Rate-Limited Tokens (Anonymous Credentials)

Victor Youdom Kemmoe Anna Lysyanskaya Ngoc Khanh Nguyen



KING'S College LONDON

2026-10-28 @ NIST WPEC 2026

Motivation

Rate-Limited Access



Bob

Article ; cookie / account ID = Bob

Article, if count[Bob] $< N$



News Outlet

reader	reads
Bob	$3/N$
Alice	N/N
Carol	$1/N$

Motivation

Rate-Limited Access



Bob

Article ; cookie / account ID = Bob

Article, if count[Bob] $< N$



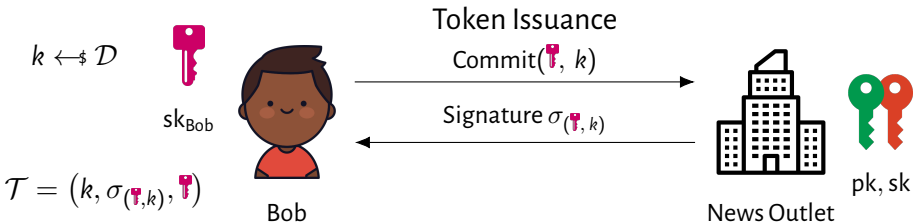
News Outlet

reader	reads
Bob	$3/N$
Alice	N/N
Carol	$1/N$

News Outlet knows *who* the user is.

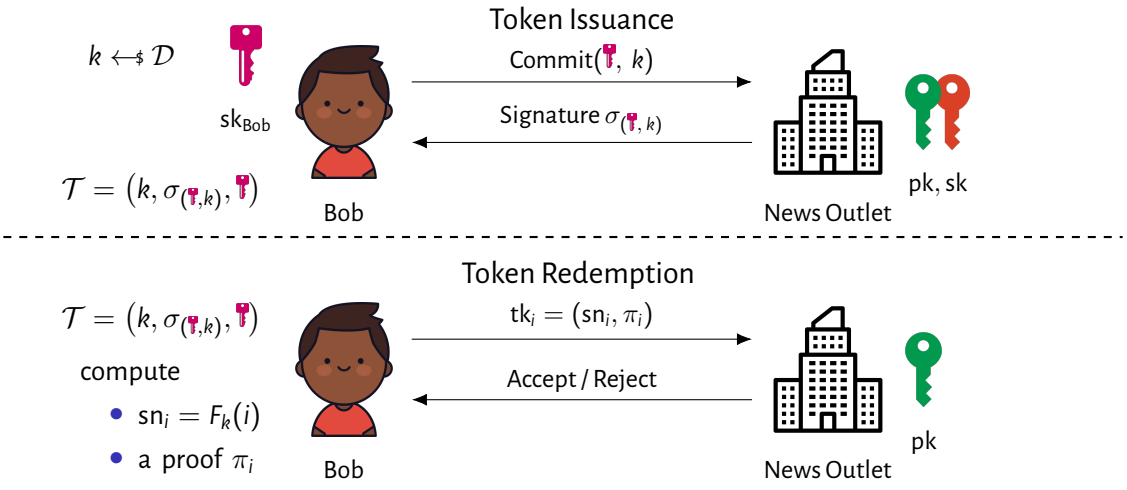
Anonymous Rate-Limited Tokens

[CHL05; CHK+06; CDL+25]



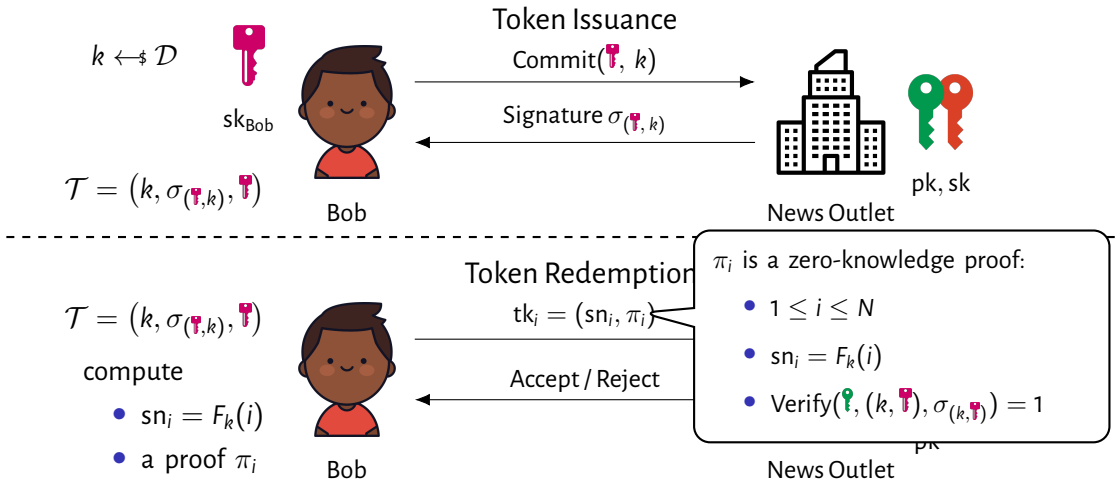
Anonymous Rate-Limited Tokens

[CHL05; CHK+06; CDL+25]



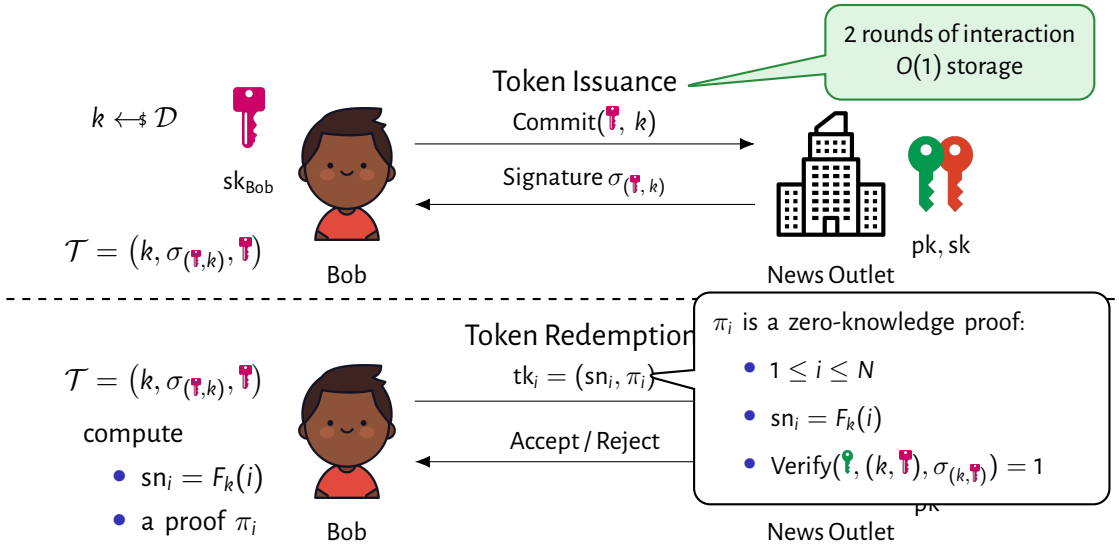
Anonymous Rate-Limited Tokens

[CHL05; CHK+06; CDL+25]



Anonymous Rate-Limited Tokens

[CHL05; CHK+06; CDL+25]



Anonymous Rate-Limited Tokens

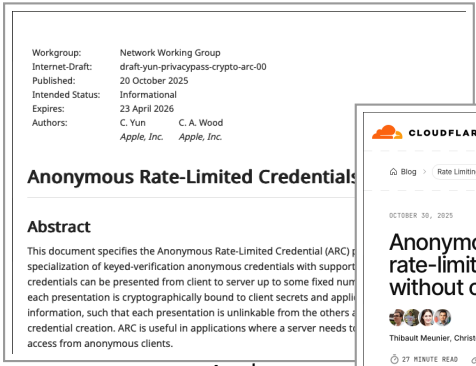
[CHL05; CHK+06; CDL+25]

- **Anonymity**: Tokens are unlinkable to each other and to issuance.
- **Soundness/ One-more Unforgeability**: A user cannot redeem more than N distinct tokens.
- **Exculpability**: Honest users can never be framed for double-spending.
- **Linkability**: We can always recover the identity of a double spender.

Double-spending occurs if we have $\mathsf{tk}_i = (\mathsf{sn}_i, \pi_i)$, $\mathsf{tk}_j = (\mathsf{sn}_j, \pi_j)$ such that $\mathsf{sn}_i = \mathsf{sn}_j$

Anonymous Rate-Limited Tokens

Applications



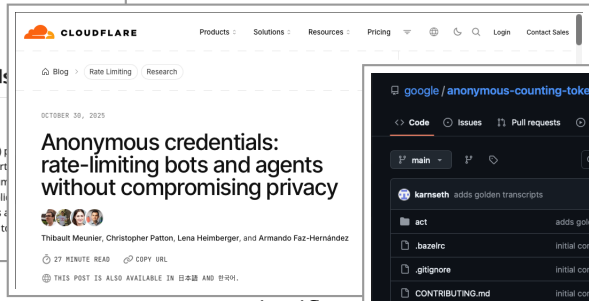
Workgroup: Network Working Group
Internet-Draft: draft-yun-privacypass-crypto-arc-00
Published: 20 October 2025
Intended Status: Informational
Expires: 23 April 2026
Authors: C. Yun (*Apple, Inc.*) C. A. Wood (*Apple, Inc.*)

Anonymous Rate-Limited Credentials

Abstract

This document specifies the Anonymous Rate-Limited Credential (ARC) p
specialization of keyed-verification anonymous credentials with support
credentials can be presented from client to server up to some fixed num
each presentation is cryptographically bound to client secrets and appli
information, such that each presentation is unlinkable from the others
credential creation. ARC is useful in applications where a server needs t
access from anonymous clients.

Apple



CLOUDFLARE Products Solutions Resources Pricing Login Contact Sales

Blog › Rate Limiting Research

OCTOBER 30, 2025

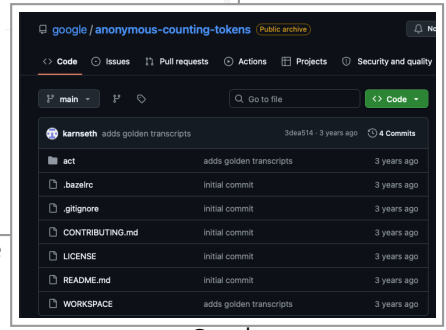
Anonymous credentials: rate-limiting bots and agents without compromising privacy

Thibault Meunier, Christopher Patton, Lena Heimberger, and Armando Faz-Hernández

27 MINUTE READ COPY URL

THIS POST IS ALSO AVAILABLE IN 日本語 AND 한국어.

Cloudflare



google / anonymous-counting-tokens Public archive

Code Issues Pull requests Actions Projects Security and quality

main Go to file Code

karnseth adds golden transcripts 3dea514 · 3 years ago 4 Commits

act	adds golden transcripts	3 years ago
.bazelrc	initial commit	3 years ago
.gitignore	initial commit	3 years ago
CONTRIBUTING.md	initial commit	3 years ago
LICENSE	initial commit	3 years ago
README.md	initial commit	3 years ago
WORKSPACE	adds golden transcripts	3 years ago

Google

Anonymous Rate-Limited Tokens

Prior Works vs. Ours

Scheme	**Token Size** (Estimate)	**Anonymity**	**Assumptions**
[CHL05]	$<$ 50KB	Computational	ROM + Strong DDH Inversion
[CDL+25]	$<$ 50 KB	Unconditional	GGM + q-ARSDH + SXDH
[BCK+09]	$<$ 50 KB	Computational	DLIN + Strong DDH Inversion + Triple DH
[LN26]	$<$ 50 KB	Computational	GGM + Strong DH Inversion
[LLN+17; DLN+20]	$>$ 3 MB* Unless you use a SNARG	Computational	ROM + LWE + SIS

- ROM: Random Oracle Model
- GGM: Generic Group Model
- ARSDH: adaptive Rational Strong DH

Anonymous Rate-Limited Tokens

Prior Works vs. Ours

Scheme	**Token Size** (Estimate)	**Anonymity**	**Assumptions**
[CHL05]	$<$ 50KB	Computational	ROM + Strong DDH Inversion
[CDL+25]	$<$ 50 KB	Unconditional	GGM + q-ARSDH + SXDH
[BCK+09]	$<$ 50 KB	Computational	DLIN + Strong DDH Inversion + Triple DH
[LN26]	$<$ 50 KB	Computational	GGM + Strong DH Inversion
[LLN+17; DLN+20]	$>$ 3 MB* Unless you use a SNARG	Computational	ROM + LWE + SIS
Ours	$<$ 1 MB* For N=256	Computational	ROM + LWE + SIS

- ROM: Random Oracle Model
- GGM: Generic Group Model
- ARSDH: adaptive Rational Strong DH

Anonymous Rate-Limited Tokens

Prior Works vs. Ours

Scheme	Token Size (Estimate)	Anonymity	Assumptions
[CHL05]	$<$ 50KB	Computational	ROM + Strong DDH Inversion
[CDL+25]	$<$ 50 KB	Unconditional	GGM + q-ARSDH + SXDH
[BCK+09]	$<$ 50 KB	Computational	DLIN + Strong DDH Inversion + Triple DH
[LN26]	$<$ 50 KB	Computational	GGM + Strong DH Inversion
[LLN+17; DLN+20]		mputational	ROM + LWE + SIS
Ours	For N=256	omputational	ROM + LWE + SIS

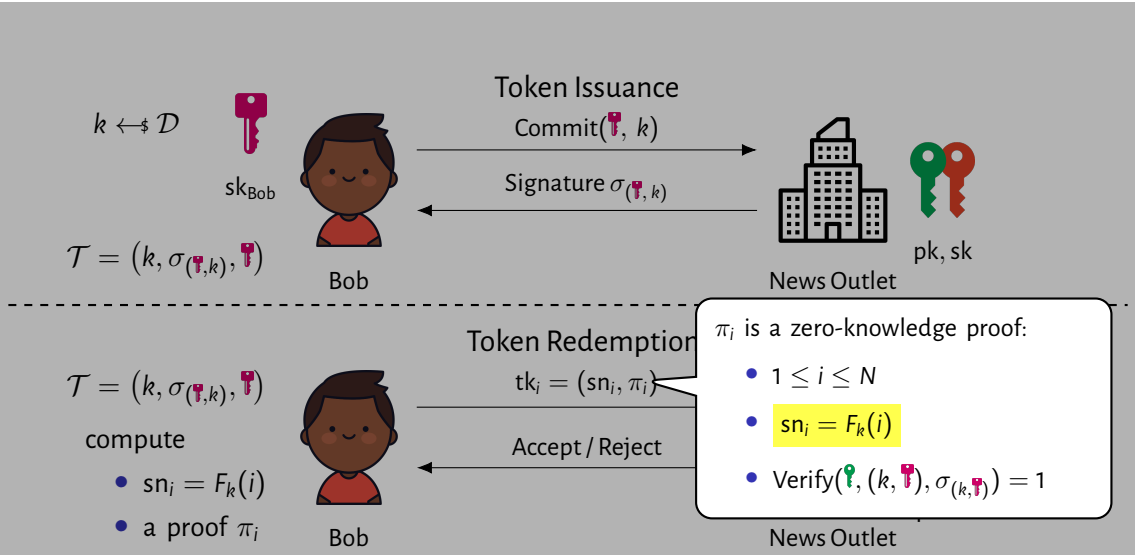
Focus:

- Linkability
- Soundness

- ROM: Random Oracle Model
- GGM: Generic Group Model
- ARSDH: adaptive Rational Strong DH

Our Construction: Lattice-Based Rate-Limited Tokens

Pseudo-Random Function Issues



Our Construction: Lattice-Based Rate-Limited Tokens

Pseudo-Random Function Issues

Lattice-based pseudo-random functions [BP14; BLM+13; Kim20] secure in the standard-model share one shape:

$$F_{\mathbf{a},\mathbf{B}}(x) = \left\lfloor \mathbf{a}^\top g(\mathbf{B}, x) \right\rceil_p$$

where:

- w.l.o.g, $\mathbf{a}$ is a secret vector and $\mathbf{B}$ a public matrix.
- $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, where $p < q$ and q is superpolynomial in magnitude
- $g(\cdot, \cdot)$ is a function that returns a matrix based on $\mathbf{B}$ and x.

Our Construction: Lattice-Based Rate-Limited Tokens

Pseudo-Random Function Issues

Lattice-based pseudo-random functions [BP14; BLM+13; Kim20] secure in the standard-model share one shape:

$$F_{\mathbf{a},\mathbf{B}}(x) = \left\lfloor \mathbf{a}^\top g(\mathbf{B}, x) \right\rfloor_p$$

where:

- w.l.o.g, $\mathbf{a}$ is a secret vector and $\mathbf{B}$ a public matrix.
- $\lfloor \cdot \rfloor_p : \mathbb{Z}_q \to \mathbb{Z}_p$, where $p < q$ and q is superpolynomial in magnitude
- $g(\cdot, \cdot)$ is a function that returns a matrix based on $\mathbf{B}$ and x.

Our Construction: Lattice-Based Rate-Limited Tokens

Pseudo-Random Function Issues

Lattice-based pseudo-random functions [BP14; BLM+13; Kim20] secure in the standard-model share one shape:

$$F_{\mathbf{a},\mathbf{B}}(x) = \left\lfloor \mathbf{a}^\top g(\mathbf{B}, x) \right\rfloor_p$$

where:

- w.l.o.g, $\mathbf{a}$ is a secret vector and $\mathbf{B}$ a public matrix.
- $\lfloor \cdot \rfloor_p : \mathbb{Z}_q \to \mathbb{Z}_p$, where $p < q$ and q is superpolynomial in magnitude
- $g(\cdot, \cdot)$ is a function that returns a matrix based on $\mathbf{B}$ and x.

Proving a correct evaluation of F implies proving g, which is a large arithmetic circuit.

Our Construction: Lattice-Based Rate-Limited Tokens

Pseudo-Random Function Issues

In the random oracle model, we have an efficient lattice-based pseudo-random functions [BLM+13]:

$$F_{\mathbf{k}}(x) = \left\lfloor \mathbf{k}^{\top} H(x) \right\rceil_p$$

where:

- w.l.o.g, $\mathbf{k}$ is a secret vector from a high min-entropy distribution over $\mathbb{Z}_q^n$ and H is a random oracle that returns random matrices.
- $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, where $p < q$ and q is polynomial in magnitude
- No complex g function, but we need to deal with a random oracle for the zero-knowledge proofs

Our Construction: Lattice-Based Rate-Limited Tokens

Pseudo-Random Function Issues

In the random oracle model, we have an efficient lattice-based pseudo-random functions [BLM+13]:

$$F_{\mathbf{k}}(x) = \left\lfloor \mathbf{k}^\top H(x) \right\rceil_p$$

where:

- w.l.o.g, $\mathbf{k}$ is a secret vector from a high min-entropy distribution over $\mathbb{Z}_q^n$ and H is a random oracle that returns random matrices.
- $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, where $p < q$ and q is polynomial in magnitude
- No complex g function, but we need to deal with a random oracle for the zero-knowledge proofs
- Security is based on the Learning with Rounding Assumption:

$$\left(\mathbf{A}, \left\lfloor \mathbf{k}^\top \mathbf{A} \right\rceil_p\right) \overset{c}{\approx} \left(\mathbf{A}, \mathcal{U}(\mathbb{Z}_p^m)\right)$$

Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

We can always recover the identity of a double spender.

Double-spending occurs if we have $\mathsf{tk}_i = (\mathsf{sn}_i, \pi_i)$, $\mathsf{tk}_j = (\mathsf{sn}_j, \pi_j)$ such that $\mathsf{sn}_i = \mathsf{sn}_j$, where the sns are outputs of pseudo-random function. However, if tk_i and tk_j belong to different users and $\mathsf{sn}_i = \mathsf{sn}_j$ with high probability, this is a problem.

Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

We can always recover the identity of a double spender.

Double-spending occurs if we have $\mathsf{tk}_i = (\mathsf{sn}_i, \pi_i)$, $\mathsf{tk}_j = (\mathsf{sn}_j, \pi_j)$ such that $\mathsf{sn}_i = \mathsf{sn}_j$, where the sns are outputs of pseudo-random function. However, if tk_i and tk_j belong to different users and $\mathsf{sn}_i = \mathsf{sn}_j$ with high probability, this is a problem.

Given $F_{\mathbf{k}}(x) = \left\lfloor \mathbf{k}^\top H(x) \right\rfloor_p$, we cannot rely on a user to honestly sample $\mathbf{k}$, e.g., taking $\mathbf{k} = \mathbf{0}^n$ gaurantees a collision with any token $\mathsf{tk}^* = (\mathsf{sn}^*, \pi^*)$, where $\mathsf{sn}^* = 0$.

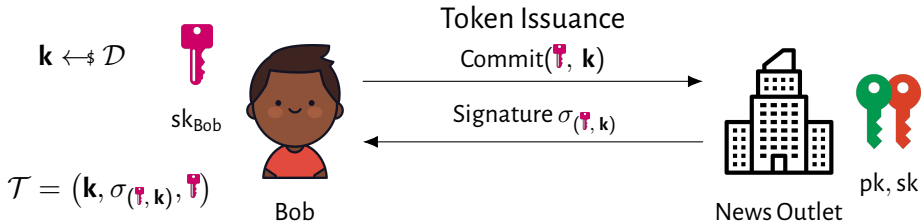
Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

We can always recover the identity of a double spender.

Double-spending occurs if we have $\mathsf{tk}_i = (\mathsf{sn}_i, \pi_i)$, $\mathsf{tk}_j = (\mathsf{sn}_j, \pi_j)$ such that $\mathsf{sn}_i = \mathsf{sn}_j$, where the sns are outputs of pseudo-random function. However, if tk_i and tk_j belong to different users and $\mathsf{sn}_i = \mathsf{sn}_j$ with high probability, this is a problem.

Given $F_{\mathbf{k}}(x) = \left\lfloor \mathbf{k}^\top H(x) \right\rfloor_p$, we cannot rely on a user to honestly sample $\mathbf{k}$, e.g., taking $\mathbf{k} = \mathbf{0}^n$ gaurantees a collision with any token $\mathsf{tk}^* = (\mathsf{sn}^*, \pi^*)$, where $\mathsf{sn}^* = 0$.



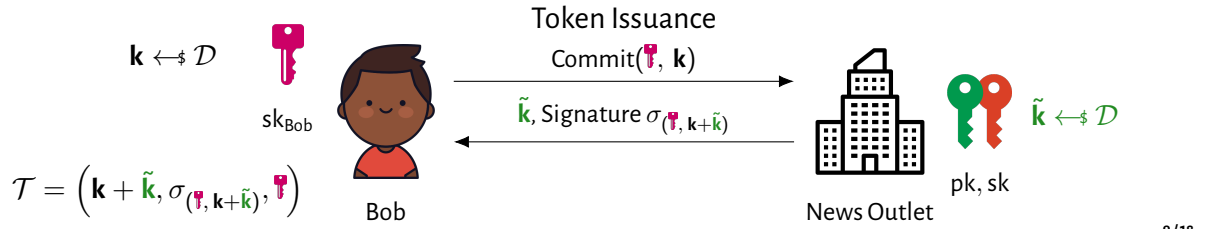
Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

We can always recover the identity of a double spender.

Double-spending occurs if we have $\mathsf{tk}_i = (\mathsf{sn}_i, \pi_i)$, $\mathsf{tk}_j = (\mathsf{sn}_j, \pi_j)$ such that $\mathsf{sn}_i = \mathsf{sn}_j$, where the sns are outputs of pseudo-random function. However, if tk_i and tk_j belong to different users and $\mathsf{sn}_i = \mathsf{sn}_j$ with high probability, this is a problem.

Given $F_{\mathbf{k}}(x) = \left\lfloor \mathbf{k}^\top H(x) \right\rfloor_p$, we cannot rely on a user to honestly sample $\mathbf{k}$, e.g., taking $\mathbf{k} = \mathbf{0}^n$ gaurantees a collision with any token $\mathsf{tk}^* = (\mathsf{sn}^*, \pi^*)$, where $\mathsf{sn}^* = 0$.



Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

Prior work [LLN+17; DLN+20] relied on N to be poly and $\mathcal{D} = \mathcal{U}(\mathbb{Z}_q^n)$, i.e., $\mathbf{k} + \tilde{\mathbf{k}} \sim \mathcal{U}(\mathbb{Z}_q^n)$, to argue that $F_{\mathbf{k}+\tilde{\mathbf{k}}}(x) = \left\lfloor (\mathbf{k} + \tilde{\mathbf{k}})^\top H(x) \right\rceil_p$ is *collision resistant*.

Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

Prior work [LLN+17; DLN+20] relied on N to be poly and $\mathcal{D} = \mathcal{U}(\mathbb{Z}_q^n)$, i.e., $\mathbf{k} + \tilde{\mathbf{k}} \sim \mathcal{U}(\mathbb{Z}_q^n)$, to argue that $F_{\mathbf{k}+\tilde{\mathbf{k}}}(x) = \left\lfloor (\mathbf{k} + \tilde{\mathbf{k}})^\top H(x) \right\rfloor_p$ is *collision resistant*.

- However, working with keys sampled over $\mathcal{U}(\mathbb{Z}_q^n)$ leads to large proof sizes of correct execution.

Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

Prior work [LLN+17; DLN+20] relied on N to be poly and $\mathcal{D} = \mathcal{U}(\mathbb{Z}_q^n)$, i.e., $\mathbf{k} + \tilde{\mathbf{k}} \sim \mathcal{U}(\mathbb{Z}_q^n)$, to argue that $F_{\mathbf{k}+\tilde{\mathbf{k}}}(x) = \left\lfloor (\mathbf{k} + \tilde{\mathbf{k}})^\top H(x) \right\rceil_p$ is *collision resistant*.

- However, working with keys sampled over $\mathcal{U}(\mathbb{Z}_q^n)$ leads to large proof sizes of correct execution.

Our Solution:

Lemma (Informal)

Let F be a secure key-homomorphic PRF with a polynomial-size domain $\mathcal{X}$ and a super-polynomial range $\mathcal{Y}$. If every key has the form $k_1 + k_2$, where k_2 is sampled honestly, then for all $x_1, x_2 \in \mathcal{X}$, then $F_{k_1+k_2}(x_1) \neq F_{k_1'+k_2'}(x_2)$ with overwhelming probability.

Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

Prior work [LLN+17; DLN+20] relied on N to be poly and $\mathcal{D} = \mathcal{U}(\mathbb{Z}_q^n)$, i.e., $\mathbf{k} + \tilde{\mathbf{k}} \sim \mathcal{U}(\mathbb{Z}_q^n)$, to argue that $F_{\mathbf{k}+\tilde{\mathbf{k}}}(x) = \left\lfloor (\mathbf{k} + \tilde{\mathbf{k}})^\top H(x) \right\rceil_p$ is *collision resistant*.

- However, working with keys sampled over $\mathcal{U}(\mathbb{Z}_q^n)$ leads to large proof sizes of correct execution.

Our Solution: $F_{k_1+k_2}(x) = F_{k_1}(x) + F_{k_2}(x)$

Lemma (Informal)

Let F be a secure key-homomorphic PRF with a polynomial-size domain $\mathcal{X}$ and a super-polynomial range $\mathcal{Y}$. If every key has the form $k_1 + k_2$, where k_2 is sampled honestly, then for all $x_1, x_2 \in \mathcal{X}$, then $F_{k_1+k_2}(x_1) \neq F_{k_1'+k_2'}(x_2)$ with overwhelming probability.

Our Construction: Lattice-Based Rate-Limited Tokens

Linkability

Prior work [LLN+17; DLN+20] relied on N to be poly and $\mathcal{D} = \mathcal{U}(\mathbb{Z}_q^n)$, i.e., $\mathbf{k} + \tilde{\mathbf{k}} \sim \mathcal{U}(\mathbb{Z}_q^n)$, to argue that $F_{\mathbf{k}+\tilde{\mathbf{k}}}(x) = \left\lfloor (\mathbf{k} + \tilde{\mathbf{k}})^\top H(x) \right\rceil_p$ is *collision resistant*.

- However, working with keys sampled over $\mathcal{U}(\mathbb{Z}_q^n)$ leads to large proof sizes of correct execution.

Our Solution: $F_{k_1+k_2}(x) = F_{k_1}(x) + F_{k_2}(x)$

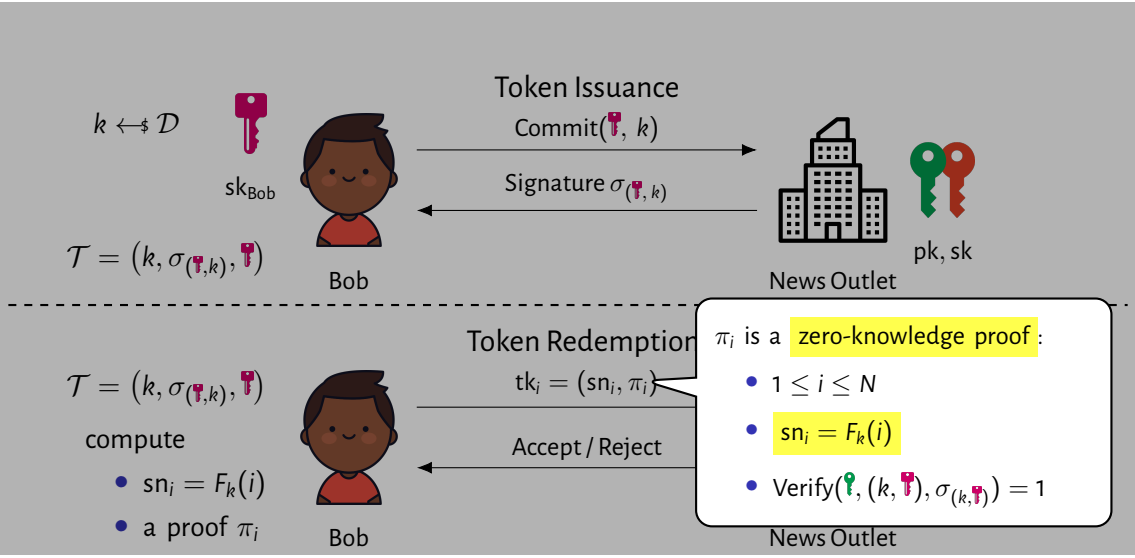
Lemma (Informal)

Let F be a secure key-homomorphic PRF with a polynomial-size domain $\mathcal{X}$ and a super-polynomial range $\mathcal{Y}$. If every key has the form $k_1 + k_2$, where k_2 is sampled honestly, then for all $x_1, x_2 \in \mathcal{X}$, then $F_{k_1+k_2}(x_1) \neq F_{k'_1+k'_2}(x_2)$ with overwhelming probability.

- No restriction on keys' distributions, i.e., any distribution $\mathcal{D}$ with high min-entropy works as long as F is secure. Moreover, taking $\mathcal{D}$ such that $\mathbf{k} \sim \mathcal{D}$, $\|\mathbf{k}\|_\infty < q/2$ leads to smaller proof sizes.
- Key-homomorphism can be relaxed to concatenation, i.e., $F_{k_1}(x) \| F_{k_2}(x)$.

Our Construction: Lattice-Based Rate-Limited Tokens

Soundness



Our Construction: Lattice-Based Rate-Limited Tokens

Soundness

The number of tokens N is public. Therefore, we can carve out the random oracle from the proof π by rewritting the statement as:

$$\exists i \in \{1, \ldots, N\}, \mathsf{sn}_i = F_k(H(i))$$

where $H(i)$ is provided by the verifier (*NewsOutlet*).

Our Construction: Lattice-Based Rate-Limited Tokens

Soundness

The number of tokens N is public. Therefore, we can carve out the random oracle from the proof π by rewritting the statement as:

$$\exists i \in \{1, \ldots, N\}, \mathsf{sn}_i = F_k(H(i))$$

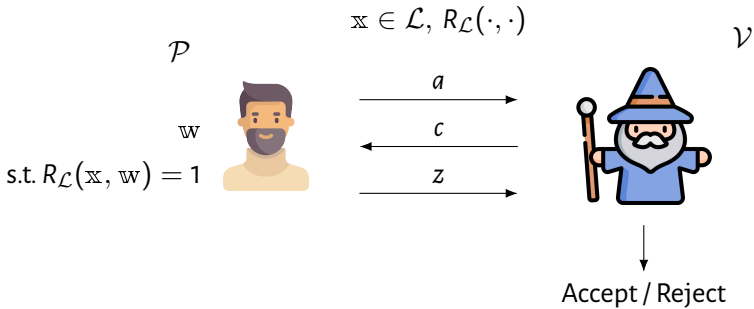
where $H(i)$ is provided by the verifier (*NewsOutlet*).
More concretely, setting $\mathbf{X}_i = H(i)$, where $\mathbf{X}_i \in \mathbb{Z}_q^{n \times m}$, we want to prove:

$$\text{Given } \{\mathbf{X}_1, \ldots, \mathbf{X}_n\} \text{ and } \mathbf{y} \in \mathbb{Z}_q^m, \text{there exist } \mathbf{k} \in \mathbb{Z}_q^n \text{ with } \|\mathbf{k}\| \leq \beta$$
$$\text{and } i \in \{1, \ldots, N\} \text{ such that } \mathbf{y}^\top = \mathbf{k}^\top \mathbf{X}_i$$

This a Disjunctive/OR-statement that we know how to prove using a Σ-protocol [Lyu12].

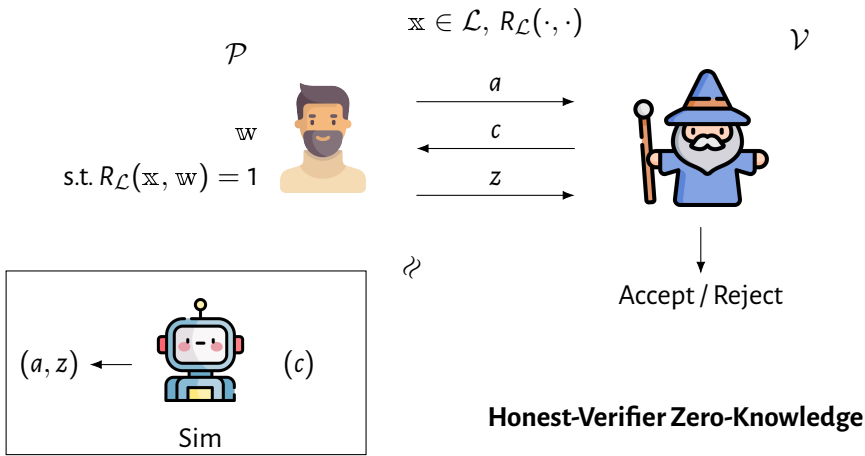
Σ-Protocol

Definition



Σ-Protocol

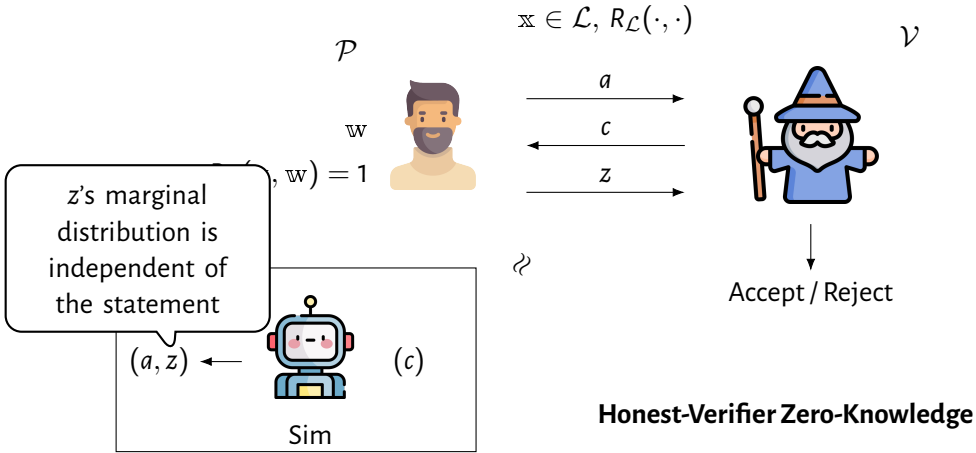
Definition



Honest-Verifier Zero-Knowledge

Σ-Protocol

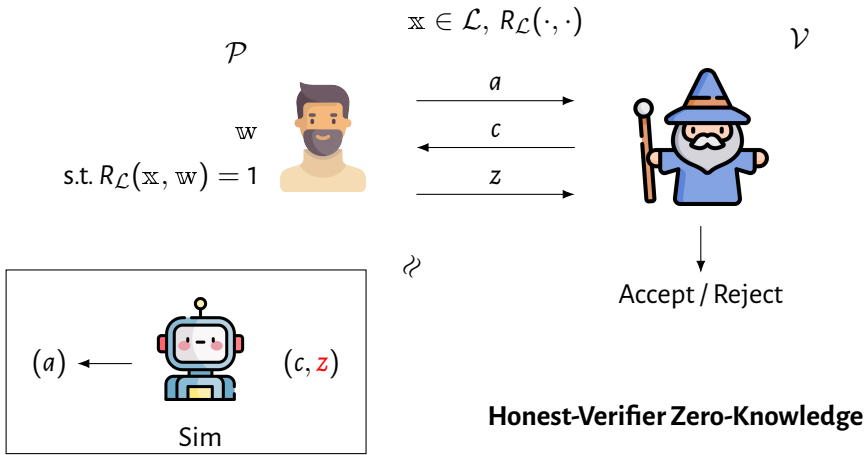
Definition



Honest-Verifier Zero-Knowledge

Σ-Protocol

Definition



Honest-Verifier Zero-Knowledge

Σ-Protocol

Disjunctive Statement [GGH+22]

Given $\mathbb{x}_1, \ldots, \mathbb{x}_N \in \mathcal{L}$, where $\mathcal{L}$ admits a Σ-protocol, we want to prove knowledge of a witness $\mathbb{w}$ such that $R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$ for one of the statements $\mathbb{x}_i$.

To do so efficiently, Goel et al. [GGH+22] introduced a primitive called *Partial-Binding Vector Commitment*.

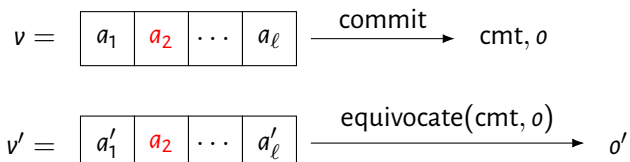
Σ-Protocol

Disjunctive Statement [GGH+22]

Given $\mathbb{x}_1, \ldots, \mathbb{x}_N \in \mathcal{L}$, where $\mathcal{L}$ admits a Σ-protocol, we want to prove knowledge of a witness $\mathbb{w}$ such that $R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$ for one of the statements $\mathbb{x}_i$.

To do so efficiently, Goel et al. [GGH+22] introduced a primitive called *Partial-Binding Vector Commitment*.

- $1 - \ell$ Partial-binding vector commitment



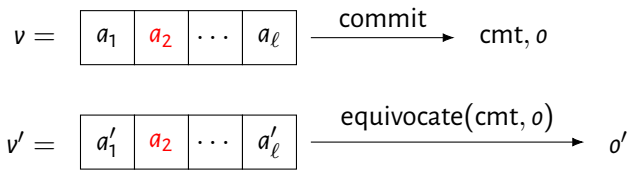
Σ-Protocol

Disjunctive Statement [GGH+22]

Given $\mathbb{x}_1, \ldots, \mathbb{x}_N \in \mathcal{L}$, where $\mathcal{L}$ admits a Σ-protocol, we want to prove knowledge of a witness $\mathbb{w}$ such that $R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$ for one of the statements $\mathbb{x}_i$.

To do so efficiently, Goel et al. [GGH+22] introduced a primitive called *Partial-Binding Vector Commitment*.

- $1 - \ell$ Partial-binding vector commitment



$$\text{open}(\text{cmt}, v, o) = 1 \wedge \text{open}(\text{cmt}, v', o') = 1$$

$$o \approx o'$$

Security: Can only equivocate on $\ell - 1$ positions

Σ-Protocol

Disjunctive Statement [GGH+22]

$\mathcal{P}$

$\mathbb{x}_1, \mathbb{x}_2, \ldots, \mathbb{x}_n \in \mathcal{L},\ R_{\mathcal{L}}(\cdot, \cdot)$

$\mathcal{V}$

$\mathbb{w}$

s.t. $\exists i \in \{1, \ldots, n\}$

$R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$





Σ-Protocol

Disjunctive Statement [GGH+22]

$\mathcal{P}$ $\qquad$ $\mathbb{x}_1, \mathbb{x}_2, \ldots, \mathbb{x}_n \in \mathcal{L}$, $R_{\mathcal{L}}(\cdot, \cdot)$ $\qquad$ $\mathcal{V}$

$\mathbb{w}$
s.t. $\exists i \in \{1, \ldots, n\}$
$R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$



- **Compute** a_i
- **Sample** $a_j \xleftarrow{\$} \{0,1\}^t$**, for** $j \neq i$
- cmt $\leftarrow$ commit$(a_1, \ldots, a_i, \ldots, a_n)$

cmt $\rightarrow$

$\leftarrow$ c



Σ-Protocol

Disjunctive Statement [GGH+22]

$\mathcal{P}$ $\qquad$ $\mathbb{x}_1, \mathbb{x}_2, \ldots, \mathbb{x}_n \in \mathcal{L},\ R_{\mathcal{L}}(\cdot,\cdot)$ $\qquad$ $\mathcal{V}$

$\mathbb{w}$
s.t. $\exists i \in \{1,\ldots,n\}$
$R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$



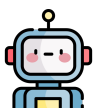
- **Compute** a_i
- **Sample** $a_j \xleftarrow{\$} \{0,1\}^t$**, for** $j \neq i$
- cmt $\leftarrow$ commit$(a_1, \ldots, a_i, \ldots, a_n)$

cmt $\rightarrow$
$\leftarrow$ c



Compute z_i

$a'_j \longleftarrow$ (c, z_i)



- **Compute** $o' \leftarrow$ equivocate$\big(\text{cmt}, (a'_1, \ldots, a_i, \ldots, a'_n), o\big)$

o', z_i $\rightarrow$

Σ-Protocol

Disjunctive Statement [GGH+22]

$\mathcal{P}$ $\qquad$ $\mathbb{x}_1, \mathbb{x}_2, \ldots, \mathbb{x}_n \in \mathcal{L}$, $R_{\mathcal{L}}(\cdot, \cdot)$ $\qquad$ $\mathcal{V}$

$\mathbb{w}$
s.t. $\exists i \in \{1, \ldots, n\}$
$R_{\mathcal{L}}(\mathbb{x}_i, \mathbb{w}) = 1$



- **Compute** a_i
- **Sample** $a_j \xleftarrow{\$} \{0,1\}^t$, **for** $j \neq i$
- cmt $\leftarrow$ commit$(a_1, \ldots, a_i, \ldots, a_n)$

cmt →
← c



Compute z_i

$a'_j \longleftarrow$ (c, z_i)



- **Compute** $o' \leftarrow$ equivocate$\big(\text{cmt}, (a'_1, \ldots, a_i, \ldots, a'_n), o\big)$

o', z_i →

Proof size is $O(\log n)$

Goel et al. partial-binding vector commitment is based on the discrete logarithm assumption, which is not post-quantum secure

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions

Case of $1 - 2$ **binding.**

Public Parameters: $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_q^{n \times m}$.

- $\mathrm{Gen}(b \in \{0,1\})$: Sample a low-norm matrix $\mathbf{T}$;
  Then compute $\mathbf{D}_{1-b} = \mathbf{A} \cdot \mathbf{T}$; $\mathbf{D}_b = \mathbf{B} - \mathbf{D}_{1-b}$.

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions

Case of $1-2$ binding.

$$\text{Public Parameters: } \mathbf{A}, \mathbf{B} \in \mathbb{Z}_q^{n \times m}.$$

- $\text{Gen}(b \in \{0,1\})$: Sample a low-norm matrix $\mathbf{T}$;
  Then compute $\mathbf{D}_{1-b} = \mathbf{A} \cdot \mathbf{T}$; $\mathbf{D}_b = \mathbf{B} - \mathbf{D}_{1-b}$.
- $\text{Commit}(\mathbf{v}_0, \mathbf{v}_1)$: Given low-now vectors $\mathbf{v}_0, \mathbf{v}_1 \in \mathbb{Z}_q^m$, Sample $\mathbf{r} \leftarrow \mathcal{D}^m$
  Return the commitment

  $$\mathbf{t} = \mathbf{A}\mathbf{r} + \mathbf{D}_0\mathbf{v}_0 + \mathbf{D}_1\mathbf{v}_1$$

  and opening $\mathbf{r}$.

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions

Case of $1-2$ binding.

$$\text{Public Parameters: } \mathbf{A}, \mathbf{B} \in \mathbb{Z}_q^{n \times m}.$$

- $\text{Gen}(b \in \{0,1\})$: Sample a low-norm matrix $\mathbf{T}$;
  Then compute $\mathbf{D}_{1-b} = \mathbf{A} \cdot \mathbf{T}$; $\mathbf{D}_b = \mathbf{B} - \mathbf{D}_{1-b}$.
- $\text{Commit}(\mathbf{v}_0, \mathbf{v}_1)$: Given low-now vectors $\mathbf{v}_0, \mathbf{v}_1 \in \mathbb{Z}_q^m$, Sample $\mathbf{r} \leftarrow \mathcal{D}^m$
  Return the commitment

  $$\mathbf{t} = \mathbf{A}\mathbf{r} + \mathbf{D}_0\mathbf{v}_0 + \mathbf{D}_1\mathbf{v}_1$$

  and opening $\mathbf{r}$.
- $\text{Equiv}(\mathbf{v}'_{1-b}, \mathbf{r}, \mathbf{T})$: Given a low-norm vector $\mathbf{v}'_{1-b} \neq \mathbf{v}_{1-b}$, opening $\mathbf{r}$, and trapdoor $\mathbf{T}$. Compute

  $$\mathbf{r}' = \mathbf{r} + \mathbf{T} \cdot \boldsymbol{\Delta}, \qquad \boldsymbol{\Delta} = \mathbf{v}_{1-b} - \mathbf{v}'_{1-b}$$

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions

Case of $1-2$ binding.

$$\text{Public Parameters: } \mathbf{A}, \mathbf{B} \in \mathbb{Z}_q^{n \times m}.$$

- $\text{Gen}(b \in \{0,1\})$: Sample a low-norm matrix $\mathbf{T}$;
  Then compute $\mathbf{D}_{1-b} = \mathbf{A} \cdot \mathbf{T}$; $\mathbf{D}_b = \mathbf{B} - \mathbf{D}_{1-b}$.
- $\text{Commit}(\mathbf{v}_0, \mathbf{v}_1)$: Given low-now vectors $\mathbf{v}_0, \mathbf{v}_1 \in \mathbb{Z}_q^m$, Sample $\mathbf{r} \leftarrow \mathcal{D}^m$
  Return the commitment
  $$\mathbf{t} = \mathbf{A}\mathbf{r} + \mathbf{D}_0\mathbf{v}_0 + \mathbf{D}_1\mathbf{v}_1$$
  and opening $\mathbf{r}$.
- $\text{Equiv}(\mathbf{v}'_{1-b}, \mathbf{r}, \mathbf{T})$: Given a low-norm vector $\mathbf{v}'_{1-b} \neq \mathbf{v}_{1-b}$, opening $\mathbf{r}$, and trapdoor $\mathbf{T}$. Compute

$$\mathbf{r}' = \mathbf{r} + \mathbf{T} \cdot \boldsymbol{\Delta}, \qquad \boldsymbol{\Delta} = \mathbf{v}_{1-b} - \mathbf{v}'_{1-b}$$

Correctness of Equiv

$$\mathbf{A}\mathbf{r}' + \mathbf{D}_b\mathbf{v}_b + \mathbf{D}_{1-b}\mathbf{v}'_{1-b} = \mathbf{A}\mathbf{r} + \mathbf{D}_{1-b}(\mathbf{v}_{1-b} - \mathbf{v}'_{1-b}) + \mathbf{D}_b\mathbf{v}_b + \mathbf{D}_{1-b}\mathbf{v}'_{1-b} = \mathbf{A}\mathbf{r} + \mathbf{D}_b\mathbf{v}_b + \mathbf{D}_{1-b}\mathbf{v}_{1-b} = \mathbf{t}$$

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions : Security

Case of $1 - 2$ **binding.**

Short Integer Solution (n, m, β)

Given $\bar{\mathbf{A}} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \neq \mathbf{0}$ such that $\|\mathbf{v}\| \leq \beta$ and

- $\bar{\mathbf{A}}\mathbf{v} = \mathbf{0}$, for the homogeneous case.
- $\bar{\mathbf{A}}\mathbf{v} = \mathbf{t}$, for the inhomogeneous case w.r.t target $\mathbf{t} \neq 0$.

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions : Security

Case of $1 - 2$ **binding.**

Short Integer Solution (n, m, β)

Given $\bar{\mathbf{A}} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \neq \mathbf{0}$ such that $\|\mathbf{v}\| \leq \beta$ and

- $\bar{\mathbf{A}}\mathbf{v} = \mathbf{0}$, for the homogeneous case.
- $\bar{\mathbf{A}}\mathbf{v} = \mathbf{t}$, for the inhomogeneous case w.r.t target $\mathbf{t} \neq 0$.

Let $\mathcal{A}$ be a PPT adversary that given $\mathbf{A}, \mathbf{B}$ outputs $(\mathbf{D}_0, \mathbf{D}_1, \text{cmt} = \mathbf{t})$ and $(\mathbf{v}_0, \mathbf{v}_1, \mathbf{r})$ and $(\mathbf{v}_0', \mathbf{v}_1', \mathbf{r}')$ such that $\mathbf{v}_0 \neq \mathbf{v}_0'$ and $\mathbf{v}_1 \neq \mathbf{v}_1'$.

$$\mathbf{t} = \mathbf{A}\mathbf{r} + \mathbf{D}_0\mathbf{v}_0 + \mathbf{D}_1\mathbf{v}_1 = \mathbf{A}\mathbf{r}' + \mathbf{D}_0\mathbf{v}_0' + \mathbf{D}_1\mathbf{v}_1'$$

$$\implies [\mathbf{A} \mid \mathbf{D}_0 \mid \mathbf{D}_1] \begin{bmatrix} \mathbf{r} - \mathbf{r}' \\ \mathbf{v}_0 - \mathbf{v}_0' \\ \mathbf{v}_1 - \mathbf{v}_1' \end{bmatrix} = 0$$

Our Construction: Lattice-Based Rate-Limited Tokens

Partial-Binding Vector Commitment from Lattice Assumptions : Security

Case of $1-2$ **binding.**

Short Integer Solution (n, m, β)

Given $\bar{\mathbf{A}} \leftarrow\$ \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \neq \mathbf{0}$ such that $\|\mathbf{v}\| \leq \beta$ and

- $\bar{\mathbf{A}}\mathbf{v} = \mathbf{0}$, for the homogeneous case.
- $\bar{\mathbf{A}}\mathbf{v} = \mathbf{t}$, for the inhomogeneous case w.r.t target $\mathbf{t} \neq 0$.

Let $\mathcal{A}$ be a PPT adversary that given $\mathbf{A}, \mathbf{B}$ outputs $(\mathbf{D}_0, \mathbf{D}_1, \text{cmt} = \mathbf{t})$ and $(\mathbf{v}_0, \mathbf{v}_1, \mathbf{r})$ and $(\mathbf{v}_0', \mathbf{v}_1', \mathbf{r}')$ such that $\mathbf{v}_0 \neq \mathbf{v}_0'$ and $\mathbf{v}_1 \neq \mathbf{v}_1'$.

$$\mathbf{t} = \mathbf{A}\mathbf{r} + \mathbf{D}_0\mathbf{v}_0 + \mathbf{D}_1\mathbf{v}_1 = \mathbf{A}\mathbf{r}' + \mathbf{D}_0\mathbf{v}_0' + \mathbf{D}_1\mathbf{v}_1'$$

$$\implies [\mathbf{A} \mid \mathbf{D}_0 \mid \mathbf{D}_1] \begin{bmatrix} \mathbf{r} - \mathbf{r}' \\ \mathbf{v}_0 - \mathbf{v}_0' \\ \mathbf{v}_1 - \mathbf{v}_1' \end{bmatrix} = 0$$

However, this is not complete. Either $\mathbf{D}_0 = \mathbf{A}\mathbf{T}$ or $\mathbf{D}_1 = \mathbf{A}\mathbf{T}$. To solve this, $\mathcal{A}$ is asked to provide a proof that $(\mathbf{D}_0 = \mathbf{A}\mathbf{T} \vee \mathbf{D}_1 = \mathbf{A}\mathbf{T})$

Summary of Our Contributions

1. Lattice-based rate-limited tokens in the random oracle.
2. Lattice-based partial-binding vector commitment.
3. A batch proof for conjunctive normal form of

$$\bigwedge_i \left(\mathbf{s}^\top \mathbf{A}_{i,0} = \mathbf{t}_i^\top \vee \mathbf{s}^\top \mathbf{A}_{i,1} = \mathbf{t}_i^\top\right)$$

4. Lattice-based Anonymous Counting Tokens.
5. New approaches to handle **linkability** and **exculpability** in the lattice setting

https://ia.cr/2026/1649



Some icons were sourced from Flaticon.com

Reference I

[BCK+09] M. Belenkiy et al. “Compact E-Cash and Simulatable VRFs Revisited”. In: *Pairing*. Vol. 5671. Lecture Notes in Computer Science. Springer, 2009, pp. 114–131.

[BLM+13] D. Boneh et al. “Key Homomorphic PRFs and Their Applications”. In: *CRYPTO (1)*. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 410–428.

[BP14] A. Banerjee and C. Peikert. “New and Improved Key-Homomorphic Pseudorandom Functions”. In: *CRYPTO (1)*. Vol. 8616. Lecture Notes in Computer Science. Springer, 2014, pp. 353–370.

[CDL+25] R. Chairattana-Apirom et al. “Everlasting Anonymous Rate-Limited Tokens”. In: *ASIACRYPT (6)*. Vol. 16250. Lecture Notes in Computer Science. Springer, 2025, pp. 435–468.

[CHK+06] J. Camenisch et al. “How to win the clonewars: efficient periodic n-times anonymous authentication”. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*. CCS ’06. Association for Computing Machinery, 2006, pp. 201–210.

Reference II

[CHL05] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. “Compact E-Cash”. In: *EUROCRYPT*. Vol. 3494. Lecture Notes in Computer Science. Springer, 2005, pp. 302–321.

[DLN+20] A. Deo et al. “Lattice-Based E-Cash, Revisited”. In: *ASIACRYPT (2)*. Vol. 12492. Lecture Notes in Computer Science. Springer, 2020, pp. 318–348.

[GGH+22] A. Goel et al. “Stacking Sigmas: A Framework to Compose Σ-Protocols for Disjunctions”. In: *EUROCRYPT (2)*. Vol. 13276. Lecture Notes in Computer Science. Springer, 2022, pp. 458–487.

[Kim20] S. Kim. “Key-Homomorphic Pseudorandom Functions from LWE with Small Modulus”. In: *Advances in Cryptology – EUROCRYPT 2020*. Springer, 2020, pp. 576–607.

[LLN+17] B. Libert et al. “Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash”. In: *ASIACRYPT (3)*. Vol. 10626. Lecture Notes in Computer Science. Springer, 2017, pp. 304–335.

Reference III

[LN26] A. Lysyanskaya and E. Nolan. “SMA^{2}RT: Secret-Metadata Attribute-Based Anonymous Rate-Limited Tokens”. In: *CRYPTO (10)*. Vol. 16809. Lecture Notes in Computer Science. Springer, 2026, pp. 576–606.

[Lyu12] V. Lyubashevsky. “Lattice Signatures without Trapdoors”. In: *EUROCRYPT*. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 738–755.