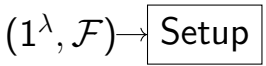
Faster ABE for Turing Machines from Circular Evasive LWE

Valerio Cini Hoeteck Wee

Bocconi NTTResearch

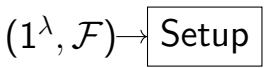
Attribute-Based Encryption [SahaiWaters05]

Attribute-Based Encryption [SahaiWaters05]



Attribute-Based Encryption [SahaiWaters05]

class description $\mathcal{F}$



Attribute-Based Encryption [SahaiWaters05]

class description $\mathcal{F}$, e.g. $\begin{cases} \text{arithmetic circuits} \\ \\ \end{cases}$

$(1^\lambda, \mathcal{F}) \longrightarrow$ Setup

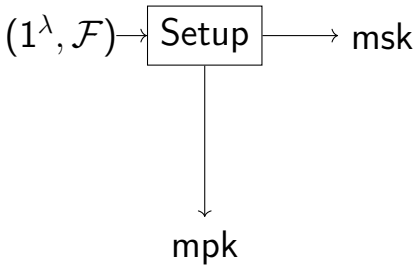
Attribute-Based Encryption [SahaiWaters05]

class description $\mathcal{F}$, e.g. $\begin{cases} \text{arithmetic circuits} \\ \underline{\text{Turing machines}} \end{cases}$

$(1^\lambda, \mathcal{F}) \longrightarrow \boxed{\text{Setup}}$

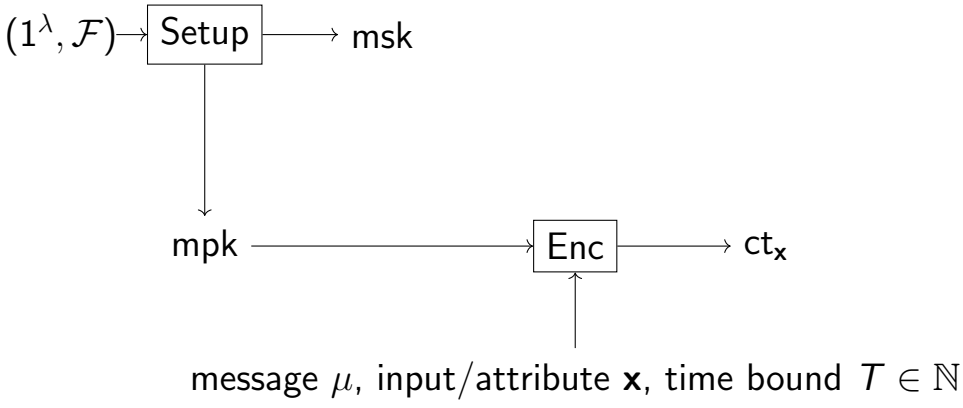
Attribute-Based Encryption [SahaiWaters05]

class description $\mathcal{F}$, e.g. $\begin{cases} \text{arithmetic circuits} \\ \underline{\text{Turing machines}} \end{cases}$

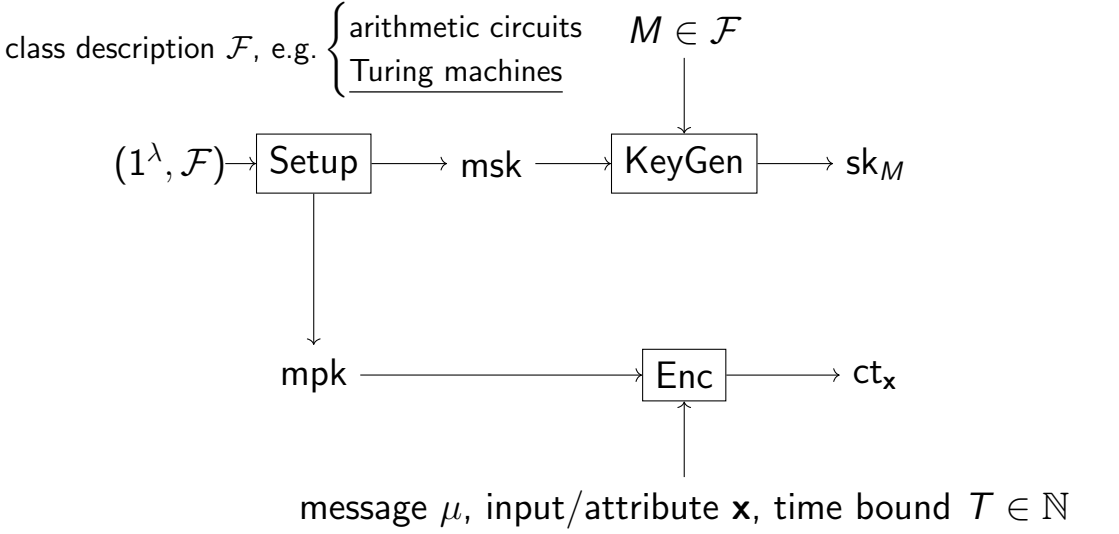


Attribute-Based Encryption [SahaiWaters05]

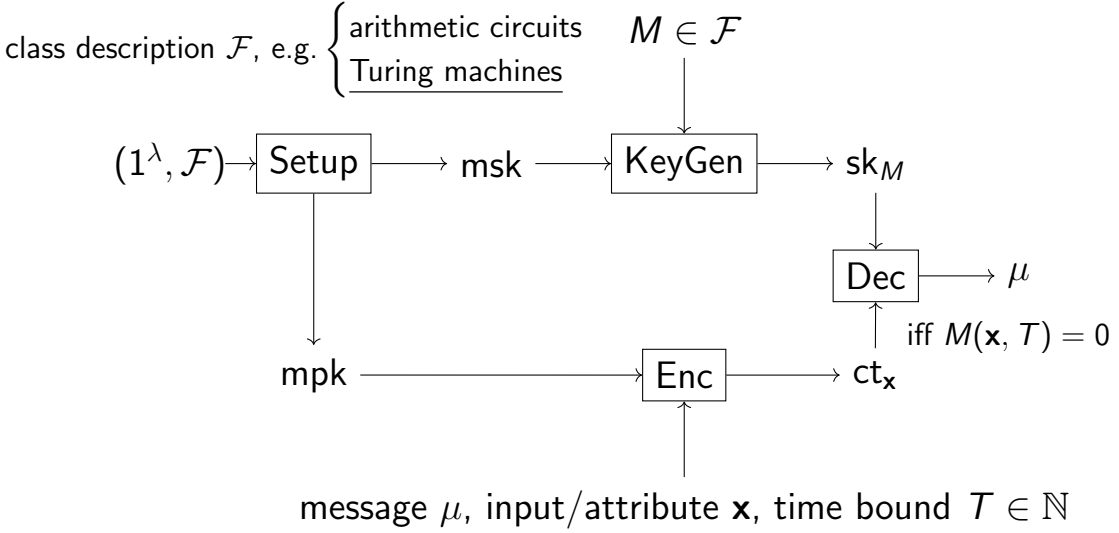
class description $\mathcal{F}$, e.g. { arithmetic circuits / Turing machines }



Attribute-Based Encryption [SahaiWaters05]



Attribute-Based Encryption [SahaiWaters05]



ABE for Turing Machines

[AgrawalKumariYamada24]

- $|\mathsf{ct}| = O(T^2)$
- $|\mathsf{sk}| = O(|M|^2)$
- from Circular Evasive LWE [HLL23] + Tensor LWE [W22]

ABE for Turing Machines

Our Results

- $|\mathsf{ct}| = O(T)$ and $\mathsf{Time}(\mathsf{Enc}) = O(T)$
- $|\mathsf{sk}| = O(1)$ and $\mathsf{Time}(\mathsf{KeyGen}) = O(|M|)$
- from Circular Evasive LWE [HLL23] + ~~Tensor LWE [W22]~~

ABE for Turing Machines

Our Results

- $|\mathsf{ct}| = O(T)$ and $\mathsf{Time}(\mathsf{Enc}) = O(T)$
- $|\mathsf{sk}| = O(1)$ and $\mathsf{Time}(\mathsf{KeyGen}) = O(|M|)$
- from Circular Evasive LWE [HLL23] + ~~Tensor LWE [W22]~~

new encoding and techniques to switch b/w them

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG^+ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G}) | \ldots | \mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG^+ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G})| \dots |\mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

✓ homomorphically evaluate any circuit

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG^+ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G}) | \ldots | \mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

✓ homomorphically evaluate any circuit ✗ $|\mathbf{A}| = O(|\mathbf{z}|)$

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG$^+$ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G})| \ldots |\mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

✓ homomorphically evaluate any circuit ✗ $|\mathbf{A}| = O(|\mathbf{z}|)$

this work : dual encodings of $\mathbf{z} \in \{0,1\}^\ell$

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG$^+$ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G}) | \ldots | \mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

✓ homomorphically evaluate any circuit ✗ $|\mathbf{A}| = O(|\mathbf{z}|)$

this work : dual encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G} = [\mathbf{s}_1(\mathbf{A}_0 - z_1\mathbf{G}) \,\backslash\backslash\, \ldots \,\backslash\backslash\, \mathbf{s}_\ell(\mathbf{A}_0 - z_\ell\mathbf{G})]$$

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG^+ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G}) | \ldots | \mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

✓ homomorphically evaluate any circuit ✗ $|\mathbf{A}| = O(|\mathbf{z}|)$

this work : dual encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{S}\mathbf{A}_0 - \mathsf{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G} = [\mathbf{s}_1(\mathbf{A}_0 - z_1\mathbf{G}) \,\|\, \ldots \,\|\, \mathbf{s}_\ell(\mathbf{A}_0 - z_\ell\mathbf{G})]$$

✓ $|\mathbf{A}_0| = O(1)$

Attribute Encodings

[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14] : BGG$^+$ encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{s}(\mathbf{A} - \mathbf{z} \otimes \mathbf{G}) = [\mathbf{s}(\mathbf{A}_1 - z_1\mathbf{G}) | \ldots | \mathbf{s}(\mathbf{A}_\ell - z_\ell\mathbf{G})]$$

✓ homomorphically evaluate any circuit ✗ $|\mathbf{A}| = O(|\mathbf{z}|)$

this work : dual encodings of $\mathbf{z} \in \{0,1\}^\ell$

$$\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G} = [\mathbf{s}_1(\mathbf{A}_0 - z_1\mathbf{G}) \,\|\, \ldots \,\|\, \mathbf{s}_\ell(\mathbf{A}_0 - z_\ell\mathbf{G})]$$

✗ only support projections ✓ $|\mathbf{A}_0| = O(1)$

Recoding of Attribute Encodings

Main Idea:
- dual encoding for (global) work tape
- BGG^{+} encodings for (local) computation

Recoding of Attribute Encodings

Main Idea:
- dual encoding for (global) work tape
- BGG^{+} encodings for (local) computation

how to switch between the two types of encodings?

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \quad \longrightarrow \quad \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \longrightarrow \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

$$(\mathbf{C}, \mathbf{C}') = (\mathbf{S}\mathbf{B}, \mathbf{S}\mathbf{W} + \mathbf{S}'\mathbf{G})$$

$$\mathbf{K} \leftarrow \mathbf{B}^{-1}\big(\,\mathbf{A}_0\mathbf{G}^{-1}(\mathbf{W}) - \mathbf{W}\mathbf{G}^{-1}(\mathbf{A}'_0)\,\big)$$

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \longrightarrow \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

$$\mathbf{B}, \mathbf{W} \in \mathsf{mpk}$$

$$(\mathbf{C}, \mathbf{C}') = (\mathbf{S}\mathbf{B}, \mathbf{S}\mathbf{W} + \mathbf{S}'\mathbf{G})$$

$$\mathbf{K} \leftarrow \mathbf{B}^{-1}\big(\mathbf{A}_0\mathbf{G}^{-1}(\mathbf{W}) - \mathbf{W}\mathbf{G}^{-1}(\mathbf{A}'_0)\big)$$

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \longrightarrow \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

$\mathbf{B}, \mathbf{W} \in \mathsf{mpk}$

$$\text{ciphertext} \quad (\mathbf{C}, \mathbf{C}') = (\mathbf{S}\mathbf{B}, \mathbf{S}\mathbf{W} + \mathbf{S}'\mathbf{G})$$

$$\mathbf{K} \leftarrow \mathbf{B}^{-1}\big(\mathbf{A}_0\mathbf{G}^{-1}(\mathbf{W}) - \mathbf{W}\mathbf{G}^{-1}(\mathbf{A}'_0)\big)$$

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \longrightarrow \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

$\mathbf{B}, \mathbf{W} \in \mathsf{mpk}$

ciphertext $(\mathbf{C}, \mathbf{C}') = (\mathbf{S}\mathbf{B}, \mathbf{S}\mathbf{W} + \mathbf{S}'\mathbf{G})$

secret key $\mathbf{K} \leftarrow \mathbf{B}^{-1}\big(\mathbf{A}_0\mathbf{G}^{-1}(\mathbf{W}) - \mathbf{W}\mathbf{G}^{-1}(\mathbf{A}'_0)\big)$

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \longrightarrow \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

$\mathbf{B}, \mathbf{W} \in \mathsf{mpk}$

ciphertext $(\mathbf{C}, \mathbf{C}') = (\mathbf{S}\mathbf{B}, \mathbf{S}\mathbf{W} + \mathbf{S}'\mathbf{G})$

secret key $\mathbf{K} \leftarrow \mathbf{B}^{-1}\big(\mathbf{A}_0\mathbf{G}^{-1}(\mathbf{W}) - \mathbf{W}\mathbf{G}^{-1}(\mathbf{A}'_0)\big)$

$|(\mathbf{C}, \mathbf{C}')| = O(|\mathbf{z}|) \longleftarrow$ linear in size of attribute / depend on $\mathbf{S}, \mathbf{S}'$

$|\mathbf{K}| = O(1) \longleftarrow$ constant size / independent

Recoding of Attribute Encodings

$$\mathbf{z},\ \overbrace{\mathbf{S}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}, \mathbf{A}_0} \longrightarrow \overbrace{\mathbf{S}'\mathbf{A}'_0 - \mathrm{diag}(\mathbf{z}) \cdot \mathbf{S}'\mathbf{G}}^{\text{dual encoding of } \mathbf{z} \text{ under } \mathbf{S}', \mathbf{A}'_0}$$

$\mathbf{B}, \mathbf{W} \in \mathsf{mpk}$

ciphertext $(\mathbf{C}, \mathbf{C}') = (\mathbf{S}\mathbf{B}, \mathbf{S}\mathbf{W} + \mathbf{S}'\mathbf{G})$

secret key $\mathbf{K} \leftarrow \mathbf{B}^{-1}\big(\mathbf{A}_0\mathbf{G}^{-1}(\mathbf{W}) - \mathbf{W}\mathbf{G}^{-1}(\mathbf{A}'_0)\big)$

$|\text{ciphertext component}| \longleftarrow$ linear in size of attribute

$|\text{key component}| \longleftarrow$ constant size

similar results hold for all other possible recodings
1) dual-to-dual
2) BGG^+-to-dual
3) dual-to-BGG^+

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \mathsf{read}, \mathsf{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \text{read}, \text{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \text{read}, \text{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$\mathbf{z}_0 = \mathbf{x} || 0^{S-\ell}$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \text{read}, \text{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$\mathbf{z}_0 = \mathbf{x} || 0^{S-\ell} \rightarrow \cdots \rightarrow \mathbf{z}_t$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \mathsf{read}, \mathsf{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$$\mathbf{z}_0 = \mathbf{x}||0^{S-\ell} \to \cdots \to \mathbf{z}_t = \begin{cases} \mathbf{z}_t[\overline{\mathsf{write}(t)}] = \mathbf{z}_{t-1}[\overline{\mathsf{write}(t)}] \\ \end{cases}$$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \mathsf{read}, \mathsf{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$$\mathbf{z}_0 = \mathbf{x} || 0^{S-\ell} \to \cdots \to \mathbf{z}_t = \begin{cases} \mathbf{z}_t[\overline{\mathsf{write}(t)}] = \mathbf{z}_{t-1}[\overline{\mathsf{write}(t)}] \\ \mathbf{z}_t[\mathsf{write}(t)] = f(\mathbf{z}_{t-1}[\mathsf{read}(t)]) \end{cases}$$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \mathsf{read}, \mathsf{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$$\mathbf{z}_0 = \mathbf{x} || 0^{S-\ell} \to \cdots \to \mathbf{z}_t = \begin{cases} \mathbf{z}_t[\overline{\mathsf{write}(t)}] = \mathbf{z}_{t-1}[\overline{\mathsf{write}(t)}] \\ \mathbf{z}_t[\mathsf{write}(t)] = f(\mathbf{z}_{t-1}[\mathsf{read}(t)]) \end{cases} \to \cdots \to \mathbf{z}_T$$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \text{read}, \text{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$$\mathbf{z}_0 = \mathbf{x}||0^{S-\ell} \to \cdots \to \mathbf{z}_t = \begin{cases} \mathbf{z}_t[\overline{\text{write}(t)}] = \mathbf{z}_{t-1}[\overline{\text{write}(t)}] \\ \mathbf{z}_t[\text{write}(t)] = f(\mathbf{z}_{t-1}[\text{read}(t)]) \end{cases} \to \cdots \to \mathbf{z}_T$$

It captures Oblivious TM with 2^{L-1} states and alphabet $\{0,1\}$

Iterated Computation

ABE for Iterated Computation with locality L, space S, and time T

$$f : \{0,1\}^L \longrightarrow \{0,1\}^L, \quad \mathsf{read}, \mathsf{write} : [T] \longrightarrow \binom{S}{L}, \quad L \ll S \leq T$$

- $\mathbf{z}_t \in \{0,1\}^S$, $t = 0, 1, \ldots, T$, denotes the work tape at step t

$$\mathbf{z}_0 = \mathbf{x}||0^{S-\ell} \rightarrow \cdots \rightarrow \mathbf{z}_t = \begin{cases} \mathbf{z}_t[\overline{\mathsf{write}(t)}] = \mathbf{z}_{t-1}[\overline{\mathsf{write}(t)}] \\ \mathbf{z}_t[\mathsf{write}(t)] = f(\mathbf{z}_{t-1}[\mathsf{read}(t)]) \end{cases} \rightarrow \cdots \rightarrow \mathbf{z}_T$$

It captures Oblivious TM with 2^{L-1} states and alphabet $\{0,1\}$

Arbitrary TM with $O(\log T)$ overhead [PippengerFischer79]

Roadmap to final scheme

Decryption invariant: $\mathbf{S}_t\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$

Roadmap to final scheme

Decryption invariant: $\mathbf{S}_t\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$

$\underbrace{\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_T}_{\text{associated with ciphertext}} \in \mathbb{Z}_q^{S \times n}$ $\qquad$ $\underbrace{\mathbf{A}_0}_{\text{associated with secret key}} \in \mathbb{Z}_q^{n \times m}$

Roadmap to final scheme

Decryption invariant: $\mathbf{S}_t\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$

$$\underbrace{\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_T}_{\text{associated with ciphertext}} \in \mathbb{Z}_q^{S \times n} \qquad \underbrace{\mathbf{A}_0}_{\text{associated with secret key}} \in \mathbb{Z}_q^{n \times m}$$

- warm-up: all $\mathbf{S}_t$ are independent, secure but quadratic size/time

Roadmap to final scheme

Decryption invariant: $\mathbf{S}_t\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$

$\underbrace{\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_T}_{\text{associated with ciphertext}} \in \mathbb{Z}_q^{S \times n}$ $\qquad$ $\underbrace{\mathbf{A}_0}_{\text{associated with secret key}} \in \mathbb{Z}_q^{n \times m}$

- warm-up: all $\mathbf{S}_t$ are independent, secure but quadratic size/time
- attempt 1: all $\mathbf{S}_t$ are the same, linear time but insecure

Roadmap to final scheme

Decryption invariant: $\mathbf{S}_t\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$

$$\underbrace{\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_T}_{\text{associated with ciphertext}} \in \mathbb{Z}_q^{S \times n} \qquad \underbrace{\mathbf{A}_0}_{\text{associated with secret key}} \in \mathbb{Z}_q^{n \times m}$$

- warm-up: all $\mathbf{S}_t$ are independent, secure but quadratic size/time
- attempt 1: all $\mathbf{S}_t$ are the same, linear time but insecure
- final: each $\mathbf{S}_t$ fresh random in U_t, with $|U_t| = O(L)$.

Warm-Up Construction

step t computation

$$\tilde{\mathbf{C}}_{t-1} \coloneqq \mathbf{S}_{t-1}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_{t-1}) \cdot \mathbf{S}_{t-1}\mathbf{G}$$

$$\tilde{\mathbf{C}}_{t} \coloneqq \mathbf{S}_{t}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_{t}) \cdot \mathbf{S}_{t}\mathbf{G}$$

Warm-Up Construction

step t computation

$$\tilde{\mathbf{C}}_{t-1} \coloneqq \mathbf{S}_{t-1}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_{t-1}) \cdot \mathbf{S}_{t-1}\mathbf{G}$$

$\tilde{\mathbf{C}}_{t-1}[\mathsf{read}(t)]$

$\tilde{\mathbf{C}}_{t-1}[\overline{\mathsf{write}(t)}]$

$$\tilde{\mathbf{C}}_t \coloneqq \mathbf{S}_t\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$$

Warm-Up Construction

step t computation

$$\tilde{\mathbf{C}}_{t-1} \coloneqq \mathbf{S}_{t-1}\mathbf{A}_0 - \mathsf{diag}(\mathbf{z}_{t-1}) \cdot \mathbf{S}_{t-1}\mathbf{G}$$

$\tilde{\mathbf{C}}_{t-1}[\mathsf{read}(t)]$

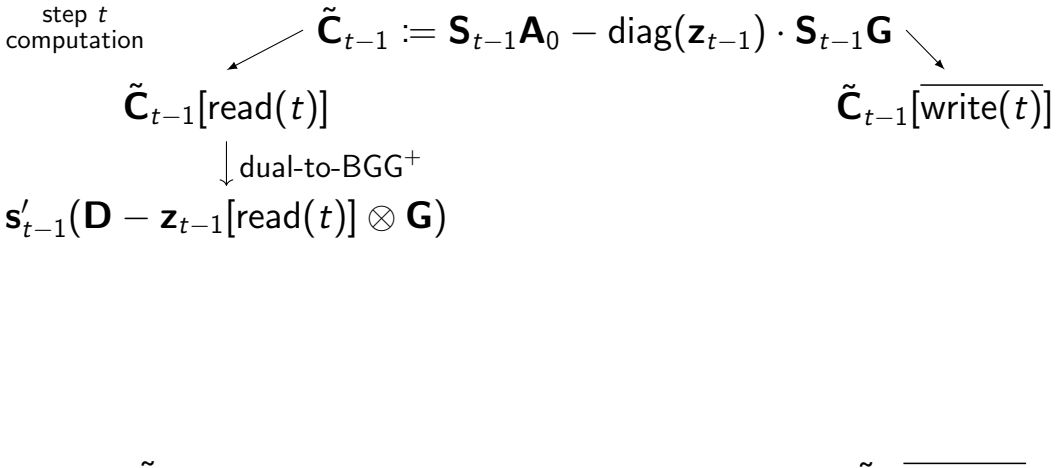
$\tilde{\mathbf{C}}_{t-1}[\overline{\mathsf{write}(t)}]$

$\tilde{\mathbf{C}}_t[\mathsf{write}(t)]$

$\tilde{\mathbf{C}}_t[\overline{\mathsf{write}(t)}]$

$$\tilde{\mathbf{C}}_t \coloneqq \mathbf{S}_t\mathbf{A}_0 - \mathsf{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$$

Warm-Up Construction



Warm-Up Construction

step t computation

$$\tilde{\mathbf{C}}_{t-1} \coloneqq \mathbf{S}_{t-1}\mathbf{A}_0 - \mathsf{diag}(\mathbf{z}_{t-1}) \cdot \mathbf{S}_{t-1}\mathbf{G}$$

$$\tilde{\mathbf{C}}_{t-1}[\mathsf{read}(t)] \qquad \tilde{\mathbf{C}}_{t-1}[\overline{\mathsf{write}(t)}]$$

$\downarrow$ dual-to-BGG$^+$

$$\mathbf{s}'_{t-1}(\mathbf{D} - \mathbf{z}_{t-1}[\mathsf{read}(t)] \otimes \mathbf{G})$$

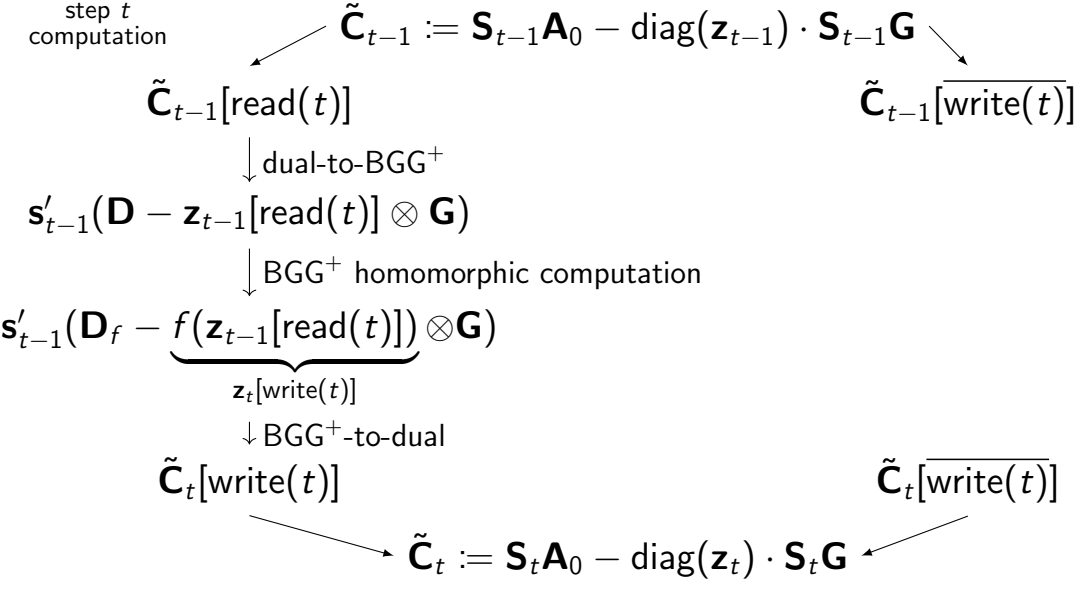
$\downarrow$ BGG$^+$ homomorphic computation

$$\mathbf{s}'_{t-1}(\mathbf{D}_f - \underbrace{f(\mathbf{z}_{t-1}[\mathsf{read}(t)])}_{\mathbf{z}_t[\mathsf{write}(t)]} \otimes \mathbf{G})$$

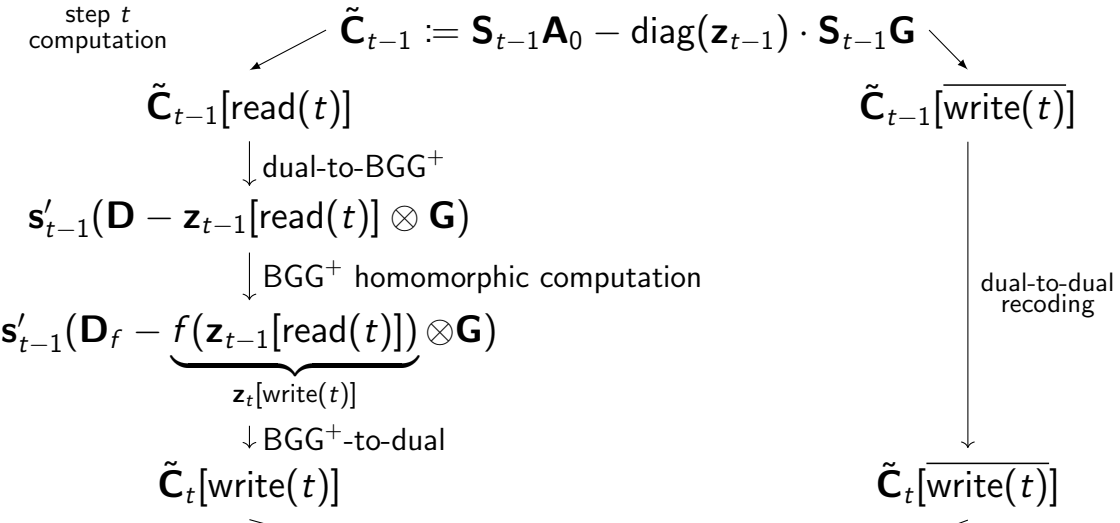
$$\tilde{\mathbf{C}}_t[\mathsf{write}(t)] \qquad \tilde{\mathbf{C}}_t[\overline{\mathsf{write}(t)}]$$

$$\tilde{\mathbf{C}}_t \coloneqq \mathbf{S}_t\mathbf{A}_0 - \mathsf{diag}(\mathbf{z}_t) \cdot \mathbf{S}_t\mathbf{G}$$

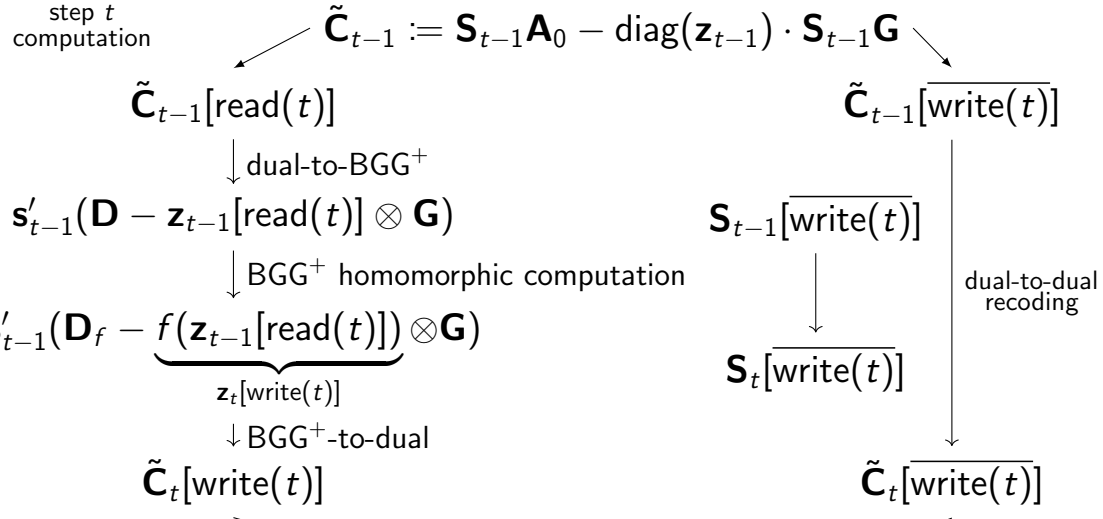
Warm-Up Construction



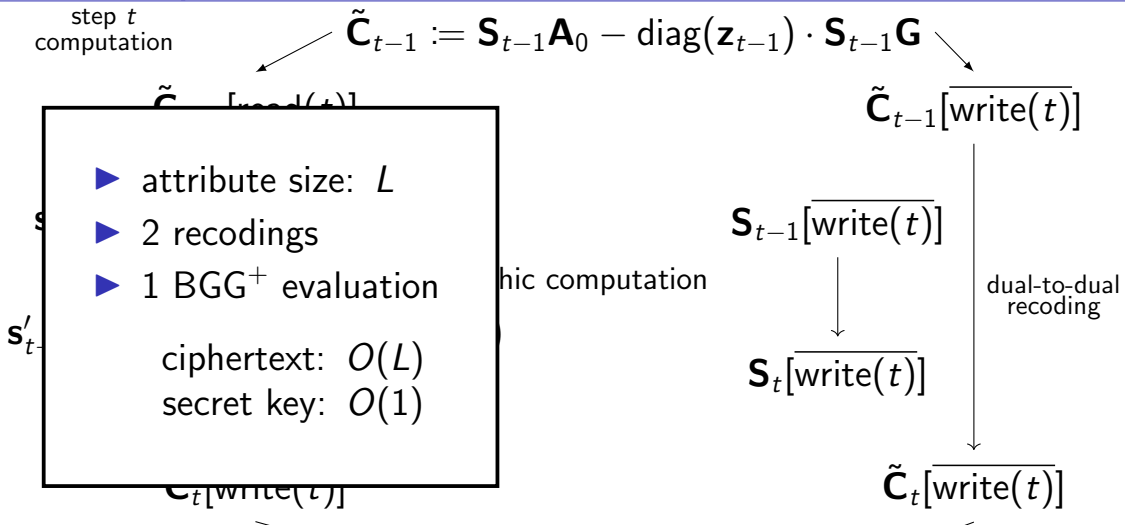
Warm-Up Construction



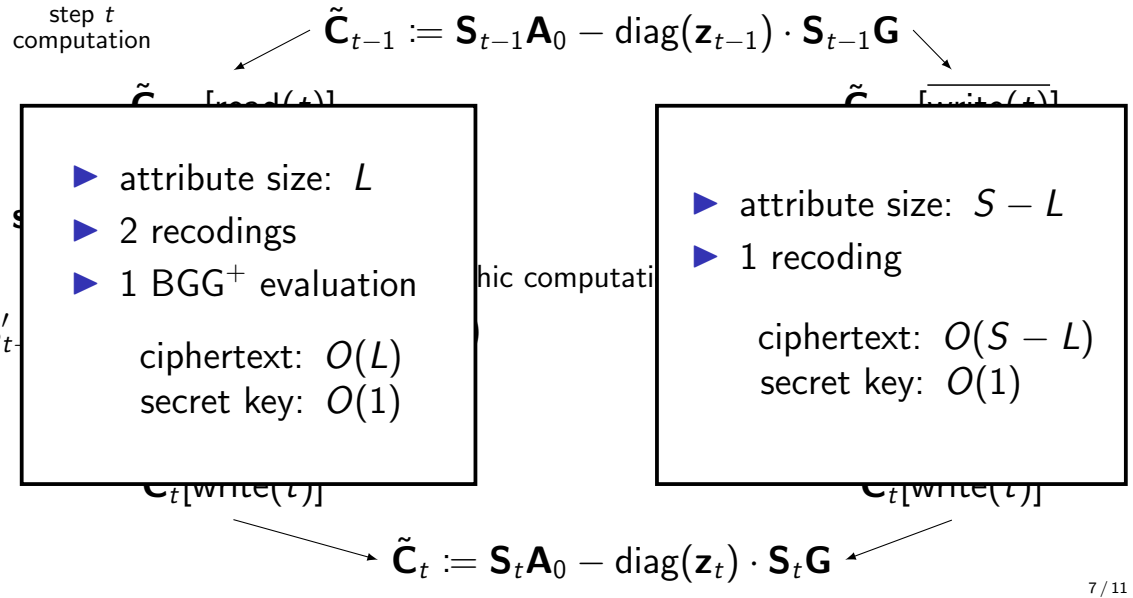
Warm-Up Construction



Warm-Up Construction



Warm-Up Construction



Warm-Up Construction

step t computation

$$\tilde{\mathbf{C}}_{t-1} := \mathbf{S}_{t-1}\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_{t-1}) \cdot \mathbf{S}_{t-1}\mathbf{G}$$

$\tilde{\mathbf{C}}$ [read(t)]

$\tilde{\mathbf{C}}$ [write(t)]

$\mathbf{s}$

hic computati

$\mathbf{s}'_{t-}$

- attribute size: L
- 2 recodings
- 1 BGG$^+$ evaluation

ciphertext: $O(L)$
secret key: $O(1)$

- attribute size: $S - L$
- 1 recoding

ciphertext: $O(S - L)$
secret key: $O(1)$

over T computation steps $\begin{cases} \text{ciphertext: } O(S \cdot T) \\ \text{secret key: } O(1) \end{cases}$

Improving Efficiency (1/2)

Can we set $\mathbf{S}_0 = \mathbf{S}_1 = \cdots = \mathbf{S}_T$?

Improving Efficiency (1/2)

Can we set $\mathbf{S}_0 = \mathbf{S}_1 = \cdots = \mathbf{S}_T$?

$$\mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_0) \cdot \mathbf{S}_0\mathbf{G}, \quad \mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_1) \cdot \mathbf{S}_0\mathbf{G}$$

$\Longrightarrow$ it leaks partial information about $\mathbf{S}_0$ whenever $\mathbf{z}_0 \neq \mathbf{z}_1$ ✗

Improving Efficiency (1/2)

Can we set $\mathbf{S}_0 = \mathbf{S}_1 = \cdots = \mathbf{S}_T$?

$$\mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_0) \cdot \mathbf{S}_0\mathbf{G}, \quad \mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_1) \cdot \mathbf{S}_0\mathbf{G}$$

$\Longrightarrow$ it leaks partial information about $\mathbf{S}_0$ whenever $\mathbf{z}_0 \neq \mathbf{z}_1$ ✗

Instead, we use fresh randomness for

$$\mathbf{S}_1[U_1], \mathbf{S}_2[U_2], \ldots, \mathbf{S}_T[U_T]$$

for some sets $U_1, U_2, \ldots, U_T$.

Improving Efficiency (1/2)

Can we set $\mathbf{S}_0 = \mathbf{S}_1 = \cdots = \mathbf{S}_T$?

$$\mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_0) \cdot \mathbf{S}_0\mathbf{G}, \quad \mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_1) \cdot \mathbf{S}_0\mathbf{G}$$

$\Longrightarrow$ it leaks partial information about $\mathbf{S}_0$ whenever $\mathbf{z}_0 \neq \mathbf{z}_1$ ✗

Instead, we use fresh randomness for

$$\mathbf{S}_1[U_1], \mathbf{S}_2[U_2], \ldots, \mathbf{S}_T[U_T]$$

for some sets $U_1, U_2, \ldots, U_T$. Need $|U_i| = O(L)$ for efficiency

Improving Efficiency (1/2)

Can we set $\mathbf{S}_0 = \mathbf{S}_1 = \cdots = \mathbf{S}_T$?

$$\mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_0) \cdot \mathbf{S}_0\mathbf{G}, \quad \mathbf{S}_0\mathbf{A}_0 - \mathrm{diag}(\mathbf{z}_1) \cdot \mathbf{S}_0\mathbf{G}$$

$\Longrightarrow$ it leaks partial information about $\mathbf{S}_0$ whenever $\mathbf{z}_0 \neq \mathbf{z}_1$ ✗

Instead, we use fresh randomness for $\boxed{U_t := \mathsf{write}(t) \cup \mathsf{read}(t)}$

$$\mathbf{S}_1[U_1], \mathbf{S}_2[U_2], \ldots, \mathbf{S}_T[U_T]$$

for some sets $U_1, U_2, \ldots, U_T$. Need $|U_i| = O(L)$ for efficiency

Improving Efficiency (2/2)

before:

$\tilde{\mathbf{C}}_{t-1}[\overline{\mathsf{write}(t)}]$

dual-to-dual recoding

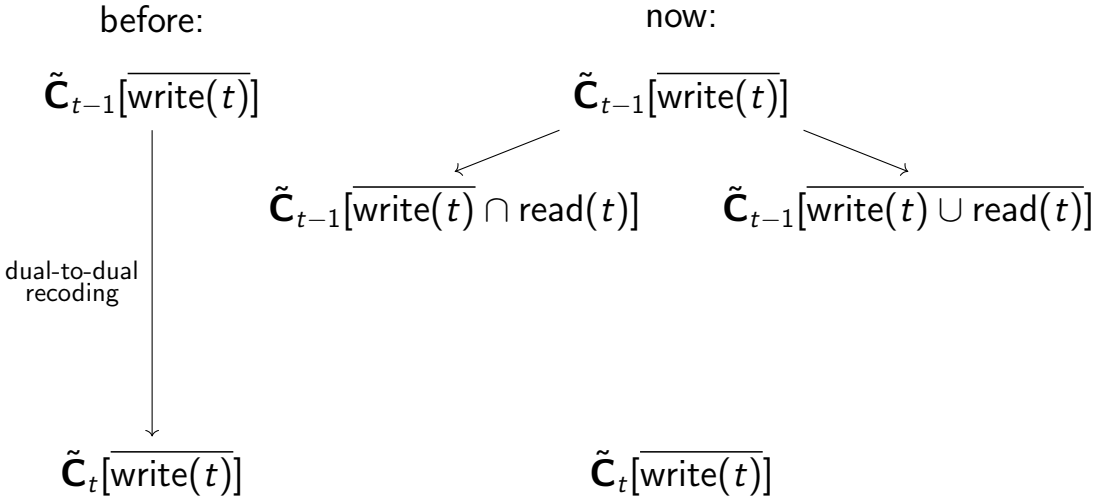
$\tilde{\mathbf{C}}_{t}[\overline{\mathsf{write}(t)}]$

now:

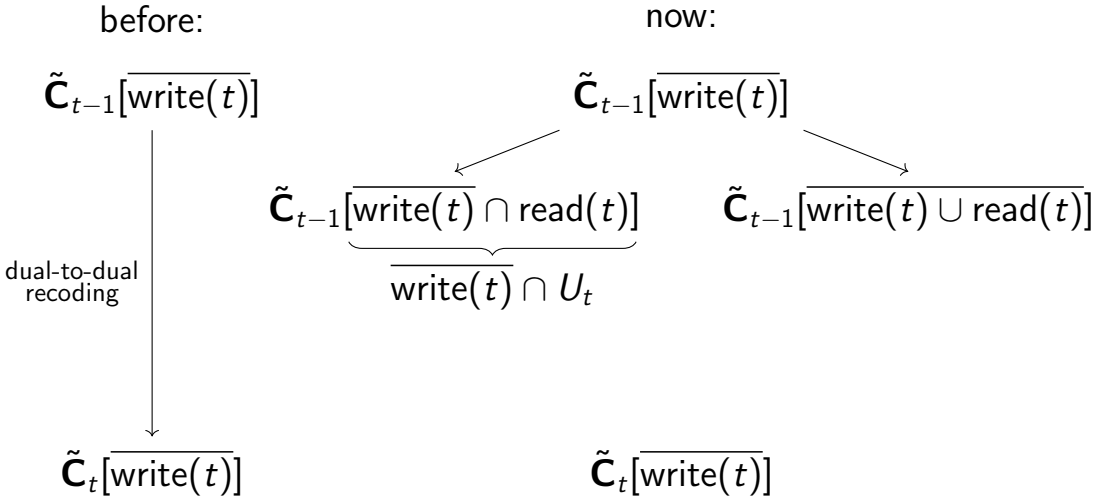
$\tilde{\mathbf{C}}_{t-1}[\overline{\mathsf{write}(t)}]$

$\tilde{\mathbf{C}}_{t}[\overline{\mathsf{write}(t)}]$

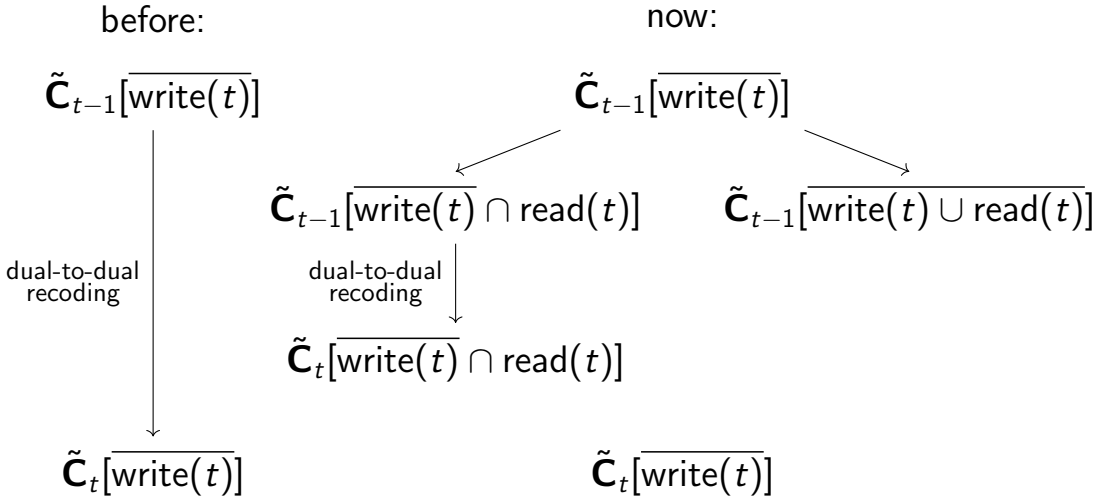
Improving Efficiency (2/2)



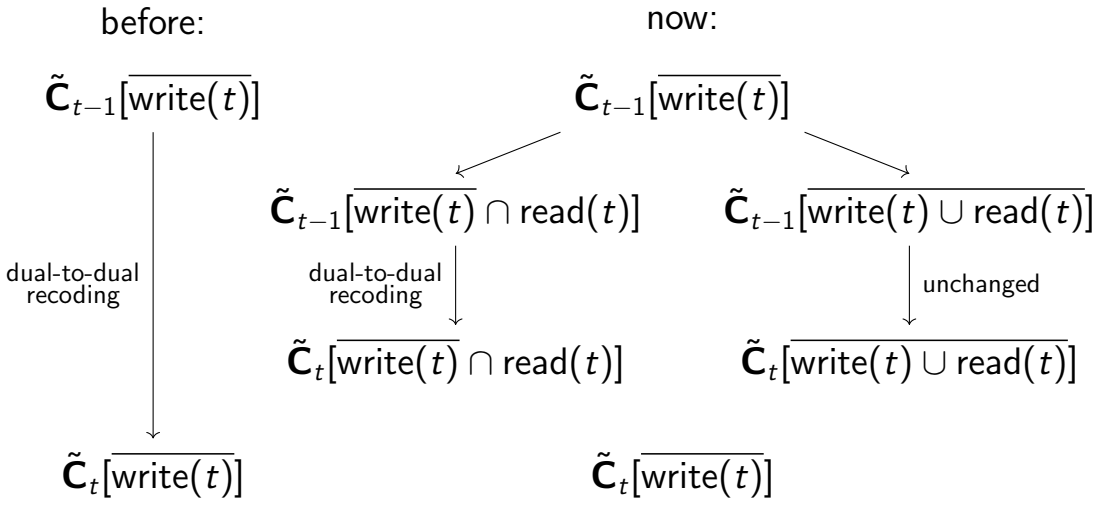
Improving Efficiency (2/2)



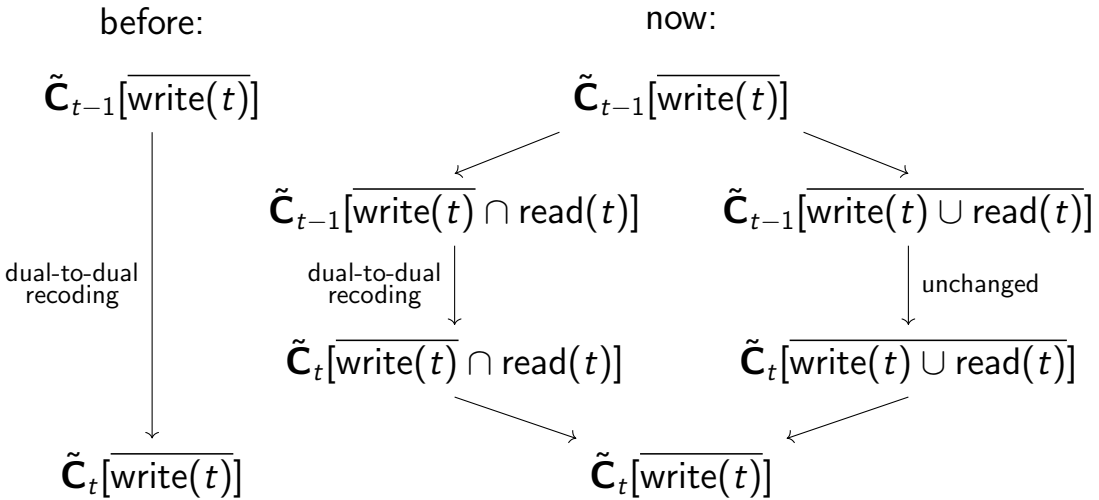
Improving Efficiency (2/2)



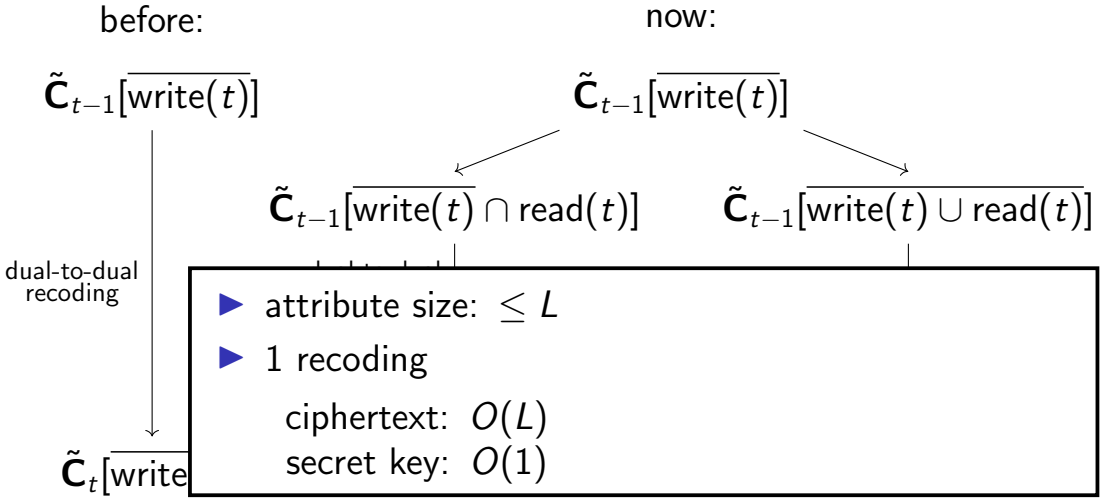
Improving Efficiency (2/2)



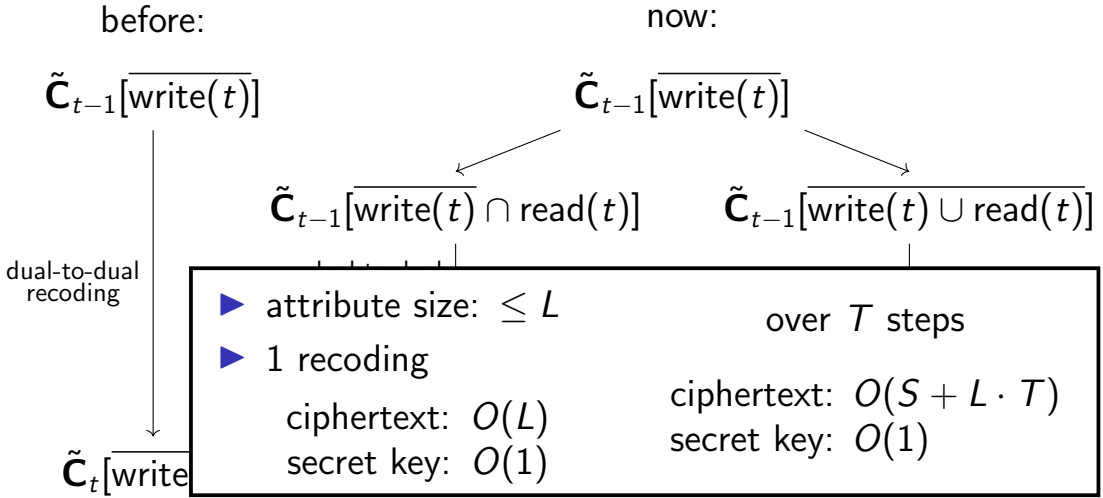
Improving Efficiency (2/2)



Improving Efficiency (2/2)



Improving Efficiency (2/2)



Security

- security under evasive LWE?

Security

- security under evasive LWE?

need to show that all the intermediate quantities computed during decryption are jointly pseudorandom

Security

- security under evasive LWE?

need to show that all the intermediate quantities computed during decryption are jointly pseudorandom

$\Uparrow$

LWE

Security

- security under evasive LWE?

need to show that all the intermediate quantities computed during decryption are jointly pseudorandom

$\Uparrow$

LWE

What about noise-growth?

Security

- security under evasive LWE?

need to show that all the intermediate quantities computed during decryption are jointly pseudorandom

$\Uparrow$ LWE

What about noise-growth?

$\Downarrow$

techniques from [HseihLinLuo23]
to handle unbounded depth computation

Security

- security under evasive LWE?

need to show that all the intermediate quantities computed during decryption are jointly pseudorandom

$\Uparrow$ LWE

What about noise-growth?

$\Downarrow$

techniques from [HseihLinLuo23] to handle unbounded depth computation

$\Downarrow$

need to use their circular-secure variant of evasive LWE

Security

- security under evasive LWE?

need to show that all the intermediate quantities computed during decryption are jointly pseudorandom

$\Uparrow$ LWE

What about noise-growth?

$\Downarrow$

techniques from [HseihLinLuo23] to handle unbounded depth computation

$\Downarrow$

need to use their circular-secure variant of evasive LWE

- construction gets modified accordingly

(need to add circular encryptions)

Conclusion

- New Encoding and Recoding Techniques

Conclusion

- New Encoding and Recoding Techniques
- New ABE for Turing Machines with better efficiency

Conclusion

- New Encoding and Recoding Techniques
- New ABE for Turing Machines with better efficiency
- Improving assumption? [AgrawalModiYadavYamada25]

Conclusion

- New Encoding and Recoding Techniques
- New ABE for Turing Machines with better efficiency
- Improving assumption? [AgrawalModiYadavYamada25]
- Other applications?

Conclusion

- New Encoding and Recoding Techniques
- New ABE for Turing Machines with better efficiency
- Improving assumption? [AgrawalModiYadavYamada25]
- Other applications?

Thank you!