A New Approach To Efficient Revocable Attribute-Based Anonymous Credentials

David Derler, Christian Hanser, and Daniel Slamanig,
IAIK, Graz University of Technology, Austria

December 15, 2015

Supported by EU H2020 Project prisma cloud

Outline

1. Introduction
2. Novel ABC Paradigm [HS14]
3. Novel Revocation Approach
   - Security Model
   - Constructions
4. Conclusion

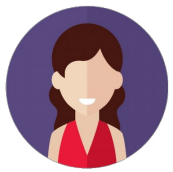
Outline

1. Introduction
2. Novel ABC Paradigm [HS14]
3. Novel Revocation Approach
   - Security Model
   - Constructions
4. Conclusion

Attribute-Based Anonymous Credentials (ABCs)

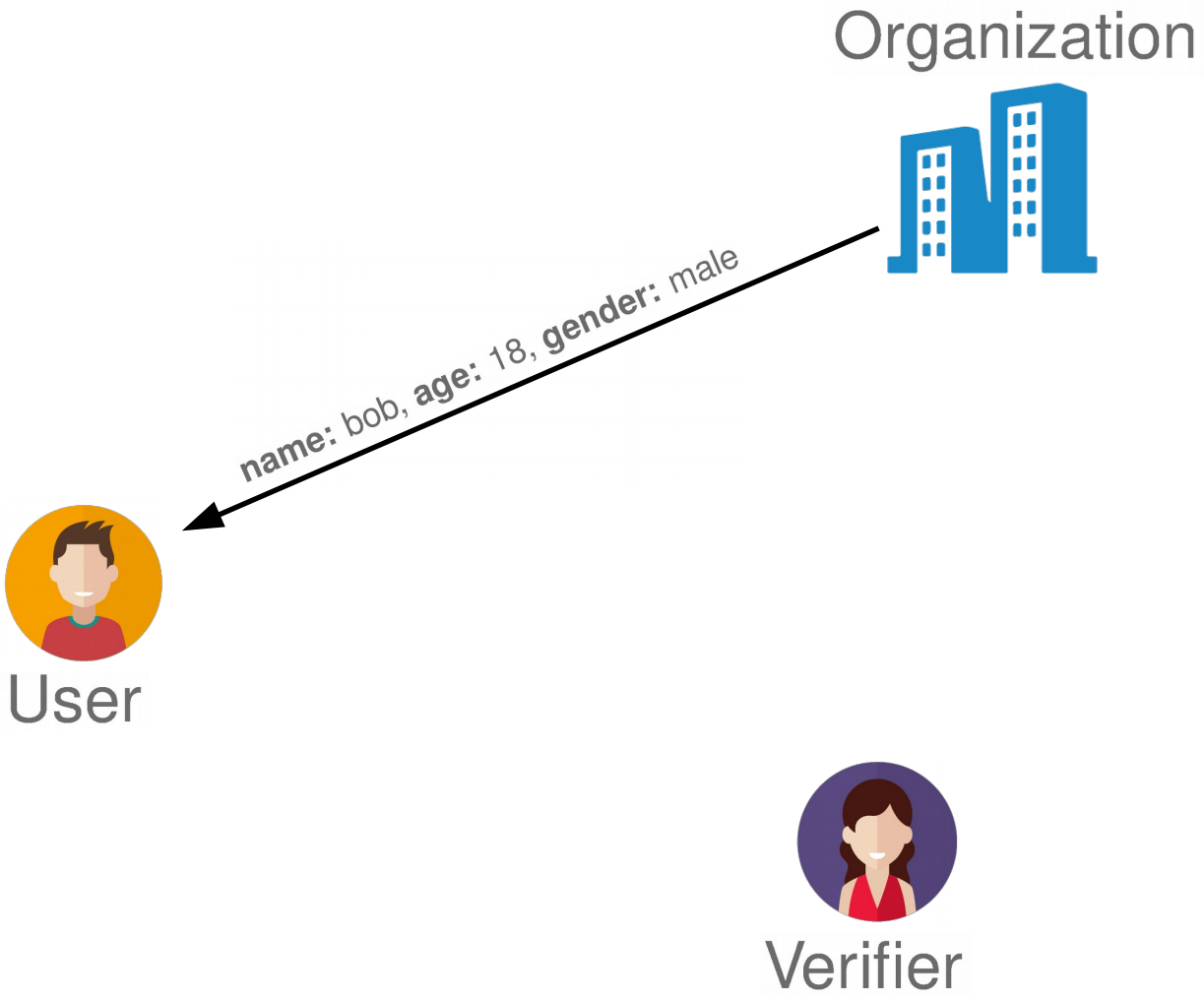
Organization

User

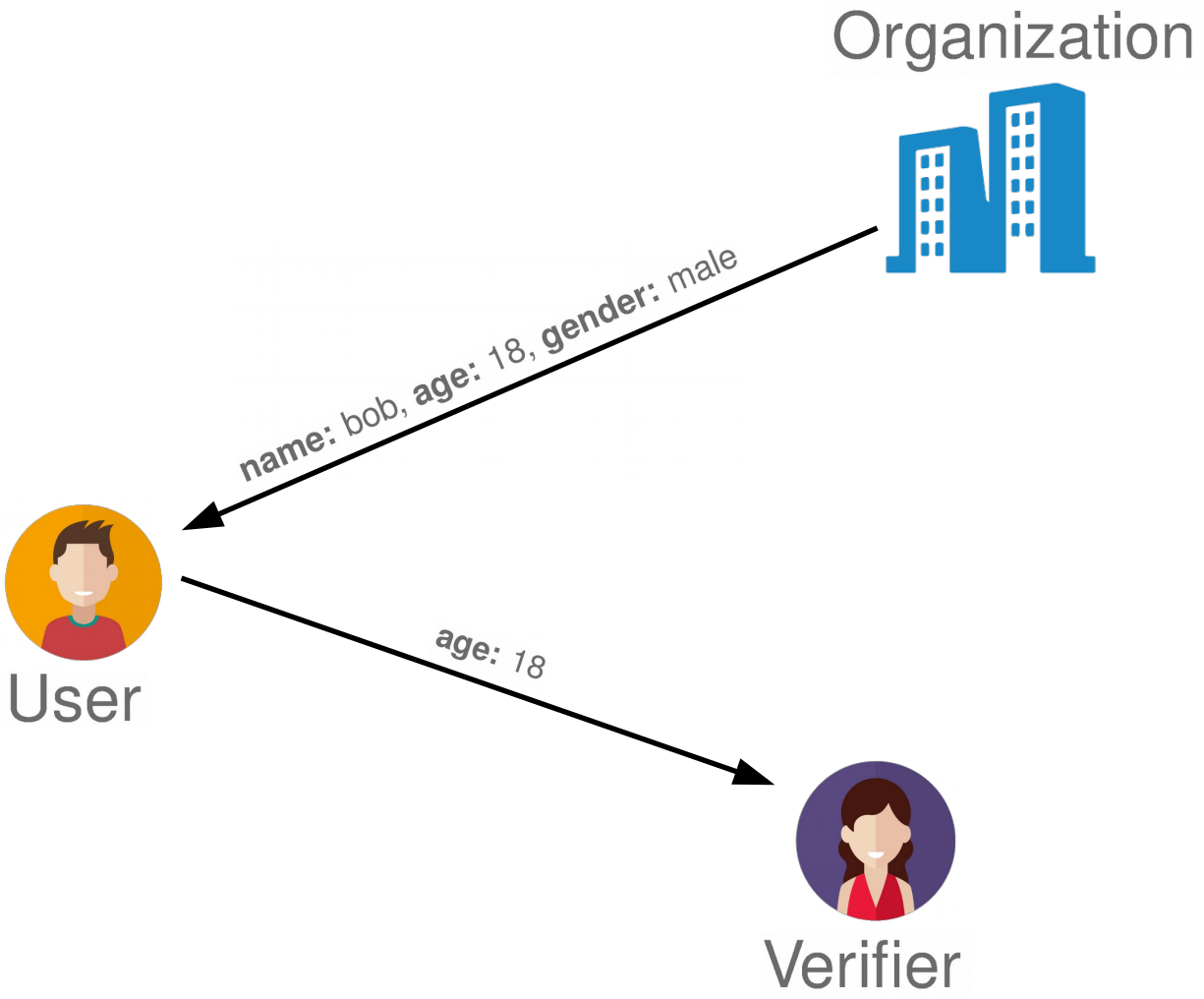


Verifier

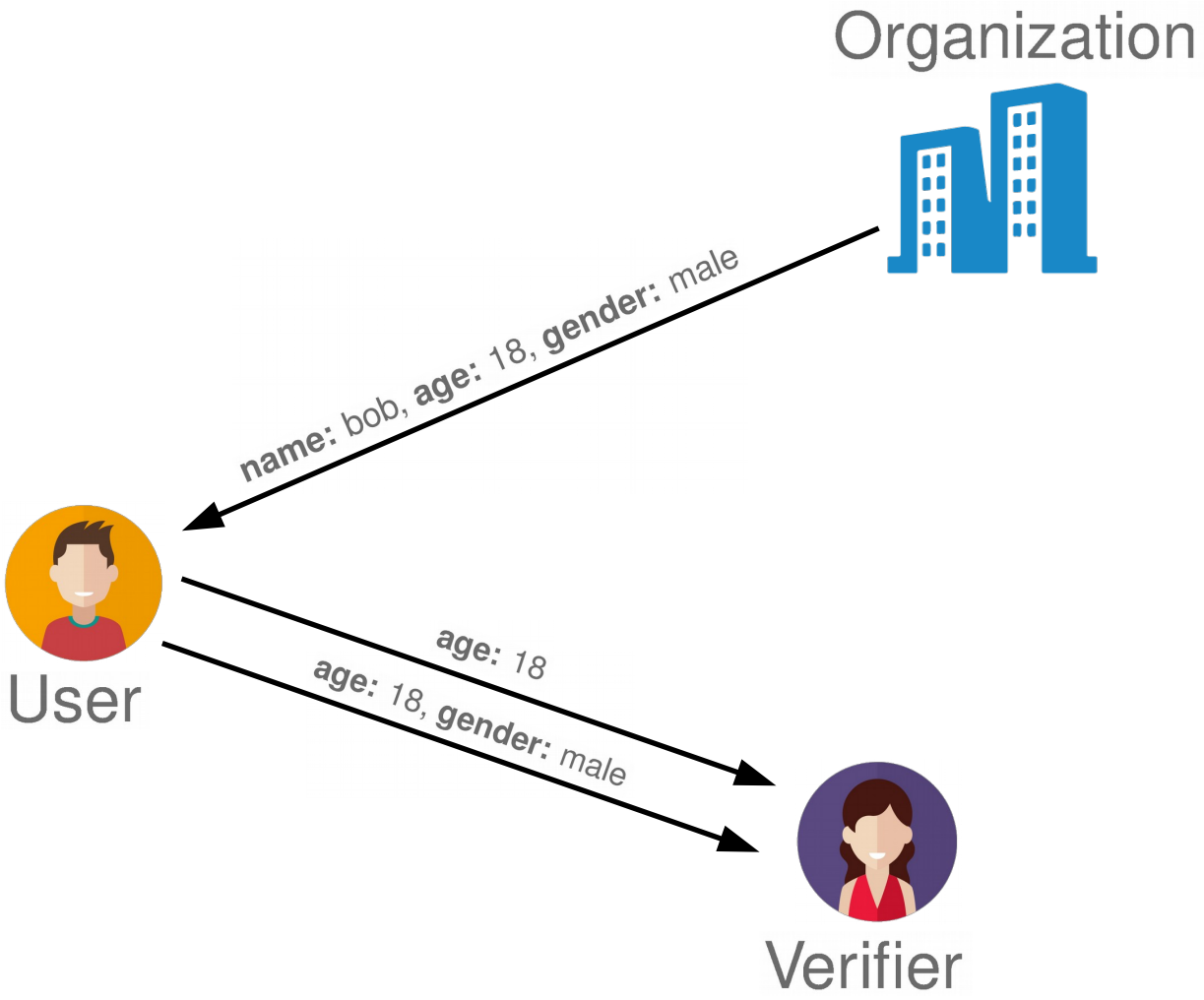
Attribute-Based Anonymous Credentials (ABCs)



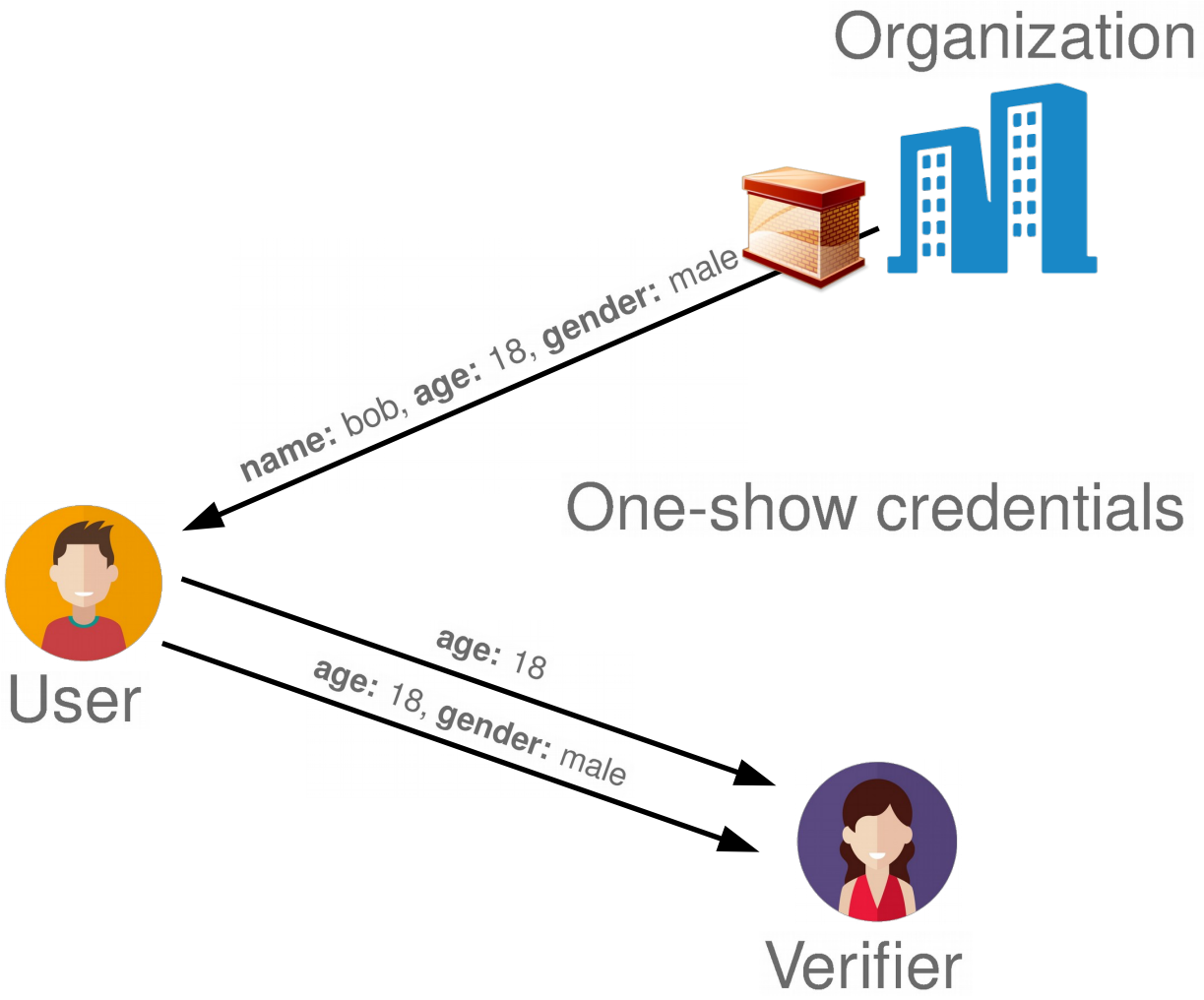
Attribute-Based Anonymous Credentials (ABCs)



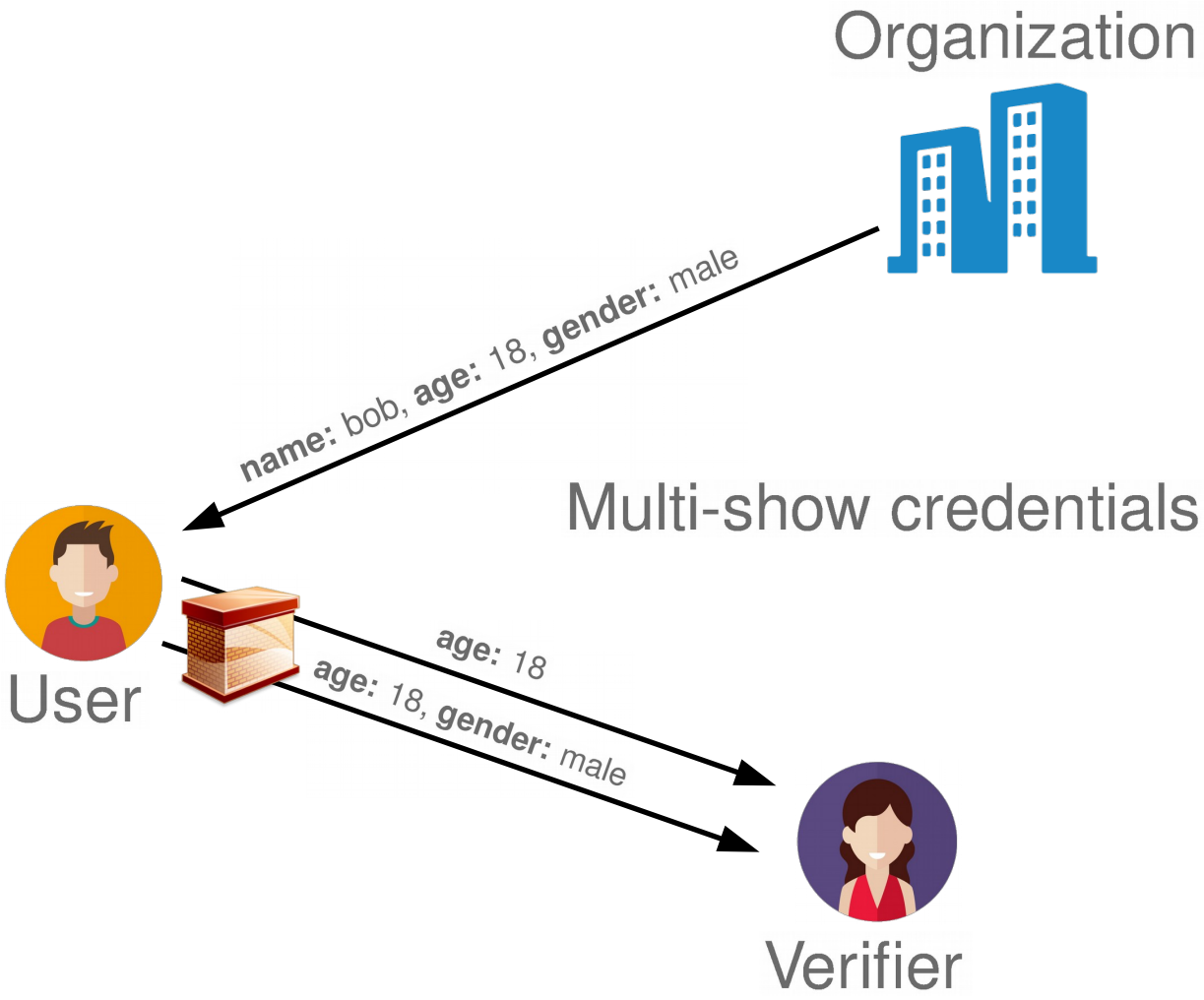
Attribute-Based Anonymous Credentials (ABCs)



Attribute-Based Anonymous Credentials (ABCs)



Attribute-Based Anonymous Credentials (ABCs)



Attribute-Based Anonymous Credentials (ABCs)

Work in the field is wide

- Most prominent: IBM's Idemix, Microsoft's U-Prove

Attribute-Based Anonymous Credentials (ABCs)

Work in the field is wide

- Most prominent: IBM's Idemix, Microsoft's U-Prove

Novel approach to multi-show ABCs [HS14]

- **S**tructure **P**reserving **S**ignatures on **E**quivalence **C**lasses
  - (**SPS-EQ**)
- Interesting properties
  - $O(1)$ size of creds and $O(1)$ communication
  - No PoK for unrevealed attributes
  - Only single $O(1)$ PoK for freshness

Motivation

Revocation: important feature in practice

Question

Revocation mechanism

- Following similar principles
- Preserving the nice asymptotic properties

Contribution

Accumulator-based blacklist revocation for [HS14]

Contribution

Accumulator-based blacklist revocation for [HS14]

(1) Following similar principles as underlying ABC

Contribution

Accumulator-based blacklist revocation for [HS14]

(1) Following similar principles as underlying ABC

(2) Port revocation mechanism from U-Prove

Contribution

Accumulator-based blacklist revocation for [HS14]

(1) Following similar principles as underlying ABC

(2) Port revocation mechanism from U-Prove

Revocation typically considered as an add-on

- Extend model of [HS14]
- Prove security of both approaches in this model

Contribution

Accumulator-based blacklist revocation for [HS14]

(1) Following similar principles as underlying ABC

(2) Port revocation mechanism from U-Prove

Revocation typically considered as an add-on

- Extend model of [HS14]
- Prove security of both approaches in this model

Comparison of both approaches

Preliminaries

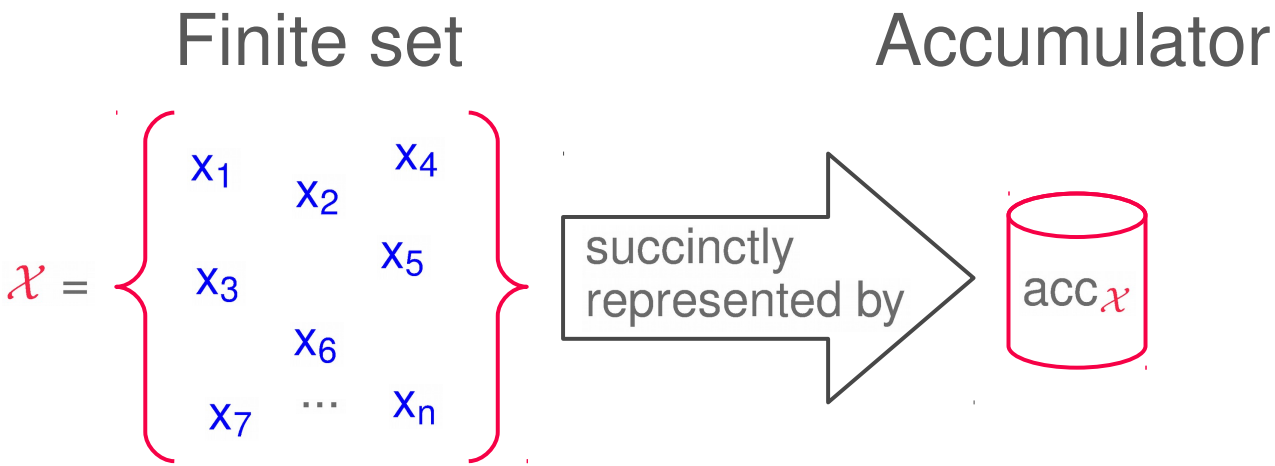
Asymmetric bilinear map (pairing)

- $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = p$
- $e(aP, b\hat{P}) = e(P, \hat{P})^{ab}$ (Bilinearity)
- $e(P, \hat{P}) \neq 1_{\mathbb{G}_T}$ (Non-degeneracy)
- $e(\cdot, \cdot)$ efficiently computable (Efficiency)

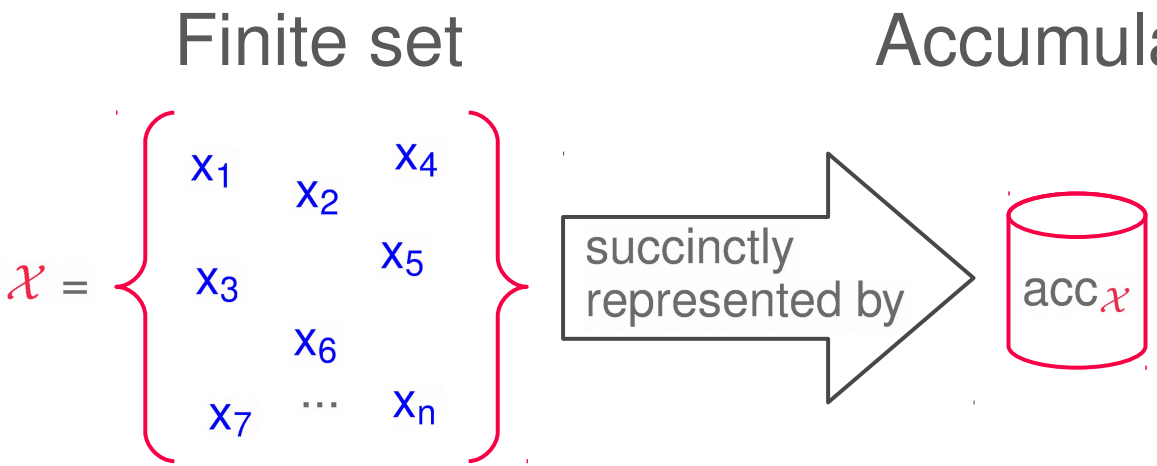
SXDH setting

$\Rightarrow$ DDH assumed to hold in $\mathbb{G}_1$ and $\mathbb{G}_2$

Cryptographic Accumulators



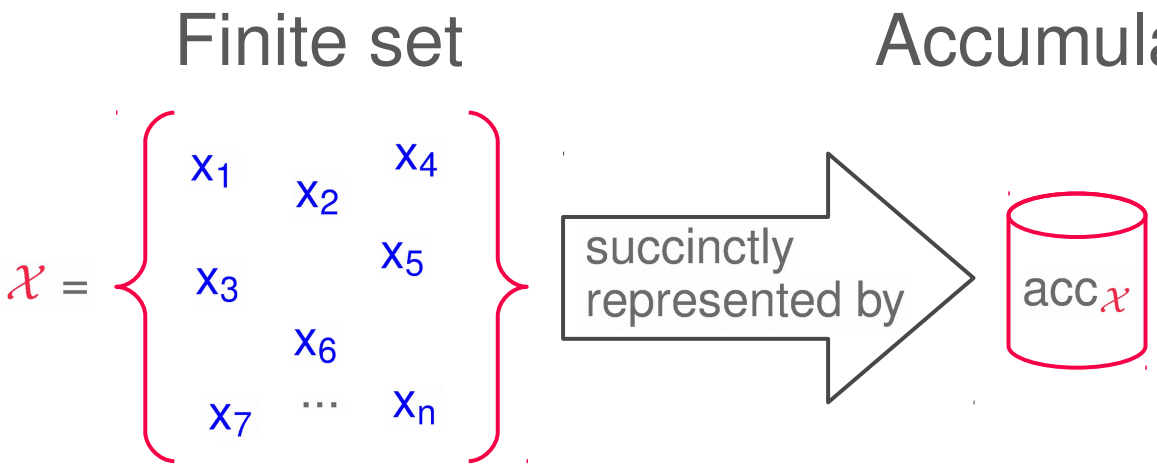
Cryptographic Accumulators



Witnesses wit$_x$ certifying membership of x in acc$_{\mathcal{X}}$

- Efficiently computable $\forall\ x \in \mathcal{X}$
- Intractable $\forall\ x \notin \mathcal{X}$

Cryptographic Accumulators



Witnesses wit$_x$ certifying membership of x in acc$_{\mathcal{X}}$

- Efficiently computable $\forall\ x \in \mathcal{X}$
- Intractable $\forall\ x \notin \mathcal{X}$

$\Rightarrow$ **Collision freeness**

Outline

1. Introduction
2. Novel ABC Paradigm [HS14]
3. Novel Revocation Approach
   - Security Model
   - Constructions
4. Conclusion

Structure Preserving Signatures [AFG+10]

Sign group element vectors

$\Rightarrow$ Sigs and PKs only consist of group elements

Verification solely via

- Pairing-product equations
- Group membership tests

Signing Equivalence Classes [HS14]

Partition $\mathbb{G}_i^\ell$ into projective equivalence classes

$$M \in \mathbb{G}_i^\ell \sim_{\mathcal{R}} N \in \mathbb{G}_i^\ell \Leftrightarrow \exists k \in \mathbb{Z}_p^* : N = k \cdot M$$

SPS-EQ

- Given σ on M
- Publicly derive σ' on $M' \in [M]_{\mathcal{R}}$

$\Rightarrow$ IND of classes under DDH in $\mathbb{G}_i$

Signing Equivalence Classes [HS14] II

Security properties

- Correctness
- EUF-CMA security (w.r.t. equivalence classes)
- Perfect adaption of signatures
  - (M', σ') obtained by re-randomizing (M, σ)
  - Indistinguishable from fresh signature on M'

Novel ABC Paradigm [HS14]

Credential

- SPS-EQ signed commitment representing attribute set
- Commitment compatible with re-randomization
- **No** PoK of unrevealed attributes required

Novel ABC Paradigm [HS14]

Credential

- SPS-EQ signed commitment representing attribute set
- Commitment compatible with re-randomization
- **No** PoK of unrevealed attributes required

Showing

- Re-randomize signature and commitment
- Provide witness for revealed attributes
  - Unrevealed attributes hidden in witness

Novel ABC Paradigm [HS14]

Credential

- SPS-EQ signed commitment representing attribute set
- Commitment compatible with re-randomization
- **No** PoK of unrevealed attributes required

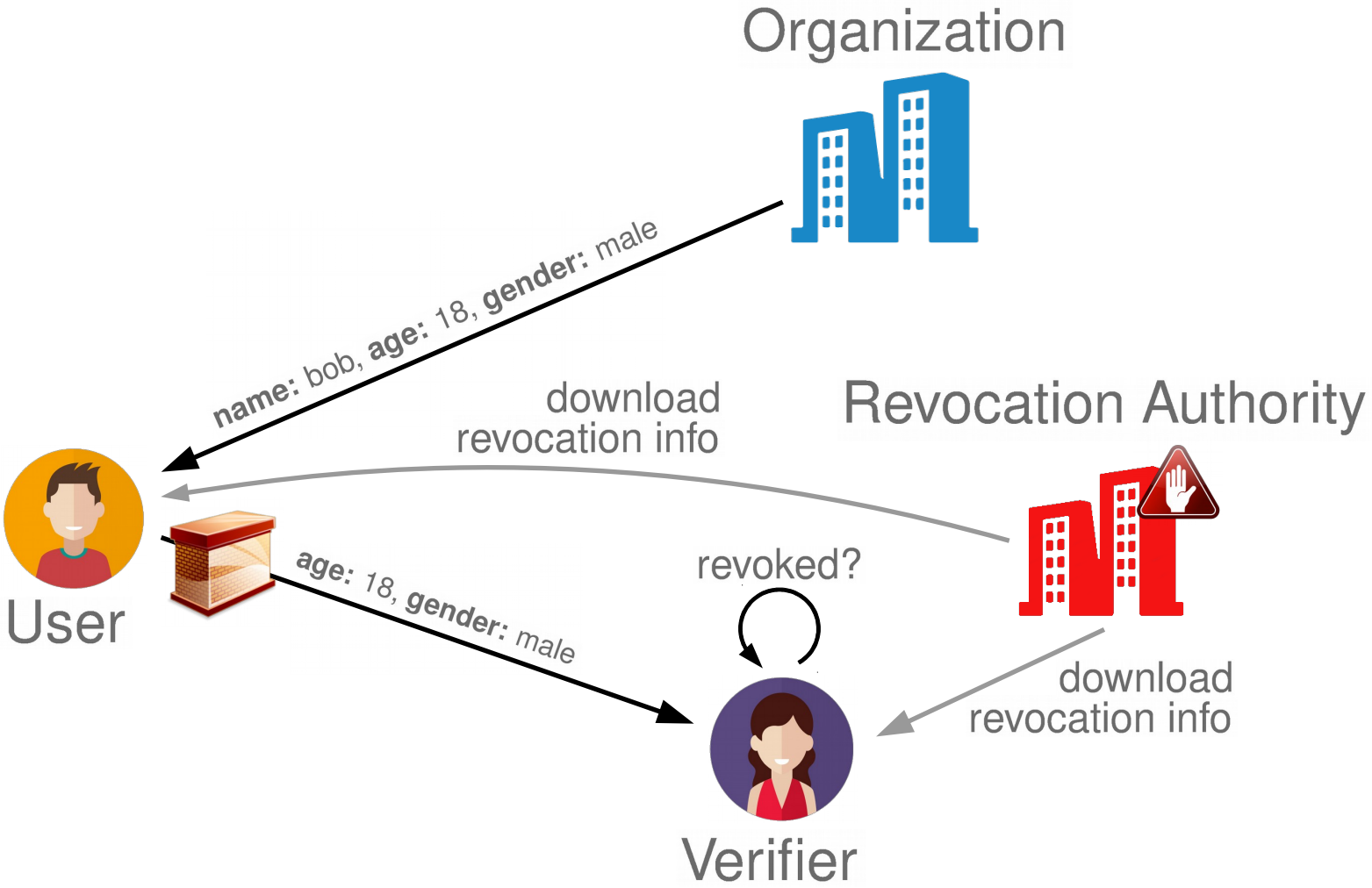
Showing

- Re-randomize signature and commitment
- Provide witness for revealed attributes
  - Unrevealed attributes hidden in witness
- Single $O(1)$ PoK

Outline

1. Introduction
2. Novel ABC Paradigm [HS14]
3. Novel Revocation Approach
   - Security Model
   - Constructions
4. Conclusion

Revokable ABCs



Revokable ABCs - Security Model I

Correctness: everything works if honestly computed

Revokable ABCs - Security Model I

Correctness: everything works if honestly computed

Unforgeability:

- No showings for **non-issued** creds

Revokable ABCs - Security Model I

Correctness: everything works if honestly computed

Unforgeability:

- No showings for **non-issued** creds
- No showings for **invalid** attribute sets

Revokable ABCs - Security Model I

Correctness: everything works if honestly computed

Unforgeability:

- No showings for **non-issued** creds
- No showings for **invalid** attribute sets
- No showings for **revoked** creds

Revokable ABCs - Security Model I

Correctness: everything works if honestly computed

Unforgeability:

- No showings for **non-issued** creds
- No showings for **invalid** attribute sets
- No showings for **revoked** creds
- No **replays**

Revokable ABCs - Security Model I

Correctness: everything works if honestly computed

Unforgeability:

- No showings for **non-issued** creds
- No showings for **invalid** attribute sets
- No showings for **revoked** creds
- No **replays**

$\Rightarrow$ Adversary:

  - Can corrupt users, obtain secret keys of users, revoke users
  - Acts as dishonest user

Revokable ABCs - Security Model II

Anonymity:

- Showing hides **identity** of
  - Honest, non-corrupted users

Revokable ABCs - Security Model II

Anonymity:

- Showing hides **identity** of
  - Honest, non-corrupted users
- **Backward** unlinkability
  - Revocation does not endanger privacy
  - (Previous showings unlinkable)

Revokable ABCs - Security Model II

Anonymity:

- Showing hides **identity** of
  - Honest, non-corrupted users
- **Backward** unlinkability
  - Revocation does not endanger privacy
  - (Previous showings unlinkable)

$\Rightarrow$ Adversary:

- Can corrupt users, obtain secret keys of users, revoke users
- Acts as dishonest organization

Novel Revocation Approach

Idea:

- Choose accumulator s.t. compatible with re-randomization

Construction (sketch):

- Incorporate **nym** as credential component
- Accumulator contains all revoked *nym*s

Novel Revocation Approach

Idea:

- Choose accumulator s.t. compatible with re-randomization

Construction (sketch):

- Incorporate **nym** as credential component
- Accumulator contains all revoked *nym*s
- **Showing**
  - Consistently randomize accumulator/witnesses
  - Plug-in randomized **nym** into verification relation

Novel Revocation Approach

Idea:

- Choose accumulator s.t. compatible with re-randomization

Construction (sketch):

- Incorporate **nym** as credential component
- Accumulator contains all revoked *nym*s
- **Showing**
  - Consistently randomize accumulator/witnesses
  - Plug-in randomized **nym** into verification relation
  - \+ Simple $O(1)$ PoK for technical reasons

Security

Unforgeability

- ≈ Unforgeability of underlying ABC
- \+ Case for collision freeness of accu
- \+ Some technicalities regarding extraction
  - 3 additional DLOG proofs

Security

Unforgeability

- ≈ Unforgeability of underlying ABC
- \+ Case for collision freeness of accu
- \+ Some technicalities regarding extraction
  - 3 additional DLOG proofs

Anonymity

- Components depending on the challenge bit
  - Indistinguishable from random

Security II

Anonymity contd'

- Indistinguishability shown under
  - Perfect adaption of signatures
  - DDH in $\mathbb{G}_1$
  - 2 DDH-like assumptions in SXDH setting

Security II

Anonymity contd'

- Indistinguishability shown under
  - Perfect adaption of signatures
  - DDH in $\mathbb{G}_1$
  - 2 DDH-like assumptions in SXDH setting

DDH-like assumptions

- 1 holds in GGM
- 1 follows from (R, S, T, f)-DDH [Boy08]

U-Prove Based Revocation Approach

Follow classical revocation approach

- Adapt U-Prove revocation [ACN13, NP14]

U-Prove Based Revocation Approach

Follow classical revocation approach

- Adapt U-Prove revocation [ACN13, NP14]

Construction (sketch):

- Incorporate **nym** in credentials
- Accumulator contains revoked *nyms*

U-Prove Based Revocation Approach

Follow classical revocation approach

- Adapt U-Prove revocation [ACN13, NP14]

Construction (sketch):

- Incorporate **nym** in credentials
- Accumulator contains revoked *nyms*
- PoK of non-membership witness and **nym**
- PoK that **nym** coincides with **nym** in credential

Security

Unforgeability

- ≈ Unforgeability of underlying ABC
- \+ Additional case for collision freeness of accu
- \+ Some technicalities regarding extraction

Anonymity

- Components depending on the challenge bit
  - Indistinguishable from random

Security

Unforgeability

- $\approx$ Unforgeability of underlying ABC
- \+ Additional case for collision freeness of accu
- \+ Some technicalities regarding extraction

Anonymity

- Components depending on the challenge bit
  - Indistinguishable from random
  - Shown under DDH in $\mathbb{G}_1$
  - ... and perfect adaption of signatures

Comparison

Comparison based on [UW14]

- BN implementation on ARM-Cortex-M0+

Obtain:

- Novel Approach: +15 $\mathbb{G}_1$ equivalents
- Classic Approach: +14 $\mathbb{G}_1$ equivalents

Comparison

Comparison based on [UW14]

- BN implementation on ARM-Cortex-M0+

Obtain:

- Novel Approach: +15 $\mathbb{G}_1$ equivalents
- Classic Approach: +14 $\mathbb{G}_1$ equivalents

Show:

- Novel Approach: +20 $\mathbb{G}_1$ equivalents
- Classic Approach: +33 $\mathbb{G}_1$ equivalents

$\Rightarrow$ worst case (best case: even 2 $\times$ faster)

Outline

1. Introduction
2. Novel ABC Paradigm [HS14]
3. Novel Revocation Approach
   - Security Model
   - Constructions
4. Conclusion

Conclusions

New conceptually simple approach

- Easy to comprehend
- Easy to implement

$\Rightarrow$ New direction in revocation for ABC systems

Conclusions

New conceptually simple approach

- Easy to comprehend
- Easy to implement

$\Rightarrow$ New direction in revocation for ABC systems

Performance

- Both approaches practically efficient
- Novel approach yields more efficient showings

Thank you.

david.derler@iaik.tugraz.at

Supported by prisma cloud

References I

[ACN13] Tolga Acar, Sherman S. M. Chow, and Lan Nguyen. Accumulators and U-Prove Revocation. In *Financial Cryptography*, LNCS. 2013.

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-Preserving Signatures and Commitments to Group Elements. In *CRYPTO*, LNCS. Springer, 2010.

[Boy08] Xavier Boyen. The Uber-Assumption Family – A Unified Complexity Framework for Bilinear Groups. In *PAIRING*, LNCS. Springer, 2008.

[HS14] Christian Hanser and Daniel Slamanig. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In *ASIACRYPT*, 2014.

[NP14] Lan Nguyen and Christian Paquin. U-Prove Designated-Verifier Accumulator Revocation Extension. Technical report, Microsoft Research, 2014.

[UW14] Thomas Unterluggauer and Erich Wenger. Efficient Pairings and ECC for Embedded Systems. In *CHES*, LNCS. Springer, 2014.