Improved (Hierarchical) Inner-Product Encryption from Lattices

Keita Xagawa

NTT Secure Platform Laboratories
xagawa.keita@lab.ntt.co.jp

Abstract. Inner-product encryption (IPE) provides fine-grained access control and has attractive applications. Agrawal, Freeman, and Vaikuntanathan (Asiacrypt 2011) proposed the first IPE scheme from lattices by twisting the identity-based encryption (IBE) scheme by Agrawal, Boneh, and Boyen (Eurocrypt 2010). Their IPE scheme supports inner-product predicates over R^μ, where the ring is $R = \mathbb{Z}_q$. Several applications require the ring R to be exponentially large and, thus, they set $q = 2^{O(n)}$ to implement such applications. This choice results in the AFV IPE scheme with public parameters of size $O(\mu n^2 \lg^3 q) = O(\mu n^5)$ and ciphertexts of size $O(\mu n \lg^3 q) = O(\mu n^4)$, where n is the security parameter. Hence, this makes the scheme impractical, as they noted.
We address this efficiency issue by "untwisting" their twist and providing another twist. Our scheme supports inner-product predicates over R^μ where $R = \mathrm{GF}(q^n)$ instead of $\mathbb{Z}_q$. Our scheme has public parameters of size $O(\mu n^2 \lg^2 q)$ and ciphertexts of size $O(\mu n \lg^2 q)$. Since the cardinality of $\mathrm{GF}(q^n)$ is inherently exponential in n, we have no need to set q as the exponential size for applications.
As side contributions, we extend our IPE scheme to a hierarchical IPE (HIPE) scheme and propose a fuzzy IBE scheme from IPE. Our HIPE scheme is more efficient than that developed by Abdalla, De Caro, and Mochetti (Latincrypt 2012). Our fuzzy IBE is secure under a much weaker assumption than that employed by Agrawal et al. (PKC 2012), who constructed the first lattice-based fuzzy IBE scheme.
Keywords. predicate encryption, (hierarchical) inner-product encryption, lattices, learning with errors, full-rank difference encoding, pseudo-commutativity.

1 Introduction

Background: Predicate encryption (PE) gives fine-grained access control beyond identity-based encryption (IBE). In a PE scheme, a receiver corresponding to a *key attribute* v can decrypt a ciphertext corresponding to a *ciphertext attribute* w if and only if $\mathcal{P}(v, w) = 1$, where $\mathcal{P}$ is a predicate.

Katz, Sahai, and Waters [30] introduced inner-product encryption (IPE), which is PE that supports the inner-product predicate: that is, predicate $\mathcal{P}^{\mathsf{IPE}} : R^\mu \times R^\mu \to \{0, 1\}$, where R is a finite ring, defined as $\mathcal{P}^{\mathsf{IPE}}(\vec{v}, \vec{w}) = 1$ if and only if $\vec{w}^\top \vec{v} = 0$. They showed that several predicates, for example, equalities, hidden-vector predicates, polynomial evaluations, and CNF/DNF formulae, can be encoded as an inner product that exemplifies the serviceability of IPE. Following their work and by exploiting the properties of the pairing on composite-number or prime order groups, recent studies on IPE

have enhanced security or introduced compact schemes [30,36,31,37,10,40,38,39], and have left an open problem of constructing IPE from other assumptions, say, factoring, decisional Diffie-Hellman (DDH), or the learning with errors (LWE) assumptions.

In 2011, Agrawal, Freeman, and Vaikuntanathan [6] overcame the hurdle, i.e., the problem of constructing IPE *without pairing*. They proposed the first IPE scheme based on the LWE assumption [46] and left three open problems: improving security, efficiency, and functionality.

Let us focus on the second problem, the efficiency issue. Their scheme supports an inner-product predicate over $R = \mathbb{Z}_q$, and has public parameters of size $\Theta(\mu n^2 \lg^3 q)$ and ciphertexts of size $\Theta(\mu n \lg^3 q + \ell \lg q)$, where n is the security parameter, μ is the dimension of the vector space, and ℓ is the length of a message. (In what follows, we will ignore $\Theta(\ell \lg q)$.) This seems satisfactory for actual use.

In several applications of IPE, we require exponentially large R (see below). To implement such applications, Agrawal et al. set $q = 2^{O(n)}$ [6, Section 6]. This setting results in the length of ciphertext $\Theta(\mu n^4)$, which shows the impracticality of the scheme in the real world.

Motivated by applications: We were motivated to improve the efficiency by applications of IPE that require large R, which we discuss here. Roughly speaking, we require the ring R to be exponentially large in order to implement an application when we have to take AND (logical conjunction) of predicates by using the technique proposed by Katz, Sahai, and Waters [30][1]. Since the existing pairing-based IPE serves inner products over the ring $R = \mathbb{Z}_q$ or $\mathbb{Z}_N$, where q, N is an exponential of a security parameter, there are no problematic issues. Unfortunately, the exponential magnitude of R makes the AFV IPE scheme impractical, since the length of the ciphertext is the cubic order of $\lg(\#R) = \lg q$.

We have several attractive applications that are implemented by IPE with logical conjunctions. These include CNF formulae [30], hidden vector encryption [15], which serves a comparison and a range query on a small set, and wild-carded IBE [1]. We will review and discuss the applications of IPE schemes in the full version.

Moreover, for a realistic scenario, we will treat a colossal set as a domain of the predicate, e.g., one billion users ($10^9 \approx 2^{30}$), addresses of IPv6 (2^{128}), verification keys of one-time signature (2^{128}–), and hash values of SHA3 candidates (2^{256}–2^{512}). In such a situation, even the equality predicate requires logical conjunctions to split them into chunks in R.

Hence, we should make IPE efficient even for exponentially large R for the IPE applications.

[1] Suppose that we have two implementations of two predicates f and g; one is embedded as $\vec{v}_f$ and $\vec{w}_f$, and the other is embedded as $\vec{v}_g$ and $\vec{w}_g$. The Katz-Sahai-Waters (KSW) technique embeds $f \wedge g$ into two vectors $\vec{v}_{f\wedge g} = (\vec{v}_f, \vec{w}_g)$ and $\vec{w}_{f\wedge g} = (r_f \vec{v}_f, r_g \vec{w}_g)$, where r_f, r_g are chosen uniformly at random from R. The inner product of $\vec{v}_{f\wedge g}$ and $\vec{w}_{f\wedge g}$ is $r_f \vec{w}_f^{\top} \vec{v}_f + r_g \vec{w}_g^{\top} \vec{v}_g$. If the two inner products are 0, that is, two predicates f and g are true, then the inner product becomes 0. The inversion is not true; if not, then the inner product is not 0 without probability, say, $1/\#R$. This shows that R should be exponentially large, say, at least 2^{80} from the security requirement.

1.1 Our Contribution

Our main contribution is to improve the efficiency of the AFV IPE scheme. More formally, we construct an IPE scheme under the LWE assumption, which supports an inner-product predicate over the field $\mathrm{GF}(q^n)$ instead of $\mathbb{Z}_q$ and has public parameters of size $\Theta(\mu n^2 \lg^2 q)$ and ciphertexts of size $\Theta(\mu n \lg^2 q + \ell \lg q)$. Since the cardinality of $\mathrm{GF}(q^n)$ is $q^n = 2^{\Omega(n)}$, and $\mathrm{GF}(q^n)$ is a field, we can set $q = \mathrm{poly}(n)$ even for the above applications. We note that Agrawal et al. [6, Section 6] expected the *ring-LWE* assumption [32] to resolve the issue, but we solve it *without the ring-LWE assumption*.

In addition, we have two side contributions; One is an extension of *hierarchical inner-product encryption* (HIPE) [36], which implies spatial encryption (SE) [14,29,21]. We apply our techniques to again drastically improve the existing HIPE scheme from lattices [3] in the case of exponentially large R. The other is a fuzzy IBE (FIBE) scheme over a small universe $\{0,1\}$ from IPE under the LWE assumption with *conservative* parameters, whereas the existing fuzzy IBE scheme from lattices are under the LWE assumption with *sub-exponential* parameters [5].

Comparison: Since the description size of the public parameters is n times that of ciphertexts, we compare the efficiency of the schemes by the length of the ciphertext. For simplicity, we let L_{ours} and L_{AFV} denote the lengths of ciphertexts of our scheme and the AFV scheme, respectively.

When $q = \mathrm{poly}(n)$, our scheme improves the size by only a factor of $\lg q = O(\lg n)$ ($L_{\mathrm{ours}} = \Theta(\mu n \lg^2 q)$ and $L_{\mathrm{AFV}} = \Theta(\mu n \lg^3 q)$). Moreover, if we restrict $\vec{v}$ in a small domain, say, $\{0,1\}^\mu$, then $L_{\mathrm{AFV}} = \Theta(\mu n \lg^2 q)$, and there is no improvement.

On the other hand, if we set $\#R = 2^{\Theta(n)}$ to implement applications, the improvement is drastic: $L_{\mathrm{ours}} = \Theta(\mu n \lg^2 q)$ since $\#\,\mathrm{GF}(q^n) = 2^{\Omega(n)}$ and $L_{\mathrm{AFV}} = \Theta(\mu n \lg^3 q) = \Theta(\mu n^4)$ since they need to set $q = 2^{\Theta(n)}$. In this case, efficiency is improved by a factor of $\tilde{O}(n^3)$.

Next, we compare the FIBE schemes with a small universe; that is, their identities are binary vectors of length N. Agrawal, Boyen, Vaikuntanathan, Voulgaris, and Wee [5] proposed a FIBE scheme based on the LWE assumption with *sub-exponential* parameters. They restricted $N = n^\epsilon$ with $\epsilon \in (0, 1/2)$ in order to obtain the security under the hardness of lattice problems. Their scheme is based on the worst-case hardness of lattice problems of approximation factor $2^{O(N)} = 2^{O(n^\epsilon)}$ with a subexponential-time algorithm. The length of their ciphertext is $\Theta(Nm \lg q) = \Theta(N^2 n \lg^2 n)$.

On the contrary, our scheme enjoys flexible $N = \mathrm{poly}(n)$ and a weaker assumption, which is the worst-case hardness of lattice problem of approximation factor $\tilde{O}(n^{4.5})$. The length of our ciphertext is $O(N^2 n \lg^2 n)$, which is the same as theirs.

We note that Agrawal et al. also extended their scheme to support identity space $(\mathbb{Z}_q^n)^N$ without changing parameters or the assumption (see [5, Appendix B]).

On the ring-LWE assumption: We finally note that there are the variants of the ABB IBE schemes based on the ring-LWE assumption and the variants of the AFV IPE scheme also [35,34], which yield certain exponentially large R. Our technique is orthogonal to their techniques and improves the variants of the AFV IPE scheme by a factor of $\lg q$. We will describe concrete schemes in the full version.

1.2 Related Works

IPE was introduced by Katz, Sahai, and Waters [30], who gave a fully attribute-hiding but selectively secure IPE scheme based on the composite-order pairings. Following them, several researchers proposed (H)IPE schemes based on the pairings [36,31,37,10,38,39].

On IPE based on lattices, Agrawal et al. [6] constructed the first IPE scheme which is selectively secure and weakly attribute hiding under the LWE assumption. Another study on a lattice-based HIPE scheme was done by Abdalla, De Caro, and Mochetti [3], who extended the AFV IPE scheme to a HIPE scheme. They also proposed two extensions of the HIPE scheme, a wild-carded IBE scheme and a CCA secure HIPE scheme. The CCA2 construction exemplifies the requirement of large R, since, in the construction, the attribute space of the basic scheme includes a one-time verification key as required for the CHK conversion [13].

Another line of study of IPE is initiated as spatial encryption (SE) defined by Boneh and Hamburg [14]. Hamburg [29] observed that HIPE and SE are strongly related, and Chen, Lim, Ling, and Wang [21] gave explicit property-preserving conversions between them, which enable us to treat SE schemes as (H)IPE schemes. For SE, see Hamburg's thesis [29].

From the perspective of lattice-based encryption beyond IBE, we refer to fuzzy IBE schemes by Agrawal et al. [5], a revocable IBE scheme by Chen, Lim, Ling, Wang, and Ngyuen [22], and an attribute-based encryption scheme by Boyen [16].

1.3 Overview of Our Construction

We give an overview of our construction. For simplicity, we focus on the construction of IPE and omit HIPE. After briefly explaining the basics and the AFV IPE, we present our ideas for "half untwisting" and "half twisting."

The basics: We first review the "dual" public-key encryption (PKE) scheme proposed by Gentry, Peikert, and Vaikuntanathan [26] (or the Peikert KEM [41]). Their public key is a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$. The ciphertext is a vector close to the lattice $\Lambda_q(\boldsymbol{A}) = \{\boldsymbol{z} \in \mathbb{Z}^m : \boldsymbol{z} \equiv \boldsymbol{A}^\top \boldsymbol{s} \text{ for some } \boldsymbol{s} \in \mathbb{Z}_q^n\}$. The secret key is a short basis of $\Lambda_q^\perp(\boldsymbol{A}) = \{\boldsymbol{z} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{z} \equiv \boldsymbol{0}\}$, which enables us to recover a lattice vector in $\Lambda_q(\boldsymbol{A})$ from a vector close to $\Lambda_q(\boldsymbol{A})$. Cash, Hofheinz, Kiltz, and Peikert [20] proposed the first IBE scheme based on the lattices in the standard model.

After that, Agrawal, Boneh, and Boyen [4] proposed a lattice analogue of the Boneh–Boyen IBE [12] (and that of the Waters IBE [48]). Let $id = \mathfrak{w} = w_0 + w_1 X + \cdots + w_{n-1} X^{n-1} \in \mathrm{GF}(q^n)$. Let H be an invertible (or full-rank) difference encoding [23] that maps a polynomial in $\mathrm{GF}(q^n)$ to an n by n matrix of elements in $\mathbb{Z}_q$. [2] In the ABB IBE

[2] Originally, H is called as "full-rank difference" encoding [23]. Recently, this concept was generalized for composite q and others [35,8]: The one of reviews suggested to call it "invertible difference" and the author follows. We say that $H : R \to \mathbb{Z}_q^{n \times n}$ is invertible difference if for any distinct $\mathfrak{w} \neq \mathfrak{w}' \in R$, matrix $H(\mathfrak{w}) - H(\mathfrak{w}') \in \mathbb{Z}_q^{n \times n}$ is invertible (rather than the matrix has rank n). See Section 4 for a concrete construction.

scheme, the public parameters consist of $\boldsymbol{A}_0$, $\boldsymbol{A}_1$, and $\boldsymbol{B}$, and the encryption lattice for id is

$$\Lambda_{id} = \Lambda_q(\boldsymbol{A}_0 \mid \boldsymbol{A}_1 + H(id) \cdot \boldsymbol{B}).$$

The master has a short basis for $\Lambda_q^{\perp}(\boldsymbol{A}_0)$, and it can generate secret keys for $\Lambda_{id}^{\perp}$ using the basis sampling techniques as in [20]. For the security proof, we require H to be invertible difference.

The "twist" by Agrawal, Freeman, and Vaikuntanathan: Agrawal, Freeman, and Vaikuntanathan [6] gave a novel twist on the ABB IBE [4] and obtained an IPE scheme.

In the AFV IPE scheme, the encryption lattice for ciphertext-attribute vector $\vec{w} \in \mathbb{Z}_q^{\mu}$ is defined as

$$\Lambda_{\vec{w}} = \Lambda_q\left(\boldsymbol{A}_0 \mid \boldsymbol{A}_1 + w_1\boldsymbol{B} \mid \cdots \mid \boldsymbol{A}_{\mu} + w_{\mu}\boldsymbol{B}\right).$$

The ciphertext is a vector $\boldsymbol{c} = (\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\mu}) \in (\mathbb{Z}_q^m)^{\mu+1}$ close to $\Lambda_{\vec{w}}$.

They define the mapping $F_{\vec{v}} : (\mathbb{Z}_q^m)^{\mu+1} \to (\mathbb{Z}_q^m)^2$ as

$$F_{\vec{v}}(\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\mu}) = \left(\boldsymbol{c}_0, \textstyle\sum_{i=1}^{\mu} v_i \boldsymbol{c}_i\right) \in \mathbb{Z}_q^{2m}$$

for decryption, where F means "fold." Notice that, if $\vec{v}$ is a *short* vector, e.g., $\vec{v} \in \{0,1\}^{\mu} \subset \mathbb{Z}_q^{\mu}$, then $F_{\vec{v}}(\boldsymbol{c})$ is a vector close to the lattice

$$\Lambda_{\vec{v},\vec{w}} = \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^{\mu} v_i(\boldsymbol{A}_i + w_i\boldsymbol{B})\Big) = \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^{\mu} v_i\boldsymbol{A}_i + (\vec{w}^{\top}\vec{v})\boldsymbol{B}\Big).$$

If $\vec{w}^{\top}\vec{v} = 0$ then the masking term, $(\vec{w}^{\top}\vec{v})\boldsymbol{B}$, vanishes. The secret key for $\vec{v} \in \mathbb{Z}_q^{\mu}$ is defined as a short basis of $\Lambda_q^{\perp}(\boldsymbol{A}_0 \mid \sum_{i=1}^{\mu} v_i\boldsymbol{A}_i)$.

They also gave a binary decomposition technique for $\vec{v}$ of long norm, which expands the public parameters and ciphertext by a factor of $\lg q$: they replaced $\vec{w}$ and $\vec{v}$ with $\vec{w}' = (1, 2, \ldots, 2^{k-1}) \otimes \vec{w}$, where $k = \lceil \lg q \rceil$ and $\otimes$ denotes the standard tensor product, and $\vec{v} \in \mathbb{Z}_q^{\mu}$ with $\vec{v}' \in \{0,1\}^{\mu k}$ such that $\vec{w}^{\top}\vec{v} = (\vec{w}')^{\top}\vec{v}'$. This technique is already exploited in the constructions of fully homomorphic encryption [19,18,17].

Our Ideas: Here, we present our two ideas for changing R from $\mathbb{Z}_q$ to $\mathrm{GF}(q^n)$.

Half untwist: We first change the domain of attributes $\vec{w}$ from $\mathbb{Z}_q^{\mu}$ to $\mathrm{GF}(q^n)^{\mu}$, while $\vec{v}$'s domain is the same as the original, $\mathbb{Z}_q^{\mu} \subset \mathrm{GF}(q^n)^{\mu}$.

Let us turn back to the invertible difference encoding H, which appeared in the ABB IBE but was omitted from the AFV IPE. We have the following facts on the typical construction of $H : \mathrm{GF}(q^n) \to \mathbb{Z}_q^{n \times n}$:

- Fact 1: H maps $w \in \mathbb{Z}_q \subseteq \mathrm{GF}(q^n)$ to $H(w) = w\boldsymbol{I}_n$, where $\boldsymbol{I}_n$ is the n-dimensional identity matrix.
- Fact 2: H is $\mathbb{Z}_q$-linear and is an isomorphism from $\mathrm{GF}(q^n)$ to a field contained in $\mathbb{Z}_q^{n \times n}$.

From Fact 1, we have $w\boldsymbol{B} = w\boldsymbol{I}_n\boldsymbol{B} = H(w)\cdot\boldsymbol{B}$. We can rewrite the encryption lattice of the AFV IPE for $\vec{w} \in \mathbb{Z}_q^\mu \subseteq \mathrm{GF}(q^n)^\mu$ as

$$\Lambda_{\vec{w}} = \Lambda_q(\boldsymbol{A}_0 \mid \boldsymbol{A}_1 + H(w_1 + 0X + \cdots + 0X^{n-1})\boldsymbol{B} \mid \cdots \mid \boldsymbol{A}_\mu + H(w_\mu + 0X + \cdots + 0X^{n-1})\boldsymbol{B}).$$

We discover the hidden H in the AFV IPE and find $(n-1)$ empty slots for each $i \in [\mu]$.

Now, we can change the domain of ciphertext-attribute vector $\vec{w}$ from $\mathbb{Z}_q^\mu$ to $\mathrm{GF}(q^n)^\mu$. We naturally define $\Lambda_{\vec{w}}$ for $\vec{w} = (\mathfrak{w}_1, \ldots, \mathfrak{w}_\mu)^\top \in \mathrm{GF}(q^n)^\mu$ as

$$\Lambda_{\vec{w}} = \Lambda_q(\boldsymbol{A}_0 \mid \boldsymbol{A}_1 + H(\mathfrak{w}_1)\boldsymbol{B} \mid \cdots \mid \boldsymbol{A}_\mu + H(\mathfrak{w}_\mu)\boldsymbol{B}).$$

For a short key vector $\vec{v} \in \mathbb{Z}_q^\mu \subset \mathrm{GF}(q^n)^\mu$ and a ciphertext $\boldsymbol{c} = (\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\mu)$ close to $\Lambda_{\vec{w}}$, we observe that $F_{\vec{v}}(\boldsymbol{c}) = (\boldsymbol{c}_0, \sum_{i=1}^\mu v_i\boldsymbol{c}_v)$ is close to

$$\Lambda_{\vec{w},\vec{v}} = \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^\mu v_i(\boldsymbol{A}_i + H(\mathfrak{w}_i)\cdot\boldsymbol{B})\Big) = \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^\mu v_i\boldsymbol{A}_i + H(\vec{w}^\top\vec{v})\cdot\boldsymbol{B}\Big),$$

where the latter equality follows from the linearity of H (Fact 2). If $\vec{w}^\top\vec{v} = 0$ then $H(\vec{w}^\top\vec{v}) = \boldsymbol{O}$. By using a short basis of $\Lambda_q^\perp(\boldsymbol{A}_0 \mid \sum_{i=1}^\mu v_i\boldsymbol{A}_i)$, one can decrypt the ciphertext if the inner product is 0. Otherwise, the masking matrix $H(\vec{w}^\top\vec{v})\cdot\boldsymbol{B}$ survives and $H(\vec{w}^\top\vec{v})$ is invertible.

Half twist: We next change the domain of $\vec{v}$ from $\mathbb{Z}_q^\mu$ to $\mathrm{GF}(q^n)^\mu$.

We observe that the proof of security by Agrawal et al. [6] does not require randomness of $\boldsymbol{B}$. Hence, we can safely replace a random matrix $\boldsymbol{B}$ with a very structured matrix $\boldsymbol{G} = \boldsymbol{I}_n \otimes (1, 2, 2^2, \ldots, 2^{k-1})$ as in Micciancio and Peikert [35], where $\otimes$ denotes the Kronecker product, and $k = \lceil \lg q \rceil$,

We exploit the structure of $\boldsymbol{G}$ and define a new encoding, $H' : \mathrm{GF}(q^n) \to \{0,1\}^{m\times m}$ (see Section 4), which gives *pseudo-commutativity* with respect to $\boldsymbol{G}$ and H, that is, for any $\mathfrak{v} \in \mathrm{GF}(q^n)$, it holds that $\boldsymbol{G}\cdot H'(\mathfrak{v}) = H(\mathfrak{v})\cdot\boldsymbol{G}$.

We apply the above idea and new encoding to the half untwist version of the AFV IPE. The encryption lattice for $\vec{w}$ is $\Lambda_{\vec{w}} = \Lambda_q(\boldsymbol{A}_0 \mid \boldsymbol{A}_1 + H(\mathfrak{w}_1)\cdot\boldsymbol{G} \mid \cdots \mid \boldsymbol{A}_\mu + H(\mathfrak{w}_\mu)\cdot\boldsymbol{G})$ as in the previous version. We modify the key-extraction and decryption algorithms for $\vec{v} = (\mathfrak{v}_1, \ldots, \mathfrak{v}_\mu) \in \mathrm{GF}(q^n)^\mu$. In decryption, a ciphertext $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\mu)$ is folded up by $H'(\mathfrak{v}_i)$ instead of v_i, that is,

$$F'_{\vec{v}}(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\mu) = \Big(\boldsymbol{c}_0, \textstyle\sum_{i=1}^\mu \boldsymbol{c}_i\cdot H'(\mathfrak{v}_i)\Big).$$

By the pseudo-commutativity, the sum $F'_{\vec{v}}(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\mu)$ is a vector close to the lattice

$$\begin{aligned}
\Lambda_{\vec{w},\vec{v}} &= \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^\mu(\boldsymbol{A}_i + H(\mathfrak{w}_i)\cdot\boldsymbol{G})\cdot H'(\mathfrak{v}_i)\Big)\\
&= \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^\mu \boldsymbol{A}_i\cdot H'(\mathfrak{v}_i) + \sum_{i=1}^\mu H(\mathfrak{w}_i)\cdot H(\mathfrak{v}_i)\cdot\boldsymbol{G}\Big)\\
&= \Lambda_q\Big(\boldsymbol{A}_0 \,\Big|\, \textstyle\sum_{i=1}^\mu \boldsymbol{A}_i\cdot H'(\mathfrak{v}_i) + H(\vec{w}^\top\vec{v})\cdot\boldsymbol{G}\Big),
\end{aligned}$$

since the matrix norm of $H'(\mathfrak{v}_i) \in \{0,1\}^{m\times m}$ is at most m. The secret key is a short basis of lattice $\Lambda_q^\perp(\boldsymbol{A}_0 \mid \sum_{i=1}^\mu \boldsymbol{A}_i\cdot H'(\mathfrak{v}_i))$.

We note that the binary-decomposition technique is built into our new encoding H' and the structured matrix $\boldsymbol{G}$. Therefore, we can save the $\lg q$ factor introduced by the binary decomposition in the AFV IPE scheme.

2 Preliminaries

A security parameter is denoted by κ. We use the standard O-notations, O, Θ, Ω, and ω. We use capital bold symbols $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ for matrices. In particular, $\boldsymbol{I}_n$ denotes an n by n identity matrix. We use lower-case bold symbols $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ for vectors. In addition, we use over-arrows to denote ciphertext- and key-attribute vectors as $\vec{w}$, $\vec{v}$. We use lower-case fraktur symbols $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ for polynomials and elements of $\mathrm{GF}(q^n)$. The abbreviations DPT and PPT stand for deterministic polynomial time and probabilistic polynomial time. For any integer $q \geq 3$, we write $\mathbb{Z}_q$ for the ring $\{-(q-1)/2, \ldots, -1, 0, 1, \ldots, (q-1)/2\}$ with addition and multiplication modulo q.

A function $f(\kappa)$ is said to be negligible if $f(\kappa) = \kappa^{-\omega(1)}$. We denote a set of negligible functions by $\mathsf{negl}(\kappa)$. For a positive integer n, $[n]$ denotes $\{1, 2, \ldots, n\}$. For $x \in \mathbb{R}$, we define $\lfloor x \rceil = \lceil x - 1/2 \rceil$ as the integer closest to x. For $\boldsymbol{x} = (x_1, \ldots, x_\ell) \in \mathbb{R}^\ell$, we define $\lfloor \boldsymbol{x} \rceil$ as $(\lfloor x_1 \rceil, \ldots, \lfloor x_\ell \rceil) \in \mathbb{Z}^\ell$. For two matrices $\boldsymbol{X} \in \mathbb{R}^{m \times n_1}$ and $\boldsymbol{Y} \in \mathbb{R}^{m \times n_2}$, $[\boldsymbol{X} \mid \boldsymbol{Y}] \in \mathbb{R}^{m \times (n_1 + n_2)}$ is the concatenation of the columns of $\boldsymbol{X}$ and $\boldsymbol{Y}$. For two matrices $\boldsymbol{X} \in \mathbb{R}^{m_1 \times n}$ and $\boldsymbol{Y} \in \mathbb{R}^{m_2 \times n}$, $[\boldsymbol{X}; \boldsymbol{Y}] \in \mathbb{R}^{(m_1 + m_2) \times n}$ is the concatenation of the rows of $\boldsymbol{X}$ and $\boldsymbol{Y}$. For a vector $\boldsymbol{x} \in \mathbb{R}^m$, $\|\boldsymbol{x}\|_p$ denotes the ℓ_p norm of $\boldsymbol{x}$. For ease of notation, we omit the subscript if $p = 2$.

For matrix $\boldsymbol{X} = [\boldsymbol{x}_1 \ \ldots \ \boldsymbol{x}_n]$, $\tilde{\boldsymbol{X}}$ denotes the Gram-Schmidt orthogonalization of $\boldsymbol{X}$. For a matrix $\boldsymbol{X} = [\boldsymbol{x}_1; \ldots; \boldsymbol{x}_m] \in \mathbb{R}^{m \times n}$, $\|\boldsymbol{X}\|_{\mathrm{row}} = \max_i \|\boldsymbol{x}_i\|$. For a matrix $\boldsymbol{X} \in \mathbb{R}^{m \times n}$, $s_1(\boldsymbol{X})$ denotes the largest singular value of $\boldsymbol{X}$; we have that $s_1(\boldsymbol{X}) = \sup_{\boldsymbol{u} \in \mathbb{R}^n, \|\boldsymbol{u}\|=1} \|\boldsymbol{X}\boldsymbol{u}\| = \sup_{\boldsymbol{u}' \in \mathbb{R}^m, \|\boldsymbol{u}'\|=1} \|\boldsymbol{X}^\top \boldsymbol{u}'\|$. For two matrices $\boldsymbol{X} \in \mathbb{R}^{n \times m}$ and $\boldsymbol{Y} \in \mathbb{R}^{m \times k}$, we have $s_1(\boldsymbol{X}\boldsymbol{Y}) \leq s_1(\boldsymbol{X}) \cdot s_1(\boldsymbol{Y})$. We also have for any $\boldsymbol{X} \in \mathbb{R}^{n \times m}$, $\|\boldsymbol{X}\|_{\mathrm{row}}, \|\boldsymbol{X}^\top\|_{\mathrm{row}} \leq s_1(\boldsymbol{X})$. Finally, for ring R and positive integer n, $\mathrm{GL}_n(R)$ denotes the set of n by n invertible matrices whose entries in R.

Distribution: We recall distributions in the lattice-based cryptography. For a distribution χ, we often write $x \leftarrow \chi$, which indicates that we take a sample x from χ. For a finite set S, $U(S)$ denotes the uniform distribution over S. The Gaussian distribution with mean 0 and variance s^2, denoted by $N(0, s^2)$, is defined by density function $(1/s\sqrt{2\pi}) \cdot \exp(-x^2/2s^2)$ over $\mathbb{R}$. For $\alpha \in (0, 1)$ and positive integer q, we define the *discretized* Gaussian $\bar{\Psi}_\alpha$ as: take sample x from $N(0, \alpha^2/2\pi)$ and output $\lfloor qx \rceil \bmod q$. For positive real s, the n-dimensional Gaussian function is defined as $\rho_s(\boldsymbol{x}) = \exp(-\pi\|\boldsymbol{x}\|^2/s^2)$. For positive real s and countable set A, the *discrete* Gaussian distribution $D_{A,s}$ is defined by $D_{A,s}(\boldsymbol{x}) = \frac{\rho_s(\boldsymbol{x})}{\sum_{\boldsymbol{y} \in A} \rho_s(\boldsymbol{y})}$.

2.1 Lattices

A (full-rank) lattice in $\mathbb{R}^n$ is $\Lambda = \{\sum_{i=1}^n x_i \boldsymbol{b}_i : x_i \in \mathbb{Z}\}$, where $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^n$ are linearly independent over $\mathbb{R}^n$. Matrix $\boldsymbol{B} = [\boldsymbol{b}_1 \ \ldots \ \boldsymbol{b}_n]$ is a basis of lattice Λ. For $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and $\boldsymbol{u} \in \mathbb{Z}_q^n$, we define lattices and their shift:

$$
\begin{aligned}
\Lambda_q(\boldsymbol{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m : \exists \boldsymbol{s} \in \mathbb{Z}_q^n \text{ such that } \boldsymbol{y} \equiv \boldsymbol{A}^\top \boldsymbol{s} \pmod q\}, \\
\Lambda_q^\perp(\boldsymbol{A}) &= \{\boldsymbol{e} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{e} \equiv \boldsymbol{0} \pmod q\}, \\
\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}) &= \{\boldsymbol{e} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{e} \equiv \boldsymbol{u} \pmod q\}.
\end{aligned}
$$

We recall the property of very structured matrix $\boldsymbol{G}$.

Theorem 2.1 (Adapted version of [35, Theorem 4.1]). *Let $q \geq 2$, $n \geq 1$, $k = \lceil \lg q \rceil$, and $\bar{m} = nk$ be integers. Let $\boldsymbol{g} = (1, 2, \ldots, 2^{k-1}) \in \mathbb{Z}^k$ and $\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g}$. Then the lattice $\Lambda_q^{\perp}(\boldsymbol{G})$ has a known basis $\boldsymbol{S} \in \mathbb{Z}^{\bar{m} \times \bar{m}}$ with $\|\tilde{\boldsymbol{S}}\| \leq \sqrt{5}$ and $\|\boldsymbol{S}\| \leq \max\{\sqrt{5}, \sqrt{k}\}$.*

Recently, Micciancio and Peikert introduced a new notion of "trapdoors" for lattices. Let $m = \bar{m} + nk$, where $k = \lceil \lg q \rceil$. We review their notion of trapdoors.

Definition 2.1 (Adapted, [35, Definition 5.2]). *Let $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and $\boldsymbol{G} \in \mathbb{Z}_q^{n \times w}$ be matrices with $m \geq w \geq n$. We say a matrix $\boldsymbol{R} \in \mathbb{Z}^{(m-w) \times w}$ is a $\boldsymbol{G}$-trapdoor with tag $\boldsymbol{H} \in \mathrm{GL}_n(\mathbb{Z}_q) \subseteq \mathbb{Z}_q^{n \times n}$ if $\boldsymbol{A}\,[\boldsymbol{R}; \boldsymbol{I}_w] = \boldsymbol{HG}$. The* quality *of the trapdoor is measured by $s_1(\boldsymbol{R})$.*

Theorem 2.2. *We borrow the following algorithms in [35], which are improvements of those in the literature [7,26,9,4,42]. We set $k = \lceil \lg q \rceil$ and $m = \bar{m} + nk$ for simplicity of notation.*

$\mathsf{GenTrap}^D(\bar{\boldsymbol{A}}, \boldsymbol{H})$**:** *Given a matrix $\bar{\boldsymbol{A}} \in \mathbb{Z}_q^{n \times \bar{m}}$, an invertible matrix $\boldsymbol{H} \in \mathrm{GL}_n(\mathbb{Z}_q)$, and a distribution D over $\mathbb{Z}_q$, it outputs $\boldsymbol{A} = [\bar{\boldsymbol{A}} \mid \boldsymbol{HG} - \bar{\boldsymbol{A}}\boldsymbol{R}] \in \mathbb{Z}_q^{n \times (\bar{m}+nk)}$ and its trapdoor $\boldsymbol{R} \in \mathbb{Z}_q^{\bar{m} \times nk}$ with tag $\boldsymbol{H}$, where $\boldsymbol{R}$ is chosen from distribution D.*
In particular, we often set q as an odd prime, $\bar{m} = n \lg q + \omega(\lg \kappa)$, $D = U(\{-1, +1\})$, and choose $\bar{\boldsymbol{A}}$ from $\mathbb{Z}_q^{n \times \bar{m}}$ uniformly at random. These settings yield the obtained matrix $\boldsymbol{A}$ as $\mathsf{negl}(\kappa)$-uniform and $s_1(\boldsymbol{R}) \leq C(\sqrt{\bar{m}} + \sqrt{nk})$ with overwhelming probability.

$\mathsf{SampleD}(\boldsymbol{R}, \boldsymbol{A}, \boldsymbol{H}, \boldsymbol{u}, s)$**:** *The input is $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, its trapdoor $\boldsymbol{R} \in \mathbb{Z}_q^{\bar{m} \times nk}$ with tag $\boldsymbol{H} \in \mathrm{GL}_n(\mathbb{Z}_q)$, and a target vector $\boldsymbol{u}$, and Gaussian parameter $s > \sqrt{s_1(\boldsymbol{R})^2 + 1} \cdot \sqrt{7} \cdot \omega(\sqrt{\lg n})$. It outputs $\boldsymbol{x}$ according to a distribution statistically close to $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}), s}$; roughly speaking, it samples $\boldsymbol{x}$ from $D_{\mathbb{Z}, s}^m$ conditioned on $\boldsymbol{Ax} = \boldsymbol{u}$.*

2.2 Assumption

The learning with errors (LWE) problem proposed by Regev [46] is a generalization of the learning parity noise (LPN) problem.

For vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ and distribution χ over $\mathbb{Z}_q$, let $A(\boldsymbol{s}, \chi)$ be a distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ defined by taking samples $\boldsymbol{a} \leftarrow \mathbb{Z}_q^n$ and $x \leftarrow \chi$, and outputting $(\boldsymbol{a}, \boldsymbol{a}^{\top}\boldsymbol{s} + x)$.

Definition 2.2 (The LWE problem and assumption). *For integer $q = q(n)$ and distribution χ over $\mathbb{Z}_q$, the learning with errors problem,* $\mathrm{LWE}(q, \chi)$*, distinguishes oracle $A(\boldsymbol{s}, \chi)$ from oracle $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ for uniformly random $\boldsymbol{s} \in \mathbb{Z}_q^n$.*

We say the LWE assumption holds if for any PPT adversary $\mathcal{A}$, its advantage

$$\mathsf{Adv}_{\mathcal{A}, \mathrm{LWE}(q,\chi)}(n) = \left| \Pr[\mathcal{A}^{A(\boldsymbol{s},\chi)}(1^n) = 1] - \Pr[\mathcal{A}^{U(\mathbb{Z}_q^n \times \mathbb{Z}_q)}(1^n) = 1] \right| = \mathsf{negl}(n),$$

where $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$.

It is well-known that under (quantum) reductions, solving the LWE problem *on average* is as hard as the *worst* case of the approximation version of the shortest independent vector problem, SIVP_γ, and the decision version of the shortest vector problem, GapSVP_γ, where γ is an approximation factor for appropriate parameters. In particular, we have a reduction with parameter $\chi = \bar{\Psi}_\alpha$, $\alpha q \geq 2\sqrt{n}$, and $\gamma = \tilde{O}(n/\alpha)$. See [46,41] for details.

3 Predicate Encryption

We review the syntax of predicate encryption.

Definition 3.1. *Let $\mathcal{P} : \Phi \times \Sigma \to \{0,1\}$ be a predicate where Φ and Σ denote "key attribute" and "ciphertext attribute" spaces. A predicate encryption scheme for $\mathcal{P}$ is a fourtuplet of algorithms.*

$\mathsf{Setup}(1^\kappa) \to (pp, msk)$**:** *The setup algorithm takes as input security parameter 1^κ and outputs public parameters pp and master secret key msk.*

$\mathsf{Extract}(msk, \phi) \to dk_\phi$**:** *The extraction algorithm takes as input msk and key attribute $\phi \in \Phi$. It outputs decryption key dk_ϕ.*

$\mathsf{Enc}(pp, \sigma, M) \to ct$**:** *The encryption algorithm takes as input pp, ciphertext attribute $\sigma \in \Sigma$, and message $M \in \mathcal{M}$. It outputs ciphertext ct.*

$\mathsf{Dec}(pp, dk_\phi, ct) \to M$ **or** $\perp$**:** *The decryption algorithm takes as input decryption key dk_ϕ and ciphertext ct. It outputs either $M \in \mathcal{M}$ or rejection symbol $\perp$.*

We define slightly weak correctness for decryption. For any $\phi \in \Phi$, $\sigma \in \Sigma$, and $M \in \mathcal{M}$, if $\mathcal{P}(\phi, \sigma) = 1$ then

$$\Pr\left[M = \tilde{M} : \begin{array}{l}(pp, msk) \leftarrow \mathsf{Setup}(1^\kappa); dk_\phi \leftarrow \mathsf{Extract}(msk, \phi); \\ ct \leftarrow \mathsf{Enc}(pp, \sigma, M); \tilde{M} \leftarrow \mathsf{Dec}(pp, dk_\phi, ct);\end{array}\right]$$

is overwhelming probability and if $\mathcal{P}(\phi, \sigma) = 0$ then

$$\Pr\left[\tilde{M} = \perp : \begin{array}{l}(pp, msk) \leftarrow \mathsf{Setup}(1^\kappa); dk_\phi \leftarrow \mathsf{Extract}(msk, \phi); \\ ct \leftarrow \mathsf{Enc}(pp, \sigma, M); \tilde{M} \leftarrow \mathsf{Dec}(pp, dk_\phi, ct);\end{array}\right]$$

is overwhelming probability. As in [6], our construction satisfies the different correctness condition: the latter condition is replaced with the condition that if $\mathcal{P}(\phi, \sigma) = 0$ then $\mathsf{Dec}(pp, dk_\phi, ct)$ is computationally indistinguishable from a uniformly random element in $\mathcal{M}$. One can use a suitable message padding to obtain the original correctness, if an IPE scheme has message space $\{0,1\}^\ell$ for sufficiently large ℓ.

We next review the security definition of predicate encryption. Roughly speaking, we say that a PE scheme is weakly attribute hiding in a selective attribute setting against chosen-plaintext attacks (wAH-sA-CPA), if any adversary cannot distinguish $\mathsf{Enc}(pp, \sigma_0, M_0)$ or $\mathsf{Enc}(pp, \sigma_1, M_1)$, where σ_0 and σ_1 are declared at the initialization, even if the adversary can query the decryption key dk_ϕ for $\mathcal{P}(\sigma_0, \phi) = \mathcal{P}(\sigma_1, \phi) = 0$. The precise definition follows:

Definition 3.2 (wAH-sA-CPA security). *Let* PE *be a predicate encryption scheme,* $\mathcal{A}$ *an adversary, and* κ *a security parameter. The experiment between a challenger and adversary* $\mathcal{A}$*,* $\mathsf{Expt}^{\text{wah-sa-cpa}}_{\mathcal{A},\mathsf{PE}}(1^\kappa)$*, is defined as follows:*

Initialization: *Given security parameter* 1^κ*, run adversary* $\mathcal{A}$ *with* 1^κ*. Receive two ciphertext attributes* $\sigma_0, \sigma_1 \in \Sigma$ *from* $\mathcal{A}$*. Run* $(pp, msk) \leftarrow \mathsf{Setup}(1^\kappa)$*. Flip a coin* $b \leftarrow \{0,1\}$*.*

Learning Phase: *Feed pp to adversary* $\mathcal{A}$*. Adversary* $\mathcal{A}$ *could issue queries to the following oracles in any order and many times except for the constraint regarding oracle* Challenge*.*

- *Oracle* Extract *receives key attribute* $\phi \in \Phi$ *subject to the restriction that* $\mathcal{P}(\phi, \sigma_0) = \mathcal{P}(\phi, \sigma_1) = 0$*. If so, it obtains* $dk_\phi \leftarrow \mathsf{Extract}(msk, \phi)$ *and provides* $\mathcal{A}$ *with* dk_ϕ*.*
- *Oracle* Challenge *receives two messages* M_0 *and* M_1*. It obtains* $C \leftarrow \mathsf{Enc}(pp, \sigma_b, M_b)$ *and provides* $\mathcal{A}$ *with* C*.*

Eventually, $\mathcal{A}$ *halts after it outputs its decision,* $b' \in \{0,1\}$*.*

Finalization: *Output* 1 *if* $b' = b$*. Otherwise, output* 0*.*

We define the advantage of $\mathcal{A}$ *as*

$$\mathsf{Adv}^{\text{wah-sa-cpa}}_{\mathcal{A},\mathsf{PE}}(\kappa) = \left|\Pr[\mathsf{Expt}^{\text{wah-sa-cpa}}_{\mathcal{A},\mathsf{PE}}(1^\kappa) = 1 \mid b = 0] - \Pr[\mathsf{Expt}^{\text{wah-sa-cpa}}_{\mathcal{A},\mathsf{PE}}(1^\kappa) = 1 \mid b = 1]\right|.$$

We say that PE *is weakly attribute hiding against chosen-plaintext attacks in selective attribute setting (*wAH-sA-CPA*-secure) if* $\mathsf{Adv}^{\text{wah-sa-cpa}}_{\mathcal{A},\mathsf{PE}}(\kappa)$ *is negligible for every PPT adversary* $\mathcal{A}$*.*

4 Pseudo-Commutativity of Invertible Difference Encoding

In this section, we define H and $H_{\boldsymbol{g}}$ such that, for any $\mathfrak{a}$, $H(\mathfrak{a}) \cdot \boldsymbol{G} = \boldsymbol{G} \cdot H_{\boldsymbol{g}}(\mathfrak{a})$ holds and $s_1(H_{\boldsymbol{g}}(\mathfrak{a}))$ is small. We first recall the polynomial rings. After a reminder of the invertible difference encoding, we define its companion $H_{\boldsymbol{g}}$.

4.1 Quick Reminder of Rings

Consider a finite ring $R = \mathbb{Z}_q[X]/\langle \mathfrak{g} \rangle$, where $\mathfrak{g} \in \mathbb{Z}_q[X]$ is monic and of degree n. If q is prime and $\mathfrak{g}$ is irreducible over $\mathbb{Z}_q$, ring R is the field $\mathrm{GF}(q^n)$.

We define the mapping $\tau : R \to \mathbb{Z}_q^n$ by $\mathfrak{a} = a_0 + a_1 X + \ldots a_{n-1} X^{n-1} \mapsto (a_0, \ldots, a_{n-1})^\top$. By this mapping (as known as "coefficient embedding"), we can identify a polynomial in R with a vector in $\mathbb{Z}_q^n$. We next define $\mathrm{Rot} : R \to \mathbb{Z}_q^{n \times n}$ by

$$\mathfrak{a} = a_0 + a_1 X + \ldots a_{n-1} X^{n-1} \mapsto [\tau(\mathfrak{a})\, \tau(\mathfrak{a}X)\, \ldots\, \tau(\mathfrak{a}X^{n-1})],$$

which is borrowed from Micciancio [33]. We note that

$$\mathrm{Rot}(\mathfrak{a}) \cdot \tau(\mathfrak{b}) = \tau(\mathfrak{a}\mathfrak{b}), \mathrm{Rot}(\mathfrak{a}) \cdot \mathrm{Rot}(\mathfrak{b}) = \mathrm{Rot}(\mathfrak{a}\mathfrak{b}), \text{ and } \mathrm{Rot}(\mathfrak{a}) + \mathrm{Rot}(\mathfrak{b}) = \mathrm{Rot}(\mathfrak{a} + \mathfrak{b}),$$

and, thus, Rot is a ring-homomorphism from R into $\mathbb{Z}_q^{n \times n}$.

4.2 Invertible Difference Encoding H

Lattice-based cryptography often employs an encoding $H : \mathrm{GF}(q^n) \to \mathbb{Z}_q^{n\times n}$ for prime q, e.g., [43, due to Micciancio] and [4]. Hereafter we stick to prime q.

We say that H is an invertible difference if for any two distinct polynomials $\mathfrak{a} \neq \mathfrak{a}' \in \mathrm{GF}(q^n)$, the difference of outputs, $H(\mathfrak{a}) - H(\mathfrak{a}')$, is always invertible.

In this paper, we employ explicit H defined by $H(\mathfrak{a}) := \mathrm{Rot}(\mathfrak{a})$. It holds that $H(\mathfrak{a}) - H(\mathfrak{a}') = H(\mathfrak{a}-\mathfrak{a}')$ for any $\mathfrak{a} \neq \mathfrak{a}'$. If $\mathfrak{a}-\mathfrak{a}'$ is a unit, that is, $\mathfrak{a} \neq \mathfrak{a}' \in \mathrm{GF}(q^n)$, then $H(\mathfrak{a}-\mathfrak{a}')$ is also a unit in $\mathbb{Z}_q^{n\times n}$. In addition, we note that for any constant $a \in \mathbb{Z}_q \subset \mathrm{GF}(q^n)$, $H(a) = a\boldsymbol{I}_n$.

4.3 New Encoding $H_{\boldsymbol{g}}$

We define a new encoding, denoted by $H_{\boldsymbol{g}}$, that maps an element in $\mathrm{GF}(q^n)$ to matrices in $\{0, 1, \ldots, b-1\}^{nk\times nk}$ and gives pseudo-commutativity with $\boldsymbol{G}$ and H.

Let $b \geq 2$ be a positive integer and let B be the range $\{0, 1, \ldots, b-1\} \subset \mathbb{Z}_q$. We define $k = \lceil \log_b q \rceil$ and $\boldsymbol{g} = (1, b, \ldots, b^{k-1})$. The gadget matrix $\boldsymbol{G}$ in [35] is defined by

$$\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g} = \begin{bmatrix} \text{—}\boldsymbol{g}\text{—} & & & \\ & \text{—}\boldsymbol{g}\text{—} & & \\ & & \ddots & \\ & & & \text{—}\boldsymbol{g}\text{—} \end{bmatrix} = \begin{bmatrix} 1\ b \ldots\ b^{k-1} & & & \\ & 1\ b \ldots\ b^{k-1} & & \\ & & \ddots & \\ & & & 1\ b \ldots\ b^{k-1} \end{bmatrix} \in \mathbb{Z}_q^{n\times nk}.$$

For $a \in \mathbb{Z}_q$, we define b-ary decomposition of a by $d_{\boldsymbol{g}}(a) = (a_1, \ldots, a_k)^\top \in B^k$, on which we have that $\boldsymbol{g} \cdot d_{\boldsymbol{g}}(a) = \sum_{i=1}^{k} a_i \cdot b^{i-1} = a$.

We define $H_{\boldsymbol{g}}(\mathfrak{a})$ as the b-ary decomposition of $H(\mathfrak{a})$. More formally, we first define the mapping $D_{\boldsymbol{g}}$ by

$$D_{\boldsymbol{g}} : a \in \mathbb{Z}_q \mapsto [d_{\boldsymbol{g}}(a)\ d_{\boldsymbol{g}}(ba)\ \ldots\ d_{\boldsymbol{g}}(b^{k-1}a)] \in B^{k\times k}.$$

By the definition of $D_{\boldsymbol{g}}$, we have that $\boldsymbol{g} \cdot D_{\boldsymbol{g}}(a) = (a, ba, \ldots, b^{k-1}a) = a \cdot \boldsymbol{g}$, which is a source of the pseudo-commutativity. Next, we extend the domain of $D_{\boldsymbol{g}}$ to any matrix $\boldsymbol{A} = \{a_{i,j}\} \in \mathbb{Z}_q^{n\times m}$ as follows:

$$D_{\boldsymbol{g}}(\boldsymbol{A}) = \begin{bmatrix} D_{\boldsymbol{g}}(a_{1,1})\ D_{\boldsymbol{g}}(a_{1,2}) \ldots D_{\boldsymbol{g}}(a_{1,m}) \\ D_{\boldsymbol{g}}(a_{2,1})\ D_{\boldsymbol{g}}(a_{2,2}) \ldots D_{\boldsymbol{g}}(a_{2,m}) \\ \vdots \quad\ \vdots \quad\ \ddots \quad\ \vdots \\ D_{\boldsymbol{g}}(a_{n,1})\ D_{\boldsymbol{g}}(a_{n,2}) \ldots D_{\boldsymbol{g}}(a_{n,m}) \end{bmatrix} \in B^{nk\times mk}.$$

Finally, we define $H_{\boldsymbol{g}}$ that maps a polynomial into a matrix as follows:

$$\mathfrak{a} = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathrm{GF}(q^n) \mapsto D_{\boldsymbol{g}}(\mathrm{Rot}(\mathfrak{a})) \in B^{nk\times nk}.$$

The mapping $H_{\boldsymbol{g}}$ has two properties that are crucial for our construction. One is pseudo-commutativity with $\boldsymbol{G}$ and H and the other is a small matrix norm.

Lemma 4.1. *Let $\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g} \in \mathbb{Z}_q^{n\times nk}$. It holds that, for any $\mathfrak{a} \in \mathrm{GF}(q^n)$, $\boldsymbol{G} \cdot H_{\boldsymbol{g}}(\mathfrak{a}) = H(\mathfrak{a}) \cdot \boldsymbol{G}$.*

Proof. We show that for any matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times n}$, $\boldsymbol{G} \cdot D_{\boldsymbol{g}}(\boldsymbol{A}) = \boldsymbol{A} \cdot \boldsymbol{G}$, where $\boldsymbol{A} = [\boldsymbol{a}_1 \mid \cdots \mid \boldsymbol{a}_n]$. We divide the matrices into k submatrices; $\boldsymbol{G} \cdot D_{\boldsymbol{g}}(\boldsymbol{A}) = [\boldsymbol{L}_1 \mid \cdots \mid \boldsymbol{L}_k]$ and $\boldsymbol{A} \cdot \boldsymbol{G} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_k]$, where $\boldsymbol{L}_i, \boldsymbol{R}_i \in \mathbb{Z}_q^{n\times n}$. It is easy to check that $\boldsymbol{L}_i = \boldsymbol{a}_i \otimes \boldsymbol{g} = \boldsymbol{R}_i$ for any i. □

Lemma 4.2. *For any* $\mathfrak{a} \in \mathrm{GF}(q^n)$, $\|H_{\boldsymbol{g}}(\mathfrak{a})\|_{\mathrm{row}} \le (b-1)\cdot\sqrt{nk}$ *and* $s_1(H_{\boldsymbol{g}}(\mathfrak{a})) \le (b-1)nk$.

Proof. Since $H_{\boldsymbol{g}} \in B^{nk\times nk}$, the maximal length of the rows is at most $(b-1)\sqrt{nk}$. The latter bound is obtained by the upper bound on the length of $(b-1)\cdot\mathbf{1}\cdot\boldsymbol{u}$, where $\mathbf{1}$ is an nk-dimensional all-1 matrix and $\boldsymbol{u}$ is a unit vector. □

4.4 On the Case Composite q

Although we have stuck to prime q here, lattice-based cryptography often employs $q = p^e$, say $q = 2^k$, or $q = \prod_i p_i$ for small prime p_i for the sake of easiness and speed of implementations. Therefore, one would extend our technique into such cases.

Micciancio and Peikert [35, Section 6.1 of the ePrint version] and Alperin-Sheriff and Peikert [8, Section 5.1] defined an encoding $H : \mathbb{Z}_q[X]/\langle\mathfrak{g}\rangle \to \mathbb{Z}_q^{n\times n}$, where $\mathfrak{g}$ is a monic degree-n polynomial in $\mathbb{Z}[X]$ and irreducible modulo every prime p dividing q. In their constructions, H is a ring homomorphism from $R = \mathbb{Z}_q[X]/\langle\mathfrak{g}\rangle$ into $\mathbb{Z}_q^{n\times n}$. Thus, if $\mathfrak{u} \in R$ is a unit, then $H(\mathfrak{u})$ is invertible. In general, $H(\mathfrak{u})$ is not invertible even for non-zero $\mathfrak{u} \in R \setminus R^*$.

This property suffices for public-key encryption, IBE, and signature, but, may trouble designers of predicates. If one can ensure that the inner product results in either a unit or zero of R, one can employ the above techniques.

4.5 On the Ring-LWE Setting

When q is a prime, then we can extend our new encoding into the ring-LWE setting [32]. Let us consider the cyclotomic ring $\mathcal{R} = \mathbb{Z}[X]/\langle\Phi_m(X)\rangle$, where $\Phi_m(X)$ denotes the m-th cyclotomic polynomial. Let n be the degree of $\Phi_m(X)$. For any poly(n)-bounded prime q, we let $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$.

The Micciancio–Peikert algorithm in the ring-LWE setting: Let $\boldsymbol{g} = (1, b, \ldots, b^{k-1}) \in \mathcal{R}_q^k$. In the ring setting, we will use $\boldsymbol{g}$ directly instead of $\boldsymbol{G}$. Let us set $R = \mathbb{Z}_q[X]/\langle\mathfrak{g}\rangle \simeq \mathrm{GF}(q^n)$ as in the LWE case.

Micciancio and Peikert [34] define $\mathcal{R}$ to be R-module [3] by extending the ideas in [35, Section 6.1 of the ePrint version] and [8, Section 5.1]. Formally speaking, for $\mathfrak{a} \in R$ and $b \in \mathcal{R}$, scalar multiplication $\mathfrak{a} \odot b \in \mathcal{R}$ is defined by $\sigma^{-1}(\mathfrak{a}\cdot\sigma(b)) \in \mathcal{R}$, where $\sigma : \mathcal{R} \to R$ is an additive isomorphism. (Notice that R and $\mathcal{R}$ are additively isomorphic to $\mathbb{Z}_q^n$.) By the construction, $\mathcal{R}$ is an R-module and $\mathfrak{a}$ acts as the linear transformation over $\mathcal{R}$. Now, the trapdoor of $\boldsymbol{a} \in \mathcal{R}_q^{\bar{m}+k}$ with tag $\mathfrak{h} \in R$ is short $\boldsymbol{R} \in \mathcal{R}_q^{\bar{m}+k}$ satisfying $\boldsymbol{a} = [\bar{\boldsymbol{a}} \mid \mathfrak{h}\odot\boldsymbol{g} - \bar{\boldsymbol{a}}\boldsymbol{R}]$. We can define the new encoding $h_{\boldsymbol{g}} : R \to R^{k\times k}$ in a similar way to the LWE case. We defer the details to the full version.

[3] We say $\mathcal{R}$ is R-module if for any $\mathfrak{r}, \mathfrak{s} \in R$ and any $x, y \in \mathcal{R}$, we have $\mathfrak{r}(x+y) = \mathfrak{r}x + \mathfrak{r}y$, $(\mathfrak{r}+\mathfrak{s})x = \mathfrak{r}x + \mathfrak{s}x$, $(\mathfrak{r}\mathfrak{s})x = \mathfrak{r}(\mathfrak{s}x)$, and $1_R x = x$.

Langlois and Stehlé [47] also pointed out another way. Let us consider the case that n is even and $\Phi_m(X)$ is split into two polynomials $\mathfrak{f}_1$ and $\mathfrak{f}_2$ of degree $n/2$ which are irreducible over $\mathbb{Z}_q$. In such a case, we have $\mathcal{R}_q \simeq \mathbb{Z}_q[X]/\langle \mathfrak{f}_1 \rangle \times \mathbb{Z}_q[X]/\langle \mathfrak{f}_2 \rangle \simeq \mathrm{GF}(q^{n/2})^2$. We let $R = \mathrm{GF}(q^{n/2})$ and consider $H : R \to \mathcal{R}_q$ as follows:

We first define a duplicating function $\mathrm{dp} : \mathrm{GF}(q^{n/2}) \to \mathrm{GF}(q^{n/2})^2$ as $\mathfrak{a} \mapsto (\mathfrak{a}, \mathfrak{a})$. By the Chinese remainder theorem, we have invertible mapping $\tau : \mathbb{Z}_q[X]/\langle \Phi_m(X) \rangle \to \mathbb{Z}_q[X]/\langle \mathfrak{f}_1 \rangle \times \mathbb{Z}_q[X]/\langle \mathfrak{f}_2 \rangle$ as $\mathfrak{a} \mapsto (\mathfrak{a} \bmod \mathfrak{g}_1, \mathfrak{a} \bmod \mathfrak{g}_2)$. Then, we define the full-rank difference encoding from $\mathrm{GF}(q^{n/2})$ to R_q as $H = \tau^{-1} \circ \mathrm{dp}$. By the construction, H is an isomorphism from $\mathrm{GF}(q^{n/2})$ to a sub-ring of $\mathcal{R}_q$, which is a field.

Now, the trapdoor of $\boldsymbol{a} \in \mathcal{R}_q^{\bar{m}+k}$ with tag $\mathfrak{h} \in R$ is $\boldsymbol{R} \in \mathcal{R}_q^{\bar{m}+k}$ satisfying $\boldsymbol{a} = [\bar{\boldsymbol{a}} \mid H(\mathfrak{h})\boldsymbol{g} - \bar{\boldsymbol{a}}\boldsymbol{R}]$. We can define the new encoding $H_{\boldsymbol{g}} : R \to \mathcal{R}_q^{k \times k}$ in a similar way to the LWE case. We defer the details to the full version.

5 Our Construction

We describe our IPE scheme that supports inner-product predicates over $\mathrm{GF}(q^n)^\mu$. The scheme is obtained by applying our ideas in the introduction to the AFV IPE scheme. The extension to HIPE is deferred to the full version.

Let $\kappa \in \mathbb{N}$ be a security parameter. Let μ be the length of predicate and attribute vectors. Let n be a dimension of lattices and let q and m be the parameters that define the matrices. Let $\mathfrak{g} = \mathfrak{g}(x) \in \mathbb{Z}_q[x]$ be a monic, irreducible polynomial of degree n that explicitly defines $\mathrm{GF}(q^n)$.

For simplicity, we set $b = 2$, $B = \{0, 1\}$, and $k = k(\kappa, \mu) = \lceil \lg q \rceil$. Other choices are possible. For simplicity, we let $\zeta = \zeta(n)$ denote a fixed $\omega(\sqrt{\lg n})$ function. Let $s = s(\kappa, \mu)$ and $\alpha = \alpha(\kappa, \mu)$ be positive reals that define the Gaussians.

5.1 Construction

$\mathsf{Setup}(1^\kappa, n, q, m, \ell, s, \alpha, \mathfrak{g}, k)$**:** On input a security parameter 1^κ and additional parameters:

1. Generate a random matrix with a trapdoor by running $(\boldsymbol{A}, \boldsymbol{R}_{\boldsymbol{A}}) \leftarrow \mathsf{GenTrap}(1^\kappa, q, n, m)$.
2. Choose μ uniformly random matrices $\boldsymbol{B}_i \leftarrow \mathbb{Z}_q^{n \times nk}$ for $i \in [\mu]$.
3. Choose a random matrix $\boldsymbol{U} = [\boldsymbol{u}_1 \mid \cdots \mid \boldsymbol{u}_\ell] \leftarrow \mathbb{Z}_q^{n \times \ell}$.

Output $pp = ((n, q, m, \ell, s, \alpha, \mathfrak{g}, k), \boldsymbol{A}, \{\boldsymbol{B}_i\}, \boldsymbol{U})$ and $msk = (\boldsymbol{R}_{\boldsymbol{A}}, pp)$.

$\mathsf{Extract}(pp, msk, \vec{v})$**:** On input a key-attribute vector $\vec{v} = (\mathfrak{v}_1, \ldots, \mathfrak{v}_\mu)^\top \in \mathrm{GF}(q^n)^\mu$:

1. Define the matrices $\boldsymbol{B}_{\vec{v}} = \sum_{i=1}^{\mu} \boldsymbol{B}_i \cdot H_{\boldsymbol{g}}(\mathfrak{v}_i) \in \mathbb{Z}_q^{n \times nk}$ and $\boldsymbol{A}_{\vec{v}} = [\boldsymbol{A} \mid \boldsymbol{B}_{\vec{v}}] \in \mathbb{Z}_q^{n \times (m+nk)}$.
2. Sample vectors $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_\ell$ by using the master secret key $\boldsymbol{R}_{\boldsymbol{A}}$; Formally, for $i = 1, \ldots, \ell$, take sample $\boldsymbol{e}_i \leftarrow \mathsf{SampleD}(\boldsymbol{R}_{\boldsymbol{A}}, \boldsymbol{A}_{\vec{v}}, \boldsymbol{I}, \boldsymbol{u}_i, s)$.
3. Set $\boldsymbol{E}_{\vec{v}} = [\boldsymbol{e}_1 \mid \cdots \mid \boldsymbol{e}_\ell]$. (Notice that $\boldsymbol{A}_{\vec{v}} \cdot \boldsymbol{E}_{\vec{v}} = \boldsymbol{U}$.)

Output $dk_{\vec{v}} = \boldsymbol{E}_{\vec{v}}$.

$\mathsf{Enc}(pp, \vec{w}, \boldsymbol{m})$**:** On input pp, a ciphertext-attribute vector $\vec{w} = (\mathfrak{w}_1, \ldots, \mathfrak{w}_\mu)^\top \in \mathrm{GF}(q^n)^\mu$, and a message $\boldsymbol{m} \in \{0, 1\}^\ell$:

1. Choose a random vector $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$.

2. Set $\boldsymbol{c}_0 \leftarrow \boldsymbol{A}^\top \boldsymbol{s} + \boldsymbol{x}_0$, where $\boldsymbol{x}_0 \leftarrow \chi^m$.
3. Set $\boldsymbol{c}' \leftarrow \boldsymbol{U}^\top \boldsymbol{s} + \boldsymbol{x}' + \lfloor q/2 \rfloor \boldsymbol{m}$, where $\boldsymbol{x}' \leftarrow \chi^\ell$.
4. For $i = 1, \ldots, \mu$; sample $\boldsymbol{R}_i \leftarrow \{-1, +1\}^{m \times nk}$ and set $\boldsymbol{c}_i \leftarrow (\boldsymbol{B}_i + H(\mathfrak{w}_i) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_i^\top \boldsymbol{x}_0 \in \mathbb{Z}_q^{nk}$.
5. Output $ct = (\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\mu, \boldsymbol{c}')$.

$\mathsf{Dec}(pp, dk_{\vec{v}}, ct)$**:** On input pp, a decryption key $\boldsymbol{E}_{\vec{v}}$, and $ct = (\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\mu, \boldsymbol{c}')$:

1. Compute $\boldsymbol{c}_{\vec{v}} \leftarrow \sum_{i=1}^{\mu} H_{\boldsymbol{g}}(\mathfrak{v}_i) \cdot \boldsymbol{c}_i$.
2. Let $\boldsymbol{c} \leftarrow [\boldsymbol{c}_0; \boldsymbol{c}_{\vec{v}}] \in \mathbb{Z}_q^{m+\tilde{m}}$.
3. Compute $\boldsymbol{d} \leftarrow \boldsymbol{c}' - \boldsymbol{E}_{\vec{v}}^\top \boldsymbol{c} \bmod q$ and output $\lfloor (2/q)\boldsymbol{d} \rceil \bmod 2$.

Remark 5.1. In the following, we will take the noise of $\boldsymbol{c}_0$ and $\boldsymbol{c}'$ from $\chi = \bar{\Psi}_\alpha$. We note that $\bar{\Psi}_\alpha$ has a good tail bound on the inner product and this is why we employ the conservative distribution $\bar{\Psi}_\alpha$.

We can replace the distribution $\bar{\Psi}_\alpha$ with $D_{\mathbb{Z},\sigma}$. We then change the noises $\boldsymbol{x}_i$ with $\boldsymbol{x}_i \leftarrow D_{\mathbb{Z},r}^{nk}$ where $r = \sqrt{\|\boldsymbol{x}_0\|^2 + nk\sigma^2} \cdot \zeta$ as in the CCA2 secure PKE scheme in [35]. The problem $\mathrm{LWE}(n, q, D_{\mathbb{Z}, \sqrt{2} \cdot \alpha q})$ is as hard as $\mathrm{LWE}(n, q, \bar{\Psi}_\alpha)$, which is shown by Gordon, Katz, and Vaikuntanathan [28, Lemma 1] employing [42, Theorem 3.1]. Hence, even if we change the noise distribution from $\bar{\Psi}_\alpha$ to $D_{\mathbb{Z}, \sqrt{2}\alpha q}$, we can reduce the security to the lattice problems.

5.2 Correctness, Security, and Parameters

The scheme is correct and secure as the following theorems.

Theorem 5.1. *Let $\chi = \bar{\Psi}_\alpha$. Suppose that $s > 4Cm \cdot \omega(\sqrt{\lg n})$ and $(\alpha q \cdot \omega(\sqrt{\lg \kappa}) + \sqrt{m}/2) \cdot 4C\mu s m^2 < q/5$. Then our scheme is correct.*

Theorem 5.2. *Let $m = 2n \lg q + \omega(\lg \kappa)$ and $s \geq 3C\mu m^{1.5} \cdot \omega(\sqrt{\lg n})$. Suppose that the $\mathrm{LWE}(n, q, \chi)$ assumption holds. Then, the scheme is selectively and weakly attribute hiding.*

The proofs are obtained by merging those of [6] and [35]. We defer the proofs to the full version of the paper.

Parameter settings: Let us summarize the constraints on the parameters:

- To satisfy the correctness (Theorem 5.1), we require that $\chi = \bar{\Psi}_\alpha$, $s > 4Cm\omega(\sqrt{\lg n})$, and $(\alpha q \cdot \omega(\sqrt{\lg \kappa}) + \sqrt{m}/2) \cdot 4C\mu s m^2 < q/5$. For example, we can take $q = \Omega(\mu m^{5/2} s)$ and $\alpha \leq \left(\mu m^2 s \cdot \omega(\sqrt{\lg \kappa})\right)^{-1}$ to satisfy the above condition with $q\alpha \cdot \omega(\sqrt{\lg \kappa}) = \sqrt{m}/2$.
- From the security (Theorem 5.2), we obtain the bound that $m = 2n \lg q + \omega(\lg \kappa)$ and $s \geq 3C\mu m^{1.5} \cdot \omega(\sqrt{\lg n})$.
- In order to reduce the security to the worst-case hardness of lattice problems, we require that $q\alpha > 2\sqrt{n}$ and $1/\alpha = \mathrm{poly}(n)$.

For example, the following setting fulfills the above requirements:

$$k = \lceil \lg q \rceil, \qquad \zeta = \omega(\sqrt{\lg(2m)}), \qquad m = 3n \lg q,$$
$$s = 3C\mu m^{1.5} \cdot \zeta, \qquad q = 60C^2\mu^2 \cdot m^4 \cdot \zeta, \qquad \alpha = (120C^2\mu^2 \cdot m^{3.5} \cdot \zeta^2)^{-1}.$$

By these settings, the security is based on the worst-case hardness of GapSVP_γ or SIVP_γ, where $\gamma = \tilde{\Omega}(\mu^2 n^{4.5})$, while the AFV scheme is based on that with $\gamma = \tilde{\Omega}(\mu^2 n^4)$. (We note that if the AFV scheme also employs the Micciancio–Peikert trapdoor [35] as we did, γ is reduced to $\tilde{\Omega}(\mu^2 n^{3.5})$.)

In our scheme, the size of the public parameter is $nm \lg q + \mu n^2 k \lg q + \ell n \lg q = \Theta(\mu n^2 \lg^2 q) = \tilde{\Theta}(\mu n^2)$, and the size of the ciphertext is $m \lg q + \mu n k \lg q + \ell \lg q = \Theta(\mu n \lg^2 q)$, where ℓ denotes the length of plaintexts.

6 Fuzzy Identity-based Encryption

In this section, we construct a FIBE scheme from a weakly attribute-hiding IPE scheme in general way. We first review the embedding of exact threshold by Katz, Sahai, and Waters. If the IPE scheme hides attribute weakly, we can take logical disjunction in a lazy way as Waters pointed out [6, Remark 5.1 of the ePrint version].

Exact threshold: For binary vector $\vec{x} \in \{0,1\}^N$, $H_w(\vec{x})$ denotes a Hamming weight of $\vec{x}$, that is, the number of 1 in $\vec{x}$. For binary vectors $\vec{a}, \vec{x} \in \{0,1\}^u$, the exact threshold predicate is denoted by $\mathcal{P}^{\mathsf{th}}_{=t}(\vec{a}, \vec{x})$ and outputs 1 if and only if $H_w(\vec{a} \,\&\, \vec{x}) = t$, where $\&$ denotes the logical conjunction. Suppose that $t < q$. Katz, Sahai, and Waters [30] gave an embedding $\mathcal{P}^{\mathsf{th}}_{=t}$ into $\mathcal{P}^{\mathsf{ipe}}$ as follows:

$$\mu = N + 1,\ \vec{v} = (\vec{a}, 1) \in \mathbb{Z}_q^\mu, \text{ and } \vec{w} = (\vec{x}, -t) \in \mathbb{Z}_q^\mu.$$

We have that $\vec{w}^\top \vec{v} = 0$ if and only if $H_w(\vec{a} \,\&\, \vec{x}) = t$.

6.1 Construction

Now, we implement FIBE on small universe $\{0,1\}$ from IPE. Let $\{0,1\}^N$ be a space of identities. The threshold predicate over $\{0,1\}^N$ is defined by $\mathcal{P}^{\mathsf{th}}_{\geq t}(\vec{a}, \vec{x}) = 1$ if and only if $H_w(\vec{a} \,\&\, \vec{x}) \geq t$.

We observe that the above predicate can be written as $\bigvee_{i=t}^N \mathcal{P}^{\mathsf{th}}_{=i}(\vec{a}, \vec{x})$. Hence, repeating ciphertexts of an IPE scheme that supports the relations $\mathcal{P}^{\mathsf{th}}_{=i}$ for $i = t, \ldots, N$, we can implement a FIBE scheme by the relation $\mathcal{P}^{\mathsf{th}}_{\geq t}$.

When we employ our IPE scheme, the obtained scheme has a ciphertext of length $(N - t + 1) \cdot O(Nm \lg q) = O(N^2 n \lg^2 q)$ and enjoys the security reduced to the worst-case hardness of lattice problems with approximation factor $\tilde{O}(n^{4.5})$.

Comparison: Agrawal et al. already presented FIBE schemes from lattices [5]. Their small-universe construction is defined with the identity space $\{0,1\}^N$ as in our case. They gave concrete parameter settings for $\epsilon \in (0, 1/2)$ as follows:

$$N = n^\epsilon, q \in [n^6 2^{5N}, 2n^6 2^{5N}], m = n^{1.5} \geq 5n \lg q, \text{ and } \alpha = 2\sqrt{m}/q = 1/(2^{5n^\epsilon} \cdot \mathrm{poly}(n)).$$

The length of the ciphertext is $N \cdot O(m \lg q) = O(n^{1.5+2\epsilon} \lg n)$. The security is reduced to the worst-case hardness of $2^{O(n^\epsilon)}$-approximating gapSVP or SIVP using $2^{O(n^\epsilon)}$-time algorithms, which is stronger assumption than that we employ.

We finally note that, their scheme allows identity space $(\mathbb{Z}_q^n)^u$ without drastic changes of parameters whereas our scheme cannot.

Acknowledgments

The author thanks Damien Stehlé, Chris Peikert, Daniele Micciancio, and reviewers for helpful discussions and comments.

References

1. Abdalla, M., Birkett, J., Catalano, D., Dent, A.W., Malone-Lee, J., Neven, G., Schuldt, J.C.N., Smart, N.P.: Wildcarded identity-based encryption. Journal of Cryptology 24(1), 42–82 (2011), combined and extended of two papers [2,11]
2. Abdalla, M., Catalano, D., Dent, A.W., Malone-Lee, J., Neven, G., Smart, N.P.: Identity-based encryption gone wild. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006, Part II. LNCS, vol. 4052, pp. 300–311. Springer, Heidelberg (2006), the full version is available at `http://eprint.iacr.org/2006/304`
3. Abdalla, M., De Caro, A., Mochetti, K.: Lattice-based hierarchical inner product encryption. In: Hevia, A., Neven, G. (eds.) LATINCRYPT 2012. LNCS, vol. 7533, pp. 121–138. Springer, Heidelberg (2012)
4. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert [27], pp. 553–572
5. Agrawal, S., Boyen, X., Vaikuntanathan, V., Voulgaris, P., Wee, H.: Functional encryption for threshold functions (or, fuzzy IBE) from lattices. In: Fischlin et al. [25], pp. 280–297
6. Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: Functional encryption for inner product predicates from learning with errors. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 21–40. Springer, Heidelberg (2011), the full version is available at `http://eprint.iacr.org/2011/410`
7. Ajtai, M.: Generating hard instances of the short basis problem. In: Wiedermann, J., van Emde Boas, P., Nielsen, M. (eds.) ICALP '99. LNCS, vol. 1644, pp. 1–9 (1999)
8. Alperin-Sheriff, J., Peikert, C.: Circular and KDM security for identity-based encryption. In: Fischlin et al. [25], pp. 334–352
9. Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. In: Albers, S., Marion, J.Y. (eds.) STACS 2009. LIPIcs, vol. 3, pp. 75–86. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, Germany (2009)
10. Attrapadung, N., Libert, B.: Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 384–402. Springer, Heidelberg (2010)

11. Birkett, J., Dent, A.W., Neven, G., Schuldt, J.C.N.: Efficient chosen-ciphertext secure identity-based encryption with wildcards. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 274–292. Springer, Heidelberg (2007)
12. Boneh, D., Boyen, X.: Efficient selective identity-based encryption without random oracles. Journal of Cryptology 24(4), 659–693 (2011), a preliminary version appeared in *EUROCRYPT 2004*, 2004
13. Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM Journal on Computing 36(5), 1301–1328 (12 2006)
14. Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption schemes. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer, Heidelberg (2008)
15. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)
16. Boyen, X.: Attribute-based encryption from lattices (2012), to appear *TCC 2013*.
17. Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical GapSVP. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 868–886. Springer, Heidelberg (2012), see also `http://eprint.iacr.org/2012/078`
18. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. In: Goldwasser, S. (ed.) ITCS 2012. pp. 309–325. ACM (2012), see also `http://eprint.iacr.org/2011/277`
19. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: FOCS 2011. pp. 97–106. IEEE Computer Society (2011), see also `http://eprint.iacr.org/2011/344`
20. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert [27], pp. 523–552
21. Chen, J., Lim, H.W., Ling, S., Wang, H.: The relation and transformation between hierarchical inner product encryption and spatial encryption. Cryptology ePrint Archive, Report 2011/455 (2011), available at `http://eprint.iacr.org/2011/455`
22. Chen, J., Lim, H.W., Ling, S., Wang, H., Nguyen, T.T.K.: Revocable identity-based encryption from lattices. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 390–403. Springer, Heidelberg (2012), the full version is available at `http://eprint.iacr.org/2011/583`
23. Cramer, R., Damgård, I.: On the amortized complexity of zero-knowledge protocols. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 177–191. Springer, Heidelberg (2009)
24. Dwork, C. (ed.): Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008. ACM (2008)
25. Fischlin, M., Buchmann, J., Manulis, M. (eds.): Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proceedings, LNCS, vol. 7293. Springer, Heidelberg (2012)
26. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork [24], pp. 197–206, see also `http://eprint.iacr.org/2007/432`
27. Gilbert, H. (ed.): Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30-June 3, 2010. Proceedings, LNCS, vol. 6110. Springer, Heidelberg (2010)
28. Gordon, S.D., Katz, J., Vaikuntanathan, V.: A group signature scheme from lattice assumptions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 395–412. Springer, Heidelberg (2010)
29. Hamburg, M.: Spatial Encryption. Ph.D. thesis, Stanford University (2011), available at `http://eprint.iacr.org/2011/389`

30. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008), the full version is available at http://eprint.iacr.org/2007/404
31. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert [27], pp. 62–91, the full version is available at http://eprint.iacr.org/2010/110
32. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert [27], pp. 1–23
33. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity 16, 365–411 (2007), a preliminary version appeared in *FOCS 2002*, 2002. See also ECCC TR04-095
34. Micciancio, D., Peikert, C.: Private communication (December 2012), 2012-12-10
35. Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Pointcheval and Johansson [44], pp. 700–718, available at http://eprint.iacr.org/2011/501
36. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)
37. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin [45], pp. 191–208, the full version is available at http://eprint.iacr.org/2010/563
38. Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 138–159. Springer, Heidelberg (2011), the full version is available at http://eprint.iacr.org/2010/648
39. Okamoto, T., Takashima, K.: Adaptively attribute-hiding (hierarchical) inner product encryption. In: Pointcheval and Johansson [44], pp. 591–608, the full version is available at http://eprint.iacr.org/2010/543
40. Park, J.H.: Inner-product encryption under standard assumptions. Designs, Codes and Cryptography 58(3), 235–257 (March 2011)
41. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Mitzenmacher, M. (ed.) STOC 2009. pp. 333–342. ACM (2009)
42. Peikert, C.: An efficient and parallel gaussian sampler for lattices. In: Rabin [45], pp. 80–97
43. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: Dwork [24], pp. 187–196
44. Pointcheval, D., Johansson, T. (eds.): Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings, LNCS, vol. 7237. Springer, Heidelberg (2012)
45. Rabin, T. (ed.): Advances in Cryptology - CRYPTO 2010, 30th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings, LNCS, vol. 6223. Springer, Heidelberg (2010)
46. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM 56(6), Article 34 (2009), a preliminary version appeared in *STOC 2005*, 2005.
47. Stehlé, D.: Private communication (December 2012), 2012-12-12
48. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005), the full version is available at http://eprint.iacr.org/2004/180