)$</td>
</tr>
</tbody>
</table>

$k_1^L = H(g^{r_1}, U) + k_1^R$  
$k_i^L = H(g^{r_i - 1}, U)$  
$k_i^R = H(g^{r_i + 1}, U)$  
$T_1^* = K_1^L \oplus K_1^R$  
$T_i^* = K_i^L \oplus K_i^R$  
$\sigma_1^* = \text{Sign}(LK_1, k_1^*, T_1^*, U)$  
$\sigma_i^* = \text{Sign}(LK_i, k_i^*, T_i^*, U)$

$k_1^*, T_1^*, \sigma_1^*$  
$k_2, T_2, \sigma_2^*$  
$k_i^*, T_i^*, \sigma_i^*$  
$k_{n-1}^*, T_{n-1}^*, \sigma_{n-1}^*$  
$k_n^*, T_n^*, \sigma_n^*$

$K_{i+1} = T_{i+1} \oplus K_i^R$  
$K = H(k_1^*, k_2^*, \cdots, k_n^*)$  
$K_n^L = H(g^{r_n - 2r_{n-1}}, U)$  
$K_n^R = H(g^{r_n - 1}, U)$  
$T_n^* = k_n^L \oplus K_n^R$  
$\sigma_n^* = \text{Sign}(LK_n, T_n^*, U)$
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**: takes a message $M$ to be committed as input and returns a commitment $C$ and an opening key $\vartheta$
  - **CVF**: takes $C$, $M$, $\vartheta$ 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 $M_0 \neq M_1$ & $\text{CVF}(C, M_0, \vartheta_0) = 1$ & $\text{CVF}(C, M_1, \vartheta_1) = 1$
  - **Uniformly Distributed**: for any message $M$, an honest execution of $\text{CMT}(M)$ generates a commitment $C$ that is uniformly distributed in the range of $\text{CMT}(\cdot)$

- **Pseudo random function**
  - **$F_K(m)$**: takes a secret key $K \in \text{KeySpace}_F$, a message $m \in \text{Domain}_F$ as input and generates an output in a specific range $\text{Range}_F$
  - **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**

$i = 1, \cdots, n$

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

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

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

$g^{r_i}, c_i$

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

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

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

$T_i = K_i^L \oplus K_i^R$

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

$k_1, o_1, T_1, \sigma_1$

$k_2, o_2, T_2, \sigma_2$

$\cdots$

$T', T_n, \sigma_n$

New Authenticated Dynamic Group Key Exchange (3/3)

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

\begin{align*}
    i &= 1, \cdots, n \\
    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) \\
    H_i^L &= F_{g^{r_{i-1}r_i}} (0) \\
    H_i^R &= F_{g^{r_{i+1}r_i}} (0) \\
    r' &= F'_{k_1 \oplus k_2 \oplus \cdots \oplus k_n} (0)
\end{align*}
New Authenticated Dynamic Group Key Exchange: Join (1/3)

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

<table>
<thead>
<tr>
<th>User 1</th>
<th>User 2</th>
<th>User 3</th>
<th>( \cdots )</th>
<th>User n</th>
<th>User n+1</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H_1^L, H_1^R, r )</td>
<td>( H_2^L, H_2^R, r )</td>
<td>( i = 3, \cdots, n - 1 )</td>
<td>( H_i^L, H_i^R, r )</td>
<td>( k_i^* \in {0, 1}^k )</td>
<td>( k_{n+1}^* \in {0, 1}^k )</td>
</tr>
<tr>
<td>( k_1^* \in {0, 1}^k )</td>
<td>( k_2^* \in {0, 1}^k )</td>
<td>( r_2^* = r )</td>
<td>( k_i^* \in {0, 1}^k )</td>
<td>( r_{n+1}^* \in [1, q - 1] )</td>
<td>( (c_i^<em>, o_i^</em>) = \text{CMT}(k_i^*) )</td>
</tr>
<tr>
<td>( r_1^* \in [1, q - 1] )</td>
<td>( r_2^* = r )</td>
<td>( (c_2^<em>, o_2^</em>) = \text{CMT}(k_2) )</td>
<td>( (c_i^<em>, o_i^</em>) = \text{CMT}(k_i^*) )</td>
<td>( (c_n^<em>, o_n^</em>) = \text{CMT}(k_n) )</td>
<td></td>
</tr>
<tr>
<td>( (c_1^<em>, o_1^</em>) = \text{CMT}(k_1) )</td>
<td>( (c_2^<em>, o_2^</em>) = \text{CMT}(k_2) )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\( g_1^{r_1}, c_1^* \)
\( g_2^{r_2}, c_2^* \)
\( c_i^* \)
\( g_n^{r_n}, c_n^* \)
\( g_{n+1}^{r_{n+1}}, c_{n+1}^* \)

\( k_{n+1}^* \in \{0, 1\}^k \)
\( r_{n+1}^* \in [1, q - 1] \)
\( (c_{n+1}^*, o_{n+1}^*) = \text{CMT}(k_{n+1}) \)
New Authenticated Dynamic Group Key Exchange: Join (2/3)

A new group of users

\[ U^* = \{U_1, U_2, \ldots, U_n, U_{n+1}\} \]

\[ \text{sid}^* = c_1^* || c_2^* || \cdots || c_{n+1}^* \]

\[ K_{i}^{*L} = F_{g_{i-1}^{r_{i}}}^x (1) \]

\[ K_{i}^{*R} = F_{g_{i}^{r_{i+1}}}^x (1) \]

\[ T_i^* = K_i^{*L} \oplus K_i^{*R} \]

\[ \sigma_i^* = \text{Sign}(LK_i, g_i^{r_i}, c_i^*, k_i^*, o_i^*, T_i^*, U^*, \text{sid}^*) \]

\[ K_n^{*L} = F_{g_{n}^{r_{n}}}^x (1) \]

\[ K_n^{*R} = F_{g_{n+1}^{r_{n}}}^x (1) \]

\[ T_n^* = K_n^{*L} \oplus K_n^{*R} \]

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

\[ \sigma_n^* = \text{Sign}(LK_n, g_n^{r_n}, c_n^*, \bar{T}', T_n^*, U^*, \text{sid}^*) \]

\[ i = 3, \ldots, n - 1 \]

\[ \sigma_i^* = \text{Sign}(LK_i, c_i^*, k_i^*, o_i^*, U^*, \text{sid}^*) \]

\[ k_1^*, o_1^*, T_1^*, \sigma_1^* \quad k_2^*, o_2^*, T_2^*, \sigma_2^* \quad k_n^*, o_n^*, T_n^*, \sigma_n^* \quad \cdots \quad \bar{T}', T_n^*, \sigma_n^* \quad k_{n+1}^*, o_{n+1}^*, T_{n+1}^*, \sigma_{n+1}^* \]
# New Authenticated Dynamic Group Key Exchange: Join (3/3)

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

<table>
<thead>
<tr>
<th>User 1</th>
<th>User 2</th>
<th>User 3</th>
<th>$\cdots$</th>
<th>User n</th>
<th>User n+1</th>
</tr>
</thead>
</table>

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

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

$$K = F_{k_1^* \oplus k_2^* \oplus \cdots \oplus k_{n+1}^*}^i (1)$$

$$r^* = F_{k_1^* \oplus k_2^* \oplus \cdots \oplus k_{n+1}^*}^i (0)$$

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

$$H_1^{*L} = F_{g^{r_{n+1}r_1}}^i (0)$$

$$H_1^{R}$$

$$H_i^{L}$$

$$H_i^{R}$$

$$H_n^{L}$$

$$H_n^{*R} = F_{g^{r_n^*r_n}} (0)$$

$$H_{n+1}^{*L} = F_{g^{r_{n+1}r_n^*}} (0)$$

$$H_{n+1}^{*R} = F_{g^{r_{n+1}r_1^*}} (0)$$
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

\[
\begin{align*}
i &= 1, \cdots, j-2, j+2, \cdots, n \\
H^L_i, H^R_i, r \\
k^*_i &\in \{0, 1\}^k \\
(c^*_i, o^*_i) &= \text{CMT}(k^*_i)
\end{align*}
\]

\[
\begin{align*}
i &= j - 1, j + 1 \\
H^L_i, H^R_i, r \\
k^*_i &\in \{0, 1\}^k \\
r^*_i &\in [1, q - 1] \\
(c^*_i, o^*_i) &= \text{CMT}(k^*_i)
\end{align*}
\]
New Authenticated Dynamic Group Key Exchange : Leave (2/3)

A new group of users
\[ U^* = \{ U_1, \ldots, U_{j-1}, U_{j+1}, \ldots, U_n \} \]
Leaving user

User 1 \[ \cdots \] User j-1 User j User j+1 \[ \cdots \] User n

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

\[ i = 1, \ldots, j-2, j+2, \ldots, n \]
\[ K_{i}^{*L} = F_{H_i}^L(1) \]
\[ K_{i}^{*R} = F_{H_i}^R(1) \]
\[ T_i^* = K_i^{*L} \oplus K_i^{*R} \]
\[ \sigma_i^* = \text{Sign}(L, K_i, c_i^*, k_i^*, o_i^*, T_i^*, U^*, \text{sid}^*) \]

\[ K_{j-1}^{*L} = F_{H_{j-1}}^L(1) \]
\[ K_{j-1}^{*R} = F_{g_{j-1}^*}^R(0) \]
\[ T_{j-1}^* = K_{j-1}^{*L} \oplus K_{j-1}^{*R} \]
\[ \sigma_{j-1}^* = \text{Sign}(L, K_i, g_{j-1}^*, c_{j-1}^*, k_{j-1}^*, o_{j-1}^*, T_{j-1}^*, U^*, \text{sid}^*) \]

\[ K_{j+1}^{*L} = F_{H_{j+1}}^L(1) \]
\[ K_{j+1}^{*R} = F_{g_{j+1}^*}^R(0) \]
\[ T_{j+1}^* = K_{j+1}^{*L} \oplus K_{j+1}^{*R} \]
\[ \sigma_{j+1}^* = \text{Sign}(L, K_i, g_{j+1}^*, c_{j+1}^*, k_{j+1}^*, o_{j+1}^*, T_{j+1}^*, U^*, \text{sid}^*) \]

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

\[ \bar{T}', T_n^*, \sigma_n^* \]

28-Oct-2011

NTU's CCRG Seminar
New Authenticated Dynamic Group Key Exchange : Leave (3/3)

A new group of users

\[ U^* = \{ U_1, \ldots, U_{j-1}, U_{j+1}, \ldots, U_n \} \]

Leaving user

\[ i \neq j \]

\[ K^*_{i+1} = T^*_i \oplus K^*_{i+1} \]

\[ \kappa^*_n \| o^*_n = T' \oplus K^*_{n} \]

\[ K = F'_{k^*_1 \oplus \cdots \oplus k^*_{j-1} \oplus k^*_{j+1} \oplus \cdots \oplus k^*_n} (1) \]

\[ r^* = F'_{k^*_1 \oplus \cdots \oplus k^*_{j-1} \oplus k^*_{j+1} \oplus \cdots \oplus k^*_n} (0) \]

\[ H_{i}^{L} = F_{H_{i}^{*L}} (0) \]

\[ H_{i}^{R} = F_{H_{i}^{*R}} (0) \]
Conclusion

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