Affiliation-Hiding Key Exchange with Untrusted Group Authorities

Mark Manulis[1], Bertram Poettering[1], Gene Tsudik[2]

[1]Cryptographic Protocols Group, TU Darmstadt & CASED, Germany

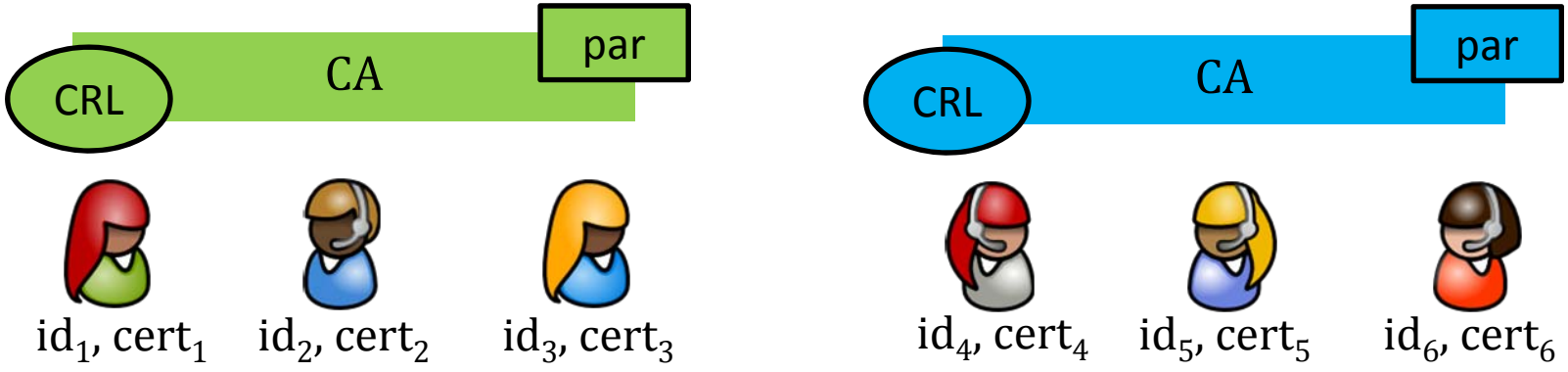
[2]University of California, Irvine, USA

PKI-based Authentication and Key Exchange

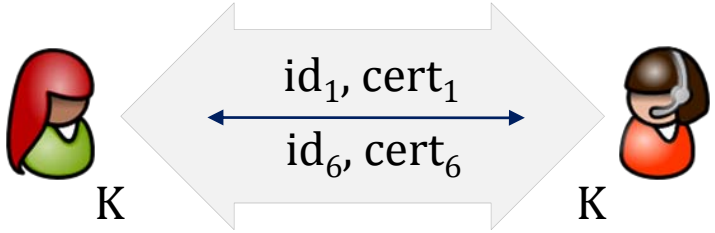
Certification Authorities mainly responsible for

Registration register users, issue certificates on user ids/keys

Revocation revoke user certificates, manage CRLs



Authenticated Key Exchange succeeds if users prove *possession of valid certificates.*



successful/unsuccessful executions
reveal corresponding CAs

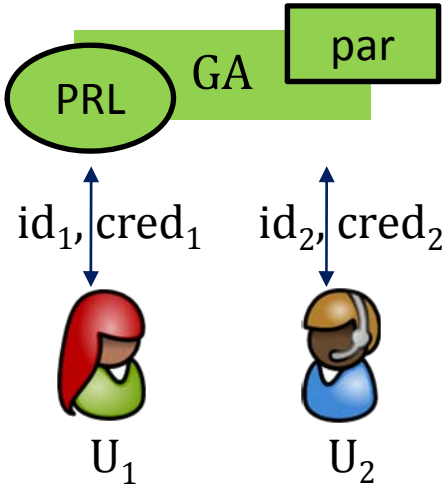
(to communication partners and outsiders)

Affiliation-Hiding Authenticated Key Exchange

Group Authorities mainly responsible for

Registration	admit members, issue pseudonyms and credentials
Revocation	revoke credentials via pseudonym revocation lists (PRLs)

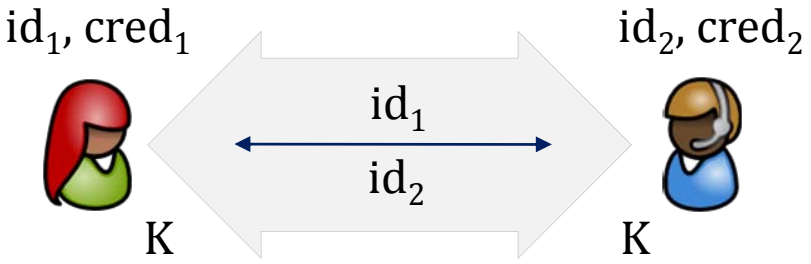
Admission of Members



each user U_i obtains

pseudonym id_i and *credential* $cred_i$

Affiliation-Hiding Authenticated Key Exchange



succeeds if valid $cred_1$ and $cred_2$ have been issued by the *same* GA

if unsuccessful then GA is not revealed

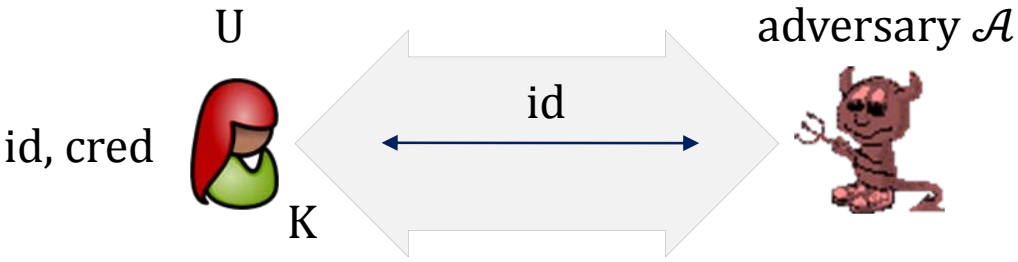
(Linkable) AH-AKE Syntax

CreateGroup(1^κ)	Algorithm executed by the GA to create a group G. Outputs (G.sk, G.pk) and G.PRL.
AddUser(U, GA)	Protocol between GA and a new user U. U obtains *pseudonym* id and *credential* cred. Each U can be a member of multiple groups.
Handshake(id_i, id_j)	Protocol between users with id_i and id_j. Each user uses own cred for some group G. If both users use credentials for the same group G then they compute a shared key K.
Revoke(G.sk, G.PRL, id)	Algorithm executed by the GA of G. Adds pseudonym id to G.PRL. G.PRL is distributed in an authentic way.

(Linkable) Affiliation-Hiding Property

Affiliation-Hiding is the distinguished *privacy property* of AH-AKE protocols.

Let U be a member of some group G ⇒ U holds (id, cred) for G.



If $\mathcal{A}$ does *not* have valid credential for G then

no information about G should leak to $\mathcal{A}$.

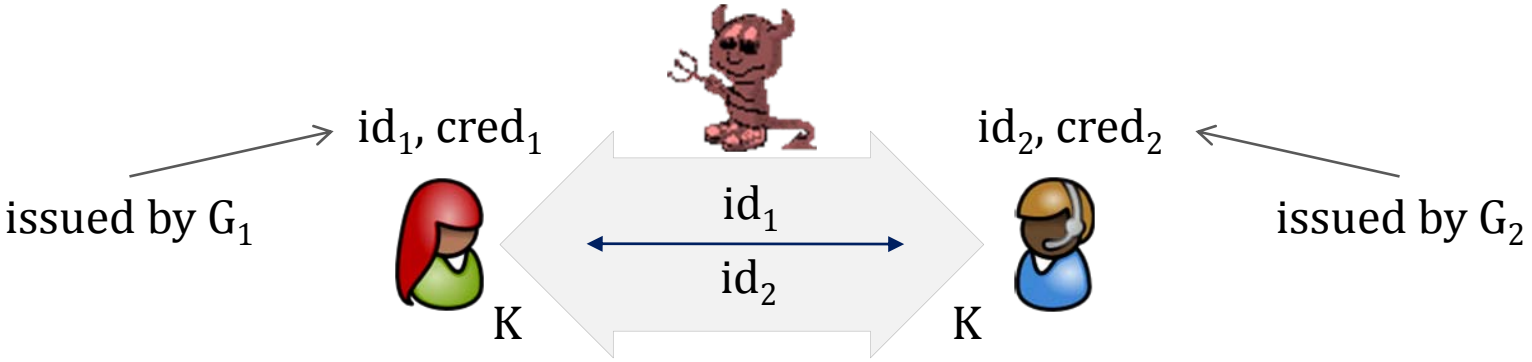
affiliation-hiding is a privacy goal *shared* by all members of the group

Remark We consider *linkable* protocols where users participate via pseudonyms.

Authenticated Key Exchange Security

Authenticated Key Exchange (AKE) Security

Essentially the same goal as in the classical authenticated key exchange protocols.



If $G_1 = G_2$ then U_1 and U_2 compute a secure session key k.

- Requires *key secrecy* modeled as indistinguishability of K from a random key.
- Requires *forward secrecy*, i.e. key secrecy in case U_1 and U_2 become corrupted.

Malicious Group Authorities

Current AH-AKE protocols, e.g. [BDS+03,CJT04,XY04,TX06, AKB07,JKT08], assume that GAs are fully trusted

Our goal is to reduce this trust by considering *malicious* behaviour of the GAs.

Case 1: adversary $\mathcal{A}$ controls GAs from the beginning

- $\mathcal{A}$ may generate public group parameters in some rogue way.
- $\mathcal{A}$ may admit honest users to its groups and misbehave upon their admission.
- $\mathcal{A}$ may bias handshake executions amongst honest members of its group.
- $\mathcal{A}$ may trace real identity U of a user from later handshake sessions.

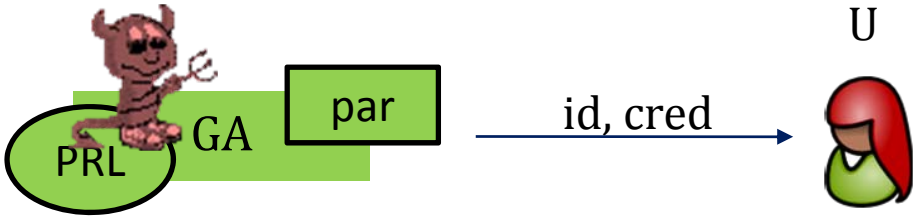
Case 2: adversary $\mathcal{A}$ corrupts GAs at a later stage

- $\mathcal{A}$ may mount attacks as in Case 1 except for the rogue generation of parameters.

What is the impact of malicious GAs on the security and privacy in AH-AKE protocols?

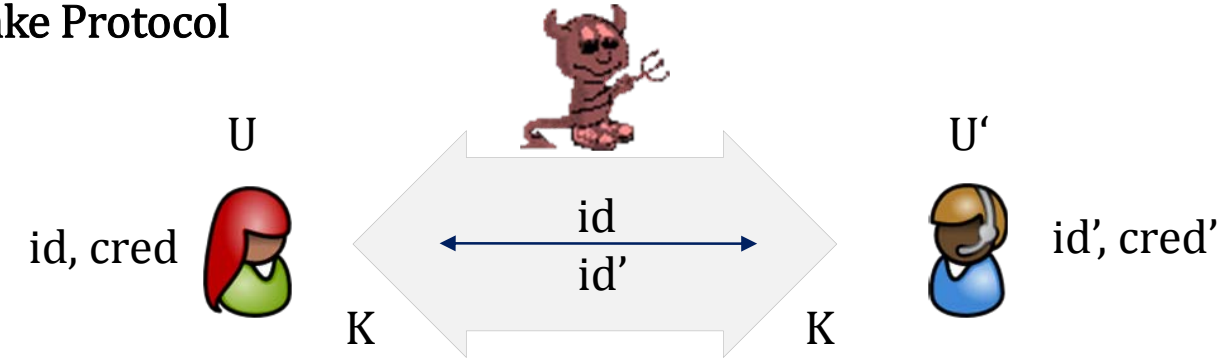
Malicious GAs against Affiliation-Hiding

in AddUser Protocol



In existing schemes $\mathcal{A}$ learns id (and even cred) of U.

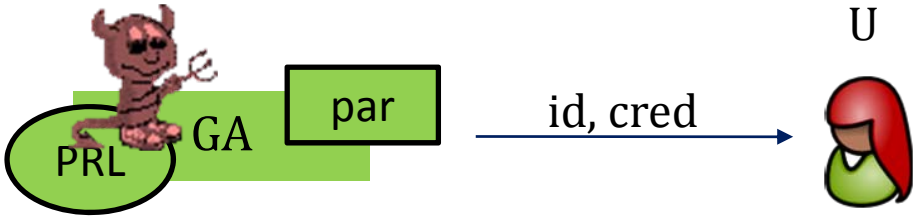
in Handshake Protocol



Even if $\mathcal{A}$ does not introduce phantom group members
it can immediately tell the affiliation of U upon seeing the pseudonym id.

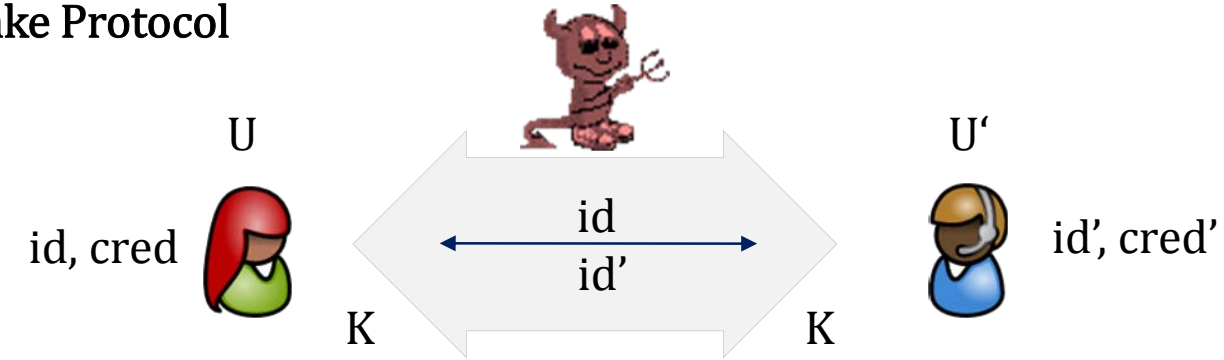
Malicious GAs against AKE-Security

in AddUser Protocol



In existing schemes $\mathcal{A}$ learns id (and even cred) of U.

in Handshake Protocol

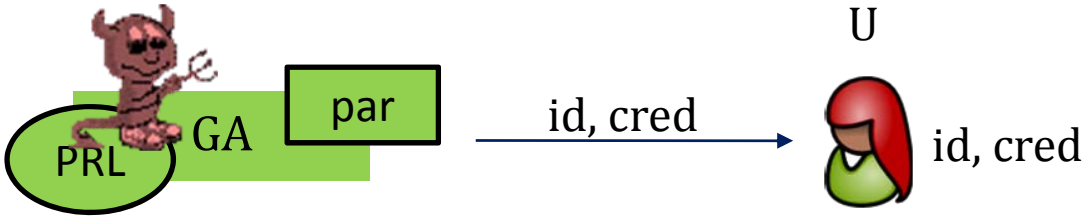


Even if $\mathcal{A}$ does not introduce phantom group members

it can usually distinguish key K from random by impersonating id'.

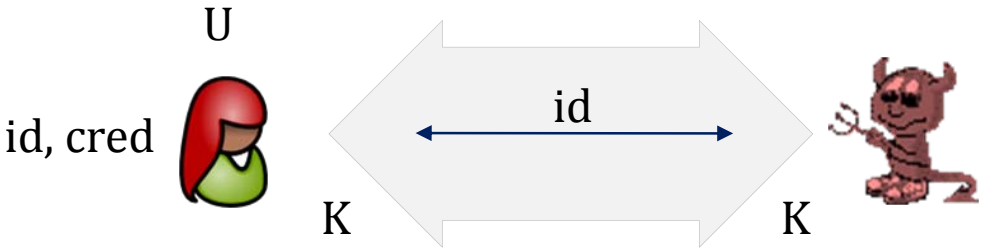
New Requirement: Untraceability

in AddUser Protocol



$\mathcal{A}$ can store (id, U) and possibly cred for the later use.

in Handshake Protocol



$\mathcal{A}$ can easily trace real identity U in its handshake sessions from pseudonym id.

untraceability is an *individual* privacy goal of each user

State-of-the-Art Linkable AH-AKE

Jarecki-Kim-Tsudik, CT-RSA 2008

RSA modulus $n = pq$ where $p = 2p' + 1$, $q = 2q' + 1$ are safe primes.

RSA exponents (e, d) where $e = d^{-1} \bmod \varphi(n)$.

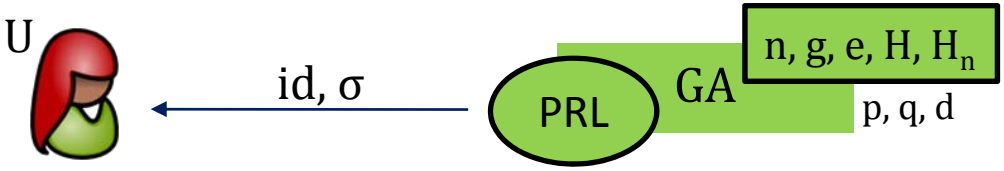
Generator g s.t. $\mathrm{ord}(q) = 2p'q'$ and $-1 \notin \langle g \rangle \Rightarrow \mathbb{Z}_n^* \cong \langle -1 \rangle \times \langle g \rangle$.

Hash functions $H_n: \{0,1\}^* \longrightarrow \mathbb{Z}_n^*$ and $H: \{0,1\}^* \longrightarrow \{0,1\}^\kappa$.

Group Parameters G.sk := (p, q, d), public: G.pk := (n, g, e), G.PRL, H, H_n

AddUser Protocol GA issues cred as an FDH-RSA signature on some id

$\sigma := H_n(\mathrm{id})^d \bmod n$ with $\mathrm{id} \in \{0,1\}^\kappa$



Remark From AddUser protocol GA learns (U, id, σ).

⇒ All previously discussed attacks of a malicious GA apply.

State-of-the-Art Linkable AH-AKE (II)

Handshake Protocol U_A is in G_A, U_B is in G_B $\quad \mathbb{Z}_{n_A}^* \cong \langle -1 \rangle \times \langle g_A \rangle$, $\mathbb{Z}_{n_B}^* \cong \langle -1 \rangle \times \langle g_B \rangle$

(id_A, σ_A)
$(n_A, g_A, e_A, G_A.PRL)$

U_A

U_B

(id_B, σ_B)
$(n_B, g_B, e_B, G_B.PRL)$

random bit · exponent · padding (hides n_A)

$$\theta_A := \underbrace{(-1)^{b_A} \cdot \sigma_A \cdot g_A^{x_A} \bmod n_A}_{\text{uniform in } \mathbb{Z}_{n_A}^*} + k_A \cdot n_A$$

$H_{n_B}(id_B)^{d_B} \bmod n_B$

$$\theta_B := (-1)^{b_B} \cdot \sigma_B \cdot g_B^{x_B} \bmod n_B + k_B \cdot n_B$$

$id_A, \theta_A \rightarrow$
$\leftarrow id_B, \theta_B$

if $id_B \notin G_A.PRL$:
$K_A := H(r_A, sid_A)$, $C_A := H(r_A, sid_A, 0)$
s.t. $r_A := (\theta_B^{e_A} \cdot H_{n_A}(id_B)^{-1})^{2x_A} \bmod n_A$
else:
$K_A, C_A \leftarrow_R \{0,1\}^\kappa$

if $id_A \notin G_B.PRL$:
$K_B := H(r_B, sid_B)$, $C_A := H(r_B, sid_B, 1)$
s.t. $r_B := (\theta_A^{e_B} \cdot H_{n_B}(id_A)^{-1})^{2x_B} \bmod n_B$
else:
$K_B, C_B \leftarrow_R \{0,1\}^\kappa$

$C_A \rightarrow$
$\leftarrow C_B$

check C_B, accept K_A (random if check fails)

check C_A, accept K_B

Remark if $G_A = G_B$ then $r_A = r_B = g^{2ex_Ax_B}$ (Diffie-Hellman value in $\langle g \rangle$)

Avoiding Rogue Group Parameters

How to enforce honest generation of parameters?

Applies only if GA is malicious from the beginning.

In general GA must prove that parameters have been generated in a correct way.
This can be done by using appropriate *(non-interactive) zero-knowledge proofs*.

In JKT08 protocol

GA must provide a **ZKPoK $\Pi_{n,g}$** for the following statement where (n, g, κ) are public:

$$n = pq \wedge p = 2p'+1 \wedge q=2q'+1 \wedge |p'|=\kappa \wedge |q'|=\kappa \wedge p', q' \in \mathit{PRIMES} \wedge \mathrm{ord}(g) = 2p'q' \wedge -1 \notin \langle g \rangle$$

Camenisch-Michels, Eurocrypt 1999 show how to prove part of this, namely

$$n = pq \wedge p = 2p'+1 \wedge q=2q'+1 \wedge |p'|=\kappa \wedge |q'|=\kappa \wedge p', q' \in \mathit{PRIMES}$$

We *extend* their proof towards the missing part $\wedge \mathrm{ord}(g) = 2p'q' \wedge -1 \notin \langle g \rangle$

We use the sufficient condition that $g^{p'q'} = \pm\omega \bmod n$ for some $\omega \in \mathbb{Z}_n^*$, $\omega \neq 1$.

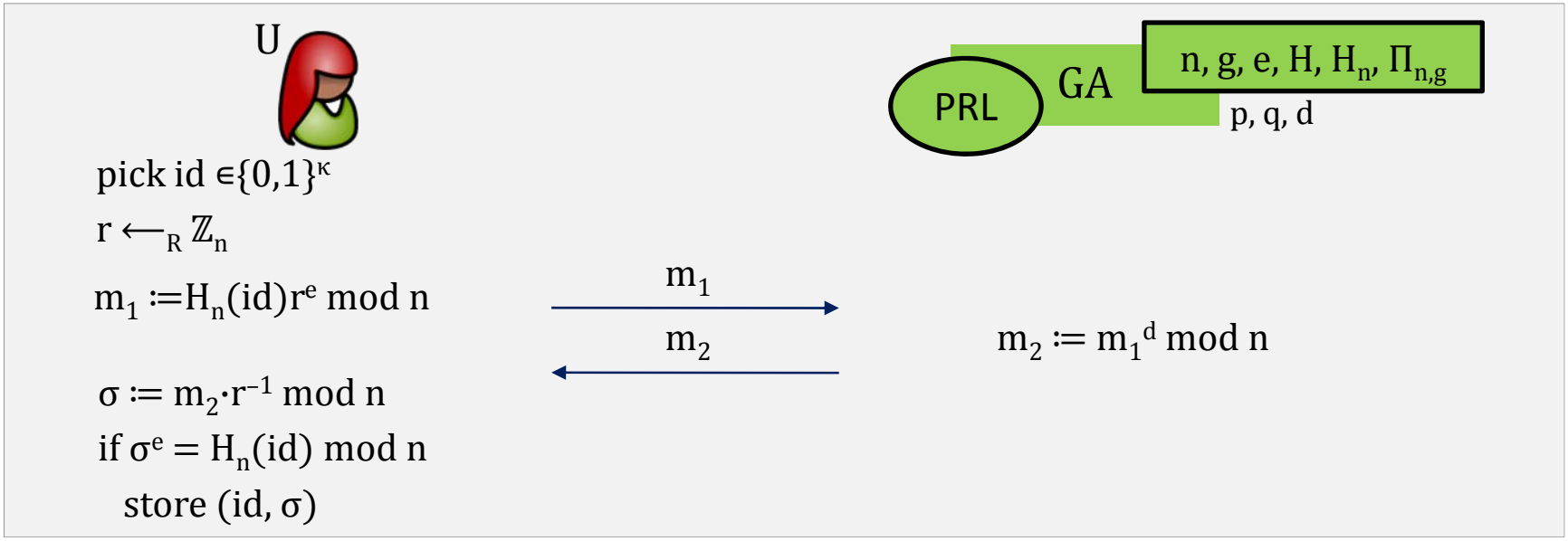
First Step Towards Untraceability

We need to break the link between real identity U and pseudonym id in AddUser.

In JKT08 protocol

Instead of GA issuing (id, σ) we use blind FDH-RSA signature (Chaum, Crypto 1982).

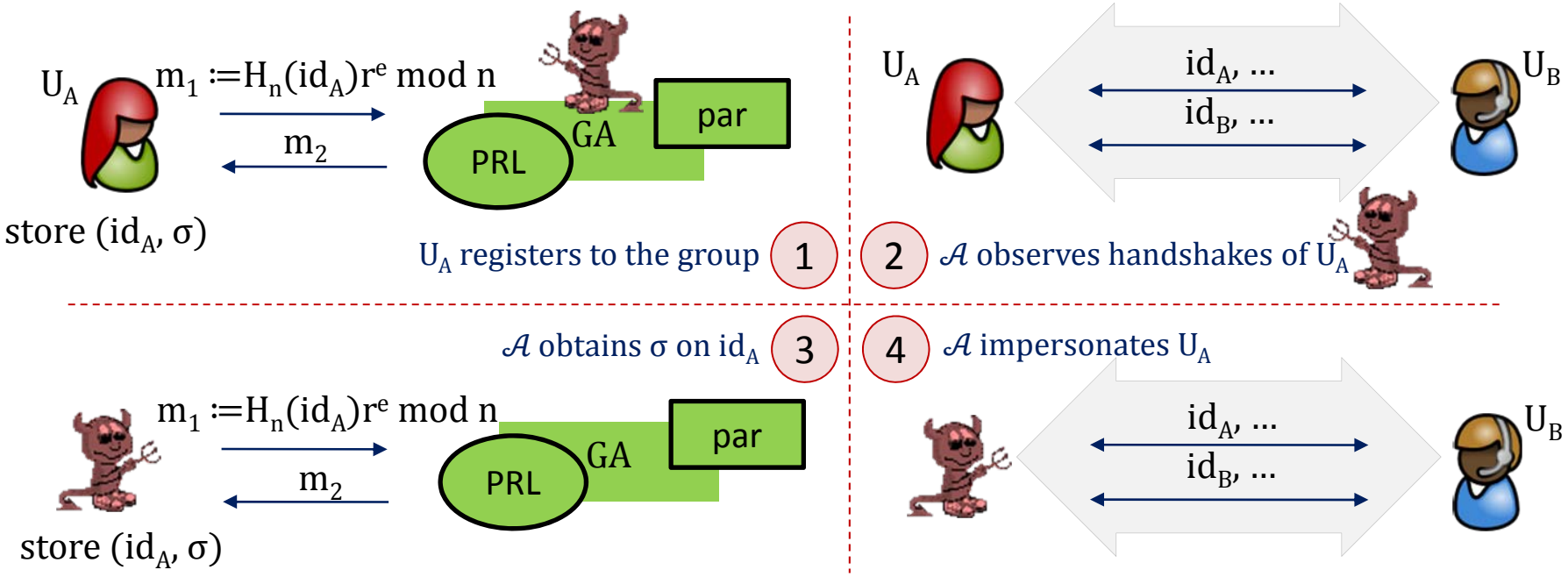
We assume that U checks ZKPoK $\Pi_{n,g}$ beforehand.



Preventing Impersonation of Honest Users

The use of a blind signature on id alone is not sufficient!

We should also care about impersonation attacks on honest users.

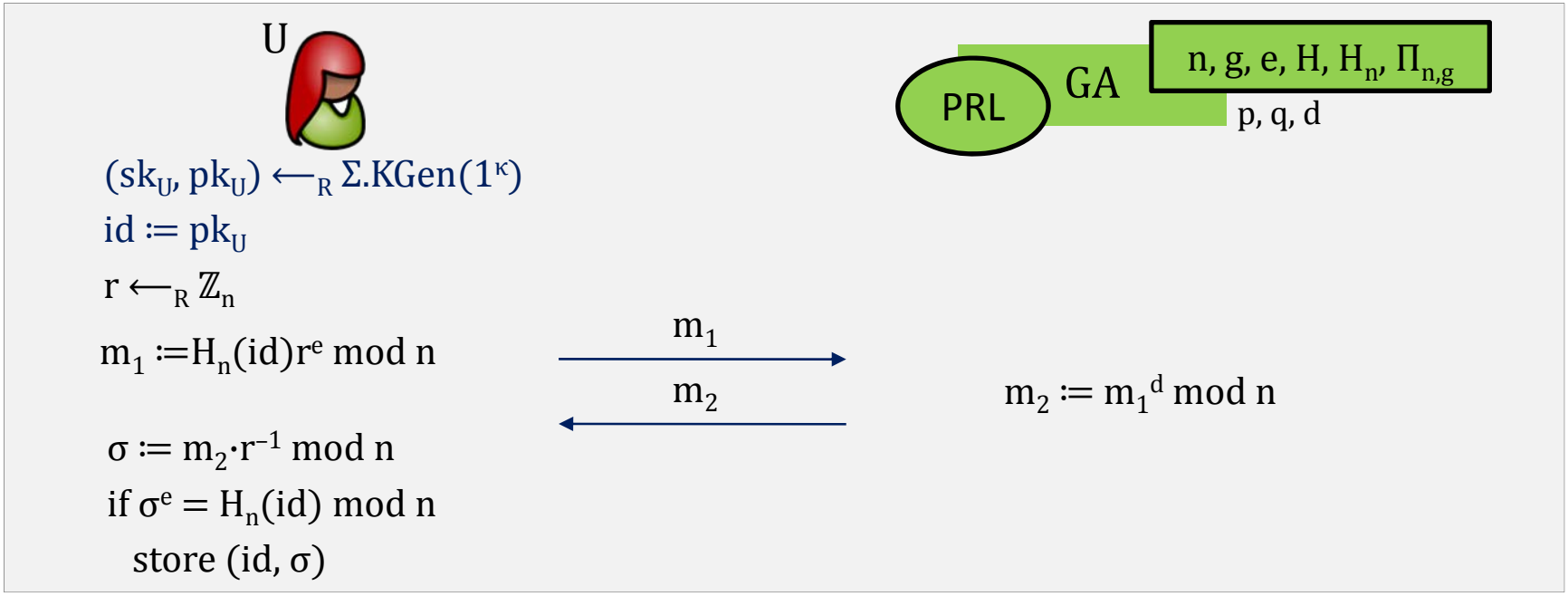


We must ensure that each user can claim *possession* of the pseudonym!

Our AH-AKE with Untrusted GAs: AddUser

Let $\Sigma := (\mathrm{KGen}, \mathrm{Sign}, \mathrm{Verify})$ be a EUF-CMA secure digital signature scheme.

Main Idea **Bind pseudonyms to signature keys.**



The proof of possession of sk_U is postponed to the handshake protocol.

Our AH-AKE with Untrusted GAs: Handshake

U_A (sk_A, id_A, σ_A) $(n_A, g_A, e_A, G_A.PRL)$

U_B (sk_B, id_B, σ_B) $(n_B, g_B, e_B, G_B.PRL)$

random bit, exponent, padding (hides n_A)

$\theta_A := (-1)^{b_A} \cdot \sigma_A \cdot g_A^{x_A} \bmod n_A + k_A \cdot n_A$

uniform in $\mathbb{Z}_{n_A}^*$

id_A, θ_A →

← id_B, θ_B

$H_{n_B}(id_B)^{d_B} \bmod n_B$

$\theta_B := (-1)^{b_B} \cdot \sigma_B \cdot g_B^{x_B} \bmod n_B + k_B \cdot n_B$

if $id_B \notin G_A.PRL$:

$K_A := H(r_A, sid_A)$, $C_A := H(r_A, sid_A, 0)$

s.t. $r_A := (\theta_B{}^{e_A} \cdot H_{n_A}(id_B)^{-1})^{2x_A} \bmod n_A$

else:

$K_A, C_A \leftarrow_R \{0,1\}^\kappa$

$s_A := \Sigma.Sign(sk_A, (C_A, sid_A))$

s_A →

← s_B

$s_B := \Sigma.Sign(sk_B, (C_B, sid_B))$

check s_B, accept K_A (random if check fails)

if $id_A \notin G_B.PRL$:

$K_B := H(r_B, sid_B)$, $C_A := H(r_B, sid_B, 1)$

s.t. $r_B := (\theta_A{}^{e_B} \cdot H_{n_B}(id_A)^{-1})^{2x_B} \bmod n_B$

else:

$K_B, C_B \leftarrow_R \{0,1\}^\kappa$

check s_A, accept K_B

signatures s_A and s_B prevent impersonation attacks and provide key confirmation

Security of Our (Linkable) AH-AKE Scheme

Original JKT08 Protocol	secure in a model with **trusted GAs** + ROM
Affiliation-Hiding	RSA assumption with Safe RSA Moduli (given n, e, g find z such that $z^e = g \bmod n$)
AKE-Security	same assumptions as for affiliation-hiding
Our AH-AKE Protocol	secure in a model with **untrusted GAs** + ROM
Affiliation-Hiding	- RSA assumption with Safe RSA Moduli - CDH assumption in $\langle g \rangle \subset \mathbb{Z}_n^*$, $\mathrm{ord}(g) = 2p'q'$ (given g, g^a, g^b find g^{ab}) - soundness + zero-knowledge of $\Pi_{n,g}$ - EUF-CMA security of Σ
AKE-Security	same assumptions as for affiliation-hiding
Untraceability	soundness of $\Pi_{n,g}$

Remark In practice we may *not* need $\Pi_{n,g}$ (e.g. if G.par are validated by TTP). In this case **untraceability becomes *unconditional***.

Summary of Contributions and Conclusion

Untrusted GA Model for (Linkable) AH-AKE Protocols

- *stronger* model for security and privacy of AH-AKE protocols (than JKT08)
- distinction between *initially malicious* and *later corruptable* GAs
- definition of *untraceability* as an additional (individual) privacy goal of users

(Linkable) AH-AKE Protocol Resistant against Malicious GAs

- *extended Camenisch-Michels ZK proof* towards $\wedge \text{ord}(g) = 2p'q' \wedge -1 \notin \langle g \rangle$
- *blind registration* with *cryptographically protected pseudonyms* in AddUser
- moving to *signature-based confirmation* in JKT08 handshake
- similar *efficiency* as in the original JKT08 protocol (if we omit $\Pi_{n,g}$ in practice)

Thank you!