Practical Affiliation-Hiding Authentication from Improved Polynomial Interpolation

M. Manulis B. Poettering

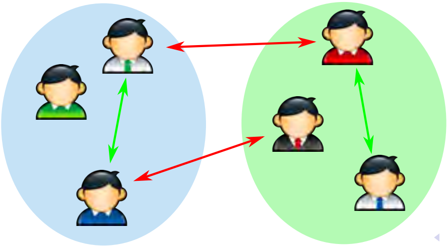
Cryptographic Protocols Group
TU Darmstadt & CASED (Germany)

ACM ASIACCS 2011

Affiliation-Hiding Authentication

Affiliation-Hiding Authentication (AHA) protocols . . .

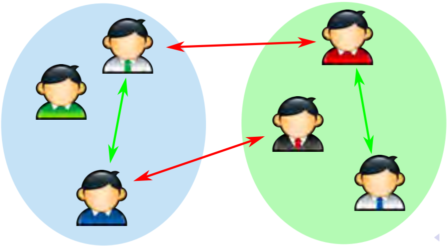
- are interactive two-party protocols
- offer authentication by affiliation to groups
- preserve users' privacy against group outsiders
  - members of the same group recognize each other
  - their affiliations do not leak to outsiders
- (optionally) output secure session keys



Affiliation-Hiding Authentication

Affiliation-Hiding Authentication (AHA) protocols . . .

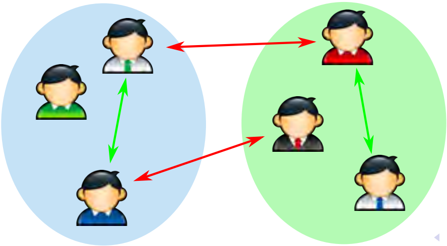
- are interactive two-party protocols
- offer authentication by affiliation to groups
- preserve users' privacy against group outsiders
  - members of the same group recognize each other
  - their affiliations do not leak to outsiders
- (optionally) output secure session keys



Affiliation-Hiding Authentication

Affiliation-Hiding Authentication (AHA) protocols . . .

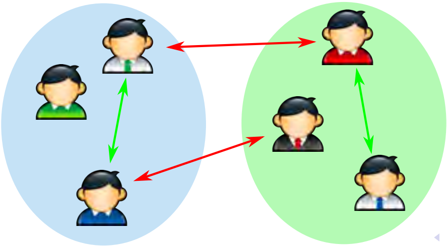
- are interactive two-party protocols
- offer authentication by affiliation to groups
- preserve users' privacy against group outsiders
  - members of the same group recognize each other
  - their affiliations do not leak to outsiders
- (optionally) output secure session keys



Affiliation-Hiding Authentication

Affiliation-Hiding Authentication (AHA) protocols . . .

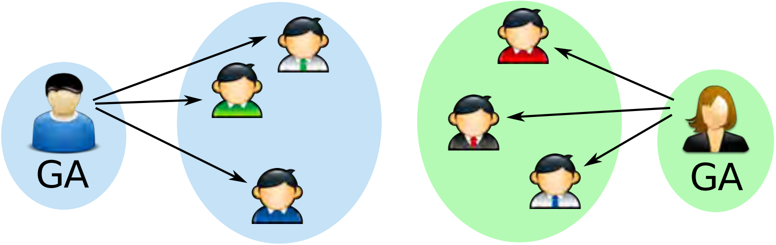
- are interactive two-party protocols
- offer authentication by affiliation to groups
- preserve users' privacy against group outsiders
  - members of the same group recognize each other
  - their affiliations do not leak to outsiders
- (optionally) output secure session keys



Group Management in AHA

Groups are managed by Group Authorities (GAs)

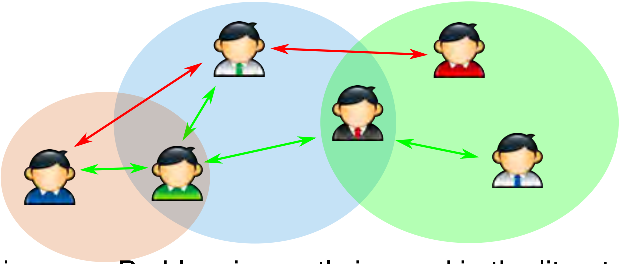
- users register with GAs
- users obtain membership credentials
- credentials are private input to later AHA invocations
- users can be revoked by GAs



Group Discovery

In case of multiple available groups ...

- AHA protocols should detect all groups in common (Group Discovery Problem [JKT08])
- authentication succeeds if intersection is non-empty



Group Discovery Problem is mostly ignored in the literature ...

Linkable vs. Unlinkable AHA

AHA protocols are either

- Unlinkable: it is impossible to recognize participants across different sessions
  - strong anonymity guarantees
  - challenging part: revocation of members

or

- Linkable: participants are recognized across different sessions
  - often use pseudonyms (transmitted in clear)
  - revocation handled via blacklisting of pseudonyms
  - typical application: social networks

Linkable vs. Unlinkable AHA

AHA protocols are either

- Unlinkable: it is impossible to recognize participants across different sessions
  - strong anonymity guarantees
  - challenging part: revocation of members

or

- Linkable: participants are recognized across different sessions
  - often use pseudonyms (transmitted in clear)
  - revocation handled via blacklisting of pseudonyms
  - typical application: social networks

Security Model for AHA

AHA protocols have two security goals:

- Affiliation-Hiding
  - simulation-based for single-affiliation schemes [JKT08]
  - game-based for multi-affiliation schemes [MPP10]
- AKE-security
  - secure key exchange with forward secrecy [JKT08]
  - [BR93,CK01]-like approach

History of Group Discovery

AHA milestones and Group Discovery:

- first single-affiliation AHA protocol in [BDS+03]
- first multi-affiliation solution in [JL08]
  - single secret key per user, disclosed to all GAs
- multi-affiliation solution in [MPP10]

No practical efficiency analysis done so far ...

Are AHA protocols
with Group Discovery
efficient in practice?

History of Group Discovery

AHA milestones and Group Discovery:

- first single-affiliation AHA protocol in [BDS+03]
- first multi-affiliation solution in [JL08]
  - single secret key per user, disclosed to all GAs
- multi-affiliation solution in [MPP10]

No practical efficiency analysis done so far . . .

Are AHA protocols with Group Discovery efficient in practice?

History of Group Discovery

AHA milestones and Group Discovery:

- first single-affiliation AHA protocol in [BDS+03]
- first multi-affiliation solution in [JL08]
  - single secret key per user, disclosed to all GAs
- multi-affiliation solution in [MPP10]

No practical efficiency analysis done so far …

Are AHA protocols with Group Discovery efficient in practice?

Overview of the AHA Protocol from [MPP10]

The AHA scheme by Manulis, Pinkas, Poettering (ACNS 10) . . .

- is linkable
- is RSA-based
- offers key establishment with forward secrecy
- implements group discovery
- $O(n)$ public key operations and $O(n^2)$ *cheap* operations
- builds on Okamoto-Tanaka key exchange [O87]
- is secure under safe RSA assumption in ROM

CASED CRYPTO

Okamoto-Tanaka Certified Key Agreement [O87]
(simplified)

CreateGroup

GA sets up SafeRSA parameters: (n, e, d) and $\langle g \rangle \subseteq \mathbb{Z}_n^*$

AddUser

User with $id \in \{0, 1\}^*$ receives credential $\sigma_{id} = H(id)^{-d} \bmod n$

Key Exchange

$\theta_A = g^{t_A} \sigma_{id_A} \bmod n$ $\xrightarrow{id_A, \theta_A}$ $\theta_B = g^{t_B} \sigma_{id_B} \bmod n$

$\xleftarrow{id_B, \theta_B}$

$K_A = ((\theta_B)^e H(id_B))^{t_A}$ $K_B = ((\theta_A)^e H(id_A))^{t_B}$

$$K_A = g^{e t_A t_B} = K_B$$

RevokeUser

Add user's *id* to public revocation list

CASED CRYP

AHA from Okamoto-Tanaka (OT)
The Motivation

Application of appropriate padding scheme to OT lets ...

- messages not reveal affiliations/groups
- messages look random in $\{0, \ldots, 2^L - 1\}$, for some L

This yields simple single-group AHA protocol with FS [JKT08].

Extending this idea to multi-group AHA [MPP10]:

- run several OT in parallel (one for each group)
- map groups to resp. OT-messages
- mapping should not reveal the groups/GAs
- [MPP10] introduces Index-Hiding Message Encoding

CASED CRYP

Application of appropriate padding scheme to OT lets ...

- messages not reveal affiliations/groups
- messages look random in $\{0, \ldots, 2^L - 1\}$, for some L

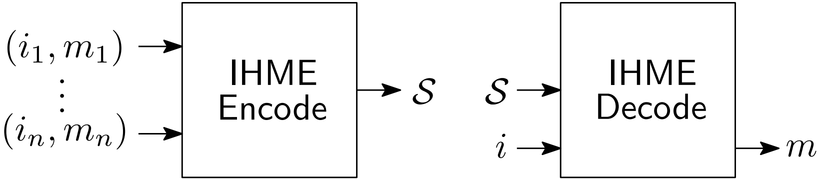
This yields simple single-group AHA protocol with FS [JKT08].

Extending this idea to multi-group AHA [MPP10]:

- run several OT in parallel (one for each group)
- map groups to resp. OT-messages
- mapping should not reveal the groups/GAs
- [MPP10] introduces Index-Hiding Message Encoding

Constructing IHME [MPP10]

Input: Indices $i_1, \ldots, i_n \in \mathcal{I}$, messages $m_1, \ldots, m_n \in \mathcal{M}$
Output: IHME structure $\mathcal{S}$

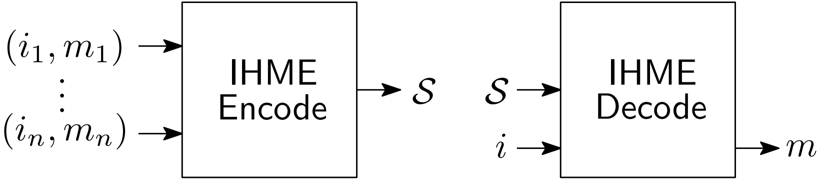


Construction via Polynomial Interpolation in Finite Fields:

- Let $\mathcal{I} = \mathcal{M} = \mathbb{F}$ for finite field $\mathbb{F}$
- Consider $(i_1, m_1), \ldots, (i_n, m_n) \in \mathbb{A}(\mathbb{F}) = \mathbb{F}^2$
- Let $\mathcal{S}$ be list of coefficients of interpolation polynomial
- Index-Hiding (for random messages)

Constructing IHME [MPP10]

Input: Indices $i_1, \ldots, i_n \in \mathcal{I}$, messages $m_1, \ldots, m_n \in \mathcal{M}$
Output: IHME structure $\mathcal{S}$



Construction via Polynomial Interpolation in Finite Fields:

- Let $\mathcal{I} = \mathcal{M} = \mathbb{F}$ for finite field $\mathbb{F}$
- Consider $(i_1, m_1), \ldots, (i_n, m_n) \in \mathbb{A}(\mathbb{F}) = \mathbb{F}^2$
- Let $\mathcal{S}$ be list of coefficients of interpolation polynomial
- Index-Hiding (for random messages)

CASED CRYP

We improve Efficiency of IHME

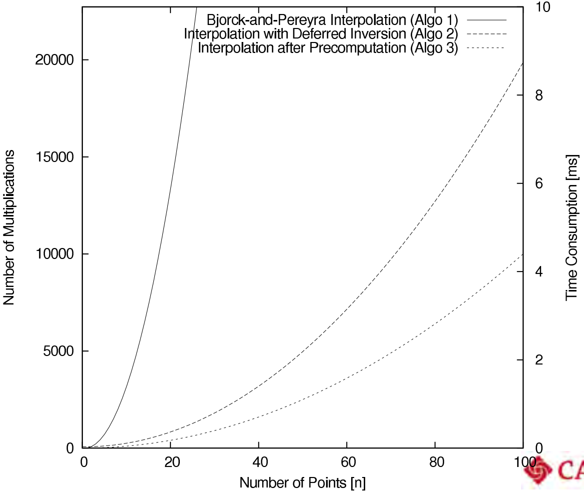
Contribution: Improving Polynomial Interpolation in Finite Fields

Björck & Pereyra (1970)	$\frac{n(n-1)}{2}(D+M)$
Deferred Inversion	$\left(\frac{5n(n-1)}{2}+1\right)M+1I$
with Precomputation	n^2M

M: Multiplication D: Division I: Inversion

IHME Implementation in Practice
(on Intel XEON 2.66GHz, for $|\mathbb{F}| = 2^{80}$)

Efficiency measurements for IHME:



Example with two users:

- Alice has credentials $\sigma_{A,2}, \sigma_{A,3}$ for groups 2 and 3
- Bob has credentials $\sigma_{B,3}, \sigma_{B,8}$ for groups 3 and 8

Multi-affiliation AHA Handshake using IHME:

Alice:

$$\theta_{A,2} = g^{t_2}\sigma_{A,2}$$
$$\theta_{A,3} = g^{t_3}\sigma_{A,3}$$
$$\mathcal{S}_A = \text{IHME\_Enc}(\{2 : \theta_{A,2}, 3 : \theta_{A,3}\})$$

Bob:

$$\theta_{B,3} = g^{t_3}\sigma_{B,3}$$
$$\theta_{B,8} = g^{t_8}\sigma_{B,8}$$
$$\mathcal{S}_B = \text{IHME\_Enc}(\{3 : \theta_{B,3}, 8 : \theta_{B,8}\})$$

Alice → Bob: $id_A, \mathcal{S}_A$

Bob → Alice: $id_B, \mathcal{S}_B$

Alice:

$$\theta_{B,2} = \text{IHME\_Dec}(\mathcal{S}_B, 2)$$
$$\theta_{B,3} = \text{IHME\_Dec}(\mathcal{S}_B, 3)$$
$$K_{A,2} = (\theta_{B,2} \ldots)$$
$$K_{A,3} = (\theta_{B,3} \ldots)$$

Bob:

$$\theta_{A,3} = \text{IHME\_Dec}(\mathcal{S}_A, 3)$$
$$\theta_{A,8} = \text{IHME\_Dec}(\mathcal{S}_A, 8)$$
$$K_{B,3} = (\theta_{A,3} \ldots)$$
$$K_{B,8} = (\theta_{A,8} \ldots)$$

Alice ↔ Bob: key confirmation

We introduce Interleaved IHME

Contribution: We improve IHME scheme from [MPP10]

Idea:

- in [MPP10]'s IHME: $\mathcal{I} = \mathcal{M} = \mathbb{F}$ where $|\mathbb{F}| = 2^L$
- suppose $L = L_1 \cdot L_2$
- consider $\mathcal{M} \simeq (\mathbb{F}')^{L_1}$ where $|\mathbb{F}'| = 2^{L_2}$
- that is $m = (m^1, \ldots, m^{L_1})$ where $m^i \in \{0, \ldots, 2^{L_2} - 1\}$
- encode component-wise

Advantage:

- switch from large field $\mathbb{F}$ to small field $\mathbb{F}'$
- arithmetic operations in small field are much faster
- caveat: will now need L_1 many encodings

CASED CRYPTO

We introduce Interleaved IHME

Contribution: We improve IHME scheme from [MPP10]

Idea:

- in [MPP10]'s IHME: $\mathcal{I} = \mathcal{M} = \mathbb{F}$ where $|\mathbb{F}| = 2^L$
- suppose $L = L_1 \cdot L_2$
- consider $\mathcal{M} \simeq (\mathbb{F}')^{L_1}$ where $|\mathbb{F}'| = 2^{L_2}$
- that is $m = (m^1, \dots, m^{L_1})$ where $m^i \in \{0, \dots, 2^{L_2} - 1\}$
- encode component-wise

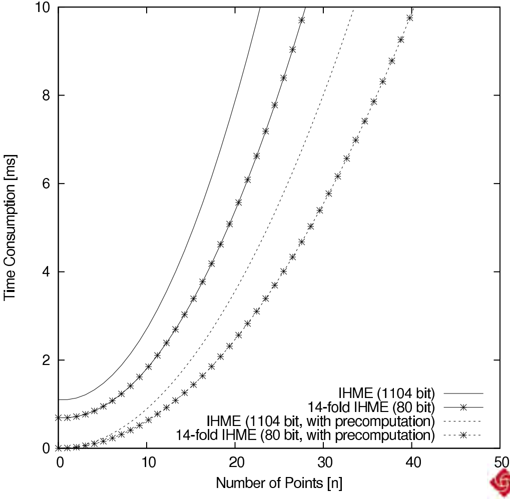
Advantage:

- switch from large field $\mathbb{F}$ to small field $\mathbb{F}'$
- arithmetic operations in small field are much faster
- caveat: will now need L_1 many encodings

CASED CRYP

Interleaved IHME outperforms [MPP10] IHME by 30%

Typical values: $L = 1120 = 14 \cdot 80 = L_1 \cdot L_2$



CASED CRYPTO

AHA with Interleaved IHME

Multi-affiliation AHA with IHME from [MPP10]

$\mathcal{S}_A = \text{IHME\_Enc}(\{2 : \theta_{A,2}, 3 : \theta_{A,3}\})$ $\quad\quad$ $\mathcal{S}_B = \text{IHME\_Enc}(\{3 : \theta_{B,3}, 8 : \theta_{B,8}\})$

$\xrightarrow{id_A, \mathcal{S}_A}$

$\xleftarrow{id_B, \mathcal{S}_B}$

$\theta_{B,2} = \text{IHME\_Dec}(\mathcal{S}_B, 2)$ $\quad\quad$ $\theta_{A,3} = \text{IHME\_Dec}(\mathcal{S}_A, 3)$
$\theta_{B,3} = \text{IHME\_Dec}(\mathcal{S}_B, 3)$ $\quad\quad$ $\theta_{A,8} = \text{IHME\_Dec}(\mathcal{S}_A, 8)$

Multi-affiliation AHA with Interleaved IHME

$\mathcal{S}_A = \overline{\text{IHME\_Enc}}(\{2 : \theta_{A,2}, 3 : \theta_{A,3}\})$ $\quad\quad$ $\mathcal{S}_B = \overline{\text{IHME\_Enc}}(\{3 : \theta_{B,3}, 8 : \theta_{B,8}\})$

$\xrightarrow{id_A, \mathcal{S}_A}$

$\xleftarrow{id_B, \mathcal{S}_B}$

$\theta_{B,2} = \overline{\text{IHME\_Dec}}(\mathcal{S}_B, 2)$ $\quad\quad$ $\theta_{A,3} = \overline{\text{IHME\_Dec}}(\mathcal{S}_A, 3)$
$\theta_{B,3} = \overline{\text{IHME\_Dec}}(\mathcal{S}_B, 3)$ $\quad\quad$ $\theta_{A,8} = \overline{\text{IHME\_Dec}}(\mathcal{S}_A, 8)$

Further Protocol Improvements

In CreateGroup

- choose $N = pq$ with $p = 11 \bmod 24$ and $q = 23 \bmod 24$
- guarantees that $g = 2$ is appropriate generator
- leads to compact public group keys (just N)

In AddUser

- change credential from $\sigma_{id} = H(id)^{d}$ to $\sigma_{id} = H(id)^{-d}$
- saves one division per session
- use CRT decomposition to speed up exponentiation

Further Protocol Improvements (cont.)

In Handshake

- deployment of Interleaved IHME
- shorter confirmation messages (from 1024 to 80 bits)
- simpler session key derivation (no need to sort groups)
  - XORing together group-wise keys
- faster exponentiation (small exponents, fixed basis)

The New AHA Protocol in Practice
(1024 bit RSA, 80 bit symmetric security, Intel XEON 2.66GHz)

Timing of full protocol run with *n* groups per user and session:

Without precomputation

n	10	50	100	250
total (ms)	29	188	492	2096
expos (ms)	26 (90%)	131 (69%)	263 (53%)	657 (31%)
IHME (ms)	2.8 (9%)	57 (30%)	229 (46%)	1438 (68%)

With precomputation

n	10	50	100	250
total (ms)	27	164	394	1480
expos (ms)	26 (95%)	131 (80%)	263 (66%)	657 (44%)
IHME (ms)	1.2 (4%)	32 (19%)	131 (33%)	823 (55%)

CASED CRYP

Conclusion

Are AHA protocols
with Group Discovery
efficient in practice?

YES!

Conclusion

Are AHA protocols
with Group Discovery
efficient in practice?

YES!

Further Reading

- [BDS+03]: Balfanz, Durfee, Shankar et al.
  Secret Handshakes from Pairing-Based Key Agreements
  IEEE S&P 2003
- [JKT08]: Jarecki, Kim, Tsudik
  Beyond Secret Handshakes: Affiliation-Hiding Authenticated Key Exchange.
  CT-RSA 2008
- [JL08]: Jarecki, Liu
  Affiliation-Hiding Envelope and Authentication Schemes with Efficient Support for Multiple Credentials
  ICALP 2008 (2)

CASED CRYPTO

Further Reading (cont.)

- [MPP10]: Manulis, Pinkas, Poettering
  Privacy-Preserving Group Discovery with Linear Complexity
  ACNS 2010
- [O87]: Okamoto
  Key Distribution Systems Based on Identification Information
  CRYPTO 1987

CASED CRYPTO