Dually Computable Cryptographic Accumulators and Their Application to Attribute-Based Encryption

Journées Codages et Cryptographie

Anaïs Barthoulot [1,2] Olivier Blazy [3] Sébastien Canard [4]

[1]Orange [2]Université de Limoges [3]École Polytechnique [4]Télécom Paris

October 17, 2023

Table of contents

Cryptographic Accumulators [Bd94]

- Introduced in 1994 by Benaloh and De Mare
- Compact representation of a set

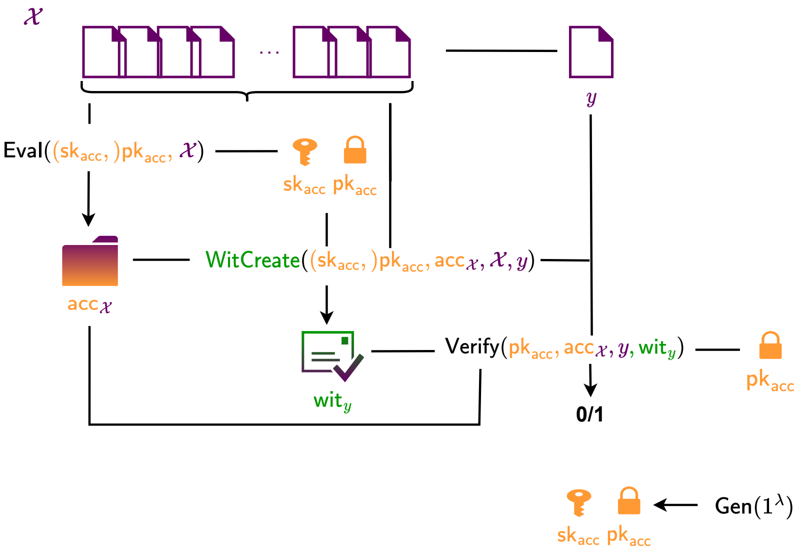
- Membership proof for one element $\cdots$
- $\cdots$ that cannot be forged

- RSA-based, pairing-based, lattice-based constructions

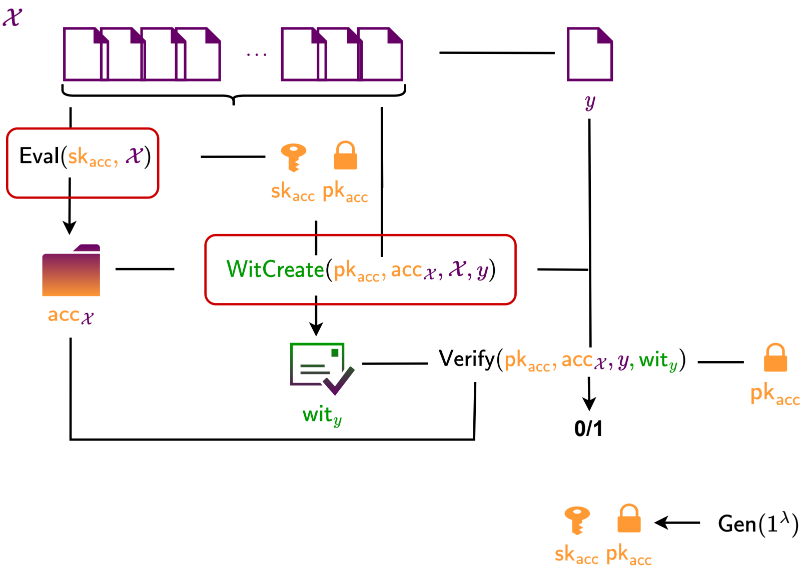
- Several applications:
  - timestamping
  - (anonymous) credentials
  - ecash
  - $\cdots$

Never used for **encryption**

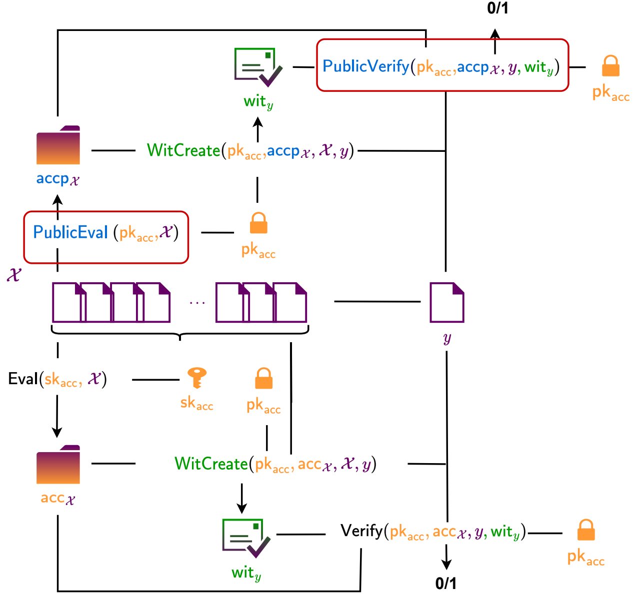
Asymmetric Accumulators [Bd94, DHS15]



Special Type of Accumulator



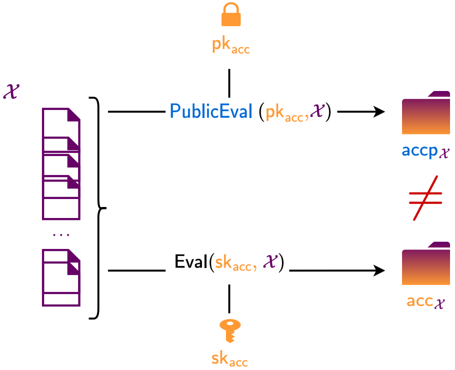
New Functionality: Dually Computable



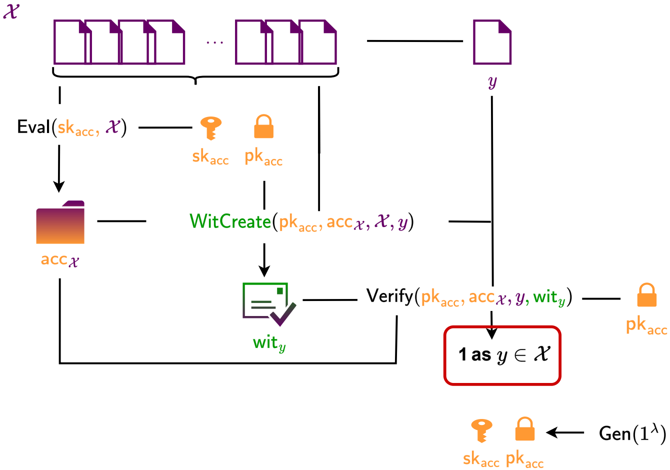
Sizes Requirements And Distinguishability

Sizes requirements: $|\mathsf{acc}_{\mathcal{X}}|$ and $|\mathsf{wit}_y|$ are small as for any accumulator

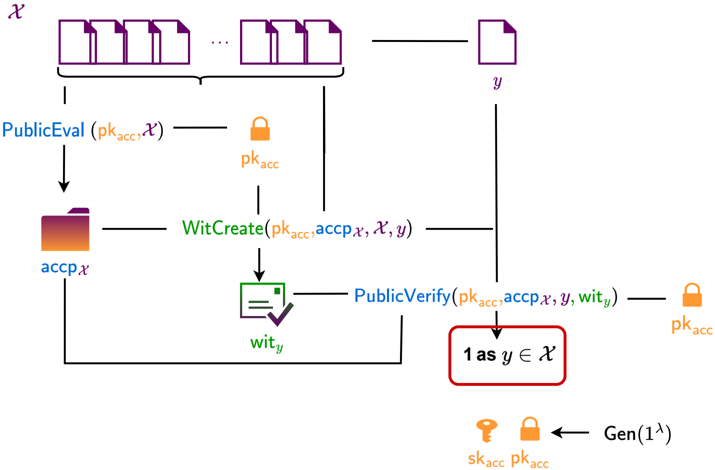
Distinguishability:



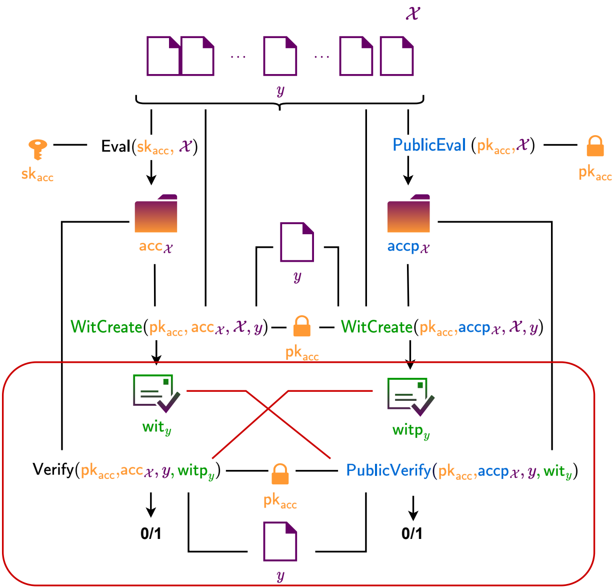
Correctness



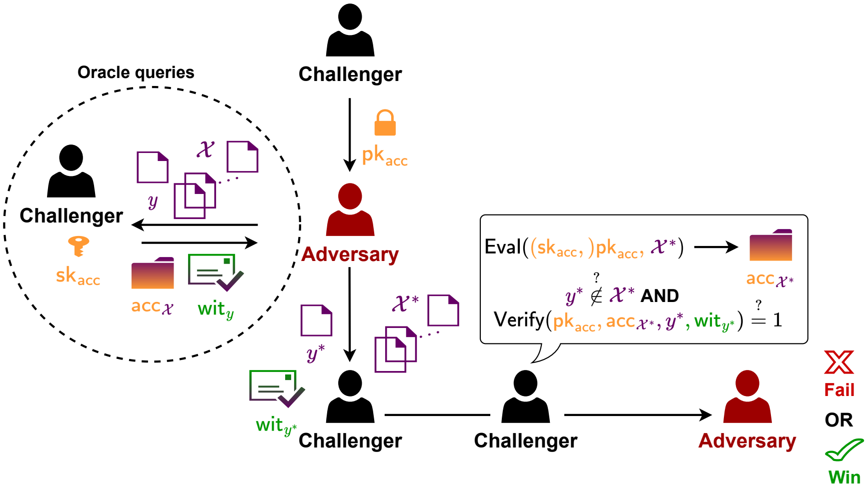
Correctness



Correctness of Duality



Asymmetric Cryptographic Accumulator Security: Collision Resistance



Dually Computable Accumulator Security: Dual Collision Resistance

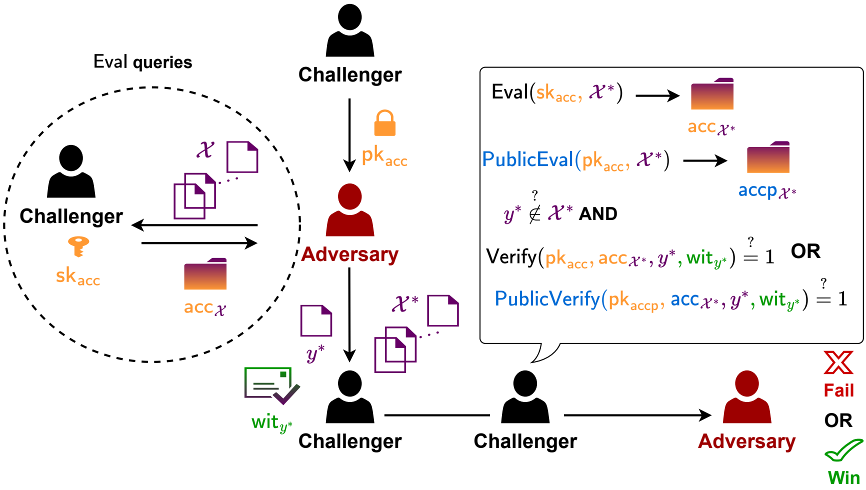


Table of contents

Mathematical Background

Asymmetric bilinear pairing:

- $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ cyclic (multiplicative) groups of order p (prime)
- $\mathbb{G}_1 =< g_1 >$, $\mathbb{G}_2 =< g_2 >$
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ a function s.t.:
  - $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $a, b \in \mathbb{Z}_p$ (*bilinear*)
  - $e(g_1, g_2) \neq 1$, 1: identity element in $\mathbb{G}_T$ (*non-degenerate*)
  - $e(X, Y)$ efficiently computable $\forall X \in \mathbb{G}_1, Y \in \mathbb{G}_2$ (*efficiently computable*)

Asymmetric bilinear pairing groups:

- $\mathit{\Gamma} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ as above
- and efficient algorithm to decide membership of the groups

Mathematical Background

Dual Pairing Vector Spaces (DPVS) [CLL+13]

- Prime p and a fixed (constant) dimension n
- Asymmetric bilinear pairing group $\mathit{\Gamma} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$
- $\mathbb{D} = (\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n)$ and $\mathbb{D}^* = (\boldsymbol{d}_1^*, \cdots, \boldsymbol{d}_n^*)$ of $\mathbb{Z}_p^n$ two random bases
- **Dual orthonormal**, meaning that
  - $\boldsymbol{d}_i \cdot \boldsymbol{d}_j^* = 0 \pmod p$ whenever $i \neq j$,
  - $\boldsymbol{d}_i \cdot \boldsymbol{d}_i^* = \psi \pmod p$ for all i,

  where ψ is a uniformly random element of $\mathbb{Z}_p$
- Generated by algorithm $\mathsf{Dual}(\mathbb{Z}_p^n)$

In our setting: $n = 2$, $\mathbb{D} = (\boldsymbol{d}_1, \boldsymbol{d}_2)$ and $\mathbb{D}^* = (\boldsymbol{d}_1^*, \boldsymbol{d}_2^*)$: $\boldsymbol{d}_1 \cdot \boldsymbol{d}_2^* = 0$ and $\boldsymbol{d}_1 \cdot \boldsymbol{d}_1^* = \psi$

Note: elements of $\mathbb{D}, \mathbb{D}^*$ are **vectors**

Pairings and Vectors & Characteristic Polynomial

- $g_i \in \mathbb{G}_i$ group element for $i \in \{1,2\}$, $\boldsymbol{u}, \boldsymbol{v}$ two vectors of length ℓ
- $g_i^{\boldsymbol{v}} := (g_i^{v_1}, \cdots, g_i^{v_\ell})$
- $g_i^{\boldsymbol{u}\cdot\boldsymbol{v}} = g_i^{\alpha}$, where $\alpha = \boldsymbol{u}\cdot\boldsymbol{v} = u_1 \cdot v_1 + u_2 \cdot v_2 + \cdots + u_\ell \cdot v_\ell$
- $$e(g_1^{\boldsymbol{u}}, g_2^{\boldsymbol{v}}) := \prod_{i=1}^{\ell} e(g_1^{u_i}, g_2^{v_i}) = e(g_1, g_2)^{\boldsymbol{u}\cdot\boldsymbol{v}}$$
- For set $\mathcal{X}$:
  characteristic polynomial $\mathsf{Ch}_{\mathcal{X}}[Z] = \prod_{x\in\mathcal{X}} (x+Z) = \sum_{i=0}^{|\mathcal{X}|} a_i \cdot Z^i$

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N}$, $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, $s \in \mathbb{Z}_p^*$, $(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{sk}_{\mathsf{acc}} = (s, \mathbb{D}, \mathbb{D}^*)$

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N},\ \Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2),\ s \in \mathbb{Z}_p^*,\ (\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{sk}_{\mathsf{acc}} = (s, \mathbb{D}, \mathbb{D}^*)$

- $\mathsf{acc}_{\mathcal{X}} = g_1^{\boldsymbol{d}_1 \mathsf{Ch}_{\mathcal{X}}(s)} = g_1^{\boldsymbol{d}_1 \prod_{x \in \mathcal{X}} (x+s)} = g_1^{\boldsymbol{d}_1 \sum_{i=0}^{q} a_i s^i}$ *Private Evaluation*

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N}$, $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, $s \in \mathbb{Z}_p^*$, $(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{sk}_{\mathsf{acc}} = (s, \mathbb{D}, \mathbb{D}^*)$
- $\mathsf{acc}_{\mathcal{X}} = g_1^{\boldsymbol{d}_1 \mathsf{Ch}_{\mathcal{X}}(s)} = g_1^{\boldsymbol{d}_1 \prod_{x \in \mathcal{X}} (x+s)} = g_1^{\boldsymbol{d}_1 \sum_{i=0}^{q} a_i s^i}$ *Private Evaluation*
- $\mathsf{pk}_{\mathsf{acc}} = (\Gamma, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, \cdots)$

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N}$, $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, $s \in \mathbb{Z}_p^*$, $(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{sk}_{\mathsf{acc}} = (s, \mathbb{D}, \mathbb{D}^*)$
- $\mathsf{acc}_{\mathcal{X}} = g_1^{\boldsymbol{d}_1 \mathsf{Ch}_{\mathcal{X}}(s)} = g_1^{\boldsymbol{d}_1 \prod_{x \in \mathcal{X}} (x+s)} = g_1^{\boldsymbol{d}_1 \sum_{i=0}^{q} a_i s^i}$ *Private Evaluation*
- $\mathsf{pk}_{\mathsf{acc}} = (\Gamma, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, \cdots)$
- $\mathsf{accp}_{\mathcal{X}} = g_2^{\boldsymbol{d}_1^* \mathsf{Ch}_{\mathcal{X}}(s)} = g_2^{\boldsymbol{d}_1^* \prod_{x \in \mathcal{X}} (x+s)} = g_2^{\boldsymbol{d}_1^* \sum_{i=0}^{q} a_i s^i}$ *Public Evaluation*

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N}$, $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, $s \in \mathbb{Z}_p^*$, $(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{pk}_{\mathsf{acc}} = (\Gamma, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, g_2^{\boldsymbol{d}_2^*}, g_2^{\boldsymbol{d}_2^* s}, \cdots, g_2^{\boldsymbol{d}_2^* s^q}, \cdots)$

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N}$, $\mathit{\Gamma} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, $s \in \mathbb{Z}_p^*$, $(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{pk}_{\mathsf{acc}} = (\mathit{\Gamma}, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, g_2^{\boldsymbol{d}_2^*}, g_2^{\boldsymbol{d}_2^* s}, \cdots, g_2^{\boldsymbol{d}_2^* s^q}, \cdots)$
- $\mathsf{wit}_y = {g_2}^{\boldsymbol{d}_2^* \mathsf{Ch}_{\mathcal{X} \setminus \{y\}}(s)} = {g_2}^{\boldsymbol{d}_2^* \prod_{x \in \mathcal{X} \setminus \{y\}} (x+s)} = {g_2}^{\boldsymbol{d}_2^* \sum_{i=0}^{q} b_i s^i}$

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N}$, $\mathit{\Gamma} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, $s \in \mathbb{Z}_p^*$, $(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{pk}_{\mathsf{acc}} = (\mathit{\Gamma}, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, g_2^{\boldsymbol{d}_2^*}, g_2^{\boldsymbol{d}_2^* s}, \cdots, g_2^{\boldsymbol{d}_2^* s^q}, g_1^{\boldsymbol{d}_2}, g_1^{\boldsymbol{d}_2 s}, \cdots)$
- $\mathsf{wit}_y = g_2^{\boldsymbol{d}_2^* \mathsf{Ch}_{\mathcal{X} \setminus \{y\}}(s)} = g_2^{\boldsymbol{d}_2^* \prod_{x \in \mathcal{X} \setminus \{y\}} (x+s)} = g_2^{\boldsymbol{d}_2^* \sum_{i=0}^{q} b_i s^i}$

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N},\ \mathit{\Gamma} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2),\ s \in \mathbb{Z}_p^*,\ (\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{pk}_{\mathsf{acc}} = (\mathit{\Gamma}, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, g_2^{\boldsymbol{d}_2^*}, g_2^{\boldsymbol{d}_2^* s}, \cdots, g_2^{\boldsymbol{d}_2^* s^q}, g_1^{\boldsymbol{d}_2}, g_1^{\boldsymbol{d}_2 s}, \cdots)$
- $\mathsf{wit}_y = g_2^{\boldsymbol{d}_2^* \mathsf{Ch}_{\mathcal{X}\setminus\{y\}}(s)} = g_2^{\boldsymbol{d}_2^* \prod_{x \in \mathcal{X}\setminus\{y\}} (x+s)} = g_2^{\boldsymbol{d}_2^* \sum_{i=0}^{q} b_i s^i}$
- $e(\mathsf{acc}_{\mathcal{X}}, g_2^{\boldsymbol{d}_1^*}) \stackrel{?}{=} e(g_1^{\boldsymbol{d}_2 y} \cdot g_1^{\boldsymbol{d}_2 s}, \mathsf{wit}_y)$ *Verification*

Our Dually Computable Accumulator

[Ngu05]'s pairing-based accumulator + DPVS of dimension 2

$q \in \mathbb{N},\ \Gamma = (p, \mathbb{G}_1, \mathbb{G}_2,\ \mathbb{G}_T, e, g_1, g_2),\ s \in \mathbb{Z}_p^*,\ (\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)$

- $\mathsf{pk}_{\mathsf{acc}} = (\Gamma, g_2^{\boldsymbol{d}_1^*}, g_2^{\boldsymbol{d}_1^* s}, \cdots, g_2^{\boldsymbol{d}_1^* s^q}, g_2^{\boldsymbol{d}_2^*}, g_2^{\boldsymbol{d}_2^* s}, \cdots, g_2^{\boldsymbol{d}_2^* s^q}, g_1^{\boldsymbol{d}_2}, g_1^{\boldsymbol{d}_2 s}, g_1^{\boldsymbol{d}_1})$
- $\mathsf{wit}_y = g_2^{\boldsymbol{d}_2^* \mathsf{Ch}_{\mathcal{X} \setminus \{y\}}(s)} = g_2^{\boldsymbol{d}_2^* \prod_{x \in \mathcal{X} \setminus \{y\}} (x+s)} = g_2^{\boldsymbol{d}_2^* \sum_{i=0}^{q} b_i s^i}$
- $e(\mathsf{acc}_{\mathcal{X}}, g_2^{\boldsymbol{d}_1^*}) \stackrel{?}{=} e(g_1^{\boldsymbol{d}_2 y} \cdot g_1^{\boldsymbol{d}_2 s}, \mathsf{wit}_y)$ *Verification*
- $e(g_1^{\boldsymbol{d}_1}, \mathsf{accp}_{\mathcal{X}}) \stackrel{?}{=} e(g_1^{\boldsymbol{d}_2 y} \cdot g_1^{\boldsymbol{d}_2 s}, \mathsf{wit}_y)$ *Public Verification*

All Properties Are Satisfied

- **Correctness**: [Ngu05]'s correctness + DVPS
$e(g_1^{d_2 y+s}, \mathsf{wit}_y) = e({g_1}^{d_2 \mathsf{Ch}_{\{y\}}(s)}, {g_2}^{d_2^* \mathsf{Ch}_{\mathcal{X}\setminus\{y\}}(s)}) = e(g_1, g_2)^{\psi \mathsf{Ch}_{\mathcal{X}}(s)}$,
and $e(\mathsf{acc}_{\mathcal{X}}, g_2^{d_1^*}) = e(g_1, g_2)^{\psi \mathsf{Ch}_{\mathcal{X}}(s)} = e(g_1^{d_1}, \mathsf{accp}_{\mathcal{X}})$

All Properties Are Satisfied

- **Correctness**: [Ngu05]'s correctness + DVPS
- **Distinguishability**: $\mathsf{acc}_{\mathcal{X}} \in \mathbb{G}_1^2 \neq \mathsf{accp}_{\mathcal{X}} \in \mathbb{G}_2^2$

All Properties Are Satisfied

- **Correctness**: [Ngu05]'s correctness + DVPS
- **Distinguishability**: $\mathsf{acc}_{\mathcal{X}} \in \mathbb{G}_1^2 \neq \mathsf{accp}_{\mathcal{X}} \in \mathbb{G}_2^2$
- **Correctness of duality**:

$$\underbrace{e(\mathsf{acc}_{\mathcal{X}}, g_2^{\boldsymbol{d}_1^*})}_{\text{from } \mathsf{Eval}} = \underbrace{e(g_1^{\boldsymbol{d}_2(y+s)}, \mathsf{wit}_y)}_{\text{from } \mathsf{WitCreate}} = \underbrace{e(g_1^{\boldsymbol{d}_1}, \mathsf{accp}_{\mathcal{X}})}_{\text{from } \mathsf{PublicEval}}$$

All Properties Are Satisfied

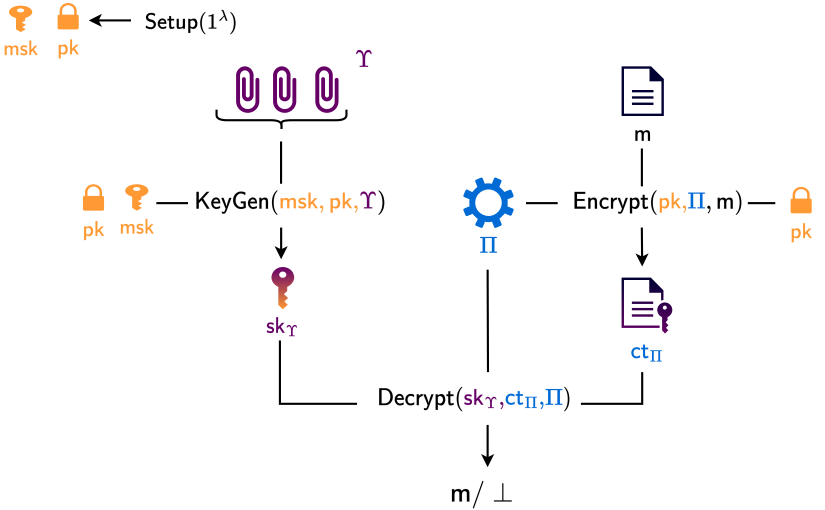
- **Correctness**: [Ngu05]'s correctness + DVPS
- **Distinguishability**: $\mathsf{acc}_{\mathcal{X}} \in \mathbb{G}_1^2 \neq \mathsf{accp}_{\mathcal{X}} \in \mathbb{G}_2^2$
- **Correctness of duality**:

$$\underbrace{e(\mathsf{acc}_{\mathcal{X}}, g_2^{\boldsymbol{d}_1^*})}_{\text{from } \mathsf{Eval}} = \underbrace{e(g_1^{\boldsymbol{d}_2(y+s)}, \mathsf{wit}_y)}_{\text{from } \mathsf{WitCreate}} = \underbrace{e(g_1^{\boldsymbol{d}_1}, \mathsf{accp}_{\mathcal{X}})}_{\text{from } \mathsf{PublicEval}}$$

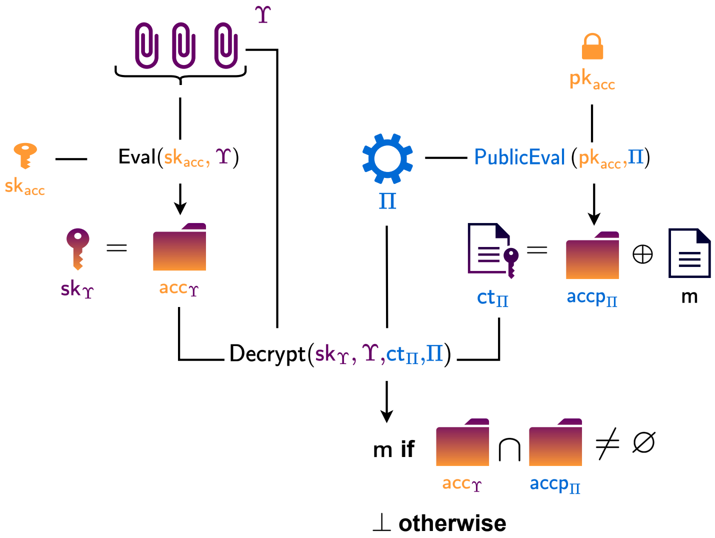
- **Dual collision resistance**: from *q-Strong Bilinear Diffie Hellman* assumption, as Nguyen's scheme

Table of contents

Ciphertext Policy Attribute-Based Encryption (CP-ABE)



CP-ABE from Dually Computable Accumulators



Access Policies and Accumulators: an Example

- Access policies: disjunctions of conjunctions
- $\mathcal{H}$: {set of attributes} $\to \mathbb{Z}_p$, hash function

- $\Pi = (a_1 \wedge a_3) \vee a_4$
- $\mathcal{Y} = \{\mathcal{H}(\{a_1, a_3\}), \mathcal{H}(\{a_4\})\}$
- $\mathsf{accp}_\Pi \leftarrow \mathsf{PublicEval}(\mathsf{pk}_{\mathsf{acc}}, \mathcal{Y})$

- $\Upsilon = \{a_1, a_2, a_3\}$
- $\mathcal{X} = \left\{\mathcal{H}(\{a_i\}_{i=1}^{3}), \mathcal{H}(\{a_i, a_j\}_{1 \le i < j \le 3}), \mathcal{H}(\{a_1, a_2, a_3\})\right\}$
- $\mathsf{acc}_\Upsilon \leftarrow \mathsf{Eval}(\mathsf{sk}_{\mathsf{acc}}, \mathcal{X})$

- $\mathcal{H}(\{a_1, a_3\}) \in \mathsf{acc}_\Upsilon \cap \mathsf{accp}_\Pi$ and $\{a_1, a_3\}$ satisfies Π

Our CP-ABE

- Combination of previous idea + our dually computable accumulator
- Intersection of two accumulators: more details in the paper
- Advantages:
  - Constant size ciphertext
  - Constant size secret key
- Drawbacks:
  - Public key size exponential
  - No generic construction
  - Simple access policies

Table of contents

Conclusion

Our contributions

- Improvement of accumulator state of the art
- Introduction of dually computable accumulators
- Construction of a dually computable accumulator
- New application of accumulators: encryption
- Improvement of attribute-based encryption state of the art

Futur works

- Reducing our CP-ABE public key size
- Developing generic construction of ABE from dually computable accumulators
- Dealing with fine-grained access policies

Paper accepted at CANS 2023 (October, 31^{st}- November, 2^{nd})
Eprint version: `https://eprint.iacr.org/2023/1277`

Bibliography I

Man Ho Au, Qianhong Wu, Willy Susilo, and Yi Mu.
Compact e-cash from bounded accumulator.
pages 178–195, 2007.

Josh Cohen Benaloh and Michael de Mare.
One-way accumulators: A decentralized alternative to digital sinatures (extended abstract).
pages 274–285, 1994.

Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Hoeteck Wee.
Shorter IBE and signatures via asymmetric pairings.
pages 122–140, 2013.

David Derler, Christian Hanser, and Daniel Slamanig.
Revisiting cryptographic accumulators, additional properties and relations to other primitives.
pages 127–144, 2015.

Lan Nguyen.
Accumulators from bilinear pairings and applications.
pages 275–292, 2005.