Advanced Encryption for the Sharing of Sensitive Data

PHD Defense

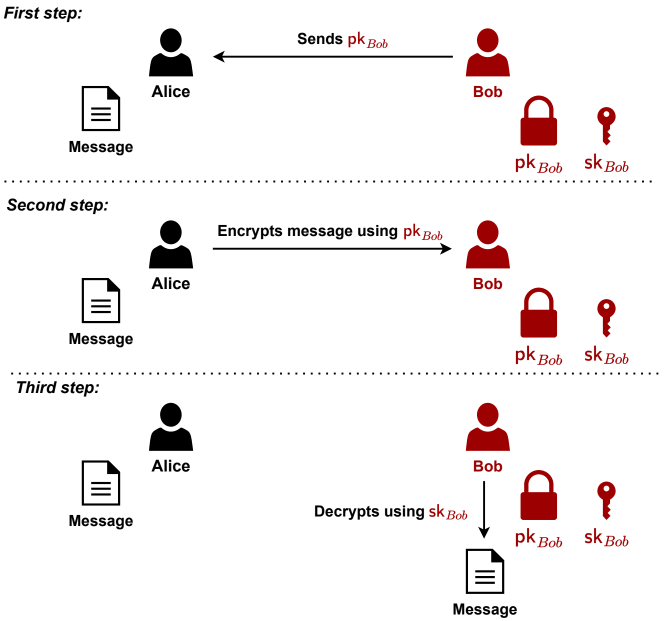
Anaïs Barthoulot [1,2]

[1]Orange [2]Université de Limoges

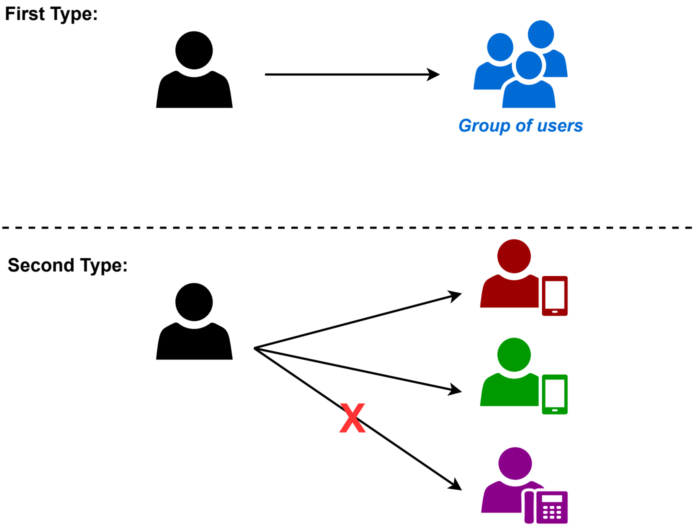
December 18th, 2023

Table of contents

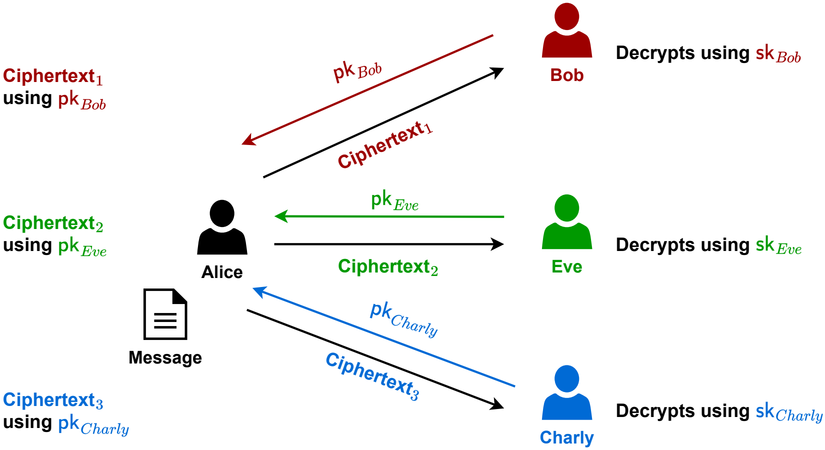
Asymmetric Cryptography



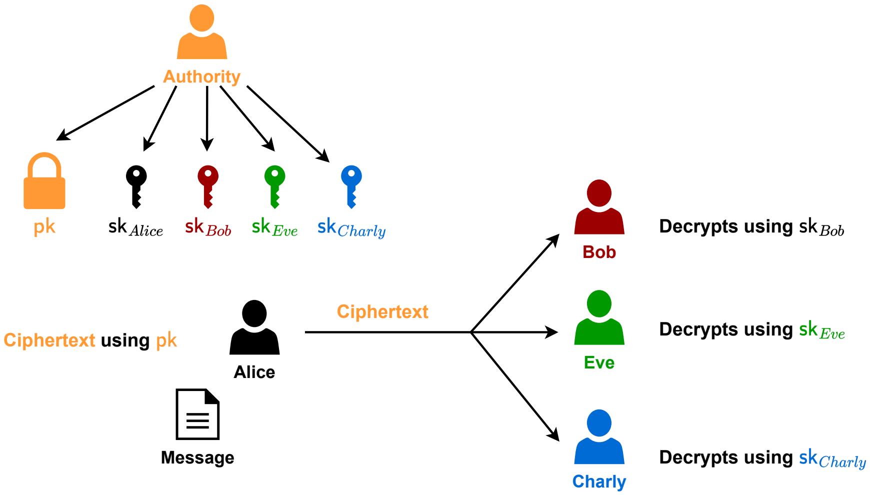
Two Types of Sharing



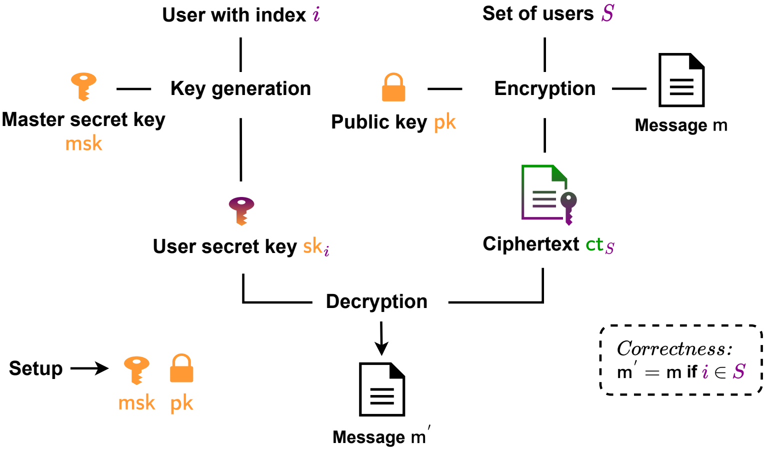
Sharing to Several Persons: Trivial Way



Sharing to Several Persons: Efficient Way

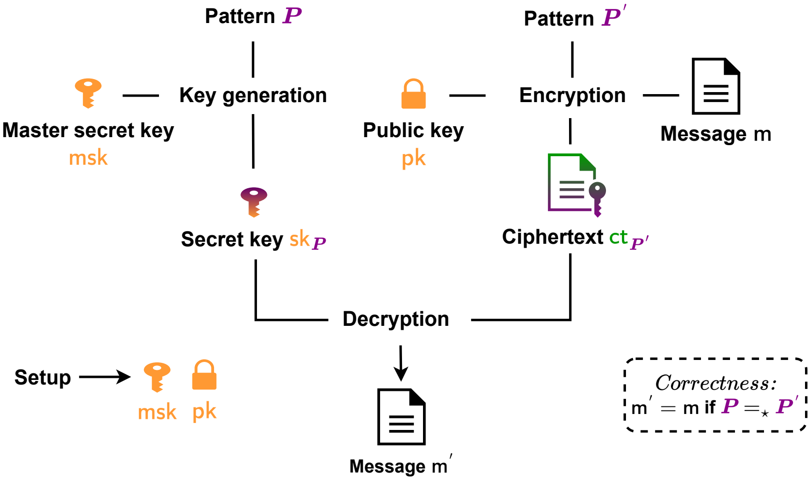


Advanced Encryption Scheme For Sharing to a Group of Users



Broadcast Encryption scheme

First Tool: Identity-Based Encryption with Wildcards



Our Contributions (1)

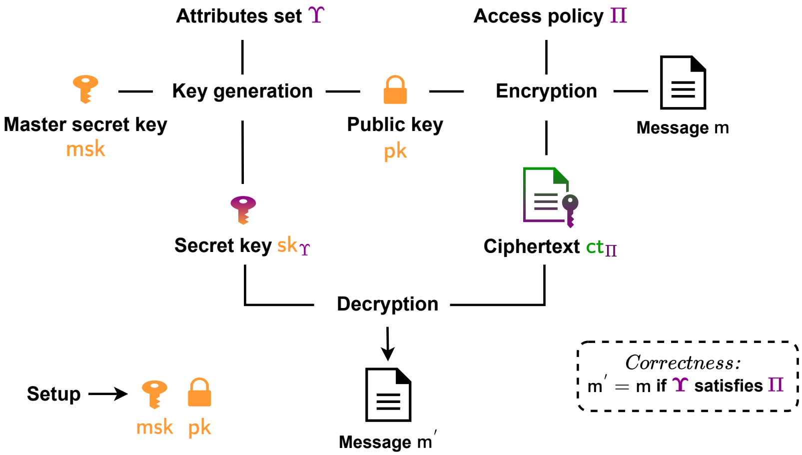
Main Contributions

- **Generic construction of Broadcast Encryption scheme from Identity-Based Encryption with Wildcards**
- New pairing-based Broadcast Encryption scheme with *constant size ciphertext*

Auxiliary Contribution

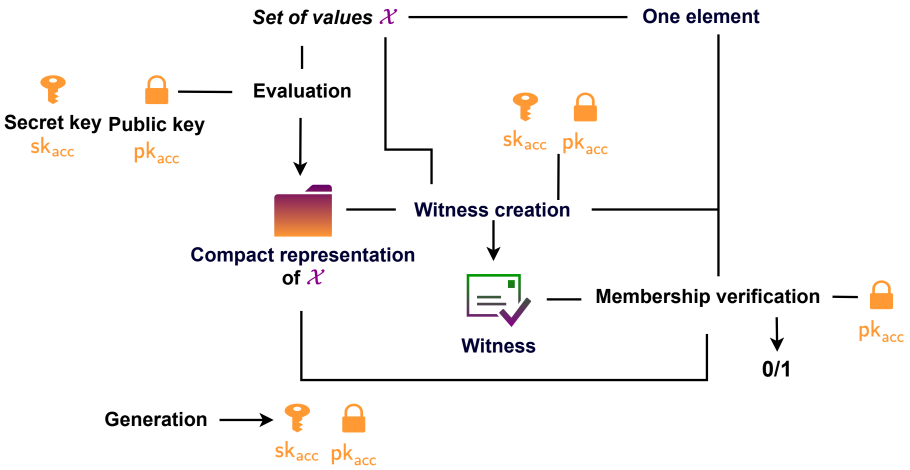
- New pairing-based Identity-Based Encryption with Wildcards scheme, with *constant size ciphertext*

Advanced Encryption Scheme For Sharing to a Group With Common Attributes



Ciphertext Policy Attribute-Based Encryption scheme

Second Tool: Cryptographic Accumulators



Our Contributions (2)

Main Contribution

- **New pairing-based Ciphertext Policy Attribute-Based Encryption with both constant size ciphertext and secret keys based on Cryptographic Accumulators**

Auxiliary Contributions

- **Introducing a new type of Cryptographic Accumulators: dually computable accumulators**
- **First dually computable accumulator scheme, based on pairings**

Going Further: Our Other Contributions

In Submission

- Main contribution:
  - An Attribute-Based Encryption scheme from Identity-Based Encryption with Wildcards, protecting privacy of *both* access policies and attributes
- Auxiliary contributions:
  - Introducing a new functionality for Identity-Based Encryption with Wildcards scheme: *privacy-preserving key generation*
  - Pairing-based privacy-preserving key generation Identity-Based Encryption with Wildcards scheme

Cryptographic Accumulators Systematization of Knowledge (*In submission*)

- New security property, *unforgeability of private evaluation*
- Discussions on applications and properties of accumulators

Table of contents

Table of contents

Broadcast Encryption

Broadcast Encryption (BE) [FN94]

- $\mathsf{Setup}(1^\lambda, N) \to (\mathsf{pk}, \mathsf{msk})$
- $\mathsf{Encrypt}(\mathsf{pk}, \mathsf{m}, S) \to \mathsf{ct}_S$
- $\mathsf{KeyGen}(\mathsf{msk}, i) \to \mathsf{sk}_i$ for $i = 1, \cdots, N$
- $\mathsf{Decrypt}(\mathsf{sk}_i, \mathsf{ct}_S, S) \to \mathsf{m}'$

Correctness:

For all $\lambda, N \in \mathbb{N}$, for $(\mathsf{pk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, N)$ **honestly generated** and for all index and subset i, S such that $i \in S$:

$$\mathsf{Decrypt}(\mathsf{KeyGen}(\mathsf{msk}, i), \mathsf{Encrypt}(\mathsf{pk}, \mathsf{m}, S), S) = \mathsf{m}$$

Broadcast Encryption Security: Indistinguishability

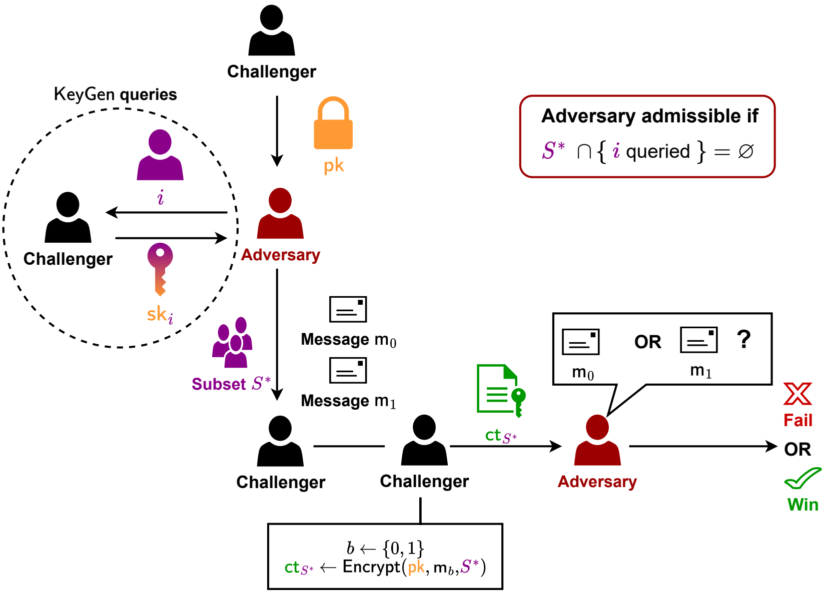


Table of contents

Patterns

Patterns [ACD+06, KLLO18]

- Pattern $\boldsymbol{P} = (P_1, \cdots, P_L) \in \mathcal{U}^L$, where
  - $\mathcal{U}$: set with a special wildcard symbol "$\star$",
  - $L \in \mathbb{N}$

- $\boldsymbol{P}^{'} = (P_1^{'}, \cdots, P_L^{'})$ and $\boldsymbol{P} = (P_1, \cdots, P_L)$:
  - $\boldsymbol{P}$ **belongs** to $\boldsymbol{P}^{'}$, denoted $\boldsymbol{P} \in_\star \boldsymbol{P}^{'}$, iff $\forall i \in \{1, \cdots, L\}$, $(P_i^{'} = P_i) \vee (P_i^{'} = \star)$
  - $\boldsymbol{P}$ **matches** $\boldsymbol{P}^{'}$, denoted $\boldsymbol{P} =_\star \boldsymbol{P}^{'}$, iff $\forall i \in \{1, \cdots, L\}$, $(P_i^{'} = P_i) \vee (P_i = \star) \vee (P_i^{'} = \star)$

Patterns: Example

$$\mathcal{U} = \{0, 1, \star\}$$

$$P = 0\ 1\ 1\ \star\ 0$$
$$P' = \star\ 1\ 1\ 0\ \star$$

$$P =_\star P'$$

$$P = 0\ 1\ 1\ \star\ 0$$
$$P' = \star\ 0\ 1\ 0\ \star$$

$$P \neq_\star P'$$

$$P = 0\ 1\ 1\ 0\ 0$$
$$P' = \star\ 1\ 1\ 0\ \star$$

$$P \in_\star P'$$

$$P = 0\ 1\ 1\ 1\ 0$$
$$P' = \star\ 0\ 1\ 0\ \star$$

$$P \notin_\star P'$$

Equal to $\star$

Equals

Differents

Identity-Based Encryption with Wildcards

Identity-Based Encryption with Wildcards (WIBE) [ACD+06]

- $\mathsf{Setup}(1^\lambda, L) \to (\mathsf{pk}, \mathsf{msk})$
- $\mathsf{KeyGen}(\mathsf{msk}, \boldsymbol{P}) \to \mathsf{sk}_{\boldsymbol{P}}$
- $\mathsf{Encrypt}(\mathsf{pk}, \boldsymbol{P}', \mathsf{m}) \to \mathsf{ct}_{\boldsymbol{P}'}$
- $\mathsf{Decrypt}(\mathsf{sk}_{\boldsymbol{P}}, \boldsymbol{P}, \mathsf{ct}_{\boldsymbol{P}'}, \boldsymbol{P}') \to \mathsf{m}'$

Correctness:

For all $\lambda, L \in \mathbb{N}$, for $(\mathsf{pk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, L)$ **honestly generated** and for all patterns $\boldsymbol{P}, \boldsymbol{P}'$ such that $\boldsymbol{P} =_\star \boldsymbol{P}'$:

$$\mathsf{Decrypt}(\mathsf{KeyGen}(\mathsf{msk}, \boldsymbol{P}), \boldsymbol{P}, \mathsf{Encrypt}(\mathsf{pk}, \boldsymbol{P}', \mathsf{m}), \boldsymbol{P}') = \mathsf{m}$$

WIBE Security: Indistinguishability

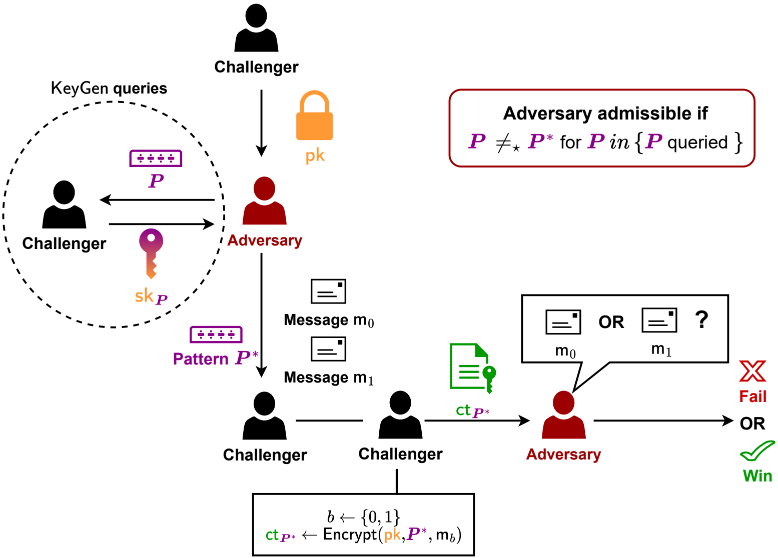
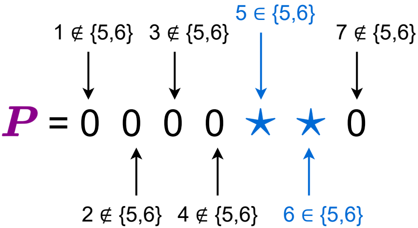


Table of contents

Building BE From WIBE

- Any subset $S \subseteq [N]$ can be represented as a pattern $\boldsymbol{P} \in \{0, \star\}^N$: for $j \in [1, N]$,
  - $P_j = \star$ if $j \in S$
  - $P_j = 0$ otherwise

Example: for $N = 7$

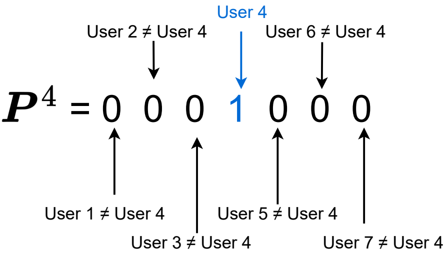


Creating a pattern in {0,★}^{7} representing the set {5,6}

Building BE From WIBE

- Any user identity $i \in [N]$ can be represented as a pattern $\boldsymbol{P^i} \in \{0,1\}^N$: for $j \in [1, N]$,
  - $P^i_j = 1$ if $j = i$
  - $P^i_j = 0$ otherwise

Example: for $N = 7$



Creating a pattern in $\{0,1\}^7$ representing identity of User 4

Building BE From WIBE

- $i \in S \iff \boldsymbol{P}^i \in_\star \boldsymbol{P}$

Example: $N = 7$, $\boldsymbol{P}$ for subset $\{5, 6\}$

$$\begin{array}{rl} \boldsymbol{P} = & (0\ 0\ 0\ 0\ \star\ \star\ 0) \\ \boldsymbol{P}^4 = & (0\ 0\ 0\ 1\ 0\ 0\ 0) \end{array} \qquad \begin{array}{rl} \boldsymbol{P} = & (0\ 0\ 0\ 0\ \star\ \star\ 0) \\ \boldsymbol{P}^6 = & (0\ 0\ 0\ 0\ 0\ 1\ 0) \end{array}$$

When User 4 tries to decrypt: $\boldsymbol{P}^4 \notin_\star \boldsymbol{P}$

When User 6 tries to decrypt: $\boldsymbol{P}^6 \in_\star \boldsymbol{P}$

Generic Construction

Ciphertext pattern space: $\{0, \star\}^N$, Key pattern space: $\{0, 1\}^N$

Broadcast Encryption from WIBE

- $\mathsf{Setup}(1^\lambda, N) = \mathsf{WIBE.Setup}(1^\lambda, N) \rightarrow (\mathsf{pk}, \mathsf{msk})$
- $\mathsf{KeyGen}(\mathsf{msk}, i \in [N]) = \mathsf{WIBE.KeyGen}(\mathsf{msk}, \boldsymbol{P}^i) \rightarrow \mathsf{sk}_{\boldsymbol{P}^i}$ for $\boldsymbol{P}^i \in \{0, 1\}^N$ as above
- $\mathsf{Encrypt}(\mathsf{pk}, S, \mathsf{m}) = \mathsf{WIBE.Encrypt}(\mathsf{pk}, \boldsymbol{P}, \mathsf{m}) \rightarrow \mathsf{ct}_{\boldsymbol{P}}$, for $\boldsymbol{P}$ in $\{0, \star\}^N$ as above
- $\mathsf{Decrypt}(\mathsf{sk}_i, \mathsf{ct}_{\boldsymbol{P}}, S) = \mathsf{WIBE.Decrypt}(\mathsf{sk}_{\boldsymbol{P}^i}, \boldsymbol{P}^i, \mathsf{ct}_{\boldsymbol{P}}, \boldsymbol{P}) \rightarrow \mathsf{m}'$

Correctness:

Correctness of the obtained BE comes from correctness of the underlying WIBE

Security

Theorem

If WIBE satisfies indistinguishability security, the obtained BE satisfies indistinguishability security.

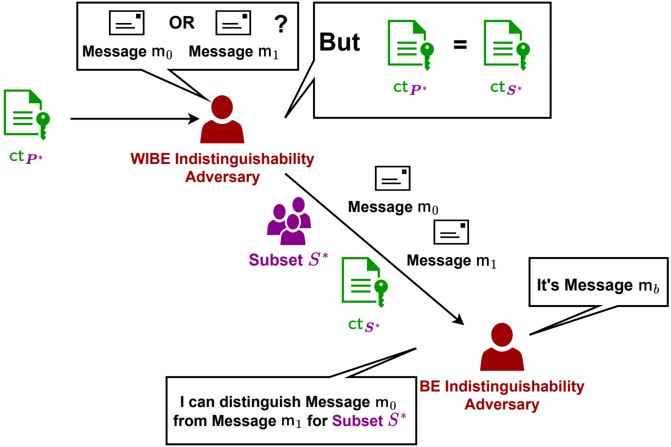


Table of contents

Other Main Contributions

- Generic construction of Augmented Broadcast Encryption scheme, a variant of Broadcast Encryption scheme, from Identity-Based Encryption with Wildcards
- First (pairing-based) Augmented Broadcast Encryption scheme secure in the *standard model*

Other Auxiliary Contributions

- New security property for Identity-Based Encryption with Wildcards: *pattern-hiding*
- First (pairing-based) Identity-Based Encryption with Wildcards scheme satisfying *pattern-hiding security*

All results are in an article accepted at CANS 2022

Table of contents

Table of contents

Attribute-Based Encryption [SW05]

Ciphertext Policy Attribute-Based Encryption (CP-ABE)

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{pk}, \mathsf{msk})$
- $\mathsf{KeyGen}(\mathsf{msk}, \mathsf{pk}, \Upsilon) \to \mathsf{sk}_\Upsilon$
- $\mathsf{Encrypt}(\mathsf{pk}, \Pi, \mathsf{m}) \to \mathsf{ct}_\Pi$
- $\mathsf{Decrypt}(\mathsf{sk}_\Upsilon, \Upsilon, \mathsf{ct}_\Pi, \Pi) \to \mathsf{m}'$

Key Policy Attribute-Based Encryption (KP-ABE)

Similar to CP-ABE except that attributes and policies are swapped in KeyGen and Encrypt

CP-ABE Properties

Correctness:

For all $\lambda \in \mathbb{N}$, for $(\mathsf{pk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ **honestly generated**, and all Υ, Π such that Υ satisfies Π:

$$\mathsf{Decrypt}(\mathsf{KeyGen}(\mathsf{msk}, \mathsf{pk}, \Upsilon), \Upsilon, \mathsf{Encrypt}(\mathsf{pk}, \Pi, \mathsf{m}), \Pi) = \mathsf{m}$$

Bounded:

Number of attributes in the scheme is **bounded** by $q \in \mathbb{N}$

Attribute Based Encryption Security: Indistinguishability

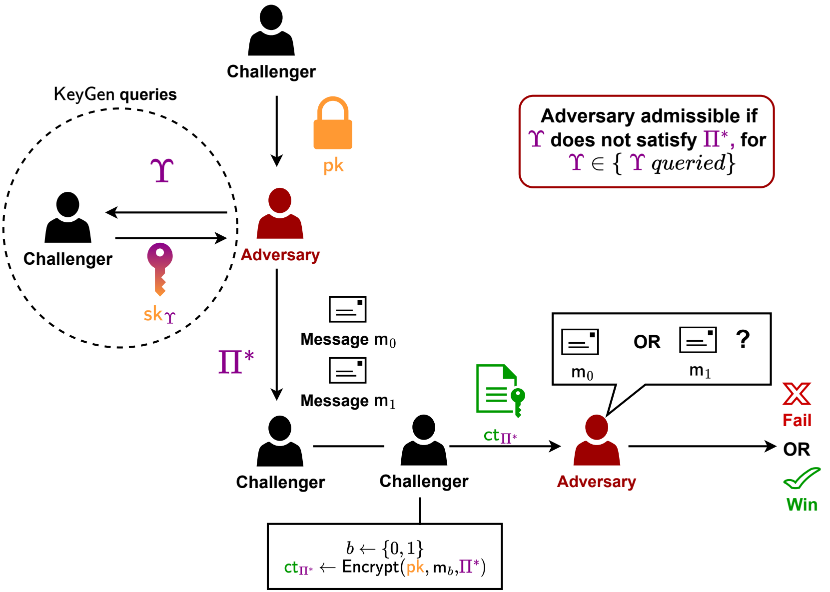


Table of contents

Cryptographic Accumulators [Bd94]

Asymmetric Cryptographic Accumulator

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{pk_{acc}}, \mathsf{sk_{acc}})$
- $\mathsf{Eval}((\mathsf{sk_{acc}},)\mathsf{pk_{acc}}, \mathcal{X}) \to \mathsf{acc}_\mathcal{X}$
- $\mathsf{WitCreate}((\mathsf{sk_{acc}},)\mathsf{pk_{acc}}, \mathsf{acc}_\mathcal{X}, \mathcal{X}, y) \to \mathsf{wit}_y$
- $\mathsf{Verify}(\mathsf{pk_{acc}}, \mathsf{acc}_\mathcal{X}, \mathsf{wit}_y, y) \to 0/1$

Symmetric Cryptographic Accumulator

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{pk_{acc}}, \mathsf{sk_{acc}})$
- $\mathsf{Eval}((\mathsf{sk_{acc}},)\mathsf{pk_{acc}}, \mathcal{X}) \to \mathsf{acc}_\mathcal{X}$
- $\mathsf{Verify}(\mathsf{pk_{acc}}, \mathsf{acc}_\mathcal{X}, y) \to 0/1$

Asymmetric Accumulators: Properties and Requirements

Correctness:

For all $\lambda \in \mathbb{N}$, for $(\mathsf{pk_{acc}}, \mathsf{sk_{acc}}) \leftarrow \mathsf{Setup}(1^\lambda)$ **honestly generated**, for all $y \in \mathcal{X}$ and $\mathsf{acc}_{\mathcal{X}} \leftarrow \mathsf{Eval}((\mathsf{sk_{acc}},)\mathsf{pk_{acc}}, \mathcal{X})$:

$$\mathsf{Verify}(\mathsf{pk_{acc}}, \mathsf{acc}_{\mathcal{X}}, \mathsf{WitCreate}((\mathsf{sk_{acc}},)\mathsf{pk_{acc}}, \mathsf{acc}_{\mathcal{X}}, \mathcal{X}, y), y) = 1$$

Bounded:

For all $\mathcal{X}$, $|\mathcal{X}| \leq q$, where $q \in \mathbb{N}$ is a **bound** given as input of Gen.

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

Accumulators Security: Collision Resistance

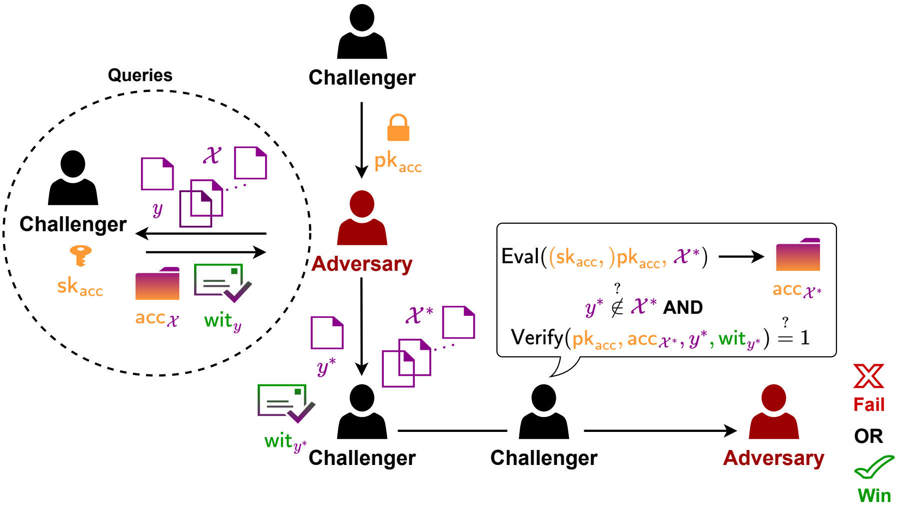


Table of contents

Dually Computable Cryptographic Accumulators

Dually Computable Cryptographic Accumulators

- $\mathsf{Gen}(1^\lambda) \rightarrow (\mathsf{pk_{acc}}, \mathsf{sk_{acc}})$
- $\mathsf{Eval}(\mathsf{sk_{acc}}, \mathcal{X}) \rightarrow \mathsf{acc}_{\mathcal{X}}$ Private Evaluation
- $\mathsf{WitCreate}(\mathsf{pk_{acc}}, \mathsf{acc}_{\mathcal{X}}, \mathcal{X}, y) \rightarrow \mathsf{wit}_y$ Public Witness Generation
- $\mathsf{Verify}(\mathsf{pk_{acc}}, \mathsf{acc}_{\mathcal{X}}, \mathsf{wit}_y, y) \rightarrow 0/1$

Two additional algorithms

- $\mathsf{PublicEval}(\mathsf{pk_{acc}}, \mathcal{X}) \rightarrow \mathsf{accp}_{\mathcal{X}}$
- $\mathsf{PublicVerify}(\mathsf{pk_{acc}}, \mathsf{accp}_{\mathcal{X}}, \mathsf{wit}_y, y) \rightarrow 0/1$

Dually Computable Cryptographic Accumulators
Correctness

Correctness:

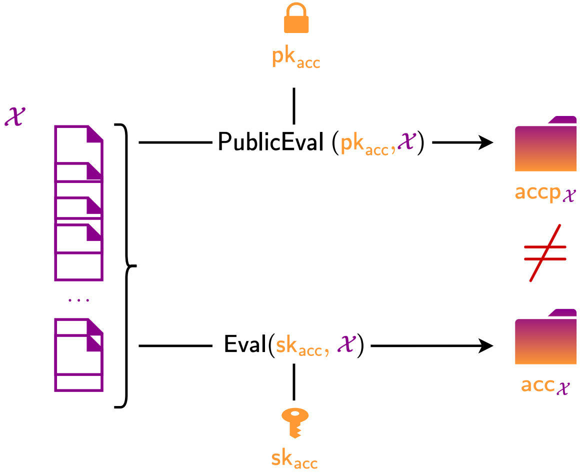
For all $\lambda \in \mathbb{N}$, for $(\mathsf{pk_{acc}}, \mathsf{sk_{acc}}) \leftarrow \mathsf{Setup}(1^\lambda)$ **honestly generated**, for all $y \in \mathcal{X}$, $\mathsf{acc}_{\mathcal{X}} \leftarrow \mathsf{Eval}(\mathsf{sk_{acc}}\mathcal{X})$ and $\mathsf{accp}_{\mathcal{X}} \leftarrow \mathsf{PublicEval}(\mathsf{pk_{acc}}, \mathcal{X})$:

$$\mathsf{Verify}(\mathsf{pk_{acc}}, \mathsf{acc}_{\mathcal{X}}, \mathsf{WitCreate}(\mathsf{pk_{acc}}, \mathsf{acc}_{\mathcal{X}}, \mathcal{X}, y), y) = 1$$

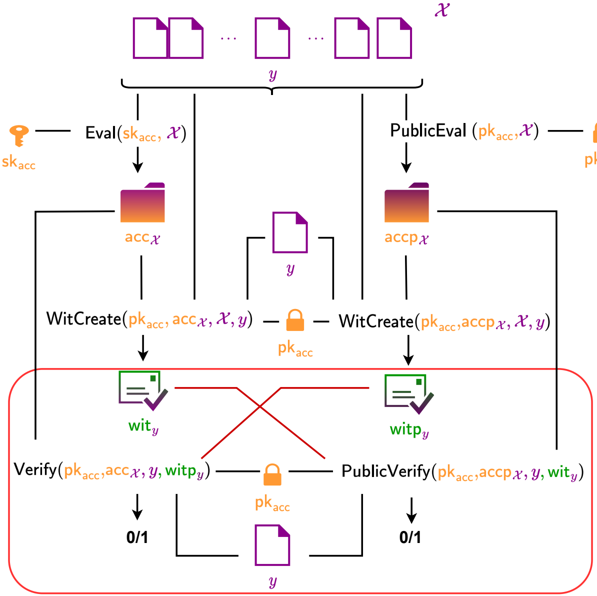
and

$$\mathsf{PublicVerify}(\mathsf{pk_{acc}}, \mathsf{accp}_{\mathcal{X}}, \mathsf{WitCreate}(\mathsf{pk_{acc}}, \mathsf{accp}_{\mathcal{X}}, \mathcal{X}, y), y) = 1$$

Distinguishability



Correctness of Duality



Dually Computable Accumulators Security : Dual Collision Resistance

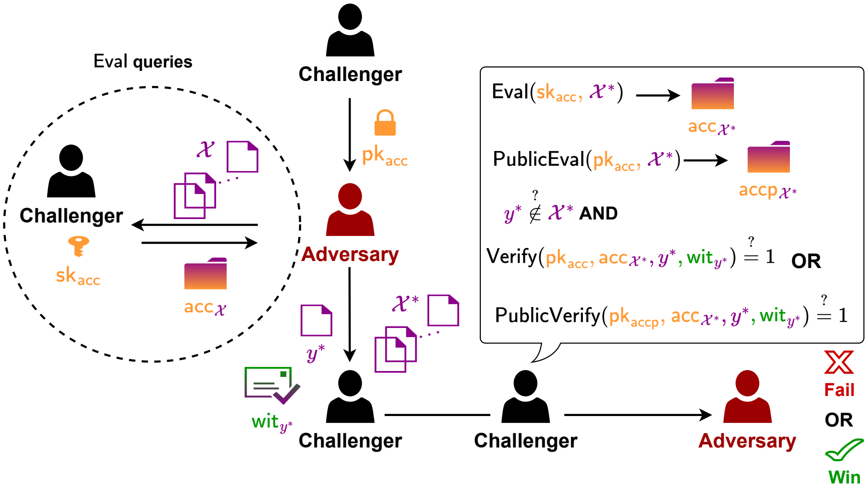


Table of contents

CP-ABE From Dually Computable Cryptographic Accumulators

Main Idea

- Use Eval on Υ and set $\mathsf{sk}_\Upsilon = \mathsf{acc}_\Upsilon$
- Use PublicEval on Π, randomize accp_Π to get accp'_Π and set $\mathsf{ct}_\Pi = \mathsf{m} \oplus \mathsf{accp}'_\Pi$
- To decrypt, compute accp'_Π

Security and Correctness

- *Protection against unauthorized decryption:* accp'_Π computable only if $\mathsf{acc}_\Upsilon \cap \mathsf{accp}_\Pi \neq \varnothing$
- *Correctness:* $\mathsf{acc}_\Upsilon \cap \mathsf{accp}_\Pi \neq \varnothing \Longleftrightarrow \Upsilon$ satisfies Π

Accumulators Over Access Policies

Access Policies: *disjunctions of conjunctions*

Our Idea

- $\mathcal{H}$: {set of attributes} $\rightarrow$ accumulator space, hash function
- For the access policy:
  - run $\mathcal{H}$ on *each set* representing a *conjunction* of Π
  - add the obtained element to a set $\mathcal{Y}$
  - run PublicEval on $\mathcal{Y}$

An Example

- $\Pi = (a_1 \wedge a_3) \vee (a_2 \wedge a_4)$
- $\mathcal{Y} = \{\mathcal{H}(\{a_1, a_3\}), \mathcal{H}(\{a_2, a_4\})\}$

Intersection

Intersection And Satisfied Access Policy

- For the attributes set:
  - run $\mathcal{H}$ on *all non-empty subsets* of Υ
  - add all obtained elements to a set $\mathcal{X}$
  - run Eval on $\mathcal{X}$
- For the intersection:
  - Π is satisfied by Υ
  - $\iff \exists\, S \subseteq \Upsilon$ that satisfies one conjunction of Π
  - By construction, $\mathcal{H}(S) \in \mathcal{X}$ and $\mathcal{H}(S) \in \mathcal{Y}$
  - $\iff \mathsf{acc}_{\Upsilon} \cap \mathsf{accp}_{\Pi} = \{\mathcal{H}(S)\} \neq \varnothing$

An Example

- $\Pi = (a_1 \wedge a_3) \vee (a_2 \wedge a_4)$, $\mathcal{Y} = \{\mathcal{H}(\{a_1, a_3\}), \mathcal{H}(\{a_2, a_4\})\}$
- $\Upsilon = \{a_1, a_2, a_3\}$, $\mathcal{X} = \{\mathcal{H}(\{a_1\}), \mathcal{H}(\{a_2\}), \cdots, \mathcal{H}(\{a_1, a_2, a_3\})\}$
- $\mathcal{H}(\{a_1, a_3\}) \in \mathcal{X} \cap \mathcal{Y}$

Table of contents

Asymmetric Bilinear Pairing Group

Cyclic (multiplicative) groups

Generator of $\mathbb{G}_2$

$$\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$$

Prime number

Generator of $\mathbb{G}_1$

Asymmetric bilinear pairing

$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 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 of $\mathbb{G}_T$ (**non-degenerate**)
- $e(X, Y)$ **efficiently computable** for all $X \in \mathbb{G}_1, Y \in \mathbb{G}_2$

Asymmetric Bilinear Pairing Group

Cyclic (multiplicative) groups

Generator of $\mathbb{G}_2$

$$\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$$

+ ***Efficient algorithm to decide membership of the groups***

Prime number

Generator of $\mathbb{G}_1$

Asymmetric bilinear pairing

$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 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 of $\mathbb{G}_T$ (**non-degenerate**)
- $e(X, Y)$ **efficiently computable** for all $X \in \mathbb{G}_1, Y \in \mathbb{G}_2$

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

Fixed constant dimension

$$\left(\ \Gamma, n,\ \mathbb{D} = (\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n), \mathbb{D}^* = (\boldsymbol{d}_1^*, \cdots, \boldsymbol{d}_n^*)\ \right)$$

Asymmetric bilinear pairing group

Random bases of $\mathbb{Z}_p^n$

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

Fixed constant dimension

$$\left(\Gamma, n, \mathbb{D} = (\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n), \mathbb{D}^* = (\boldsymbol{d}_1^*, \cdots, \boldsymbol{d}_n^*) \right)$$

Asymmetric bilinear pairing group

Random bases of $\mathbb{Z}_p^n$

Dual orthonormal, i.e. :
•$\boldsymbol{d}_i \cdot \boldsymbol{d}_j^* = 0$ whenever $i \neq j$
•$\boldsymbol{d}_i \cdot \boldsymbol{d}_i^* = \psi$ for all i, where $\psi \in \mathbb{Z}_p^*$

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

Fixed constant dimension

$$\left(\Gamma, n, \mathbb{D} = (\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n), \mathbb{D}^* = (\boldsymbol{d}_1^*, \cdots, \boldsymbol{d}_n^*) \right)$$

Asymmetric bilinear pairing group

Random bases of $\mathbb{Z}_p^n$

$(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^n)$

Dual orthonormal, i.e. :
- $\boldsymbol{d}_i \cdot \boldsymbol{d}_j^* = 0$ **whenever** $i \neq j$
- $\boldsymbol{d}_i \cdot \boldsymbol{d}_i^* = \psi$ **for all** i**, where** $\psi \in \mathbb{Z}_p^*$

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

Fixed constant dimension

$$\big(\ \Gamma,\ n,\ \mathbb{D} = (\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n), \mathbb{D}^* = (\boldsymbol{d}_1^*, \cdots, \boldsymbol{d}_n^*)\ \big)$$

Asymmetric bilinear pairing group

Random bases of $\mathbb{Z}_p^n$

$(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^n)$

Dual orthonormal, i.e. :
- $\boldsymbol{d}_i \cdot \boldsymbol{d}_j^* = 0$ **whenever** $i \neq j$
- $\boldsymbol{d}_i \cdot \boldsymbol{d}_i^* = \psi$ **for all** i**, where** $\psi \in \mathbb{Z}_p^*$

In our settings, $n = 2, \mathbb{D} = (\boldsymbol{d}_1, \boldsymbol{d}_2), \mathbb{D}^* = (\boldsymbol{d}_1^*, \boldsymbol{d}_2^*)$

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

Fixed constant dimension

$$\left(\Gamma, n, \mathbb{D} = (\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n), \mathbb{D}^* = (\boldsymbol{d}_1^*, \cdots, \boldsymbol{d}_n^*) \right)$$

Asymmetric bilinear pairing group

Random bases of $\mathbb{Z}_p^n$

$(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^n)$

Dual orthonormal, i.e. :
- $\boldsymbol{d}_i \cdot \boldsymbol{d}_j^* = 0$ **whenever** $i \neq j$
- $\boldsymbol{d}_i \cdot \boldsymbol{d}_i^* = \psi$ **for all** i**, where** $\psi \in \mathbb{Z}_p^*$

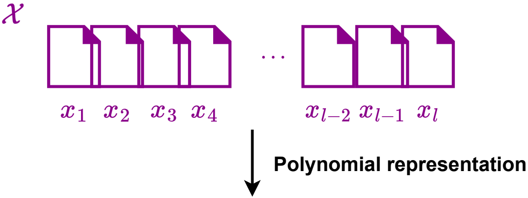
In our settings, $n = 2, \mathbb{D} = (\boldsymbol{d}_1, \boldsymbol{d}_2), \mathbb{D}^* = (\boldsymbol{d}_1^*, \boldsymbol{d}_2^*)$

All elements of $\mathbb{D}, \mathbb{D}^*$ are vectors!

Pairings and Vectors

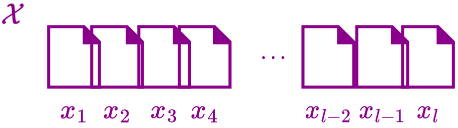
- $g_i \in \mathbb{G}_i$ group element for $i \in \{1, 2\}$, $\boldsymbol{u}, \boldsymbol{v}$ two vectors of length ℓ
- $g_i^{\boldsymbol{v}} := (g_i^{v_1}, \cdots, g_i^{v_\ell})$
- $g_i^{\boldsymbol{u} \cdot \boldsymbol{v}} = g_i^{\alpha}$, where $\alpha = \boldsymbol{u} \cdot \boldsymbol{v} = u_1 \cdot v_1 + u_2 \cdot v_2 + \cdots + u_\ell \cdot v_\ell$
- $$e(g_1^{\boldsymbol{u}}, g_2^{\boldsymbol{v}}) := \prod_{i=1}^{\ell} e(g_1^{u_i}, g_2^{v_i}) = e(g_1, g_2)^{\boldsymbol{u} \cdot \boldsymbol{v}}$$

Characteristic Polynomial



$$Ch_{\mathcal{X}}[Z] = (x_1+Z)\cdot(x_2+Z)\cdots(x_l+Z) = \prod_{i=1}^{l}(x_i+Z) = \sum_{i=0}^{l} a_i Z^i$$

Characteristic Polynomial



$\downarrow$ **Polynomial representation**

$$Ch_{\mathcal{X}}[Z] = (x_1+Z)\cdot(x_2+Z)\cdots(x_l+Z) = \prod_{i=1}^{l}(x_i+Z) = \sum_{i=0}^{l} a_i Z^i$$

Evaluation at point s: $\mathrm{Ch}_{\mathcal{X}}(s) = \prod_{i=1}^{l}(x_i+s) = \sum_{i=0}^{l} a_i s^i$

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

Idea: using [Ngu05]'s pairing-based accumulator:

- $s \leftarrow \mathbb{Z}_p^*$
- $\Gamma = (p, \mathbb{G}, \mathbb{G}_T, g, e)$ **symmetric** pairing group
- $\mathsf{acc}_{\mathcal{X}} = g^{Ch_{\mathcal{X}}(s)}$
- $\mathsf{wit}_y = g^{Ch_{\mathcal{X} \setminus \{y\}}(s)}$
- *Verification:* $e(\mathsf{acc}_{\mathcal{X}}, g) \stackrel{?}{=} e(\mathsf{wit}_y, g^y \cdot g^s)$

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

Idea: using [Ngu05]'s pairing-based accumulator:

- $\boxed{\mathsf{sk}_{\mathsf{acc}} = s \leftarrow \mathbb{Z}_p^*}$
- $\Gamma = (p, \mathbb{G}, \mathbb{G}_T, g, e)$ **symmetric** pairing group
- $\mathsf{acc}_{\mathcal{X}} = g^{Ch_{\mathcal{X}}(s)}$ privately computed
- $\mathsf{wit}_y = g^{Ch_{\mathcal{X} \setminus \{y\}}(s)}$ privately computed
- *Verification:* $e(\mathsf{acc}_{\mathcal{X}}, g) \stackrel{?}{=} e(\mathsf{wit}_y, g^y \cdot g^s)$ privately computed

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

Idea: using [Ngu05]'s pairing-based accumulator:

- $\mathsf{sk_{acc}} = s \leftarrow \mathbb{Z}_p^*$
- $\boxed{\mathsf{pk_{acc}} = (\mathit{\Gamma} = (p, \mathbb{G}, \mathbb{G}_T, g, e), g^s, g^{s^2}, \cdots, g^{s^q})}$ $\quad q \in \mathbb{N}$ **bound**
- $\mathsf{acc}_{\mathcal{X}} = g^{Ch_{\mathcal{X}}(s)} = g^{\sum_{i=0}^{q} a_i s^i} = \prod_{i=0}^{q} (g^{s^i})^{a_i}$ $\quad$ publicly computed
- $\mathsf{wit}_y = g^{Ch_{\mathcal{X}\setminus\{y\}}(s)} = g^{\sum_{i=0}^{q} b_i s^i} = \prod_{i=0}^{q} (g^{s^i})^{b_i}$ $\quad$ publicly computed
- *Verification:* $e(\mathsf{acc}_{\mathcal{X}}, g) \stackrel{?}{=} e(\mathsf{wit}_y, g^y \cdot g^s)$ $\quad$ publicly computed

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

Idea: using [Ngu05]'s pairing-based accumulator:

- $s \leftarrow \mathbb{Z}_p^*$
- $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ **asymmetric** pairing group
- $\mathsf{acc}_{\mathcal{X}} = g_{\mathbf{1}}^{Ch_{\mathcal{X}}(s)}$
- $\mathsf{wit}_y = g_{\mathbf{2}}^{Ch_{\mathcal{X}\setminus\{y\}}(s)}$
- *Verification:* $e(\mathsf{acc}_{\mathcal{X}}, g_{\mathbf{2}}) \stackrel{?}{=} e(g_{\mathbf{1}}^{y} \cdot g_{\mathbf{1}}^{s}, \mathsf{wit}_y)$

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

Idea: using [Ngu05]'s pairing-based accumulator:

- $\mathsf{sk}_{\mathsf{acc}} = s \leftarrow \mathbb{Z}_p^*$
- $\boxed{\mathsf{pk}_{\mathsf{acc}} = (\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e), g_2^s, g_2^{s^2}, \cdots, g_2^{s^q})}$
- $\mathsf{acc}_{\mathcal{X}} = g_1^{Ch_{\mathcal{X}}(s)}$ privately computed
- $\mathsf{wit}_y = g_2^{Ch_{\mathcal{X}\setminus\{y\}}(s)} = g_2^{\sum_{i=0}^{q} b_i s^i} = \prod_{i=0}^{q} (g_2^{s^i})^{b_i}$ publicly computed
- *Verification:* $e(\mathsf{acc}_{\mathcal{X}}, g_2) \stackrel{?}{=} e(g_1^y \cdot g_1^s, \mathsf{wit}_y)$ **privately** computed

Our Dually Computable Accumulator

First step: *private* evaluation and *public* witness generation

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

- $\mathsf{sk}_{\mathsf{acc}} = (s \leftarrow \mathbb{Z}_p^*, \boxed{(\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2)})$
- $\boxed{\mathsf{pk}_{\mathsf{acc}} = (\Gamma, g_2^{\boldsymbol{d}_2^*}, g_2^{\boldsymbol{d}_2^* s}, g_2^{\boldsymbol{d}_2^* s^2}, \cdots, g_2^{\boldsymbol{d}_2^* s^q}, g_2^{\boldsymbol{d}_1^*}, g_1^{\boldsymbol{d}_2}, g_1^{\boldsymbol{d}_2 s})}$
- $\mathsf{acc}_{\mathcal{X}} = g_1^{\boldsymbol{d}_1 Ch_{\mathcal{X}}(s)}$ privately computed
- $\mathsf{wit}_y = g_2^{\boldsymbol{d}_2^* Ch_{\mathcal{X}\setminus\{y\}}(s)} = g_2^{\boldsymbol{d}_2^* \sum_{i=0}^{q} b_i s^i} = \prod_{i=0}^{q} (g_2^{\boldsymbol{d}_2^* s^i})^{b_i}$ publicly computed
- *Verification:* $e(\mathsf{acc}_{\mathcal{X}}, g_2^{\boldsymbol{d}_1^*}) \stackrel{?}{=} e(g_1^{\boldsymbol{d}_2 y} \cdot g_1^{\boldsymbol{d}_2 s}, \mathsf{wit}_y)$ publicly computed

Our Dually Computable Accumulator

Second step: *public* evaluation and *public* verification

- $\mathsf{sk}_{\mathsf{acc}} = (s \leftarrow \mathbb{Z}_p^*, (\mathbb{D}, \mathbb{D}^*) \leftarrow \mathsf{Dual}(\mathbb{Z}_p^2))$

- $\mathsf{pk}_{\mathsf{acc}} =$
$(\Gamma, g_2^{d_2^*}, g_2^{d_2^* s}, g_2^{d_2^* s^2}, \cdots, g_2^{d_2^* s^q}, g_2^{d_1^*}, g_1^{d_2}, g_1^{d_2 s}, \boxed{g_2^{d_1^* s}, \cdots, g_2^{d_1^* s^q}, g_1^{d_1}})$

- $\mathsf{accp}_{\mathcal{X}} = g_2^{d_1^* Ch_{\mathcal{X}}(s)} = g_2^{d_1^* \sum_{i=0}^{q} a_i s^i} = \prod_{i=0}^{q} (g_2^{d_1^* s^i})^{a_i}$ publicly computed

- *Verification:* $e(g_1^{d_1}, \mathsf{accp}_{\mathcal{X}}) \stackrel{?}{=} e(g_1^{d_2 y} \cdot g_1^{d_2 s}, \mathsf{wit}_y)$ publicly computed

All Properties Are Satisfied

- **Small sizes:** $|\mathsf{acc}| = 2 \cdot |\mathbb{G}_1|$, $|\mathsf{accp}| = 2 \cdot |\mathbb{G}_2|$, $|\mathsf{wit}| = 2 \cdot |\mathbb{G}_2|$

All Properties Are Satisfied

- **Small sizes:** $|\mathsf{acc}| = 2 \cdot |\mathbb{G}_1|$, $|\mathsf{accp}| = 2 \cdot |\mathbb{G}_2|$, $|\mathsf{wit}| = 2 \cdot |\mathbb{G}_2|$
- **Correctness**: [Ngu05]'s correctness + DPVS

All Properties Are Satisfied

- **Small sizes:** $|\mathsf{acc}| = 2 \cdot |\mathbb{G}_1|$, $|\mathsf{accp}| = 2 \cdot |\mathbb{G}_2|$, $|\mathsf{wit}| = 2 \cdot |\mathbb{G}_2|$
- **Correctness**: [Ngu05]'s correctness + DPVS
- **Distinguishability**: $\mathsf{acc}_{\mathcal{X}} \in \mathbb{G}_1^2 \neq \mathsf{accp}_{\mathcal{X}} \in \mathbb{G}_2^2$

All Properties Are Satisfied

- **Small sizes:** $|\mathsf{acc}| = 2 \cdot |\mathbb{G}_1|$, $|\mathsf{accp}| = 2 \cdot |\mathbb{G}_2|$, $|\mathsf{wit}| = 2 \cdot |\mathbb{G}_2|$
- **Correctness**: [Ngu05]'s correctness + DPVS
- **Distinguishability**: $\mathsf{acc}_{\mathcal{X}} \in \mathbb{G}_1^2 \neq \mathsf{accp}_{\mathcal{X}} \in \mathbb{G}_2^2$
- **Correctness of duality**:

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

All Properties Are Satisfied

- **Small sizes:** $|\mathsf{acc}| = 2 \cdot |\mathbb{G}_1|$, $|\mathsf{accp}| = 2 \cdot |\mathbb{G}_2|$, $|\mathsf{wit}| = 2 \cdot |\mathbb{G}_2|$
- **Correctness**: [Ngu05]'s correctness + DPVS
- **Distinguishability**: $\mathsf{acc}_{\mathcal{X}} \in \mathbb{G}_1^2 \neq \mathsf{accp}_{\mathcal{X}} \in \mathbb{G}_2^2$
- **Correctness of duality**:

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

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

Our CP-ABE Scheme

- Combination of previous ideas + our dually computable accumulator
- Protection against unauthorized decryption: relies on *characteristic polynomial property*
- Advantages:
  - Constant size ciphertext $(2 \cdot |\mathbb{G}_2|)$
  - Constant size secret key $(2 \cdot |\mathbb{G}_1|)$
- Drawbacks:
  - Public key size exponential in the number of attributes in the scheme
  - No generic construction and No security reduction
  - Simple access policies

Table of contents

Other Main Contribution

- New pairing-based Key Policy Attribute-Based Encryption with both *constant size ciphertext and secret keys* based on Cryptographic Accumulators

Other Auxiliary Contribution

- First (pairing-based) Cryptographic Accumulator scheme with *private evaluation* and *public witness generation*

All results are in an article accepted at CANS 2023

Table of contents

Conclusion

- Aim of this Phd thesis: **building efficient and secure schemes for data sharing**
- How did we do this? By **establishing relations between primitives**
  - Link between Broadcast Encryption and Identity-Based Encryption with Wildcards
  - Link between Attribute-Based Encryption and Cryptographic Accumulators
- Means: introducing **new properties and functionalities** for building block primitives

Summary of Our Works

Contribution	In submission	Accepted
Broadcast Encryption from WIBE		CANS 2022
ABE from Accumulators		CANS 2023
ABE from WIBE	$\checkmark$	
SoK on Accumulators	$\checkmark$	

Future Works

Improving current results

- Create a constant size ciphertext pattern-hiding Identity-Based Encryption with Wildcards scheme
- Develop a generic construction of ABE from Dually Computable Cryptographic Accumulators
- Reduce our CP-ABE public key size and deal with fine-grained access policies

Going further

- Develop quantum resistant schemes
- Study the relation between Cryptographic Accumulators and another recently introduced primitive, Locally Verifiable Aggregate Signature[a]

[a] Short article about it accepted at CFAIL 2023

Bibliography I

Michel Abdalla, Dario Catalano, Alex Dent, John Malone-Lee, Gregory Neven, and Nigel Smart.
Identity-based encryption gone wild.
pages 300–311, 2006.

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.

Amos Fiat and Moni Naor.
Broadcast encryption.
pages 480–491, 1994.

Jihye Kim, Seunghwa Lee, Jiwon Lee, and Hyunok Oh.
Scalable wildcarded identity-based encryption.
pages 269–287, 2018.

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

Bibliography II

Amit Sahai and Brent R. Waters.
Fuzzy identity-based encryption.
pages 457–473, 2005.