Revisiting Keyed-Verification Anonymous Credentials Michele Orrù, CNRS





Authentication protocols



Authentication protocols

















Present





Present



- 2023. draft-irtf-cfrg-bbs-signatures
- 2024. draft-kalos-bbs-blind-signatures
- 2024. draft-kalos-bbs-per-verifier-linkability
- 2024. draft-ladd-privacypass-bbs
- 2025. draft-yun-cfrg-arc
- 2025. <u>draft-google-cfrg-libzk</u>



Present





























Age verification system for access to online content





Figure 4. General flow: Evidence



















! Credentials can be based on one-way functions.



Credentials can be based on one-way functions.



In practice, one can also build a credential system with an accumulator and a cryptographic proof. See e.g. semaphore.dev.













l credential engineers are on their own





l credential engineers are on their own

These systems are already deployed!

Contribution

- 1. Modular view of credentials + extensions.
- 2. New schemes: μ BBS (BBS MAC) and μ CMZ (PS MAC).



First contribution

Modular view of credentials + extensions.



Extensions

What can be built on top of selective disclosure of attributes.

Expiry

The user has a timestamp attribute that is not expired.

Pseudonyms

The user can access a new resource with an ephemeral identity. $url \leftrightarrow identity$

Metadata

Assign some attributes to the user.

The user can access a resource at most N times.

Issuer-hiding

The user can access a new resource with a new ephemeral identity.

Rate-Limiting

Revocation

The user is not in a blocklist.



[malicious user] **Unforgeability**



[malicious user] **Unforgeability**

[malicious issuer] Anonymity

- covers both issuance and presentation
- computationally unbounded adversaries



[malicious user]

Extractability

- extract from issuance and presentation
- man-in-the middle adversaries
- stronger guarantees, useful for extensions

[malicious user] **One-more unforgeability**

• forging more messages than allowed • weaker guarantees, useful for tokens

[malicious issuer] Anonymity

- covers both issuance and presentation
- computationally unbounded adversaries



keyed-verification credentials

[malicious user]

Extractability

- extract from issuance and presentation
- man-in-the middle adversaries
- stronger guarantees, useful for extensions

[malicious user] **One-more unforgeability**

• forging more messages than allowed • weaker guarantees, useful for tokens

[malicious issuer] Anonymity

- covers both issuance and presentation
- computationally unbounded adversaries



keyed-verification credentials

[malicious user]

Extractability

- extract from issuance and presentation
- man-in-the middle adversaries
- stronger guarantees, useful for extensions





Second contribution

New schemes: μ BBS (BBS MAC) and μ CMZ (PS MAC).

Definitions

Adapt the security analysis to extractability, one-more unforgeability, anonymity.



Fix inaccuracies in the previous proofs of CMZ and BBS.

Efficiency

Improved efficiency of CMZ to O(1) communication and one less group element for BBS



Upgrade CMZ to statistical anonymity.




Second contribution

New schemes: μ BBS (BBS MAC) and μ CMZ (PS MAC).

Definitions

Adapt the security analysis to extractability, one-more unforgeability, anonymity.



Fix inaccuracies in the previous proofs of CMZ and BBS.

Efficiency

Improved efficiency of CMZ to O(1) communication and one less group element for BBS





Adapt the security analysis to extractability, one-more unforgeability, anonymity.

Second contribution

New schemes: μ BBS (BBS MAC) and μ CMZ (PS MAC).

Definitions



Fix inaccuracies in the previous proofs of CMZ and BBS.

Efficiency

Improved efficiency of CMZ to O(1) communication and one less group element for BBS





Second contribution

New schemes: μ BBS (BBS MAC) and μ CMZ (PS MAC).

Definitions

Adapt the security analysis to extractability, one-more unforgeability, anonymity.



Fix inaccuracies in the previous proofs of CMZ and BBS.

Efficiency

Improved efficiency of CMZ to O(1) communication and one less group element for BBS





Second contribution

New schemes: μ BBS (BBS MAC) and μ CMZ (PS MAC).

Definitions

Adapt the security analysis to extractability, one-more unforgeability, anonymity.



Fix inaccuracies in the previous proofs of CMZ and BBS.

Efficiency

Improved efficiency of CMZ to O(1) communication and one less group element for BBS





	Public parameters	Credential
CMZ	(n+1)g	2 <i>g</i>
BBDT	g	$g + 2\lambda$

 λ is the security parameter. *n* is the number of attributes that the user has. g is the size of a group element. $|\pi|$ the size of the zero-knowledge proof.



sizeIssuancePresentation
$$(2n+1)g + |\pi|$$
 $(n+2)g + |\pi|$ $g + |\pi|$ $2g + |\pi|$

Efficiency of the old schemes

	Public parameters	Credential
μCMZ	(n + 2)g	2g
μBBS	g	$g + 2\lambda$

 λ is the security parameter. n is the number of attributes that the user has. g is the size of a group element. $|\pi|$ the size of the zero-knowledge proof.





	Public parameters	Credential
μCMZ	(n + 2)g	2g
μBBS	g	$g + 2\lambda$

 λ is the security parameter. n is the number of attributes that the user has. g is the size of a group element. $|\pi|$ the size of the zero-knowledge proof.





	Public parameters	Credential size	Issuance	Presentation
	$7 \qquad (n + 2)$	7 a		(m + 2) = 1 = 1
$\mu CIVIZ$	$\angle (n + 2)g$	$\angle g$	$g + \pi $	$(n + 2)g + \pi $
μBBS	8	$g + 2\lambda$	$g + \pi $	$2g + \pi $
μCMZ _{AT}	(n+2)g	2 <i>g</i>	8	$(n+2)g + \pi $
μBBS_{AT}	8	$g + 2\lambda$	8	$2g + \pi $

	Public parameters	Credential size	Issuance	Presentation
μCMZ	(n + 2)g	2 <i>g</i>	$g + \pi $	$(n+2)g + \pi $
μBBS	8	$g + 2\lambda$	$g + \pi $	$2g + \pi $
uCMZ _{AT}	(n + 2)g	2 <i>g</i>	8	$(n+2)g + \pi $
μBBS_{AT}	g	$g + 2\lambda$	8	$2g + \pi $
				μCMZ better for $n \leq 2$

	Unforgeability
CMZ	GGM
BBDT	q-SDH

Security of the old schemes

Anonymity

DDH

	Extractability
μCMZ	3-DL
μBBS	(q + 2)-DL

q-DL: given G

Best attack:

q is the number of series to the signing oracle.

My contribution: security

Anonymity

statistical

$$G, xG, ..., x^{q}G \text{ compute } x.$$

 $O\left(\sqrt{q} + \sqrt{(p \pm 1)/q}\right).$

	Extractability
μCMZ	3-DL
μBBS	(q + 2)-DL

q-DL: given G

Best attack:

q is the number of series to the signing oracle.

My contribution: security

Anonymity

statistical

$$G, xG, ..., x^{q}G \text{ compute } x.$$

 $O\left(\sqrt{q} + \sqrt{(p \pm 1)/q}\right).$

	Extractability
μCMZ	3-DL
μBBS	(q + 2)-DL

q-DL: given G

Best attack:

q is the number of series to the signing oracle.

My contribution: security

Anonymity

statistical

$$G, xG, ..., x^{q}G$$
 compute x .
 $O\left(\sqrt{q} + \sqrt{(p \pm 1)/q}\right).$





Construct an algebraic MAC

- correctness,
- unforgeability



Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic)



Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic)

Proof $ZKP\{(sk, \sigma): verify(sk, m, \sigma) = 1\}$



Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic) with public parameters

Proof $ZKP\{(sk, \sigma): verify(sk, m, \sigma) = 1 \land pp = Com(sk)\}^*$



Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic) with public parameters and validity oracle

Proof $ZKP\{(sk, \sigma): \text{ verify}(sk, m, \sigma) = 1 \land pp = Com(sk)\}^*$ $ZKP\{(m, \sigma): \text{ verify}(sk, m, \sigma) = 1\}$



Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic) with public parameters and validity oracle

Proof

$\mathsf{ZKP}\{(\mathsf{sk},\sigma): \mathsf{verify}(\mathsf{sk},m,\sigma)=1 \land \mathsf{pp}=\mathsf{Com}(\mathsf{sk})\}^*$ $\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$

Blind issuance and presentation

- issue a MAC over blind attributes
- prove that a MAC is correctly issued
- allow for arbitrary additional predicates to be proven

Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic) with public parameters and validity oracle

Proof

$\mathsf{ZKP}\{(\mathsf{sk},\sigma): \mathsf{verify}(\mathsf{sk},m,\sigma)=1 \land \mathsf{pp}=\mathsf{Com}(\mathsf{sk})\}^*$ $\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$

Blind issuance and presentation

- issue a MAC over blind attributes
- prove that a MAC is correctly issued
- allow for arbitrary additional predicates to be proven

Extension

Construct an algebraic MAC

- correctness,
- unforgeability (probabilistic) with public parameters and validity oracle

Proof

$\mathsf{ZKP}\{(\mathsf{sk},\sigma): \mathsf{verify}(\mathsf{sk},m,\sigma) = 1 \land \mathsf{pp} = \mathsf{Com}(\mathsf{sk})\}^*$ $\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$

Blind issuance and presentation

- issue a MAC over blind attributes
- prove that a MAC is correctly issued
- allow for arbitrary additional predicates to be proven

Extension

Set a predicate to be used within a credential system

Overview of our scheme for n = 1 attributes.

Secret key

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1. sk =
$$(x_0, x_1) \leftarrow \mathbb{Z}_p$$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m \right) U \right)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1. sk =
$$(x_0, x_1) \leftarrow \mathbb{Z}_p$$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m\right)U\right)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1. sk =
$$(x_0, x_1) \leftarrow \mathbb{Z}_p$$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m\right)U\right)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1. sk =
$$(x_0, x_1) \leftarrow \mathbb{Z}_p$$

MAC for $m \in \mathbb{Z}_p$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m\right)U\right)$

Unforgeability (AGM) $u, \quad u \cdot (x_0 + m \cdot x_1)$

e authentication code
oroof system
dential system
extensions

Overview of our scheme for n = 1 attributes.

Secret key

1. sk =
$$(x_0, x_1) \leftarrow \mathbb{Z}_p$$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m\right)U\right)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1. sk =
$$(x_0, x_1) \leftarrow \mathbb{Z}_p$$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m\right)U\right)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H + x_rG, X_1 = x_1G)$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m \right) U \right)$

Unforgeability (AGM)
h,
$$x_0h + x_r$$

u, $u \cdot (x_0 + m \cdot x_1)$
u', $u' \cdot (x_0 + m' \cdot x_1)$
 \vdots
 u^* , $u^* \cdot (x_0 + m^* \cdot x_1)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H + x_rG, X_1 = x_1G)$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m \right) U \right)$

Unforgeability (AGM)
h,
$$x_0h + x_r$$

u, $u \cdot (x_0 + m \cdot x_1)$
u', $u' \cdot (x_0 + m' \cdot x_1)$
 \vdots
 u^* , $u^* \cdot (x_0 + m^* \cdot x_1)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H + x_rG, X_1 = x_1G)$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_1 m \right) U \right)$

Unforgeability (AGM)
h,
$$x_0h + x_r$$

u, $u \cdot (x_0 + m \cdot x_1)$
u', $u' \cdot (x_0 + m' \cdot x_1)$
 \vdots
 u^* , $u^* \cdot (x_0 + m^* \cdot x_1)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_r + x_1 m \right) U \right)$

Unforgeability (AGM)
h,
$$x_0h$$
, x_r
u, $u \cdot (x_0 + m \cdot x_1)$
u', $u' \cdot (x_0 + m' \cdot x_1)$
 \vdots
 \mathscr{A}
u*, $u^* \cdot (x_0 + m^* \cdot x_1)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_r + x_1 m \right) U \right)$

Unforgeability (AGM)
h,
$$x_0h$$
, x_r
u, $u \cdot (x_0 + m \cdot x_1)$
u', $u' \cdot (x_0 + m' \cdot x_1)$
 \vdots
 \mathscr{A}
u*, $u^* \cdot (x_0 + m^* \cdot x_1)$

entication code
system
al system
nsions

Overview of our scheme for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

1. sample
$$U \leftarrow \mathbb{G}$$

2. return $\left(U, \left(x_0 + x_r + x_1 m \right) U \right)$

Unforgeability (AGM)
h,
$$x_0h$$
, x_r
u, $u \cdot (x_0 + m \cdot x_1)$
u', $u' \cdot (x_0 + m' \cdot x_1)$
 \vdots
 \mathscr{A}
u*, $u^* \cdot (x_0 + m^* \cdot x_1)$

entication code
system
al system
nsions
Overview of our scheme for *n* attributes.

Secret key

1. $sk = (x_0, x_r, x_1, ..., x_n)$ 2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G, ..., X_n = x_nG)$

MAC for $m_1, ..., m_n$

- 1. sample $U \leftarrow \mathbb{G}$
- 2. return $(U, (x_0 + x_r + x_1m_1 + \dots + x_nm_n)U)$



entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 \in \mathbb{G}$

1. sample
$$u \leftarrow \mathbb{Z}_p$$

2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u \right)$



entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 \in \mathbb{G}$

1. sample $u \leftarrow \mathbb{Z}_p$ 2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u \right)$ $= (x_0 + x_r + x_1m)U$



entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 \in \mathbb{G}$

1. sample
$$u \leftarrow \mathbb{Z}_p$$

2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u \right)$



entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1.
$$sk = (x_0, x_r, x_1)$$

2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 \in \mathbb{G}$

1. sample
$$u \leftarrow \mathbb{Z}_p$$

2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u \right)$

One-more unforgeability

Is loose and relies on O(1)-DL

message authentication code	>
proof system	
credential system	
extensions	

One-more unforgeability intuition for n = 1 attributes.

Secret key

1. $sk = (x_0, x_r, x_1, ..., x_n)$ 2. pp = $(X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 + \rho H \in \mathbb{G}$

1. sample $u \leftarrow \mathbb{Z}_p$ 2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u - \rho U\right)$





entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1. $sk = (x_0, x_r, x_1, ..., x_n)$ 2. pp = $(X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 + \rho H \in \mathbb{G}$

1. sample $u \leftarrow \mathbb{Z}_p$ 2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u - \rho U\right)$





entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1. $sk = (x_0, x_r, x_1, ..., x_n)$ 2. pp = $(X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 + \rho H \in \mathbb{G}$

1. sample $u \leftarrow \mathbb{Z}_p$ 2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u - \rho U\right)$





entication code
system
al system
nsions

One-more unforgeability intuition for n = 1 attributes.

Secret key

1. $sk = (x_0, x_r, x_1, ..., x_n)$ 2. $pp = (X_0 = x_0H, X_r = x_rG, X_1 = x_1G)$

MAC for $C = mX_1 + \rho H \in \mathbb{G}$

1. sample $u \leftarrow \mathbb{Z}_p$ 2. return $\left(U = uH, (x_0 + x_r)U + C \cdot u - \rho U \right)$



 μCMZ relies on a single Pedersen commitment.

CMZ relied on ElGamal encryption.

entication code
system
al system
nsions

µCMZ proof systems



µCMZ proof systems

 $\mathsf{ZKP}\{(\mathsf{sk},\sigma): | \mathsf{verify}(\mathsf{sk},m,\sigma) = 1 \land \mathsf{pp} = \mathsf{Com}(\mathsf{sk})\}$





μCMZ proof systems

$ZKP\{(sk, \sigma): verify(sk, m, \sigma) = 1 \land$ $\implies ZKP\{(x_0, x_r, (U, V)): V= U = UH \land x_0 H = X_0$

$$pp = Com(sk) \}$$

$$\land V = (x_0 + x_r)U + uC$$

$$\land x_r G = X_r$$

$$\land x_r G = X_r$$





µCMZ credentials







µCMZ credentials







μCMZ credentials







μCMZ credentials



Extractability: extract attributes



μCMZ credentials





from mac_proof, then simulate presentation_message. 28

$\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$



$\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$ $\implies \mathsf{ZKP}\{(m,\rho): \quad V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\}$ where $\begin{cases} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{cases}$



$\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$ $\implies \mathsf{ZKP}\{(m,\rho): \quad V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\}$ where $\begin{cases} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{cases}$



$\mathsf{ZKP}\{(m,\sigma): \text{ verify}(\mathsf{sk},m,\sigma)=1\}$ $\implies \mathsf{ZKP}\{(m,\rho): \quad V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\}$ where $\begin{cases} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{cases}$



$\begin{aligned} \mathsf{ZKP}\big\{(m,\sigma)\colon & \mathsf{verify}(\mathsf{sk},m,\sigma) = 1\big\} \\ \implies \mathsf{ZKP}\big\{(m,\rho)\colon V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\big\} \\ & \mathsf{where} \left\{ \begin{array}{l} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{array} \right. \end{aligned}$



$\begin{aligned} \mathsf{ZKP}\big\{(m,\sigma)\colon & \mathsf{verify}(\mathsf{sk},m,\sigma) = 1\big\} \\ \implies \mathsf{ZKP}\big\{(m,\rho)\colon V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\big\} \\ & \mathsf{where} \left\{ \begin{array}{l} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{array} \right. \end{aligned}$



$\begin{aligned} \mathsf{ZKP}\big\{(m,\sigma)\colon & \mathsf{verify}(\mathsf{sk},m,\sigma) = 1\big\} \\ \implies \mathsf{ZKP}\big\{(m,\rho)\colon V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\big\} \\ & \mathsf{where} \left\{ \begin{array}{l} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{array} \right. \end{aligned}$

1. The reduction needs help in building the instance to verify the proof!



$\begin{aligned} \mathsf{ZKP}\big\{(m,\sigma)\colon & \mathsf{verify}(\mathsf{sk},m,\sigma) = 1\big\} \\ \implies \mathsf{ZKP}\big\{(m,\rho)\colon V' - (x_0 + x_r)U' - x_1C = \rho H - rX_1\big\} \\ & \mathsf{where} \left\{ \begin{array}{l} C = mU' + rG \\ V' = U' + \rho H \\ U' = \alpha U \end{array} \right. \end{aligned}$

In the reduction needs help in building the instance to verify the proof.
Solution: zkp instance recovery + decision oracle



μCMZ_{AT} credentials







µCMZ_{AT} credentials

Present presentation_message







Rate Limiting

Current solutions:

- Cookies
- Location (GeoIP tracking)
- Internet challenges (captchas)







Rate Limiting

Current solutions:

- Cookies
- Location (GeoIP tracking)
- Internet challenges (captchas)



Rate Limiting

Current solutions:

- Cookies
- Location (GeoIP tracking)
- Internet challenges (captchas)

[malicious user]	[malicious issuel
Unforgeability	Anonymity
Users cannot spend more than allowed.	The user's requests are u



Current approach: batch issuance of many spend-once credentials.







Server issues a credential for a secret PRF key k.

To present the i-th time, the user sends:





Server issues a credential for a secret PRF key k.

To present the i-th time, the user sends:

$$\begin{split} t_i &= \mathsf{PRF}(k,i) \\ \pi &= \mathsf{ZKP} \left\{ \begin{matrix} (k,\sigma,i) \colon & \mathsf{verify}(\mathsf{sk},k,\sigma) = 1 \ \land \\ & \mathsf{PRF}(k,i) = t_i \ \land \ 0 \leq i < \mathsf{MAX} \end{matrix} \right. \end{split}$$



Server issues a credential for a secret PRF key k.

To present the i-th time, the user sends:

$$\begin{split} t_i &= \mathsf{PRF}(k,i) \\ \pi &= \mathsf{ZKP} \begin{cases} (k,\sigma,i) \colon & \mathsf{verify}(\mathsf{sk},k,\sigma) = 1 \land \\ & \mathsf{PRF}(k,i) = t_i \land 0 \leq i < \mathsf{MAX} \end{cases} \end{split}$$


Rate limiting Extension

Server issues a credential for a secret PRF key k.

To present the i-th time, the user sends:

$$\begin{split} t_i &= \mathsf{PRF}(k,i) \\ \pi &= \mathsf{ZKP} \begin{cases} (k,\sigma,i) \colon & \mathsf{verify}(\mathsf{sk},k,\sigma) = 1 \land \\ & \mathsf{PRF}(k,i) = t_i \land 0 \leq i < \mathsf{MAX} \end{cases} \end{split}$$

Server checks t_i has not been already used.



Rate limiting Extension

Server issues a credential for a secret PRF key k.

To present the i-th time, the user sends:

$$\begin{split} t_i &= \mathsf{PRF}(k,i) \\ \pi &= \mathsf{ZKP} \begin{cases} (k,\sigma,i) \colon & \mathsf{verify}(\mathsf{sk},k,\sigma) = 1 \land \\ & \mathsf{PRF}(k,i) = t_i \land 0 \leq i < \mathsf{MAX} \end{cases} \end{split}$$

Server checks t_i has not been already used.

Anonymity

Anonymity of the underlying credential. Pseudorandomness of the PRF.



Rate limiting Extension

Server issues a credential for a secret PRF key k.

To present the i-th time, the user sends:

$$\begin{split} t_i &= \mathsf{PRF}(k,i) \\ \pi &= \mathsf{ZKP} \begin{cases} (k,\sigma,i) \colon & \mathsf{verify}(\mathsf{sk},k,\sigma) = 1 \land \\ & \mathsf{PRF}(k,i) = t_i \land 0 \leq i < \mathsf{MAX} \end{cases} \end{split}$$

Server checks t_i has not been already used.

Anonymity

Anonymity of the underlying credential. Pseudorandomness of the PRF.

Unforgeability

One-more unforgeability suffices.





Pseudorandomness holds under q-DDHI assumption for i in a small space.





Pseudorandomness holds (in the random oracle model) under q-DDHI assumption for i in a small space. The message $m \in \{0,1\}^*$ can be from an arbitrarily large space!



















More in the paper:







More in the paper:

• analysis of μBBS







More in the paper:

- analysis of μBBS
- other extensions
 expiry, pseudonyms, public metadata, attribute randomization







More in the paper:

- analysis of μBBS
- other extensions
 expiry, pseudonyms, public metadata, attribute randomization
- other proof systems constant-size range proofs without pairings







Revisiting Keyed-Verification Anonymous Credentials





