Almost Optimal KP and CP-ABE for Circuits from Succinct LWE

Hoeteck Wee, NTT Research

In memory of Luca Trevisan (1971–2024)

Abstract. We present almost-optimal lattice-based attribute-based encryption (ABE) and laconic function evaluation (LFE). For depth d circuits over ℓ-bit inputs, we obtain

- key-policy and ciphertext-policy ABE schemes with ciphertext, secret key and public key size $O(1)$;
- LFE with ciphertext size $\ell + O(1)$ as well as CRS and digest size $O(1)$;

where $O(\cdot)$ hides $\mathsf{poly}(d, \lambda)$ factors. Our parameter sizes are *optimal*, up to the $\mathsf{poly}(d)$ dependencies. The security of our schemes rely on succinct LWE (Wee, CRYPTO 2024). Our results constitute a substantial improvement over the state of the art; none of our results were known even under the stronger evasive LWE assumption.

1 Introduction

In this work, we study attribute-based encryption [26,19] and laconic function evaluation [25,12], two fundamental primitives in the study of computing on encrypted data:

- Attribute-based encryption (ABE) [26,19] is a generalization of public-key encryption to support fine-grained access control for encrypted data. Here, ciphertexts and keys are associated with descriptive values which determine whether decryption is possible. In a key-policy ABE (KP-ABE) scheme, ciphertexts ct_x are associated with an attribute $x \in \{0,1\}^\ell$ and a message μ and keys sk_f with a predicate f, and decryption returns μ when x satisfies f (i.e, $f(x) = 0$). A ciphertext-policy (CP-ABE) scheme is the dual of KP-ABE with ciphertexts associated with predicates f and keys with attributes x.
- In laconic function evaluation (LFE), a server publishes a short digest dig to a function f. Anyone can use dig to efficiently encrypt an input $x \in \{0,1\}^\ell$. Given f, the ciphertext ct can then be decrypted to recover $f(x)$, but hides everything else about x.

1.1 Our Results

In this work, we present almost-optimal lattice-based ABE and LFE schemes for circuits. For depth d circuits over ℓ-bit inputs where ℓ and d are fixed at set-up, we construct

- a KP-ABE and a CP-ABE with parameters:

$$|\mathsf{mpk}| = O(1), \quad |\mathsf{ct}| = O(1), \quad |\mathsf{sk}| = O(1);$$

  both of which satisfy selective security against unbounded collusions;
- a LFE with parameters:

$$|\mathsf{crs}| = O(1), \quad |\mathsf{ct}| = \ell + O(1), \quad |\mathsf{dig}| = O(1),$$
$$\text{encryption time } O(\ell)$$

where $O(\cdot)$ hides $\mathsf{poly}(d, \lambda)$ factors. Our parameter sizes are *optimal*, up to the $\mathsf{poly}(d)$ dependencies[1]. The security of our schemes rely on the succinct LWE assumption [28], a simple, falsifiable assumption implied by evasive LWE. As an immediate corollary of our CP-ABE, we also obtain an optimal broadcast encryption scheme for N users with parameter size $\mathsf{poly}(\log N)$ based on succinct LWE.

[1] For the subclass of NC^1 circuits, we can bound $d = O(\log \ell) \le \lambda$, the $\mathsf{poly}(d)$ factors are subsumed by the $\mathsf{poly}(\lambda)$ factors.

KP-ABE	$\|\mathsf{mpk}\|$	$\|\mathsf{ct}\|$	$\|\mathsf{sk}\|$	**Assumption**
GVW13 [17]	$O(\ell)$	$O(\ell)$	$O(s)$	LWE
BGGHNSVV14 [6]	$O(\ell)$	$O(\ell)$	$O(1)$	LWE
BV16 [9]	$O(1)$	$O(\ell)$	$\ell + O(1)$	LWE
CW23 [13]	$O(\ell)$	$O(\ell)$	$O(1)^\dagger$	LWE
HLL23 [20]	$O(\ell)^\dagger$	$O(\ell)^\dagger$	$O(1)^\dagger$	evasive + circular LWE $\times$
W24 [28]	$O(\ell^2)$	$O(1)$	$O(1)$	ℓ-succinct LWE
W24 [28]	$O(\ell^{2/3})$	$O(\ell^{2/3})$	$O(1)$	$\ell^{1/3}$-succinct LWE
this work	$O(1)$	$O(1)$	$O(1)$	$\mathsf{poly}(d,\lambda)$-succinct LWE

CP-ABE	$\|\mathsf{mpk}\|$	$\|\mathsf{ct}\|$	$\|\mathsf{sk}\|$	**Assumption**
BV22 [10]	$O(\ell)$	$O(\ell)$	$O(\ell)$	heuristic $\times$
W22 [27]	$O(\ell)$	$O(1)$	$O(\ell)$	evasive LWE + tensor LWE $\times$
HLL24 [21]	$O(\ell)$	$O(1)$	$O(\ell)$	evasive LWE (structured) $\times$
AKY24 [3]	$O(\ell)^\dagger$	$O(1)^\dagger$	$O(\ell)^\dagger$	circular evasive + tensor LWE $\times$
this work	$O(1)$	$O(1)$	$O(1)$	$\mathsf{poly}(d,\lambda)$-succinct LWE

LFE	$\|\mathsf{crs}\|$	$\|\mathsf{ct}\|$	$\|\mathsf{dig}\|$	**Assumption**
QWW18 [25]	$O(\ell)$	$O(\ell)$	$O(1)$	LWE
HLL23 [20]	$O(\ell)^\dagger$	$O(\ell)^\dagger$	$O(1)^\dagger$	circular LWE
W24 [28]	$O(\ell^2)$	$\ell + O(1)$	$O(1)$	ℓ-succinct LWE
W24 [28]	$O(\ell^{2/3})$	$\ell + O(\ell^{2/3})$	$O(1)$	$\ell^{1/3}$-succinct LWE
this work	$O(1)$	$\ell + O(1)$	$O(1)$	$\mathsf{poly}(d,\lambda)$-succinct LWE

Fig. 1. Comparison with prior lattice-based ABE and LFE for circuits of size s and depth d. Here, $O(\cdot)$ hides $\mathsf{poly}(d,\lambda)$ factors, whereas $O(\cdot)^\dagger$ hides $\mathsf{poly}(\lambda)$ factors; when restricted to NC^1, the $\mathsf{poly}(d)$ factors can be omitted. For ABE, the quantities $|\mathsf{ct}|, |\mathsf{sk}|$ refer to the cryptographic overhead beyond transmitting x and f in the clear. A $\times$ indicates a non-falsifiable assumption. The ABE schemes marked $\times$ only achieve very selective security, whereas all the other ABE schemes, including ours, achieve standard selective security.

Comparison with prior works. Our results constitute a substantial improvement over the state of the art:

- Our KP-ABE and LFE schemes improve on the recent work of Wee [28] in two ways: (i) we reduce the $\mathsf{mpk}, \mathsf{crs}$ sizes from $O(\ell^2)$ to $O(1)$; (ii) we rely on quantitatively weaker assumptions, namely $\mathsf{poly}(d,\lambda)$-succinct LWE instead of ℓ-succinct LWE.
- Our CP-ABE scheme improve on the works of Wee [27] as well as Hsieh, Lin and Luo [21] in three ways: (i) we reduce $|\mathsf{mpk}|, |\mathsf{sk}|$ from $O(\ell)$ to $O(1)$; (ii) we rely a weaker and simple, falsifiable assumption, and (iii) we achieve standard selective security as opposed to very selective security.
- We stress that none of these results were known even under the stronger evasive LWE assumption, nor did we have *heuristic* lattice-based candidates for almost-optimal KP-ABE, CP-ABE or LFE (except via lattice-based iO candidates).

We refer to Fig 1 for additional comparison with prior works.

1.2 Technical Overview

We proceed directly to a technical overview of our constructions, which are remarkably quite simple, conceptually.

ℓ-succinct LWE [28]. Fix LWE parameters $n, q, m = O(n \log q)$. Sample $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{W} \in \mathbb{Z}_q^{\ell n \times m}$ along with a random Gaussian $\mathbf{T} \in \mathbb{Z}^{(\ell+1)m \times \ell m}$ such that $[\mathbf{I}_\ell \otimes \mathbf{B} \mid \mathbf{W}] \cdot \mathbf{T} = \mathbf{I}_\ell \otimes \mathbf{G}$. The ℓ-succinct LWE assumption stipulates that

$$(\mathbf{B}, \mathbf{sB} + \mathbf{e}, \mathbf{W}, \mathbf{T}) \approx_c (\mathbf{B}, \mathbf{c}, \mathbf{W}, \mathbf{T})$$

where $\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \mathscr{D}_{\mathbb{Z},\chi}^m, \mathbf{c} \leftarrow \mathbb{Z}_q^m$. We write $\mathsf{pp}_\ell := (\mathbf{B}, \mathbf{W}, \mathbf{T})$, which has size $O(\ell^2)$. Note that 1-succinct LWE is equivalent to LWE, and the assumption becomes stronger as ℓ increases.

The Wee24 KP-ABE and LFE. The starting point of our work are the Wee24 [28] KP-ABE and LFE schemes based on ℓ-succinct LWE, with almost-optimal ciphertext and key / digest sizes, but $O(\ell^2)$ public key / CRS sizes. Our goal would be to reduce public key / CRS sizes to $O(1)$, and the assumption to $O(1)$-succinct LWE. At the heart of Wee24 KP-ABE and LFE is a new succinct commitment scheme for vectors in $\{0,1\}^\ell$ with the following properties:

- given pp and $\mathbf{x} \in \{0,1\}^\ell$, we can derive a commitment $\mathbf{C}_\mathbf{x} \in \mathbb{Z}_q^{n \times m}$ and an opening $\mathbf{Z}_\mathbf{x} \in \mathbb{Z}_q^{m \times \ell m}$ such that $\|\mathbf{Z}_\mathbf{x}\|$ is small;
- given $\mathsf{pp}, 1^\ell$, we can derive a verification matrix $\mathbf{V}_\ell \in \mathbb{Z}_q^{m \times \ell m}$ such that $\|\mathbf{V}_\ell\|$ is small;
- the commitment and opening satisfy

$$\mathbf{C}_\mathbf{x} \cdot \mathbf{V}_\ell = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_\mathbf{x} \tag{1}$$

In the Wee24 scheme, $\mathsf{pp} = \mathsf{pp}_\ell$, hence the $|\mathsf{pp}_\ell| = O(\ell^2)$ public key / CRS size. The security proof relies on $(\mathbf{B}, \mathbf{sB} + \mathbf{e})$ being pseudorandom given pp, which corresponds exactly to ℓ-succinct LWE when $\mathsf{pp} = \mathsf{pp}_\ell$. Looking ahead, we will crucially leverage the structure in (1); on the other hand, the details of how $\mathbf{C}_\mathbf{x}, \mathbf{Z}_\mathbf{x}, \mathbf{V}_\ell$ are computed are not relevant to our constructions.

A new succinct commitment scheme. In this work, we present a new succinct commitment scheme for vectors in $\{0,1\}^\ell$ satisfying the above requirements, with $\mathsf{pp} := \mathsf{pp}_{2m^2}$, independent of of ℓ. Plugging this scheme into the Wee24 framework immediately yields KP-ABE and LFE schemes with public key / CRS of size $\mathsf{poly}(m)$, with security based on $2m^2$-succinct LWE. Here, $m = \mathsf{poly}(d, \lambda) \ll \ell$.

To build our new commitment scheme for vectors $\mathbf{x} \in \{0,1\}^\ell$, we start with the a-priori seemingly harder goal of building a commitment scheme for matrices $\mathbf{M} \in \mathbb{Z}_q^{n \times L}$ with the following properties:

- given pp_{2m^2} and $\mathbf{M} \in \mathbb{Z}_q^{n \times L}$, we can derive a commitment $\mathbf{C} \in \mathbb{Z}_q^{n \times m}$ and an opening $\mathbf{Z} \in \mathbb{Z}_q^{m \times L}$ such that $\|\mathbf{Z}\|$ is small;
- given $\mathsf{pp}, 1^L$, we can derive a verification matrix $\mathbf{V}_L^{\mathsf{mx}} \in \mathbb{Z}_q^{m \times L}$ such that $\|\mathbf{V}_L^{\mathsf{mx}}\|$ is small;
- the commitment and opening satisfy

$$\mathbf{C} \cdot \mathbf{V}_L^{\mathsf{mx}} = \mathbf{M} - \mathbf{B} \cdot \mathbf{Z} \tag{2}$$

Given the latter, we obtain the former by committing to the matrix $\mathbf{x} \otimes \mathbf{G} \in \mathbb{Z}_q^{n \times \ell m}$. The advantage of committing to matrices is that we can recurse by committing to commitments!

Warm-up: $L = 2m$. The commitment to $\mathbf{M} \in \mathbb{Z}_q^{n \times 2m}$ would simply be the Wee24 commitment $\mathbf{C}$ to the bit-decomposition of $\mathbf{M}$ as a row vector, which we denote by $\mathsf{bits}(\mathbf{M}) \in \{0,1\}^{2m^2}$. In particular, we can compute, given pp_{2m^2}, an opening $\mathbf{Z}$ and a verification matrix $\mathbf{V}_{2m^2}$ satisfying:

$$\mathbf{C} \cdot \mathbf{V}_{2m^2} = \mathsf{bits}(\mathbf{M}) \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}$$

Applying the compactification "trick" of [8], we have $(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}) \cdot (\mathbf{I}_{2m} \otimes \mathsf{vec}(\mathbf{I}_m)) = \mathbf{M}$, and voilà,

$$\mathbf{C} \cdot \overbrace{\mathbf{V}_{2m^2}(\mathbf{I}_{2m} \otimes \mathsf{vec}(\mathbf{I}_m))}^{\mathbf{V}_{2m}^{\mathsf{mx}}} = \mathbf{M} - \mathbf{B} \cdot \overbrace{\mathbf{Z}(\mathbf{I}_{2m} \otimes \mathsf{vec}(\mathbf{I}_m))}^{\text{opening}}$$

From $L = 2m$ to $L = 4m$. Next, we show how to "bootstrap" from $2m$ to $4m$. We parse $\mathbf{M} \in \mathbb{Z}_q^{n\times 4m}$ as $[\mathbf{M}_0 \mid \mathbf{M}_1]$ where $\mathbf{M}_0, \mathbf{M}_1 \in \mathbb{Z}_q^{n\times 2m}$. We start by computing commitments $\mathbf{C}_0, \mathbf{C}_1 \in \mathbb{Z}_q^{n\times m}$ to $\mathbf{M}_0, \mathbf{M}_1$ along with openings $\mathbf{Z}_0, \mathbf{Z}_1$ satisfying

$$\mathbf{C}_\beta \cdot \mathbf{V}_{2m}^{\mathsf{mx}} = \mathbf{M}_\beta - \mathbf{B}\cdot\mathbf{Z}_\beta, \quad \beta \in \{0,1\}$$

Then $[\mathbf{C}_0 \mid \mathbf{C}_1] \in \mathbb{Z}_q^{n\times 2m}$ satisfies

$$[\mathbf{C}_0 \mid \mathbf{C}_1] \cdot (\mathbf{I}_2 \otimes \mathbf{V}_{2m}^{\mathsf{mx}}) = [\mathbf{M}_0 \mid \mathbf{M}_1] - \mathbf{B}\cdot[\mathbf{Z}_0 \mid \mathbf{Z}_1] \tag{3}$$

This almost satisfies our requirement for a commitment to $[\mathbf{M}_0 \mid \mathbf{M}_1]$, except $[\mathbf{C}_0 \mid \mathbf{C}_1]$ has width $2m$ instead of m. Now, we simply compute a commitment $\mathbf{C} \in \mathbb{Z}_q^{n\times m}$ to $[\mathbf{C}_0 \mid \mathbf{C}_1] \in \mathbb{Z}_q^{n\times 2m}$ along with an opening $\mathbf{Z}'$ satisfying

$$\mathbf{C}\cdot\mathbf{V}_{2m}^{\mathsf{mx}} = [\mathbf{C}_0 \mid \mathbf{C}_1] - \mathbf{B}\cdot\mathbf{Z}'$$

Multiplying both sides of the preceding equation by $\mathbf{I}_2 \otimes \mathbf{V}_{2m}^{\mathsf{mx}}$ and adding to (3) yields

$$\mathbf{C}' \cdot \overbrace{\mathbf{V}_{2m}^{\mathsf{mx}}(\mathbf{I}_2 \otimes \mathbf{V}_{2m}^{\mathsf{mx}})}^{\mathbf{V}_{4m}^{\mathsf{mx}}} = [\mathbf{M}_0 \mid \mathbf{M}_1] - \mathbf{B}\cdot\Big(\overbrace{\mathbf{Z}'(\mathbf{I}_2 \otimes \mathbf{V}_{2m}^{\mathsf{mx}}) + [\mathbf{Z}_0 \mid \mathbf{Z}_1]}^{\mathbf{Z}'}\Big)$$

That is, $\mathbf{C} \in \mathbb{Z}_q^{n\times m}$ constitutes a commitment to $\mathbf{M} \in \mathbb{Z}_q^{n\times 4m}$ with opening $\mathbf{Z}'$; moreover, $\mathbf{V}_{4m}^{\mathsf{mx}}, \mathbf{Z}'$ are also low-norm.

Arbitrary L. At this point, it should be clear that we can keep recursing to support arbitrary L with a norm blow-up that is exponential in $\log L$. Later on, we show how to reduce this blow-up to a multiplicative factor in $\log L$. An intriguing corollary of this construction is that $2m^2$-succinct LWE implies hardness of L-succinct LWE, for an arbitrary L; see Remark 1.

Commitment to circuits. As a stepping stone towards our CP-ABE[2], we construct a commitment scheme for depth d circuits over ℓ-bit inputs that supports opening to an evaluation $f(x)$. That is,

- given pp_{2m^2} and a circuit f, we can derive a commitment $\mathbf{C}_f \in \mathbb{Z}_q^{n\times m}$;
- given pp_{2m^2}, a circuit f and an input $x \in \{0,1\}^\ell$, we can derive an opening $\mathbf{Z}_{f,x} \in \mathbb{Z}_q^{m\times m}$ such that $\|\mathbf{Z}_{f,x}\| = m^{O(d)}$;
- given $\mathsf{pp}_{2m^2}, x, 1^d$, we can derive a verification matrix $\mathbf{V}_{x,d} \in \mathbb{Z}_q^{m\times m}$ such that $\|\mathbf{V}_{x,d}\| = m^{O(1)}$;
- the three matrices satisfy

$$\mathbf{C}_f \cdot \mathbf{V}_{x,d} = f(x)\mathbf{G} - \mathbf{B}\cdot\mathbf{Z}_{f,x}$$

This essentially constitutes a non-interactive functional commitment scheme for circuits [7,23], although none of the lattice-based schemes in the literature [**?**,30] satisfies the above algebraic verification relation (cf. Remark 2). Looking ahead, $\mathbf{C}_f$ shows up in our CP-ABE ciphertext, and $\mathbf{V}_{x,d}$ shows up in our CP-ABE secret keys.

To construct such a commitment scheme, it suffices to handle input gates, addition gates, and multiplication gates. Input gates (or, circuits of depth 0) essentially correspond to linear (affine) functions, and can be realized using our vector commitment combined with simple linear homomorphism. The main challenge lies in handling multiplication gates, and more simply, homomorphic multiplication of scalars x_0, x_1 instead of functions f_0, f_1. Namely, given commitments $\mathbf{C}_0, \mathbf{C}_1 \in \mathbb{Z}_q^{n\times m}$ to $x_0, x_1 \in \{0,1\}$ along with openings $\mathbf{Z}_0, \mathbf{Z}_1$ satisfying $\mathbf{C}_\beta \cdot \mathbf{V} = x_\beta\mathbf{G} - \mathbf{B}\cdot\mathbf{Z}_\beta$, we want to derive a commitment $\hat{\mathbf{C}} \in \mathbb{Z}_q^{n\times m}$ to x_0x_1 along an opening that satisfies an analogous verification relation.[3] In prior works [6,15,18], homomorphically multiplying $\mathbf{C}_0, \mathbf{C}_1$ simply yields $\mathbf{C}_0\mathbf{G}^{-1}(\mathbf{C}_1)$. Here, we have to do more work.

First, we homomorphically multiply $\mathbf{C}_0\mathbf{V}, \mathbf{C}_1\mathbf{V}$ to obtain:

$$\mathbf{C}_0\mathbf{V}\cdot\mathbf{G}^{-1}(\mathbf{C}_1\mathbf{V}) = x_0x_1\mathbf{G} - \mathbf{B}\cdot\big(\mathbf{Z}_0\cdot\mathbf{G}^{-1}(\mathbf{C}_1\mathbf{V}) + x_0\mathbf{Z}_1\big) \tag{4}$$

The RHS matches what we need, but the LHS is not of the form $\hat{\mathbf{C}}\cdot\hat{\mathbf{V}}$. To fix the latter issue, we make two simple observations:

[2] Our KP-ABE yields a non-trivial CP-ABE via universal circuits. However, in the ensuing CP-ABE, key generation requires an a-priori bound s on circuit size and runs in time $O(s)$. We show how to avoid this restriction and also achieve $O(\ell)$-time key generation.

[3] The same idea would allow us to start with $\mathbf{C}_\beta, \mathbf{Z}_\beta$ satisfying $\mathbf{C}_\beta\cdot\mathbf{V}_{x,d} = f_\beta(x)\mathbf{G} - \mathbf{B}\cdot\mathbf{Z}_\beta$ and derive $\hat{\mathbf{C}}$ that opens to $f_0(x)f_1(x)$.

– We replace $\mathbf{G}^{-1}(\mathbf{C}_1\mathbf{V})$ in (4) with $\mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V}$ to obtain

$$\mathbf{C}_0\mathbf{V}\cdot\mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V} = x_0x_1\mathbf{G} - \mathbf{B}\cdot\Big(\overbrace{\mathbf{Z}_0\cdot\mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V} + x_0\mathbf{Z}_1}^{:=\mathbf{Z}'}\Big)$$

– We can rewrite $\mathbf{C}_0\mathbf{V}\cdot\mathbf{G}^{-1}(\mathbf{C}_1)\cdot\mathbf{V}$ –by switching the order of $\mathbf{V}\cdot\mathbf{G}^{-1}(\mathbf{C}_1)$ using tensor products– as the following product

$$\overbrace{(\mathsf{bits}(\mathbf{C}_1)\otimes\mathbf{C}_0)}^{:=\mathbf{C}^\times}\cdot\overbrace{(\mathbf{I}_m\otimes\mathrm{vec}(\mathbf{V}))\mathbf{V}}^{:=\mathbf{V}^\times}$$

This is almost what we need, except $\mathbf{C}^\times\in\mathbb{Z}_q^{n\times m^3}$ has width m^3 instead of m. As before, we compute a commitment $\hat{\mathbf{C}}\in\mathbb{Z}_q^{n\times m}$ to the matrix $\mathbf{C}^\times$ (using our earlier scheme with $L=m^3$), along with an opening $\mathbf{Z}^\times$ satisfying

$$\hat{\mathbf{C}}\cdot\mathbf{V}_{m^3}^{\mathsf{mx}} = \mathbf{C}^\times - \mathbf{B}\cdot\mathbf{Z}^\times \tag{5}$$

Multiplying both sides on the right by $\mathbf{V}^\times$ and combining with $\mathbf{C}^\times\mathbf{V}^\times = x_0x_1\mathbf{G} - \mathbf{B}\mathbf{Z}'$ yields

$$\hat{\mathbf{C}}\cdot\mathbf{V}_{m^3}^{\mathsf{mx}}\mathbf{V}^\times = x_0x_1\mathbf{G} - \mathbf{B}\cdot(\mathbf{Z}^\times\mathbf{V}^\times + \mathbf{Z}')$$

That is, $\hat{\mathbf{C}}$ is a commitment to x_0x_1 with opening $\mathbf{Z}^\times\mathbf{V}^\times + \mathbf{Z}_0\cdot\mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V} + x_0\mathbf{Z}_1$ and verification matrix $\mathbf{V}_{m^3}^{\mathsf{mx}}\mathbf{V}^\times$.

Reducing norm blow-up. Our construction for circuits so far incur a norm blow-up (in the opening) that is doubly-exponential in circuit depth d, whereas we would like a norm blow-up that is singly-exponential in d. To achieve this, we would compute a commitment $\hat{\mathbf{C}}$ to $\mathbf{C}^\times\mathbf{G}_{m^3}$ instead of $\mathbf{C}^\times$. This means that in the RHS of (5), we have $\mathbf{C}^\times\mathbf{G}_{m^3}$ instead of $\mathbf{C}^\times$, and in the next step, we would multiply both sides on the right by $\mathbf{G}_{m^3}^{-1}(\mathbf{V}^\times)$ instead of $\mathbf{V}^\times$. This means that with each additional multiplication, the norm of the openings and the verification matrix increases multiplicatively by fixed $\mathsf{poly}(\|\mathbf{T}\|, m)$ and $\mathsf{poly}(m)$ factors respectively, instead of squaring. This in turn yields a norm blow-up that is singly-exponential in circuit depth.

Our CP-ABE. Our CP-ABE scheme for depth d circuits over ℓ-bit inputs is as follows, omitting error terms in the ciphertext:

$$\begin{aligned}
\mathsf{mpk} &= \overbrace{\mathbf{B},\mathbf{W},\mathbf{T}}^{\mathsf{pp}_{2m^2}},\ \mathbf{B}_1\leftarrow\mathbb{Z}_q^{n\times m}, \mathbf{p}\leftarrow\mathbb{Z}_q^n\\
\mathsf{ct}_f &= \mathbf{s}\mathbf{B}, \mathbf{s}(\mathbf{B}_1+\mathbf{C}_f), \mathbf{s}\cdot\mathbf{p}^\top + \mu\cdot\lfloor\tfrac{q}{2}\rfloor\\
\mathsf{sk}_x &= \mathbf{k}_x^\top \text{ s.t. } [\mathbf{B}\mid\mathbf{A}_x]\cdot\mathbf{k}_x^\top = \mathbf{p}^\top,\quad \mathbf{A}_x := -\mathbf{B}_1\mathbf{V}_{x,d}
\end{aligned}$$

where $\mathbf{C}_f, \mathbf{V}_{x,d}$ are computed using our commitment scheme for circuits. We will set the LWE parameters so that $m = \mathsf{poly}(d,\lambda)$, which yields $|\mathsf{mpk}|, |\mathsf{ct}_f|, |\mathsf{sk}_x| = \mathsf{poly}(d,\lambda)$. Combining $\mathbf{C}_f\mathbf{V}_{x,d} = f(x)\mathbf{G} - \mathbf{B}\mathbf{Z}_{f,x}$ and $\mathbf{A}_x = -\mathbf{B}_1\mathbf{V}_{x,d}$, we have:

$$[\mathbf{B}\mid\mathbf{B}_1+\mathbf{C}_f]\cdot\begin{pmatrix}-\mathbf{Z}_{f,x}\\ -\mathbf{V}_{x,d}\end{pmatrix} = \mathbf{A}_x - f(x)\mathbf{G} \tag{6}$$

This means that starting from $\mathbf{s}(\mathbf{B}_1+\mathbf{C}_f)$, we can derive $\mathbf{s}\mathbf{A}_x$ whenever $f(x)=0$, which combined with $\mathbf{k}_x^\top$ allows us to recover $\mathbf{s}\cdot\mathbf{p}^\top$ and thus μ. The security reduction to $2m^2$-succinct LWE samples a low-norm $\mathbf{U}\leftarrow\{0,1\}^{m\times m}$ and programs $\mathbf{B}_1 := \mathbf{B}\mathbf{U} - \mathbf{C}_f$. This allows the reduction to simulate the challenge ciphertext. From (6), we have

$$\mathbf{A}_x = \mathbf{B}\cdot\overbrace{[\mathbf{I}\mid\mathbf{U}]\cdot\begin{pmatrix}-\mathbf{Z}_{f,x}\\ -\mathbf{V}_{x,d}\end{pmatrix}}^{\text{small}} + f(x)\mathbf{G}$$

This means the reduction has a trapdoor for the matrix $[\mathbf{B}\mid\mathbf{A}_x]$ since $f(x)\neq 0$, which it can then use to answer key queries.

1.3 Discussion

Additional related works. The work of [22] showed that assuming iO, we can get optimal ABE (and even FE) for circuits with $|\mathsf{mpk}|, |\mathsf{ct}|, |\mathsf{sk}| = \mathsf{poly}(\lambda)$. Combined with existing lattice-based iO candidates such as [11,29], this yields lattice-based candidates for optimal ABE for circuits. However, the ensuing constructions are extremely complex and relies heavily on non-black-box use of lattice algorithms. From a feasibility perspective, we do not know to construct almost-optimal ABE for circuits starting from witness encryption.

Several recent works [13,20,3] improved on the dependency on d in existing ABE and LFE schemes, replacing several $\mathsf{poly}(d,\lambda)$ factors with $\mathsf{poly}(\lambda)$ factors; these improvements are orthogonal to the ones in this work, which focuses on the dependency on ℓ, and rely on completely different and largely complementary techniques. In particular, for NC^1 circuits, these works do not provide any improvements over prior works, whereas we do. It is straight-forward to see that we can combine the techniques in HLL23 [20] with our schemes to obtain candidate optimal KP-ABE and LFE schemes with $\mathsf{poly}(\lambda)$ instead of $\mathsf{poly}(d,\lambda)$ dependencies: simply append a "circular encoding" of the LWE secret $\mathbf{s}$ to the ciphertext, and upon expanding to $\mathbf{s}(\mathbf{A}-\mathbf{x}\otimes\mathbf{G})$, apply HLL23 homomorphic evaluation on unbounded-depth circuits. The question remains: what can we prove about the ensuing schemes? In the case of LFE, it seems quite plausible that the ensuing scheme is secure under a circular small-secret variant of the succinct LWE assumption. In the case of KP-ABE, one can hope to show that the ensuing scheme is secure under the (public-coin) circular evasive LWE assumption.

Concurrent and follow-up works. We mention two concurrent works with related results:

- Agrawal, Kumari and Yamada [4] constructed optimal KP-ABE and CP-ABE for circuits with $|\mathsf{mpk}|, |\mathsf{ct}|, |\mathsf{sk}| = \mathsf{poly}(\lambda)$, under a (variant) of the evasive LWE assumption. In particular, their schemes achieve better parameters than we do under stronger assumptions.
- Abram, Malavolta and Roy [2] constructed LFE for circuits with ciphertext size $\ell + d\cdot\mathsf{poly}(\lambda)$ as well as CRS and digest size $\mathsf{poly}(\lambda)$ under the LWE assumption. That is, they achieve better parameters than we do under weaker assumptions.

In a follow-up work, Abram, Malavolta and Roy [1] introduced the decomposed LWE assumption, which is a weaker variant of succinct LWE that does not refer to trapdoors. Their main results are new succinct randomized encodings, LFE and KP-ABE for RAM programs, assuming the decomposed LWE assumption (and strengthenings there-of). In particular, their results also imply an almost optimal KP-ABE for circuits with $|\mathsf{mpk}|, |\mathsf{ct}|, |\mathsf{sk}| = \mathsf{poly}(d,\lambda)$ under the decomposed LWE assumption. In Appendix C, we present an alternative derivation of the latter result, as well as CP-ABE for circuits with $|\mathsf{mpk}|, |\mathsf{ct}|, |\mathsf{sk}| = \mathsf{poly}(d,\lambda)$ under the decomposed LWE assumption.

2 Preliminaries

Notations. We use boldface lower case for row vectors (e.g. $\mathbf{v}$) and boldface upper case for matrices (e.g. $\mathbf{V}$). For integral vectors and matrices (i.e., those over $\mathbb{Z}$), we use the notation $|\mathbf{v}|, |\mathbf{V}|$ to denote the maximum absolute value over all the entries. We use $v \leftarrow \mathscr{D}$ to denote a random sample from a distribution $\mathscr{D}$, as well as $v \leftarrow S$ to denote a uniformly random sample from a set S. We use $\approx_s$ and $\approx_c$ as the abbreviation for statistically close and computationally indistinguishable.

Matrix operations. The tensor product (Kronecker product) for matrices $\mathbf{A} = (a_{i,j}) \in \mathbb{Z}^{\ell\times m}$, $\mathbf{B} \in \mathbb{Z}^{n\times p}$ is defined as

$$\mathbf{A}\otimes\mathbf{B} = \begin{bmatrix} a_{1,1}\mathbf{B}, & \ldots, & a_{1,m}\mathbf{B} \\ \ldots, & \ldots, & \ldots \\ a_{\ell,1}\mathbf{B}, & \ldots, & a_{\ell,m}\mathbf{B} \end{bmatrix} \in \mathbb{Z}^{\ell n\times mp}.$$

The mixed-product property for tensor product says that

$$(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D}) = (\mathbf{AC})\otimes(\mathbf{BD})$$

The vectorization of a matrix $\mathbf{A}$, denoted by $\mathrm{vec}(\mathbf{A})$, is the column vector obtained by stacking the columns of the matrix $\mathbf{A}$ on top of one another. We have the identity $\mathrm{vec}(\mathbf{ABC}) = (\mathbf{C}^\top\otimes\mathbf{A})\mathrm{vec}(\mathbf{B})$.

2.1 Lattices background

We use $\mathcal{D}_{\mathbb{Z},\chi}$ to denote the discrete Gaussian distribution over $\mathbb{Z}$ with standard deviation χ. We write $\mathbf{G}_L = \mathbf{I}_L \otimes \mathbf{g}$ to denote the gadget matrix [24] of height L, and $\mathbf{G} = \mathbf{G}_n$. We write $\mathbf{G}^{-1}(\cdot)$ to denote the standard deterministic entry-wise bit decomposition.

Learning with errors (LWE). Given $n, m, q, \chi \in \mathbb{N}$, the $\mathsf{LWE}_{n,m,q,\chi}$ assumption states that

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

where

$$\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\chi}, \mathbf{c} \leftarrow \mathbb{Z}_q^m$$

Trapdoor and preimage sampling [24,14]. Given any $\mathbf{Z} \in \mathbb{Z}_q^{n\times n'}$, $\sigma > 0$, we use $\mathbf{B}^{-1}(\mathbf{Z}, \sigma)$ to denote the distribution of a matrix $\mathbf{Y}$ sampled from $\mathcal{D}_{\mathbb{Z}^{m\times n'},\sigma}$ conditioned on $\mathbf{BY} = \mathbf{Z} \pmod q$. We sometimes suppress σ when the context is clear.

There is an efficient algorithm $\mathsf{TrapGen}(1^n, 1^m, q)$ that, given the modulus $q \geq 2$ and dimension n and $m \geq 2n\log q$, outputs $\mathbf{B} \approx_s U(\mathbb{Z}_q^{n\times 2n\log q})$ with a trapdoor $\mathbf{T}$ such that $\mathbf{BT} = \mathbf{G}$. Moreover, there is an efficient algorithm $\mathsf{SamplePre}(\mathbf{B}, \mathbf{T}, \mathbf{Z}, \sigma)$ that given $\mathbf{B}$ and any $\mathbf{T}$ such that $\mathbf{BT} = \mathbf{G}$, $\sigma \geq 2\sqrt{n\log q} \cdot |\mathbf{T}|$ and $\mathbf{Z} \in \mathbb{Z}_q^{n\times n'}$, outputs a sample from $\mathbf{B}^{-1}(\mathbf{Z}, \sigma)$. Note that given $\mathbf{B}, \mathbf{T}$ such that $\mathbf{BT} = \mathbf{G}$, we have $[\mathbf{B} \mid \mathbf{B}']\binom{\mathbf{T}}{\mathbf{0}} = \mathbf{G}$; we will sometimes abuse notation and write $\mathbf{T}$ as a trapdoor for $[\mathbf{B} \mid \mathbf{B}']$.

2.2 Homomorphic Computation on Matrices

Lemma 1 ($\mathsf{EvalF}, \mathsf{EvalFX}$ [6,15]). *Fix lattice parameters n, q and $m \geq 2n\log q$. Let $\mathcal{F}_{\ell,d,s}$ denote the family of functions $f : \{0,1\}^\ell \to \{0,1\}$ computable by circuits of depth d and size s. There exist a pair of efficient algorithms* ($\mathsf{EvalF}, \mathsf{EvalFX}$) *where*

- $\mathsf{EvalF}(\mathbf{A}, f) \to \mathbf{A}_f$*: On input a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times \ell m}$ and a function $f \in \mathcal{F}_{\ell,d,s}$, outputs a matrix $\mathbf{A}_f \in \mathbb{Z}_q^{n\times m}$;*
- $\mathsf{EvalFX}(\mathbf{A}, f, \mathbf{x}) \to \mathbf{H}_{\mathbf{A},f,\mathbf{x}}$*: On input a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times \ell m}$, a function $f \in \mathcal{F}_{\ell,d,s}$, and an input $\mathbf{x} \in \{0,1\}^\ell$, outputs a matrix $\mathbf{H}_{\mathbf{A},f,\mathbf{x}} \in \mathbb{Z}^{\ell m\times m}$.*

For all $\mathbf{A} \in \mathbb{Z}_q^{n\times \ell m}$, $f \in \mathcal{F}_{\ell,d,s}, \mathbf{x} \in \{0,1\}^\ell$, the matrices $\mathbf{A}_f \leftarrow \mathsf{EvalF}(\mathbf{A}, f)$ and $\mathbf{H}_{\mathbf{A},f,\mathbf{x}} \leftarrow \mathsf{EvalFX}(\mathbf{A}, f, \mathbf{x})$ satisfy

$$\begin{aligned}(\mathbf{A} - \mathbf{x}\otimes\mathbf{G}) \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} &= \mathbf{A}_f - f(\mathbf{x})\mathbf{G} \\ |\mathbf{H}_{\mathbf{A},f,\mathbf{x}}| &= m^{O(d)} \cdot s\end{aligned} \tag{7}$$

2.3 ℓ-Succinct Lattice Assumptions

Assumption 1 (ℓ-succinct LWE [28]) *Fix security parameter λ and LWE parameters n, m, q, χ where $m \geq 2n\log q$. The (ℓ, σ)-succinct LWE assumption stipulates that*

$$(\mathbf{B}, \mathbf{sB} + \mathbf{e}, \mathbf{W}, \mathbf{T}) \approx_c (\mathbf{B}, \mathbf{c}, \mathbf{W}, \mathbf{T})$$

where

$$\begin{aligned}&\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z},\chi}^m, \mathbf{c} \leftarrow \mathbb{Z}_q^m \\ &\mathbf{W} \leftarrow \mathbb{Z}_q^{\ell n\times m}, \mathbf{T} \leftarrow [\mathbf{I}_\ell \otimes \mathbf{B} \mid \mathbf{W}]^{-1}(\mathbf{I}_\ell \otimes \mathbf{G}, \sigma)\end{aligned}$$

We abbreviate the assumption to ℓ-succinct LWE when $\sigma = \mathsf{poly}(\lambda, \ell, m)$. The results in this work primarily rely on polynomial-time hardness of ℓ-succinct LWE for modulus-to-noise ratio $q/\chi \approx 2^{n^\epsilon}$, for some $0 < \epsilon < 1$.

3 New Succinct Commitments

Fix lattice parameters n, q and $m \geq 2n\log q$. Throughout this section, we write:

$$\mathsf{pp} := (\mathbf{B}, \mathbf{W}, \mathbf{T}) \text{ s.t. } [\mathbf{I}_{2m^2} \otimes \mathbf{B} \mid \mathbf{W}] \cdot \mathbf{T} = \mathbf{I}_{2m^2} \otimes \mathbf{G}$$

where $\mathbf{B} \in \mathbb{Z}_q^{n\times m}, \mathbf{W} \in \mathbb{Z}_q^{2m^2 n\times m}, \mathbf{T} \in \mathbb{Z}_q^{(2m^2+1)m\times 2m^3}$.

3.1 Matrix identities

Lemma 2. *For any matrices $\mathbf{X}, \mathbf{Y}$ of the dimensions $h \times \ell$ and $\ell \times w$, we have:*

$$\mathbf{XY} = (\mathrm{vec}(\mathbf{Y})^\top \otimes \mathbf{I}_h)(\mathbf{I}_w \otimes \mathrm{vec}(\mathbf{X})) \tag{8}$$

A proof is given in Section A.

Compactification. For any $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$, we write $\mathsf{bits}(\mathbf{M}) := \mathrm{vec}(\mathbf{G}^{-1}(\mathbf{M}))^\top \in \{0,1\}^{Lm}$ (the bit decomposition of $\mathbf{M}$ as a row vector). The next claim underlies the "compactification technique" used in [8] (the closed-form expression $\mathbf{I}_L \otimes \mathrm{vec}(\mathbf{I}_m)$ is new here).

Lemma 3. *For any $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$, we have:*

$$(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}) \cdot (\mathbf{I}_L \otimes \mathrm{vec}(\mathbf{I}_m)) = \mathbf{M} \tag{9}$$

Proof. The proof proceeds in two steps:

- Apply (8) to $\mathbf{I}_m \cdot \mathbf{G}^{-1}(\mathbf{M})$ to get:
$$\overbrace{(\mathrm{vec}(\mathbf{G}^{-1}(\mathbf{M}))^\top}^{=\mathsf{bits}(\mathbf{M})} \otimes \mathbf{I}_m) \cdot (\mathbf{I}_L \otimes \mathrm{vec}(\mathbf{I}_m)) = \mathbf{G}^{-1}(\mathbf{M})$$
- Multiply both sides on the left by $\mathbf{G}$ and use $\mathbf{G} \cdot (\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_m) = \mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}$. □

Next, we state a strengthening with $\mathbf{M} \cdot \mathbf{G}_L$ instead of $\mathbf{M}$ on the RHS:

Lemma 4. *For any $L \in \mathbb{N}$, we can efficiently compute $\mathbf{J}_L \in \{0,1\}^{Lm^2 \times L\lceil \log q\rceil}$ so that for all $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$, we have:*

$$(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}) \cdot \mathbf{J}_L = \mathbf{M} \cdot \mathbf{G}_L$$

In particular, $\mathbf{J}_L = \mathbf{G}_{Lmn}^{-1}\big(\mathbf{G}_{Lmn}(\mathbf{I}_L \otimes \mathrm{vec}(\mathbf{I}_m))\mathbf{G}_L\big)$.

Proof. Multiplying both sides of (9) on the right by $\mathbf{G}_L$, we have:

$$\begin{aligned} \mathbf{M} \cdot \mathbf{G}_L &= (\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G})(\mathbf{I}_L \otimes \mathrm{vec}(\mathbf{I}_m))\mathbf{G}_L \\ &= (\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}) \cdot \mathbf{G}_{Lmn}^{-1}\big(\mathbf{G}_{Lmn}(\mathbf{I}_L \otimes \mathrm{vec}(\mathbf{I}_m))\mathbf{G}_L\big) \end{aligned}$$

where the second equality uses $\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G} = (\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n)\mathbf{G}_{Lmn}$. □

3.2 Matrix commitment

Lemma 5 (matrix commitment). *There exist efficient algorithms $(\mathsf{Com}^{\mathsf{mx}}, \mathsf{Ver}^{\mathsf{mx}}, \mathsf{Open}^{\mathsf{mx}})$ where*

- $\mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})$*: on input $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$, outputs $\mathbf{C} \in \mathbb{Z}_q^{n\times m}$;*
- $\mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^L)$*: on input 1^L, outputs $\mathbf{V}_L^{\mathsf{mx}} \in \mathbb{Z}_q^{m\times L\lceil \log q\rceil}$;*
- $\mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})$*: on input $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$, outputs $\mathbf{Z} \in \mathbb{Z}_q^{m\times L\lceil \log q\rceil}$.*

For all $\mathsf{pp}, L \in \mathbb{N}, \mathbf{M} \in \mathbb{Z}_q^{n\times L}$, the matrices $\mathbf{C} \leftarrow \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M}), \mathbf{V}_L^{\mathsf{mx}} \leftarrow \mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^L), \mathbf{Z} \leftarrow \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})$ satisfy:

$$\begin{aligned} \mathbf{C} \cdot \mathbf{V}_L^{\mathsf{mx}} &= \mathbf{M} \cdot \mathbf{G}_L - \mathbf{B} \cdot \mathbf{Z} \\ \|\mathbf{V}_L^{\mathsf{mx}}\| &\leq O(\|\mathbf{T}\| \cdot m^4 \log q) \\ \|\mathbf{Z}\| &\leq O(\|\mathbf{T}\| \cdot m^7 \log q \cdot \log L) \end{aligned}$$

The running times of the algorithms are $L\log L \cdot \mathsf{poly}(m)$.

Proof. We present the construction in 2, described recursively over L. We may assume WLOG via padding that $L/2m$ is a power of 2. We proceed with the analysis.

Base case: $L = 2m$

$\underline{\mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})}$
output $\mathbf{C} := (\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n)\mathbf{W}$

$\underline{\mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})}$
output $\mathbf{Z} := (\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_m)\overline{\mathbf{T}} \cdot \mathbf{J}_{2m}$

$\underline{\mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^{2m})}$
output $\mathbf{V}_L^{\mathsf{mx}} := \underline{\mathbf{T}} \cdot \mathbf{J}_{2m}$

Recursive: $L > 2m$

$\underline{\mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M} = [\mathbf{M}_0 \mid \mathbf{M}_1])}$
$\mathbf{C}_\beta := \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M}_\beta), \beta = 0, 1$
output $\mathbf{C} := \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, [\mathbf{C}_0 \mid \mathbf{C}_1])$

$\underline{\mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M} = [\mathbf{M}_0 \mid \mathbf{M}_1])}$
$\mathbf{Z}_\beta := \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M}_\beta), \beta = 0, 1$
$\mathbf{Z}' := \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, [\mathbf{C}_0 \mid \mathbf{C}_1])$
output $\mathbf{Z} := \mathbf{Z}'(\mathbf{I}_2 \otimes \mathbf{G}_m^{-1}(\mathbf{V}_{L/2}^{\mathsf{mx}})) + [\mathbf{Z}_0 \mid \mathbf{Z}_1]$

$\underline{\mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^L)}$
output $\mathbf{V}_L^{\mathsf{mx}} := \mathbf{V}_{2m}^{\mathsf{mx}}(\mathbf{I}_2 \otimes \mathbf{G}_m^{-1}(\mathbf{V}_{L/2}^{\mathsf{mx}}))$

Fig. 2. Matrix commitment.

Base case: $L = 2m$. From $\mathsf{pp} = (\mathbf{B}, \mathbf{W}, \mathbf{T})$, let $\mathbf{T} = \binom{\overline{\mathbf{T}}}{\underline{\mathbf{T}}}, \overline{\mathbf{T}} \in \mathbb{Z}_q^{2m^3 \times 2m^3}, \underline{\mathbf{T}} \in \mathbb{Z}_q^{m \times 2m^3}$ so that

$$[\mathbf{I}_{2m^2} \otimes \mathbf{B} \mid \mathbf{W}] \cdot \begin{pmatrix} \overline{\mathbf{T}} \\ \underline{\mathbf{T}} \end{pmatrix} = \mathbf{I}_{2m^2} \otimes \mathbf{G} \tag{10}$$

Multiply both sides of (10) on the left by $\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n$ (where $\mathsf{bits}(\mathbf{M}) \in \{0,1\}^{2m^2}$) and use the fact that $\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n$ "commutes" with $\mathbf{I}_{2m^2} \otimes \mathbf{B}$ —i.e., $(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n)(\mathbf{I}_{2m^2} \otimes \mathbf{B}) = \mathbf{B}(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_m)$— to obtain:

$$\mathbf{B} \cdot \overbrace{(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_m)\overline{\mathbf{T}}}^{\mathbf{Z}_0} + \overbrace{(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n)\mathbf{W}}^{\mathbf{C}_0} \cdot \overbrace{\underline{\mathbf{T}}}^{\mathbf{V}_0} = \mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}_n \tag{11}$$

Next, we multiply both sides of (11) on the right by $\mathbf{J}_{2m}$ to obtain

$$\mathbf{B} \cdot \overbrace{(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_m)\overline{\mathbf{T}} \cdot \mathbf{J}_{2m}}^{\mathbf{Z}} + \overbrace{(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{I}_n)\mathbf{W}}^{\mathbf{C}} \cdot \overbrace{\underline{\mathbf{T}} \cdot \mathbf{J}_{2m}}^{\mathbf{V}_{2m}^{\mathsf{mx}}} = \mathbf{M} \cdot \mathbf{G}_{2m}$$

In particular, $\|\mathbf{V}_{2m}^{\mathsf{mx}}\| \le \|\mathbf{T}\| \cdot 4m^4$ and $\|\mathbf{Z}\| \le \|\mathbf{T}\| \cdot 4m^6$.

Recursive step: from $L/2$ to L. We have

$$\mathbf{C}_\beta \cdot \mathbf{V}_{L/2}^{\mathsf{mx}} = \mathbf{M}_\beta \cdot \mathbf{G}_{L/2} - \mathbf{B} \cdot \mathbf{Z}_\beta, \quad \beta \in \{0,1\}$$

which means

$$[\mathbf{C}_0 \mid \mathbf{C}_1] \cdot (\mathbf{I}_2 \otimes \mathbf{V}_{L/2}^{\mathsf{mx}}) = \mathbf{M} \cdot \mathbf{G}_L - \mathbf{B} \cdot [\mathbf{Z}_0 \mid \mathbf{Z}_1] \tag{12}$$

Moreover,

$$\mathbf{C} \cdot \mathbf{V}_{2m}^{\mathsf{mx}} = [\mathbf{C}_0 \mid \mathbf{C}_1] \cdot \mathbf{G}_{2m} - \mathbf{B} \cdot \mathbf{Z}' \tag{13}$$

where $\|\mathbf{Z}'\| \le B_{2m}$. Multiplying both sides of (13) by $\mathbf{I}_2 \otimes \mathbf{G}_m^{-1}(\mathbf{V}_{L/2}^{\mathsf{mx}})$ and adding to (12) yields

$$\overbrace{\mathbf{C} \cdot \mathbf{V}_{2m}^{\mathsf{mx}}(\mathbf{I}_2 \otimes \mathbf{G}_m^{-1}(\mathbf{V}_{L/2}^{\mathsf{mx}}))}^{\mathbf{V}_L^{\mathsf{mx}}} = \mathbf{M} \cdot \mathbf{G}_L - \mathbf{B} \cdot \overbrace{\left(\mathbf{Z}'(\mathbf{I}_2 \otimes \mathbf{G}_m^{-1}(\mathbf{V}_{L/2}^{\mathsf{mx}})) + [\mathbf{Z}_0 \mid \mathbf{Z}_1]\right)}^{\mathbf{Z}}$$

Norm bounds. We have $\|\mathbf{V}_L^{\mathsf{mx}}\| \le \|\mathbf{V}_{2m}^{\mathsf{mx}}\| \cdot m\lceil \log q \rceil = \|\mathbf{T}\| \cdot 2m^4 \lceil \log q \rceil$. Let B_L denote the bound on $\|\mathbf{Z}\|$ for matrices of width L. We have $\|\mathbf{Z}\| \le \|\mathbf{Z}'\| \cdot m\lceil \log q \rceil + \max\{\|\mathbf{Z}_0\|, \|\mathbf{Z}_1\|\}$, which means $B_L \le B_{2m} m \lceil \log q \rceil + B_{L/2}$. This yields $B_L = O(\|\mathbf{T}\| \cdot m^7 \log q \cdot \log L)$.

Running times. The running times for length L is twice that for $L/2$ plus $L \cdot \mathsf{poly}(m)$, and are therefore bounded by $L \log L \cdot \mathsf{poly}(m)$. □

3.3 Commitment to vectors

Lemma 6 (vector commitment). *Consider*

- $\mathsf{Com}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{x} \in \mathbb{Z}_q^\ell)$*: outputs* $\mathbf{C} := \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{x} \otimes \mathbf{I}_n) \in \mathbb{Z}_q^{n \times m}$.
- $\mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp}, 1^\ell)$*: outputs* $\mathbf{V}_\ell := \mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^{\ell n}) \in \mathbb{Z}_q^{m \times \ell m}$.
- $\mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{x})$*: outputs* $\mathbf{Z} := \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{x} \otimes \mathbf{I}_n) \in \mathbb{Z}_q^{m \times \ell m}$.

For all $\mathsf{pp}, \ell \in \mathbb{N}, \mathbf{x} \in \mathbb{Z}_q^\ell$*, the matrices* $\mathbf{C} \leftarrow \mathsf{Com}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{x}), \mathbf{V}_\ell \leftarrow \mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp}, 1^\ell), \mathbf{Z} \leftarrow \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{x})$ *satisfy:*

$$\begin{aligned} \mathbf{C} \cdot \mathbf{V}_\ell &= \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z} \\ \|\mathbf{V}_\ell\| &\le O(\|\mathbf{T}\| \cdot m^4 \log q) \\ \|\mathbf{Z}\| &\le O(\|\mathbf{T}\| \cdot \log \ell \cdot m^7 \log q) \end{aligned}$$

This follows readily from Lemma 5 plus the fact that $(\mathbf{x} \otimes \mathbf{I}_n)\mathbf{G}_{\ell n} = \mathbf{x} \otimes \mathbf{G}$.

Remark 1 (Amplifying ℓ-succinct LWE). Let $\mathbf{C}_i$ be a commitment to the unit vector $\mathbf{u}_i \in \{0,1\}^\ell$ (whose i'th entry is 1), along with an opening $\mathbf{Z}_i$ such that $\mathbf{C}_i \cdot \mathbf{V}_\ell = \mathbf{u}_i \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_i$. Now, if we stack the $\mathbf{C}_i$'s and $\mathbf{Z}_i$'s vertically to obtain $\mathbf{C} \in \mathbb{Z}_q^{\ell n \times m}, \mathbf{Z} \in \mathbb{Z}_q^{\ell m \times m}$, we have:

$$[\mathbf{I}_\ell \otimes \mathbf{B} \mid \mathbf{C}] \cdot \begin{pmatrix} \mathbf{Z} \\ \mathbf{V}_\ell \end{pmatrix} = \mathbf{I}_\ell \otimes \mathbf{G}$$

This allows us to show that hardness of $2m^2$-succinct LWE implies hardness of ℓ-succinct LWE for general ℓ. The distribution of $\mathbf{W}$ in the latter will not be uniform, but it implies hardness for the uniform distribution with a $O(\ell)$ blow-up in $\|\mathbf{T}\|$. (The latter follows from [28, Sec 6.1]: given a trapdoor for $[\mathbf{I} \otimes \mathbf{B} \mid \mathbf{C}]$, we can derive a trapdoor for $[\mathbf{I} \otimes \mathbf{B} \mid (\mathbf{I} \otimes \mathbf{B})\mathbf{R} + \mathbf{C}]$, where $\mathbf{R} \leftarrow \{0,1\}^{\ell m \times \ell}$. By left-over hash lemma, $(\mathbf{I} \otimes \mathbf{B})\mathbf{R} + \mathbf{C}$ is statistically close to a uniformly random $\mathbf{W}$.)

3.4 Commitment to circuits

We present a commitment scheme for depth d circuits over ℓ-bit inputs that supports opening to an evaluation $f(x)$ at a point x. In Section B, we present a "dual" scheme for ℓ-bit inputs that supports opening to $f(x)$ with respect to a circuit f.

Lemma 7. *There exist efficient algorithms* $(\mathsf{Com}^{\mathsf{c}}, \mathsf{Ver}^{\mathsf{c}}, \mathsf{Open}^{\mathsf{c}})$ *where*

- $\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f)$*: on input* $f \in \mathscr{F}_{\ell,d,s}$*, outputs* $\mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$*;*
- $\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^d)$*: on input* $x \in \{0,1\}^\ell$*, outputs* $\mathbf{V}_{x,d} \in \mathbb{Z}_q^{m \times m}$*;*
- $\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f, x)$*: on input* $f \in \mathscr{F}_{\ell,d,s}, x \in \{0,1\}^\ell$*, outputs* $\mathbf{Z}_{f,x} \in \mathbb{Z}_q^{m \times m}$.

For all $\mathsf{pp}, \ell, d, s \in \mathbb{N}, f \in \mathscr{F}_{\ell,d,s}, x \in \{0,1\}^\ell$*, the matrices* $\mathbf{C}_f \leftarrow \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f), \mathbf{V}_{x,d} \leftarrow \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^d), \mathbf{Z}_{f,x} \leftarrow \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f, x)$ *satisfy:*

$$\begin{aligned} \mathbf{C}_f \cdot \mathbf{V}_{x,d} &= f(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_{f,x} \\ \|\mathbf{V}_{x,d}\| &\le O(\|\mathbf{T}\| \cdot m^9) \\ \|\mathbf{Z}_{f,x}\| &\le \ell \cdot O(\|\mathbf{T}\| \cdot m^{12})^d \end{aligned}$$

Input gates: $\pi_i(x) := \mathbf{u}_i(x,1)^\top, i \in [\ell+1]$

$\underline{\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, \pi_i)}$
output $\mathbf{C}_{\pi_i} := \mathsf{Com}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{u}_i)$

$\underline{\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, \pi_i, x)}$
$\mathbf{Z}_i := \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{u}_i)$
output $\mathbf{Z}_{\pi_i,x} := \mathbf{Z}_i((x,1)^\top \otimes \mathbf{I}_m)$

$\underline{\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^0)}$
$\mathbf{V}_{\ell+1} := \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, 1^{\ell+1})$
output $\mathbf{V}_{x,0} := \mathbf{V}_{\ell+1}((x,1)^\top \otimes \mathbf{I}_m)$

Subtraction gate:

$\underline{\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f = f_0 - f_1)}$
$\mathbf{C}_\beta := \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f_\beta), \beta = 0,1$
output $\mathbf{C}_f := \mathbf{C}_0 - \mathbf{C}_1$

$\underline{\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f = f_0 - f_1, x)}$
$\mathbf{Z}_\beta := \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f_\beta, x), \beta = 0,1$
output $\mathbf{Z}_{f,x} := \mathbf{Z}_0 - \mathbf{Z}_1$

Multiplication gate:

$\underline{\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f = f_0 \cdot f_1)}$
$\mathbf{C}_\beta := \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f_\beta), \beta = 0,1$
$\mathbf{C}^\times := \mathsf{bits}(\mathbf{C}_1) \otimes \mathbf{C}_0$
output $\mathbf{C}_f := \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{C}^\times)$

$\underline{\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f = f_0 \cdot f_1, x)}$
$\mathbf{Z}_\beta := \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f_\beta, x), \beta = 0,1$
$\mathbf{Z}^\times := \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{C}^\times)$
$\mathbf{Z}' := \mathbf{Z}_0 \cdot \mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V}_{x,d-1} + f_0(x)\mathbf{Z}_1$
output $\mathbf{Z}_{f,x} := \mathbf{Z}^\times \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times) + \mathbf{Z}'$

$\underline{\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^d)}$
$\mathbf{V}_{x,d-1} := \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^{d-1})$
$\mathbf{V}^\times := (\mathbf{I}_m \otimes \mathsf{vec}(\mathbf{V}_{x,d-1}))\mathbf{V}_{x,d-1}$
$\mathbf{V}^{\mathsf{mx}}_{m^3} := \mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^{m^3})$
output $\mathbf{V}_{x,d} := \mathbf{V}^{\mathsf{mx}}_{m^3} \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)$

Fig. 3. Commitment to circuits

Remark 2 (comparison with BGGHNSVV ABE). We highlight the differences between our verification relation $\mathbf{C}_f \cdot \mathbf{V}_{x,d} = f(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_{f,x}$ and the key equation underlying the BGGHNSVV ABE in Lemma 1, namely $\mathbf{A}_f = f(x)\mathbf{G} + [\mathbf{A} - \mathbf{x} \otimes \mathbf{G}] \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}}$:

- the dimensions of $\mathbf{B}, \mathbf{Z}_{f,x}$ unlike those of $\mathbf{A} - \mathbf{x} \otimes \mathbf{G}, \mathbf{H}_{\mathbf{A},f,\mathbf{x}}$ are independent of ℓ;
- the dependence on x shows up in $\mathbf{V}_{x,d}$ instead of $\mathbf{A} - \mathbf{x} \otimes \mathbf{G}$.

Looking ahead to our CP-ABE, the first bullet yields smaller secret keys (i.e., $O(1)$ instead of $O(\ell)$), and the second bullet facilitates a reduction to succinct LWE, improving upon the use of evasive LWE plus tensor LWE in the W22 CP-ABE [27].

Proof. To support boolean circuit with NAND-gates, where $\mathrm{NAND}(a,b) = 1 - ab$, it suffices to handle leveled circuits of multiplicative depth d. In particular,

- depth 0 correspond to input wires x_i and the constant 1 wire;
- a multiplication gate f of depth d computes $f_0 \cdot f_1$, where f_0, f_1 are of depth $d-1$;
- a subtraction gate f of depth d computes $f_0 - f_1$, where f_0, f_1 are of depth d.

We present the construction in Fig 3, described recursively over d. We proceed with the analysis.

Input gates (i.e, $d = 0$). Every gate computes an affine function of the form $\pi_i(x) := \mathbf{u}_i(x,1)^\top, i \in [\ell+1]$ where $x \in \{0,1\}^\ell$ and $\mathbf{u}_i \in \{0,1\}^{\ell+1}$ is the unit vector whose i'th coordinate is 1. By correctness of $(\mathsf{Com}^{\mathsf{vc}}, \mathsf{Open}^{\mathsf{vc}}, \mathsf{Ver}^{\mathsf{vc}})$, we have

$$\mathbf{C}_{\pi_i} \cdot \mathbf{V}_{\ell+1} = \mathbf{u}_i \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_i$$

Multiplying both sides by $(x,1)^\top \otimes \mathbf{I}_m$, we have

$$\mathbf{C}_{\pi_i} \cdot \overbrace{\mathbf{V}_{\ell+1} \cdot \left((x,1)^\top \otimes \mathbf{I}_m\right)}^{=\mathbf{V}_{x,0}} = \pi_i(x)\mathbf{G} - \mathbf{B} \cdot \overbrace{\mathbf{Z}_i\left((x,1)^\top \otimes \mathbf{I}_m\right)}^{=\mathbf{Z}_{\pi_i,x}}$$

We have:

$$\|\mathbf{Z}_{\pi_i,x}\| \le \|\mathbf{Z}_i\| \cdot (\ell+1) = O(\|\mathbf{T}\| \cdot \ell m^8), \quad \|\mathbf{V}_{x,0}\| \le \|\mathbf{V}_{\ell+1}\| \cdot (\ell+1) = O(\|\mathbf{T}\| \cdot \ell m^5)$$

Subtraction gate. Suppose $f = f_0 - f_1$, where f_0, f_1 are circuits of depth d (so f also has depth d). By recursion, we have:

$$\mathbf{C}_0 \cdot \mathbf{V}_{x,d} = f_0(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_0$$
$$\mathbf{C}_1 \cdot \mathbf{V}_{x,d} = f_1(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_1$$

Subtracting the two yields:

$$(\mathbf{C}_0 - \mathbf{C}_1) \cdot \mathbf{V}_{x,d} = (f_0(x) - f_1(x))\mathbf{G} - \mathbf{B} \cdot (\mathbf{Z}_0 - \mathbf{Z}_1)$$

Multiplication gate. Suppose $f = f_0 \cdot f_1$, where f_0, f_1 are circuits of depth $d-1$. By recursion, we have

$$\mathbf{C}_0 \cdot \mathbf{V}_{x,d-1} = f_0(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_0 \tag{14}$$
$$\mathbf{C}_1 \cdot \mathbf{V}_{x,d-1} = f_1(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_1 \tag{15}$$

Adding (14) $\cdot \mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V}_{x,d-1}$ to (15) $\cdot f_0(x)$, we have

$$\mathbf{C}_0 \cdot \mathbf{V}_{x,d-1} \cdot \mathbf{G}^{-1}(\mathbf{C}_1) \cdot \mathbf{V}_{x,d-1} = f_0(x)f_1(x)\mathbf{G} - \mathbf{B} \cdot \Big(\overbrace{\mathbf{Z}_0 \cdot \mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V}_{x,d-1} + f_0(x)\mathbf{Z}_1}^{=\mathbf{Z}'}\Big)$$

On the other hand, applying (8) to $\mathbf{V}_{x,d-1} \cdot \mathbf{G}^{-1}(\mathbf{C}_1)$ and using $\mathsf{bits}(\mathbf{C}_1) = \mathrm{vec}(\mathbf{G}^{-1}(\mathbf{C}_1))^\top$, we have

$$\mathbf{V}_{x,d-1}\mathbf{G}^{-1}(\mathbf{C}_1) = (\mathsf{bits}(\mathbf{C}_1) \otimes \mathbf{I}_m)(\mathbf{I}_m \otimes \mathrm{vec}(\mathbf{V}_{x,d-1}))$$

This yields:

$$\mathbf{C}_0\mathbf{V}_{x,d-1}\mathbf{G}^{-1}(\mathbf{C}_1)\mathbf{V}_{x,d-1} = \overbrace{(\mathsf{bits}(\mathbf{C}_1) \otimes \mathbf{C}_0)}^{=\mathbf{C}^\times} \cdot \overbrace{(\mathbf{I}_m \otimes \mathrm{vec}(\mathbf{V}_{x,d-1}))\mathbf{V}_{x,d-1}}^{=\mathbf{V}^\times}$$

Therefore,

$$\mathbf{C}^\times \cdot \mathbf{V}^\times = f_0(x)f_1(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}' \tag{16}$$

From correctness of $(\mathsf{Com}^{\mathsf{mx}}, \mathsf{Open}^{\mathsf{mx}}, \mathsf{Ver}^{\mathsf{mx}})$, we have:

$$\mathbf{C}_f \cdot \mathbf{V}^{\mathsf{mx}}_{m^3} = \mathbf{C}^\times \cdot \mathbf{G}_{m^3} - \mathbf{B} \cdot \mathbf{Z}^\times$$

where $\|\mathbf{Z}^\times\| \le O(\|\mathbf{T}\| \cdot m^8)$. Multiplying both sides by $\mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)$ and combining with (16) yields:

$$\mathbf{C}_f \cdot \overbrace{\mathbf{V}^{\mathsf{mx}}_{m^3} \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)}^{=\mathbf{V}_{x,d}} = f_0(x)f_1(x)\mathbf{G} - \mathbf{B} \cdot \Big(\overbrace{\mathbf{Z}^\times \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times) + \mathbf{Z}'}^{=\mathbf{Z}_{f,x}}\Big)$$

as desired.

Norm bounds. First, we have

$$\|\mathbf{V}_{x,d}\| \le \|\mathbf{V}^{\mathsf{mx}}_{m^3}\| \cdot m^3 \lceil \log q \rceil = O(\|\mathbf{T}\| \cdot m^9)$$

Let B_d denote the bound on $\|\mathbf{Z}_{f,x}\|$ for depth d. We have

$$\begin{aligned} B_d &\le \overbrace{O(\|\mathbf{T}\| \cdot m^{12})}^{\mathbf{Z}^\times \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)} + \overbrace{2B_{d-1} \cdot \|\mathbf{V}_{x,d-1}\| \cdot m}^{\mathbf{Z}'} \\ &\le B_{d-1} \cdot O(\|\mathbf{T}\| \cdot m^{12}) \end{aligned}$$

Combined with $B_0 = O(\|\mathbf{T}\| \cdot \ell m^8)$, we have $B_d = \ell \cdot O(\|\mathbf{T}\| \cdot m^{12})^d$.

Running times. During the computation, we proceed layer by layer, and we memoize the values (i.e., commitments and openings) computed for previous layers. This way, the running times for $\mathsf{Com}^{\mathsf{c}}, \mathsf{Open}^{\mathsf{c}}$ are $sd \cdot \mathsf{poly}(m)$ and that for $\mathsf{Ver}^{\mathsf{c}}$ is $(\ell + d) \cdot \mathsf{poly}(m)$. □

4 Attribute-Based Encryption

4.1 Attribute-based encryption

Definition 1 (KP-ABE [26,19]). *A key-policy attribute-based encryption (KP-ABE) scheme for some class $\mathscr{F}$ consists of four algorithms:*

- $\mathsf{Setup}(1^\lambda, \mathscr{F}) \to (\mathsf{mpk}, \mathsf{msk})$. *The setup algorithm gets as input the security parameter 1^λ and class description $\mathscr{F}$. It outputs the master public key* mpk *and the master secret key* msk.
- $\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}$. *The encryption algorithm gets as input* mpk*, an input x and a message $\mu \in \{0,1\}^\lambda$. It outputs a ciphertext* ct.
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, f) \to \mathsf{sk}$. *The key generation algorithm gets as input* mpk, msk *and $f \in \mathscr{F}$. It outputs a secret key* sk.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}, f, \mathsf{ct}, x) \to \mu$. *The decryption algorithm gets as input* mpk, sk, f, ct, x *for which $f(x) = 0$.*[4] *It outputs a message μ.*

Correctness. *For all inputs x and f with $f(x) = 0$ and all $\mu \in \{0,1\}^\lambda$, we require*

$$\Pr\left[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}, f, \mathsf{ct}, x) = \mu : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathscr{F}) \\ \mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, f) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, \mu) \end{array}\right] = 1 - \mathit{negl}(\lambda).$$

Security. *For a stateful adversary $\mathscr{A}$, we define the advantage function*

$$\mathsf{Adv}^{\mathrm{ABE}}_{\mathscr{A}}(\lambda) := \Pr\left[b = b' : \begin{array}{l} x \leftarrow \mathscr{A}(1^\lambda) \\ (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathscr{F}) \\ (\mu_0, \mu_1) \leftarrow \mathscr{A}^{\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)}(\mathsf{mpk}) \\ b \leftarrow \{0,1\};\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, \mu_b) \\ b' \leftarrow \mathscr{A}^{\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)}(\mathsf{ct}) \end{array}\right] - \frac{1}{2}$$

with the restriction that all queries f that $\mathscr{A}$ sent to $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$ *satisfy $f(x) \neq 0$. An ABE scheme is* selectively secure *if for all PPT adversaries $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{ABE}}_{\mathscr{A}}(\lambda)$ is a negligible function in λ.*

CP-ABE. Ciphertext-policy attribute-based encryption (CP-ABE) is defined analogously, except we switch the roles of x and f.

4.2 KP-ABE for Circuits

Construction 1 (KP-ABE for circuits) *We construct a KP-ABE scheme for the family $\mathscr{F}_{\ell,d,s}$ of circuits of depth d and size s over ℓ-bit inputs as follows:*

– $\mathsf{Setup}(1^n, \mathscr{F}_{\ell,d,s})$*: Sample*

$$\begin{aligned} (\mathbf{B}, \mathbf{T_B}) &\leftarrow \mathsf{TrapGen}(1^n, 1^m, q),\ \mathbf{W} \leftarrow \mathbb{Z}_q^{2m^2 n \times m}, \\ \mathbf{T} &\leftarrow \mathsf{SamplePre}([\mathbf{I}_{2m^2} \otimes \mathbf{B} \mid \mathbf{W}], \mathbf{I}_{2m^2} \otimes \mathbf{T_B}, \mathbf{I}_{2m^2} \otimes \mathbf{G}, \sigma_0) \\ \mathbf{B}_1 &\leftarrow \mathbb{Z}_q^{n \times m},\ \mathbf{P} \leftarrow \mathbb{Z}_q^{n \times \lambda} \end{aligned}$$

[4] We follow the convention in [6] where $f(x) = 0$ corresponds to "authorized".

Output

$$\mathsf{mpk} := \big(\overbrace{\mathbf{B},\mathbf{W},\mathbf{T}}^{:=\mathsf{pp}},\mathbf{B}_1,\mathbf{P}\big) \in \mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^{2m^2n\times m}\times\mathbb{Z}_q^{(2m^2+1)m\times 2m^2\cdot m}\times\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^{n\times\lambda}$$
$$\mathsf{msk} := (\mathbf{T}_{\mathbf{B}})$$

– $\mathsf{Enc}(\mathsf{mpk},\mathbf{x},\mathbf{m})$. *Sample*

$$\mathbf{s}\leftarrow\mathbb{Z}_q^n,\ \mathbf{e}_0\leftarrow\mathscr{D}_{\mathbb{Z},\chi}^m,\mathbf{e}_1\leftarrow\mathscr{D}_{\mathbb{Z},\chi'}^{\ell m},\mathbf{e}_2\leftarrow\mathscr{D}_{\mathbb{Z},\chi'}^{\lambda},$$

Compute $\mathbf{C}_{\mathbf{x}} := \mathsf{Com}^{\mathsf{vc}}(\mathsf{pp},\mathbf{x})$. *Output*

$$\mathsf{ct} := \big(\overbrace{\mathbf{s}\mathbf{B}+\mathbf{e}_0}^{\mathbf{c}_0},\overbrace{\mathbf{s}(\mathbf{B}_1+\mathbf{C}_{\mathbf{x}})+\mathbf{e}_1}^{\mathbf{c}_1},\overbrace{\mathbf{s}\mathbf{P}+\mathbf{e}_2+\mathbf{m}\cdot\lfloor\tfrac{q}{2}\rfloor}^{\mathbf{c}_2}\big)\in\mathbb{Z}_q^m\times\mathbb{Z}_q^{\ell m}\times\mathbb{Z}_q^{\lambda}$$

– $\mathsf{KeyGen}(\mathsf{mpk},\mathsf{msk},f)$*: Compute* $\mathbf{V}_\ell := \mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp},1^\ell)$, $\mathbf{A} := -\mathbf{B}_1\mathbf{V}_\ell$ *and* $\mathbf{A}_f := \mathsf{EvalF}(\mathbf{A},f)$. *Sample*

$$\mathbf{D}\leftarrow\mathsf{SamplePre}([\mathbf{B}\mid\mathbf{A}_f],\mathbf{T}_{\mathbf{B}},\mathbf{P},\sigma_1)$$

Output

$$\mathsf{sk} := \mathbf{D}\in\mathbb{Z}^{2m\times\lambda}$$

– $\mathsf{Dec}(\mathsf{mpk},\mathsf{sk}=\mathbf{D},f,\mathsf{ct}=(\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2),\mathbf{x})$*: Compute*

$$\begin{aligned}\mathbf{V}_\ell &:= \mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp},1^\ell)\\ \mathbf{A} &:= -\mathbf{B}_1\mathbf{V}_\ell,\\ \mathbf{H}_{\mathbf{A},f,\mathbf{x}} &:= \mathsf{EvalFX}(\mathbf{A},f,\mathbf{x})\\ \mathbf{Z}_{\mathbf{x}} &:= \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp},\mathbf{x})\\ \mathbf{c}_3 &:= [\mathbf{c}_0\mid\mathbf{c}_1]\cdot\begin{pmatrix}-\mathbf{Z}_{\mathbf{x}}\\-\mathbf{V}_\ell\end{pmatrix}\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}}.\end{aligned}$$

Output

$$\Big\lfloor\tfrac{2}{q}\cdot\big(\mathbf{c}_2-[\mathbf{c}_0\mid\mathbf{c}_3]\cdot\mathbf{D}\bmod q\big)\Big\rceil\in\{0,1\}^\lambda$$

Parameters. Fix $0<\epsilon<1$, where $2m^2$-succinct LWE is hard for a 2^{n^ϵ} modulus-to-noise ratio. We set LWE parameters

$$\begin{aligned}n &= d^{1/\epsilon}\cdot\mathsf{poly}(\lambda,\log\ell,\log s)\\ m &= nd\cdot\mathsf{poly}(\lambda)\\ q &= m^{O(d)}s\cdot\mathsf{poly}(\ell)\cdot\lambda^{\omega(1)}\\ \chi &= \mathsf{poly}(n,\lambda)\end{aligned}$$

to satisfy

$$\begin{aligned}q/4 &\geq (\chi+\chi')\cdot\sigma_0\cdot\sigma_1\cdot m^{O(d)}s\cdot\mathsf{poly}(m,\lambda) && \text{(correctness)}\\ 2^{n^\epsilon} &\geq q/\chi && \text{(modulus-to-noise ratio)}\\ m &\geq 2n\log q &&\\ \sigma_0 &= \mathsf{poly}(m,\lambda) && (2m^2\text{-succinct LWE})\\ \sigma_1 &\geq \sigma_0\cdot m^{O(d)}s\cdot\mathsf{poly}(m,\lambda) && (\mathsf{H}_2\approx_s\mathsf{H}_3)\\ \chi' &\geq \chi\cdot\sigma_0\cdot\lambda^{\omega(1)} && (\mathsf{H}_1\approx_s\mathsf{H}_2)\end{aligned}$$

where $\mathsf{H}_1,\mathsf{H}_2,\mathsf{H}_3,\mathsf{H}_4$ are defined in the proof below. This yields the following parameter sizes for our KP-ABE scheme:

$$|\mathsf{mpk}| = O_{\lambda,d}(1),\quad |\mathsf{ct}| = O_{\lambda,d}(1),\quad |\mathsf{sk}| = O_{\lambda,d}(1)$$

where $O_{\lambda,d}(\cdot)$ hides factors polynomial in $\lambda, d^{1/\epsilon}$.

Correctness. Combining $\mathbf{C_x V}_\ell = \mathbf{x}\otimes\mathbf{G} - \mathbf{B Z_x}$ and $\mathbf{A} = -\mathbf{B}_1\mathbf{V}_\ell$, we have:

$$[\mathbf{B} \mid \mathbf{B}_1 + \mathbf{C_x}] \cdot \begin{pmatrix} -\mathbf{Z_x} \\ -\mathbf{V}_\ell \end{pmatrix} = \mathbf{A} - \mathbf{x}\otimes\mathbf{G}$$

Together with (7), this yields

$$[\mathbf{B} \mid \mathbf{B}_1 + \mathbf{C_x}] \cdot \begin{pmatrix} -\mathbf{Z_x} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G} \tag{17}$$

Mutliplying both sides by $\mathbf{s}$, we have:

$$\mathbf{c}_3 = [\mathbf{c}_0 \mid \mathbf{c}_1] \cdot \begin{pmatrix} -\mathbf{Z_x} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \mathbf{s}(\mathbf{A}_f - f(\mathbf{x})\mathbf{G}) \tag{18}$$

This means that whenever $f(\mathbf{x}) = 0$,

$$\begin{aligned} \mathbf{c}_3 &\approx \mathbf{s}\mathbf{A}_f \\ [\mathbf{c}_0 \mid \mathbf{c}_3]\cdot\mathbf{D} &\approx \mathbf{s}[\mathbf{B} \mid \mathbf{A}_f]\cdot\mathbf{D} = \mathbf{s}\mathbf{P} \\ \mathbf{c}_2 - [\mathbf{c}_0 \mid \mathbf{c}_3]\cdot\mathbf{D} &\approx \mathbf{m}\cdot\lfloor\tfrac{q}{2}\rfloor \end{aligned}$$

The error term in the final $\approx$ is given by

$$\mathbf{e}_2 - [\mathbf{e}_0 \mid ([\mathbf{e}_0 \mid \mathbf{e}_1] \cdot \begin{pmatrix} -\mathbf{Z_x} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}})] \cdot \mathbf{D}$$

whose norm is bounded by

$$\overbrace{(\chi+\chi')}^{\mathbf{e}_0,\mathbf{e}_1,\mathbf{e}_2} \cdot \overbrace{\sigma_0 \cdot \mathsf{poly}(m,\lambda)}^{\mathbf{Z_x},\mathbf{V}_\ell} \cdot \overbrace{\sigma_1}^{\mathbf{D}} \cdot \overbrace{m^{O(d)}s}^{\mathbf{H}_{\mathbf{A},f,\mathbf{x}}} \cdot \mathsf{poly}(m,\lambda)$$

Correctness follows as long as the preceding quantity is bounded by $q/4$.

Theorem 2. *Under the $(2m^2,\sigma_0)$-succinct LWE assumption, Construction 1 is a selectively secure KP-ABE scheme.*

Proof. We define a series of games:

- H_0: This is the real KP-ABE security game. Given the selective challenge $\mathbf{x}$, we compute $\mathbf{C_x} := \mathsf{Com}^{\mathsf{vc}}(\mathsf{pp},\mathbf{x})$ and $\mathbf{Z_x} := \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp},\mathbf{x})$.
- H_1: Same as H_1, except the challenger samples $\mathbf{B}_1,\mathbf{P}$ as follows:
  1. samples $\mathbf{U} \leftarrow \{0,1\}^{m\times m}$, and programs $\mathbf{B}_1 := \mathbf{B}\mathbf{U} - \mathbf{C_x}$
  2. samples $\mathbf{U}_0 \leftarrow \{0,1\}^{m\times\lambda}$, and programs $\mathbf{P} := \mathbf{B}\mathbf{U}_0$.

  $\mathsf{H}_0 \approx_s \mathsf{H}_1$ follows readily from left-over hash lemma.
- H_2: Same as H_1, except the challenger in Enc samples $\mathbf{c}_1 := \mathbf{c}_0\mathbf{U} + \mathbf{e}_1, \mathbf{c}_2 := \mathbf{c}_0\mathbf{U}_0 + \mathbf{e}_2$.

  $\mathsf{H}_1 \approx_s \mathsf{H}_2$ follows readily from noise-flooding, along with $\mathbf{c}_0\mathbf{U} \approx \mathbf{s}\mathbf{B}\mathbf{U} = \mathbf{s}(\mathbf{B}_1 + \mathbf{C_x})$ and $\mathbf{c}_0\mathbf{U}_0 \approx \mathbf{s}\mathbf{B}\mathbf{U}_0 = \mathbf{s}\mathbf{P}$.
- H_3: Same as H_2, except the challenger in KeyGen
  1. computes $\mathbf{H}_{\mathbf{A},f,\mathbf{x}} := \mathsf{EvalFX}(\mathbf{A},f,\mathbf{x})$, and
  2. samples $\mathbf{D}$ using $\mathsf{SamplePre}([\mathbf{B} \mid \mathbf{A}_f], \binom{(\mathbf{Z_x}+\mathbf{U}\mathbf{V}_\ell)\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}}}{\mathbf{I}_m}, \mathbf{P}, \sigma_1)$ instead of $\mathsf{SamplePre}([\mathbf{B} \mid \mathbf{A}_f], \mathbf{T_B}, \mathbf{P}, \sigma_1)$.

  $\mathsf{H}_2 \approx_s \mathsf{H}_3$ follows from trapdoor sampling together with the following:
  - substituting $\mathbf{B}_1 + \mathbf{C_x} = \mathbf{B}\mathbf{U}$ into (17) yields

$$[\mathbf{B} \mid \mathbf{B}\mathbf{U}] \cdot \begin{pmatrix} -\mathbf{Z_x} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} = \mathbf{B}\cdot(-(\mathbf{Z_x} + \mathbf{U}\mathbf{V}_\ell))\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}} = \mathbf{A}_f - f(x)\mathbf{G} \tag{19}$$

    and thus $[\mathbf{B} \mid \mathbf{A}_f] \cdot \binom{(\mathbf{Z_x}+\mathbf{U}\mathbf{V}_\ell)\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}}}{\mathbf{I}_m} = f(x)\mathbf{G}, f(x) \neq 0$.

- $\left|(\mathbf{Z}_{\mathbf{x}} + \mathbf{U}\mathbf{V}_\ell) \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}}\right| = \sigma_0 \cdot m^{O(d)} s \cdot \mathsf{poly}(m,\lambda)$.

– H_4: Same as H_3, except the challenger samples $\mathbf{c}_0 \leftarrow \mathbb{Z}_q^m$.
$\mathsf{H}_3 \approx_c \mathsf{H}_4$ follows from $(2m^2, \sigma_0)$-succinct LWE.

– H_5: Same as H_4, except the challenger samples $\mathbf{c}_2 \leftarrow \mathbb{Z}_q^\lambda$.
$\mathsf{H}_4 \approx_s \mathsf{H}_5$ follows from left-over hash lemma, which tells us $(\mathbf{B}, \mathbf{c}_0, \mathbf{B}\mathbf{U}_0, \mathbf{c}_0\mathbf{U}_0)$ is statistically close to uniform.

In H_5, the challenge bit b is perfectly hidden, so the advantage is 0. □

4.3 Reusable Garbled Circuits

Goldwasser et al. [16], with improvements from Boneh et al. [6], showed that starting from (i) an ABE scheme for $\mathscr{F}_{\ell,d,s}$ with mpk, ciphertext and key sizes $P(\ell,d,s), C(\ell,d,s), K(\ell,d,s)$, and (ii) the LWE assumption (used for FHE with rate one ciphertexts), we can construct a reusable garbling scheme for $\mathscr{F}_{\ell,d,s}$ in the CRS model where

– the CRS has size $P(\ell',d',s')$;
– the garbled input has size $\ell' + \mathsf{poly}(\lambda) \cdot C(\ell',d',s')$;
– the garbled circuit has size $s + \mathsf{poly}(\lambda) \cdot K(\ell',d',s')$;

where $\ell' = \ell + \mathsf{poly}(\lambda, d), d' = d \cdot \mathsf{poly}(\lambda), s' = s \cdot \mathsf{poly}(\lambda, d)$. Here, ℓ' is the size of a FHE encryption of $x \in \{0,1\}^\ell$ and d', s' correspond to the depth and the size of the circuit performing FHE homomorphic evaluation of f plus symmetric-key decryption. Combined with our ABE scheme in Construction 1, we have the following corollary:

Corollary 1 (Reusable garbling scheme). *Assuming $2m^2$-succinct LWE with 2^{n^ϵ} modulus-to-noise ratio, we have a reusable garbling scheme for $\mathscr{F}_{\ell,d,s}$ in the CRS model where*

– *the CRS has size $O_{\lambda,d}(1)$*
– *the garbled input has size $\ell + O_{\lambda,d}(1)$, and*
– *the garbled circuit has size $s + O_{\lambda,d}(1)$.*

Here, $O_{\lambda,d}(\cdot)$ hides factors polynomial in $\lambda, d^{1/\epsilon}$.

4.4 CP-ABE for Circuits

Construction 3 (CP-ABE for circuits) *We construct a CP-ABE scheme for the family $\mathscr{F}_{\ell,d,s}$ of circuits of depth d and size s over ℓ-bit inputs as follows:*

– $\mathsf{Setup}(1^n, \mathscr{F}_{\ell,d,s})$*: Sample*

$$\begin{aligned}(\mathbf{B}, \mathbf{T}_{\mathbf{B}}) &\leftarrow \mathsf{TrapGen}(1^n, 1^m, q),\ \mathbf{W} \leftarrow \mathbb{Z}_q^{2m^2 n \times m},\\ \mathbf{T} &\leftarrow \mathsf{SamplePre}([\mathbf{I}_{2m^2} \otimes \mathbf{B} \mid \mathbf{W}], \mathbf{I}_{2m^2} \otimes \mathbf{T}_{\mathbf{B}}, \mathbf{I}_{2m^2} \otimes \mathbf{G}, \sigma_0)\\ \mathbf{B}_1 &\leftarrow \mathbb{Z}_q^{n \times m},\ \mathbf{P} \leftarrow \mathbb{Z}_q^{n \times \lambda}\end{aligned}$$

Output

$$\begin{aligned}\mathsf{mpk} &:= \big(\overbrace{\mathbf{B}, \mathbf{W}, \mathbf{T}}^{:=\mathsf{pp}}, \mathbf{B}_1, \mathbf{P}\big) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{2m^2 n \times m} \times \mathbb{Z}_q^{(2m^2+1)m \times 2m^2 \cdot m} \times \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{n \times \lambda}\\ \mathsf{msk} &:= (\mathbf{T}_{\mathbf{B}})\end{aligned}$$

– $\mathsf{Enc}(\mathsf{mpk}, f, \mathbf{m})$*. Sample*

$$\mathbf{s} \leftarrow \mathbb{Z}_q^n,\ \mathbf{e}_0 \leftarrow \mathscr{D}_{\mathbb{Z},\chi}^m, \mathbf{e}_1 \leftarrow \mathscr{D}_{\mathbb{Z},\chi'}^{\ell m}, \mathbf{e}_2 \leftarrow \mathscr{D}_{\mathbb{Z},\chi'}^\lambda,$$

Compute $\mathbf{C}_f := \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f)$*. Output*

$$\mathsf{ct} := \big(\overbrace{\mathbf{s}\mathbf{B} + \mathbf{e}_0}^{\mathbf{c}_0}, \overbrace{\mathbf{s}(\mathbf{B}_1 + \mathbf{C}_f) + \mathbf{e}_1}^{\mathbf{c}_1}, \overbrace{\mathbf{s}\mathbf{P} + \mathbf{e}_2 + \mathbf{m} \cdot \lfloor \tfrac{q}{2} \rfloor}^{\mathbf{c}_2}\big) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{\ell m} \times \mathbb{Z}_q^\lambda$$

– $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, x)$: *Compute* $\mathbf{V}_{x,d} := \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^d), \mathbf{A}_x := -\mathbf{B}_1\mathbf{V}_{x,d}$. *Sample*

$$\mathbf{D} \leftarrow \mathsf{SamplePre}([\mathbf{B} \mid \mathbf{A}_x], \mathbf{T}_{\mathbf{B}}, \mathbf{P}, \sigma_1)$$

Output

$$\mathsf{sk} := \mathbf{D} \in \mathbb{Z}^{2m \times \lambda}$$

– $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk} = \mathbf{D}, f, \mathsf{ct} = (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), x)$: *Compute*

$$\begin{aligned}
\mathbf{V}_{x,d} &:= \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, x, 1^d) \\
\mathbf{A}_x &:= -\mathbf{B}_1\mathbf{V}_{x,d}, \\
\mathbf{Z}_{f,x} &:= \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f, x) \\
\mathbf{c}_3 &:= [\mathbf{c}_0 \mid \mathbf{c}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix}.
\end{aligned}$$

Output

$$\left\lfloor \tfrac{2}{q} \cdot \left(\mathbf{c}_2 - [\mathbf{c}_0 \mid \mathbf{c}_3] \cdot \mathbf{D} \bmod q \right) \right\rceil \in \{0,1\}^\lambda$$

Parameters. Fix $0 < \epsilon < 1$, where $2m^2$-succinct LWE is hard for a 2^{n^ϵ} modulus-to-noise ratio. We set LWE parameters

$$\begin{aligned}
n &= d^{1/\epsilon} \cdot \mathsf{poly}(\lambda) \\
m &= nd \cdot \mathsf{poly}(\lambda) \\
q &= (m\lambda)^{O(d)} \cdot \lambda^{\omega(1)} \\
\chi &= \mathsf{poly}(n, \lambda)
\end{aligned}$$

to satisfy

$$\begin{aligned}
q/4 &\geq (\chi + \chi') \cdot \ell(\sigma_0 \cdot m)^{O(d)} \cdot \sigma_1 \cdot \mathsf{poly}(m, \lambda) && \text{(correctness)} \\
2^{n^\epsilon} &\geq q/\chi && \text{(modulus-to-noise ratio)} \\
m &\geq 2n \log q \\
\sigma_0 &= \mathsf{poly}(m, \lambda) && (2m^2\text{-succinct LWE}) \\
\sigma_1 &\geq \ell(\sigma_0 \cdot m)^{O(d)} \cdot \mathsf{poly}(m, \lambda) && (\mathsf{H}_2 \approx_s \mathsf{H}_3) \\
\chi' &\geq \chi \cdot \sigma_0 \cdot \lambda^{\omega(1)} && (\mathsf{H}_1 \approx_s \mathsf{H}_2)
\end{aligned}$$

where $\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{H}_4$ are defined in the proof below. This yields the following parameter sizes for our CP-ABE scheme:

$$|\mathsf{mpk}| = O_{\lambda,d}(1), \quad |\mathsf{ct}| = O_{\lambda,d}(1), \quad |\mathsf{sk}| = O_{\lambda,d}(1)$$

where $O_{\lambda,d}(\cdot)$ hides factors polynomial in $\lambda, d^{1/\epsilon}$.

Correctness. Combining $\mathbf{C}_f\mathbf{V}_{x,d} = f(x)\mathbf{G} - \mathbf{B}\mathbf{Z}_{f,x}$ and $\mathbf{A}_x = -\mathbf{B}_1\mathbf{V}_{x,d}$, we have

$$[\mathbf{B} \mid \mathbf{B}_1 + \mathbf{C}_f] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix} = \mathbf{A}_x - f(x)\mathbf{G} \tag{20}$$

Mutliplying both sides by $\mathbf{s}$, we have:

$$\mathbf{c}_3 = [\mathbf{c}_0 \mid \mathbf{c}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix} \approx \mathbf{s}(\mathbf{A}_x - f(x)\mathbf{G}) \tag{21}$$

This means that whenever $f(x) = 0$,

$$\begin{aligned}
\mathbf{c}_3 &\approx \mathbf{s}\mathbf{A}_x \\
[\mathbf{c}_0 \mid \mathbf{c}_3] \cdot \mathbf{D} &\approx \mathbf{s}[\mathbf{B} \mid \mathbf{A}_x] \cdot \mathbf{D} = \mathbf{s}\mathbf{P} \\
\mathbf{c}_2 - [\mathbf{c}_0 \mid \mathbf{c}_3] \cdot \mathbf{D} &\approx \mathbf{m} \cdot \lfloor \tfrac{q}{2} \rfloor
\end{aligned}$$

The error term in the final $\approx$ is given by

$$\mathbf{e}_2 - [\mathbf{e}_0 \mid ([\mathbf{e}_0 \mid \mathbf{e}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix})] \cdot \mathbf{D}$$

whose norm is bounded by

$$\overbrace{(\chi + \chi')}^{\mathbf{e}_0,\mathbf{e}_1,\mathbf{e}_2} \cdot \overbrace{\ell(\sigma_0 \cdot m)^{O(d)}}^{\mathbf{Z}_{f,x},\mathbf{V}_{x,d}} \cdot \overbrace{\sigma_1}^{\mathbf{D}} \cdot \mathsf{poly}(m, \lambda)$$

Correctness follows as long as the preceding quantity is bounded by $q/4$.

Theorem 4. *Under the $(2m^2, \sigma_0)$-succinct LWE assumption, Construction 3 is a selectively secure CP-ABE scheme.*

Proof. We define a series of games:

- H_0: This is the real CP-ABE security game. Given the selective challenge f, we compute $\mathbf{C}_f := \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, f)$.
- H_1: Same as H_1, except the challenger samples $\mathbf{B}_1, \mathbf{P}$ as follows:
  1. samples $\mathbf{U} \leftarrow \{0,1\}^{m \times m}$, and programs $\mathbf{B}_1 := \mathbf{B}\mathbf{U} - \mathbf{C}_f$
  2. samples $\mathbf{U}_0 \leftarrow \{0,1\}^{m \times \lambda}$, and programs $\mathbf{P} := \mathbf{B}\mathbf{U}_0$.

  $\mathsf{H}_0 \approx_s \mathsf{H}_1$ follows readily from left-over hash lemma.
- H_2: Same as H_1, except the challenger in Enc samples $\mathbf{c}_1 := \mathbf{c}_0\mathbf{U} + \mathbf{e}_1, \mathbf{c}_2 := \mathbf{c}_0\mathbf{U}_0 + \mathbf{e}_2$.

  $\mathsf{H}_1 \approx_s \mathsf{H}_2$ follows readily from noise-flooding, along with $\mathbf{c}_0\mathbf{U} \approx \mathbf{s}\mathbf{B}\mathbf{U} = \mathbf{s}(\mathbf{B}_1 + \mathbf{C}_f)$ and $\mathbf{c}_0\mathbf{U}_0 \approx \mathbf{s}\mathbf{B}\mathbf{U}_0 = \mathbf{s}\mathbf{P}$.
- H_3: Same as H_2, except the challenger in KeyGen
  1. computes $\mathbf{Z}_{f,x} := \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f, x)$, and
  2. samples $\mathbf{D}$ using $\mathsf{SamplePre}([\mathbf{B} \mid \mathbf{A}_x], \begin{pmatrix} \mathbf{Z}_{f,x} + \mathbf{U}\mathbf{V}_{x,d} \\ \mathbf{I}_m \end{pmatrix}, \mathbf{P}, \sigma_1)$ instead of $\mathsf{SamplePre}([\mathbf{B} \mid \mathbf{A}_x], \mathbf{T}_{\mathbf{B}}, \mathbf{P}, \sigma_1)$.

  $\mathsf{H}_2 \approx_s \mathsf{H}_3$ follows from trapdoor sampling together with the following:
  - substituting $\mathbf{B}_1 + \mathbf{C}_f = \mathbf{B}\mathbf{U}$ into (20) yields

    $$[\mathbf{B} \mid \mathbf{B}\mathbf{U}] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix} = \mathbf{B} \cdot (-(\mathbf{Z}_{f,x} + \mathbf{U}\mathbf{V}_{x,d})) = \mathbf{A}_x - f(x)\mathbf{G}$$

    and thus $[\mathbf{B} \mid \mathbf{A}_x] \cdot \begin{pmatrix} \mathbf{Z}_{f,x} + \mathbf{U}\mathbf{V}_{x,d} \\ \mathbf{I}_m \end{pmatrix} = f(x)\mathbf{G}, f(x) \neq 0$.
  - $\left|\mathbf{Z}_{f,x} + \mathbf{U}\mathbf{V}_{x,d}\right| = \ell(\sigma_0 \cdot m)^{O(d)} \cdot \mathsf{poly}(m, \lambda)$.
- H_4: Same as H_3, except the challenger samples $\mathbf{c}_0 \leftarrow \mathbb{Z}_q^m$.

  $\mathsf{H}_3 \approx_c \mathsf{H}_4$ follows from $(2m^2, \sigma_0)$-succinct LWE.
- H_5: Same as H_4, except the challenger samples $\mathbf{c}_2 \leftarrow \mathbb{Z}_q^\lambda$.

  $\mathsf{H}_4 \approx_s \mathsf{H}_5$ follows from left-over hash lemma, which tells us $(\mathbf{B}, \mathbf{c}_0, \mathbf{B}\mathbf{U}_0, \mathbf{c}_0\mathbf{U}_0)$ is statistically close to uniform.

In H_5, the challenge bit b is perfectly hidden, so the advantage is 0. □

4.5 Broadcast Encryption

As observed in [5,10], broadcast encryption for N users is captured by CP-ABE for circuits of depth $O(\log N)$ and size N. This yields the following corollary:

Corollary 2 (Broadcast encryption). *Under the $\mathsf{poly}(\lambda, \log N)$-succinct LWE assumption, we have a broadcast encryption scheme for N users with parameters*

$$|\mathsf{mpk}| = \mathsf{poly}(\lambda, \log N), \quad |\mathsf{ct}| = \mathsf{poly}(\lambda, \log N), \quad |\mathsf{sk}| = \mathsf{poly}(\lambda, \log N)$$

5 Laconic Function Evaluation

5.1 Definition of LFE

Definition 2 (LFE [25,12]). *A laconic function evaluation (LFE) scheme for some class $\mathscr{F}$ consists of four algorithms* Setup, Compress, Enc, Dec.

- $\mathsf{Setup}(1^\lambda, \mathscr{F})$ *takes as input the security parameter* 1^λ *and circuit parameters* $\mathscr{F}$ *and outputs a common reference string* crs.
- $\mathsf{Compress}(\mathsf{crs}, f)$ *is a deterministic algorithm that takes as input* crs *and* $f \in \mathscr{F}$ *and outputs a digest* dig.
- $\mathsf{Enc}(\mathsf{crs}, \mathsf{dig}, x)$ *takes as input* crs, *a digest* dig *and a message* x *and outputs a ciphertext* ct.
- $\mathsf{Dec}(\mathsf{crs}, f, \mathsf{ct})$ *takes as input* crs, $f \in \mathscr{F}$, *and a ciphertext* ct *and outputs a message* y.

Correctness. *We require that for all $\lambda, \mathscr{F}$ and $f \in \mathscr{F}$:*

$$\Pr\left[y = f(x) \;\middle|\; \begin{array}{ll} \mathsf{crs} & \leftarrow \mathsf{Setup}(1^\lambda, \mathscr{F}) \\ \mathsf{dig} & = \mathsf{Compress}(\mathsf{crs}, f) \\ \mathsf{ct} & \leftarrow \mathsf{Enc}(\mathsf{crs}, \mathsf{dig}, x) \\ y & \leftarrow \mathsf{Dec}(\mathsf{crs}, f, \mathsf{ct}) \end{array} \right] = 1.$$

Selective security. *We require that there exists a PPT simulator* Sim *such that for all stateful PPT adversary $\mathscr{A}$, we have:*

$$\left| \Pr\left[\mathrm{EXP}^{Real}_{LFE}(1^\lambda) = 1 \right] - \Pr\left[\mathrm{EXP}^{Ideal}_{LFE}(1^\lambda) \right] \right| \leq \mathsf{negl}(\lambda)$$

for the experiments $\mathrm{EXP}^{Real}_{LFE}(1^\lambda)$ and $\mathrm{EXP}^{Ideal}_{LFE}(1^\lambda)$ defined below:

$\mathrm{EXP}^{Real}_{LFE}(1^\lambda)$:

0. $(\mathscr{F}, x) \leftarrow \mathscr{A}(1^\lambda)$
1. $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, \mathscr{F})$
2. $f \leftarrow \mathscr{A}(\mathsf{crs})$:
3. $\mathsf{dig} = \mathsf{Compress}(\mathsf{crs}, f)$
4. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{crs}, \mathsf{dig}, x)$
5. *Output* $\mathscr{A}(\mathsf{ct})$

$\mathrm{EXP}^{Ideal}_{LFE}(1^\lambda)$:

0. $(\mathscr{F}, x) \leftarrow \mathscr{A}(1^\lambda)$
1. $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, \mathscr{F})$
2. $f \leftarrow \mathscr{A}(\mathsf{crs})$:
3. $\mathsf{dig} = \mathsf{Compress}(\mathsf{crs}, f)$
4. $\mathsf{ct} \leftarrow \mathsf{Sim}(\mathsf{crs}, \mathsf{dig}, f, f(x))$
5. *Output* $\mathscr{A}(\mathsf{ct})$

5.2 LFE for Circuits

Following QWW [25], we start by constructing AB-LFE for circuits, which corresponds to LFE for the following functionality:

$$(\mathbf{x}, \mathbf{m}_0, \mathbf{m}_1) \in \{0,1\}^\ell \times \{0,1\}^\lambda \times \{0,1\}^\lambda \overset{f \in \mathscr{F}_{\ell,d,s}}{\longmapsto} (\mathbf{x}, \mathbf{m}_{f(\mathbf{x})})$$

Construction 5 (AB-LFE for circuits) *We construct an AB-LFE scheme for the family $\mathscr{F}_{\ell,d,s}$ of circuits of depth d and size s over ℓ-bit inputs as follows:*

– $\mathsf{Setup}(1^n, \mathscr{F}_{\ell,d,s})$: *Sample*

$$\begin{aligned} (\mathbf{B}, \mathbf{T}_\mathbf{B}) &\leftarrow \mathsf{TrapGen}(1^n, 1^m, q),\ \mathbf{W} \leftarrow \mathbb{Z}_q^{2m^2 n \times m}, \\ \mathbf{T} &\leftarrow \mathsf{SamplePre}([\mathbf{I}_{2m^2} \otimes \mathbf{B} \mid \mathbf{W}], \mathbf{I}_{2m^2} \otimes \mathbf{T}_\mathbf{B}, \mathbf{I}_{2m^2} \otimes \mathbf{G}, \sigma_0) \\ \mathbf{B}_1 &\leftarrow \mathbb{Z}_q^{n \times m} \end{aligned}$$

Output

$$\mathsf{crs} := \big(\overbrace{\mathbf{B}, \mathbf{W}, \mathbf{T}}^{:=\mathsf{pp}}, \mathbf{B}_1\big) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{2m^2 n \times m} \times \mathbb{Z}_q^{(2m^2+1)m \times 2m^2 \cdot m} \times \mathbb{Z}_q^{n \times m}$$

– $\mathsf{Compress}(\mathsf{crs}, f)$: *Compute* $\mathbf{V}_\ell := \mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp}, 1^\ell), \mathbf{A} := -\mathbf{B}_1\mathbf{V}_\ell$ *and* $\mathbf{A}_f := \mathsf{EvalF}(\mathbf{A}, f)$. *Output*

$$\mathsf{dig} := \mathbf{A}_f \in \mathbb{Z}^{n\times m}$$

– $\mathsf{Enc}(\mathsf{crs}, \mathbf{A}_f, (\mathbf{x}, \mathbf{m}_0, \mathbf{m}_1))$. *Sample*

$$\mathbf{s} \leftarrow \mathbb{Z}_q^n,\ \mathbf{e}_0 \leftarrow \mathscr{D}_{\mathbb{Z},\chi}^m, \mathbf{e}_1 \leftarrow \mathscr{D}_{\mathbb{Z},\chi'}^{\ell_1 m}, \mathbf{e}_{2,0}, \mathbf{e}_{2,1} \leftarrow \mathscr{D}_{\mathbb{Z},\chi''}^{\lambda}, \mathbf{P}_0, \mathbf{P}_1 \leftarrow \mathbb{Z}_q^{n\times\lambda}$$

Compute

$$\begin{aligned}
\mathbf{c}_0 &:= \mathbf{s}\mathbf{B} + \mathbf{e}_0 \\
\mathbf{c}_1 &:= \mathbf{s}(\mathbf{B}_1 + \mathbf{C}_{\mathbf{x}}) + \mathbf{e}_1 \\
\mathbf{c}_{2,0} &:= \mathbf{s}\mathbf{A}_f \cdot \mathbf{G}^{-1}(\mathbf{P}_0) + \mathbf{m}_0 \cdot \lfloor \tfrac{q}{2} \rfloor + \mathbf{e}_{2,0} \\
\mathbf{c}_{2,1} &:= \mathbf{s}(\mathbf{A}_f - \mathbf{G}) \cdot \mathbf{G}^{-1}(\mathbf{P}_1) + \mathbf{m}_1 \cdot \lfloor \tfrac{q}{2} \rfloor + \mathbf{e}_{2,1}
\end{aligned}$$

Output

$$\mathsf{ct} := \left(\mathbf{x}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_{2,0}, \mathbf{c}_{2,1}, \mathbf{P}_0, \mathbf{P}_1\right) \in \{0,1\}^\ell \times \mathbb{Z}_q^m \times \mathbb{Z}_q^{\ell_1 m} \times (\mathbb{Z}_q^\lambda)^2 \times (\mathbb{Z}_q^{n\times\lambda})^2$$

– $\mathsf{Dec}(\mathsf{crs} = (\mathbf{A}_f), f, \mathsf{ct} = (\mathbf{x}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_{2,0}, \mathbf{c}_{2,1}, \mathbf{P}_0, \mathbf{P}_1))$: *Compute*

$$\begin{aligned}
\mathbf{V}_\ell &:= \mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp}, 1^\ell) \\
\mathbf{A} &:= -\mathbf{B}_1\mathbf{V}_\ell, \\
\mathbf{H}_{\mathbf{A},f,\mathbf{x}} &:= \mathsf{EvalFX}(\mathbf{A}, f, \mathbf{x}) \\
\mathbf{Z}_{\mathbf{x}} &:= \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, \mathbf{x}) \\
\mathbf{c}_3 &:= [\mathbf{c}_0 \,|\, \mathbf{c}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{\mathbf{x}} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}}
\end{aligned}$$

Output

$$\left\lfloor \tfrac{2}{q} \cdot \left(\mathbf{c}_{2,f(\mathbf{x})} - \mathbf{c}_3 \cdot \mathbf{G}^{-1}(\mathbf{P}_{f(\mathbf{x})}) \bmod q\right) \right\rceil \in \{0,1\}^\lambda$$

Parameters. Fix $0 < \epsilon < 1$, where $2m^2$-succinct LWE is hard for a 2^{n^ϵ} modulus-to-noise ratio. We will set LWE parameters as in our ABE scheme in Section 4.2

$$\begin{aligned}
n &= d^{1/\epsilon} \cdot \mathsf{poly}(\lambda, \log \ell, \log s) \\
m &= nd \cdot \mathsf{poly}(\lambda) \\
q &= m^{O(d)} s \cdot \mathsf{poly}(\ell) \cdot \lambda^{\omega(1)} \\
\chi &= \mathsf{poly}(n, \lambda)
\end{aligned}$$

which also satisfy the following minor modifications to the constraints pertaining to χ'' (in place of σ_1):

$$\begin{aligned}
q/4 &\geq (\chi'' + (\chi + \chi') \cdot \sigma_0 \cdot m^{O(d)} s) \cdot \mathsf{poly}(m, \lambda) && \text{(correctness)} \\
\chi'' &\geq (\chi + \chi') \cdot \sigma_0 \cdot m^{O(d)} s) \cdot \mathsf{poly}(m, \lambda) \cdot \lambda^{\omega(1)} && (\mathsf{H}_0 \approx_s \mathsf{H}_1 \text{ in proof below})
\end{aligned}$$

This yields the following parameter sizes for our AB-LFE scheme:

$$|\mathsf{crs}| = O_{\lambda,d}(1), \quad |\mathsf{dig}| = O_{\lambda,d}(1), \quad |\mathsf{ct}| = \ell + O_{\lambda,d}(\ell_1)$$

and the encryption running time is $O_{\lambda,d}(\ell)$. Here, $O_{\lambda,d}(\cdot)$ hides factors polynomial in $\lambda, d^{1/\epsilon}$.

Correctness. Observe that $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_3$ are the same as in the KP-ABE scheme in Section 4.2. Therefore, we have from (18) that $\mathbf{c}_3 \approx \mathbf{s}(\mathbf{A}_f - f(x)\mathbf{G})$. This yields

$$\mathbf{c}_{2,f(\mathbf{x})} \approx \mathbf{c}_3 \cdot \mathbf{G}^{-1}(\mathbf{P}_{f(\mathbf{x})}) + \mathbf{m}_{f(\mathbf{x})} \cdot \lfloor \tfrac{q}{2} \rfloor \tag{22}$$

The error term in the above $\approx$ is given by

$$\mathbf{e}_{2,f(\mathbf{x})} - ([\mathbf{e}_0 \mid \mathbf{e}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{\mathbf{x}} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}}) \cdot \mathbf{G}^{-1}(\mathbf{P}_{f(\mathbf{x})})$$

whose norm is bounded by

$$(\overbrace{\chi''}^{\mathbf{e}_{2,f(\mathbf{x})}} + (\overbrace{\chi + \chi'}^{\mathbf{e}_0,\mathbf{e}_1}) \cdot \overbrace{\sigma_0 \cdot \mathsf{poly}(m,\lambda)}^{\mathbf{Z}_{\mathbf{x}},\mathbf{V}_\ell} \cdot \overbrace{m^{O(d)} s}^{\mathbf{H}_{\mathbf{A},f,\mathbf{x}}}) \cdot \mathsf{poly}(m,\lambda)$$

Correctness follows as long as the preceding quantity is bounded by $q/4$.

Theorem 6. *Under the $(2m^2, \sigma_0)$-succinct LWE assumption, Construction 5 is selectively secure.*

Proof. We begin by specifying the simulator:

– $\mathsf{Sim}(\mathsf{crs}, \mathsf{dig}, f, (\mathbf{x}, \mathbf{z}))$: Compute $f(\mathbf{x}) \in \{0,1\}$, and sample

$$\mathbf{c}_0 \leftarrow \mathbb{Z}_q^m, \mathbf{c}_1 \leftarrow \mathbb{Z}_q^m, \mathbf{e}_{2,f(\mathbf{x})} \leftarrow \mathscr{D}^{\lambda}_{\mathbb{Z},\chi''}, \mathbf{c}_{2,1-f(\mathbf{x})} \leftarrow \mathbb{Z}_q^{\lambda}, \mathbf{P}_0, \mathbf{P}_1 \leftarrow \mathbb{Z}_q^{n \times \lambda}$$

Compute

$$\mathbf{c}_3 := [\mathbf{c}_0 \mid \mathbf{c}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{\mathbf{x}} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} \quad \text{(same as in Dec)}$$
$$\mathbf{c}_{2,f(\mathbf{x})} := \mathbf{c}_3 \cdot \mathbf{G}^{-1}(\mathbf{P}_{f(\mathbf{x})}) + \mathbf{z} \cdot \lfloor \tfrac{q}{2} \rfloor + \mathbf{e}_{2,f(\mathbf{x})}$$

Output

$$\mathsf{ct} := \left(\mathbf{x}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_{2,0}, \mathbf{c}_{2,1}, \mathbf{P}_0, \mathbf{P}_1\right)$$

We define a series of games:

– H_0: This is the real AB-LFE security game.

– H_1: Same as H_0, except the challenger computes $\mathbf{c}_3$ as in Sim, and $\mathbf{c}_{2,0}, \mathbf{c}_{2,1}$ as follows:

$$\mathbf{c}_{2,b} := \mathbf{c}_3 \cdot \mathbf{G}^{-1}(\mathbf{P}_b) + \mathbf{m}_b \cdot \lfloor \tfrac{q}{2} \rfloor + (f(\mathbf{x}) - b) \cdot \mathbf{s}\mathbf{P}_b + \mathbf{e}_{2,b}, \forall b \in \{0,1\}$$

$\mathsf{H}_0 \approx_s \mathsf{H}_1$ follows from

- a straight-forward adaptation of (22) which tells us $\mathbf{c}_{2,b}$ in H_0 satisfies:

$$\mathbf{c}_{2,b} \approx \mathbf{c}_3 \cdot \mathbf{G}^{-1}(\mathbf{P}_b) + \mathbf{m}_b \cdot \lfloor \tfrac{q}{2} \rfloor + (f(\mathbf{x}) - b) \cdot \mathbf{s}\mathbf{P}_b, \forall b \in \{0,1\}$$

- noise-flooding using $\mathbf{e}_{2,b}$ to flood the error term

$$([\mathbf{e}_0 \mid \mathbf{e}_1] \cdot \begin{pmatrix} -\mathbf{Z}_{\mathbf{x}} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}}) \cdot \mathbf{G}^{-1}(\mathbf{P}_b)$$

– H_2: Same as H_1, except the challenger samples $\mathbf{B}_1, \mathbf{P}_{1-f(\mathbf{x})}$ as follows:
1. samples $\mathbf{U} \leftarrow \{0,1\}^{m \times m}$, and programs $\mathbf{B}_1 := \mathbf{B}\mathbf{U} - \mathbf{C}_{\mathbf{x}}$
2. samples $\mathbf{U}_{1-f(\mathbf{x})} \leftarrow \{0,1\}^{m \times \lambda}$, and programs $\mathbf{P}_{1-f(\mathbf{x})} = \mathbf{B}\mathbf{U}_{1-f(\mathbf{x})}$.

$\mathsf{H}_1 \approx_s \mathsf{H}_2$ follows readily from left-over hash lemma.

– H_3: Same as H_2, except the challenger in Enc samples $\mathbf{c}_1, \mathbf{c}_{2,1-f(\mathbf{x})}$ as follows:

$$\mathbf{c}_1 := \mathbf{c}_0\mathbf{U} + \mathbf{e}_1$$
$$\mathbf{c}_{2,b} := \mathbf{c}_3 \cdot \mathbf{G}^{-1}(\mathbf{P}_b) + \mathbf{m}_b \cdot \lfloor \tfrac{q}{2} \rfloor + (f(\mathbf{x}) - b) \cdot \mathbf{c}_0\mathbf{U}_b + \mathbf{e}_{2,b}, \;\; b = 1 - f(\mathbf{x})$$

$\mathsf{H}_2 \approx_s \mathsf{H}_3$ follows readily from noise-flooding along with $\mathbf{c}_0\mathbf{U} \approx \mathbf{sBU} = \mathbf{s}(\mathbf{B}_1 + \mathbf{C}_\mathbf{x})$ and $\mathbf{c}_0\mathbf{U}_{1-f(\mathbf{x})} \approx \mathbf{sBU}_{1-f(\mathbf{x})} = \mathbf{sP}_{1-f(\mathbf{x})}$.

– H_4: Same as H_3, except the challenger samples $\mathbf{c}_0 \leftarrow \mathbb{Z}_q^m$.

$\mathsf{H}_3 \approx_c \mathsf{H}_4$ follows from $(2m^2, \sigma_0)$-succinct LWE.

– H_5: Same as H_4, except the challenger samples $\mathbf{c}_1 \leftarrow \mathbb{Z}_q^m, \mathbf{c}_{2,1-f(\mathbf{x})} \leftarrow \mathbb{Z}_q^\lambda$.

$\mathsf{H}_4 \approx_s \mathsf{H}_5$ follows from left-over hash lemma, which tells us $(\mathbf{B}, \mathbf{c}_0, \mathbf{BU}, \mathbf{c}_0\mathbf{U}, \mathbf{BU}_{1-f(\mathbf{x})}, \mathbf{c}_0\mathbf{U}_{1-f(\mathbf{x})})$ is statistically close to uniform.

Observe that H_5 is exactly the output of Sim, since $\mathbf{z} = \mathbf{m}_{f(\mathbf{x})}$. □

From AB-LFE to LFE. Prior work [25] showed —via a construction similar to that in Section 4.3—that starting from (i) an AB-LFE scheme for $\mathscr{F}_{\ell,d,s}$ with CRS, ciphertext and digest sizes $P(\ell,d,s), \ell + C(\ell,d,s), K(\ell,d,s)$, and (ii) the LWE assumption (used for FHE with rate one ciphertexts), we can construct an LFE scheme for $\mathscr{F}_{\ell,d,s}$ where

$$|\mathsf{crs}| = P(\ell',d',s'), \quad |\mathsf{dig}| = \mathsf{poly}(\lambda) \cdot K(\ell',d',s'), \quad |\mathsf{ct}| = \ell' + \mathsf{poly}(\lambda) \cdot C(\ell',d',s')$$

where $\ell' = \ell + \mathsf{poly}(\lambda, d), d' = \mathsf{poly}(\lambda, d), s' = s \cdot \mathsf{poly}(\lambda, d)$. Combined with our AB-LFE scheme in Construction 5, we have the following corollary:

Corollary 3 (LFE for circuits). *Assuming $2m^2$-succinct LWE with 2^{n^ϵ} modulus-to-noise ratio, we have an LFE scheme for $\mathscr{F}_{\ell,d,s}$ where*

$$|\mathsf{crs}| = O_{\lambda,d}(1), \quad |\mathsf{dig}| = O_{\lambda,d}(1), \quad |\mathsf{ct}| = \ell + O_{\lambda,d}(1)$$

and the encryption running time is $O_{\lambda,d}(\ell)$. Here, $O_{\lambda,d}(\cdot)$ hides factors polynomial in $\lambda, d^{1/\epsilon}$.

Acknowledgments. We thank Brent Waters and David Wu for inspiring discussions about lattice trapdoors in Austin, as well as the reviewers for helpful feedback. We also thank Damiano Abram, Giulio Malavolta and Lawrence Roy for helpful discussions regarding [2,1].

References

1. D. Abram, G. Malavolta, and L. Roy. Key-homomorphic computations for RAM: Fully succinct randomised encodings and more. Cryptology ePrint Archive, Paper 2025/339, 2025.
2. D. Abram, G. Malavolta, and L. Roy. Succinct oblivious tensor evaluation and applications: Adaptively-secure laconic function evaluation and trapdoor hashing for all circuits. In *STOC*, 2025.
3. S. Agrawal, S. Kumari, and S. Yamada. Attribute based encryption for turing machines from lattices. In L. Reyzin and D. Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 352–386. Springer, Cham, Aug. 2024.
4. S. Agrawal, S. Kumari, and S. Yamada. Compact pseudorandom functional encryption from evasive LWE. Cryptology ePrint Archive, Paper 2024/1719, 2024.
5. S. Agrawal and S. Yamada. Optimal broadcast encryption from pairings and LWE. In A. Canteaut and Y. Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 13–43. Springer, Cham, May 2020.
6. D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, and D. Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 533–556. Springer, Berlin, Heidelberg, May 2014.
7. D. Boneh, W. Nguyen, and A. Ozdemir. Efficient functional commitments: How to commit to a private function. Cryptology ePrint Archive, Paper 2021/1342, 2021.

8. Z. Brakerski, R. Tsabary, V. Vaikuntanathan, and H. Wee. Private constrained PRFs (and more) from LWE. In Y. Kalai and L. Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 264–302. Springer, Cham, Nov. 2017.
9. Z. Brakerski and V. Vaikuntanathan. Circuit-ABE from LWE: Unbounded attributes and semi-adaptive security. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 363–384. Springer, Berlin, Heidelberg, Aug. 2016.
10. Z. Brakerski and V. Vaikuntanathan. Lattice-inspired broadcast encryption and succinct ciphertext-policy ABE. In M. Braverman, editor, *ITCS 2022*, volume 215, pages 28:1–28:20. LIPIcs, Jan. / Feb. 2022.
11. Y. Chen, V. Vaikuntanathan, and H. Wee. GGH15 beyond permutation branching programs: Proofs, attacks, and candidates. In H. Shacham and A. Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 577–607. Springer, Cham, Aug. 2018.
12. C. Cho, N. Döttling, S. Garg, D. Gupta, P. Miao, and A. Polychroniadou. Laconic oblivious transfer and its applications. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 33–65. Springer, Cham, Aug. 2017.
13. V. Cini and H. Wee. ABE for circuits with $\mathsf{poly}(\lambda)$-sized keys from LWE. In *FOCS*, 2023.
14. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.
15. C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 75–92. Springer, Berlin, Heidelberg, Aug. 2013.
16. S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich. Reusable garbled circuits and succinct functional encryption. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *45th ACM STOC*, pages 555–564. ACM Press, June 2013.
17. S. Gorbunov, V. Vaikuntanathan, and H. Wee. Attribute-based encryption for circuits. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *45th ACM STOC*, pages 545–554. ACM Press, June 2013.
18. S. Gorbunov, V. Vaikuntanathan, and D. Wichs. Leveled fully homomorphic signatures from standard lattices. In R. A. Servedio and R. Rubinfeld, editors, *47th ACM STOC*, pages 469–477. ACM Press, June 2015.
19. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 89–98. ACM Press, Oct. / Nov. 2006. Available as Cryptology ePrint Archive Report 2006/309.
20. Y.-C. Hsieh, H. Lin, and J. Luo. Attribute-based encryption for circuits of unbounded depth from lattices: Garbled circuits of optimal size, laconic functional evaluation, and more. In *FOCS*, 2023.
21. Y.-C. Hsieh, H. Lin, and J. Luo. A general framework for lattice-based ABE using evasive inner-product functional encryption. In M. Joye and G. Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 433–464. Springer, Cham, May 2024.
22. A. Jain, H. Lin, and J. Luo. On the optimal succinctness and efficiency of functional encryption and attribute-based encryption. In C. Hazay and M. Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 479–510. Springer, Cham, Apr. 2023.
23. B. Libert, S. C. Ramanna, and M. Yung. Functional commitment schemes: From polynomial commitments to pairing-based accumulators from simple assumptions. In I. Chatzigiannakis, M. Mitzenmacher, Y. Rabani, and D. Sangiorgi, editors, *ICALP 2016*, volume 55 of *LIPIcs*, pages 30:1–30:14. Schloss Dagstuhl, July 2016.
24. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, Berlin, Heidelberg, Apr. 2012.
25. W. Quach, H. Wee, and D. Wichs. Laconic function evaluation and applications. In M. Thorup, editor, *59th FOCS*, pages 859–870. IEEE Computer Society Press, Oct. 2018.
26. A. Sahai and B. R. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Berlin, Heidelberg, May 2005.
27. H. Wee. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In O. Dunkelman and S. Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 217–241. Springer, Cham, May / June 2022.
28. H. Wee. Circuit ABE with $\mathsf{poly}(\mathsf{depth}, \lambda)$-sized ciphertexts and keys from lattices. In L. Reyzin and D. Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 178–209. Springer, Cham, Aug. 2024.
29. H. Wee and D. Wichs. Candidate obfuscation via oblivious LWE sampling. In A. Canteaut and F.-X. Standaert, editors, *EUROCRYPT 2021, Part III*, volume 12698 of *LNCS*, pages 127–156. Springer, Cham, Oct. 2021.
30. H. Wee and D. J. Wu. Lattice-based functional commitments: Fast verification and cryptanalysis. In J. Guo and R. Steinfeld, editors, *ASIACRYPT 2023, Part V*, volume 14442 of *LNCS*, pages 201–235. Springer, Singapore, Dec. 2023.

A Additional Proofs

Proof of Lemma 2. Let $\mathbf{u}_i \in \{0,1\}^h, \hat{\mathbf{u}}_j \in \{0,1\}^w$ denote (row) unit vectors whose i'th and j'th entries are 1 respectively. It suffices to show that for all $i \in [h], j \in [w]$, we have:

$$\mathbf{u}_i \mathbf{X}\mathbf{Y}\hat{\mathbf{u}}_j^\top = \mathbf{u}_i(\mathrm{vec}(\mathbf{Y})^\top \otimes \mathbf{I}_h)(\mathbf{I}_w \otimes \mathrm{vec}(\mathbf{X}))\hat{\mathbf{u}}_j^\top$$

For the LHS, we have:

$$\begin{aligned}\mathbf{u}_i \mathbf{X}\mathbf{Y}\hat{\mathbf{u}}_j^\top &= \mathrm{vec}(\mathbf{Y}\hat{\mathbf{u}}_j^\top)^\top \cdot \mathrm{vec}(\mathbf{u}_i\mathbf{X}) \\ &= \mathrm{vec}(\mathbf{Y})^\top(\hat{\mathbf{u}}_j^\top \otimes \mathbf{I}_\ell) \cdot (\mathbf{I}_\ell \otimes \mathbf{u}_i)\mathrm{vec}(\mathbf{X})\end{aligned}$$

For the RHS, we have:

$$\begin{aligned}\mathbf{u}_i(\mathrm{vec}(\mathbf{Y})^\top \otimes \mathbf{I}_h)(\mathbf{I}_w \otimes \mathrm{vec}(\mathbf{X}))\hat{\mathbf{u}}_j^\top &= (1 \otimes \mathbf{u}_i)(\mathrm{vec}(\mathbf{Y})^\top \otimes \mathbf{I}_h) \cdot (\mathbf{I}_w \otimes \mathrm{vec}(\mathbf{X}))(\hat{\mathbf{u}}_j^\top \otimes 1) \\ &= \mathrm{vec}(\mathbf{Y})^\top(\mathbf{I}_{\ell w} \otimes \mathbf{u}_i) \cdot (\hat{\mathbf{u}}_j^\top \otimes \mathbf{I}_{h\ell})\mathrm{vec}(\mathbf{X})\end{aligned}$$

To interpolate the two, we have:

$$\begin{aligned}(\hat{\mathbf{u}}_j^\top \otimes \mathbf{I}_\ell) \cdot (\mathbf{I}_\ell \otimes \mathbf{u}_i) &= (\hat{\mathbf{u}}_j^\top \otimes \mathbf{I}_\ell \otimes 1) \cdot (1 \otimes \mathbf{I}_\ell \otimes \mathbf{u}_i) \\ &= (\mathbf{I}_w \otimes \mathbf{I}_\ell \otimes \mathbf{u}_i) \cdot (\hat{\mathbf{u}}_j^\top \otimes \mathbf{I}_\ell \otimes \mathbf{I}_h) \\ &= (\mathbf{I}_{\ell w} \otimes \mathbf{u}_i) \cdot (\hat{\mathbf{u}}_j^\top \otimes \mathbf{I}_{h\ell})\end{aligned}$$

This completes the proof.

B Dual Commitment to Circuits

We present a "dual" of the scheme in Section 3.4.

Lemma 8. *There exist efficient algorithms* $(\mathsf{Com}^{\mathsf{c}}, \mathsf{Ver}^{\mathsf{c}}, \mathsf{Open}^{\mathsf{c}})$ *where*

- $\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, x, 1^d)$*: on input* $x \in \{0,1\}^\ell$*, outputs* $\mathbf{C}_{x,d} \in \mathbb{Z}_q^{n \times m}$*;*
- $\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, f)$*: on input* $f \in \mathscr{F}_{\ell,d,s}$*, outputs* $\mathbf{V}_f \in \mathbb{Z}_q^{m \times m}$*;*
- $\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, x, f)$*: on input* $f \in \mathscr{F}_{\ell,d,s}, x \in \{0,1\}^\ell$*, outputs* $\mathbf{Z}_{f,x} \in \mathbb{Z}_q^{m \times m}$*.*

For all $\mathsf{pp}, \ell, d, s \in \mathbb{N}, f \in \mathscr{F}_{\ell,d,s}, x \in \{0,1\}^\ell$*, the matrices* $\mathbf{C}_{x,d} \leftarrow \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, x, 1^d), \mathbf{V}_f \leftarrow \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, f), \mathbf{Z}_{f,x} \leftarrow \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f, x)$ *satisfy:*

$$\begin{aligned}\mathbf{C}_{x,d} \cdot \mathbf{V}_f &= f(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_{f,x} \\ \|\mathbf{V}_f\| &\le O(\|\mathbf{T}\| \cdot m^9) \\ \|\mathbf{Z}_{f,x}\| &\le \ell \cdot O(\|\mathbf{T}\| \cdot m^{12})^d\end{aligned}$$

Proof (sketch). As before, we consider leveled circuits of multiplicative depth d. We present the construction in Fig 4, described recursively over d. The analysis is analogous to that for Lemma 7; the main difference lies in handling multiplication gates, which we describe below.

Multiplication gate. Suppose $f = f_0 \cdot f_1$, where f_0, f_1 are circuits of depth $d-1$. By recursion, we have

$$\mathbf{C}_{x,d-1} \cdot \mathbf{V}_{f_0} = f_0(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_0 \tag{23}$$

$$\mathbf{C}_{x,d-1} \cdot \mathbf{V}_{f_1} = f_1(x)\mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_1 \tag{24}$$

Adding (23) $\cdot \mathbf{G}^{-1}(\mathbf{C}_{x,d-1})\mathbf{V}_{f_1}$ to (24) $\cdot f_0(x)$, we have

$$\mathbf{C}_{x,d-1} \cdot \mathbf{V}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{x,d-1}) \cdot \mathbf{V}_{f_1} = f_0(x)f_1(x)\mathbf{G} - \mathbf{B} \cdot \overbrace{\left(\mathbf{Z}_0 \cdot \mathbf{G}^{-1}(\mathbf{C}_{x,d-1})\mathbf{V}_{x,f_1} + f_0(x)\mathbf{Z}_1\right)}^{=\mathbf{Z}'}$$

Input gates: $\pi_i(x) := \mathbf{u}_i(x,1)^\top, i \in [\ell+1]$

$\underline{\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, x, 1^0)}$
output $\mathbf{C}_{x,0} := \mathsf{Com}^{\mathsf{vc}}(\mathsf{pp}, (x,1))$

$\underline{\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, \pi_i, 1^0)}$
$\mathbf{V}_{\ell+1} := \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, 1^{\ell+1})$
output $\mathbf{V}_{x,0} := \mathbf{V}_{\ell+1}(\mathbf{u}_i^\top \otimes \mathbf{I}_m)$

$\underline{\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, x, \pi_i)}$
$\mathbf{Z} := \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}, (x,1))$
output $\mathbf{Z}_{\pi_i,x} := \mathbf{Z}(\mathbf{u}_i^\top \otimes \mathbf{I}_m)$

Subtraction gate:

$\underline{\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, f = f_0 - f_1)}$
$\mathbf{V}_{f_\beta} := \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, f_\beta), \beta = 0,1$
output $\mathbf{V}_f := \mathbf{V}_{f_0} - \mathbf{V}_{f_1}$

$\underline{\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f = f_0 - f_1, x)}$
$\mathbf{Z}_\beta := \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, f_\beta, x), \beta = 0,1$
output $\mathbf{Z}_{f,x} := \mathbf{Z}_0 - \mathbf{Z}_1$

Multiplication gate:

$\underline{\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, x, 1^d)}$
$\mathbf{C}_{x,d-1} := \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}, x, 1^{d-1})$
$\mathbf{C}^\times := \mathsf{bits}(\mathbf{C}_{x,d-1}) \otimes \mathbf{C}_{x,d-1}$
output $\mathbf{C}_{x,d} := \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{C}^\times)$

$\underline{\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, f = f_0 \cdot f_1)}$
$\mathbf{V}_{f_\beta} := \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}, f_\beta), \beta = 0,1$
$\mathbf{V}^\times := (\mathbf{I}_m \otimes \mathrm{vec}(\mathbf{V}_{f_0}))\mathbf{V}_{f_1}$
$\mathbf{V}^{\mathsf{mx}}_{m^3} := \mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^{m^3})$
output $\mathbf{V}_f := \mathbf{V}^{\mathsf{mx}}_{m^3} \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)$

$\underline{\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, x, f = f_0 \cdot f_1)}$
$\mathbf{Z}_\beta := \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}, x, f_\beta), \beta = 0,1$
$\mathbf{Z}^\times := \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{C}^\times)$
$\mathbf{Z}' := \mathbf{Z}_0 \cdot \mathbf{G}^{-1}(\mathbf{C}_{x,d-1})\mathbf{V}_{f_1} + f_0(x)\mathbf{Z}_1$
output $\mathbf{Z}_{f,x} := \mathbf{Z}^\times \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times) + \mathbf{Z}'$

Fig. 4. A dual commitment to circuits

On the other hand, applying (8) to $\mathbf{V}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{x,d-1})$ as before, we have

$$\mathbf{C}_{x,d-1} \cdot \mathbf{V}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{x,d-1}) \cdot \mathbf{V}_{f_1} = \overbrace{(\mathsf{bits}(\mathbf{C}_{x,d-1}) \otimes \mathbf{C}_{x,d-1})}^{=\mathbf{C}^\times} \cdot \overbrace{(\mathbf{I}_m \otimes \mathrm{vec}(\mathbf{V}_{f_0}))\mathbf{V}_{f_1}}^{=\mathbf{V}^\times}$$

Therefore,

$$\mathbf{C}^\times \cdot \mathbf{V}^\times = f_0(x) f_1(x) \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}' \tag{25}$$

From correctness of $(\mathsf{Com}^{\mathsf{mx}}, \mathsf{Open}^{\mathsf{mx}}, \mathsf{Ver}^{\mathsf{mx}})$, we have:

$$\mathbf{C}_f \cdot \mathbf{V}^{\mathsf{mx}}_{m^3} = \mathbf{C}^\times \cdot \mathbf{G}_{m^3} - \mathbf{B} \cdot \mathbf{Z}^\times$$

where $\|\mathbf{Z}^\times\| \le O(\|\mathbf{T}\| \cdot m^8)$. Multiplying both sides by $\mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)$ and combining with (25) yields:

$$\mathbf{C}_f \cdot \overbrace{\mathbf{V}^{\mathsf{mx}}_{m^3} \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times)}^{=\mathbf{V}_{x,d}} = f_0(x) f_1(x) \mathbf{G} - \mathbf{B} \cdot \Big(\overbrace{\mathbf{Z}^\times \cdot \mathbf{G}^{-1}_{m^3}(\mathbf{V}^\times) + \mathbf{Z}'}^{=\mathbf{Z}_{f,x}}\Big)$$

as desired. □

C Instantiations from Decomposed LWE

In this section, we show how to modify our KP-ABE and CP-ABE schemes to achieve selective security under the decomposed LWE assumption introduced in [1]. The key insight is that the top part $\overline{\mathbf{T}}$ of the $2m^2$-succinct LWE trapdoor is only used to compute $(\mathbf{I}_{2m^2} \otimes \mathbf{sB}) \cdot \overline{\mathbf{T}}$ in our ABE schemes. Therefore, instead of giving out $\overline{\mathbf{T}}$ in public parameters, we simply give out $(\mathbf{I}_{2m^2} \otimes \mathbf{sB}) \cdot \overline{\mathbf{T}}$ in the ABE ciphertext; this preserves $|\mathsf{ct}| = \mathsf{poly}(d, \lambda)$ while allowing us to prove security from a weaker assumption that does not prefer to trapdoors or Gaussian pre-images.

C.1 Decomposed LWE assumption

We can restate the ℓ-succinct LWE assumption as follows. Sample $\mathbf{B} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{W} \in \mathbb{Z}_q^{\ell n\times m}, \mathbf{R} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_0}^{m\times \ell m}$, and $\overline{\mathbf{T}} \leftarrow (\mathbf{I}_\ell \otimes \mathbf{B})^{-1}(\mathbf{WR} + \mathbf{I}_\ell \otimes \mathbf{G})$.[5] The ℓ-succinct LWE assumption stipulates that

$$(\mathbf{B}, \mathbf{sB} + \mathbf{e}, \mathbf{W}, \mathbf{R}, \overline{\mathbf{T}}) \approx_c (\mathbf{B}, \mathbf{c}, \mathbf{W}, \mathbf{R}, \overline{\mathbf{T}})$$

where $\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z},\chi}^m, \mathbf{c} \leftarrow \mathbb{Z}_q^m$.

In the decomposed LWE assumption, the distinguisher gets $(\mathbf{I}_\ell \otimes (\mathbf{sB}+\mathbf{e}))\cdot\overline{\mathbf{T}} \approx (\mathbf{I}_\ell \otimes \mathbf{s})(\mathbf{WR}+\mathbf{I}_\ell\otimes\mathbf{G})$ instead of $(\mathbf{sB}+\mathbf{e}, \overline{\mathbf{T}})$. If we parse $\mathbf{W}, \mathbf{R}$ as $\mathbf{W}_1, \ldots, \mathbf{W}_\ell \in \mathbb{Z}_q^{n\times m}, \mathbf{R}_1, \ldots, \mathbf{R}_\ell \in \mathbb{Z}_q^{m\times m}$, then we can write $(\mathbf{I}_\ell \otimes \mathbf{s})(\mathbf{WR} + \mathbf{I}_\ell \otimes \mathbf{G})$ as $\mathbf{s}(\mathbf{W}_i\mathbf{R}_j + \delta_{ij}\mathbf{G})$. In the rest of this section, it is more convenient to sample $\mathbf{W} \in \mathbb{Z}_q^{n\times \ell m}$ (instead of $\mathbb{Z}_q^{\ell n\times m}$), and we think of $\overline{\mathbf{T}} \leftarrow \mathbf{B}^{-1}(\mathbf{W}(\mathbf{I}_\ell \otimes \mathbf{R}) + \mathrm{vec}(\mathbf{I}_\ell) \otimes \mathbf{G})$.

The ℓ-decomposed LWE assumption [1]. Sample $\mathbf{W} \in \mathbb{Z}_q^{n\times \ell m}, \mathbf{R} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_0}^{m\times \ell m}$. The ℓ-decomposed LWE assumption stipulates that

$$(\mathbf{B}, \mathbf{s}(\mathbf{W}(\mathbf{I}_\ell \otimes \mathbf{R}) + \mathrm{vec}(\mathbf{I}_\ell) \otimes \mathbf{G}) + \mathbf{e}, \mathbf{W}, \mathbf{R}) \approx_c (\mathbf{B}, \mathbf{c}, \mathbf{W}, \mathbf{R})$$

where $\mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z},\chi}^{\ell^2 m}, \mathbf{c} \leftarrow \mathbb{Z}_q^{\ell^2 m}$. As in our main result, we are mostly interested in $2m^2$-decomposed LWE.

C.2 Succinct commitments, revisited

Henceforth, we write

$$\mathsf{pp}_d := (\mathbf{W}, \mathbf{R}, \hat{\mathbf{B}})$$

where $\mathbf{W} \in \mathbb{Z}_q^{n\times 2m^3}, \mathbf{R} \leftarrow \mathcal{D}_{\mathbb{Z},\sigma_0}^{m\times 2m^3}$ and $\hat{\mathbf{B}} := \mathbf{W}(\mathbf{I}_{2m^2} \otimes \mathbf{R}) + \mathrm{vec}(\mathbf{I}_{2m^2}) \otimes \mathbf{G}) \in \mathbb{Z}_q^{n\times 4m^5}$. We restate our succinct commitment schemes in Section 3 in the setting where (i) we replace pp with pp_d, (ii) we replace $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ in the verification relation with $\hat{\mathbf{B}} \in \mathbb{Z}_q^{n\times 4m^5}$, and (iii) we increase the height of the openings $\mathbf{Z}, \mathbf{Z}_{f,x}$ from m to $4m^5$. The constructions and the analysis –apart for the base case for the matrix commitment– are the same as that in Section 3.

Lemma 9 (matrix commitment). *There exist efficient algorithms* $(\mathsf{Com}^{\mathsf{mx}}, \mathsf{Ver}^{\mathsf{mx}}, \mathsf{Open}^{\mathsf{mx}})$ *where*

- $\mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}_d, \mathbf{M})$*: on input* $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$*, outputs* $\mathbf{C} \in \mathbb{Z}_q^{n\times m}$*;*
- $\mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}_d, 1^L)$*: on input* 1^L*, outputs* $\mathbf{V}_L^{\mathsf{mx}} \in \mathbb{Z}_q^{m\times L\lceil\log q\rceil}$*;*
- $\mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}_d, \mathbf{M})$*: on input* $\mathbf{M} \in \mathbb{Z}_q^{n\times L}$*, outputs* $\mathbf{Z} \in \mathbb{Z}_q^{4m^5\times L\lceil\log q\rceil}$*.*

For all $\mathsf{pp}_d, L \in \mathbb{N}, \mathbf{M} \in \mathbb{Z}_q^{n\times L}$*, the matrices* $\mathbf{C} \leftarrow \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}_d, \mathbf{M}), \mathbf{V}_L^{\mathsf{mx}} \leftarrow \mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}_d, 1^L), \mathbf{Z} \leftarrow \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}_d, \mathbf{M})$ *satisfy:*

$$\begin{aligned} \mathbf{C}\cdot\mathbf{V}_L^{\mathsf{mx}} &= \mathbf{M}\cdot\mathbf{G}_L - \hat{\mathbf{B}}\cdot\mathbf{Z} \\ \|\mathbf{V}_L^{\mathsf{mx}}\| &\le O(\|\mathbf{R}\|\cdot m^4\log q) \\ \|\mathbf{Z}\| &\le O(\|\mathbf{R}\|\cdot m^7\log q\cdot\log L) \end{aligned}$$

The running times of the algorithms are $L\log L\cdot\mathsf{poly}(m)$*.*

Proof. The construction and the analysis are the same as before in Lemma 5, except for the base case $L = 2m$, which we modify as follows:

$\underline{\mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})}$: output $\mathbf{C} := \mathbf{W}(\mathsf{bits}(\mathbf{M})^\top \otimes \mathbf{I}_m)$
$\underline{\mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}, 1^{2m})}$: output $\mathbf{V}_L^{\mathsf{mx}} := -\mathbf{R}\cdot\mathbf{J}_{2m}$
$\underline{\mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}, \mathbf{M})}$: output $\mathbf{Z} := (\mathsf{bits}(\mathbf{M})^\top \otimes \mathbf{I}_{2m^3})\cdot\mathbf{J}_{2m}$

[5] That is, $(\mathbf{I}_\ell \otimes \mathbf{B})\cdot\overline{\mathbf{T}} = \mathbf{WR} + \mathbf{I}_\ell \otimes \mathbf{G}$. This means $[\mathbf{I}_\ell \otimes \mathbf{B} \mid \mathbf{W}]\cdot\begin{pmatrix}\overline{\mathbf{T}}\\ -\mathbf{R}\end{pmatrix} = \mathbf{I}_\ell \otimes \mathbf{G}$; that is, $\begin{pmatrix}\overline{\mathbf{T}}\\ -\mathbf{R}\end{pmatrix}$ corresponds to the trapdoor $\mathbf{T}$ in our earlier statement of ℓ-succinct LWE.

Correctness uses the fact that for all $\mathbf{x} \in \{0,1\}^{2m^2}$, we have:

$$\mathbf{W}(\mathbf{x}^\top \otimes \mathbf{I}_m) \cdot (-\mathbf{R}) = \mathbf{x} \otimes \mathbf{G} - \hat{\mathbf{B}} \cdot (\mathbf{x}^\top \otimes \mathbf{I}_{2m^3})$$

The latter in turn follows from (i) $(\mathbf{x}^\top \otimes \mathbf{I}_m)\mathbf{R} = (\mathbf{I}_{2m^2} \otimes \mathbf{R})(\mathbf{x}^\top \otimes \mathbf{I}_{2m^3})$, and (ii) $\mathrm{vec}(\mathbf{I}_{2m^2})^\top (\mathbf{x}^\top \otimes \mathbf{I}_{2m^2}) = \mathbf{x}$.

Lemma 10 (vector commitment). *Consider*

- $\mathsf{Com}^{\mathsf{vc}}(\mathsf{pp}_d, \mathbf{x} \in \mathbb{Z}_q^\ell)$*: outputs* $\mathbf{C} := \mathsf{Com}^{\mathsf{mx}}(\mathsf{pp}_d, \mathbf{x} \otimes \mathbf{I}_n) \in \mathbb{Z}_q^{n \times m}$.
- $\mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp}_d, 1^\ell)$*: outputs* $\mathbf{V}_\ell := \mathsf{Ver}^{\mathsf{mx}}(\mathsf{pp}_d, 1^{\ell n}) \in \mathbb{Z}_q^{m \times \ell m}$.
- $\mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}_d, \mathbf{x})$*: outputs* $\mathbf{Z} := \mathsf{Open}^{\mathsf{mx}}(\mathsf{pp}_d, \mathbf{x} \otimes \mathbf{I}_n) \in \mathbb{Z}_q^{4m^5 \times \ell m}$.

For all $\mathsf{pp}_d, \ell \in \mathbb{N}, \mathbf{x} \in \mathbb{Z}_q^\ell$*, the matrices* $\mathbf{C} \leftarrow \mathsf{Com}^{\mathsf{vc}}(\mathsf{pp}_d, \mathbf{x}), \mathbf{V}_\ell \leftarrow \mathsf{Ver}^{\mathsf{vc}}(\mathsf{pp}_d, 1^\ell), \mathbf{Z} \leftarrow \mathsf{Open}^{\mathsf{vc}}(\mathsf{pp}_d, \mathbf{x})$ *satisfy:*

$$\begin{aligned} \mathbf{C} \cdot \mathbf{V}_\ell &= \mathbf{x} \otimes \mathbf{G} - \hat{\mathbf{B}} \cdot \mathbf{Z} \\ \|\mathbf{V}_\ell\| &\le O(\|\mathbf{R}\| \cdot m^4 \log q) \\ \|\mathbf{Z}\| &\le O(\|\mathbf{R}\| \cdot \log \ell \cdot m^7 \log q) \end{aligned}$$

Lemma 11. *There exist efficient algorithms* $(\mathsf{Com}^{\mathsf{c}}, \mathsf{Ver}^{\mathsf{c}}, \mathsf{Open}^{\mathsf{c}})$ *where*

- $\mathsf{Com}^{\mathsf{c}}(\mathsf{pp}_d, f)$*: on input* $f \in \mathscr{F}_{\ell,d,s}$*, outputs* $\mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$*;*
- $\mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}_d, x, 1^d)$*: on input* $x \in \{0,1\}^\ell$*, outputs* $\mathbf{V}_{x,d} \in \mathbb{Z}_q^{m \times m}$*;*
- $\mathsf{Open}^{\mathsf{c}}(\mathsf{pp}_d, f, x)$*: on input* $f \in \mathscr{F}_{\ell,d,s}, x \in \{0,1\}^\ell$*, outputs* $\mathbf{Z}_{f,x} \in \mathbb{Z}_q^{4m^5 \times m}$.

For all $\mathsf{pp}_d, \ell, d, s \in \mathbb{N}, f \in \mathscr{F}_{\ell,d,s}, x \in \{0,1\}^\ell$*, the matrices* $\mathbf{C}_f \leftarrow \mathsf{Com}^{\mathsf{c}}(\mathsf{pp}_d, f), \mathbf{V}_{x,d} \leftarrow \mathsf{Ver}^{\mathsf{c}}(\mathsf{pp}_d, x, 1^d), \mathbf{Z}_{f,x} \leftarrow \mathsf{Open}^{\mathsf{c}}(\mathsf{pp}_d, f, x)$ *satisfy:*

$$\begin{aligned} \mathbf{C}_f \cdot \mathbf{V}_{x,d} &= f(x)\mathbf{G} - \hat{\mathbf{B}} \cdot \mathbf{Z}_{f,x} \\ \|\mathbf{V}_{x,d}\| &\le O(\|\mathbf{R}\| \cdot m^9) \\ \|\mathbf{Z}_{f,x}\| &\le \ell \cdot O(\|\mathbf{R}\| \cdot m^{12})^d \end{aligned}$$

C.3 KP-ABE and CP-ABE schemes

Next, we modify our KP-ABE and CP-ABE schemes to achieve selective security under $2m^2$-decomposable LWE. As before, we achieve $|\mathsf{mpk}|, |\mathsf{ct}|, |\mathsf{sk}| = \mathsf{poly}(d, \lambda)$. The idea is to replace $(\mathsf{pp}, \mathbf{B})$ with $(\mathsf{pp}_d, \hat{\mathbf{B}})$.

KP-ABE. Our KP-ABE scheme for depth d circuits over ℓ-bit inputs is as follows, omitting error terms in the ciphertext:

$$\begin{aligned} \mathsf{mpk} &= \overbrace{\mathbf{W}, \mathbf{R}, \hat{\mathbf{B}}}^{\mathsf{pp}_d}, \mathbf{B}_1 \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{p} \leftarrow \mathbb{Z}_q^n \\ \mathsf{ct}_x &= \mathbf{s}\hat{\mathbf{B}}, \mathbf{s}(\mathbf{B}_1 + \mathbf{C}_x), \mathbf{s} \cdot \mathbf{p}^\top + \mu \cdot \lfloor \tfrac{q}{2} \rfloor \\ \mathsf{sk}_f &= \mathbf{k}_f^\top \text{ s.t. } [\hat{\mathbf{B}} \mid \mathbf{A}_f] \cdot \mathbf{k}_f^\top = \mathbf{p}^\top, \quad \mathbf{A} := -\mathbf{B}_1 \mathbf{V}_\ell, \mathbf{A}_f := \mathsf{EvalF}(\mathbf{A}, f) \end{aligned}$$

where $\mathbf{C}_x, \mathbf{V}_\ell$ are computed using our vector commitment scheme. Combining $\mathbf{C}_x \mathbf{V}_\ell = \mathbf{x} \otimes \mathbf{G} - \hat{\mathbf{B}}\mathbf{Z}_{\mathbf{x}}$ and $\mathbf{A} = -\mathbf{B}_1 \mathbf{V}_\ell$, we have:

$$[\hat{\mathbf{B}} \mid \mathbf{B}_1 + \mathbf{C}_{\mathbf{x}}] \cdot \begin{pmatrix} -\mathbf{Z}_{\mathbf{x}} \\ -\mathbf{V}_\ell \end{pmatrix} = \mathbf{A} - \mathbf{x} \otimes \mathbf{G}$$

$$[\hat{\mathbf{B}} \mid \mathbf{B}_1 + \mathbf{C}_{\mathbf{x}}] \cdot \begin{pmatrix} -\mathbf{Z}_{\mathbf{x}} \\ -\mathbf{V}_\ell \end{pmatrix} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$$

CP-ABE. Our CP-ABE scheme for depth d circuits over ℓ-bit inputs is as follows, omitting error terms in the ciphertext:

$$\begin{aligned}
\mathsf{mpk} &= \overbrace{\mathbf{W}, \mathbf{R}, \hat{\mathbf{B}}}^{\mathsf{pp}_d}, \mathbf{B}_1 \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{p} \leftarrow \mathbb{Z}_q^n \\
\mathsf{ct}_f &= \mathbf{s}\hat{\mathbf{B}}, \mathbf{s}(\mathbf{B}_1 + \mathbf{C}_f), \mathbf{s}\cdot\mathbf{p}^\top + \mu \cdot \lfloor \tfrac{q}{2} \rfloor \\
\mathsf{sk}_x &= \mathbf{k}_x^\top \text{ s.t. } [\hat{\mathbf{B}} \mid \mathbf{A}_x]\cdot\mathbf{k}_x^\top = \mathbf{p}^\top, \quad \mathbf{A}_x := -\mathbf{B}_1\mathbf{V}_{x,d}
\end{aligned}$$

where $\mathbf{C}_f, \mathbf{V}_{x,d}$ are computed using our commitment scheme for circuits. We will set the LWE parameters so that $m = \mathsf{poly}(d, \lambda)$, which yields $|\mathsf{mpk}|, |\mathsf{ct}_f|, |\mathsf{sk}_x| = \mathsf{poly}(d, \lambda)$. Combining $\mathbf{C}_f\mathbf{V}_{x,d} = f(x)\mathbf{G} - \hat{\mathbf{B}}\mathbf{Z}_{f,x}$ and $\mathbf{A}_x = -\mathbf{B}_1\mathbf{V}_{x,d}$, we have:

$$[\hat{\mathbf{B}} \mid \mathbf{B}_1 + \mathbf{C}_f] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix} = \mathbf{A}_x - f(x)\mathbf{G} \tag{26}$$

This means that starting from $\mathbf{s}(\mathbf{B}_1 + \mathbf{C}_f)$, we can derive $\mathbf{s}\mathbf{A}_x$ whenever $f(x) = 0$, which combined with $\mathbf{k}_x^\top$ allows us to recover $\mathbf{s}\cdot\mathbf{p}^\top$ and thus μ. The security reduction to $2m^2$-decomposable LWE samples a low-norm $\mathbf{U} \leftarrow \{0,1\}^{4m^5\times m}$ and programs $\mathbf{B}_1 := \hat{\mathbf{B}}\mathbf{U} - \mathbf{C}_f$. This allows the reduction to simulate the challenge ciphertext. From (6), we have

$$\mathbf{A}_x = \hat{\mathbf{B}} \cdot \overbrace{[\mathbf{I} \mid \mathbf{U}] \cdot \begin{pmatrix} -\mathbf{Z}_{f,x} \\ -\mathbf{V}_{x,d} \end{pmatrix}}^{\text{small}} + f(x)\mathbf{G}$$

This means the reduction has a trapdoor for the matrix $[\hat{\mathbf{B}} \mid \mathbf{A}_x]$ since $f(x) \neq 0$, which it can then use to answer key queries.