SCIENCE CHINA
Information Sciences

• LETTER •

March 2019, Vol. 62 039101:1–039101:3
https://doi.org/10.1007/s11432-017-9412-3

A more compact multi-id identity-based FHE scheme in the standard model and its applications

Xueqing WANG[1,2*], Biao WANG[1,2], Bei LIANG[3] & Rui XUE[1,2*]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049*, China;*
[3]*Department of Computer Science and Engineering, Chalmers University of Technology, Gothenburg* SE-41296*, Sweden*

Received 25 December 2017/Accepted 16 March 2018/Published online 11 September 2018

Citation Wang X Q, Wang B, Liang B, et al. A more compact multi-id identity-based FHE scheme in the standard model and its applications. Sci China Inf Sci, 2019, 62(3): 039101, https://doi.org/10.1007/s11432-017-9412-3

Dear editor,

Fully homomorphic encryption (FHE) is a cryptographic primitive that allows anyone, even those without a secret key, to perform arbitrary computation on encrypted data. Since Gentry's breakthrough realization of FHE in 2009 [1], the research on FHE has been blown out. Furthermore, López-Alt et al. [2] proposed a new notion of multi-key FHE (MFHE), in which it is possible to compute on encrypted messages even if they were not encrypted using the same key.

Identity-based encryption (IBE) is another primitive that allows one to encrypt messages by public keys that can be efficiently derived from identity strings and system public parameters. The public parameters are chosen by a trusted authority along with a secret trapdoor, which is used to extract secret keys from users' identities. Different from previous schemes with classical algebraic structures, the work of Gentry et al. [3] constructed the first IBE scheme under the DLWE assumption in the random oracle (RO) model (abbreviated as GPV-IBE).

The advantages of combining both IBE and FHE make the identity-based fully homomorphic encryption (IBFHE) much appealing. Multi-id IBFHE (MIBFHE) is the counterpart of MFHE in the identity-based setting. However, till now, there are few results in the construction of IBFHE, and so is for that of MIBFHE. Gentry et al. [4] once described a compiler that can transform any existed lattice-based IBE schemes into IBFHE schemes. Clear and McGoldrick [5] presented a quite complex ciphertext expanding technique to construct a single-hop MIBFHE scheme based on GPV-IBE and the work of Gentry et al. [4]. Recently, for constructing IND-CCA1 secure FHE schemes, Canetti et al. [6] proposed a generic construction of MIBFHE, with the weakest compactness[1)], from MFHE and IBE in the black-box form.

In this study, we use a simpler ciphertext expansion technique to construct a more compact[2)] MIBFHE scheme secure in the standard model. The simpler ciphertext expansion technique is the identity counterpart of the one proposed by Mukherjee and Wichs for constructing an MFHE scheme [7] and needs deterministic key derivation[3)]. So we first construct an IBE scheme with such a property with a puncturable pseudorandom function (PPRF) and an indistinguishability obfuscator ($i\mathcal{O}$), the use of which are sufficient for achieving the property.

* Corresponding author (email: wangxueqing@iie.ac.cn, xuerui@iie.ac.cn)

1) The size of the result ciphertext from homomorphic evaluation is linear with the number of input ciphertexts.
2) The size of the result ciphertext from homomorphic evaluation is linear with the number of involving identities.
3) The explanation can be found in Appendix A.

Notations. We use bold lower case letters (e.g., $\boldsymbol{a}, \boldsymbol{b}$) to denote column vectors, bold upper case letters (e.g., $\boldsymbol{A}, \boldsymbol{B}$) to denote matrices, and bold calligraphy (e.g., $\vec{\mathcal{M}}$) to denote a sequence of matrices in the matrix form as required. For a matrix $\boldsymbol{A}$, $\boldsymbol{A}[i,j]$ denotes the entry in the i-th row and the j-th column, and $\|\boldsymbol{A}\|_\infty = \max_{i,j}\{|\boldsymbol{A}[i,j]|\}$ represents the infinity norm. Similarly to the norm of vectors. For any integer q, the notation ℓ_q refers to $\lceil \log_2 q \rceil$. For a set S, $s \xleftarrow{\$} S$ represents the operation of sampling element s from S uniformly at random. For $k \in \mathbb{N}$, $[k]$ denotes the set $\{1, \ldots, k\}$.

Remark 1. The definition of MIBFHE and other related definitions are provided in Appendix B.

IBE construction. Let n, q and B_χ-bounded error distribution χ be proper parameters for the $\mathsf{DLWE}_{n,q,\chi}$ assumption, $m = \mathcal{O}(n\ell_q)$, $i\mathcal{O}$ be an indistinguishability obfuscator, and $\mathsf{F} : \mathcal{K} \times \{0,1\}^{k(\lambda)} \to \{0,1\}^m$ be a puncturable family of PRFs equipped with ($\mathsf{F.Key}$, $\mathsf{F.Puncture}$), where $k(\cdot)$ is a computable function in λ.

• $\mathsf{IBE.Setup}(\cdot)$: On input 1^λ, sample $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, generate a key of PPRF $K \leftarrow \mathsf{F.Key}(1^\lambda)$ and an obfuscated program $\mathsf{H} \leftarrow i\mathcal{O}(\lambda, \mathsf{RelateID})$, where the program $\mathsf{RelateID}$ is shown in Figure 1. Output $\mathtt{mpk} = (\boldsymbol{A}, \mathsf{H})$ and $\mathtt{msk} = K$.

Input: $\mathrm{id} \in \{0,1\}^k$
Constants: $\boldsymbol{A}, K$
1. $\boldsymbol{w}_{\mathrm{id}} := \mathsf{F}(K, \mathrm{id}) \in \{0,1\}^m$,
2. output $\boldsymbol{u}_{\mathrm{id}} := \boldsymbol{A}\boldsymbol{w}_{\mathrm{id}} \in \mathbb{Z}_q^n$.

Figure 1 Program $\mathsf{RelateID}$.

• $\mathsf{IBE.KeyGen}(\cdot,\cdot)$: On input $\mathtt{msk}$ and $\mathrm{id} \in \{0,1\}^k$, evaluate $\boldsymbol{w}_{\mathrm{id}} := \mathsf{F}(K, \mathrm{id}) \in \{0,1\}^m$ and output $\boldsymbol{s}_{\mathrm{id}} = (1, \boldsymbol{w}_{\mathrm{id}}^{\mathrm{T}})^{\mathrm{T}} \in \{0,1\}^{m+1}$.

• $\mathsf{IBE.Enc}(\cdot,\cdot,\cdot)$: On input $\mathtt{mpk}$, $\mathrm{id} \in \{0,1\}^k$ and $\mu \in \{0,1\}$, sample $\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^n$, $\boldsymbol{e} \leftarrow \chi^{m+1}$ and generate $\boldsymbol{u}_{\mathrm{id}} \leftarrow \mathsf{H}(\mathrm{id})$, $\boldsymbol{A}_{\mathrm{id}} := (\boldsymbol{u}_{\mathrm{id}} || -\boldsymbol{A}) \in \mathbb{Z}_q^{n\times(m+1)}$. Compute and output

$$\boldsymbol{c}_{\mathrm{id}} := \boldsymbol{A}_{\mathrm{id}}^{\mathrm{T}}\boldsymbol{r} + \boldsymbol{e} + \left(\mu \cdot \left\lfloor \frac{q}{2} \right\rfloor, \boldsymbol{0}_{1\times m}\right)^{\mathrm{T}} \in \mathbb{Z}_q^{m+1}.$$

Note that $\boldsymbol{A}_{\mathrm{id}} \cdot \boldsymbol{s}_{\mathrm{id}} = \boldsymbol{0} \mod q$.

• $\mathsf{IBE.Dec}(\cdot,\cdot)$: On input $\boldsymbol{s}_{\mathrm{id}}$ and $\boldsymbol{c}_{\mathrm{id}}$, compute $\delta := \langle \boldsymbol{s}_{\mathrm{id}}, \boldsymbol{c}_{\mathrm{id}} \rangle$ and output $\lfloor \frac{\delta}{q/2} \rceil$.

Note that this scheme is correct because decryption works as follows:

$$\langle \boldsymbol{s}_{\mathrm{id}}, \boldsymbol{c}_{\mathrm{id}} \rangle = \langle \boldsymbol{s}_{\mathrm{id}}, \boldsymbol{e} \rangle + \mu \left\lfloor \frac{q}{2} \right\rfloor,$$

where $\|\langle \boldsymbol{s}_{\mathrm{id}}, \boldsymbol{e} \rangle\|_\infty \leqslant (m+1)B_\chi$, and μ can be decrypted correctly as long as $(m+1)B_\chi \leqslant q/4$. We confirm the security of the scheme by Theorem 1.

Theorem 1 (Security)**.** The above scheme IBE is INDr-sID-CPA secure[4] in the standard model if the $\mathsf{DLWE}_{n,q,\chi}$ assumption holds, $i\mathcal{O}$ is an indistinguishability obfuscator and F is a puncturable family of PRFs.

Proof. Refer to Appendix C.

Single-hop MIBFHE construction. For a modulus q, we first recall a gadget vector $\boldsymbol{g} = (2^0, 2^1, \ldots, 2^{\ell_q - 1})^{\mathrm{T}} \in \mathbb{Z}_q^{\ell_q}$ [8]. Note that the last entry 2^{ℓ_q-1} of $\boldsymbol{g}$ is in the interval $[q/2, q) \bmod q$. And hence we define a slightly variant of the gadget matrix from previous work [7,8]:

$$\boldsymbol{G}_m = \boldsymbol{I}_m \otimes \boldsymbol{g} = \mathrm{diag}(\boldsymbol{g}, \ldots, \boldsymbol{g}) \in \mathbb{Z}_q^{m\ell_q \times m}.$$

Correspondingly, we define the inverse function $\boldsymbol{G}_m^{-1} : \mathbb{Z}_q^{m\ell_q\times m} \to \{0,1\}^{m\ell_q \times m\ell_q}$ which decomposes each entry of the input matrix into a row of size ℓ_q in binary representation. We have the property that for any matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\ell_q\times m}$, it holds that $\boldsymbol{G}_m^{-1}(\boldsymbol{A}) \cdot \boldsymbol{G}_m = \boldsymbol{A}$.

• $\mathsf{SMIBFHE.Setup}(\cdot)$: On input 1^λ, do the same as $\mathsf{IBE.Setup}(1^\lambda)$, and finally output $\mathtt{mpk} = (\boldsymbol{A}, \mathsf{H})$ and $\mathtt{msk} = K$.

• $\mathsf{SMIBFHE.KeyGen}(\cdot,\cdot)$: On input $\mathtt{msk}$ and $\mathrm{id} \in \{0,1\}^k$, do the same as $\mathsf{IBE.KeyGen}(\mathtt{msk}, \mathrm{id})$ and output $\boldsymbol{s}_{\mathrm{id}} = (1, \boldsymbol{w}_{\mathrm{id}}^{\mathrm{T}})^{\mathrm{T}}$.

• $\mathsf{SMIBFHE.Enc}(\cdot,\cdot,\cdot)$: On input $\mathtt{mpk}$, $\mathrm{id} \in \{0,1\}^k$ and $\mu \in \{0,1\}$, choose $\boldsymbol{S} \leftarrow \chi^{(m+1)\ell_q\times n}$, $\boldsymbol{E} \leftarrow \chi^{(m+1)\ell_q\times(m+1)}$, and compute $\boldsymbol{u}_{\mathrm{id}} \leftarrow \mathsf{H}(\mathrm{id})$, $\boldsymbol{A}_{\mathrm{id}} := (\boldsymbol{u}_{\mathrm{id}} || -\boldsymbol{A})$, $\boldsymbol{C}_{\mathrm{id}} := \boldsymbol{S}\boldsymbol{A}_{\mathrm{id}} + \boldsymbol{E} + \mu\boldsymbol{G}_{m+1} \in \mathbb{Z}_q^{(m+1)\ell_q\times(m+1)}$. Additionally, for $i \in [(m+1)\ell_q], j \in [n]$, we sample $\boldsymbol{S}_{i,j} \xleftarrow{\$} \mathbb{Z}_q^{(m+1)\ell_q\times n}$ and $\boldsymbol{E}_{i,j} \leftarrow \chi^{(m+1)\ell_q\times(m+1)}$, and compute $\vec{\boldsymbol{S}}[i,j] := \boldsymbol{S}_{i,j}\boldsymbol{A}_{\mathrm{id}} + \boldsymbol{E}_{i,j} + \boldsymbol{S}[i,j]\boldsymbol{G}_{m+1} \in \mathbb{Z}_q^{(m+1)\ell_q\times(m+1)}$. Output the ciphertext $\boldsymbol{C}_{\mathrm{id}}$ associated with the materials for homomorphic evaluation $(\mathrm{id}, \vec{\boldsymbol{S}})$.

• $\mathsf{SMIBFHE.Dec}(\cdot,\cdot)$: On input $(\boldsymbol{s}_{\mathrm{id}_1}, \ldots, \boldsymbol{s}_{\mathrm{id}_N})$ and $\widehat{\boldsymbol{C}}$, let $\hat{\boldsymbol{c}}$ be the ℓ_q-th row of $\widehat{\boldsymbol{C}}$ and $\hat{\boldsymbol{s}} := (\boldsymbol{s}_{\mathrm{id}_1}^{\mathrm{T}} || \ldots || \boldsymbol{s}_{\mathrm{id}_N}^{\mathrm{T}})^{\mathrm{T}}$. Compute $\delta := \langle \hat{\boldsymbol{c}}, \hat{\boldsymbol{s}} \rangle$. Output $\lfloor \frac{\delta}{2^{\ell_q-1}} \rceil$.

• $\mathsf{SMIBFHE.Eval}(\cdot,\cdot,\cdot)$: On input $\mathtt{mpk}, f$, and $(\boldsymbol{C}_{\mathrm{id}_1}, (\mathrm{id}_1, \vec{\mathcal{S}}_1)), \ldots, (\boldsymbol{C}_{\mathrm{id}_N}, (\mathrm{id}_N, \vec{\mathcal{S}}_N))$, assume, without loss of generality, that these ciphertexts are under t different identities $\mathrm{id}_1, \ldots, \mathrm{id}_t$, respectively, and that f consists only of NAND gates with fan-in 2, which can be evaluated homomorphically gate by gate.

4) INDr-sID-CPA security implies anonymity and IND-sID-CPA security.

At first, we expand each ciphertext of message $\boldsymbol{C}_{\mathrm{id}_i}$ into $\widehat{\boldsymbol{C}}_{\mathrm{id}_i}$ with t time size, for $i \in [N]$, where $\widehat{\boldsymbol{C}}_{\mathrm{id}_i}$ consists of $t \times t$ sub-blocks with $\boldsymbol{C}_{\mathrm{id}_i}$ in the diagonal entries, $\boldsymbol{X}_j$ in the j-th row and the i-th column entry and $\boldsymbol{0}_{(m+1)\ell_q \times (m+1)}$ in others. Now, we construct

$$\boldsymbol{X}_j := \sum_{a=1}^{(m+1)\ell_q} \sum_{b=1}^{n} \boldsymbol{G}_{m+1}^{-1}(\boldsymbol{U}_{a,b})\vec{\mathcal{S}}_i[a,b],$$

in which the entry in the a-th row and the first column of $\boldsymbol{U}_{a,b}$ is the b-th entry of $\mathsf{H}(\mathrm{id}_j) - \mathsf{H}(\mathrm{id}_i)$. And then for each NAND gate with two inputs $\widehat{\boldsymbol{C}}_i$ and $\widehat{\boldsymbol{C}}_j$, compute the result ciphertext $\boldsymbol{G}_{t(m+1)\ell_q \times t(m+1)} - \boldsymbol{G}_{t(m+1)}^{-1}(\widehat{\boldsymbol{C}}_i) \times \widehat{\boldsymbol{C}}_j$. Finally, after computing all NAND gates of f, output the final result ciphertext.

The correctness of the scheme is presented in the following lemma.

Lemma 1 (Expand correctness)**.** For any polynomial N on λ and N different identities $\mathrm{id}_1, \ldots, \mathrm{id}_N$, any ciphertexts $\boldsymbol{C}_{\mathrm{id}_i}$ of μ with ciphertexts $\vec{\mathcal{S}}_i$ of its randomness $\boldsymbol{S}_i$, in which the error distribution χ is B_χ-bounded, the expanded ciphertext $\widehat{\boldsymbol{C}}_{\mathrm{id}_i}$ is the ciphertext of μ under $(\mathrm{id}_1, \ldots, \mathrm{id}_N)$ with $\mathcal{O}(m^4 \ell_q B_\chi)$ noise.

Proof. Refer to Appendix D.

Theorem 2 (Security)**.** The single-hop MIBFHE scheme $\mathsf{SMIBFHE}$ is IND-sID-CPA secure in the standard model if the IBE scheme IBE is IND-sID-CPA secure in the standard model, $i\mathcal{O}$ is an indistinguishability obfuscator, and F is a puncturable family of PRFs.

Remark 2. Because the homomorphic evaluation ability of the adversary against the IND-sID-CPA security of MIBFHE is useless for it in the game, the proof for Theorem 2 is similar to that for Theorem 1.

Applications of our single-hop MIBFHE. In [8], Brakerski and Perlman proposed a fully dynamic MFHE scheme (abbreviated as BP), from a single-hop MFHE scheme, with a short ciphertext of size $n\ell_q$ and a comparatively large public key of size $\mathcal{O}(n^5 \ell_q^5)$. Although the generic construction of MIBFHE in [6] can be fully dynamic initiated with BP scheme together with an IBE scheme, it has inherited the disadvantage of BP scheme, which contains the large public key of BP scheme as a part of its ciphertext. We construct a fully dynamic MIBFHE scheme, in Appendix E, from our single-hop MIBFHE scheme, which inherits the advantage of short ciphertext in BP scheme.

In addition, our single-hop or fully dynamic MIBFHE scheme can also be used to construct an IND-CCA1 FHE scheme through the transformation in the work of Canetti et al. [6].

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61472414, 61772514, 61602061) and National Key Research and Development Program of China (Grant No. 2017YFB1400700).

Supporting information Appendixes A–E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of ACM Symposium on Theory of Computing, Bethesda, 2009. 169–178
2 López-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the 44th ACM Symposium on Theory of Computing, New York, 2012. 1219–1234
3 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, 2008. 197–206
4 Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Proceedings of the 33rd Annual Cryptology Conference, Santa Barbara, 2013. 75–92
5 Clear M, McGoldrick C. Multi-identity and multi-key leveled FHE from learning with errors. In: Proceedings of the 35th Annual Cryptology Conference, Santa Barbara, 2015. 630–656
6 Canetti R, Raghuraman S, Richelson S, et al. Chosen-ciphertext secure fully homomorphic encryption. In: Proceedings of the 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, 2017. 213–240
7 Mukherjee P, Wichs D. Two round multiparty computation via multi-key FHE. In: Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, 2016. 735–763
8 Brakerski Z, Perlman R. Lattice-based fully dynamic multi-key FHE with short ciphertexts. In: Proceedings of the 36th Annual International Cryptology Conference, Santa Barbara, 2016. 190–213