Fully Robust Tree-Diffie-Hellman Group Key Exchange

Timo Brecher
INFODAS GmbH
Germany

Emmanuel Bresson
DCSSI Crypto Lab
France

Mark Manulis
TU Darmstadt & CASED
Germany

CRYPTOGRAPHIC PROTOCOLS

Group Key Exchange

Users in **U** = $\{U_1, \ldots, U_N\}$ run a **Group Key Exchange (GKE)** Protocol and compute a session group key k indistinguishable from $k^* \in_R \{0,1\}^\kappa$

a nice building block for group applications

U_1

U_i

U_N

accept k_1

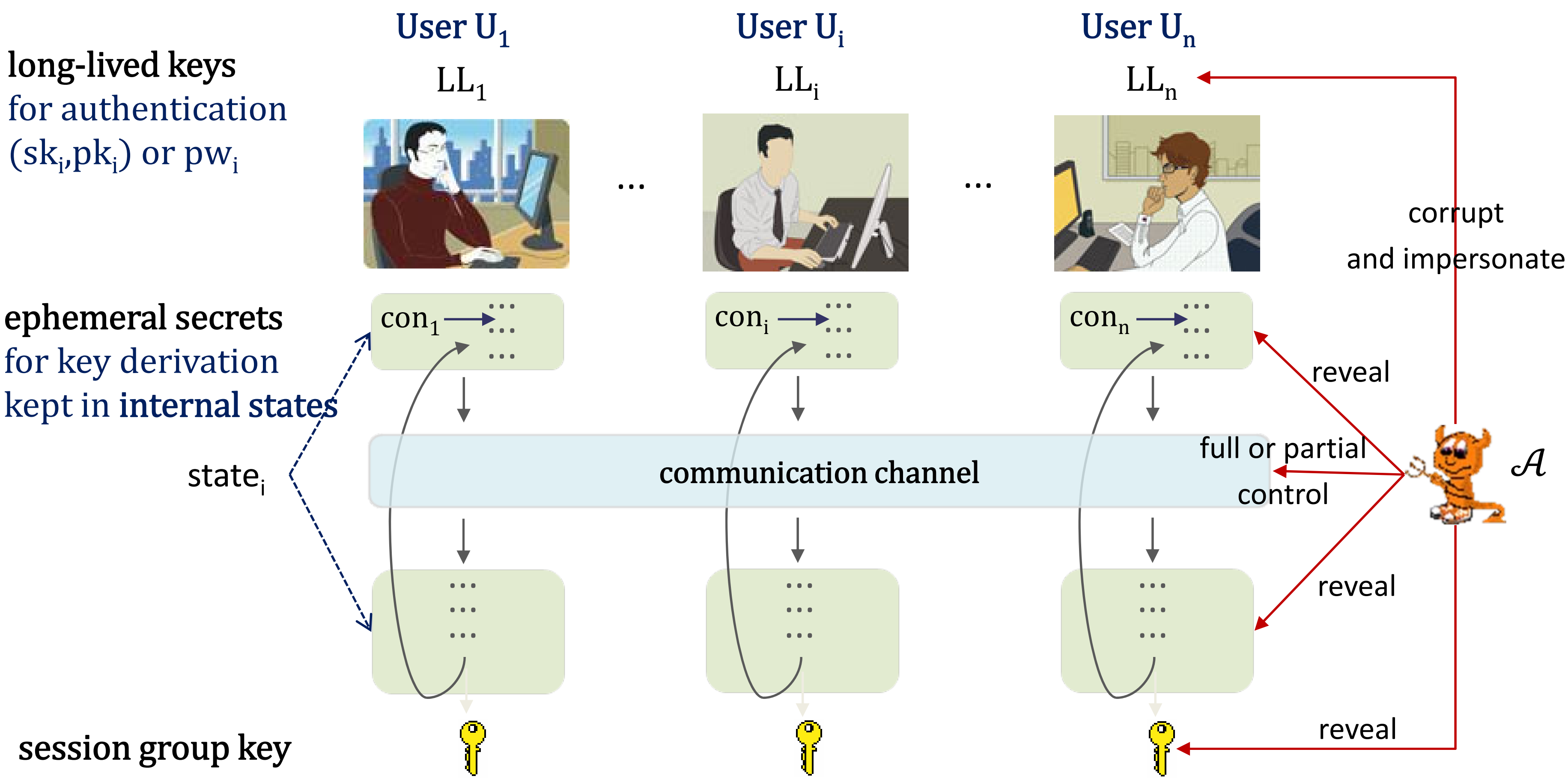
accept k_i

accept k_N

$k_1 = k_2 = \ldots = k_N$

secure (private and authenticated) group channel for $U_1, \ldots, U_N$

Adversary



long-lived keys
for authentication
(sk_i,pk_i) or pw_i
ephemeral secrets
for key derivation
kept in internal states
state_i
session group key
User U_1
User U_i
User U_n
LL_1
LL_i
LL_n
con_1
con_i
con_n
communication channel
corrupt
and impersonate
reveal
full or partial
control
reveal
reveal
𝒜

Diverse Threats and Requirements

Outsider Security
[BCPQ01,KY03,BMS07,BM08,GBG09]

indistinguishability of session keys
authentication/impersonation attacks
forward secrecy
key-compromise impersonation
⇒ **AKE-Security**

there are compilers
authentication compilers
[KY03,BMS07]

Insider Security (optional)
[KS05,DPSW06,BM08,GBG09]

mutual authentication
key confirmation
key compromise impersonation
⇒ **MA-Security**

there are compilers
for MA-security and
contributiveness
[KS05,BM07,BM08]

key replication, control
contributiveness
⇒ **Contributiveness**

Robustness
[CS04,DPSW06,JKT07,KT08]

in general the goal of robustness is to ensure fault-tolerance
(users should be able to proceed and compute session keys despite of identified failures)

Non-Robust GKE

Problems in non-robust GKE protocols

outsider and optionally insider attacks are prevented

but at the cost that the protocol execution aborts!

Robust GKE

protocol execution should continue despite of

network faults	sent messages are not delivered properly
system crashes	the system remains inoperable and needs restart
malicious user behavior	essentially the *insider attacks*

Fully Robust GKE[JKT07]

protocol execution succeeds despite of up to n–2 failed users

Amir et al.'s Robust GKE

GCS-based solution[AN-RSSKT01]

execute *dynamic GKE protocol* (e.g. [S02])

(handles joins and leaves of users)

on top of a *membership view-based group communication system*

ensures reliable communication

updates the set of alive users in a consistent way

Observations

execution of GKE can still abort

GKE protocol has to be restarted if GCS notices a failure

Cachin-Strobl‘s Robust GKE

Consensus-based solution[CS04]

asynchronous reliable channel with authentication

generalized abstraction of Burmester-Desmedt protocol[BD94]

fault-tolerance via *k-resilient consensus protocol*[CKS00,CR01]

achieves strong AKE-security
for the <u>optimal bound</u> of n – 2k corrupted users

Observations

does not address insider attacks

not fully robust … as a consequence of the consensus protocol

(the optimal bound holds only for the asynchronous communication)

Desmedt et al.'s Robust GKE

VSS-based solution[DPSW06]

weakly synchronized reliable broadcast channel without authentication

fault tolerance via *(k-out-of-n) VSS technique*[P91]

modified Katz-Yung technique[KY03] for authentication

achieves weak AKE / MA and non-malleability

non-malleability is stronger than contributiveness

but the corruption model is weak

Observations

not fully-robust … as a consequence of VSS technique

assumes weak corruption model

Jarecki et al.'s Robust GKE

„Transitive closure of a circle"-based solution[JKT07]

weakly synchronized reliable broadcast channel with authentication

4 protocols that differ in complexity / robustness

fault tolerance via *a new circle-replication technique* for [BD94]

multiple circles with different subsets of users

Observations

does not consider active/impersonation attacks

does not consider insider attacks

assumes that each user fails with the same probability

In Comparison to this…

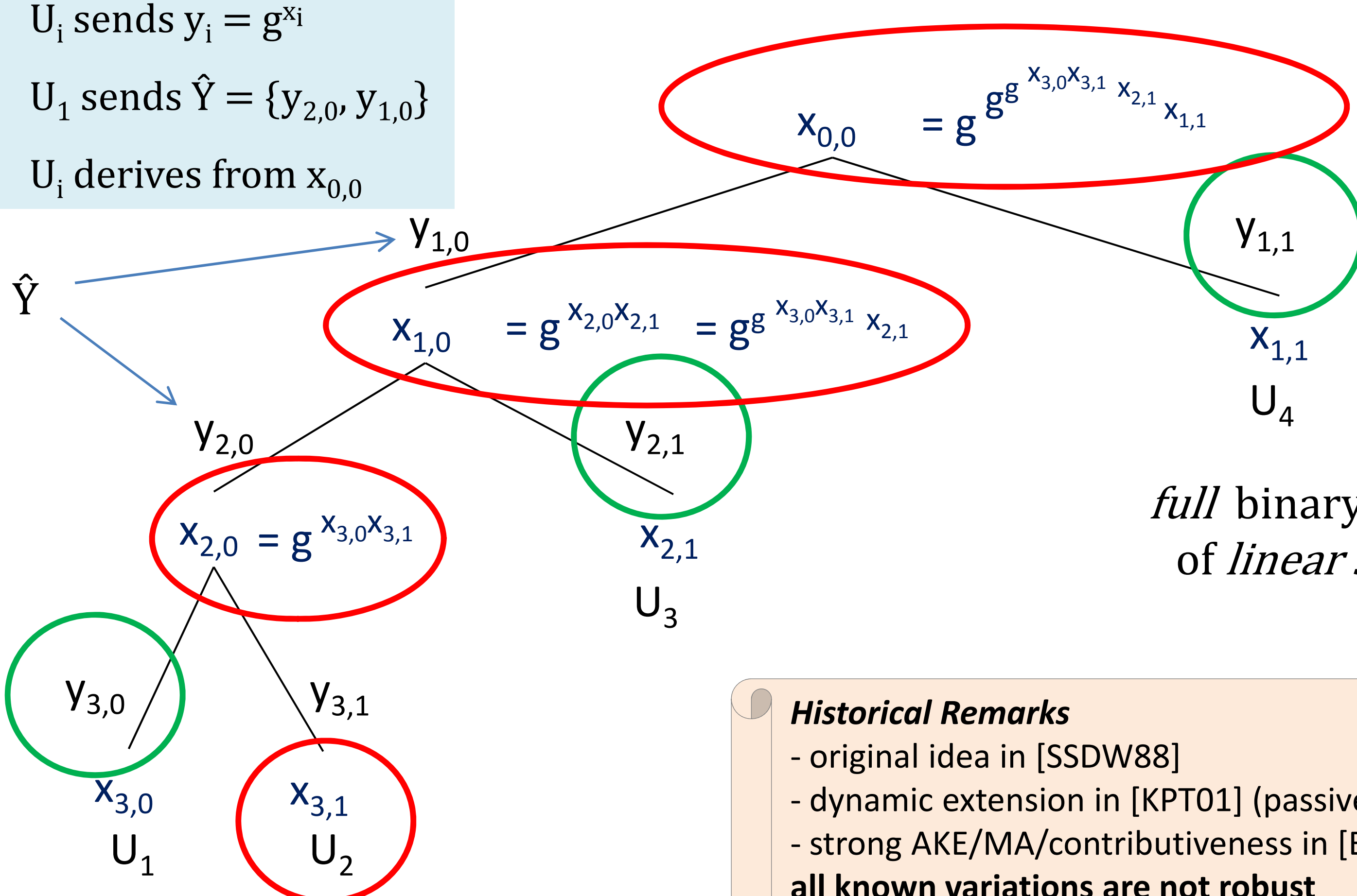
GKE	Out- /Insider Security				Robustness	Costs		
	AKE	MA	Con	Model	max. #Faults	Rnd	BCast	Ops/ User
VSS-based[DPSW06]	w	w	w	STD	n/2 – 1	8	O(nk)	O(n)
BD-RGKA[JKT07]	w	-	-	STD	n – 2	3	$O(n^3)$	$O(n^2)$
RGKA[JKT07]	w	-	-	STD	n – 2	3	$O(n^2)$	O(n)
t-RGKA[JKT07]	w	-	-	STD	2t – 1	3	O(nt)	O(t)
RGKA‘[JKT07]	w	-	-	STD	n – 2	$O(\delta)$	O(nlogn)	O(n)
R-TDH1	**s**	**-**	**-**	**STD**	**n – 2**	**3**	**$O(n^2)$**	**O(n)**
IR-TDH1	**s**	**s**	**s**	**ROM**	**n – 2**	**3**	**$O(n^2l)$**	**O(nl)**
TDH1[BM08]	s	s	s	STD	0	3	O(n)	O(n)

w – weak corruptions (reveal LLs)

s – strong corruptions (reveal LLs and states)

Tree Diffie-Hellman (simplified)

Round 1	U_i sends $y_i = g^{x_i}$
Round 2	U_1 sends $\hat{Y} = \{y_{2,0}, y_{1,0}\}$
Key	U_i derives from $x_{0,0}$



full binary tree of *linear size*

Historical Remarks

- original idea in [SSDW88]
- dynamic extension in [KPT01] (passive case)
- strong AKE/MA/contributiveness in [BM08]

all known variations are not robust

Communication Channel and Model

Channel

weakly synchronized reliable broadcast without authentication i.e. [DPSW06,JKT07]

Broadcast of Round Messages

for each round $\mathcal{A}$ is given the set S of round messages (of honest users)

the *round timer* is started (sufficiently large to cover delays)

$\mathcal{A}$ can modify the set S (e.g., change/inject, order/delete messages)

$\mathcal{A}$ outputs modified set S' (prior to timer expiration)

Delivery of Round Messages

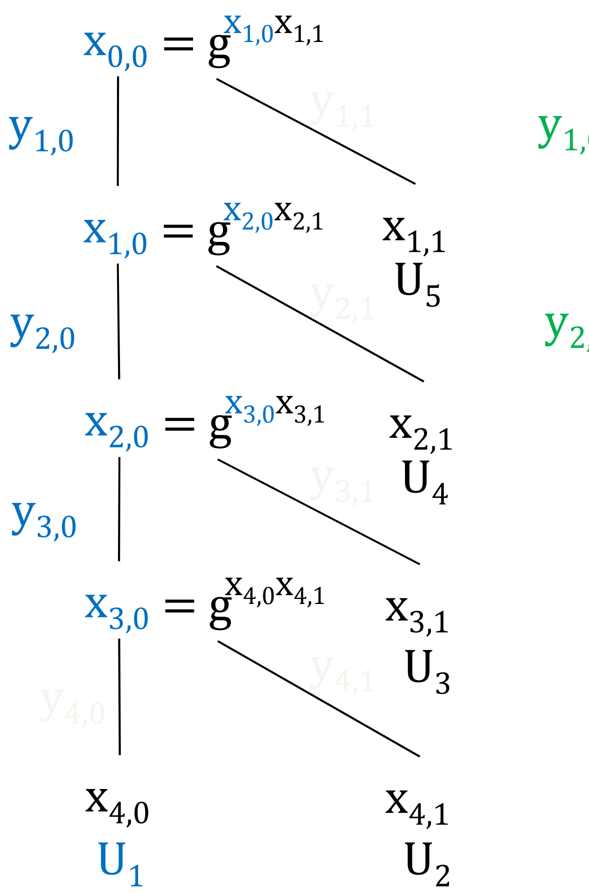
S' determines which users are still active/alive/connected

messages in S' are delivered to all connected users

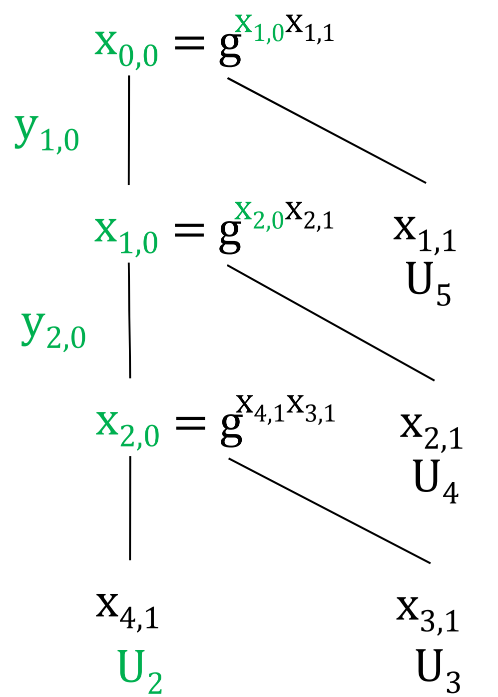
each connected user updates its own *set of active* users (denoted **pid**)

„Tree-Replication Technique“

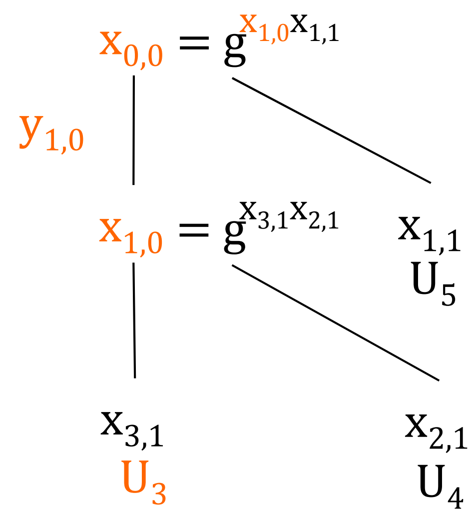
(applies in Round 2)



sends $\hat{Y}_1 = y_{3,0}, y_{2,0}, y_{1,0}$



sends $\hat{Y}_2 = y_{2,0}, y_{1,0}$



sends $\hat{Y}_3 = y_{1,0}$

U_4 and U_5 send ‘alive‘

choose $\hat{Y}_\gamma$ from all round messages

γ : lowest-index of a user U_γ

compute $x_{0,0}$ using $\hat{Y}_\gamma$

if $\gamma = 4$ then $x_{0,0} = g^{x_{2,1}x_{1,1}}$

R-TDH1 (Outsider Security) I

Preliminaries

$pid_i = U_1|\ldots|U_n$

public constant v_0

Round 1 (Broadcast)

U_i broadcasts $U_i|1|r_i$

Round 2 (Broadcast)

U_i updates pid_i and aborts* if $pid_i = U_i$

$nonces_i = r_1|\ldots|r_n$

broadcasts $U_i|2|y_i|\sigma'_i$

U_1	U_2	U_3	U_4	U_5
r_1	r_2	r_3	r_4	r_5
$y_1 = g^{x_1}$	$y_2 = g^{x_2}$	$y_3 = g^{x_3}$	$y_4 = g^{x_4}$	$y_5 = g^{x_5}$
σ'_1	σ'_2	σ'_3	σ'_4	σ'_5

* abort implies erasure of internal states

R-TDH1 (Outsider Security) II

Round 3 (Broadcast)

U_i updates pid_i and $nonces_i$

computes X_i (incl. $x_{0,0}$) and $\hat{Y}_i$

broadcasts $U_i|3|\hat{Y}_i|\sigma''_i$

U_4, U_5 broadcast $U_{4|5}|3|$'alive'$|\sigma''_i$

Group key derivation

U_i updates pid_i and $nonces_i$

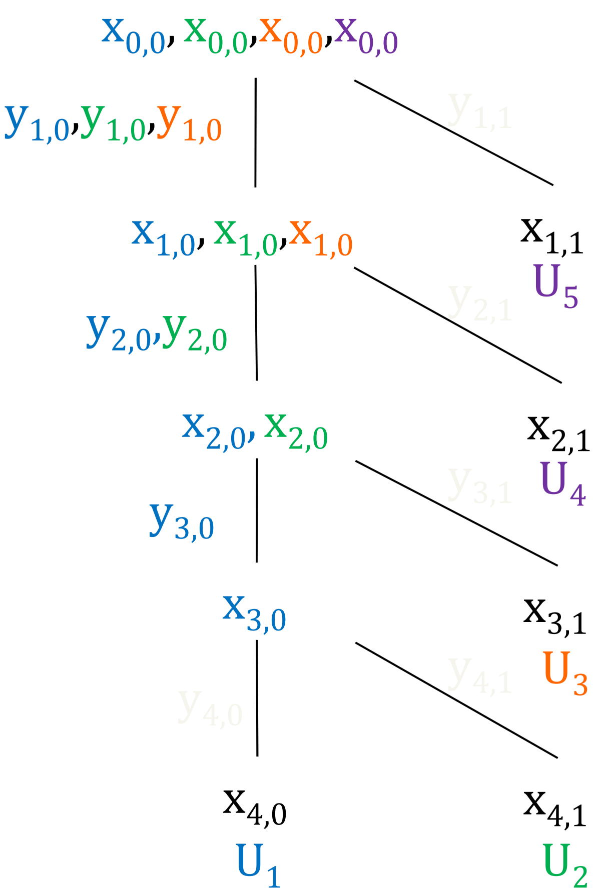
determines γ

computes $x_{0,0}$ using $\hat{Y}_\gamma$

computes $K_i = PRF_{x_{0,0}}(v_0)$

erases all ephemeral secrets

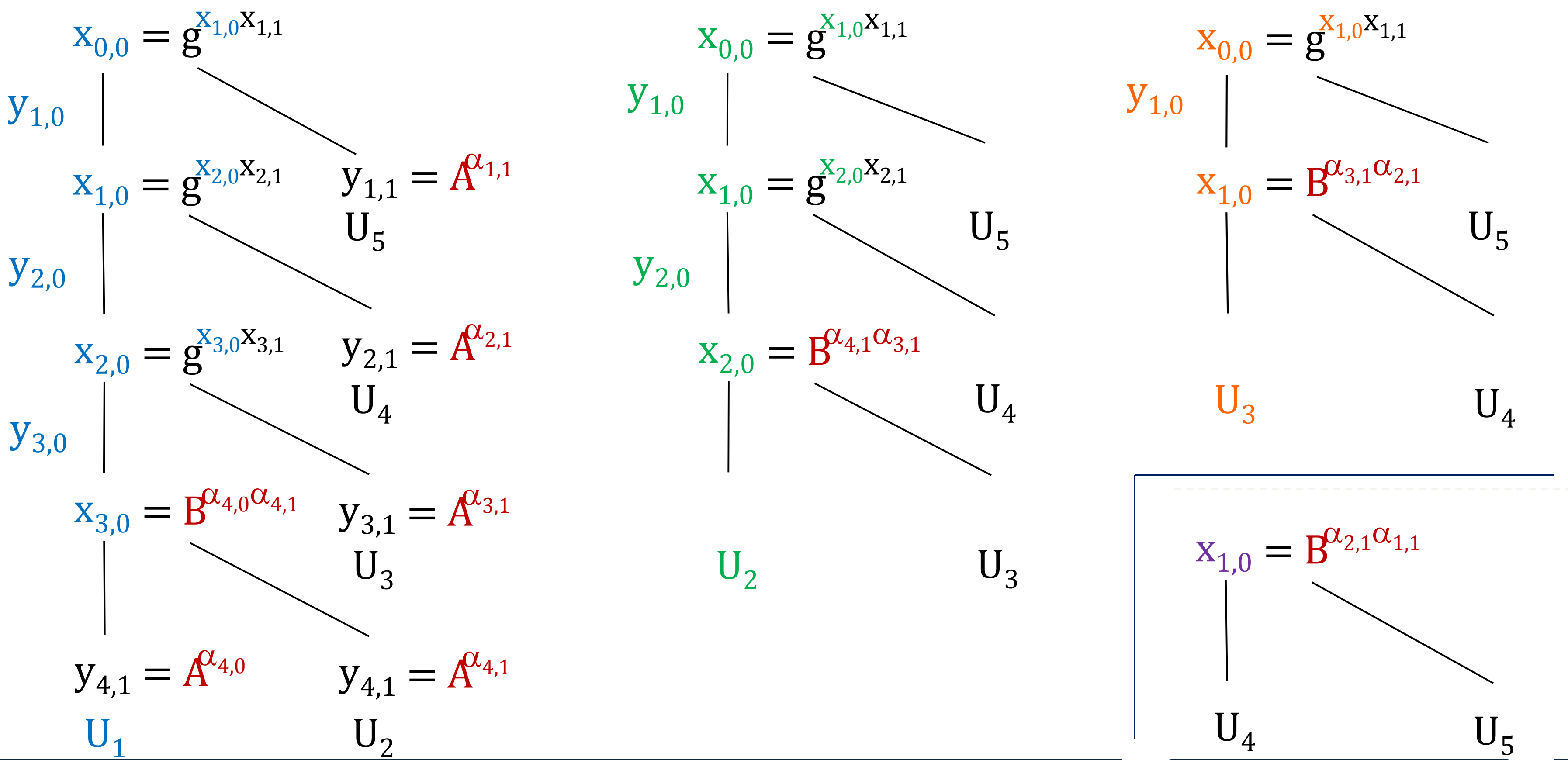
accepts K_i



Security of „Tree Replication Technique“

Square-Exponent Decisional Diffie-Hellman (SEDDH) Assumption[W99,SS01]

given $(g, A=g^a, B)$ decide whether $B=g^{a^2}$ or g^b



Consistency of $\hat{Y}_i$ for Insider Security

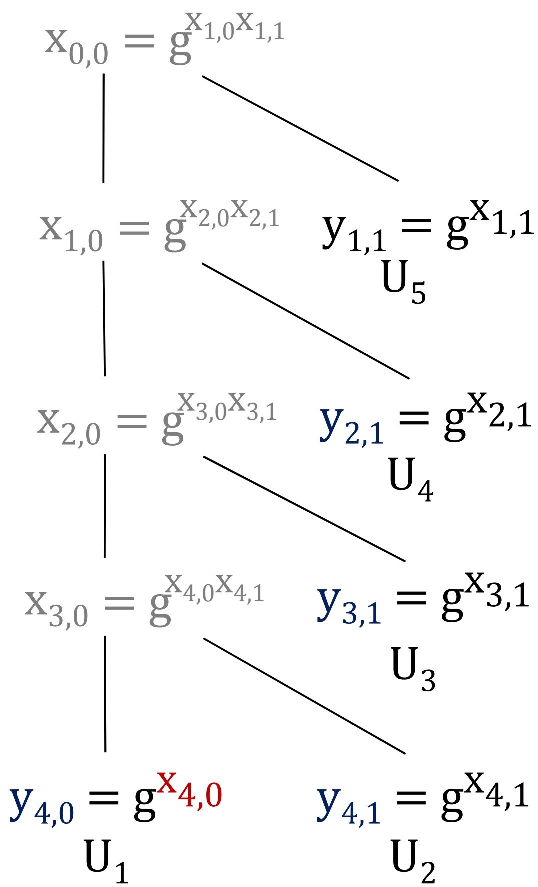
$$y_{1,0} = g^{x_{1,0}} = g^{y_{2,1}^{x_{2,0}}}$$

$$y_{2,0} = g^{x_{2,0}} = g^{y_{3,1}^{x_{3,0}}}$$

$$y_{3,0} = g^{x_{3,0}} = g^{y_{4,1}^{x_{4,0}}}$$

↑

$\hat{Y}_1$



U_i proves in ZK [S96, AST02]

$$\mathrm{Log}_g(y_{l,0}) = \mathrm{Log}_{y_{l,1}}(\mathrm{Log}_g(y_{l-1,0}))$$

starting with own $y_i = g^{x_i}$

$$y_{2,0} = g^{x_{2,0}} \quad \wedge \quad y_{1,0} = g^{y_{2,1}^{x_{2,0}}}$$

$$y_{3,0} = g^{x_{3,0}} \quad \wedge \quad y_{2,0} = g^{y_{3,1}^{x_{3,0}}}$$

$$y_{4,0} = g^{x_{4,0}} \quad \wedge \quad y_{3,0} = g^{y_{4,1}^{x_{4,0}}}$$

Conclusion

R-TDH1: Optimally Robust TDH1 with Outsider Security

robustness of Tree-Diffie-Hellman[SSDW88,KPT01,BM08] via „Tree Replication Technique“

authentication via signatures[KY03,DPSW06]

outsider security (AKE-security) in the standard model

IR-TDH1: Optimally Robust THD1 with Insider Security

consistency of tree computations via NIZK proofs

key confirmation via signatures[KS05,BMS07]

insider security (MA-security/contributiveness) in the random oracle model

Unification of Security Models (not covered by the talk)

stronger security definitions from [BM08,GBG09]

strong AKE-/MA-security, contributiveness

robustness from [DPSW06], optimality from [JKT07]

non-authenticated reliable broadcast with weak synchrony