FABEO: Fast Attribute-based Encryption with Optimal Security

Doreen Riepel[1], Hoeteck Wee[2]

November 9, 2022

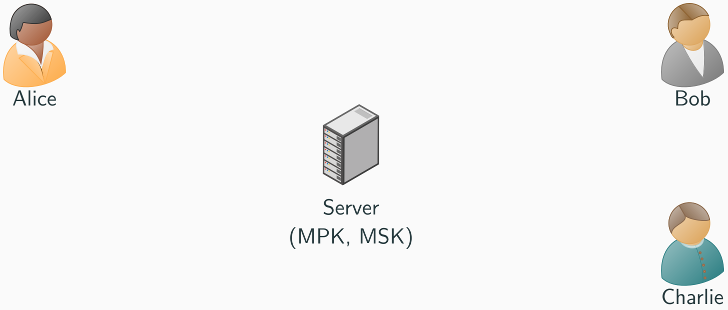
[1]Ruhr-Universität Bochum
[2]NTT Research

Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.

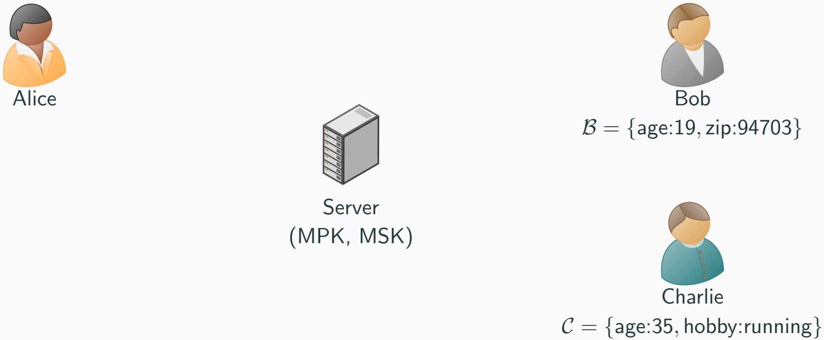
Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.



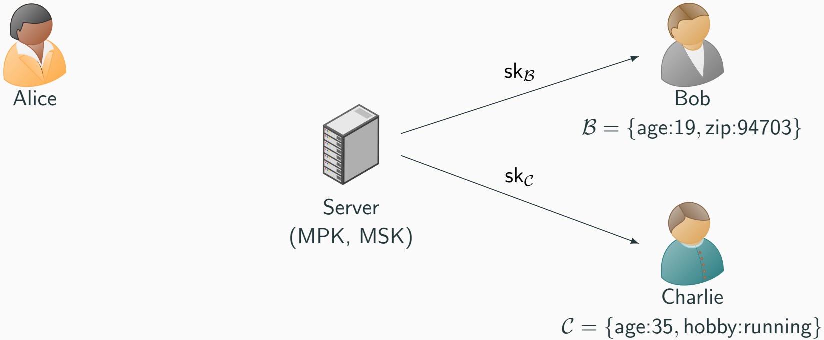
Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.



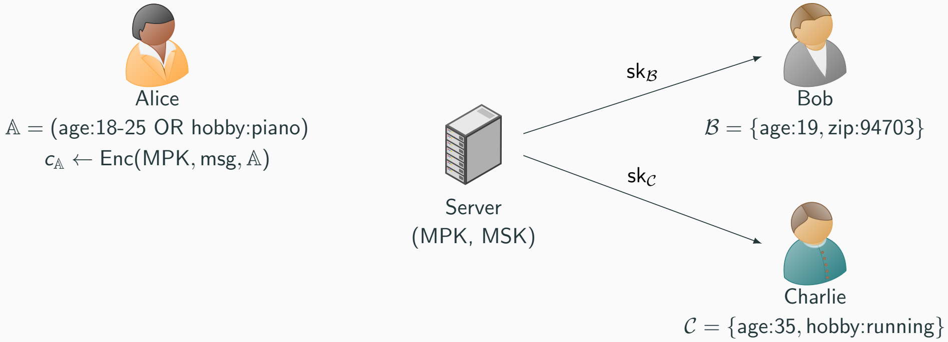
Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.



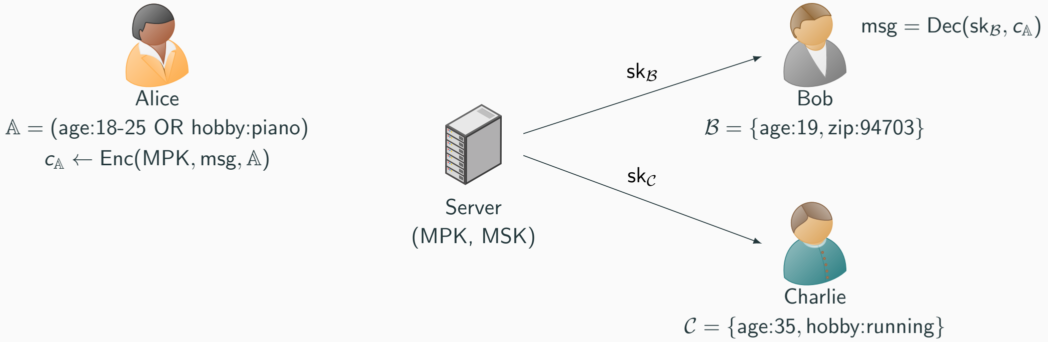
Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.



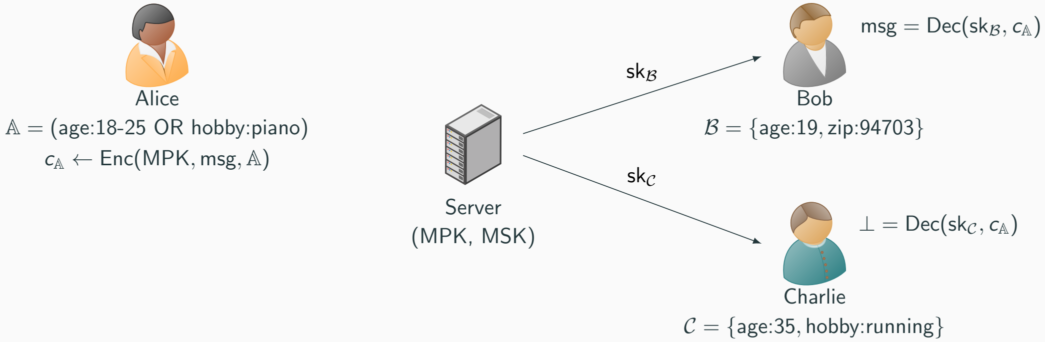
Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.



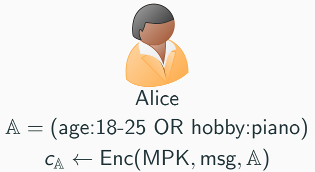
Motivation

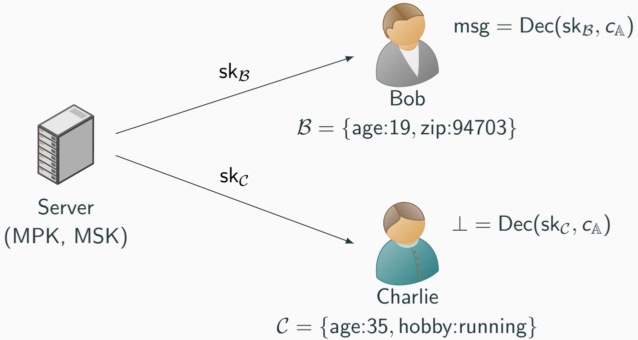
Attribute-based encryption enables fine-grained access control on encrypted data.



Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.

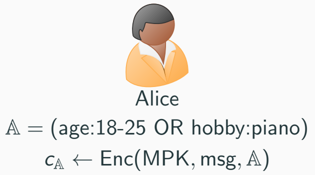


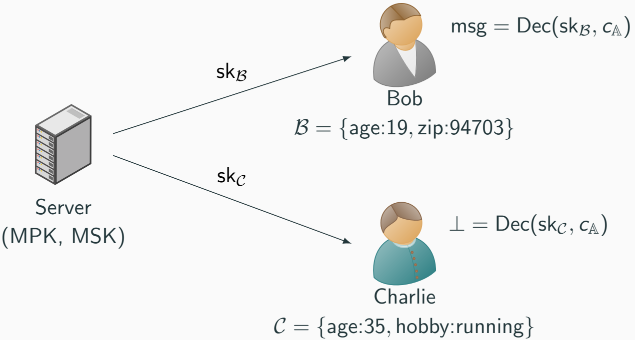


- Applications:
  - electronic medical records
  - online social networks
  - private key storage across data centers
  - ...

Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.

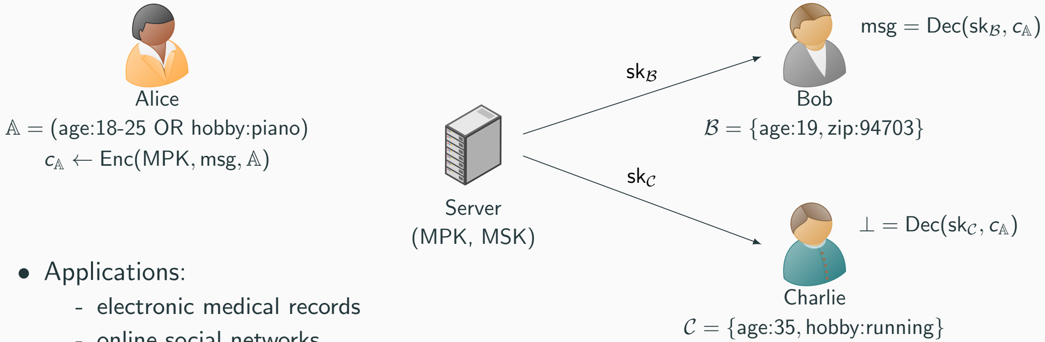




- Applications:
    - electronic medical records
    - online social networks
    - private key storage across data centers
    - ...
- ciphertext-policy (CP-ABE) vs. key-policy (KP-ABE)

Motivation

Attribute-based encryption enables fine-grained access control on encrypted data.



- Applications:
  - electronic medical records
  - online social networks
  - private key storage across data centers
  - ...
- ciphertext-policy (CP-ABE) vs. key-policy (KP-ABE)

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$

- Setup $\to$ (MPK, MSK): master public key and secret key

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P}: \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$

Attribute-based Encryption

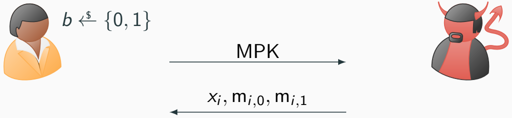
ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$

Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$

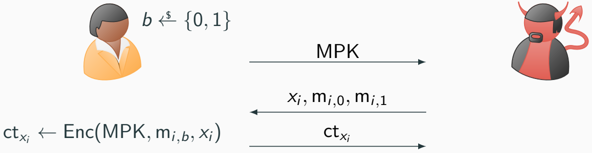
- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$



Attribute-based Encryption

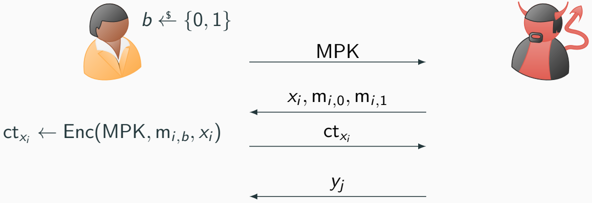
ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$



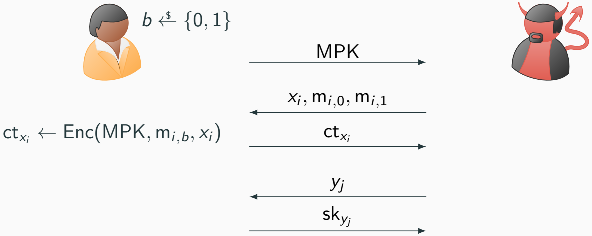
ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$



ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

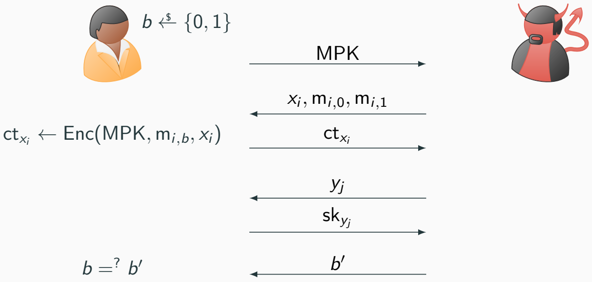
- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \bot\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$



Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

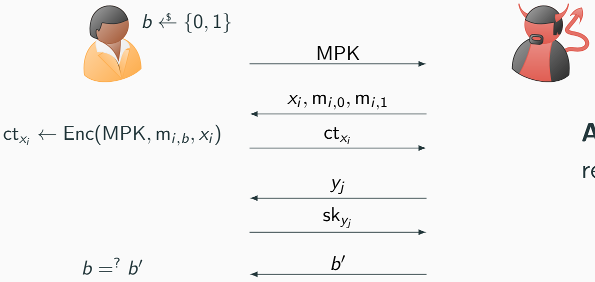
- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$



Attribute-based Encryption

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$



Adaptive Security: For all x_i, y_j, we require $\mathsf{P}(x_i, y_j) = 0$

ABE for a boolean predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

- $\mathsf{Setup} \to (\mathsf{MPK}, \mathsf{MSK})$: master public key and secret key
- $\mathsf{Enc}(\mathsf{MPK}, \mathsf{m}, x) \to \mathsf{ct}_x$: ciphertexts are associated with $x \in \mathcal{X}$ in addition to a plaintext
- $\mathsf{KeyGen}(\mathsf{MSK}, y) \to \mathsf{sk}_y$: secret keys are associated with $y \in \mathcal{Y}$
- $\mathsf{Dec}(x, y, \mathsf{ct}_x, \mathsf{sk}_y) \to \{\mathsf{m}, \perp\}$: decryption is successful if and only if $\mathsf{P}(x, y) = 1$

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

MPK →

← $x_i, \mathsf{m}_{i,0}, \mathsf{m}_{i,1}$

$\mathsf{ct}_{x_i} \leftarrow \mathsf{Enc}(\mathsf{MPK}, \mathsf{m}_{i,b}, x_i)$ — ct_{x_i} →

← y_j

sk_{y_j} →

$b \stackrel{?}{=} b'$ — ← b'

Adaptive Security: For all x_i, y_j, we require $\mathsf{P}(x_i, y_j) = 0$

$\Rightarrow$ (many-ct, many-sk) security

Attribute-based Encryption

Asymmetric Bilinear Groups

- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- $\mathbb{G}_1$ is smaller and faster
- supports efficient hashing into $\mathbb{G}_1$

Attribute-based Encryption

Asymmetric Bilinear Groups

- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- $\mathbb{G}_1$ is smaller and faster
- supports efficient hashing into $\mathbb{G}_1$

Generic Group Model (GGM)

- group operations via oracle access
- allows to prove lower bounds for generic adversaries
- much simpler and more efficient schemes

Our Contributions

New CP-ABE and KP-ABE Schemes

1. support expressive policies (boolean formula and monotone span programs)

Our Contributions

New CP-ABE and KP-ABE Schemes

1. support expressive policies (boolean formula and monotone span programs)
2. tight, adaptive (many-ct, many-sk)-security in the GGM and ROM
    - Adv $\leq q^2/|\mathbb{G}|$

Our Contributions

New CP-ABE and KP-ABE Schemes

1. support expressive policies (boolean formula and monotone span programs)
2. tight, adaptive (many-ct, many-sk)-security in the GGM and ROM
   - Adv $\leq q^2/|\mathbb{G}|$
3. smaller ciphertext/key sizes and better efficiency
   - most elements in $\mathbb{G}_1$
   - randomness re-use
   - fewer pairings

Our Contributions

New CP-ABE and KP-ABE Schemes

1. support expressive policies (boolean formula and monotone span programs)
2. tight, adaptive (many-ct, many-sk)-security in the GGM and ROM
    - $\mathsf{Adv} \leq q^2/|\mathbb{G}|$
3. smaller ciphertext/key sizes and better efficiency
    - most elements in $\mathbb{G}_1$
    - randomness re-use
    - fewer pairings

Additional Properties

- no restrictions on size of policies or attribute sets
- arbitrary strings as attributes (e.g., street addresses)

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\mathbf{b}$, $\mathbf{s}$, $\mathbf{r}$, α

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

↳ $\mathbf{s}$ = encryption randomness

↳ $\mathbf{r}$ = key generation randomness

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

$$\begin{aligned} \mathsf{MPK} &= [\mathbf{b}]_1, [\alpha]_T \\ \mathsf{ct}_x &= [c_x^1(\mathbf{s} \otimes \mathbf{b})]_1, [c_x^2(\mathbf{s})]_2 \\ \mathsf{sk}_y &= [k_y^1(\alpha, \mathbf{r}, \mathbf{b} \otimes \mathbf{r})]_1, [k_y^2(\mathbf{r})]_2 \end{aligned}$$

↳ $\mathbf{s}$ = encryption randomness

↳ $\mathbf{r}$ = key generation randomness

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

$$\mathsf{MPK} = [\mathbf{b}]_1, [\alpha]_T$$

$$\mathsf{ct}_x = [c_x^1(\mathbf{s} \otimes \mathbf{b})]_1, [c_x^2(\mathbf{s})]_2$$

$$\mathsf{sk}_y = [k_y^1(\alpha, \mathbf{r}, \mathbf{b} \otimes \mathbf{r})]_1, [k_y^2(\mathbf{r})]_2$$

↳ $\mathbf{s}$ = encryption randomness

↳ $\mathbf{r}$ = key generation randomness

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

↳ $\mathbf{s}$ = encryption randomness

↳ $\mathbf{r}$ = key generation randomness

$$\mathsf{MPK} = [\mathbf{b}]_1, [\alpha]_T$$
$$\mathsf{ct}_x = [c_x^1(\mathbf{s} \otimes \mathbf{b})]_1, [c_x^2(\mathbf{s})]_2$$
$$\mathsf{sk}_y = [k_y^1(\alpha, \mathbf{r}, \mathbf{b} \otimes \mathbf{r})]_1, [k_y^2(\mathbf{r})]_2$$

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

$$\mathsf{MPK} = [\mathbf{b}]_1, [\alpha]_T$$

$$\mathsf{ct}_x = [c_x^1(\mathbf{s} \otimes \mathbf{b})]_1, [c_x^2(\mathbf{s})]_2$$

$$\mathsf{sk}_y = [k_y^1(\alpha, \mathbf{r}, \mathbf{b} \otimes \mathbf{r})]_1, [k_y^2(\mathbf{r})]_2$$

↓ $\mathsf{P}(x, y) = 1$ (correctness)

$$\mathsf{K} = [\alpha \mathbf{s}[1]]_T$$

↳ $\mathbf{s}$ = encryption randomness

↳ $\mathbf{r}$ = key generation randomness

Our Contributions

Main Technical Result

For many ABE schemes, (one-ct, one-sk)-security implies tight (many-ct, many-sk)-security.

ABE based on Pair Encoding Schemes (PES-ABE)

Describe exponents as linear functions c, k in variables $\underbrace{\mathbf{b}, \mathbf{s}, \mathbf{r}}_{\text{vectors}}, \alpha$

↳ $\mathbf{s}$ = encryption randomness

↳ $\mathbf{r}$ = key generation randomness

$$\mathsf{MPK} = [\mathbf{b}]_1, [\alpha]_T$$

$$\mathsf{ct}_x = [c_x^1(\mathbf{s} \otimes \mathbf{b})]_1, [c_x^2(\mathbf{s})]_2$$

$$\mathsf{sk}_y = [k_y^1(\alpha, \mathbf{r}, \mathbf{b} \otimes \mathbf{r})]_1, [k_y^2(\mathbf{r})]_2$$

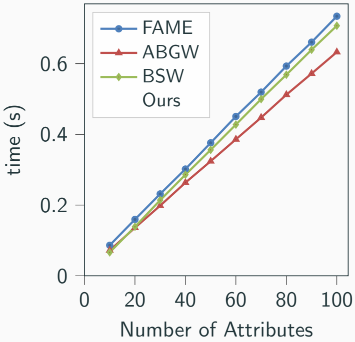
$\not\downarrow$ $\mathsf{P}(x, y) \neq 1$ (symbolic security)

$$\mathsf{K} = [\alpha \mathbf{s}[1]]_T$$

Evaluation

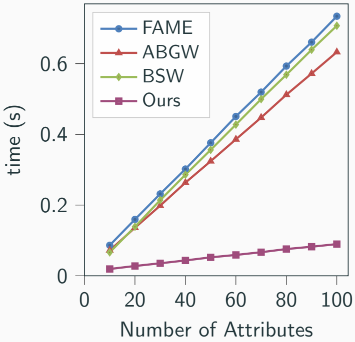
CP-ABE Benchmark

Key Generation

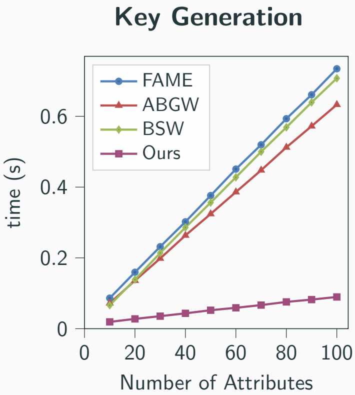


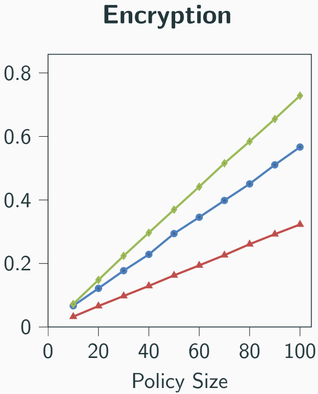
CP-ABE Benchmark

Key Generation

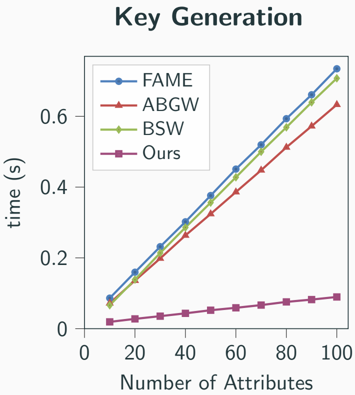


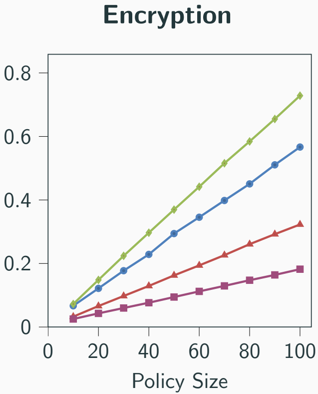
CP-ABE Benchmark



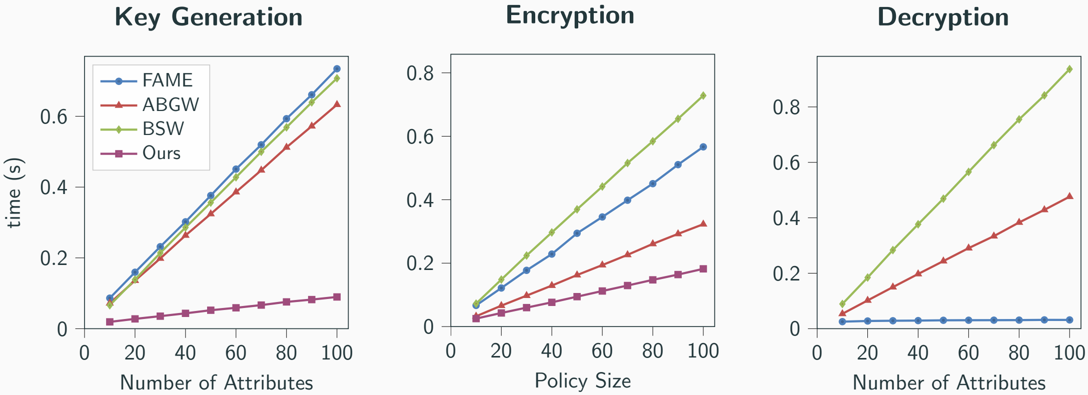


CP-ABE Benchmark

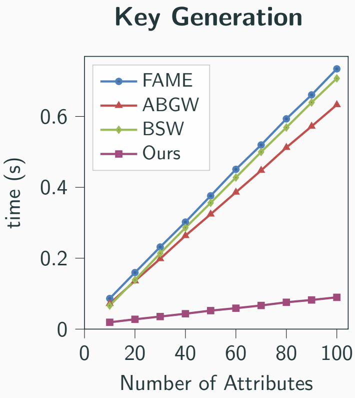


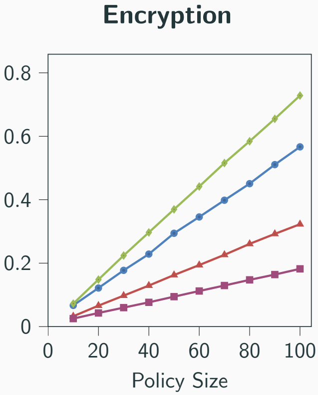


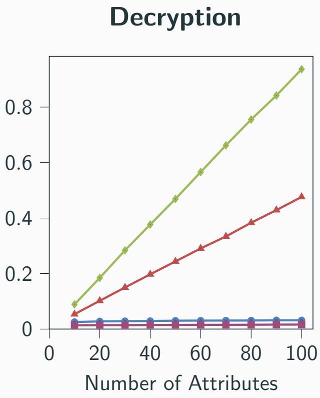
CP-ABE Benchmark



CP-ABE Benchmark







Conclusion

Summary

1. New definition for PES-ABE and symbolic security
2. Optimal tightness in the GGM achieving (many-ct, many-sk)-security
3. Smaller ciphertext/key sizes and better efficiency

Conclusion

Summary

1. New definition for PES-ABE and symbolic security
2. Optimal tightness in the GGM achieving (many-ct, many-sk)-security
3. Smaller ciphertext/key sizes and better efficiency

ePrint: `ia.cr/2022/1415`

doreen.riepel@rub.de

Thank you!