On the Vulnerability of a Group Key Transfer Protocol based on Secret Sharing

Ruxandra F. Olimid

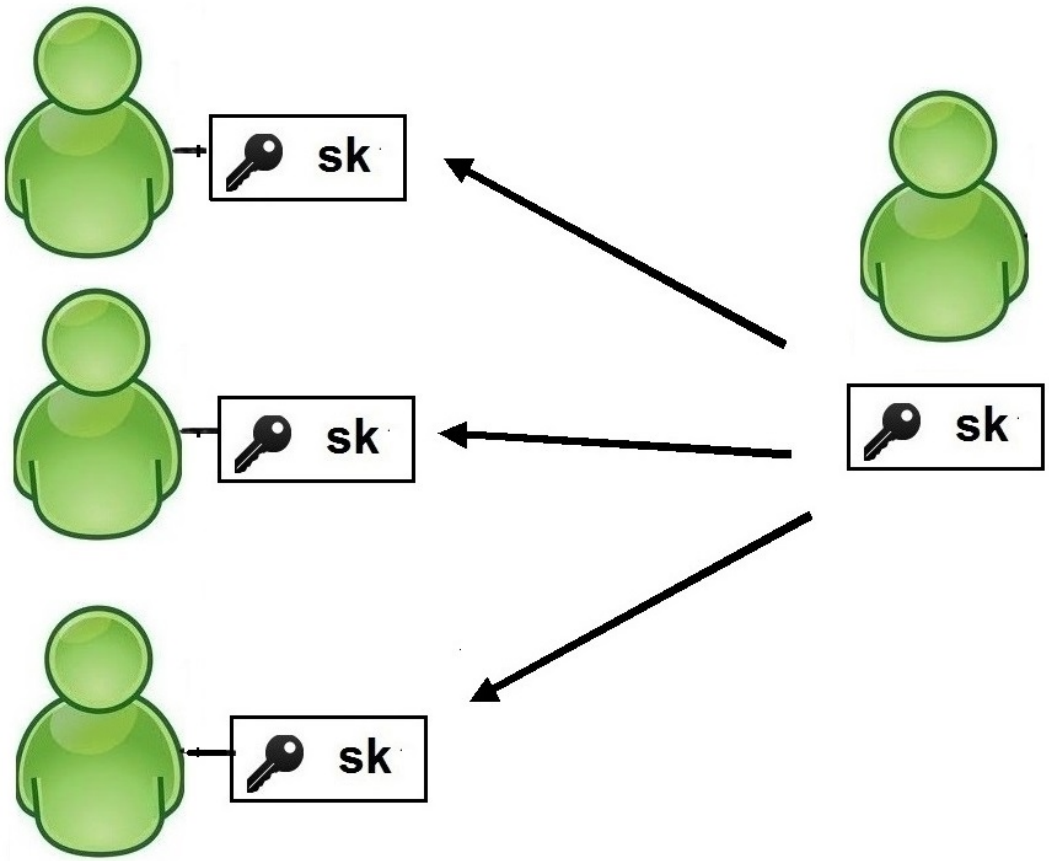
University of Bucharest
ruxandra.olimid@fmi.unibuc.ro

SACI 2014, 15 May

Outline

1. Preliminaries
2. Motivation
3. Hsu et al.'s Protocol
4. The Attack
5. Countermeasures

GKT (Group Key Transfer)



Goal: Allow multiple entities to share a common secret key.

Motivation

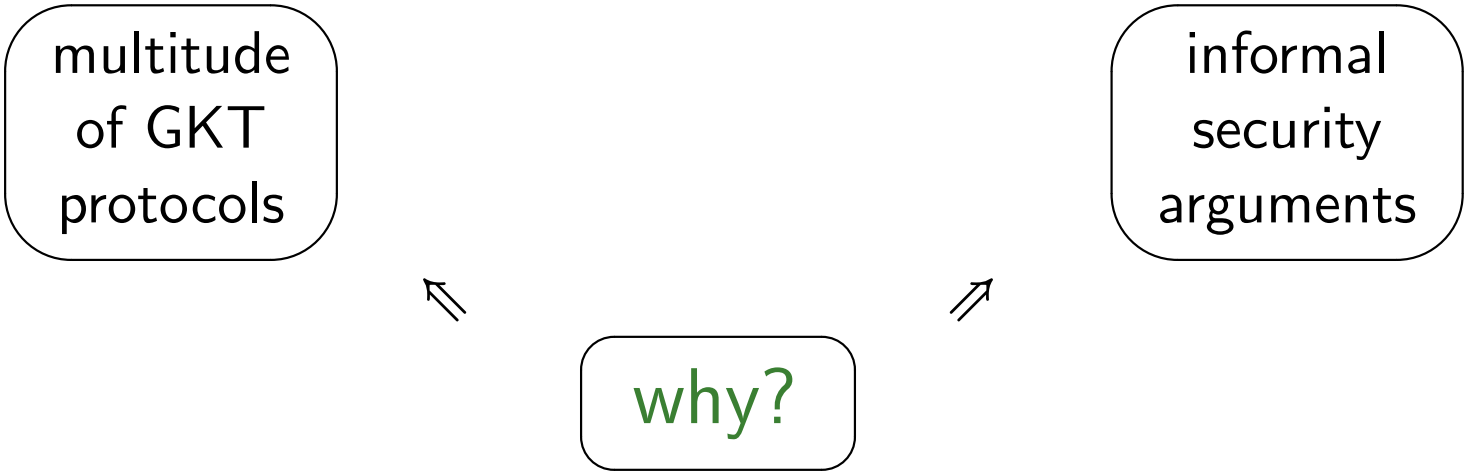
why?

Motivation

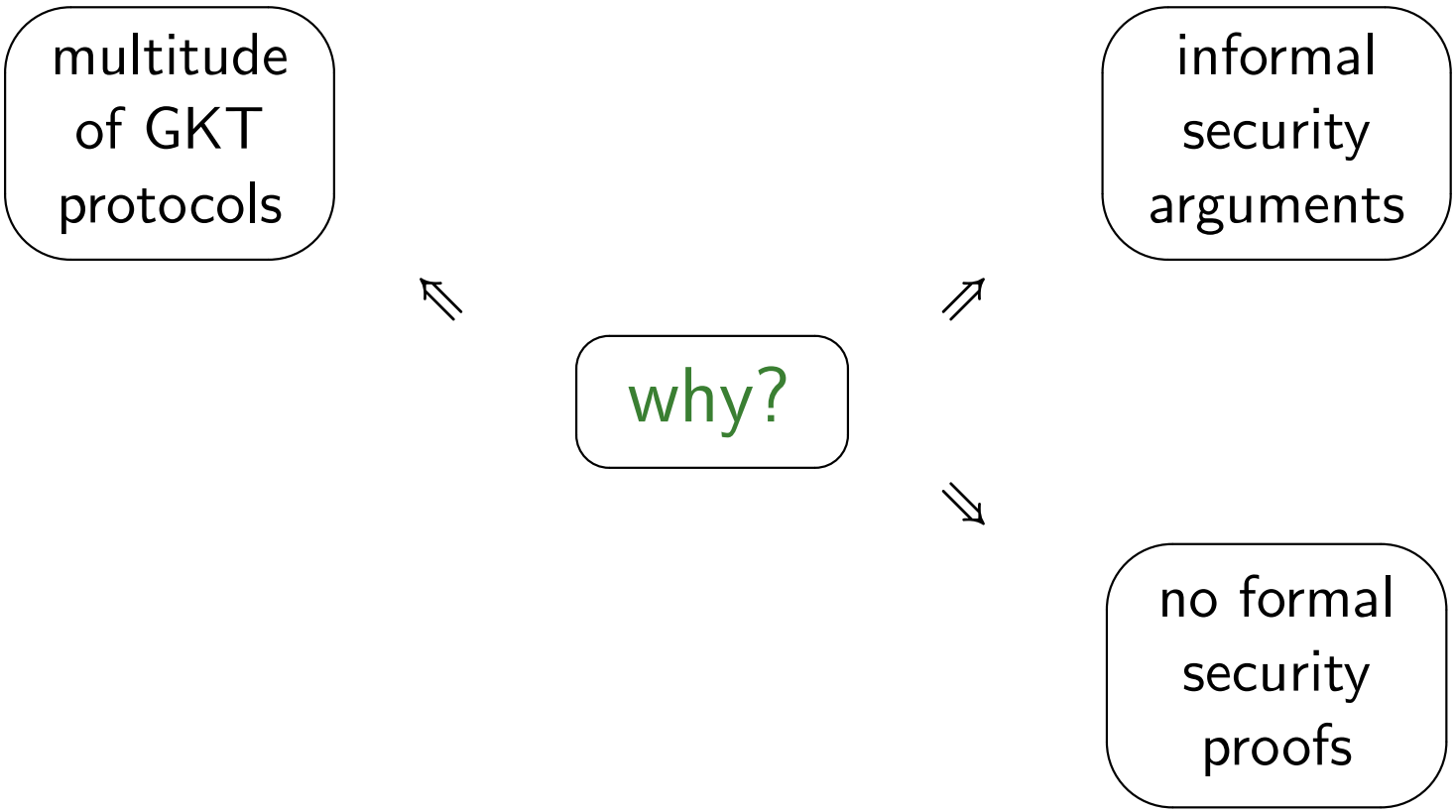
multitude of GKT protocols

why?

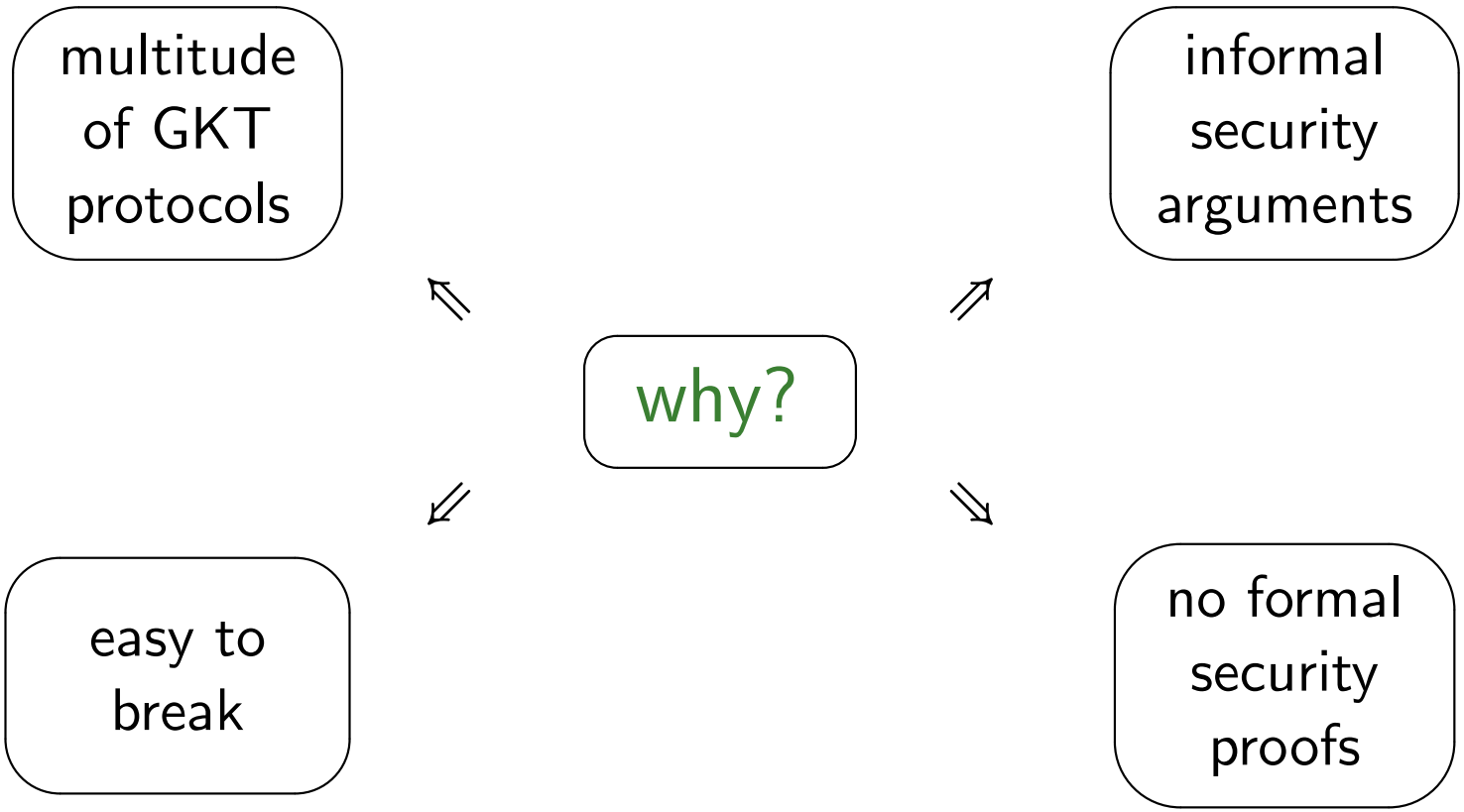
Motivation


multitude of GKT protocols
informal security arguments
why?

Motivation


multitude of GKT protocols
informal security arguments
why?
no formal security proofs

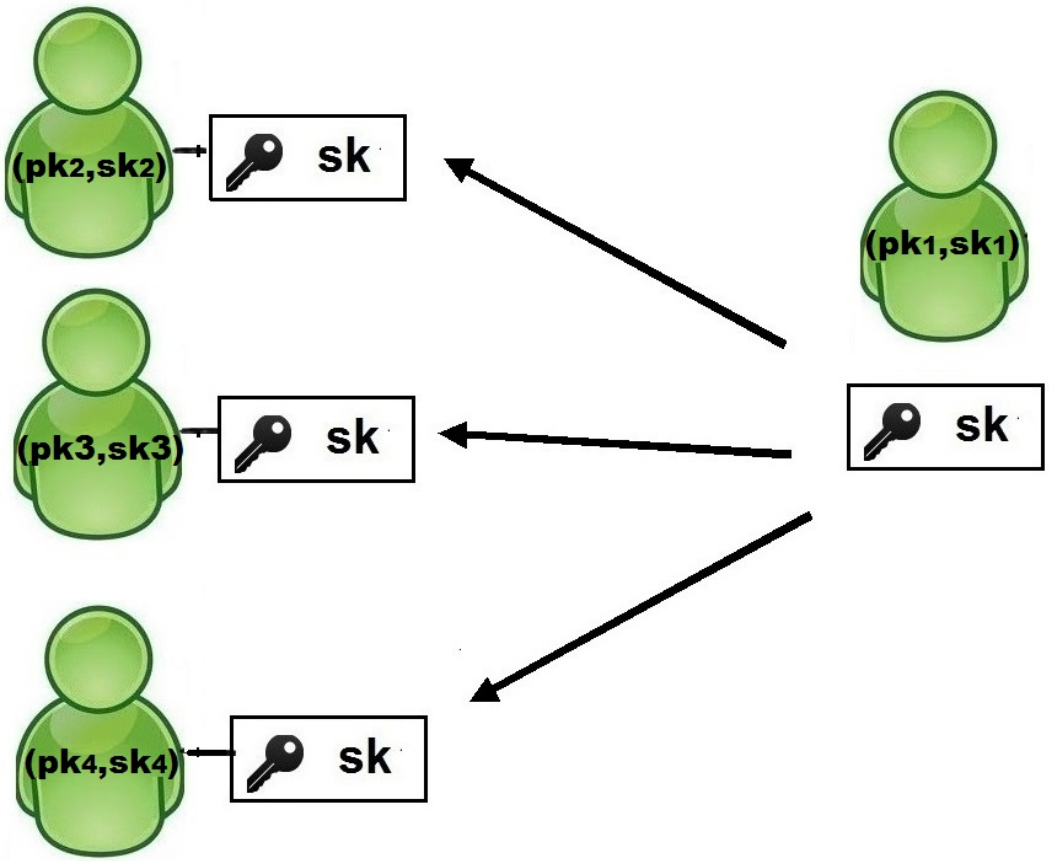
Motivation


multitude of GKT protocols
informal security arguments
why?
easy to break
no formal security proofs

Informally Secure GKT based on Secret Sharing

Original Protocol	Revealed Attacks
Harn and Lin (2010)	Nam et al. (2011) Yuan et al. (2013)
Sun et al. (2012)	Olimid (2013) Kim et. al (2013)
Hsu et al. (2012)	Olimid (2014)
Yuan et al.(2013)	Olimid (2013)

Hsu et al.'s Protocol



(pk_i, sk_i): $pk_i = g^{sk_i} \in \mathbb{G}$.

Hsu et al.'s Protocol

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$

Hsu et al.'s Protocol

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$

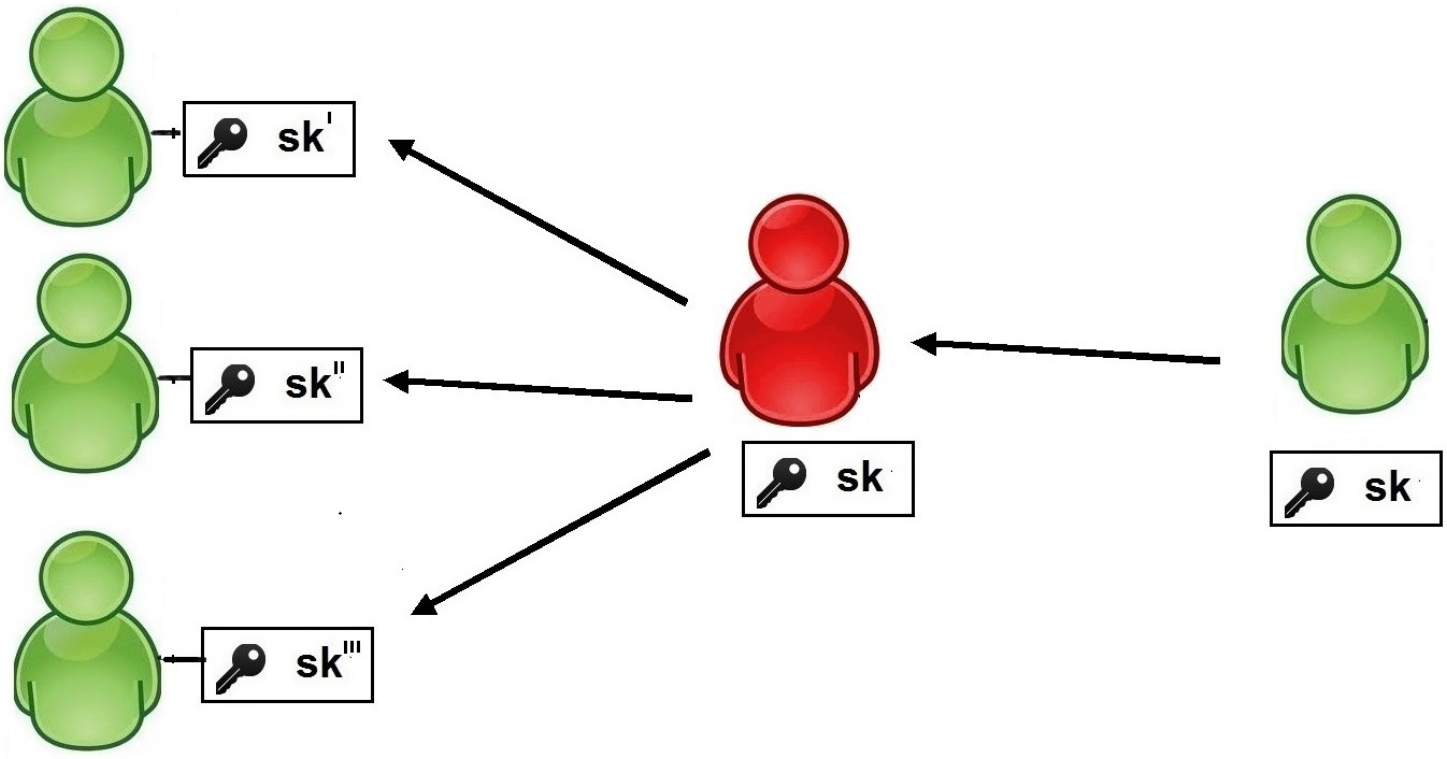
Hsu et al.'s Protocol

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$

Hsu et al.'s Protocol

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$

Insider Attack



Goal: Make different parties end up with distinct keys.

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

Insider Attack

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$ **STOP**	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_a : k = T_a + K_a$	$T_i = k - K_i$ $k_i \leftarrow^R \mathbb{Z}_p^*$; $K_i' = k_i - T_i$ $Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$ $U_a \rightarrow U_i : (Auth_i, K_2, \ldots, K_i', \ldots, K_t)$
Key computation $U_i : k_i = T_i + K_i'$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $\text{ver}.Auth_i = h(k_i, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_i', \ldots K_t)$

1^{st} Solution

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ ver.$Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i v(x_i), r)$ ver.$Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key confirmation $U_i \rightarrow^*: V_i$	$V_i = Sig_{U_i}(h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t))$ ver.$Ver_{U_j}(V_j, h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t))$

1^{st} Solution

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i v(x_i), r)$ $\text{ver}.Auth = h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t)$
Key confirmation $U_i \rightarrow^*: V_i$	$V_i = Sig_{U_i}(h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t))$ $\text{ver}.Ver_{U_j}(V_j, h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t))$

1^{st} Solution

	Sign. No.	Verif. No.	Add. Rounds	Add. Broadcasts Messages
1st Solution	t	$t(t-1)$	1	t

2^{nd} Solution

$U_1 \rightarrow^*: (\{U_1, \ldots, U_t\}, r_1, pk_1)$	$r_1 \leftarrow^R \mathbb{Z}_p^*$
$U_i \rightarrow^*: (r_i, pk_i, Auth_i)$	$r_i \leftarrow^R \mathbb{Z}_p^*$ $S_i = pk_1^{sk_i r_i r_1}$ $Auth_i = h(S_i, r_1)$
$U_1 \rightarrow^*: (Auth, K_2, \ldots, K_t)$	$S_i = pk_i^{sk_1 r_i r_1}$, $S_i = x_i \Vert y_i$ $\text{ver}.Auth_i = h(S_i, r_1)$ $k \leftarrow^R \mathbb{Z}_p^*$, $K_i = k - T_i$ $T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$, $r = (r_1, \ldots, r_t)$ $Auth = Sig_{U_i}(h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t))$
Key computation $U_i : k = T_i + K_i$	$T_i = (y_i \sum_{j=1}^{t} x_i^{j-1} e_j, r)$ $Ver_{U_1}(Auth, h(k, U_1, \ldots, U_t, r_1, \ldots, r_t, K_2, \ldots, K_t))$

2^{nd} Solution

	Sign. No.	Verif. No.	Add. Rounds	Add. Broadcasts Messages
1st Solution	t	$t(t-1)$	1	t
2nd Solution	1	$t-1$	0	0

Conclusions

- Hsu et al. is vulnerable to an insider attack

Conclusions

- Hsu et al. is vulnerable to an insider attack
- We gave 2 solutions to stand against the proposed attack ...

Conclusions

- Hsu et al. is vulnerable to an insider attack
- We gave 2 solutions to stand against the proposed attack ...
- ...that we do not claim to be secure as they lack a security proof!

Conclusions

- Hsu et al. is vulnerable to an insider attack
- We gave 2 solutions to stand against the proposed attack ...
- ...that we do not claim to be secure as they lack a security proof!

Define provable secure GKT protocols!

Thank you!

Q & A