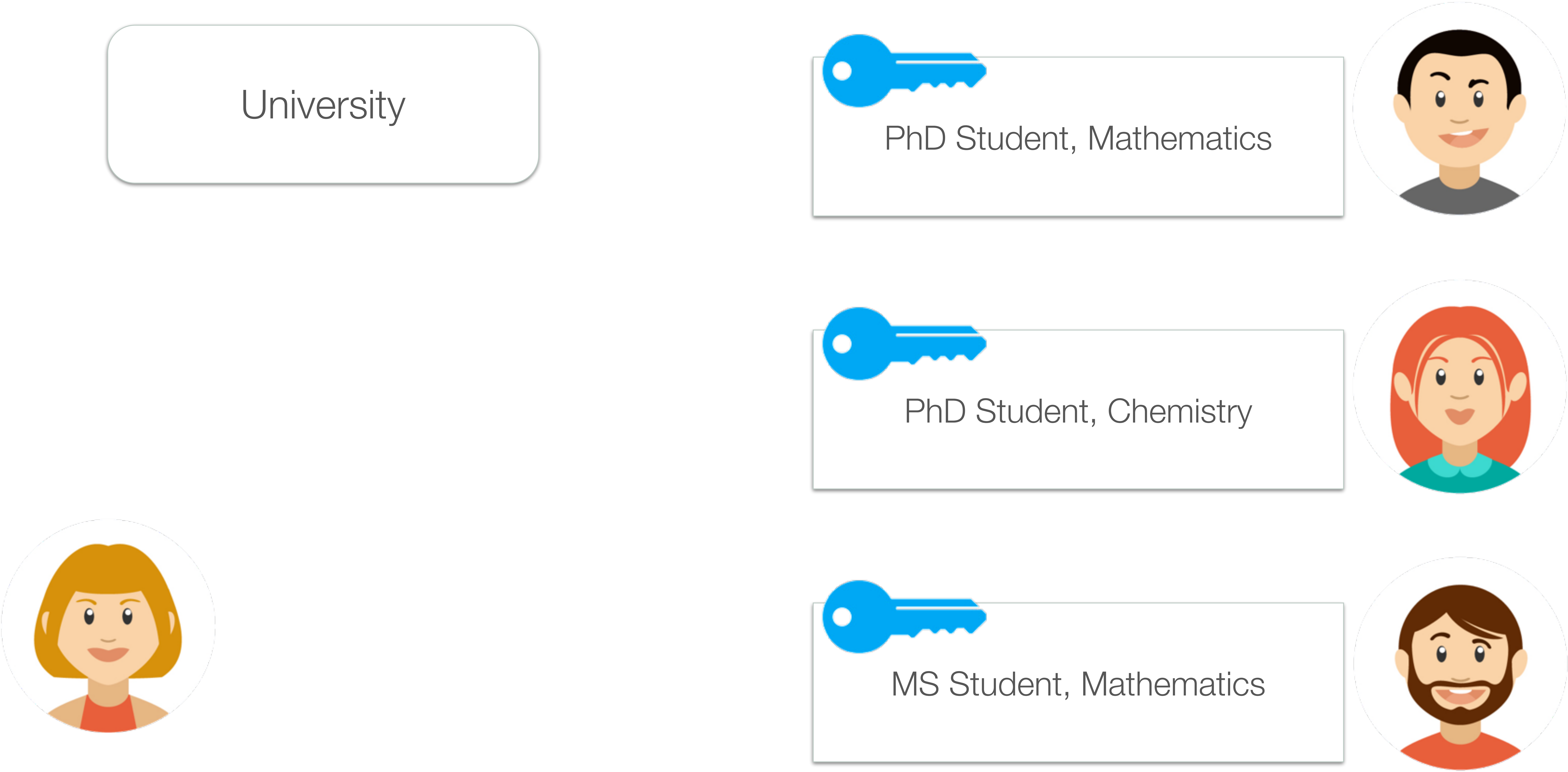
Attribute-Based Encryption in the Generic Group Model: Automated Proofs and New Constructions

M. Ambrona, G. Barthe, R. Gay, H. Wee

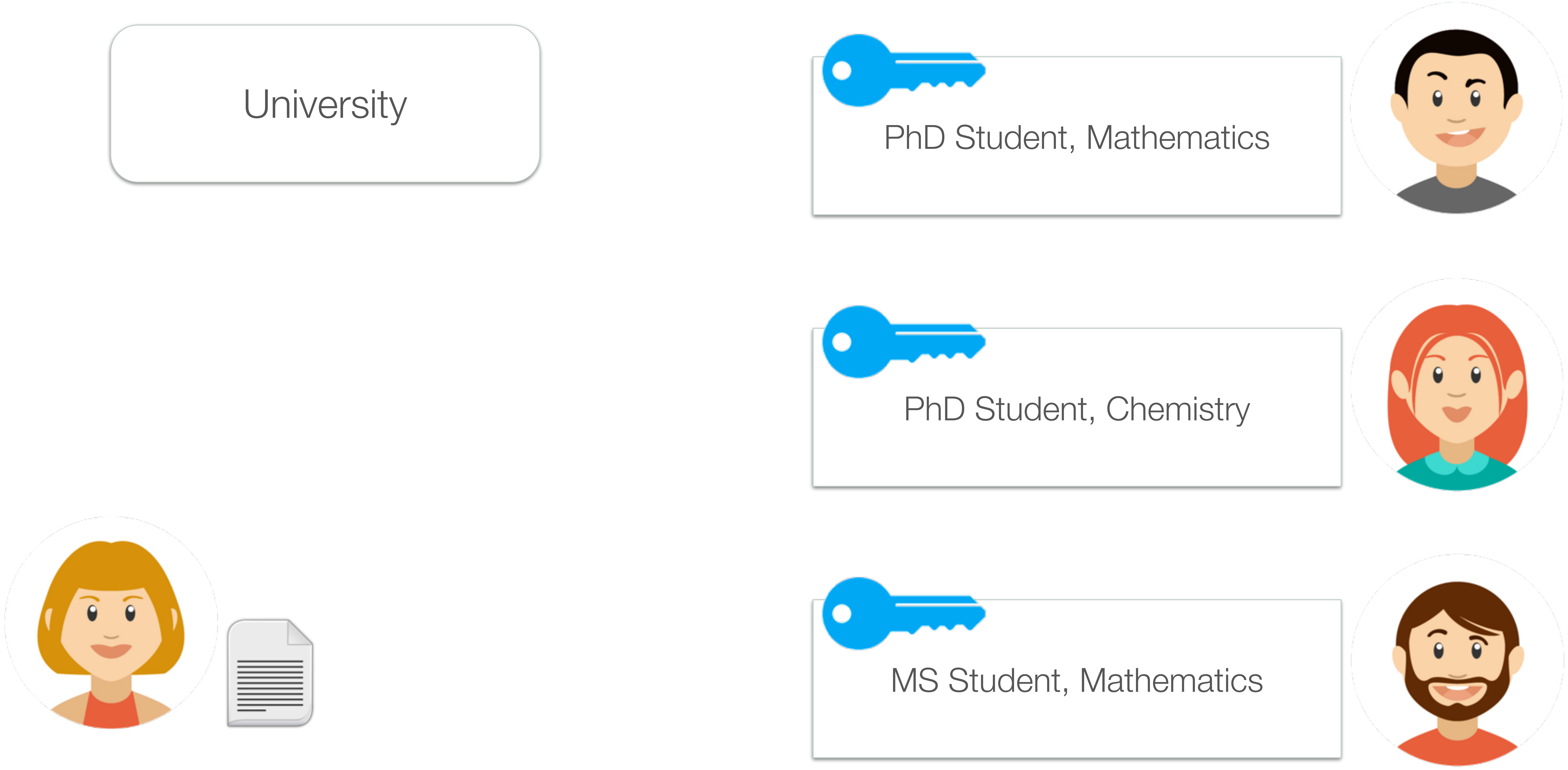
Attribute-Based Encryption

University

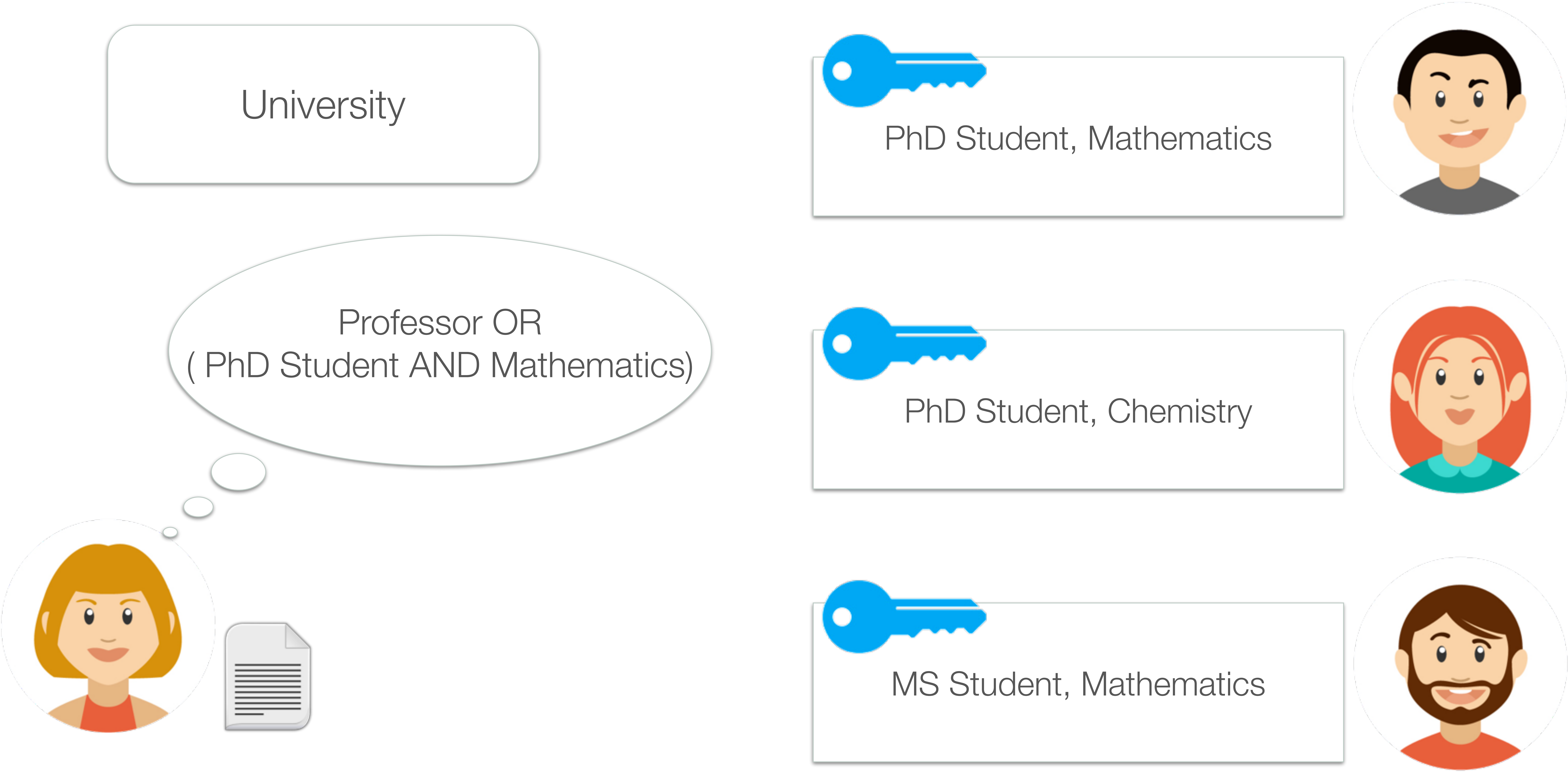
Attribute-Based Encryption



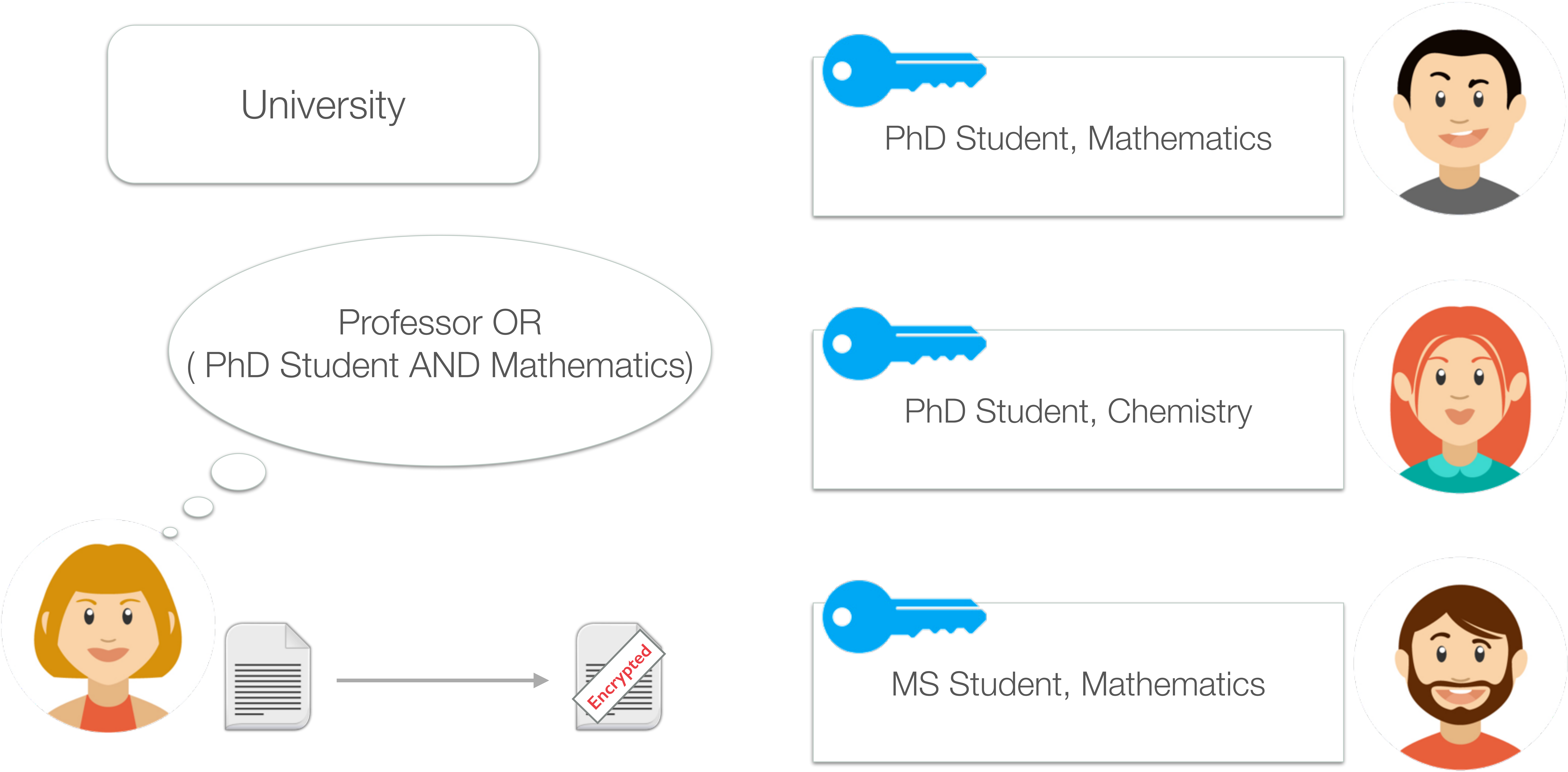
Attribute-Based Encryption



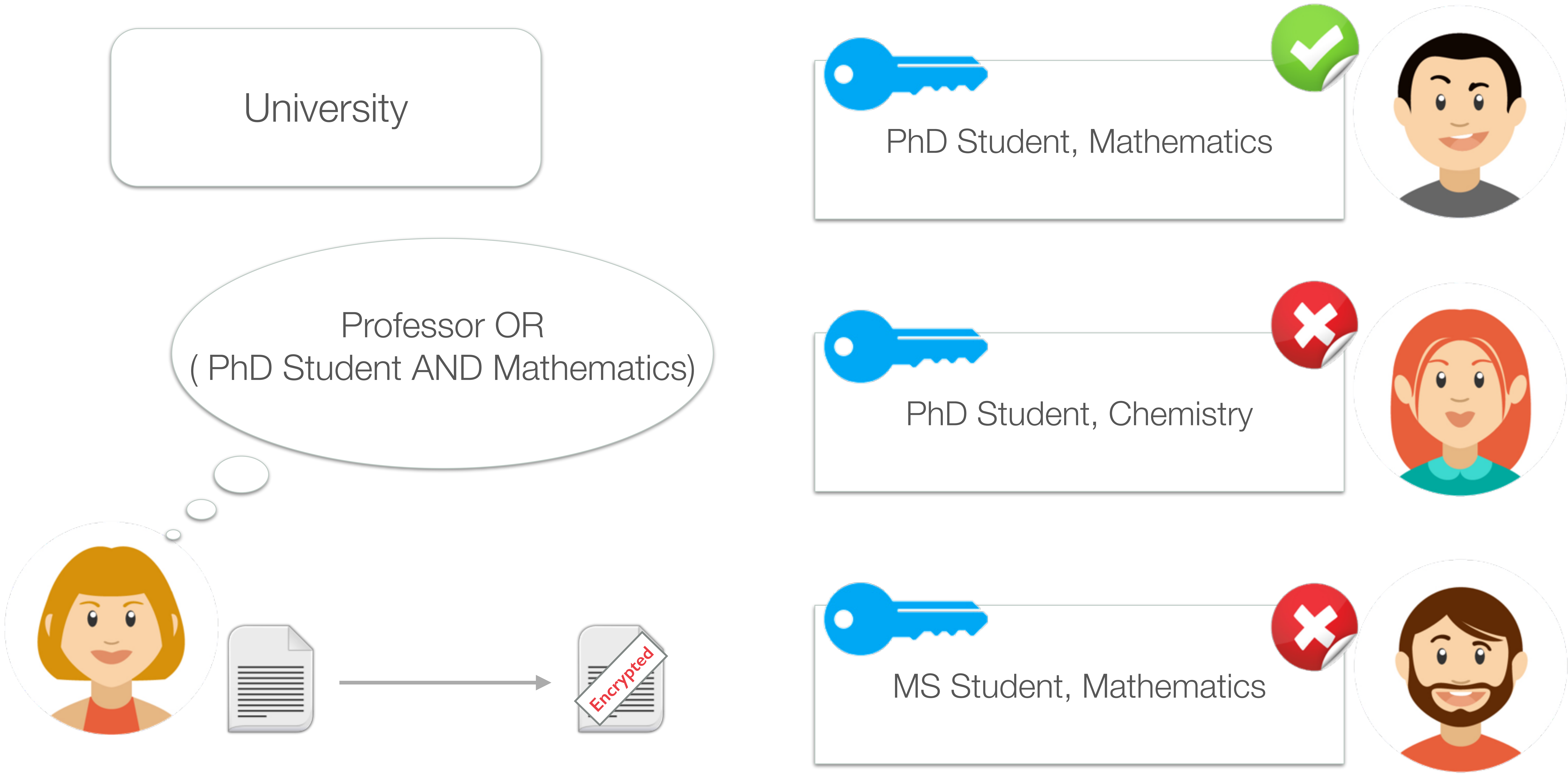
Attribute-Based Encryption



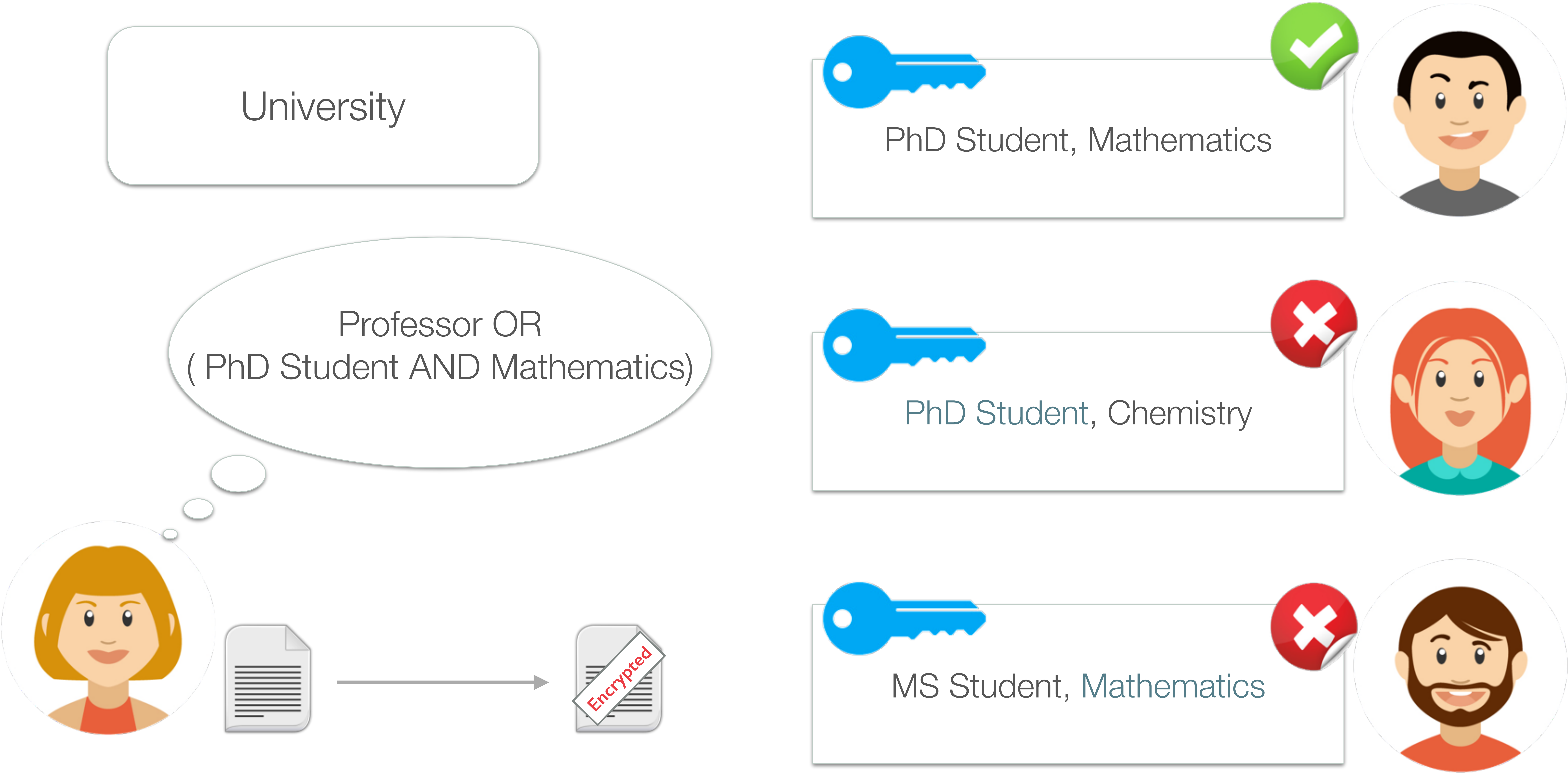
Attribute-Based Encryption



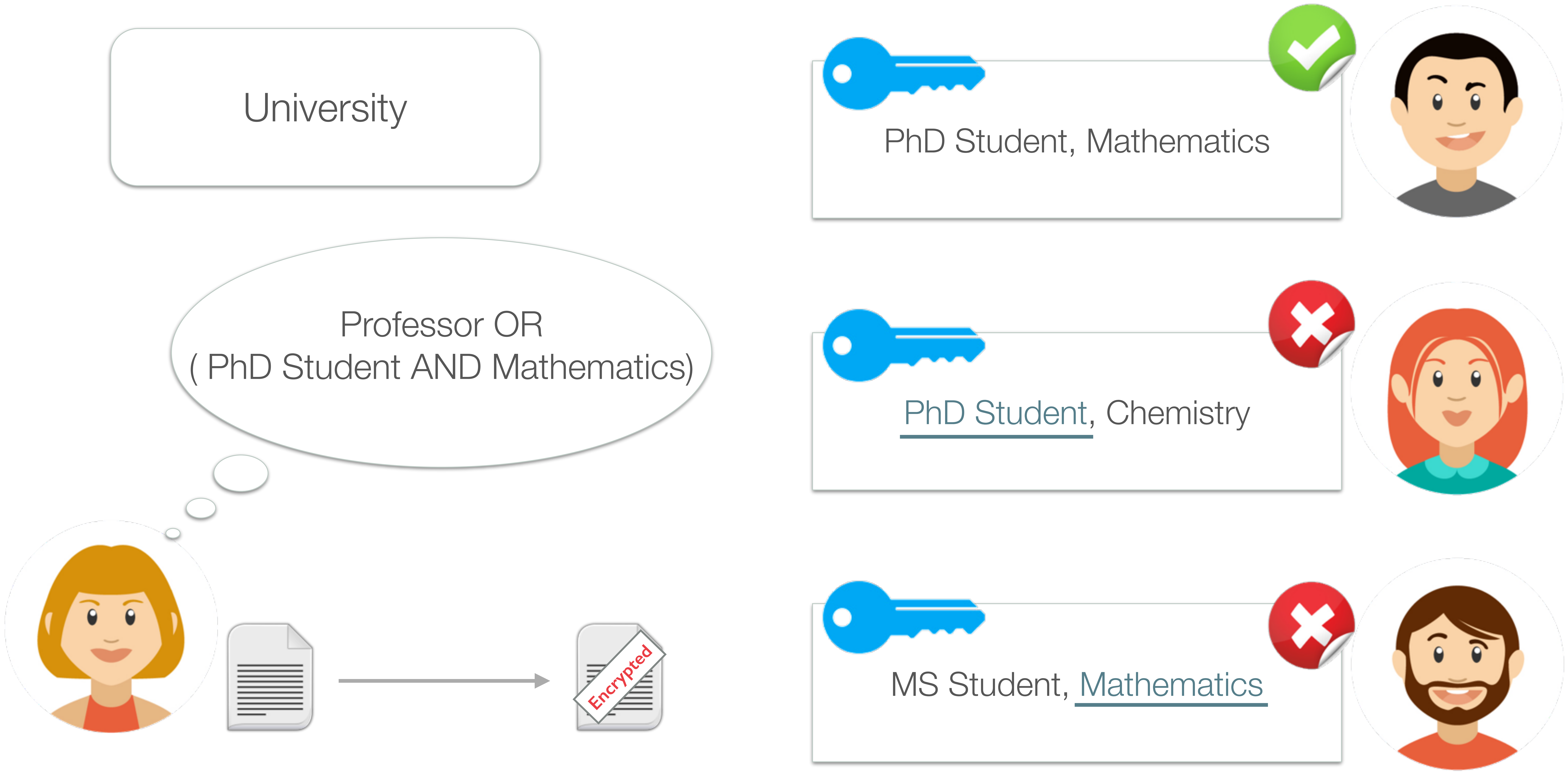
Attribute-Based Encryption



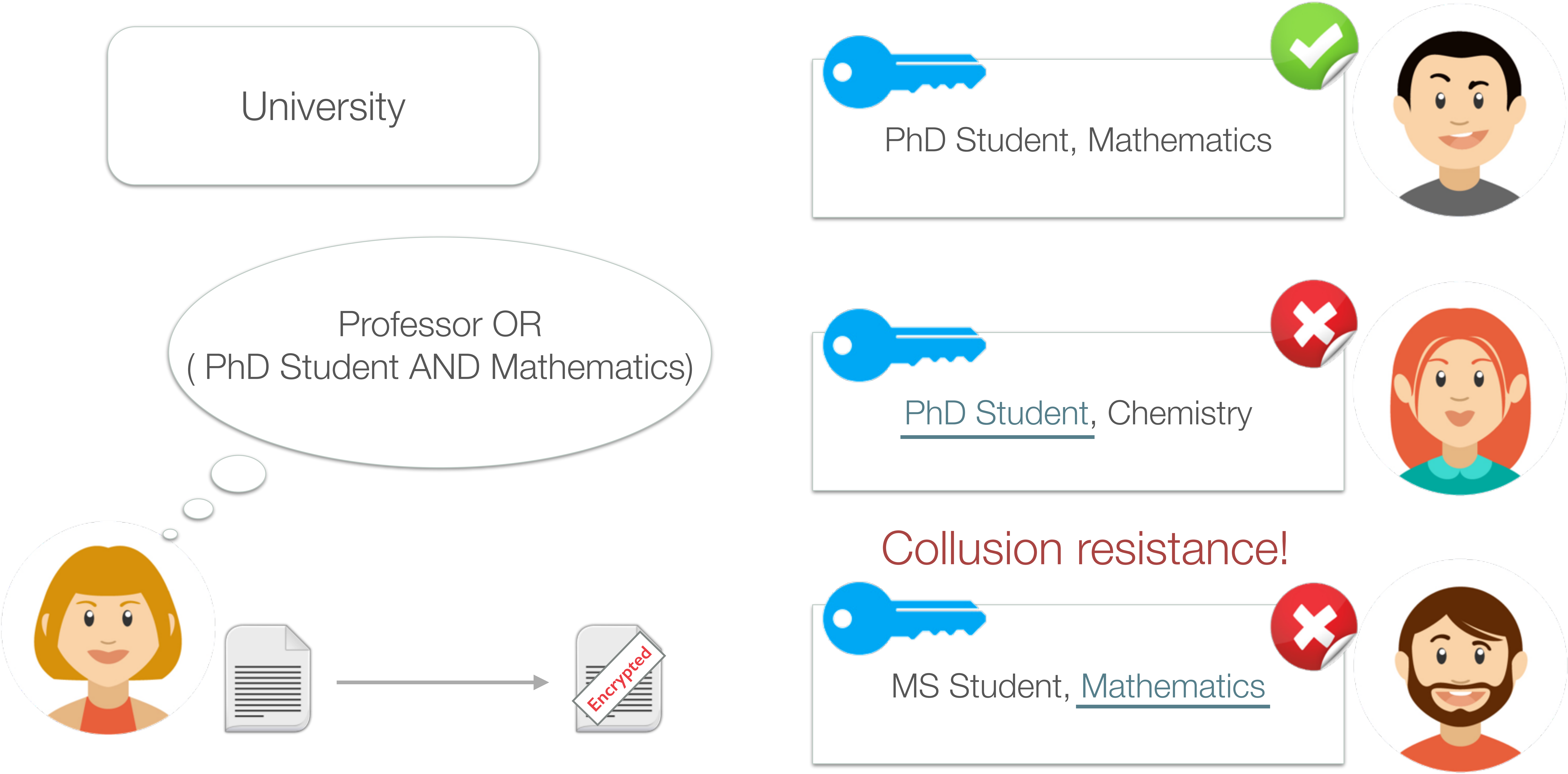
Attribute-Based Encryption



Attribute-Based Encryption



Attribute-Based Encryption



Attribute-Based Encryption

$$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$$

$$\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$$

$$\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, m)$$

$$m \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x)$$

Attribute-Based Encryption

$$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$$

$$\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$$

$$\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, m)$$

$$m \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \qquad \text{iff } \mathsf{P}(x, y) = 1$$

ABE (previous work)

Waters 2012
l-Expanded BDHE

SW 2005
BDH

OSW 2007
BDH

GPSW 2006
BDH

LOSTW 2010
3SD

Waters 2008
P-BDHE

LSW 2008
dLin, BDH

LW 2012 GSD

LSW 2008
q-MEBDH

CGW 2015
k-Lin

Attrapadung
2015 Matrix DH

LW 2012
dLin, q-PBDHE

AC 2017
q-ratio

ABE (previous work)

SW 2005
BDH

Waters 2012
l-Expanded BDHE

GPSW 2006
BDH

OSW 2007
BDH

LOSTW 2010
3SD

Waters 2008
P-BDHE

LSW 2008
dLin, BDH

LW 2012 GSD

LSW 2008
q-MEBDH

CGW 2015
k-Lin

LW 2012
dLin, q-PBDHE

Attrapadung
2015 Matrix DH

AC 2017
q-ratio

ABE (previous work)

Waters 2012
I-Expanded BDHE

SW 2005
BDH

OSW 2007
BDH

GPSW 2006
BDH

LOSTW 2010
3SD

Waters 2008
P-BDHE

LSW 2008
dLin, BDH

LW 2012 GSD

LSW 2008
q-MEBDH

CGW 2015
k-Lin

Attrapadung
2015 Matrix DH

LW 2012
dLin, q-PBDHE

AC 2017
q-ratio

ABE (previous work)

Waters 2012
I-Expanded BDHE

SW 2005
BDH

OSW 2007
BDH

GPSW 2006
BDH

LOSTW 2010
3SD

Waters 2008
P-BDHE

LSW 2008
dLin, BDH

LW 2012 GSD

LSW 2008
q-MEBDH

CGW 2015
k-Lin

Attrapadung
2015 Matrix DH

LW 2012
dLin, q-PBDHE

AC 2017
q-ratio

Bilinear groups

$$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t \qquad\qquad e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_t$$

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

Bilinear groups

$$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t \qquad e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_t$$

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

$$g_t = e(g_1, g_2)$$

Our contributions

- New framework for analyzing cryptographic constructions in the GGM
- Automated algorithm and implementation
- New ABE constructions

Security analysis

Security analysis

Attribute-Based Encryption
construction

Security analysis

Attribute-Based Encryption construction

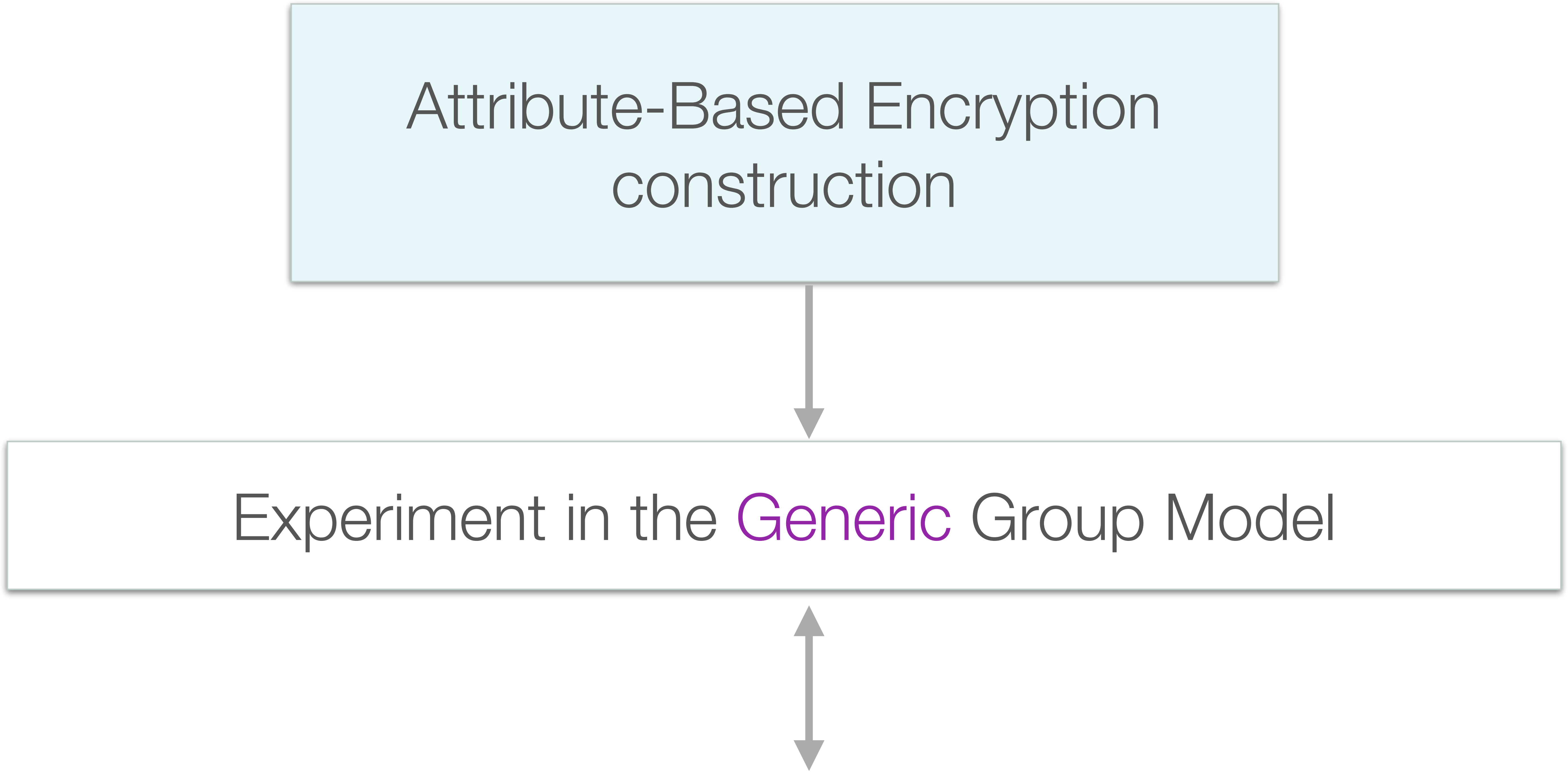
Security analysis

Attribute-Based Encryption construction

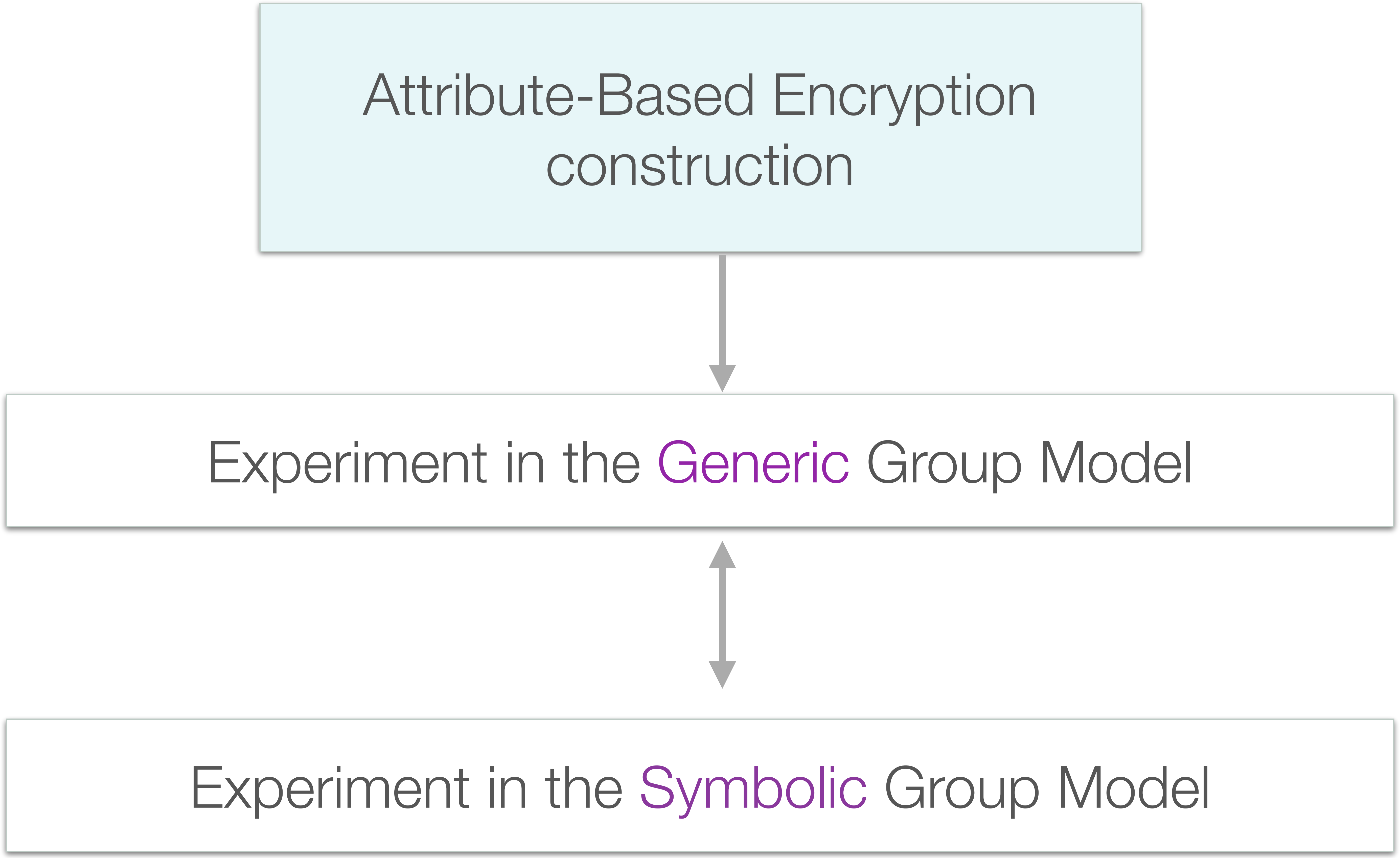
↓

Experiment in the Generic Group Model

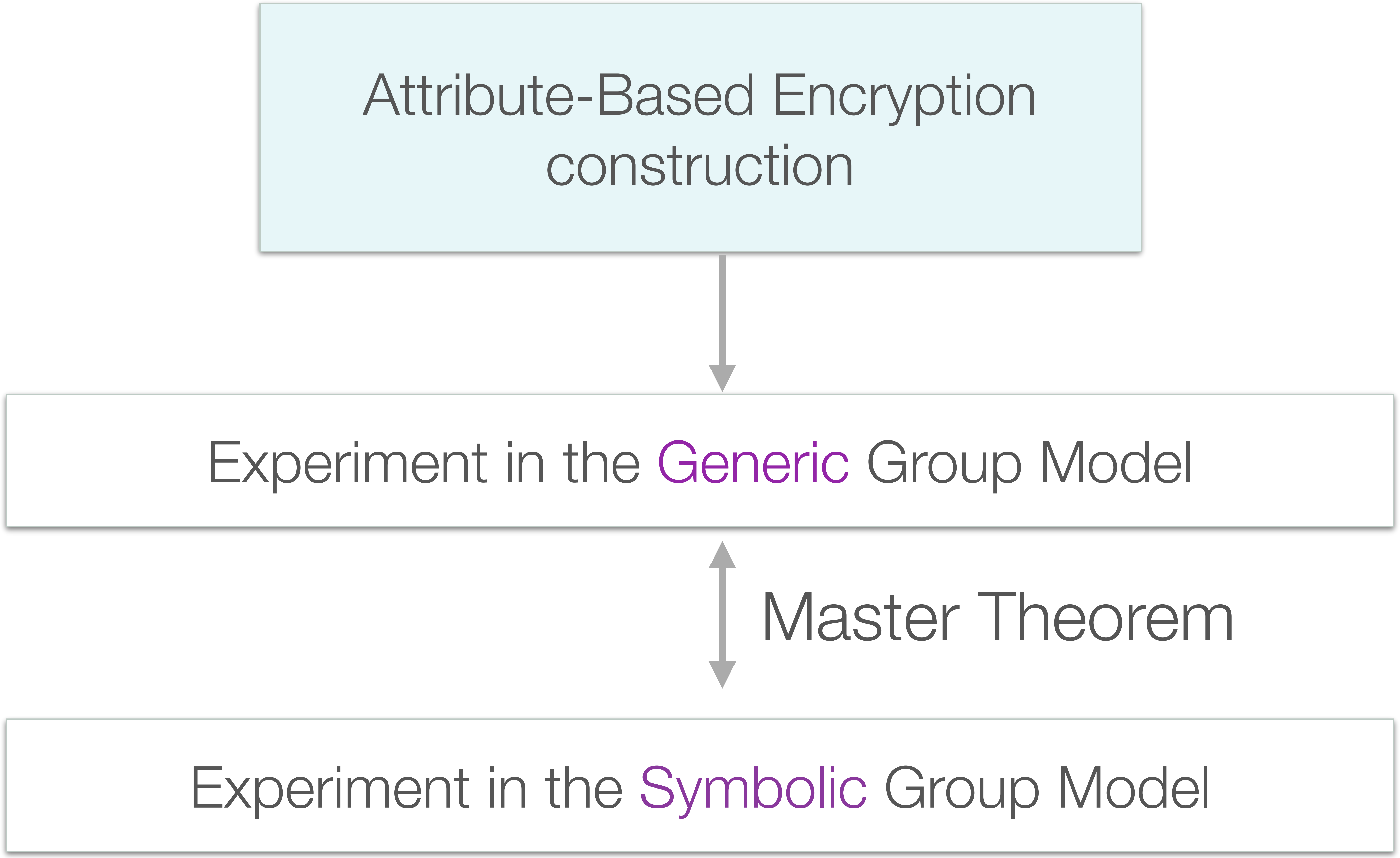
Security analysis



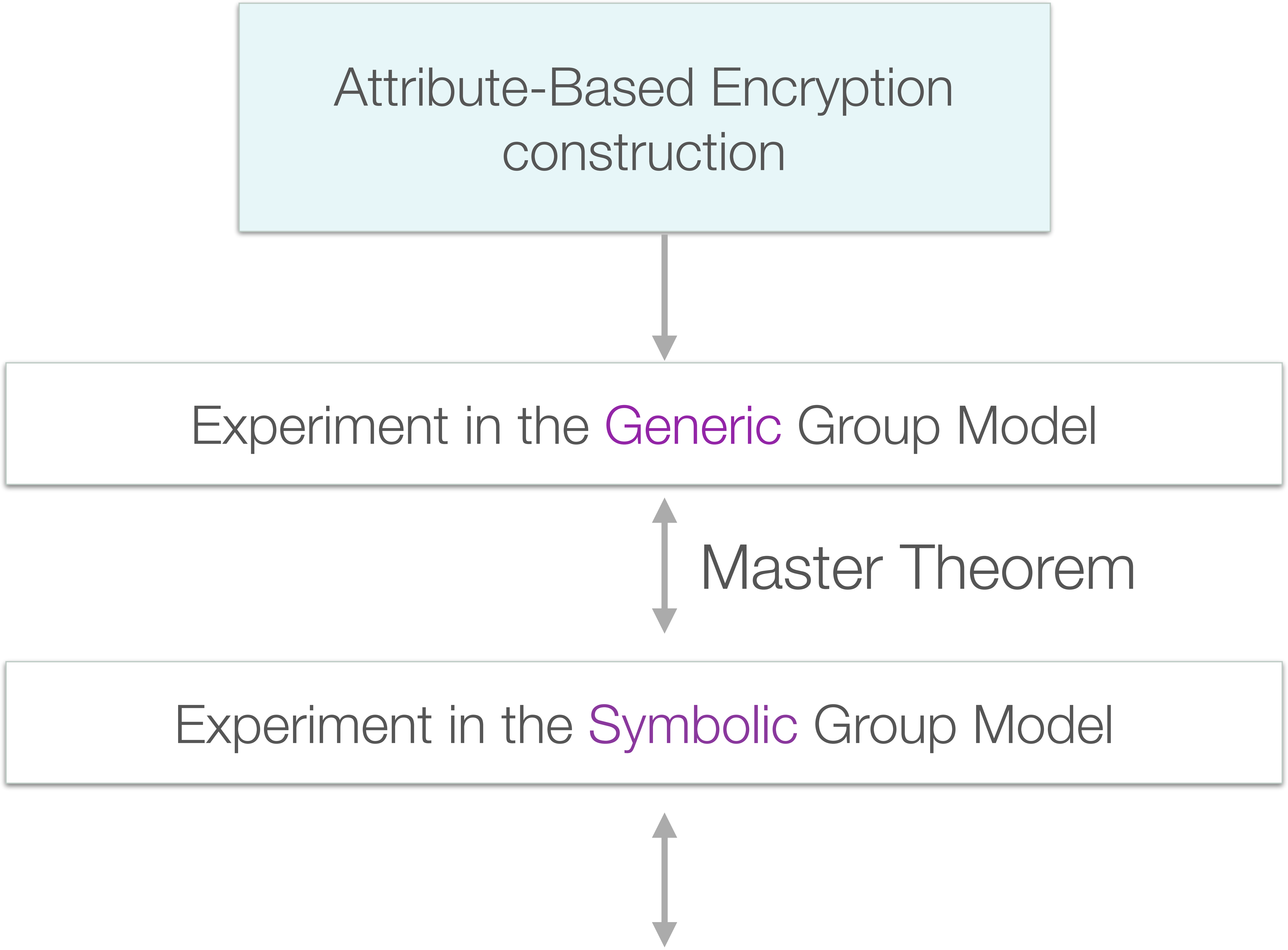
Security analysis



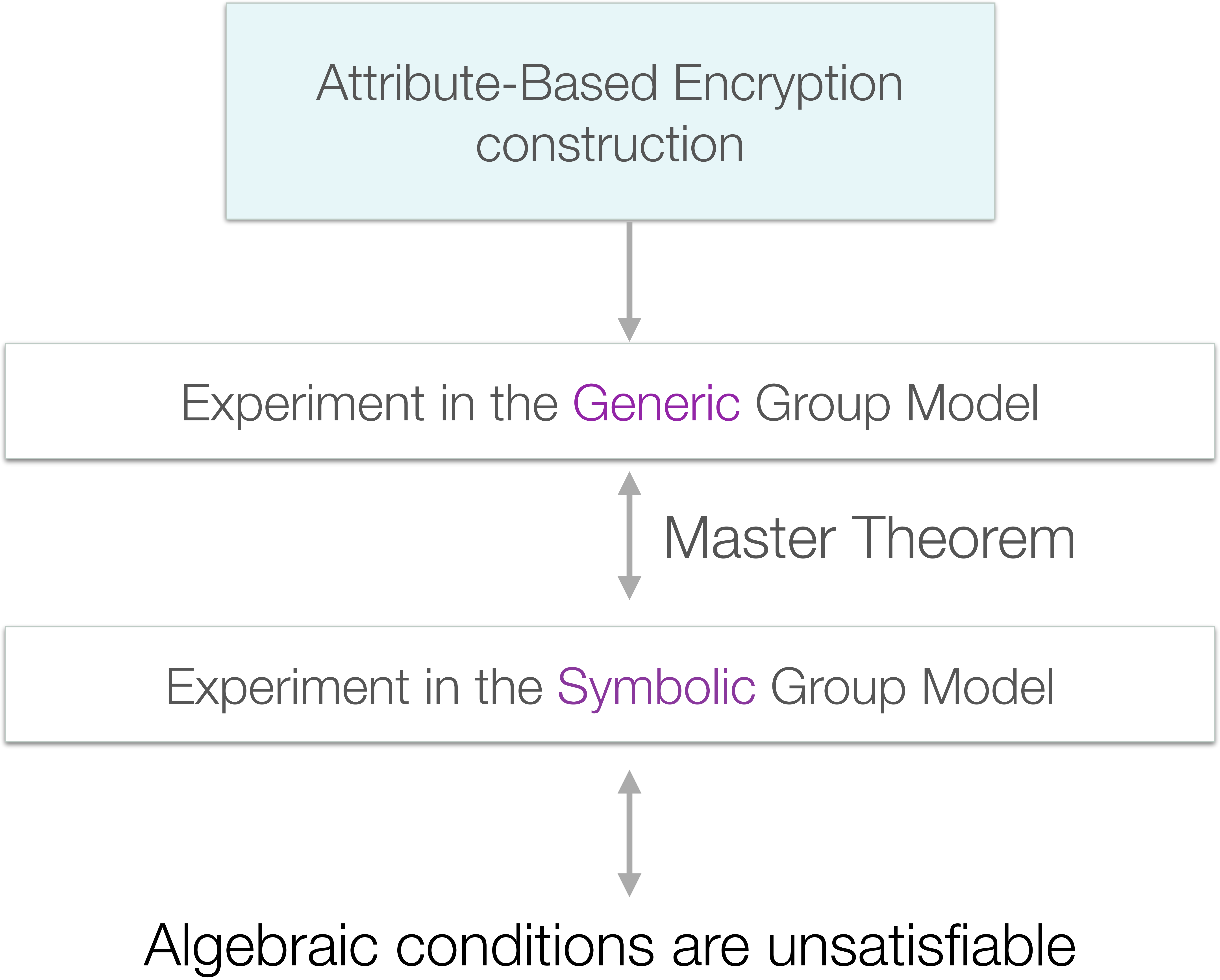
Security analysis



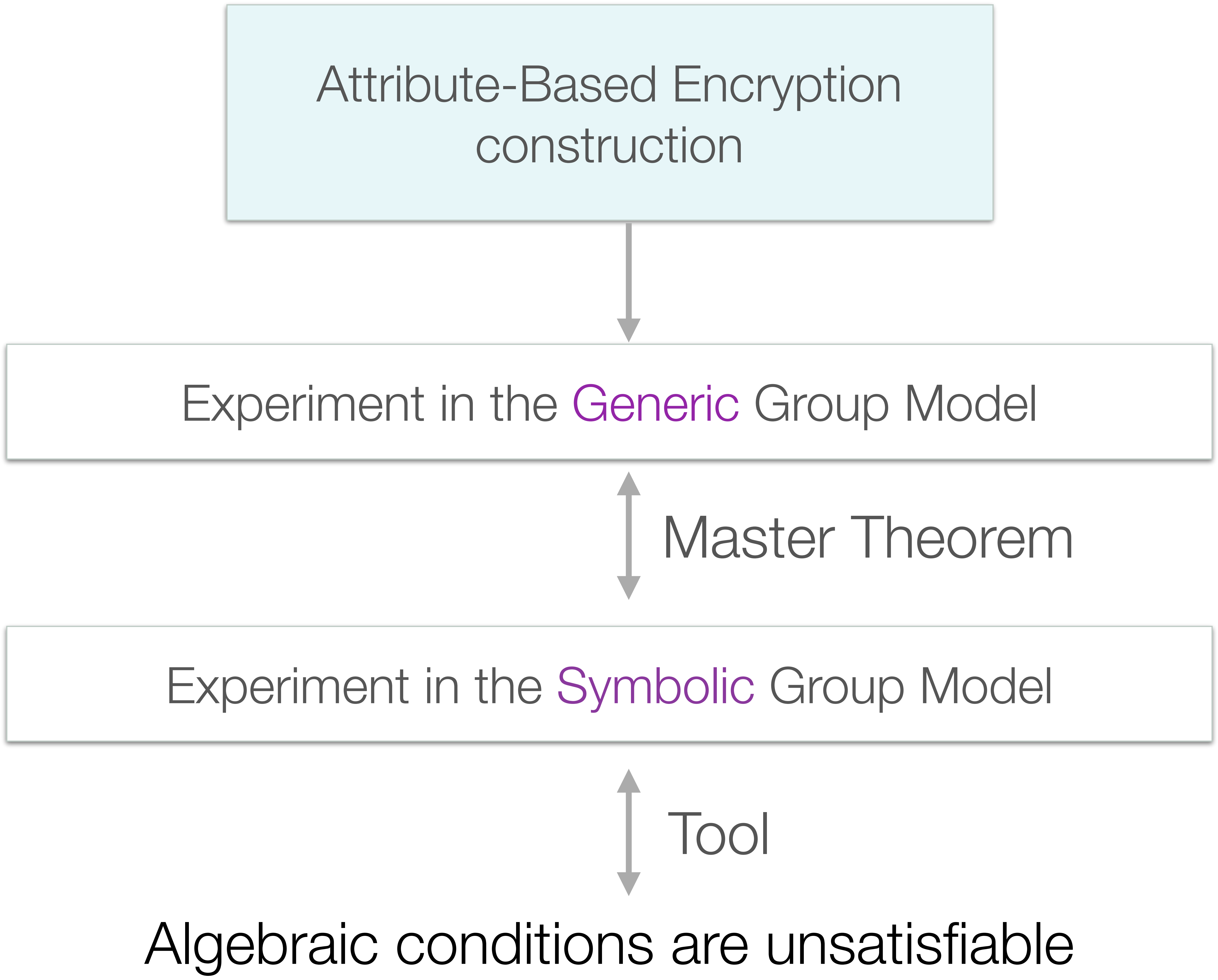
Security analysis



Security analysis



Security analysis



Petit IBE (Prime order version of Wee,TCC 2016)

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^{\alpha}, g_1^{\beta})$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct}_{\mathsf{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \; (g_t^\alpha)^s \cdot M$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M):$

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}}):$

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M):$

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \;\; (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}}):$

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^{\alpha}, g_1^{\beta})$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M):$

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct}_{\mathsf{id}} = (g_1^{\beta} \cdot g_1^{\mathsf{id}})^s, \ (g_t^{\alpha})^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathsf{id}}):$

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk}_{\mathsf{id}})$

$(g_t^{\alpha})^s \cdot M \,/$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^{\alpha}, g_1^{\beta})$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct}_{\mathsf{id}} = (g_1^{\beta} \cdot g_1^{\mathsf{id}})^s, \ (g_t^{\alpha})^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathsf{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk}_{\mathsf{id}})$

$(g_t^{\alpha})^s \cdot M \, / \, e($

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e($

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^{\alpha}, g_1^{\beta})$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct}_{\mathsf{id}} = (g_1^{\beta} \cdot g_1^{\mathsf{id}})^s, \; (g_t^{\alpha})^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathsf{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk}_{\mathsf{id}})$

$(g_t^{\alpha})^s \cdot M \,/\, e((g_1^{\beta} \cdot g_1^{\mathsf{id}})^s$

Petit IBE (Prime order version of Wee, TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \quad (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e((g_1^\beta \cdot g_1^{\mathsf{id}})^s,$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e((g_1^\beta \cdot g_1^{\mathsf{id}})^s,$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \ / \ e\left((g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ g_2^{\frac{\alpha}{\beta + \mathsf{id}}}\right)$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e\left((g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ g_2^{\frac{\alpha}{\beta+\mathsf{id}}}\right)$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \; (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e\left(g_1^{(\beta+\mathsf{id})s} \,,\, g_2^{\frac{\alpha}{\beta+\mathsf{id}}} \right)$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \quad (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e(\, g_1 \quad , \; g_2 \quad)^{(\beta+\mathsf{id})s\,\frac{\alpha}{\beta+\mathsf{id}}}$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \quad (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e(\, g_1 \quad , \; g_2 \quad)^{(\beta+\mathsf{id})s\,\frac{\alpha}{\beta+\mathsf{id}}}$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \, / \, e(g_1, g_2)^{(\beta+\mathsf{id})s \frac{\alpha}{\beta+\mathsf{id}}}$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$$(g_t^\alpha)^s \cdot M \,/\, e(g_1, g_2)^{(\beta+\mathsf{id})s \frac{\alpha}{\beta+\mathsf{id}}}$$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M):$

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}}):$

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \ / \ e(g_1, g_2)^{(\beta + \mathsf{id}) s \frac{\alpha}{\beta + \mathsf{id}}}$

Petit IBE (Prime order version of Wee, TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct}_{\mathsf{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathsf{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk}_{\mathsf{id}})$

$(g_t^\alpha)^s \cdot M \,/\, e(g_1, g_2)^{s\alpha}$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \quad (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$(g_t^\alpha)^s \cdot M \;/\; e(g_1, g_2)^{s\alpha}$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \stackrel{\$}{\leftarrow} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^{\alpha}, g_1^{\beta})$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M):$

$s \stackrel{\$}{\leftarrow} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^{\beta} \cdot g_1^{\mathsf{id}})^s, \ \ (g_t^{\alpha})^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}}):$

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

M

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^{\alpha}, g_1^{\beta})$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^{\beta} \cdot g_1^{\mathsf{id}})^s, \quad (g_t^{\alpha})^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

M ✓

Petit IBE (Prime order version of Wee, TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda)$:

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:

$\mathsf{sk}_{\mathsf{id}} = g_2^{\frac{\alpha}{\beta + \mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M)$:

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct}_{\mathsf{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \ (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathsf{id}})$:

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk}_{\mathsf{id}})$

Petit IBE (Prime order version of Wee,TCC 2016)

$\mathsf{id} \in \mathbb{Z}_p \quad M \in \mathbb{G}_t$

$\mathsf{Setup}(1^\lambda):$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, e$ of order λ-bit prime p

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{msk} = (\alpha, \beta)$

$\mathsf{mpk} = (g_t^\alpha, g_1^\beta)$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}):$

$\mathsf{sk_{id}} = g_2^{\frac{\alpha}{\beta+\mathsf{id}}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, M):$

$s \xleftarrow{\$} \mathbb{Z}_p$

$\mathsf{ct_{id}} = (g_1^\beta \cdot g_1^{\mathsf{id}})^s, \;\; (g_t^\alpha)^s \cdot M$

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk_{id}}, \mathsf{ct_{id}}):$

$\mathsf{ct}_2 / e(\mathsf{ct}_1, \mathsf{sk_{id}})$

$g_t^{\alpha s} \cdot M / e(g_1, g_2)^{(\beta+\mathsf{id})s \frac{\alpha}{\beta+\mathsf{id}'}}$

Petit IBE (Security)

Petit IBE (Security)

Petit IBE (Security)

$$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}} \qquad \mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}} \qquad \cdots \qquad \mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\cdots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta + \mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta + \mathsf{id}_2}}$ $\cdots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta + \mathsf{id}_n}}$

$g_1^{s(\beta + \mathsf{id}^*)}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\dots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\rightarrow g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\cdots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\longrightarrow g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

$$S(B+\mathsf{id}^*)\sum_{i=1}^{q}\mu_i \frac{A}{B+\mathsf{id}_i} = AS$$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\dots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

→ $g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B+\mathsf{id}_i} \right] \prod_{i=1}^{q} (B+\mathsf{id}_i) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta + \mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta + \mathsf{id}_2}}$ $\dots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta + \mathsf{id}_n}}$

$g_1^{s(\beta + \mathsf{id}^*)}$

$\rightarrow g_t^{\alpha s}$

$\forall i \in [q], \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B + \mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B + \mathsf{id}_i} \right] \prod_{i=1}^{q} (B + \mathsf{id}_i) = AS \prod_{i=1}^{q} (B + \mathsf{id}_i)$$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\cdots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\longrightarrow g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B+\mathsf{id}_i} \right] \prod_{i=1}^{q} (B+\mathsf{id}_i) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

$$S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i A \prod_{j\neq i} (B+\mathsf{id}_j)$$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta + \mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta + \mathsf{id}_2}}$ $\cdots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta + \mathsf{id}_n}}$

$g_1^{s(\beta + \mathsf{id}^*)}$

$\rightarrow g_t^{\alpha s}$

$\forall i \in [q], \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B + \mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B + \mathsf{id}_i} \right] \prod_{i=1}^{q} (B + \mathsf{id}_i) = AS \prod_{i=1}^{q} (B + \mathsf{id}_i)$$

$$S(B + \mathsf{id}^*) \sum_{i=1}^{q} \mu_i A \prod_{j \neq i} (B + \mathsf{id}_j) = AS \prod_{i=1}^{q} (B + \mathsf{id}_i)$$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\cdots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\rightarrow g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B+\mathsf{id}_i} \right] \prod_{i=1}^{q} (B+\mathsf{id}_i) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

$$S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i A \prod_{j \neq i} (B+\mathsf{id}_j) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

Evaluate in $B = -\mathsf{id}^*$:

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\quad \mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\quad \dots \quad$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\longrightarrow g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B+\mathsf{id}_i} \right] \prod_{i=1}^{q} (B+\mathsf{id}_i) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

$$S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i A \prod_{j\neq i} (B+\mathsf{id}_j) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

Evaluate in $B = -\mathsf{id}^*$: $\quad 0 = AS \prod_{i=1}^{q} (-\mathsf{id}^* + \mathsf{id}_i)$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\dots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\longrightarrow g_t^{\alpha s}$

$\forall i \in [q],\ \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B+\mathsf{id}_i} \right] \prod_{i=1}^{q} (B+\mathsf{id}_i) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

$$S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i A \prod_{j\neq i} (B+\mathsf{id}_j) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

Evaluate in $B = -\mathsf{id}^*$: $$0 = AS \prod_{i=1}^{q} (-\mathsf{id}^* + \mathsf{id}_i)$$ $\exists i \in [q] :\ -\mathsf{id}^* + \mathsf{id}_i = 0$

Petit IBE (Security)

$\mathsf{sk}_1 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_1}}$ $\mathsf{sk}_2 = g_2^{\frac{\alpha}{\beta+\mathsf{id}_2}}$ $\ldots$ $\mathsf{sk}_n = g_2^{\frac{\alpha}{\beta+\mathsf{id}_n}}$

$g_1^{s(\beta+\mathsf{id}^*)}$

$\longrightarrow g_t^{\alpha s}$

$\forall i \in [q], \mathsf{id}_i \neq \mathsf{id}^*$

$$\left[S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i \frac{A}{B+\mathsf{id}_i} \right] \prod_{i=1}^{q} (B+\mathsf{id}_i) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

$$S(B+\mathsf{id}^*) \sum_{i=1}^{q} \mu_i A \prod_{j \neq i} (B+\mathsf{id}_j) = AS \prod_{i=1}^{q} (B+\mathsf{id}_i)$$

Evaluate in $B = -\mathsf{id}^*$: $\quad 0 = AS \prod_{i=1}^{q} (-\mathsf{id}^* + \mathsf{id}_i)$

$\exists i \in [q] : -\mathsf{id}^* + \mathsf{id}_i = 0$

Automated Analysis (Grammar)

$$
\begin{array}{ll}
\mathcal{D} ::= \mathcal{D} \vee \mathcal{D} \mid \mathcal{S} & \text{disjunction} \\
\mathcal{S} ::= \exists k \in \mathcal{K}.\, \mathcal{S} \mid \mathcal{C} & \text{symbolic constraint } (k \in \mathsf{Idx}) \\
\mathcal{C} ::= \mathcal{C} \wedge \mathcal{C} \mid \forall k \in \mathcal{K}.\, \mathcal{C} & \text{conjunction } (k \in \mathsf{Idx}) \\
\quad \mid \mathcal{E} = 0 \mid \mathcal{E} \neq 0 & \\
\mathcal{E} ::= \mathcal{E} + \mathcal{E} \mid \mathcal{E} * \mathcal{E} \mid \mathcal{E}/\mathcal{E} & \text{expression } (k \in \mathsf{Idx}) \\
\quad \mid \mathcal{E} \circ \mathcal{E} \mid \mathsf{diag}(\mathcal{E}) & \\
\quad \mid \sum_{k \in \mathcal{K}} \mathcal{E} \mid \prod_{k \in \mathcal{K}} \mathcal{E} & \\
\quad \mid -\mathcal{E} \mid \mathcal{E}^{\top} \mid \mathcal{M} \mid S & \text{atom } (S \in \mathbb{Z}) \\
\mathcal{K} ::= \Gamma \mid \mathcal{K} \setminus \{k\} & \text{index set } (k \in \mathsf{Idx}, \Gamma \in \mathsf{Set})
\end{array}
$$

Automated Analysis (Simplification rules)

com-den	$\sum_{i \in K} \mathcal{E}_i / \mathcal{E}'_i \rightsquigarrow \frac{\sum_{i \in K} \mathcal{E}_i * \prod_{j \in K \setminus \{i\}} \mathcal{E}'_j}{\prod_{i \in K} \mathcal{E}'_i}$
mul-split	$\mathcal{E} * \mathcal{E}' = 0 \rightsquigarrow \mathcal{E} = 0 \lor \mathcal{E}' = 0$
div-split	$\mathcal{E} / \mathcal{E}' = 0 \rightsquigarrow \mathcal{E} = 0 \land \mathcal{E}' \neq 0$
eval-var	$\mathcal{E} = 0 \rightsquigarrow \mathcal{E} = 0 \land \mathcal{E}[v \mapsto \mathcal{E}'] = 0$ for variable v and a closed (variable-free) expression $\mathcal{E}'$
extr-coeff	$\mathcal{E} * v + \mathcal{E}' = 0 \rightsquigarrow \mathcal{E} = 0 \land \mathcal{E}' = 0$ where v is a variable and $\mathcal{E}, \mathcal{E}'$ do not contain v
zero-prod	$\prod_{i \in K} \mathcal{E}_i = 0 \rightsquigarrow \exists j \in K : \mathcal{E}_j = 0$
non-zero-sum	$\sum_{i \in K} \mathcal{E}_i \neq 0 \rightsquigarrow \exists j \in K : \mathcal{E}_j \neq 0$
idx-split	$\exists i \in K. \mathcal{S}_i \rightsquigarrow (\exists i \in K \setminus \{j\}. \mathcal{S}_i) \lor \mathcal{S}_j$

Case studies

Scheme	Time (s)	Proof	Security
IBE 1 [64]	0.016	✓	Many-key
IBE 2 [27]	0.001	✓	One-key*
IPE 1 [46]	0.001	✓	One-key*
IPE 2 (New)	0.027	✓	Many-key
KP-ABE [41]	-	×	-
Compact KP-ABE (New)	-	×	-
Unbounded KP-ABE (New)	-	×	-
KP-ABE [41]	-	×	-
(fixed-size $d = \ell = \ell' = 2$)	0.046	✓	One-key
(fixed-size $d = \ell = \ell' = 3$)	1.52	✓	One-key
CP-ABE (New)	-	×	-
(fixed-size $d = \ell = \ell' = 2$)	0.212	✓	One-key
(fixed-size $d = \ell = \ell' = 3$)	5.75	✓	One-key
Spatial Encryption [36]	0.005	✓	One-key*
Doubly Spatial Enc. [36]	0.013	✓	One-key*
KP-ABE [36]	0.256	✓	One-key*
CP-ABE [36]	0.206	✓	One-key*
NIPE,ZIPE [36]	0.003	✓	One-key*
CP-ABE for negated bf. [11]	0.084	✓	One-key*
Unbounded KP-ABE$^{\triangle}$	0.006	Attack	Insecure

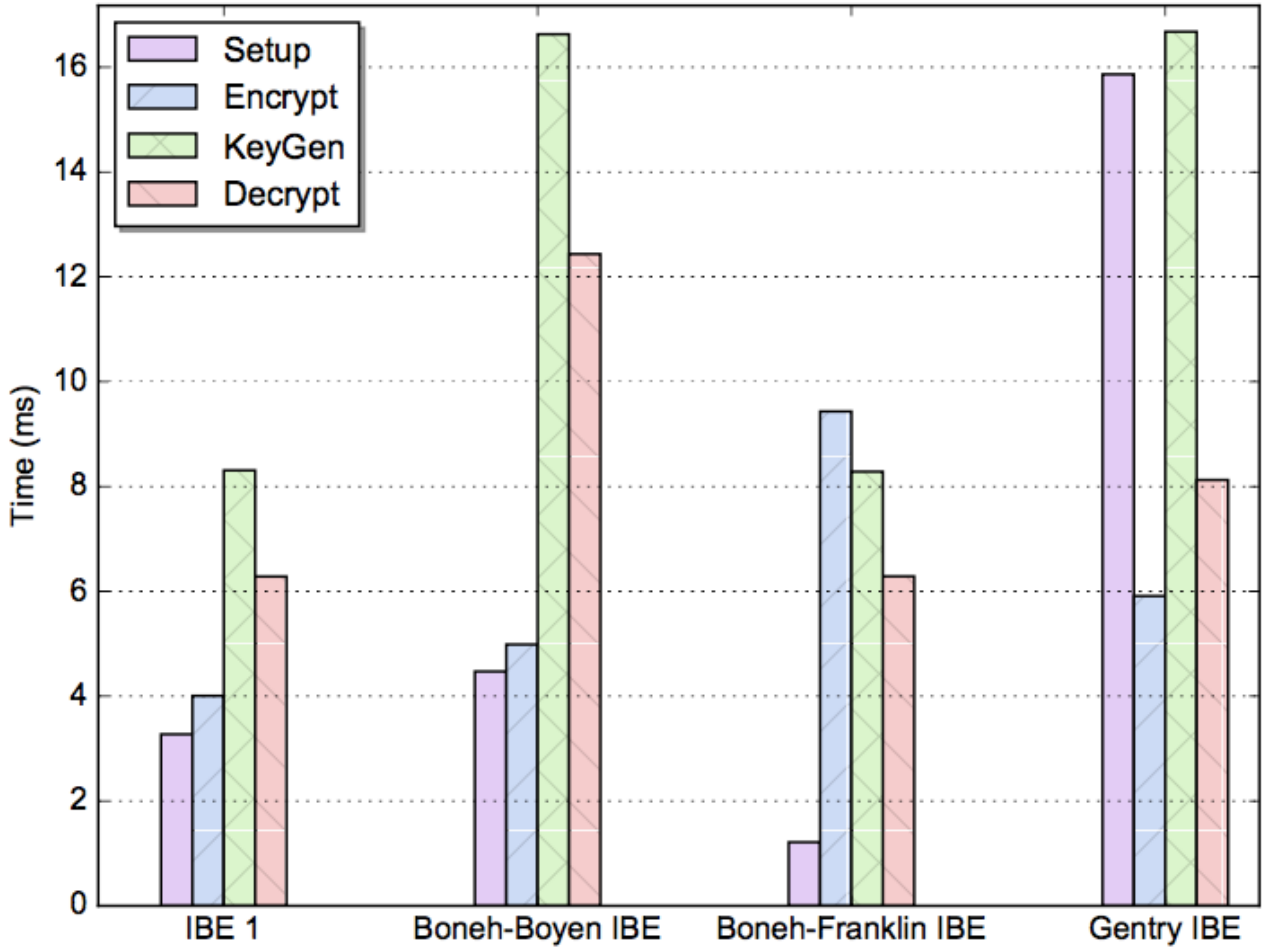
Case studies

Scheme	Time (s)	Proof	Security
IBE 1 [64]	0.016	✓	Many-key
IBE 2 [27]	0.001	✓	One-key*
IPE 1 [46]	0.001	✓	One-key*
IPE 2 (New)	0.027	✓	Many-key
KP-ABE [41]	-	×	-
Compact KP-ABE (New)	-	×	-
Unbounded KP-ABE (New)	-	×	-
KP-ABE [41]	-	×	-
(fixed-size $d = \ell = \ell' = 2$)	0.046	✓	One-key
(fixed-size $d = \ell = \ell' = 3$)	1.52	✓	One-key
CP-ABE (New)	-	×	-
(fixed-size $d = \ell = \ell' = 2$)	0.212	✓	One-key
(fixed-size $d = \ell = \ell' = 3$)	5.75	✓	One-key
Spatial Encryption [36]	0.005	✓	One-key*
Doubly Spatial Enc. [36]	0.013	✓	One-key*
KP-ABE [36]	0.256	✓	One-key*
CP-ABE [36]	0.206	✓	One-key*
NIPE,ZIPE [36]	0.003	✓	One-key*
CP-ABE for negated bf. [11]	0.084	✓	One-key*
Unbounded KP-ABE$^{\triangle}$	0.006	Attack	Insecure

$(*)$ One-key $\Rightarrow$ Many-key

Agrawal & Chase, EuroCrypt 2017

Performance evaluation (IBE)



IBE	mpk	msk	ct	sk
IBE 1	$\mathbb{G}_1 \times \mathbb{G}_T$	$\mathbb{Z}_p^2$	$\mathbb{G}_1$	$\mathbb{G}_2$
BonBoy [26]	$\mathbb{G}_1^2 \times \mathbb{G}_T$	$\mathbb{Z}_p^3$	$\mathbb{G}_1^2$	$\mathbb{G}_2^2$
BonFra [30]	$\mathbb{G}_1 \times (\mathbb{Z}_p \rightarrow \mathbb{G}_2)$	$\mathbb{Z}_p$	$\mathbb{G}_1$	$\mathbb{G}_2$
Gentry [40]	$\mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_T$	$\mathbb{Z}_p$	$\mathbb{G}_1 \times \mathbb{G}_T$	$\mathbb{Z}_p \times \mathbb{G}_2$

Tool demonstration

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.

go.
contradiction.
```

Menu

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.

go.
contradiction.
```

Menu

sets: $|Q| = q$

parameters: $id, id_i, \mu_i \in \mathbb{Z}_p$

variables: $S, A, B \in \mathbb{Z}_p$

no goals

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.

go.
contradiction.
```

Menu

sets: $|Q| = q$
parameters: $id, id_i, \mu_i \in \mathbb{Z}_p$
variables: $S, A, B \in \mathbb{Z}_p$

goal 1 out of 1

(1) $\forall i \in Q.\ id_i + -id \neq 0$ $\wedge$
(2) $S\,(B + id)\left(\sum_{i \in Q} \frac{\mu_i A}{B + id_i}\right) + -AS = 0$

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.

go.
contradiction.
```

Menu

sets:	$\lvert Q \rvert = q$
parameters:	$id, id_i, \mu_i \in \mathbb{Z}_p$
variables:	$S, A, B \in \mathbb{Z}_p$

goal 1 out of 1

(1) $\left(\sum_{i\in Q} SB\mu_i A \left(\prod_{j\in Q\setminus\{i\}} B + id_j\right)\right) + \left(\sum_{i\in Q} Sid\mu_i A \left(\prod_{j\in Q\setminus\{i\}} B + id_j\right)\right) + (-1)\left(\prod_{i\in Q} B + id_i\right) AS =$

(2) $\forall i \in Q.\ id_i + (-1)\, id \neq 0$

(3) $\forall i \in Q.\ B + id_i \neq 0$

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.


go.
contradiction.
```

Menu

sets:	$\lvert Q\rvert = q$
parameters:	$id, id_i, \mu_i \in \mathbb{Z}_p$
variables:	$S, A, B \in \mathbb{Z}_p$

goal 1 out of 1

(1) $\left(\sum_{i\in Q} SB\mu_i A\left(\prod_{j\in Q\setminus\{i\}} B + id_j\right)\right) + \left(\sum_{i\in Q} Sid\mu_i A\left(\prod_{j\in Q\setminus\{i\}} B + id_j\right)\right) + (-1)\left(\prod_{i\in Q} B + id_i\right) AS =$

(2) $\forall i \in Q.\ id_i + (-1)\, id \neq 0$

(3) $\forall i \in Q.\ B + id_i \neq 0$

(4) $\left(\sum_{i\in Q} Sid\mu_i A\left(\prod_{j\in Q\setminus\{i\}} id_j\right)\right) + (-1)\left(\prod_{i\in Q} id_i\right) AS = 0$

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.

go.
contradiction.
```

Menu

sets: $|Q| = q$
parameters: $id, id_i, \mu_i \in \mathbb{Z}_p$
variables: $S, A, B \in \mathbb{Z}_p$

goal 1 out of 1

$\exists i \in Q :$

(1) $\left(\sum_{k \in Q\setminus\{i\}} id_k \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} id_j\right) id_i\right) + id_i \mu_i \left(\prod_{j \in Q\setminus\{i\}} id_j\right) + (-1)\left(\prod_{j \in Q\setminus\{i\}} id_j\right) id_i = 0$

(2) $\left(\sum_{k \in Q\setminus\{i\}} 4\, id_k \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} id_i + id_j\right) id_i\right) + 2\, id_i \mu_i \left(\prod_{j \in Q\setminus\{i\}} id_i + id_j\right) + (-2)\left(\prod_{j \in Q\setminus\{i\}} id_i + id_j\right.$

(3) $\left(\sum_{k \in Q\setminus\{i\}} id_j \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} id_j\right) id_i\right) + id_j \mu_i \left(\prod_{j \in Q\setminus\{i\}} id_j\right) + \left(\sum_{k \in Q\setminus\{i\}} id_k \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} id_j\right) id_i\right) -$

(4) $\left(\sum_{k \in Q\setminus\{i\}} 2\, id_j \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} id_i + id_j\right) id_i\right) + id_j \mu_i \left(\prod_{j \in Q\setminus\{i\}} id_i + id_j\right) + \left(\sum_{k \in Q\setminus\{i\}} 2\, id_k \mu_k \left(\prod_{j \in Q\setminus}\right.\right.$

(5) $\left(\sum_{k \in Q\setminus\{i\}} id_j \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} B + id_j\right) B\right) + \left(\sum_{k \in Q\setminus\{i\}} id_j \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} B + id_j\right) id_i\right) + id_j \mu_i \left(\prod_{j \in Q\setminus}\right.$

(6) $\left(\sum_{k \in Q\setminus\{i\}} B \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} B + id_j\right) B\right) + \left(\sum_{k \in Q\setminus\{i\}} B \mu_k \left(\prod_{j \in Q\setminus\{i,k\}} B + id_j\right) id_i\right) + B \mu_i \left(\prod_{j \in Q\setminus\{i\}}\right.$

(7) $0 \neq 0$

(8) $B + id_i \neq 0$

(9) $\forall j \in Q \setminus \{i\}.\ B + id_j \neq 0$

$id \mapsto id_i$

$(-1)\left(\prod_{j \in Q\setminus\{i\}} (-1)\, id + id_j\right) id + \left(\prod_{j \in Q\setminus\{i\}} (-1)\, id + id_j\right) id_i \mapsto 0$

```
sets Q[q].

params forall i in Q: id, id_i, \mu_i in Zp.
vars S,A,B in Zp.

forall i in Q: id_i <> id /\
S*(B+id)*sum(i in Q: \mu_i*A/(B+id_i)) = A*S.

full_simplify.
substitute B by 0 in 1.

go.
contradiction.
```

Menu

sets: $|Q| = q$
parameters: $id, id_i, \mu_i \in \mathbb{Z}_p$
variables: $S, A, B \in \mathbb{Z}_p$

no goals

Conclusions

- New framework for proving security in the GGM
- New ABE constructions
- Tool for analyzing symbolic systems of constraints

Future work

Future work

- Prove selective security under a q-type assumption
- Improve expressivity of our grammar and heuristic
- Explore synthesis

Future work

- Prove selective security under a q-type assumption
- Improve expressivity of our grammar and heuristic
- Explore synthesis

Thanks!