Multi-Holder Anonymous Credentials from BBS Signatures

Andrea Flamini

Politecnico di Torino

↑

UNIVERSITÀ DI TRENTO

Eysa Lee

BARNARD

↑

BROWN

Anna Lysyanskaya

BROWN

Anonymous Credentials (ACs)[Cha83, CL01]

Privacy preserving digital credentials whose authorship can be cryptographically verified

Anonymous Credentials (ACs)[Cha83, CL01]

Privacy preserving digital credentials whose authorship can be cryptographically verified

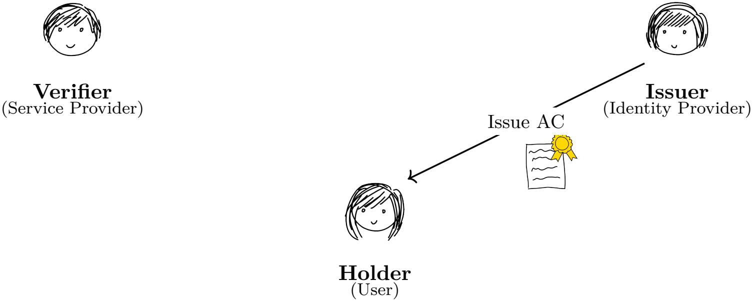
Verifier
(Service Provider)

Issuer
(Identity Provider)

Holder
(User)

Anonymous Credentials (ACs)[Cha83, CL01]

Privacy preserving digital credentials whose authorship can be cryptographically verified



Verifier
(Service Provider)

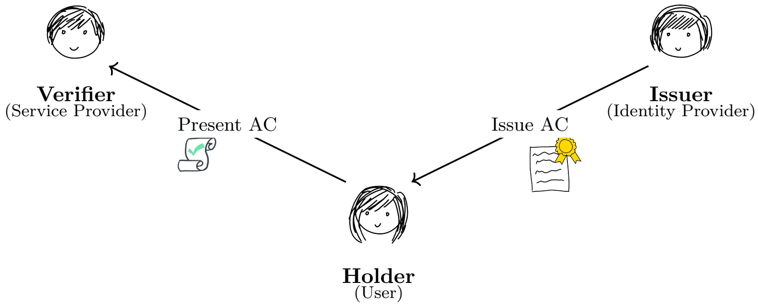
Issuer
(Identity Provider)

Issue AC

Holder
(User)

Anonymous Credentials (ACs)[Cha83, CL01]

Privacy preserving digital credentials whose authorship can be cryptographically verified



Verifier
(Service Provider)

Issuer
(Identity Provider)

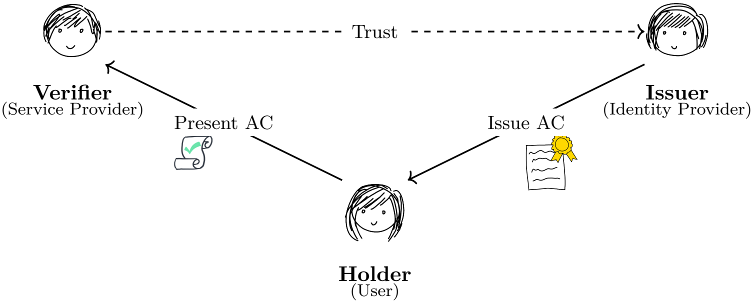
Present AC

Issue AC

Holder
(User)

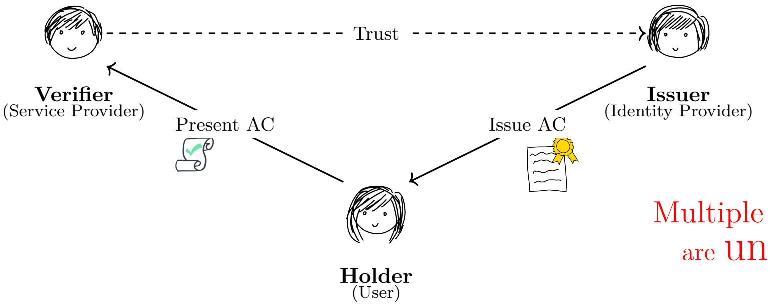
Anonymous Credentials (ACs)[Cha83, CL01]

Privacy preserving digital credentials whose authorship can be cryptographically verified



Anonymous Credentials (ACs) [Cha83, CL01]

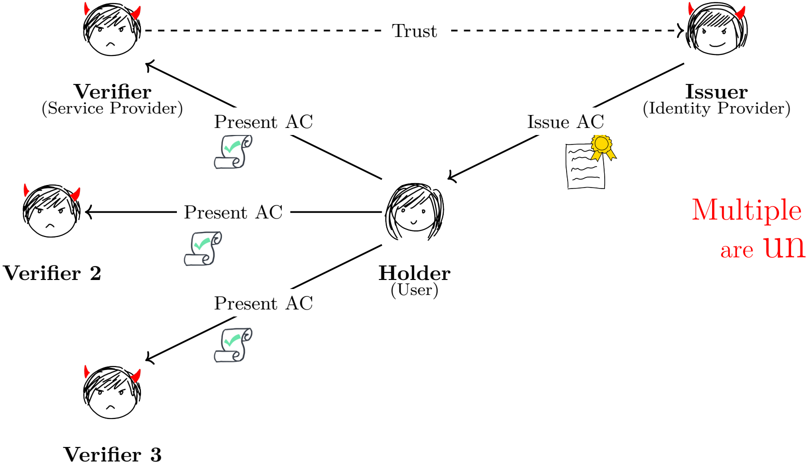
Privacy preserving digital credentials whose authorship can be cryptographically verified



Multiple presentations are unlinkable!

Anonymous Credentials (ACs)[Cha83, CL01]

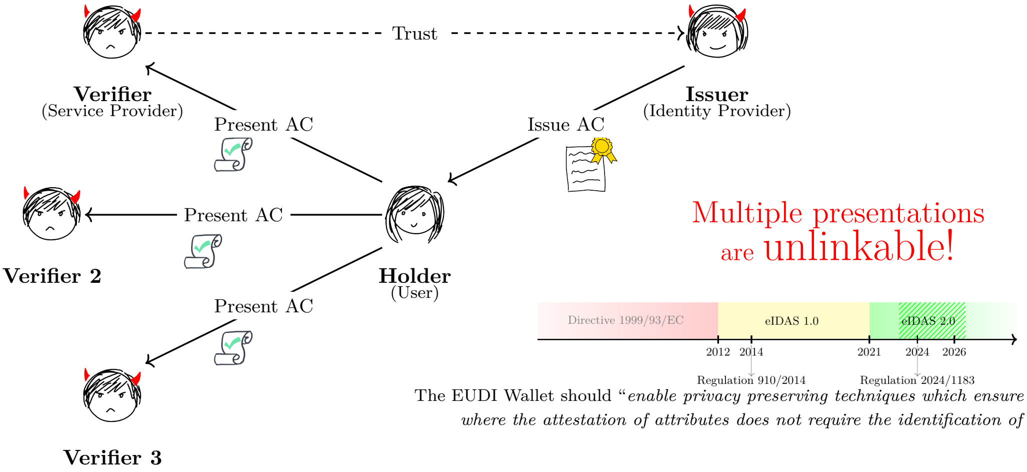
Privacy preserving digital credentials whose authorship can be cryptographically verified



Multiple presentations are unlinkable!

Anonymous Credentials (ACs)[Cha83, CL01]

Privacy preserving digital credentials whose authorship can be cryptographically verified



Verifier
(Service Provider)

Trust

Issuer
(Identity Provider)

Issue AC

Present AC

Present AC

Present AC

Holder
(User)

Verifier 2

Verifier 3

Multiple presentations are unlinkable!

The EUDI Wallet should “*enable privacy preserving techniques which ensure **unlinkability**, where the attestation of attributes does not require the identification of the user*”

The CL Framework [CL02]

A signature scheme with efficient NIZKPoK

The CL Framework [CL02]

A signature scheme with efficient NIZKPoK

Verifier

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

Holder

The CL Framework [CL02]

A signature scheme with efficient NIZKPoK

Verifier

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

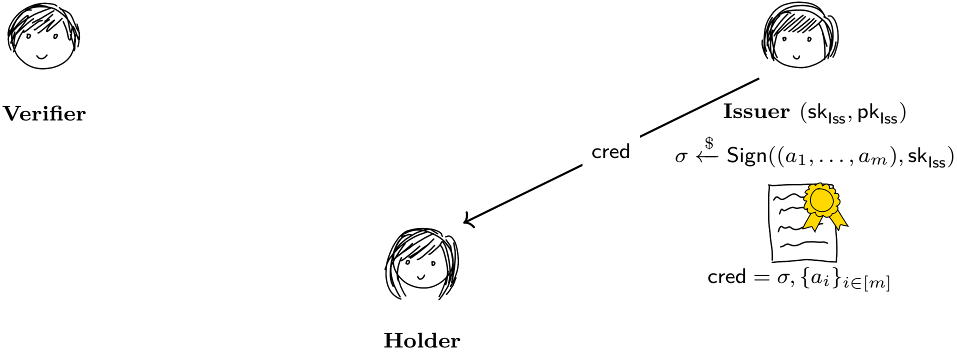
$\sigma \overset{\$}{\leftarrow} \mathsf{Sign}((a_1, \ldots, a_m), \mathsf{sk}_{\mathsf{Iss}})$

$\mathsf{cred} = \sigma, \{a_i\}_{i \in [m]}$

Holder

The CL Framework [CL02]

A signature scheme with efficient NIZKPoK



Verifier

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

$\sigma \xleftarrow{\$} \mathsf{Sign}((a_1, \ldots, a_m), \mathsf{sk}_{\mathsf{Iss}})$

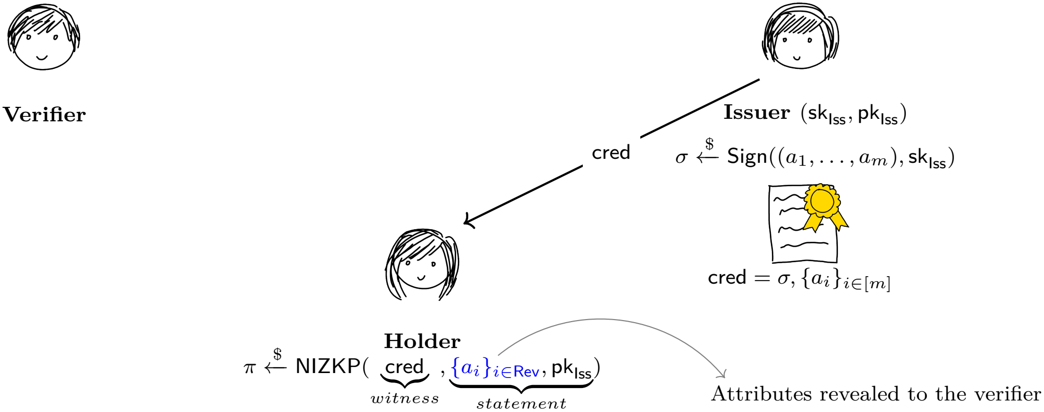
$\mathsf{cred} = \sigma, \{a_i\}_{i \in [m]}$

cred

Holder

The CL Framework [CL02]

A signature scheme with efficient NIZKPoK



Verifier

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

$\sigma \xleftarrow{\$} \mathsf{Sign}((a_1, \ldots, a_m), \mathsf{sk}_{\mathsf{Iss}})$

$\mathsf{cred} = \sigma, \{a_i\}_{i \in [m]}$

cred

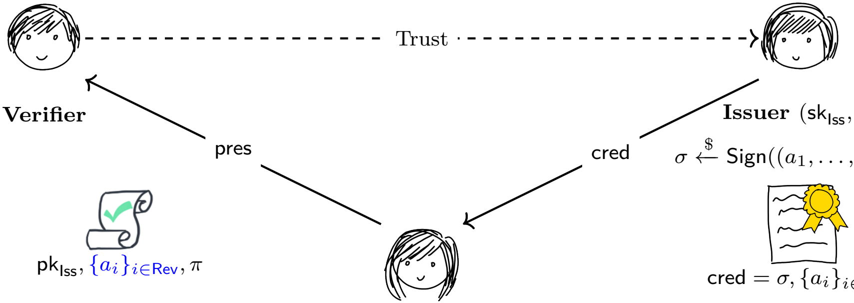
Holder

$\pi \xleftarrow{\$} \mathsf{NIZKP}(\underbrace{\mathsf{cred}}_{witness}, \underbrace{\{a_i\}_{i \in \mathsf{Rev}}, \mathsf{pk}_{\mathsf{Iss}}}_{statement})$

Attributes revealed to the verifier

The CL Framework [CL02]

A signature scheme with efficient NIZKPoK



Verifier

Trust

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

pres

cred

$\sigma \overset{\$}{\leftarrow} \mathsf{Sign}((a_1, \ldots, a_m), \mathsf{sk}_{\mathsf{Iss}})$

$\mathsf{pk}_{\mathsf{Iss}}, \{a_i\}_{i \in \mathsf{Rev}}, \pi$

$\mathsf{cred} = \sigma, \{a_i\}_{i \in [m]}$

Holder

$\pi \overset{\$}{\leftarrow} \mathsf{NIZKP}(\underbrace{\mathsf{cred}}_{witness}, \underbrace{\{a_i\}_{i \in \mathsf{Rev}}, \mathsf{pk}_{\mathsf{Iss}}}_{statement})$

Attributes revealed to the verifier

Multi-Holder Anonymous Credentials (MHAC)

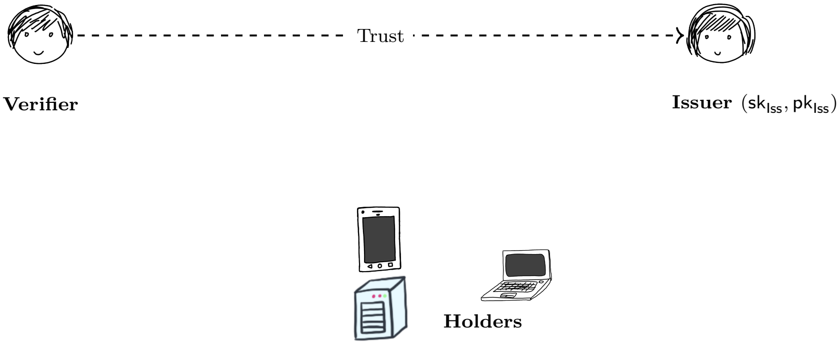
(Our first contribution)

Motivation and Intuition

Increase the security of storage of anonymous credentials to prevent identity theft

Motivation and Intuition

Increase the security of storage of anonymous credentials to prevent identity theft



Trust

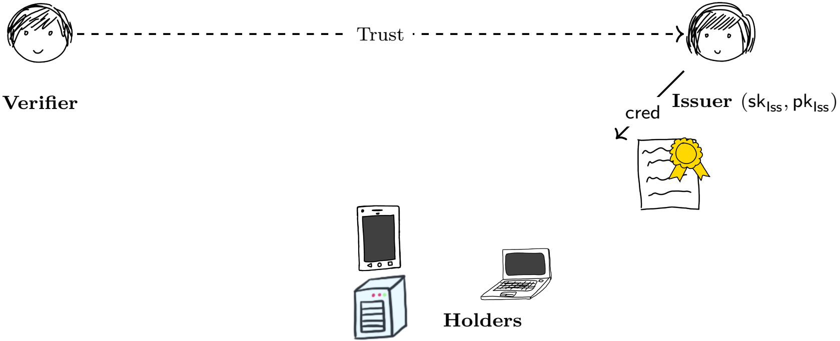
Verifier

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

Holders

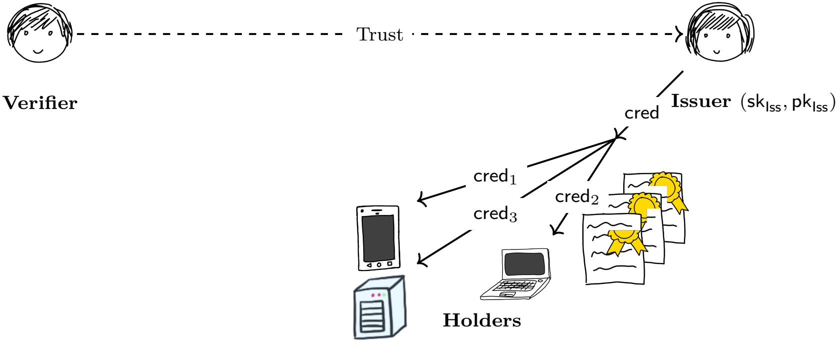
Motivation and Intuition

Increase the security of storage of anonymous credentials to prevent identity theft



Motivation and Intuition

Increase the security of storage of anonymous credentials to prevent identity theft



Verifier

Trust

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

cred

cred_1

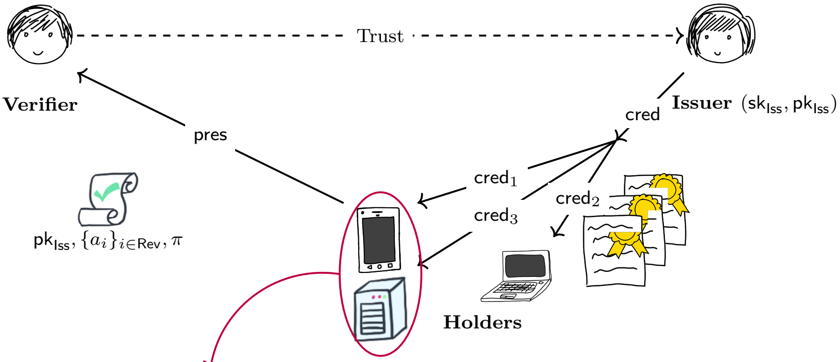
cred_2

cred_3

Holders

Motivation and Intuition

Increase the security of storage of anonymous credentials to prevent identity theft



Trust

Verifier

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

cred

pres

cred_1

cred_2

cred_3

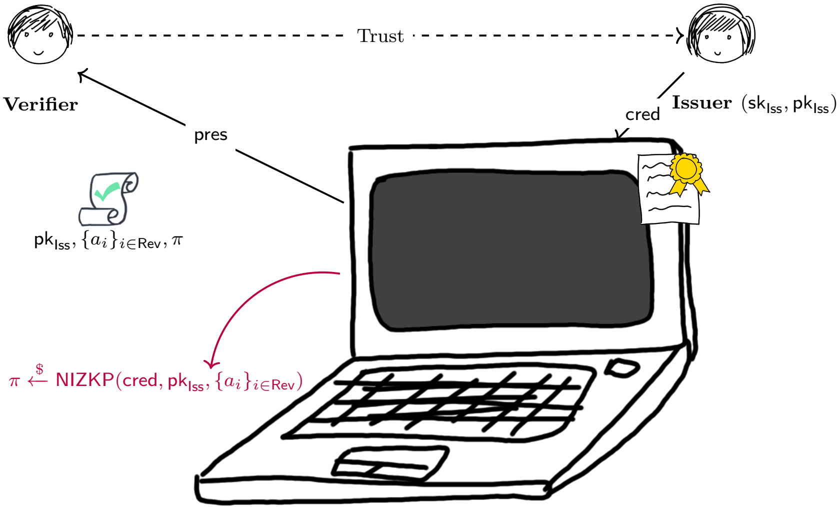
Holders

$\mathsf{pk}_{\mathsf{Iss}}, \{a_i\}_{i \in \mathsf{Rev}}, \pi$

$$\pi \xleftarrow{\$} \mathsf{NIZKP}(\mathsf{cred}, \mathsf{pk}_{\mathsf{Iss}}, \{a_i\}_{i \in \mathsf{Rev}})$$

Motivation and Intuition

Increase the security of storage of anonymous credentials to prevent identity theft



Verifier

Trust

Issuer $(\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}})$

cred

pres

$\mathsf{pk}_{\mathsf{Iss}}, \{a_i\}_{i \in \mathsf{Rev}}, \pi$

$\pi \xleftarrow{\$} \mathsf{NIZKP}(\mathsf{cred}, \mathsf{pk}_{\mathsf{Iss}}, \{a_i\}_{i \in \mathsf{Rev}})$

Security and Privacy Properties

Security and Privacy Properties

Correctness

Security and Privacy Properties

Correctness

Unlinkability

Security and Privacy Properties

Correctness

Unlinkability

Unforgeability of presentations

Security and Privacy Properties

Correctness

Unlinkability

Unforgeability of presentations

Security and Privacy Properties

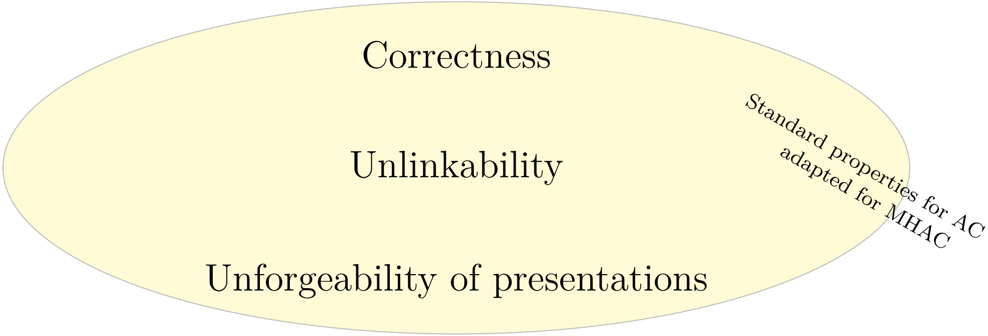
Correctness

Unlinkability

Unforgeability of presentations

Standard properties for AC
adapted for MHAC

Security and Privacy Properties



Correctness

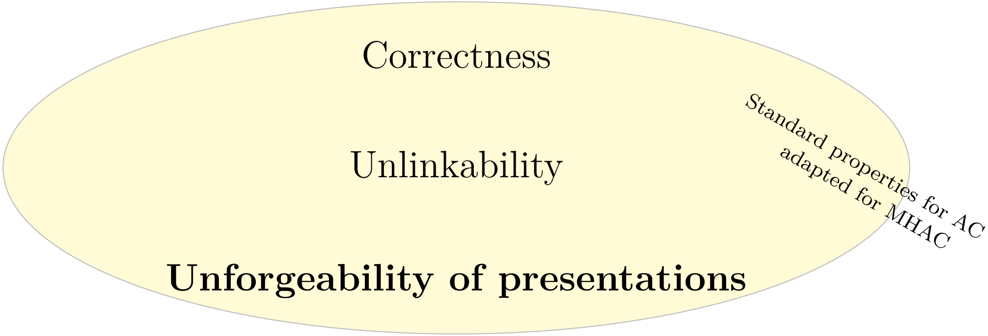
Unlinkability

Unforgeability of presentations

Standard properties for AC adapted for MHAC

Identifiable abort

Security and Privacy Properties



Correctness

Unlinkability

Unforgeability of presentations

Standard properties for AC
adapted for MHAC

Identifiable abort

Unforgeability Experiment

Adversary

Challenger

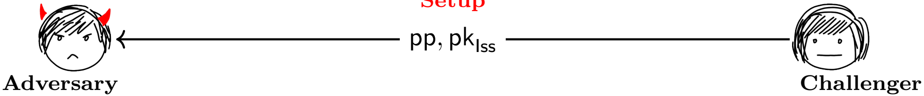
Unforgeability Experiment

Setup

Adversary

Challenger

Unforgeability Experiment



Setup

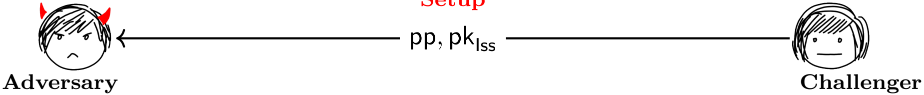
Adversary

$\mathsf{pp}, \mathsf{pk}_{\mathsf{lss}}$

Challenger

Unforgeability Experiment

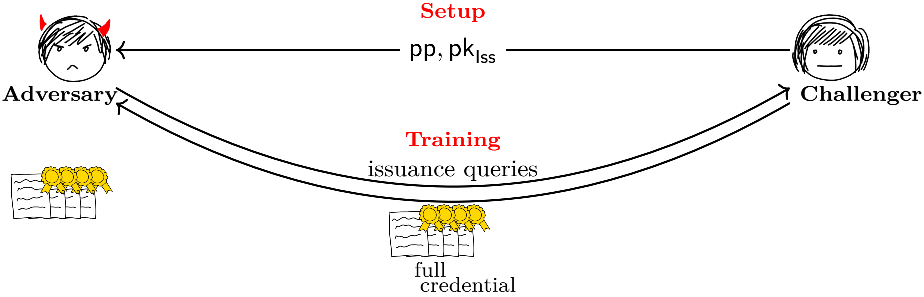
Setup



Adversary ← $\mathsf{pp}, \mathsf{pk}_{\mathsf{lss}}$ — **Challenger**

Training

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

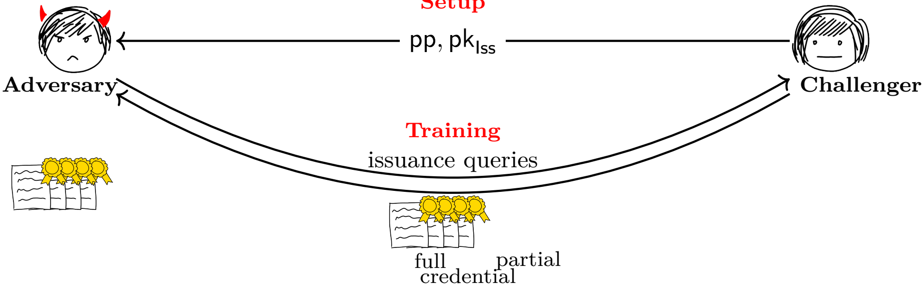
Challenger

Training

issuance queries

full credential

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

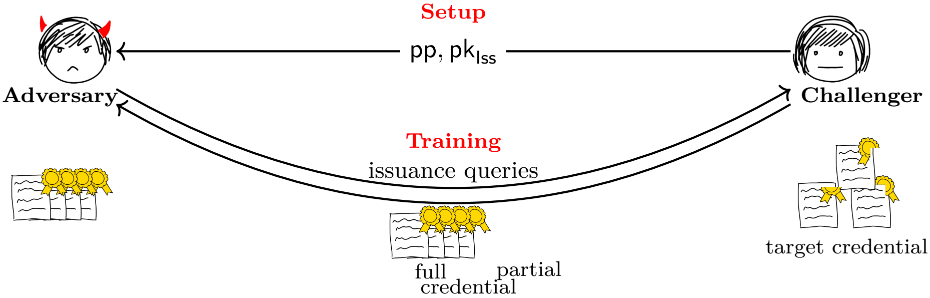
Challenger

Training

issuance queries

full partial
credential

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

Challenger

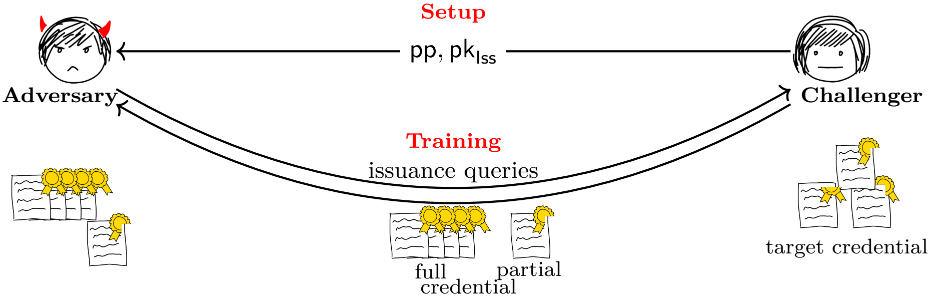
Training

issuance queries

full partial
credential

target credential

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

Challenger

Training

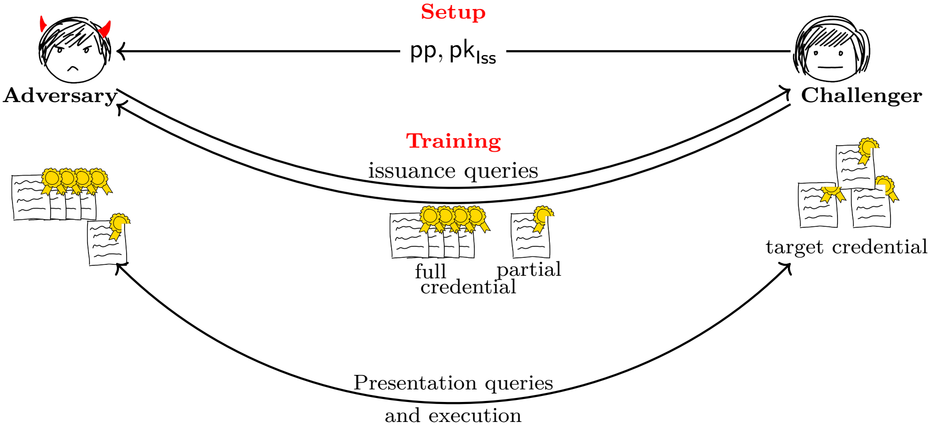
issuance queries

full credential

partial

target credential

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

Challenger

Training

issuance queries

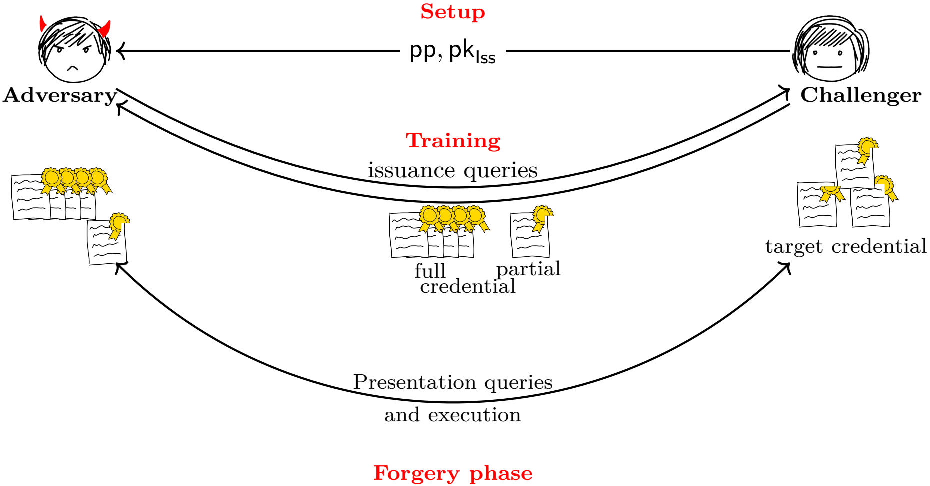
full credential

partial credential

target credential

Presentation queries and execution

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

Challenger

Training

issuance queries

full credential

partial

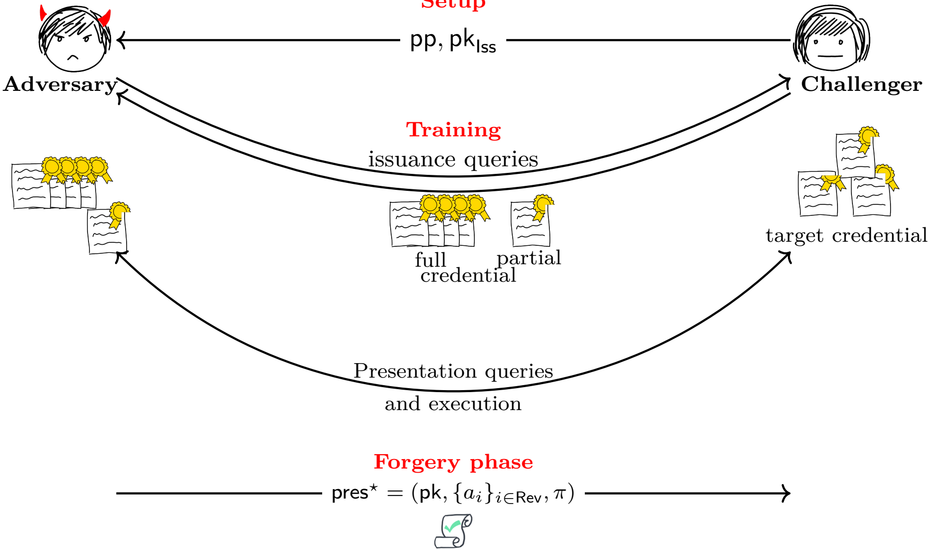
target credential

Presentation queries

and execution

Forgery phase

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

Challenger

Training

issuance queries

full credential

partial

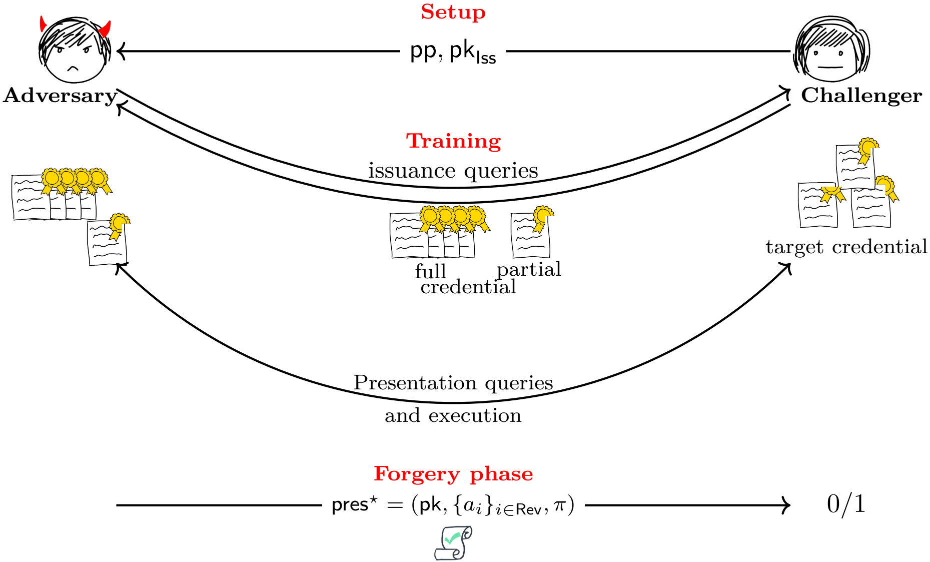
target credential

Presentation queries and execution

Forgery phase

$\mathsf{pres}^{\star} = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi)$

Unforgeability Experiment



Setup

$\mathsf{pp}, \mathsf{pk}_{\mathsf{Iss}}$

Adversary

Challenger

Training

issuance queries

full credential

partial credential

target credential

Presentation queries and execution

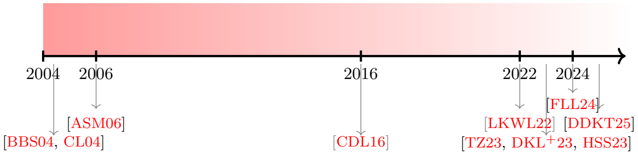
Forgery phase

$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi)$

$0/1$

BBS Anonymous Credentials

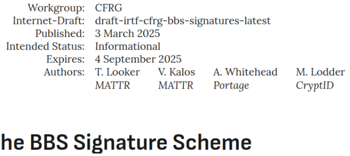
BBS Anonymous Credentials


2004
2006
2016
2022
2024
[BBS04, CL04]
[ASM06]
[CDL16]
[LKWL22]
[TZ23, DKL$^+$23, HSS23]
[FLL24]
[DDKT25]

Why BBS?

- multi-message signature
- compact public keys
- efficient signature and NIZKP

Standardization effort by DIF and IRTF


Workgroup: CFRG
Internet-Draft: draft-irtf-cfrg-bbs-signatures-latest
Published: 3 March 2025
Intended Status: Informational
Expires: 4 September 2025
Authors: T. Looker *MATTR*; V. Kalos *MATTR*; A. Whitehead *Portage*; M. Lodder *CryptID*

The BBS Signature Scheme

BBS Issuance

(For a single attribute a_1)

BBS Issuance

(For a single attribute a_1)

Setup

p-order groups $\mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle$, $\mathbb{G}_T$, and pairing $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

$$\mathsf{pp} = h_1 \xleftarrow{\$} \mathbb{G}_1 \qquad x \xleftarrow{\$} \mathbb{Z}_p \qquad (\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}}) \leftarrow (x, g_2^x)$$

BBS Issuance

(For a single attribute a_1)

Setup

p-order groups $\mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle$, $\mathbb{G}_T$, and pairing $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

$$\mathsf{pp} = h_1 \xleftarrow{\$} \mathbb{G}_1 \qquad x \xleftarrow{\$} \mathbb{Z}_p \qquad (\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}}) \leftarrow (x, g_2^x)$$

Issuance

$$C(a_1) \leftarrow g_1 h_1^{a_1} \qquad e \xleftarrow{\$} \mathbb{Z}_p \qquad A \leftarrow (C(a_1))^{\frac{1}{x+e}}$$

BBS Issuance

(For a single attribute a_1)

Setup

p-order groups $\mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle$, $\mathbb{G}_T$, and pairing $\mathbf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

$$\mathsf{pp} = h_1 \overset{\$}{\leftarrow} \mathbb{G}_1 \qquad x \overset{\$}{\leftarrow} \mathbb{Z}_p \qquad (\mathsf{sk}_{\mathsf{Iss}}, \mathsf{pk}_{\mathsf{Iss}}) \leftarrow (x, g_2^x)$$

Issuance

$$C(a_1) \leftarrow g_1 h_1^{a_1} \qquad e \overset{\$}{\leftarrow} \mathbb{Z}_p \qquad A \leftarrow (C(a_1))^{\frac{1}{x+e}}$$

$$\mathsf{cred} \leftarrow (\quad \underbrace{(A, e)}_{\text{BBS signature}} \quad , a_1)$$

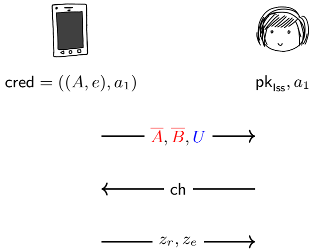
BBS Presentation[TZ23]

(full disclosure)

BBS Presentation[TZ23]

(full disclosure)

Presentation for $(\mathsf{pk}_{\mathsf{Iss}}, a_1)$ **of** $\mathsf{cred} = ((A, e), a_1)$



$\mathsf{cred} = ((A, e), a_1)$

$\mathsf{pk}_{\mathsf{Iss}}, a_1$

$\xrightarrow{\overline{A}, \overline{B}, U}$

$\xleftarrow{\mathsf{ch}}$

$\xrightarrow{z_r, z_e}$

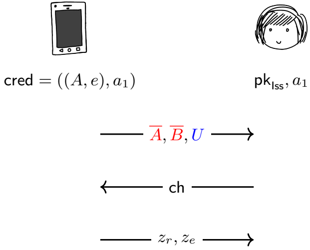
BBS Presentation[TZ23]

(full disclosure)

Presentation for $(\mathsf{pk}_{\mathsf{Iss}}, a_1)$ **of** $\mathsf{cred} = ((A, e), a_1)$

- signature randomization: $r \xleftarrow{\$} \mathbb{Z}_p$
  $\overline{A} \leftarrow A^r \qquad \overline{B} \leftarrow C(a_1)^r \overline{A}^{-e}$
- $(U, \mathsf{ch}, z_r, z_e) \xleftarrow{\$} \mathrm{NIZKPoK}\{(\alpha, \beta) : \overline{B} = C(a_1)^\alpha \overline{A}^\beta\}$
- $\pi \leftarrow (\overline{A}, \overline{B}, U, \mathsf{ch}, z_r, z_e)$

$$C(a_1) = g_1 h_1^{a_1}$$



$\mathsf{cred} = ((A, e), a_1)$

$\mathsf{pk}_{\mathsf{Iss}}, a_1$

$\overline{A}, \overline{B}, U \longrightarrow$

$\longleftarrow \mathsf{ch}$

$z_r, z_e \longrightarrow$

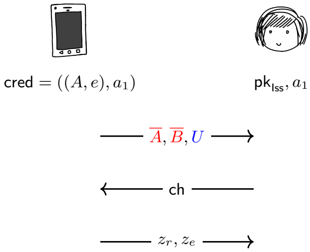
BBS Presentation[TZ23]

(full disclosure)

Presentation for $(\mathsf{pk}_{\mathsf{Iss}}, a_1)$ **of** $\mathsf{cred} = ((A, e), a_1)$

- signature randomization: $r \xleftarrow{\$} \mathbb{Z}_p$
  $\overline{A} \leftarrow A^r \qquad \overline{B} \leftarrow C(a_1)^r \overline{A}^{-e}$
- $(U, \mathsf{ch}, z_r, z_e) \xleftarrow{\$} \mathrm{NIZKPoK}\{(\alpha, \beta) : \overline{B} = C(a_1)^\alpha \overline{A}^\beta\}$
- $\pi \leftarrow (\overline{A}, \overline{B}, U, \mathsf{ch}, z_r, z_e)$

$C(a_1) = g_1 h_1^{a_1}$



$\mathsf{cred} = ((A, e), a_1)$

$\mathsf{pk}_{\mathsf{Iss}}, a_1$

$\xrightarrow{\overline{A}, \overline{B}, U}$

$\xleftarrow{\mathsf{ch}}$

$\xrightarrow{z_r, z_e}$

$$\mathsf{pres} \leftarrow (\pi, \underbrace{a_1, \mathsf{pk}_{\mathsf{Iss}}}_{\text{statement}})$$

A MHAC compatible with BBS

(Our second contribution)

BBS MHAC Issuance

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

Divide it in shares:

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

Divide it in shares:

e is never revealed!

$$\{e_i\}_{i\in[n]} \xleftarrow{\$} \mathsf{SS}(t, n, e)$$

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

Divide it in shares:

e is never revealed!

$$\{e_i\}_{i \in [n]} \xleftarrow{\$} \mathsf{SS}(t, n, e) \quad \mathsf{cred}_i \leftarrow (e_i, \underbrace{A, A^e, \{A^{e_i}\}_{i \in [n]}, a_1}_{\text{same for every holder}})$$

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

e is never revealed!

Divide it in shares:

$$\{e_i\}_{i\in[n]} \xleftarrow{\$} \mathsf{SS}(t, n, e) \quad \mathsf{cred}_i \leftarrow (e_i, \underbrace{A, A^e, \{A^{e_i}\}_{i\in[n]}, a_1}_{\text{same for every holder}})$$

Crucial observation: giving to each holder A^e is just fine!

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

e is never revealed!

Divide it in shares:

$$\{e_i\}_{i\in[n]} \xleftarrow{\$} \mathsf{SS}(t, n, e) \quad \mathsf{cred}_i \leftarrow (e_i, \underbrace{A, A^e, \{A^{e_i}\}_{i\in[n]}, a_1}_{\text{same for every holder}})$$

Crucial observation: giving to each holder A^e is just fine!

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

e is never revealed!

Divide it in shares:

$$\{e_i\}_{i\in[n]} \xleftarrow{\$} \mathsf{SS}(t, n, e) \quad \mathsf{cred}_i \leftarrow (e_i, \underbrace{A, A^e, \{A^{e_i}\}_{i\in[n]}, a_1}_{\text{same for every holder}})$$

Crucial observation: giving to each holder A^e is just fine!

enables the identifiable abort property

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

e is never revealed!

Divide it in shares:

$$\{e_i\}_{i \in [n]} \xleftarrow{\$} \mathsf{SS}(t, n, e) \quad \mathsf{cred}_i \leftarrow (e_i, \underbrace{A, A^e, \{A^{e_i}\}_{i \in [n]}, a_1}_{\text{same for every holder}})$$

Crucial observation: giving to each holder A^e is just fine!

enables the identifiable abort property

simplifies the presentation protocol

BBS MHAC Issuance

Generate a BBS credential $\mathsf{cred} = (A, e), a_1$

e is never revealed!

Divide it in shares:

$$\{e_i\}_{i\in[n]} \xleftarrow{\$} \mathsf{SS}(t, n, e) \quad \mathsf{cred}_i \leftarrow (e_i, \underbrace{A, A^e, \text{[redacted]}, a_1}_{\text{same for every holder}})$$

Crucial observation: giving to each holder A^e is just fine!

enables the identifiable abort property

simplifies the presentation protocol

can be made constant size

BBS MHAC Presentation protocol

$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j \in [n]}, a_1)$

Multi-holder case

Centralised case

$\mathsf{cred} \leftarrow ((A, e), a_1)$

$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

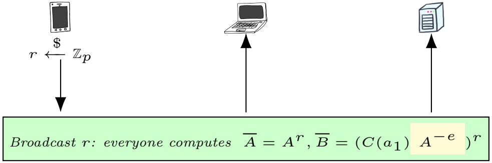
Multi-holder case

Centralised case

$\mathsf{cred} \leftarrow ((A, e), a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j \in [n]}, a_1)$



$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\, A^{-e})^r$

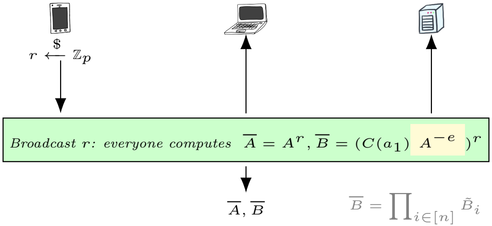
Multi-holder case

Centralised case

$\mathsf{cred} \leftarrow ((A, e), a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j \in [n]}, a_1)$



$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\, A^{-e})^r$

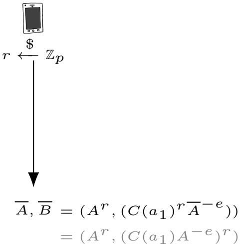
$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i \in [n]} \tilde{B}_i$

Multi-holder case

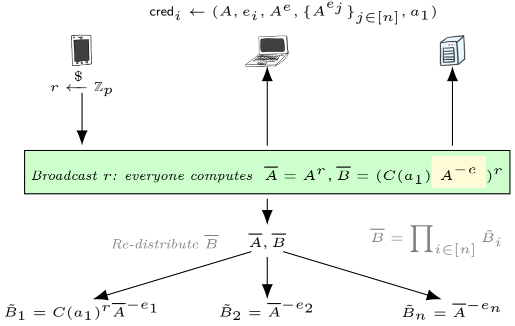
Centralised case

$\mathsf{cred} \leftarrow ((A, e), a_1)$



$r \xleftarrow{\$} \mathbb{Z}_p$

$$\overline{A}, \overline{B} = (A^r, (C(a_1)^r \overline{A}^{-e}))$$
$$= (A^r, (C(a_1) A^{-e})^r)$$



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\, A^{-e}\,)^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

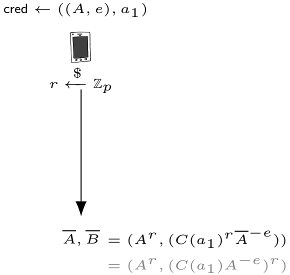
$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

Multi-holder case

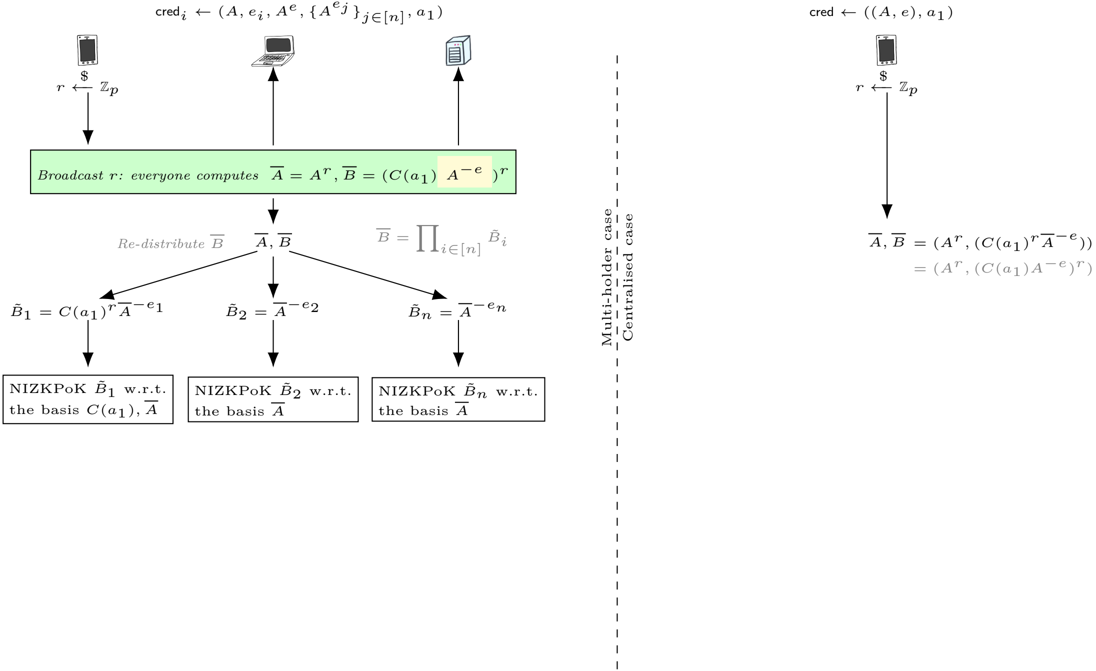
Centralised case



$\mathsf{cred} \leftarrow ((A, e), a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

$$\overline{A}, \overline{B} = (A^r, (C(a_1)^r\overline{A}^{-e}))$$
$$= (A^r, (C(a_1)A^{-e})^r)$$



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e}\ )^r$

$\overline{A}, \overline{B}$

Re-distribute $\overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

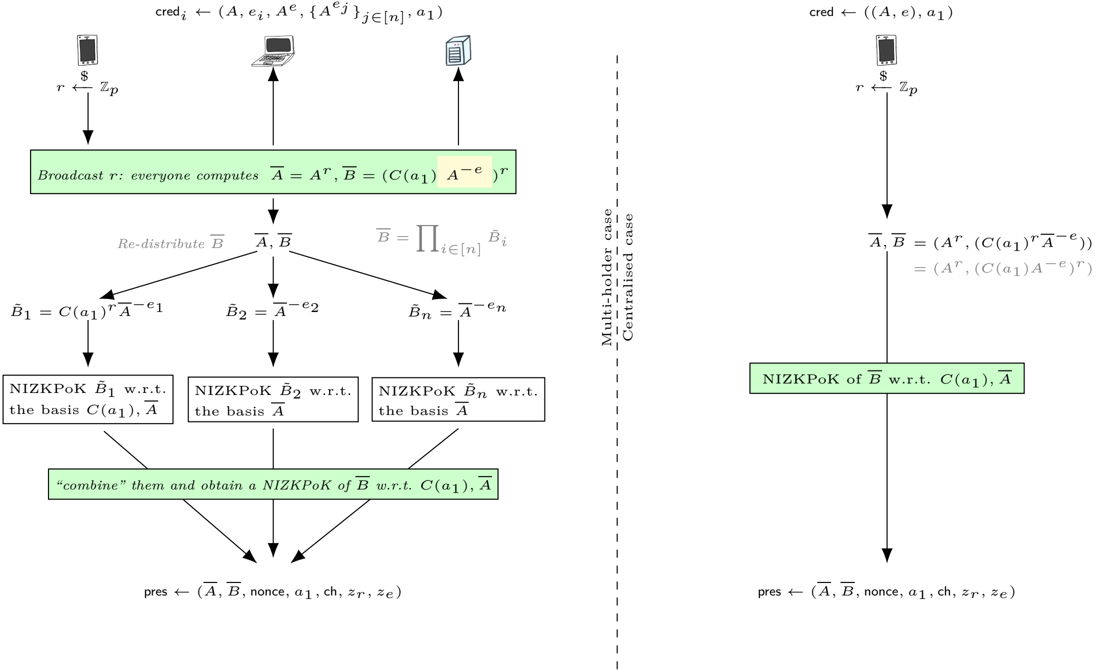
Multi-holder case

Centralised case

$\mathsf{cred} \leftarrow ((A, e), a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

$$\overline{A}, \overline{B} = (A^r, (C(a_1)^r\overline{A}^{-e}))$$
$$= (A^r, (C(a_1)A^{-e})^r)$$



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e}\ )^r$

$\overline{A}, \overline{B}$

Re-distribute $\overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Multi-holder case

Centralised case

$\mathsf{cred} \leftarrow ((A, e), a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

$\overline{A}, \overline{B} = (A^r, (C(a_1)^r\overline{A}^{-e}))$

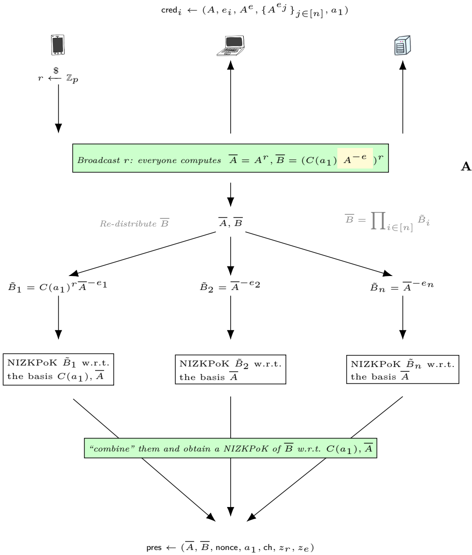
$= (A^r, (C(a_1)A^{-e})^r)$

NIZKPoK of $\overline{B}$ w.r.t. $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e})^r$

$\overline{A}, \overline{B}$

Re-distribute $\overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Adversary

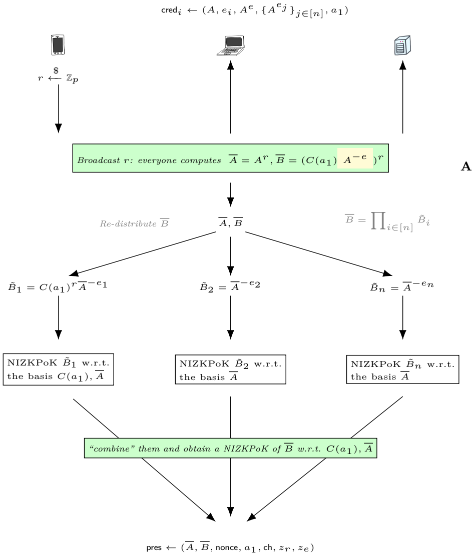
Reduction

DL **challenger**

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)

Setup



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \overset{\$}{\longleftarrow} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e})^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

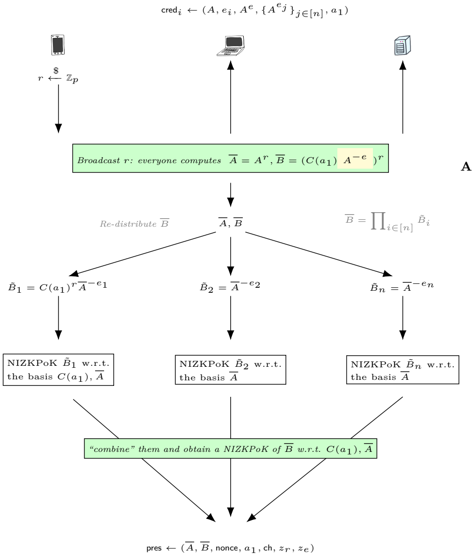
NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e})^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

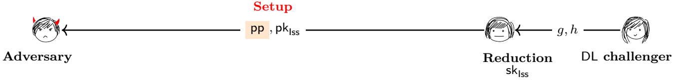
NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

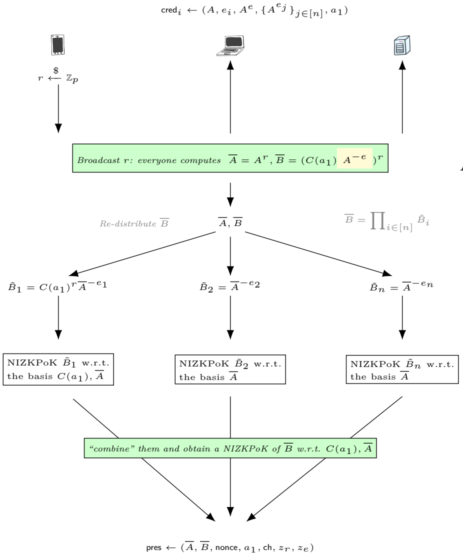
Adversary

Reduction
$\mathsf{sk}_{\mathsf{Iss}}$

DL **challenger**

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e})^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

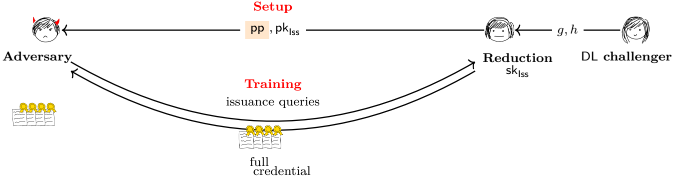
NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

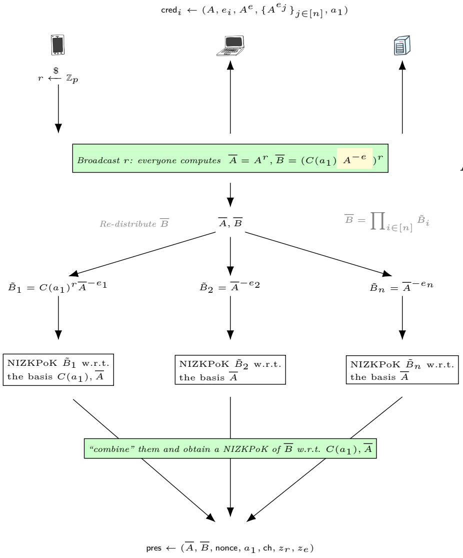
$\mathsf{sk}_{\mathsf{Iss}}$

DL **challenger**

Training

issuance queries

full credential



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j \in [n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e}\ )^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i \in [n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

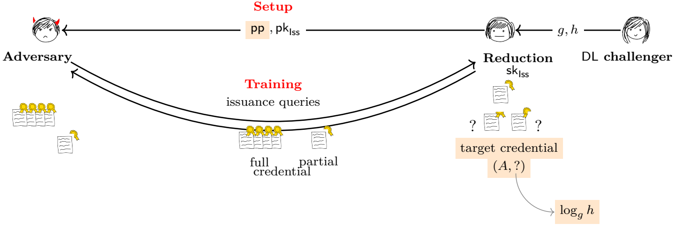
NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



Setup

pp , $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

$\mathsf{sk}_{\mathsf{Iss}}$

DL **challenger**

Training

issuance queries

full credential

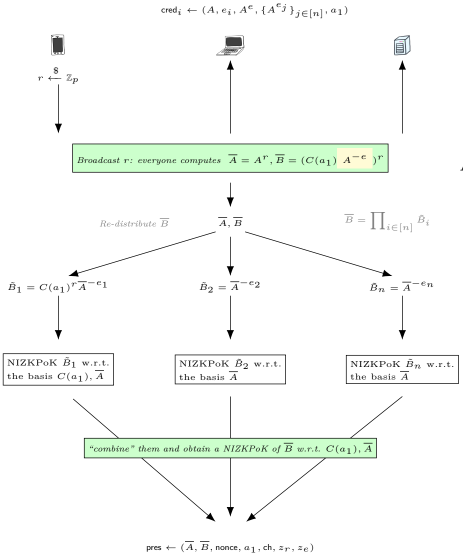
partial

? ?

target credential

$(A, ?)$

$\log_g h$



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\, A^{-e})^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

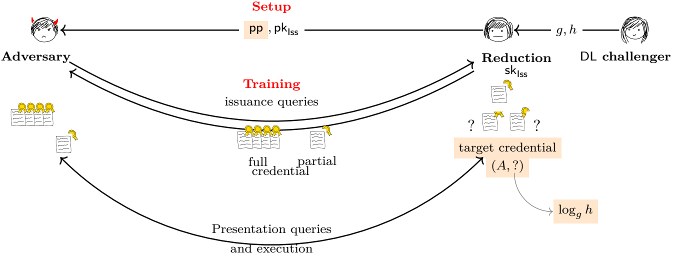
NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



Setup

pp , $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

$\mathsf{sk}_{\mathsf{Iss}}$

DL challenger

Training

issuance queries

full credential

partial

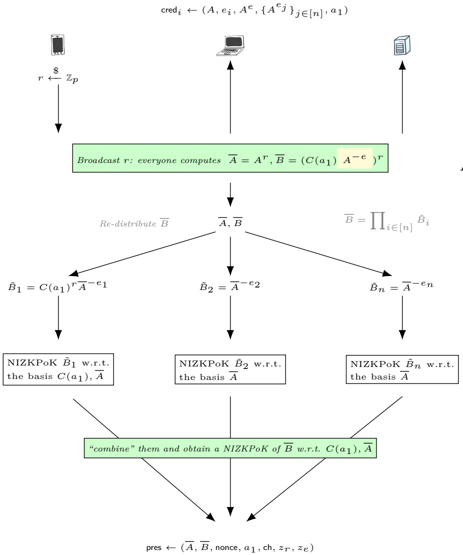
? ?

target credential

$(A, ?)$

$\log_g h$

Presentation queries and execution



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e})^r$

$\overline{A}, \overline{B}$

Re-distribute $\overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

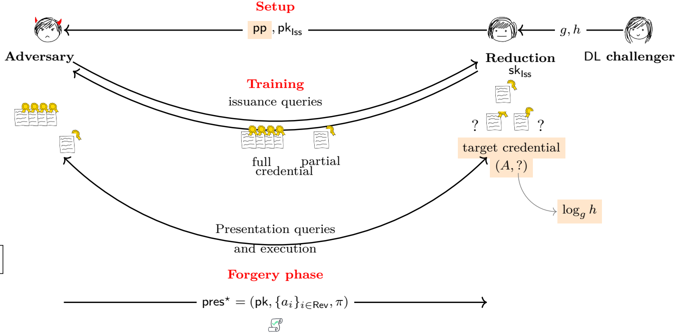
NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

$\mathsf{sk}_{\mathsf{Iss}}$

DL challenger

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

$\log_g h$

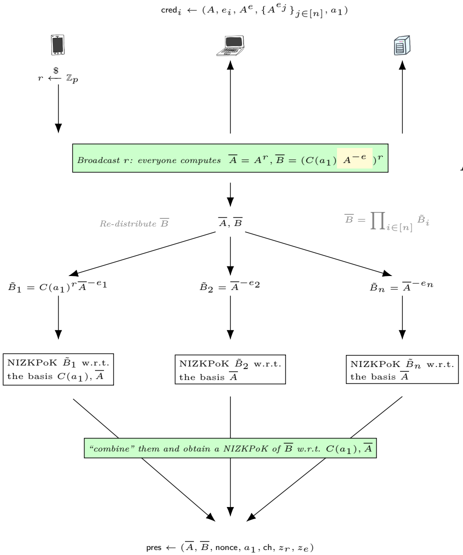
Presentation queries and execution

Forgery phase

$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi)$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e})^r$

$\overline{A}, \overline{B}$

Re-distribute $\overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

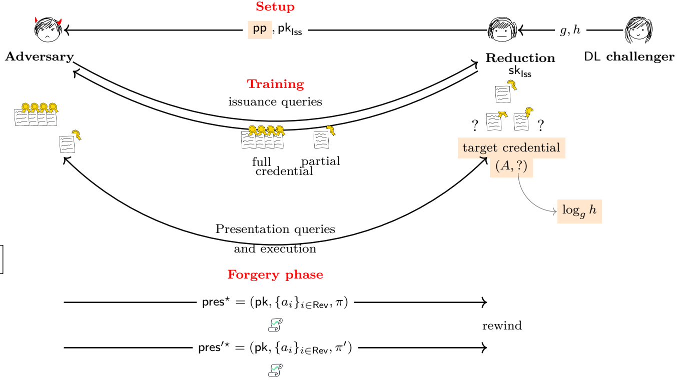
NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

$\mathsf{sk}_{\mathsf{Iss}}$

DL challenger

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

$\log_g h$

Presentation queries and execution

Forgery phase

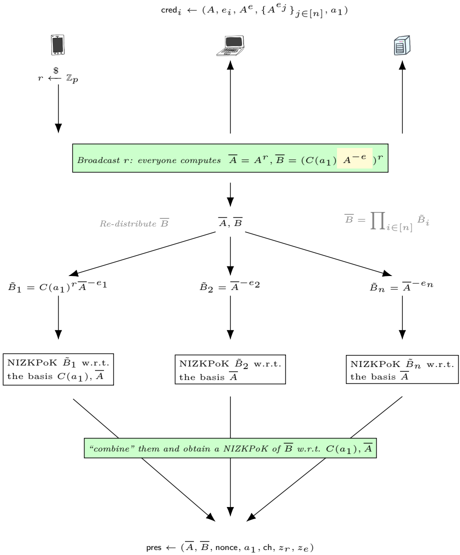
$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi)$

rewind

$\mathsf{pres}'^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi')$

Unforgeability reduces to DL assumption

(When the adversary forges the target credential)



$\mathsf{cred}_i \leftarrow (A, e_i, A^e, \{A^{e_j}\}_{j\in[n]}, a_1)$

$r \xleftarrow{\$} \mathbb{Z}_p$

Broadcast r: everyone computes $\overline{A} = A^r, \overline{B} = (C(a_1)\ A^{-e}\ )^r$

Re-distribute $\overline{B}$

$\overline{A}, \overline{B}$

$\overline{B} = \prod_{i\in[n]} \tilde{B}_i$

$\tilde{B}_1 = C(a_1)^r\overline{A}^{-e_1}$

$\tilde{B}_2 = \overline{A}^{-e_2}$

$\tilde{B}_n = \overline{A}^{-e_n}$

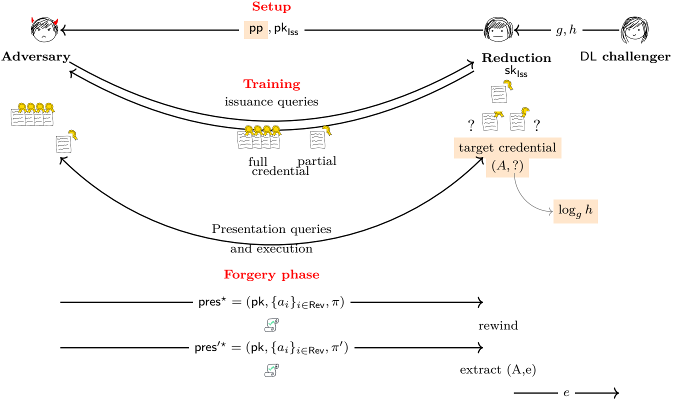
NIZKPoK $\tilde{B}_1$ w.r.t. the basis $C(a_1), \overline{A}$

NIZKPoK $\tilde{B}_2$ w.r.t. the basis $\overline{A}$

NIZKPoK $\tilde{B}_n$ w.r.t. the basis $\overline{A}$

"combine" them and obtain a NIZKPoK of $\overline{B}$ *w.r.t.* $C(a_1), \overline{A}$

$\mathsf{pres} \leftarrow (\overline{A}, \overline{B}, \mathsf{nonce}, a_1, \mathsf{ch}, z_r, z_e)$



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

$\mathsf{sk}_{\mathsf{Iss}}$

DL **challenger**

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

$\log_g h$

Presentation queries and execution

Forgery phase

$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi)$

rewind

$\mathsf{pres}'^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi')$

extract (A,e)

e

Thank you for your attention!

to Eysa Lee for the Alice-and-Bobs illustrations
https://github.com/eysalee/alice-and-bobs/tree/main

and to the QUBIP European project for funding my trip here

QUBIP

Man Ho Au, Willy Susilo, and Yi Mu.
Constant-size dynamic k-TAA.
In *SCN 2006*, volume 4116 of *LNCS*, pages 111–125, 2006.

Dan Boneh, Xavier Boyen, and Hovav Shacham.
Short group signatures.
In *Annual international cryptology conference*, pages 41–55. Springer, 2004.

Jan Camenisch, Manu Drijvers, and Anja Lehmann.
Anonymous attestation using the strong diffie hellman assumption revisited.
In *Trust and Trustworthy Computing: 9th International Conference, TRUST 2016, Vienna, Austria, August 29-30, 2016, Proceedings 9*, pages 1–20. Springer, 2016.

David Chaum.
Blind signatures for untraceable payments.
In *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Springer, 1983.

Jan Camenisch and Anna Lysyanskaya.
An efficient system for non-transferable anonymous credentials with optional anonymity revocation.
In *International conference on the theory and applications of cryptographic techniques*, pages 93–118. Springer, 2001.

Jan Camenisch and Anna Lysyanskaya.
A signature scheme with efficient protocols.
In *SCN 2002*, volume 2576 of *LNCS*, pages 268–289, 2002.

Jan Camenisch and Anna Lysyanskaya.
Signature schemes and anonymous credentials from bilinear maps.
In *Annual international cryptology conference*, pages 56–72. Springer, 2004.

Nicolas Desmoulins, Antoine Dumanois, Seyni Kane, and Jacques Traoré.
Making bbs anonymous credentials eidas 2.0 compliant.
Cryptology ePrint Archive, 2025.

Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat, and LaKyah Tyner.
Threshold bbs+ signatures for distributed anonymous credential issuance.
In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 773–789. IEEE, 2023.

Andrea Flamini, Eysa Lee, and Anna Lysyanskaya.
Multi-holder anonymous credentials from bbs signatures.
Cryptology ePrint Archive, 2024.

Julia Hesse, Nitin Singh, and Alessandro Sorniotti.
How to bind anonymous credentials to humans.

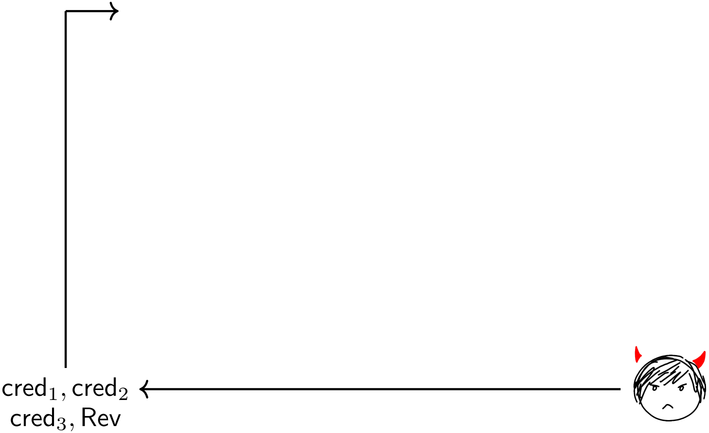
In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3047–3064, 2023.

Tobias Looker, Vasilis Kalos, Andrew Whitehead, and Mike Lodder.
The BBS Signature Scheme.
Internet-Draft draft-irtf-cfrg-bbs-signatures-01, Internet Engineering Task Force, October 2022.

Work in Progress.

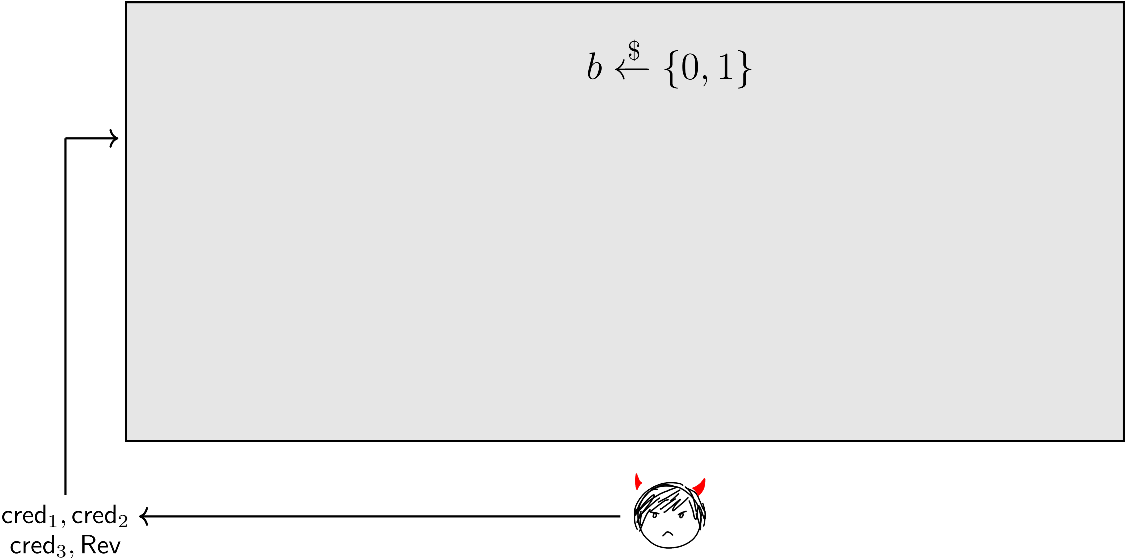
Stefano Tessaro and Chenzhi Zhu.
Revisiting BBS signatures.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 691–721. Springer, 2023.

Unlinkability Experiment



$\mathsf{cred}_1, \mathsf{cred}_2$
$\mathsf{cred}_3, \mathsf{Rev}$

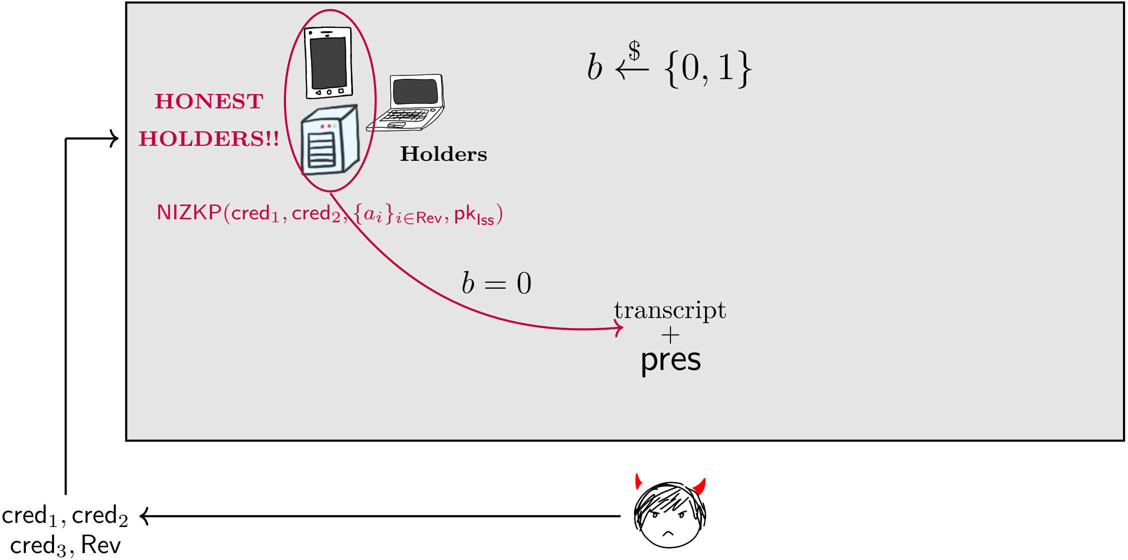
Unlinkability Experiment



$b \xleftarrow{\$} \{0,1\}$

$\mathsf{cred}_1, \mathsf{cred}_2$
$\mathsf{cred}_3, \mathsf{Rev}$

Unlinkability Experiment



$b \xleftarrow{\$} \{0, 1\}$

HONEST HOLDERS!!

Holders

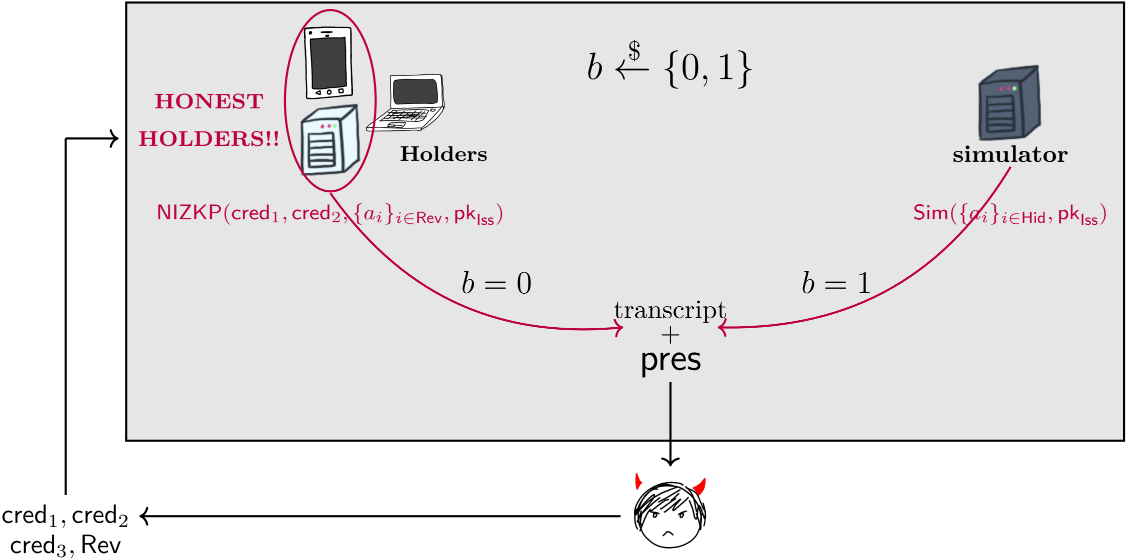
$\mathsf{NIZKP}(\mathsf{cred}_1, \mathsf{cred}_2, \{a_i\}_{i \in \mathsf{Rev}}, \mathsf{pk}_{\mathsf{Iss}})$

$b = 0$

transcript + pres

$\mathsf{cred}_1, \mathsf{cred}_2$
$\mathsf{cred}_3, \mathsf{Rev}$

Unlinkability Experiment



$b \xleftarrow{\$} \{0, 1\}$

HONEST HOLDERS!!

Holders

simulator

$\mathsf{NIZKP}(\mathsf{cred}_1, \mathsf{cred}_2, \{a_i\}_{i \in \mathsf{Rev}}, \mathsf{pk}_{\mathsf{Iss}})$

$\mathsf{Sim}(\{a_i\}_{i \in \mathsf{Hid}}, \mathsf{pk}_{\mathsf{Iss}})$

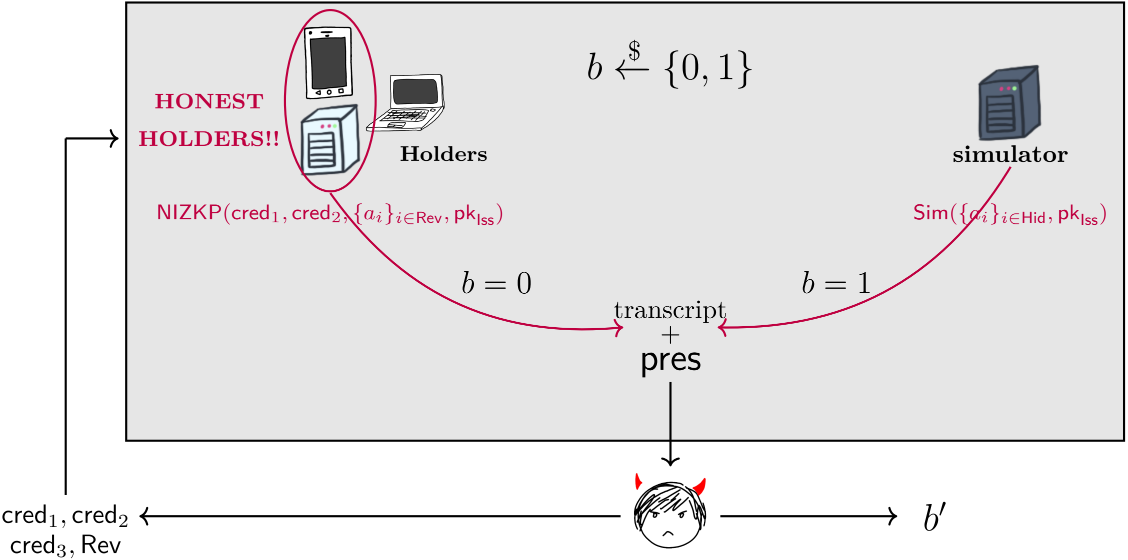
$b = 0$

$b = 1$

transcript
+
pres

$\mathsf{cred}_1, \mathsf{cred}_2$
$\mathsf{cred}_3, \mathsf{Rev}$

Unlinkability Experiment



$b \xleftarrow{\$} \{0, 1\}$

HONEST HOLDERS!!

Holders

simulator

$\mathsf{NIZKP}(\mathsf{cred}_1, \mathsf{cred}_2, \{a_i\}_{i \in \mathsf{Rev}}, \mathsf{pk}_{\mathsf{Iss}})$

$\mathsf{Sim}(\{a_i\}_{i \in \mathsf{Hid}}, \mathsf{pk}_{\mathsf{Iss}})$

$b = 0$

$b = 1$

transcript
+
pres

$\mathsf{cred}_1, \mathsf{cred}_2$
$\mathsf{cred}_3, \mathsf{Rev}$

b'

How does the combined NIZKP works?

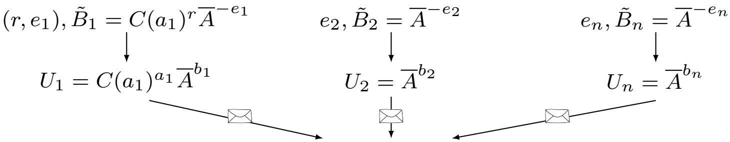
$(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$ $e_2, \tilde{B}_2 = \overline{A}^{-e_2}$ $e_n, \tilde{B}_n = \overline{A}^{-e_n}$

How does the combined NIZKP works?

$$\begin{tikzcd}
 & (r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1} \arrow[d] & e_2, \tilde{B}_2 = \overline{A}^{-e_2} \arrow[d] & e_n, \tilde{B}_n = \overline{A}^{-e_n} \arrow[d] \\
a_1, \{b_i\}_{i \in [n]} \xleftarrow{\$} \mathbb{Z}_p & {} & {} & {}
\end{tikzcd}$$

How does the combined NIZKP works?

$a_1, \{b_i\}_{i\in[n]} \xleftarrow{\$} \mathbb{Z}_p$



$(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$U_1 = C(a_1)^{a_1} \overline{A}^{b_1}$

$e_2, \tilde{B}_2 = \overline{A}^{-e_2}$

$U_2 = \overline{A}^{b_2}$

$e_n, \tilde{B}_n = \overline{A}^{-e_n}$

$U_n = \overline{A}^{b_n}$

commit and release

How does the combined NIZKP works?

$a_1, \{b_i\}_{i \in [n]} \xleftarrow{\$} \mathbb{Z}_p$

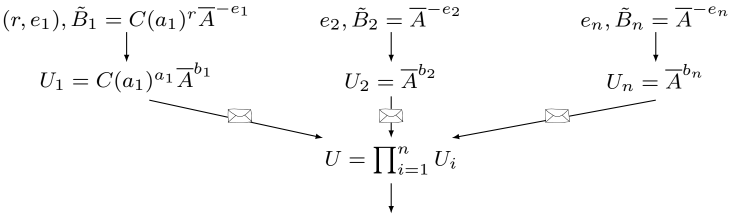
commit and release

$$\begin{tikzcd}
(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1} \arrow[d] & e_2, \tilde{B}_2 = \overline{A}^{-e_2} \arrow[d] & e_n, \tilde{B}_n = \overline{A}^{-e_n} \arrow[d] \\
U_1 = C(a_1)^{a_1} \overline{A}^{b_1} \arrow[dr, "✉"] & U_2 = \overline{A}^{b_2} \arrow[d, "✉"] & U_n = \overline{A}^{b_n} \arrow[dl, "✉"'] \\
& U = \prod_{i=1}^{n} U_i \arrow[d] & \\
& &
\end{tikzcd}$$

How does the combined NIZKP works?

$a_1, \{b_i\}_{i\in[n]} \xleftarrow{\$} \mathbb{Z}_p$

commit and release



$(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$U_1 = C(a_1)^{a_1} \overline{A}^{b_1}$

$e_2, \tilde{B}_2 = \overline{A}^{-e_2}$

$U_2 = \overline{A}^{b_2}$

$e_n, \tilde{B}_n = \overline{A}^{-e_n}$

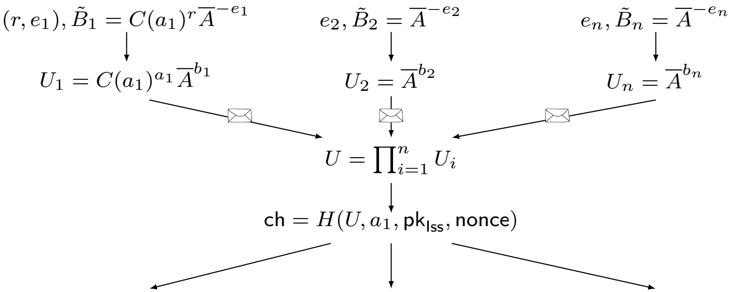
$U_n = \overline{A}^{b_n}$

$U = \prod_{i=1}^{n} U_i$

How does the combined NIZKP works?

$a_1, \{b_i\}_{i \in [n]} \xleftarrow{\$} \mathbb{Z}_p$

commit and release



$(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$e_2, \tilde{B}_2 = \overline{A}^{-e_2}$

$e_n, \tilde{B}_n = \overline{A}^{-e_n}$

$U_1 = C(a_1)^{a_1} \overline{A}^{b_1}$

$U_2 = \overline{A}^{b_2}$

$U_n = \overline{A}^{b_n}$

$U = \prod_{i=1}^{n} U_i$

$\mathsf{ch} = H(U, a_1, \mathsf{pk}_{\mathsf{Iss}}, \mathsf{nonce})$

How does the combined NIZKP works?

$a_1, \{b_i\}_{i \in [n]} \xleftarrow{\$} \mathbb{Z}_p$

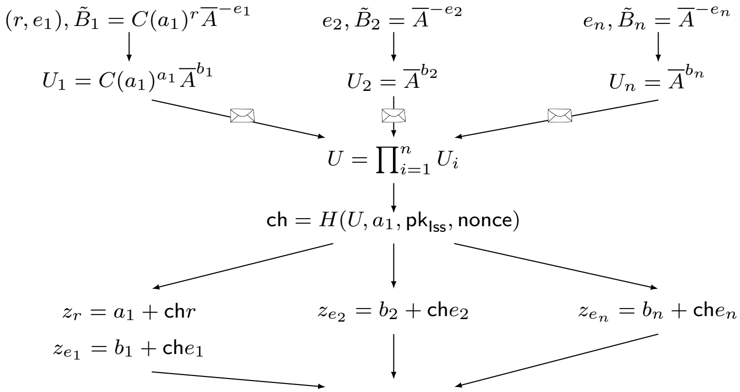
commit and release

$$\begin{tikzcd}
(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1} \arrow[d] & e_2, \tilde{B}_2 = \overline{A}^{-e_2} \arrow[d] & e_n, \tilde{B}_n = \overline{A}^{-e_n} \arrow[d] \\
U_1 = C(a_1)^{a_1} \overline{A}^{b_1} \arrow[dr, "\text{✉}" description] & U_2 = \overline{A}^{b_2} \arrow[d, "\text{✉}" description] & U_n = \overline{A}^{b_n} \arrow[dl, "\text{✉}" description] \\
 & U = \prod_{i=1}^{n} U_i \arrow[d] & \\
 & \mathsf{ch} = H(U, a_1, \mathsf{pk}_{\mathsf{Iss}}, \mathsf{nonce}) \arrow[dl] \arrow[d] \arrow[dr] & \\
z_r = a_1 + \mathsf{ch}r & z_{e_2} = b_2 + \mathsf{ch}e_2 & z_{e_n} = b_n + \mathsf{ch}e_n \\
z_{e_1} = b_1 + \mathsf{ch}e_1 & &
\end{tikzcd}$$

How does the combined NIZKP works?

$a_1, \{b_i\}_{i \in [n]} \xleftarrow{\$} \mathbb{Z}_p$

commit and release



$(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1}$

$e_2, \tilde{B}_2 = \overline{A}^{-e_2}$

$e_n, \tilde{B}_n = \overline{A}^{-e_n}$

$U_1 = C(a_1)^{a_1} \overline{A}^{b_1}$

$U_2 = \overline{A}^{b_2}$

$U_n = \overline{A}^{b_n}$

$U = \prod_{i=1}^{n} U_i$

$\mathsf{ch} = H(U, a_1, \mathsf{pk}_{\mathsf{Iss}}, \mathsf{nonce})$

$z_r = a_1 + \mathsf{ch} r$

$z_{e_1} = b_1 + \mathsf{ch} e_1$

$z_{e_2} = b_2 + \mathsf{ch} e_2$

$z_{e_n} = b_n + \mathsf{ch} e_n$

How does the combined NIZKP works?

$a_1, \{b_i\}_{i\in[n]} \xleftarrow{\$} \mathbb{Z}_p$

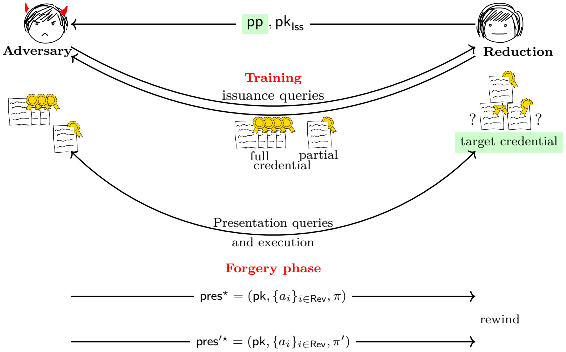
commit and release

$$\begin{tikzcd}
(r, e_1), \tilde{B}_1 = C(a_1)^r \overline{A}^{-e_1} \arrow[d] & & e_2, \tilde{B}_2 = \overline{A}^{-e_2} \arrow[d] & & e_n, \tilde{B}_n = \overline{A}^{-e_n} \arrow[d] \\
U_1 = C(a_1)^{a_1} \overline{A}^{b_1} \arrow[drr, "✉"] & & U_2 = \overline{A}^{b_2} \arrow[d, "✉"] & & U_n = \overline{A}^{b_n} \arrow[dll, "✉"'] \\
& & U = \prod_{i=1}^n U_i \arrow[d] & & \\
& & \mathsf{ch} = H(U, a_1, \mathsf{pk}_{\mathsf{Iss}}, \mathsf{nonce}) \arrow[dll] \arrow[d] \arrow[drr] & & \\
z_r = a_1 + \mathsf{ch} r & & z_{e_2} = b_2 + \mathsf{ch} e_2 \arrow[dd] & & z_{e_n} = b_n + \mathsf{ch} e_n \arrow[ddll] \\
z_{e_1} = b_1 + \mathsf{ch} e_1 \arrow[drr] & & & & \\
& & z_r, z_e \leftarrow \sum_{i=1}^n z_{e_i} & &
\end{tikzcd}$$

Unforgeability of BBS MHAC

How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



pp, $\mathsf{pk}_{\mathsf{Iss}}$

Adversary

Reduction

Training

issuance queries

full credential

partial credential

? ?

target credential

Presentation queries and execution

Forgery phase

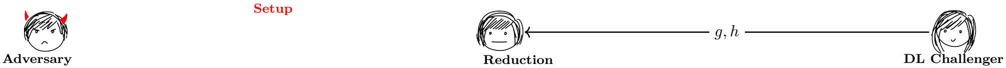
$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi)$

rewind

$\mathsf{pres}'^\star = (\mathsf{pk}, \{a_i\}_{i\in\mathsf{Rev}}, \pi')$

How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



Setup

Adversary

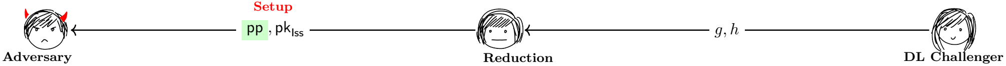
Reduction

g, h

DL Challenger

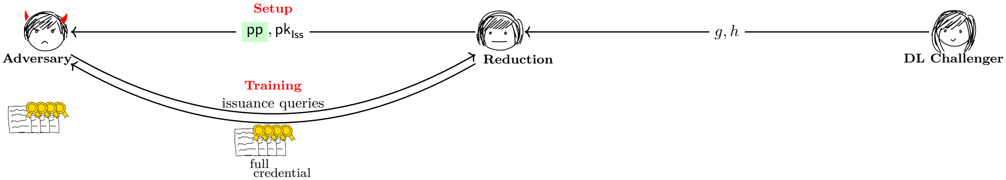
How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



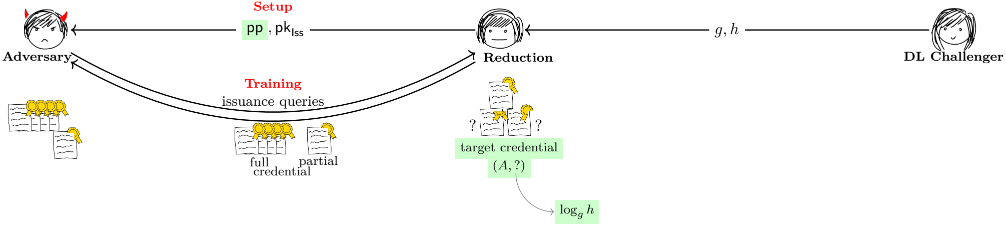
How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



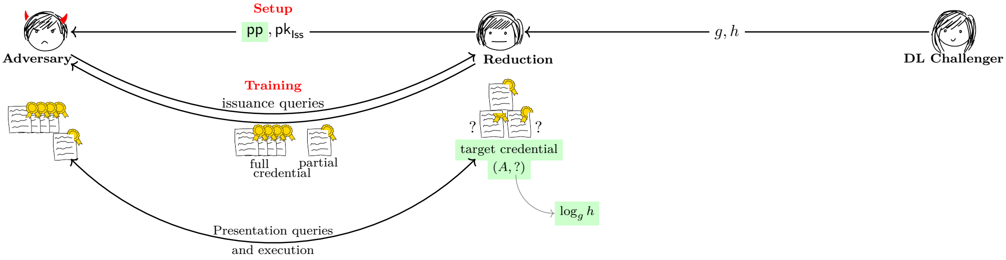
How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

DL Challenger

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

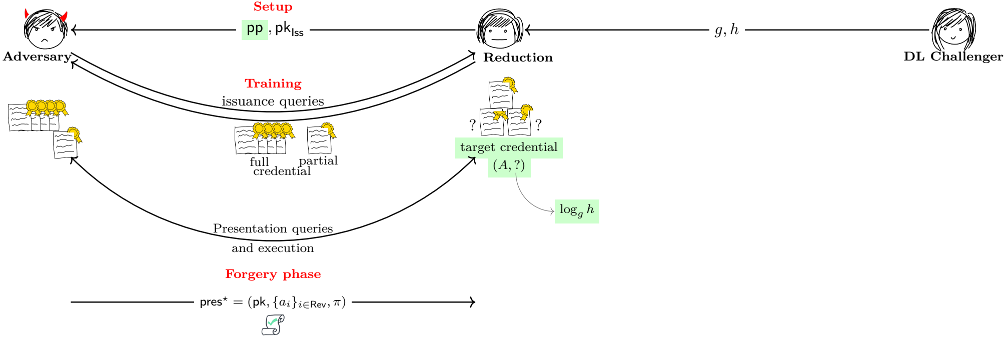
$\log_g h$

Presentation queries

and execution

How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

DL Challenger

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

$\log_g h$

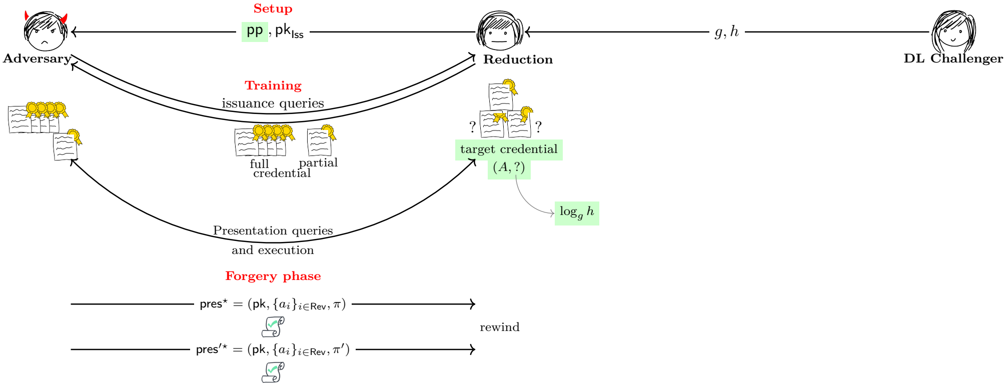
Presentation queries and execution

Forgery phase

$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi)$

How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

DL Challenger

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

$\log_g h$

Presentation queries

and execution

Forgery phase

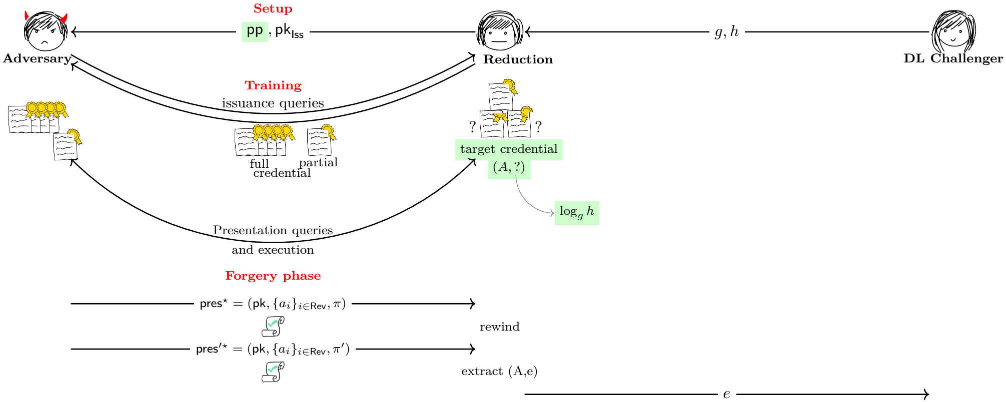
$\mathsf{pres}^\star = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi)$

rewind

$\mathsf{pres}'^\star = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi')$

How to prove Unforgeability of Presentations?

Via a reduction to DL assumption (and the unforgeability of BBS)



Setup

pp, $\mathsf{pk}_{\mathsf{Iss}}$

g, h

Adversary

Reduction

DL Challenger

Training

issuance queries

full credential

partial

? ?

target credential

$(A, ?)$

$\log_g h$

Presentation queries

and execution

Forgery phase

$\mathsf{pres}^{\star} = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi)$

rewind

$\mathsf{pres}'^{\star} = (\mathsf{pk}, \{a_i\}_{i \in \mathsf{Rev}}, \pi')$

extract (A,e)

e

A technical challenge

target credential issuance

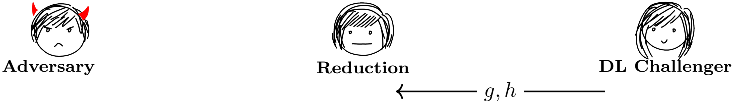
Adversary

Reduction

DL Challenger

A technical challenge

target credential issuance



Adversary

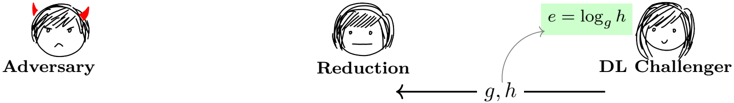
Reduction

DL Challenger

$\xleftarrow{\quad g, h \quad}$

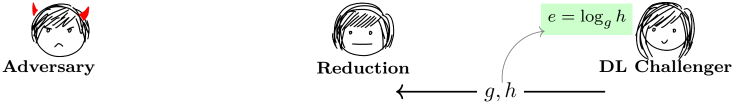
A technical challenge

target credential issuance



A technical challenge

target credential issuance


Adversary

Reduction

DL Challenger

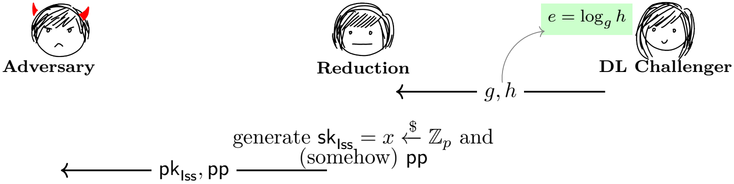
$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

generate $\mathsf{sk}_{\mathsf{Iss}} = x \overset{\$}{\leftarrow} \mathbb{Z}_p$ and
(somehow) pp

A technical challenge

target credential issuance



Adversary

Reduction

$e = \log_g h$

DL Challenger

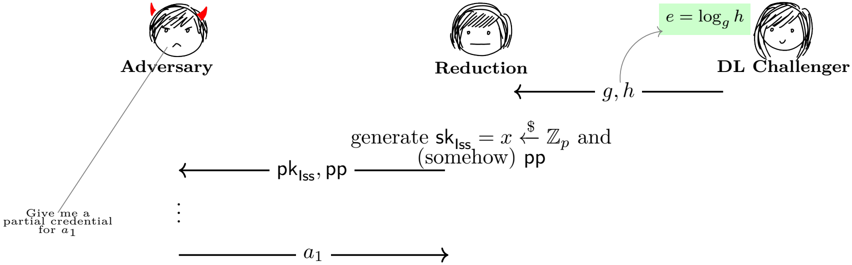
$\longleftarrow g, h \longrule$

generate $\mathsf{sk}_{\mathsf{Iss}} = x \xleftarrow{\$} \mathbb{Z}_p$ and (somehow) pp

$\longleftarrow \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp}$

A technical challenge

target credential issuance



Adversary

Reduction

$e = \log_g h$

DL Challenger

$\xleftarrow{\quad g, h \quad}$

generate $\mathsf{sk}_{\mathsf{Iss}} = x \xleftarrow{\$} \mathbb{Z}_p$ and
(somehow) pp

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

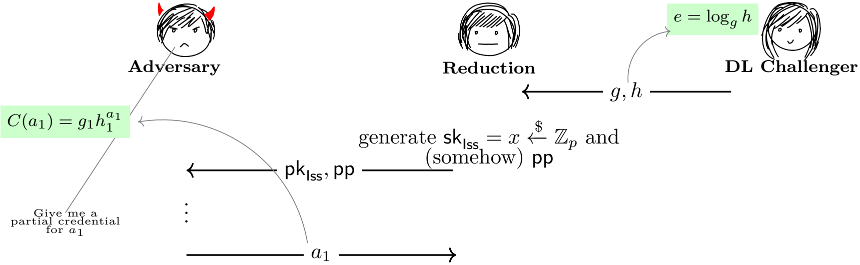
$\vdots$

Give me a
partial credential
for a_1

$\xrightarrow{\quad a_1 \quad}$

A technical challenge

target credential issuance



Adversary

Reduction

DL Challenger

$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

generate $\mathsf{sk}_{\mathsf{Iss}} = x \xleftarrow{\$} \mathbb{Z}_p$ and (somehow) pp

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$\vdots$

$\xrightarrow{\quad a_1 \quad}$

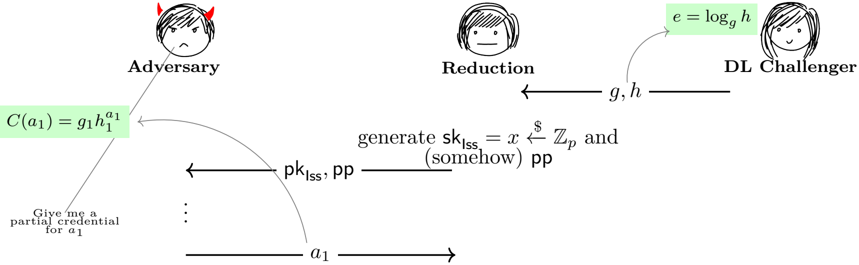
$C(a_1) = g_1 h_1^{a_1}$

Give me a partial credential for a_1

$\mathsf{cred} = ((A, e), a_1)$ is univocally determined! $(A = C(a_1)^{\frac{1}{x+e}})$

A technical challenge

target credential issuance



Adversary

Reduction

DL Challenger

$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

generate $\mathsf{sk}_{\mathsf{Iss}} = x \xleftarrow{\$} \mathbb{Z}_p$ and (somehow) pp

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$C(a_1) = g_1 h_1^{a_1}$

Give me a partial credential for a_1

⋮

$\xrightarrow{\quad a_1 \quad}$

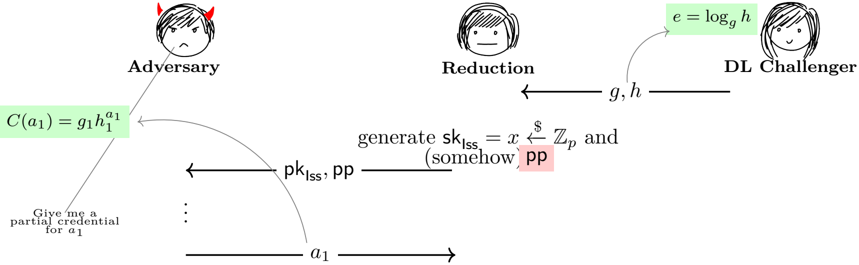
$\mathsf{cred} = ((A, e), a_1)$ is univocally determined! $(A = C(a_1)^{\frac{1}{x+e}})$

The reduction must produce A, A^e

recall: $\mathsf{cred}_i \leftarrow (A, e_i, \{A^{e_i}\}_{i \in [n]}, a_1)$

A technical challenge

target credential issuance



Adversary

Reduction

$e = \log_g h$ **DL Challenger**

$\xleftarrow{\quad g, h \quad}$

generate $\mathsf{sk}_{\mathsf{Iss}} = x \xleftarrow{\$} \mathbb{Z}_p$ and (somehow) pp

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$\vdots$

$\xrightarrow{\quad a_1 \quad}$

$C(a_1) = g_1 h_1^{a_1}$

Give me a partial credential for a_1

$\mathsf{cred} = ((A, e), a_1)$ is univocally determined! $(A = C(a_1)^{\frac{1}{x+e}})$

The reduction must produce A, A^e

recall: $\mathsf{cred}_i \leftarrow (A, e_i, \{A^{e_i}\}_{i \in [n]}, a_1)$

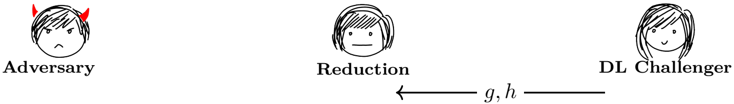
Our Solution

Adversary

Reduction

DL Challenger

Our Solution



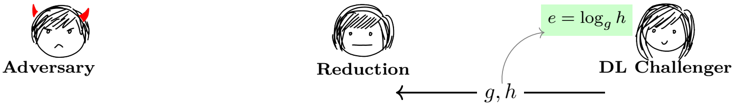
Adversary

Reduction

DL Challenger

$\xleftarrow{\quad g, h \quad}$

Our Solution



Our Solution

Adversary

Reduction

$e = \log_g h$

DL Challenger

$$\xleftarrow{\quad g, h \quad}$$

$$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{lss}} \leftarrow g_2^x$$

Our Solution

Adversary

Reduction

$e = \log_g h$

DL Challenger

$$\xleftarrow{\quad g, h \quad}$$

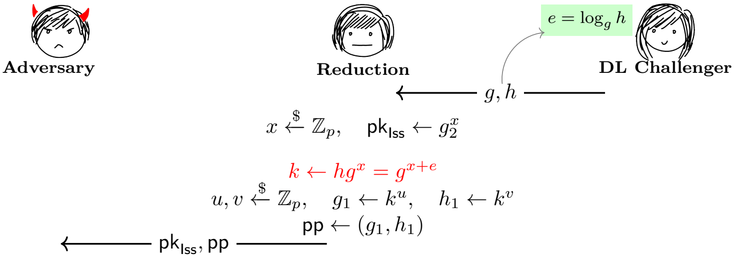
$$x \overset{\$}{\leftarrow} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{lss}} \leftarrow g_2^x$$

$$k \leftarrow hg^x = g^{x+e}$$

$$u, v \overset{\$}{\leftarrow} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$$

$$\mathsf{pp} \leftarrow (g_1, h_1)$$

Our Solution



Adversary

Reduction

DL Challenger

$e = \log_g h$

g, h

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

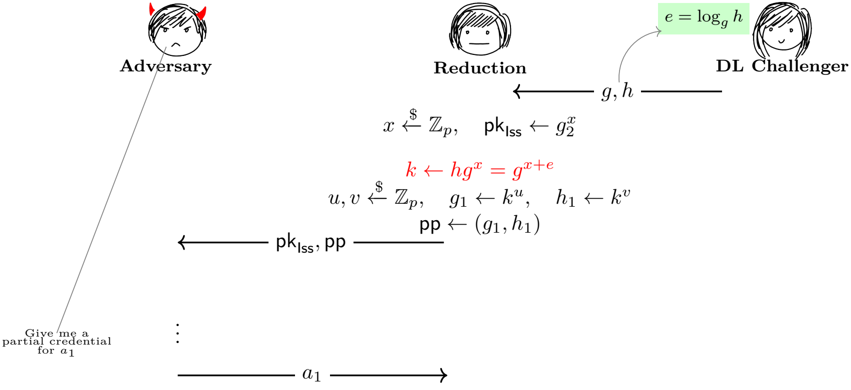
$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

$\mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp}$

Our Solution



Adversary

Reduction

DL Challenger

$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

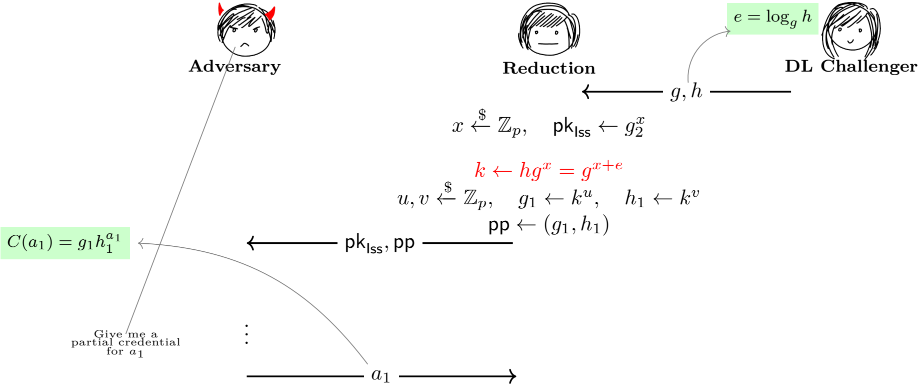
$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

Give me a partial credential for a_1

$\vdots$

$\xrightarrow{\quad a_1 \quad}$

Our Solution



Adversary

Reduction

DL Challenger

$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$C(a_1) = g_1 h_1^{a_1}$

Give me a partial credential for a_1

⋮

$\xrightarrow{\quad a_1 \quad}$

Our Solution

Adversary

Reduction

DL Challenger

$e = \log_g h$

$$\xleftarrow{\quad g, h \quad}$$

$$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$$

$$k \leftarrow hg^x = g^{x+e}$$

$$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$$

$$\mathsf{pp} \leftarrow (g_1, h_1)$$

$$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$$

$C(a_1) = g_1 h_1^{a_1}$

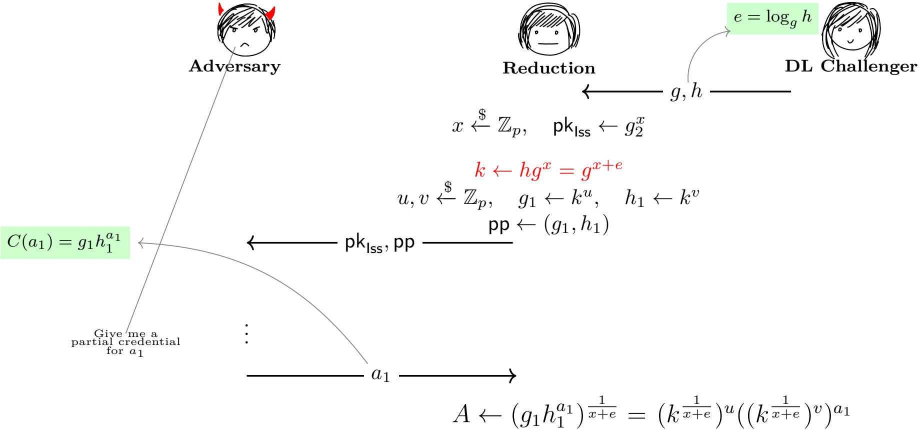
Give me a partial credential for a_1

$\vdots$

$$\xrightarrow{\quad a_1 \quad}$$

$$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = (k^u (k^v)^{a_1})^{\frac{1}{x+e}}$$

Our Solution



$e = \log_g h$

Adversary

Reduction

DL Challenger

$\xleftarrow{\quad g, h \quad}$

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

$C(a_1) = g_1 h_1^{a_1}$

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$\vdots$

Give me a partial credential for a_1

$\xrightarrow{\quad a_1 \quad}$

$$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = (k^{\frac{1}{x+e}})^u((k^{\frac{1}{x+e}})^v)^{a_1}$$

Our Solution

Adversary

Reduction

$e = \log_g h$

DL Challenger

$\xleftarrow{\quad g, h \quad}$

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

$C(a_1) = g_1 h_1^{a_1}$

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$k^{\frac{1}{x+e}} = g$

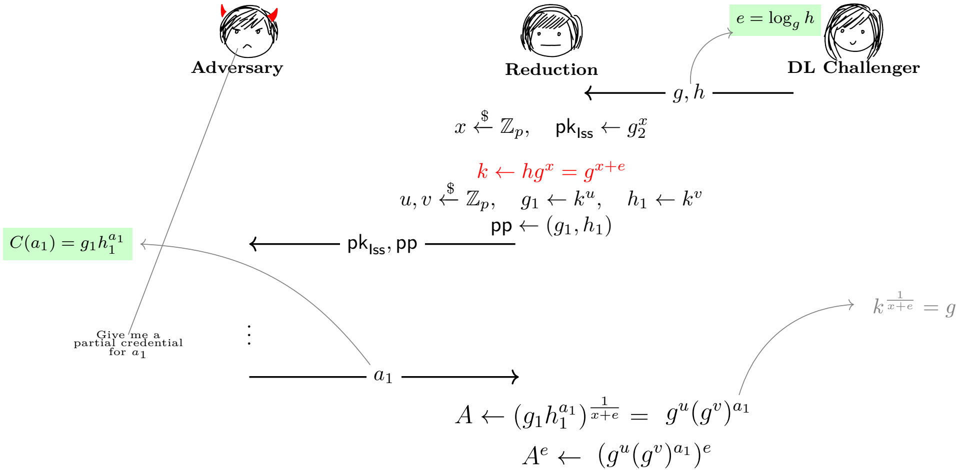
Give me a partial credential for a_1

⋮

$\xrightarrow{\quad a_1 \quad}$

$$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = (k^{\frac{1}{x+e}})^u((k^{\frac{1}{x+e}})^v)^{a_1}$$

Our Solution



Adversary

Reduction

DL Challenger

$e = \log_g h$

$$\xleftarrow{\quad g, h \quad}$$

$$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$$

$$k \leftarrow hg^x = g^{x+e}$$

$$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$$

$$\mathsf{pp} \leftarrow (g_1, h_1)$$

$$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$$

$C(a_1) = g_1 h_1^{a_1}$

$\vdots$

Give me a partial credential for a_1

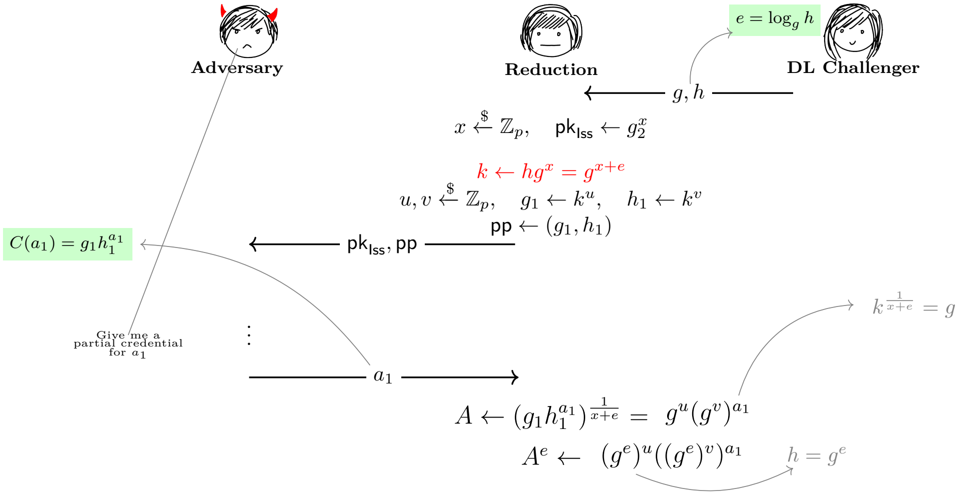
$$\xrightarrow{\quad a_1 \quad}$$

$$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = g^u (g^v)^{a_1}$$

$$A^e \leftarrow (g^u (g^v)^{a_1})^e$$

$k^{\frac{1}{x+e}} = g$

Our Solution



Adversary

Reduction

DL Challenger

$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

$C(a_1) = g_1 h_1^{a_1}$

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

$\vdots$

Give me a partial credential for a_1

$\xrightarrow{\quad a_1 \quad}$

$k^{\frac{1}{x+e}} = g$

$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = g^u (g^v)^{a_1}$

$A^e \leftarrow (g^e)^u((g^e)^v)^{a_1}$

$h = g^e$

Our Solution

Adversary

Reduction

$e = \log_g h$

DL Challenger

$$\xleftarrow{\quad g, h \quad}$$

$$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$$

$$k \leftarrow hg^x = g^{x+e}$$

$$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$$

$$\mathsf{pp} \leftarrow (g_1, h_1)$$

$C(a_1) = g_1 h_1^{a_1}$

$$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$$

$\vdots$

Give me a partial credential for a_1

$$\xrightarrow{\quad a_1 \quad}$$

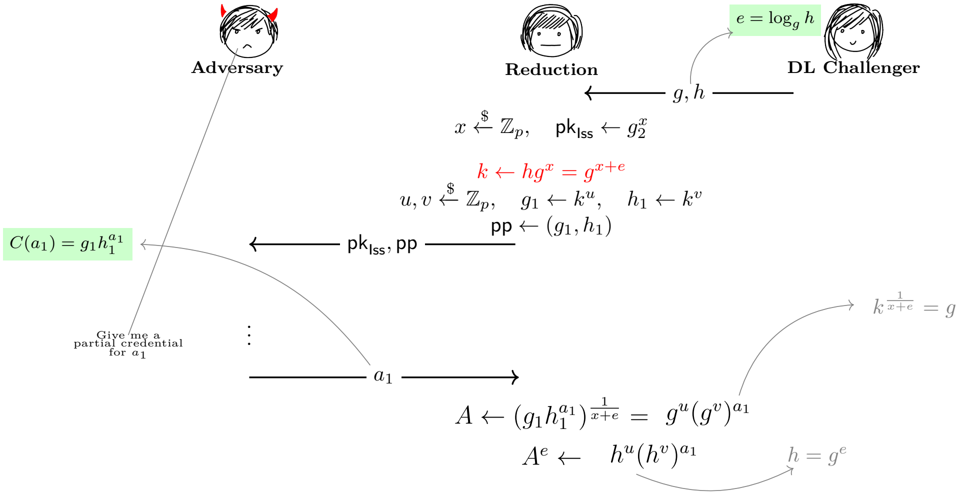
$$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = g^u (g^v)^{a_1}$$

$k^{\frac{1}{x+e}} = g$

$$A^e \leftarrow h^u (h^v)^{a_1}$$

$h = g^e$

Our Solution



Adversary

Reduction

DL Challenger

$e = \log_g h$

$\xleftarrow{\quad g, h \quad}$

$x \xleftarrow{\$} \mathbb{Z}_p, \quad \mathsf{pk}_{\mathsf{Iss}} \leftarrow g_2^x$

$k \leftarrow hg^x = g^{x+e}$

$u, v \xleftarrow{\$} \mathbb{Z}_p, \quad g_1 \leftarrow k^u, \quad h_1 \leftarrow k^v$

$\mathsf{pp} \leftarrow (g_1, h_1)$

$C(a_1) = g_1 h_1^{a_1}$

$\xleftarrow{\quad \mathsf{pk}_{\mathsf{Iss}}, \mathsf{pp} \quad}$

Give me a partial credential for a_1

⋮

$\xrightarrow{\quad a_1 \quad}$

$k^{\frac{1}{x+e}} = g$

$A \leftarrow (g_1 h_1^{a_1})^{\frac{1}{x+e}} = g^u (g^v)^{a_1}$

$A^e \leftarrow h^u (h^v)^{a_1}$

$h = g^e$

The adversary shares are $(A, \{e_i\}_{i \in \mathsf{cor}}, \{A^{e_i}\}_{i \in [n]}, a_1)$