Attribute-Based and Broadcast Encryption from Lattices

Hoeteck Wee
NTT Research

attribute-based encryption

key-policy (KP-ABE)

ciphertext-policy (CP-ABE)

attribute-based encryption

key-policy $\mathbf{ct}_x \leftarrow \mathbf{E}(x, m), \mathbf{sk}_f \leftarrow \mathbf{G}(f)$

ciphertext-policy $\mathbf{ct}_f \leftarrow \mathbf{E}(f, m), \mathbf{sk}_x \leftarrow \mathbf{G}(x)$

attribute-based encryption

key-policy $\mathbf{ct}_x \leftarrow \mathbf{E}(x, m), \mathbf{sk}_f \leftarrow \mathbf{G}(f)$

ciphertext-policy $\mathbf{ct}_f \leftarrow \mathbf{E}(f, m), \mathbf{sk}_x \leftarrow \mathbf{G}(x)$

✓ expressive **formulae**

✓ **security** pairings

attribute-based encryption

key-policy

$$|\mathbf{ct}_x| = O(|x|), |\mathbf{sk}_f| = O(\mathsf{size}(f))$$

ciphertext-policy

$$|\mathbf{ct}_f| = O(\mathsf{size}(f)), |\mathbf{sk}_f| = O(|x|)$$

✓ expressive **formulae**

✓ **security** pairings

attribute-based encryption

key-policy

$|\mathbf{ct}_x| = O(|x|), |\mathbf{sk}_f| = O(\text{size}(f))$

ciphertext-policy

$|\mathbf{ct}_f| = O(\text{size}(f)), |\mathbf{sk}_f| = O(|x|)$

✓✓ expressive **circuits**

✓ **security** pairings

attribute-based encryption

key-policy

$|\mathbf{ct}_x| = O(|x|), |\mathbf{sk}_f| = O(\mathsf{size}(f))$

ciphertext-policy

$|\mathbf{ct}_f| = O(\mathsf{size}(f)), |\mathbf{sk}_f| = O(|x|)$

✓✓ expressive **circuits**

✓✓ **security** lattices (post-quantum)

attribute-based encryption

key-policy

$|\mathbf{ct}_x| = \widetilde{O}(|x|), |\mathbf{sk}_f| = \widetilde{O}(1)$ **[BGGHNSVV14, GVW13]**

ciphertext-policy

$|\mathbf{ct}_f| = O(\text{size}(f)), |\mathbf{sk}_f| = O(|x|)$

✓✓ expressive **circuits** $\widetilde{O}(\cdot)$ hides poly(depth)

✓✓ **security** lattices (post-quantum)

attribute-based encryption

key-policy

$|\mathbf{ct}_x| = \widetilde{O}(|x|), |\mathbf{sk}_f| = \widetilde{O}(1)$ **[BGGHNSVV14, GVW13]**

ciphertext-policy

$|\mathbf{ct}_f| = \widetilde{O}(1), |\mathbf{sk}_x| = \widetilde{O}(|x|)$ **[W22, BV22, AY20]**

✓✓ expressive **circuits** $\widetilde{O}(\cdot)$ hides poly(depth)

✓✓ **security** lattices (post-quantum)

LWE: learning with errors

$$\left(\mathbf{B} \qquad\qquad\qquad\right)$$

$$\boxed{\quad \mathbf{B} \quad}$$

$$\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times O(n \log q)}$$

LWE: learning with errors

$$(\mathbf{B},\ \mathbf{sB} + \mathbf{e})$$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{B} \leftarrow \mathbb{Z}_q^{n \times O(n \log q)}$

LWE: learning with errors

$$(\mathbf{B},\ \mathbf{sB}+\mathbf{e}) \approx_c \text{uniform}$$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{B} \leftarrow \mathbb{Z}_q^{n \times O(n \log q)}$

LWE: learning with errors

$$(\mathbf{B},\ \mathbf{sB}\qquad) \approx_c \text{uniform}$$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{B} \leftarrow \mathbb{Z}_q^{n\times O(n\log q)}$

computation on matrices

$\mathbf{A}_i$

$i \in [\ell]$

computation on matrices

$$\mathbf{A}_i \quad i \in [\ell] \quad \stackrel{f}{\longmapsto} \quad \mathbf{A}_f$$

computation on matrices

$$\mathbf{A}_i \quad \xmapsto{f} \quad \mathbf{A}_f$$

$i \in [\ell]$

$$\mathbf{A}_f \approx f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)$$

computation on matrices

$$\boxed{\mathbf{A}_i}_{\,i \in [\ell]} \xmapsto{\ f\ } \boxed{\mathbf{A}_f}$$

$$\mathbf{A}_f \approx f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)$$

example. $f(x_1, x_2, x_3, x_4) = x_1 + x_3 + x_4$

$$\mathbf{A}_f = \mathbf{A}_1 + \mathbf{A}_3 + \mathbf{A}_4$$

computation on matrices

$$\mathbf{A}_i \quad \xrightarrow{f} \quad \mathbf{A}_f$$

$i \in [\ell]$

$$\mathbf{A}_f \approx f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)$$

example. $f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4$

$$\mathbf{A}_f \approx \mathbf{A}_1 \mathbf{A}_2 \qquad + \ \mathbf{A}_3 \mathbf{A}_4$$

computation on matrices

$$\boxed{\mathbf{A}_i}_{\,i \in [\ell]} \;\overset{f}{\longmapsto}\; \boxed{\mathbf{A}_f}$$

$$\mathbf{A}_f \approx f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)$$

example. $f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4$

$$\mathbf{A}_f = \mathbf{A}_1 \mathbf{G}^{-1}(\mathbf{A}_2) + \mathbf{A}_3 \mathbf{G}^{-1}(\mathbf{A}_4)$$

computation on matrices

$$\mathbf{A}_i \quad \xrightarrow{f} \quad \mathbf{A}_f$$

$i \in [\ell]$

$$\mathbf{A}_f \approx f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)$$

lemma. **[BGGHNSVV14,GSW13]**

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}] \qquad \mathbf{A}_f - f(x)\mathbf{G}$$

gadget matrix $\mathbf{G} = [\mathbf{I} \mid 2\mathbf{I} \mid 4\mathbf{I} \cdots \mid \frac{q}{2}\mathbf{I}] \in \mathbb{Z}_q^{n \times O(n \log q)}$

computation on matrices

$$\boxed{\mathbf{A}_i}_{\,i \in [\ell]} \overset{f}{\longmapsto} \boxed{\mathbf{A}_f}$$

$$\mathbf{A}_f \approx f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)$$

lemma. $\forall \mathbf{A}_i, \forall f, \forall x, \exists$ **<u>small</u>** $\mathbf{H}_{\mathbf{A},f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}] \cdot \mathbf{H}_{\mathbf{A},f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

gadget matrix $\mathbf{G} = [\mathbf{I} \mid 2\mathbf{I} \mid 4\mathbf{I} \cdots \mid \frac{q}{2}\mathbf{I}] \in \mathbb{Z}_q^{n \times O(n \log q)}$

lattice-based ABE

key-policy

ct$_x$: $[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]$

sk$_f$: $\mathbf{A}_f$

pp : $\mathbf{A}_1, \ldots, \mathbf{A}_\ell$

lattice-based ABE

key-policy

ct$_x$: $\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]$

sk$_f$: $\mathbf{A}_f$

pp : $\mathbf{A}_1, \ldots, \mathbf{A}_\ell$

lattice-based ABE

key-policy

$\mathbf{ct}_x : \underset{\sim}{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underset{\sim}{\mathbf{sA}_0}, \underset{\sim}{\mathbf{sp}} + M$

$\mathbf{sk}_f : \mathbf{A}_f$

$\mathbf{pp} : \mathbf{A}_1, \ldots, \mathbf{A}_\ell, \mathbf{A}_0, \mathbf{p}$

lattice-based ABE

key-policy

$$\mathbf{ct}_x : \underset{\sim}{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underset{\sim}{\mathbf{s}\mathbf{A}_0}, \underset{\sim}{\mathbf{s}\mathbf{p}} + M$$

$$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$$

$$\mathbf{pp} : \mathbf{A}_1, \ldots, \mathbf{A}_\ell, \mathbf{A}_0, \mathbf{p}$$

lattice-based ABE

key-policy

$$\mathbf{ct}_x : \underset{\sim}{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underset{\sim}{\mathbf{s}\mathbf{A}_0}, \underset{\sim}{\mathbf{s}\mathbf{p}} + M$$

$$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$$

$$\mathbf{D} : \mathbf{ct}_x \overset{\mathbf{H}_{\mathbf{A},f,x}}{\longmapsto} \underset{\sim}{\mathbf{s}(\mathbf{A}_f - f(x)\mathbf{G})}$$

lattice-based ABE

key-policy

$$\mathbf{ct}_x : \underbrace{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underbrace{\mathbf{s}\mathbf{A}_0}, \underbrace{\mathbf{s}\mathbf{p}} + M$$

$$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$$

$$\mathbf{D} : \mathbf{ct}_x \xmapsto{\mathbf{H}_{\mathbf{A},f,x}} \underbrace{\mathbf{s}\mathbf{A}_f} \qquad \text{if } f(x) = 0$$

lattice-based ABE

key-policy

$$\mathbf{ct}_x : \underset{\sim}{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underset{\sim}{\mathbf{s}\mathbf{A}_0}, \underset{\sim}{\mathbf{s}\mathbf{p}} + M$$

$$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$$

$$\mathbf{D} : \mathbf{ct}_x \xmapsto{\mathbf{H}_{\mathbf{A},f,x}} [\underset{\sim}{\mathbf{s}\mathbf{A}_f} \mid \underset{\sim}{\mathbf{s}\mathbf{A}_0}] \xmapsto{\mathbf{sk}_f} \underset{\sim}{\mathbf{s}\mathbf{p}} \qquad \text{if } f(x) = 0$$

lattice-based ABE

key-policy

$\mathbf{ct}_x : \underset{\sim}{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underset{\sim}{\mathbf{sA}_0}, \underset{\sim}{\mathbf{sp}} + M$

$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$

ciphertext-policy

$\mathbf{ct}_f : \underset{\sim}{\mathbf{sA}_f}$

$\mathbf{sk}_x : \qquad [\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]$

lattice-based ABE

key-policy

$$\mathbf{ct}_x : \underset{\sim}{\mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}]}, \underset{\sim}{\mathbf{s}\mathbf{A}_0}, \underset{\sim}{\mathbf{s}\mathbf{p}} + M$$

$$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$$

ciphertext-policy

$$\mathbf{ct}_f : \underset{\sim}{\mathbf{s}(\mathbf{A}_f \otimes \mathbf{I})}, \underset{\sim}{\mathbf{s}\mathbf{A}_0}, \ldots$$

$$\mathbf{sk}_x : \mathbf{A}_0 \cdot \mathbf{sk}_f = [\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}] \otimes \mathbf{r}$$

lattice-based ABE

key-policy – based on LWE

$\mathbf{ct}_x : \mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}], \mathbf{s}\mathbf{A}_0, \mathbf{s}\mathbf{p} + M$

$\mathbf{sk}_f : [\mathbf{A}_f \mid \mathbf{A}_0] \cdot \mathbf{sk}_f = \mathbf{p}$

ciphertext-policy – based on "evasive" LWE

$\mathbf{ct}_f : \mathbf{s}(\mathbf{A}_f \otimes \mathbf{I}), \mathbf{s}\mathbf{A}_0, \ldots$

$\mathbf{sk}_x : \mathbf{A}_0 \cdot \mathbf{sk}_f = [\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}] \otimes \mathbf{r}$

how to **compute** f ?

example. $f(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4$

how to **compute** f ?

example. $f(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4$

$$(x_1 x_2)(x_3 x_4) \qquad\qquad x_1(x_2(x_3 x_4))$$

how to **compute** f?

example. $f(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4$

$$(x_1 x_2)(x_3 x_4) \qquad x_1(x_2(x_3 x_4))$$

$$\mathbf{A}_1 \mathbf{G}^{-1}(\mathbf{A}_2)\mathbf{G}^{-1}(\mathbf{A}_3 \mathbf{G}^{-1}(\mathbf{A}_4)) \qquad \mathbf{A}_1 \mathbf{G}^{-1}(\mathbf{A}_2 \mathbf{G}^{-1}(\mathbf{A}_3 \mathbf{G}^{-1}(\mathbf{A}_4)))$$

how to **compute** f?

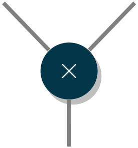
example. $f(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4$

$\times\ (x_1 x_2)(x_3 x_4)$ $\checkmark\ x_1(x_2(x_3 x_4))$

$\mathbf{A}_1\mathbf{G}^{-1}(\mathbf{A}_2)\mathbf{G}^{-1}(\mathbf{A}_3\mathbf{G}^{-1}(\mathbf{A}_4))$ $\mathbf{A}_1\mathbf{G}^{-1}(\mathbf{A}_2\mathbf{G}^{-1}(\mathbf{A}_3\mathbf{G}^{-1}(\mathbf{A}_4)))$

how to **compute** f ?

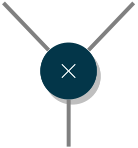
circuit



intermediate $\times$ intermediate

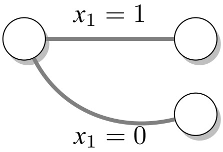
how to **compute** f?

circuit



intermediate $\times$ intermediate

branching program

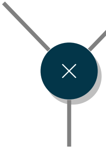


intermediate $\times$ input

how to **compute** f?

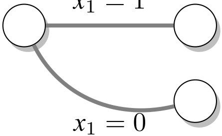
circuit $\subseteq$ **branching program**

depth $O(\log n)$



intermediate $\times$ intermediate

length poly(n)



intermediate $\times$ input

how to **compute** f ?

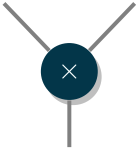
circuit

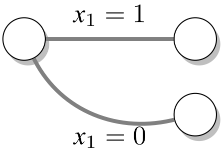
depth $O(\log n)$

$\subseteq$

branching program

length poly(n)





$\times$ modulus $n^{O(\log n)}$

$\checkmark$ modulus poly(n)

[GVW13, GV15, ...]

broadcast encryption

$$\mathbf{ct}_S \leftarrow \mathbf{E}(S \subseteq [N], m), \mathbf{sk}_x \leftarrow \mathbf{G}(x \in [N])$$

$$\mathbf{D}(\mathbf{ct}_S, \mathbf{sk}_x) = m \text{ if } x \in S$$

broadcast encryption

$$\mathbf{ct}_S \leftarrow \mathbf{E}(S \subseteq [N], m), \mathbf{sk}_x \leftarrow \mathbf{G}(x \in [N])$$

$$\mathbf{D}(\mathbf{ct}_S, \mathbf{sk}_x) = m \text{ if } x \in S$$

fact. broadcast = CP-ABE for $f_S(x) := (x \overset{?}{\in} S)$

broadcast encryption

$\mathbf{ct}_S \leftarrow \mathbf{E}(S \subseteq [N], m), \mathbf{sk}_x \leftarrow \mathbf{G}(x \in [N])$

$\mathbf{D}(\mathbf{ct}_S, \mathbf{sk}_x) = m$ if $x \in S$

fact. broadcast = CP-ABE for $f_S(x) := (x \stackrel{?}{\in} S)$

fact. $f_S \in$ deg d polynomials over $\{0,1\}^{dN^{1/d}}$

broadcast encryption

$$\mathbf{ct}_S \leftarrow \mathbf{E}(S \subseteq [N], m), \mathbf{sk}_x \leftarrow \mathbf{G}(x \in [N])$$

$$\mathbf{D}(\mathbf{ct}_S, \mathbf{sk}_x) = m \text{ if } x \in S$$

fact. broadcast = CP-ABE for $f_S(x) := (x \overset{?}{\in} S)$

fact. $f_S \in$ deg d polynomials over $\{0,1\}^{dN^{1/d}}$

state of the art for broadcast

$|\mathbf{ct}_S|, |\mathbf{sk}_x| = O(N^{1/2})$ via pairings **[BGW05, ...]**

broadcast encryption

$\mathbf{ct}_S \leftarrow \mathbf{E}(S \subseteq [N], m), \mathbf{sk}_x \leftarrow \mathbf{G}(x \in [N])$

$\mathbf{D}(\mathbf{ct}_S, \mathbf{sk}_x) = m$ if $x \in S$

fact. broadcast = CP-ABE for $f_S(x) := (x \overset{?}{\in} S)$

fact. $f_S \in$ deg d polynomials over $\{0,1\}^{dN^{1/d}}$

state of the art for broadcast

$|\mathbf{ct}_S|, |\mathbf{sk}_x| = O(N^{1/3})$ via pairings [W21]

broadcast encryption

$\mathbf{ct}_S \leftarrow \mathbf{E}(S \subseteq [N], m), \mathbf{sk}_x \leftarrow \mathbf{G}(x \in [N])$

$\mathbf{D}(\mathbf{ct}_S, \mathbf{sk}_x) = m$ if $x \in S$

fact. broadcast = CP-ABE for $f_S(x) := (x \overset{?}{\in} S)$

fact. $f_S \in$ deg d polynomials over $\{0,1\}^{dN^{1/d}}$

state of the art for broadcast

$|\mathbf{ct}_S|, |\mathbf{sk}_x| = \text{poly}(\log N)$ via lattices **[W22,BV22,AY20]**

ABE & lattices: what's **next**?

ABE & lattices: what's **next**?

theory oriented

– sublinear $|\mathbf{ct}|$ from falsifiable assumptions

– removing poly(depth) factors

ABE & lattices: what's **next**?

theory oriented

- sublinear $|\mathbf{ct}|$ from falsifiable assumptions
- removing poly(depth) factors
- surprises? (vis-à-vis pairings)

ABE & lattices: what's **next**?

theory oriented

– sublinear $|\mathbf{ct}|$ from falsifiable assumptions

– removing poly(depth) factors

– surprises? (vis-à-vis pairings)

practice oriented

– concrete efficiency & structured lattices

ABE & lattices: what's **next**?

theory oriented

– sublinear $|\mathbf{ct}|$ from falsifiable assumptions

– removing poly(depth) factors

– surprises? (vis-à-vis pairings)

practice oriented

– concrete efficiency & structured lattices

IBE: ciphertext $\approx$ Kyber, keys $\approx$ Falcon

ABE & lattices: what's **next**?

theory oriented

– sublinear $|\mathbf{ct}|$ from falsifiable assumptions

– removing poly(depth) factors

– surprises? (vis-à-vis pairings)

practice oriented

– concrete efficiency & structured lattices

– optimizing $\mathbf{A}_f$ for simple f?

ABE & lattices: what's **next**?

theory oriented

– sublinear $|\mathbf{ct}|$ from falsifiable assumptions

– removing poly(depth) factors

– surprises? (vis-à-vis pairings)

practice oriented

– concrete efficiency & structured lattices

– optimizing $\mathbf{A}_f$ for simple f?

// thanks!