Cybersecurity

RESEARCH Open Access

CCA1 secure FHE from PIO, revisited

Biao Wang[1,2*], Xueqing Wang[1,2] and Rui Xue[1,2]

Abstract

Fully homomorphic encryption (FHE) is a powerful cryptographic primitive that allows anyone to compute on encrypted data using only public information. So far, most FHE schemes are CPA secure. In PKC 2017, Canetti et al. extended the generic transformation of Boneh, Canetti, Halevi and Katz to turn any multi-key identity-based FHE scheme into a CCA1-secure FHE scheme. Their main construction of multi-key identity-based FHE is from probabilistic indistinguishability obfuscation (PIO) and statistical trapdoor encryption.

We show that the above multi-key identity-based FHE is not secure by giving an attack. Then we give a solution to avoid the attack and redesign a more succinct and efficient multi-key identity-based FHE scheme. Compared with the scheme of Canetti et al., ours has smaller secret key of one identity and more efficient homomorphic operations. Thus we obtain a more efficient CCA1 secure FHE scheme.

Keywords: Fully homomorphic encryption, CCA1, Probabilistic indistinguishability obfuscation

Introduction

Fully homomorphic encryption (FHE) is one of the holy grails of modern cryptography. For short, a FHE scheme is an encryption scheme that allows anyone to perform arbitrary computations on encrypted data using only public information. With this fascinating feature, FHE has many theoretical and practical applications, a typical one of which is outsourcing computation to untrusted entities without compromising one's privacy. The basic security property considered for FHE is security against chosen plaintext attacks (CPA), where it is required that an adversary that has access to the public parameters cannot distinguish between ciphertexts that encrypt two plaintexts chosen by the adversary.

The notion of FHE is introduced by Rivest, Adleman and Dertouzos (Rivest et al. 1978) in 1978. But the first candidate scheme, Gentry's groundbreaking work in 2009 (Gentry 2009a; b), came 30 years later. While Gentry's work is a major breakthrough, it is far from efficient in the practical point of view. Since 2009, a lot of designs (van Dijk et al. 2010; Smart and Vercauteren 2010; Brakerski and Vaikuntanathan 2011a, b; Smart and Vercauteren 2014; Brakerski et al. 2012; Brakerski 2012; Gentry et al. 2012a, b, 2013) have been proposed towards more efficient FHE. All the above FHE schemes are only proven to be CPA secure.

The security against chosen ciphertext attacks, also called CCA security (Naor and Yung 1990) which requires that ciphertexts indistinguishability holds even when the adversary can make decryption queries. CCA security contains two kinds: the first one is CCA1, where the adversary is limited to make decryption queries before she receives the challenge ciphertext; the second one is CCA2, where the adversary can make decryption queries even after she receives the challenge ciphertext. CCA2 security prevents any meaningful change of a given ciphertext, and so appears to be in direct contradiction with homomorphism, but CCA1 is not. For example, the Cramer-Shoup-lite (Cramer and Shoup 1998) scheme is both CCA1-secure and additively homomorphic. However, several works (Loftus et al. 2010; Zhang et al. 2012; Dahab et al. 2015) show CCA1 attacks against some existing FHE schemes.

Related work

In PKC 2016, Lai et al. (2016) first introduced a new primitive called convertible identity-based fully homomorphic encryption (IBFHE), which is an IBFHE with an additional transformation functionality. Based on this new primitive, IND-sID-CPA-secure convertible IBFHE,

*Correspondence: wangbiao@iie.ac.cn
[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

© The Author(s). 2018 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

and strongly EUF-CMA-secure signature, they proposed a generic paradigm of constructing CCA-secure keyed-FHE (a CCA-secure keyed-FHE scheme should provide CCA security when the evaluation key is unavailable to the adversary and remain CPA-secure when the evaluation key is exposed) by modifying CHK transformation (Canetti et al. 2004) slightly. Finally, they proposed a concrete construction of IND-sID-CPA-secure convertible IBFHE from adaptively-secure IBE scheme (Agrawal et al. 2010), indistinguishability obfuscation (IO) (Sahai and Waters 2014), and Puncturable PRF (Sahai and Waters 2014).

In PKC 2017, Canetti et al. (2017) extended the generic transformation of Boneh, Canetti, Halevi and Katz (Boneh et al. 2007) to turn any multi-key IBFHE scheme into a CCA1-secure FHE scheme. They gave three instantiations of multi-key IBFHE: The first one is a generic construction from multi-key FHE and IBE due to Brakerski et al. (2016); The second one is from LWE in the random oracle model, and the third one is from sub-exponentially secure IO (which is used to construct PIO). The first two constructions are compact with respect to the function evaluated homomorphically but not compact with respect to the number of ciphertext involved in the homomorphic evaluation. The third construction from PIO is fully compact and unleveled, which is their main construction. Finally, they adopted the approach of Naor and Yung (1990) who showed that how to go from CPA encryption to CCA1 encryption using non-interactive zero-knowledge proofs to the FHE setting. They gave a compact CCA1 secure FHE scheme from any CPA secure FHE scheme and a zero-knowledge succinct non-interactive argument of knowledge.

Our results and techniques

We focus on construction of CCA1 secure FHE schemes. Our starting point is the work of Canetti et al. (2017) who showed that CCA1-secure FHE scheme can be constructed from any multi-key IBFHE scheme. Our contributions are as follows:

1. We analyse the multi-key IBFHE scheme from PIO that proposed by Canetti et al. (2017) and show that their scheme is not secure by giving an attack. We give a solution to avoid the above attack and point out a mistake in their security proof.
2. We redesign a more succinct and efficient multi-key IBFHE scheme. Compared with the scheme of Canetti et al. (2017), ours has smaller secret key of one identity and more efficient homomorphic operations. The concrete comparison is showed in Table 1.

Our multi-key IBFHE scheme is constructed from trapdoor encryption scheme, PIO, and puncturable PRF. Our first observation is that IND-sID-CPA secure IBFHE scheme can be obtained from FHE scheme, IO, and puncturable PRF (Clear and McGoldrick 2014) using the technique of "punctured programming" (Sahai and Waters 2014). Concretely, we use the puncturable PRF for the derivation of a user's public key from her identity. Our second observation is that FHE scheme can be obtained from trapdoor encryption scheme and PIO (Canetti et al. 2015). Combining these two techniques, we can obtain an IND-sID-CPA secure IBFHE scheme. For the construction of CCA1-secure FHE schemes, we need a multi-key IBFHE scheme which is selective security for random identities. Toward this aim, we should be able to compute on IBE ciphertexts that all use the same master public key, but different identities. To keep the compactness of our scheme, we require that the identity corresponding to a resulting ciphertext that after some computation has the same length as a fresh identity. The method in (Canetti et al. 2017) is to set the resulting identity to be XOR of the identities that involved in the computation. However, we show that this method can be used to break the security of their scheme. We use the idea of randomization to avoid the above problem.

Preliminaries

Let λ denote a security parameter. When we speak of a negligible function negl(λ), we mean a function that is asymptotically bounded from above by the reciprocal of all polynomials in λ.

CCA1-Secure fully homomorphic encryption

Definition 1 (Canetti et al. 2017) *Let $\mathcal{M}$ be a message space. A CCA1-secure FHE scheme is a tuple of polynomial time algorithms* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$, *defined as follows, which satisfy the correctness, compactness and security properties below.*

- $\mathsf{Gen}(1^\lambda)$*: a randomized algorithm which outputs a public key, secret key pair* (pk, sk).
- $\mathsf{Enc}(pk, m)$*: a randomized algorithm which outputs a ciphertext* ct.
- $\mathsf{Dec}(sk, ct)$*: an algorithm which outputs a message* $m \in \mathcal{M}$.
- $\mathsf{Eval}(\{ct_i\}, C)$*: an algorithm which takes a collection of ciphertexts* $\{ct_i\}$ *and a circuit* C *to be evaluated and outputs an evaluated ciphertext* ct_{eval}.

Correctness: *For any* $m \in \mathcal{M}$, $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$,

$$\Pr[\,\mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) = m] = 1 - negl$$

Homomorphic Correctness: *For any* $\{m_i\} \in \mathcal{M}^{poly(\lambda)}$, *circuit* C *of polynomial size, and* $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$, $ct_i \leftarrow \mathsf{Enc}(pk, m_i)$

$$\Pr[\,\mathsf{Dec}(sk, \mathsf{Eval}(\{ct_i\}, C)) = C(\{m_i\})] = 1 - negl$$

Table 1 The comparison between Canetti et al's scheme and our scheme

Scheme	Secret key	Number of computation for addition	Number of computation for multiplication
Canetti et al's Scheme	An obfuscation of some decryption circuit	t	$t^2 + t$
Our Scheme	The secret key of a trapdoor encryption scheme	1	1

[1] Here t is the number of inputs for a circuit, which consists of addition gates and multiplication gates

Compactness: *There exists a polynomial* $poly(\cdot)$ *such that* $|ct_{eval}| \le poly(\lambda)$ *for all* $ct_{eval} \leftarrow \mathsf{Eval}(\{ct_i\}, C)$*. In particular,* $poly(\cdot)$ *is independent of the size, depth or number of inputs to C.*

CCA1 Security: *For any PPT adversary* $\mathcal{A}$*, its chance of winning the following game against a challenger* $\mathcal{C}$ *is at most* $1/2 + negl$*.*

1. $\mathcal{C}$ *draws* $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ *and sends pk to* $\mathcal{A}$*.*
2. *For* $\alpha = 1, ..., poly$*:* $\mathcal{A}$ *sends* ct_α *to* $\mathcal{C}$*;* $\mathcal{C}$ *computes* $m_\alpha = \mathsf{Dec}(sk, ct_\alpha)$ *and returns* m_α *to* $\mathcal{A}$*.*
3. $\mathcal{A}$ *sends* $m_0, m_1 \in \mathcal{M}$ *to* $\mathcal{C}$*.*
4. $\mathcal{C}$ *draws* $ct^* \leftarrow \mathsf{Enc}(pk, m_b)$ *for* $b \leftarrow \{0, 1\}$ *and sends* ct^* *to* $\mathcal{A}$*.*
5. $\mathcal{A}$ *outputs a guess bit* b' *and wins if* $b' = b$*.*

Remark 1 *We say that a FHE scheme is leveled if it permits evaluation of circuits of a-priori bounded polynomial depth on encrypted data. In contrast, a FHE scheme is pure (or unleveled) if it permits evaluation of circuits of any depth.*

Multi-key IBFHE

Definition 2 (Canetti et al. 2017) *Let* $\mathcal{M}, \mathcal{ID}$ *be message and identity spaces. A multi-key identity-based fully homomorphic encryption scheme is a tuple of polynomial time algorithms* (Setup, KeyGen, Enc, Dec, Eval)*, defined as follows, which satisfy the correctness and security properties below.*

- $\mathsf{Setup}(1^\lambda)$*: output the master key pair* (mpk, msk)*.*
- $\mathsf{KeyGen}(msk, id)$*: output a secret key* sk_{id} *for the identity id.*
- $\mathsf{Enc}(mpk, id, m)$*: encrypt message m under identity id, and outputs* (id, ct_{id})*.*
- $\mathsf{Dec}(sk_{id}, id, ct_{id})$*: decrypt* ct_{id} *using* sk_{id} *and outputs m.*
- $\mathsf{Eval}(\{(id_i, ct_i)\}, C)$*: take a family of ciphertexts and a circuit and outputs* (id_{eval}, ct_{eval})*.*

Correctness: *For any* $m \in \mathcal{M}, id \in \mathcal{ID}$*, and* $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda)$*,* $sk_{id} \leftarrow \mathsf{KeyGen}(msk, id)$

$$\Pr[\,\mathsf{Dec}(sk_{id}, \mathsf{Enc}(mpk, id, m)) = m] = 1 - negl$$

Homomorphic Correctness: *For any* $\{m_i\} \in \mathcal{M}^{poly(\lambda)}$*,* $\{id_i\} \in \mathcal{ID}^{poly(\lambda)}$*, circuit C of polynomial size, and* $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda)$*,* $sk_i \leftarrow \mathsf{KeyGen}(msk, id_i)$*,* $ct_i \leftarrow \mathsf{Enc}(mpk, id_i, m_i)$

$$\Pr[\,\mathsf{Dec}(sk_{eval}, \mathsf{Eval}(\{(id_i, ct_i)\}, C)) = C(\{m_i\})] = 1 - negl$$

where $sk_{eval} \leftarrow \mathsf{KeyGen}(msk, id_{eval})$*.*

Compactness: *There exists a polynomial* $poly(\cdot)$ *such that* $|id_{eval}|, |ct_{eval}| \le poly(\lambda)$ *for all* $id_{eval}, ct_{eval} \leftarrow \mathsf{Eval}(\{(id_i, ct_i)\}, C)$*. In particular,* $poly(\cdot)$ *is independent of the size, depth or number of inputs to C.*

Selective Security for Random Identities: *For any PPT adversary* $\mathcal{A}$*, its chance of winning the following game against a challenger* $\mathcal{C}$ *is at most* $1/2 + negl$*.*

1. $\mathcal{C}$ *draws* $id^* \leftarrow \mathcal{ID}$ *and* $(mpk, msk) \leftarrow \mathsf{Setup}\left(1^\lambda\right)$*, sends mpk to* $\mathcal{A}$*.*
2. $\mathcal{A}$ *makes queries to an oracle* $\mathcal{O}$ *defined by* $\mathcal{O}(id) = \begin{cases} \mathsf{KeyGen}(msk, id), & \text{if } id \neq id^*; \\ \bot, & \text{otherwise.} \end{cases}$
3. $\mathcal{A}$ *chooses two messages* $m_0, m_1 \in \mathcal{M}$ *and sends them to the challenger* $\mathcal{C}$*.*
4. $\mathcal{C}$ *uniformly samples a bit* $b \leftarrow \{0, 1\}$*, and returns* $ct^* \leftarrow \mathsf{Enc}(mpk, id^*, m_b)$*.*
5. $\mathcal{A}$ *outputs a guess bit* b' *and wins if* $b' = b$*.*

CCA1 FHE from multi-key IBFHE

Let E be a multi-key IBFHE scheme. Then the construction of CCA1 secure FHE is as follows (Canetti et al. 2017).

- $\mathsf{Gen}\left(1^\lambda\right)$: Output $(pk, sk) = (mpk, msk) \leftarrow$ E.Setup $\left(1^\lambda\right)$.
- $\mathsf{Enc}(pk, m)$: Draw $id \leftarrow \mathcal{ID}$ and compute $ct_{id} \leftarrow$ E.Enc(mpk, id, m). Output $ct = (id, ct_{id})$.
- $\mathsf{Dec}(sk, ct)$: Parse $ct = (id, ct_{id})$. Compute $sk_{id} \leftarrow$ E.KenGen(msk, id), and output $m =$ E.Dec(sk_{id}, id, ct_{id}).
- $\mathsf{Eval}(\{ct_i\}, C)$: Parse $ct_i = (id_i, ct_{id_i})$. Output $ct_{eval} = (id_{eval}, \mathsf{E}.ct_{eval}) \leftarrow$ E.Eval$(\{(id_i, ct_{id_i})\}, C)$.

Lemma 1 *The above scheme is a CCA1-secure FHE scheme.*

The proof of this lemma can be found in (Canetti et al. 2017) and (Boneh et al. 2007).

Trapdoor encryption schemes

Definition 3 (Canetti et al. 2015) *An encryption scheme* $\prod = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{tKeyGen})$ *is a trapdoor encryption scheme, if* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is a CPA-secure encryption scheme and the trapdoor key generation algorithm* $\mathsf{tKeyGen}$ *satisfies the following additional properties:*

Trapdoor Public Keys: *The following two ensembles are indistinguishable*

$$\{(pk, sk) \leftarrow \mathsf{KeyGen}(1^{\lambda}) : pk\}_{\lambda} \approx \{tpk \leftarrow \mathsf{tKeyGen}(1^{\lambda}) : tpk\}_{\lambda}$$

Computational Hiding: *The following two ensembles are indistinguishable*

$$\{tpk \leftarrow \mathsf{tKeyGen}(1^{\lambda}) : \mathsf{Enc}(tpk, m_0)\}_{\lambda} \approx \{tpk \leftarrow \mathsf{tKeyGen}(1^{\lambda}) : \mathsf{Enc}(tpk, m_1)\}_{\lambda}$$

where m_0, m_1 *are two distinct messages.*

The basic trapdoor encryption scheme does not provide any advantage in the trapdoor mode than the honest mode. Obviously, any CPA secure encryption scheme implies a trapdoor encryption scheme. The following are two stronger variants.

μ-Hiding Trapdoor Encryption Scheme The distinguishing advantage of the two ensembles in the computational hiding property of the above definition is replaced by some $\mu(\lambda)$. Typically, $\mu(\lambda)$ is much smaller than the inverse exponentiation of the ciphertext length. Canetti et al. (2015) showed that μ-hiding trapdoor encryption scheme can be constructed from any μ-rerandomizable CPA encryption scheme.

Statistical Trapdoor Encryption Scheme The computational hiding property in the above definition is replaced by statistical hiding. Note that any lossy encryption scheme implies a statistical trapdoor encryption scheme.

Probabilistic indistinguishability obfuscation (PIO)

Probabilistic Indistinguishability Obfuscation (PIO) A notion that was recently introduced by Canetti et al. (2015). Roughly speaking, this is an obfuscator for probabilistic circuits with the guarantee that the obfuscations of any two "equivalent" circuits are computationally indistinguishable. Before formally defining PIO, we introduce some relevant notions. Let $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbb{N}}$ be a family of sets of (randomized) circuits, where $\mathcal{C}_\lambda$ contains circuits of size $\text{poly}(\lambda)$. A circuit sampler for $\mathcal{C}$ is a distribution ensemble $D = \{D_\lambda\}_{\lambda \in \mathbb{N}}$ where the distribution D_λ ranges over triples (C_0, C_1, z) with $C_0, C_1 \in \mathcal{C}_\lambda$ such that C_0, C_1 take inputs of the same length, and $z \in \{0,1\}^{\text{poly}(\lambda)}$. Moreover, a class $\mathbf{S}$ of samplers for $\mathcal{C}$ is a set of circuit samplers for $\mathcal{C}$.

Definition 4 (Canetti et al. 2015) *A uniform PPT machine* $pi\mathcal{O}$ *is an indistinguishability obfuscator for a class of samplers* $\boldsymbol{S}$ *over the (potentially randomized) circuit family* $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbb{N}}$ *if the following two conditions hold:*

Correctness: $pi\mathcal{O}$ *on input a (potentially probabilistic) circuit* $C \in \mathcal{C}_\lambda$ *and the security parameter* $\lambda \in \mathbb{N}$ *(in unary), outputs a deterministic circuit* Λ *of size* $poly(|C|, \lambda)$. *Furthermore, for every non-uniform PPT distinguisher* $\mathcal{D}$, *every (potentially probabilistic) circuit* $C \in \mathcal{C}_\lambda$, *and string* z, *we define the following two experiments:*

- $Exp^1_{\mathcal{D}}(1^\lambda, C, z)$: *$\mathcal{D}$ on input $1^\lambda, C, z$, participates in an unbounded number of iterations of his choice. In iteration i, it chooses an input x_i; if x_i is the same as any of the previously chosen input x_j for $j < i$, then abort; otherwise, $\mathcal{D}$ receives $C(x_i; r_i)$ using fresh random coins r_i (r_i = null if C is deterministic). At the end of all iterations, $\mathcal{D}$ outputs a bit b. (Note that $\mathcal{D}$ can keep state across iterations.)*
- $Exp^2_{\mathcal{D}}(1^\lambda, C, z)$: *Obfuscate circuit C to obtain $\Lambda \leftarrow pi\mathcal{O}(1^\lambda, C; r)$ using fresh random coins r. Run $\mathcal{D}$ as described above, except that in each iteration, feed $\mathcal{D}$ with $\Lambda(x_i)$ instead.*

Overload the notation $Exp^i_{\mathcal{D}}(1^\lambda, C, z)$ *as the output of* $\mathcal{D}$ *in experiment* $Exp^i_{\mathcal{D}}$. *We require that for every non-uniform PPT distinguisher* $\mathcal{D}$, *there is a negligible function* μ, *such that, for every* $\lambda \in \mathbb{N}$, *every* $C \in \mathcal{C}_\lambda$, *and every auxiliary input* $z \in \{0,1\}^{poly(\lambda)}$,

$$Adv_{\mathcal{D}}(1^\lambda, C, z) = |\Pr[Exp^1_{\mathcal{D}}(1^\lambda, C, z)] - \Pr[Exp^2_{\mathcal{D}}(1^\lambda, C, z)]| = \mu(\lambda)$$

Security with Respect to S: *For every sampler* $D = \{D_\lambda\}_{\lambda \in \mathbb{N}} \in \boldsymbol{S}$, *and for every non-uniform PPT machine* $\mathcal{A}$, *there exists a negligible function* μ *such that*

$$|\Pr[(C_1, C_2, z) \leftarrow D_\lambda : \mathcal{A}(C_1, C_2, pi\mathcal{O}(1^\lambda, C_1), z) = 1] - \Pr[(C_1, C_2, z) \leftarrow D_\lambda : \mathcal{A}(C_1, C_2, pi\mathcal{O}(1^\lambda, C_2), z) = 1]| = \mu(\lambda)$$

Puncturable Pseudorandom functions

In our construction, we will use the puncturable PRFs, which are PRFs that can be defined on all bit strings of a certain length, except for some polynomial-size set of inputs. Below we recall their definition, as given by Sahai and Waters (2014):

Definition 5 *A puncturable family of PRFs F is given by a triple of Turing machines* $\mathsf{Key}, \mathsf{Puncture}, \mathsf{Eval}$, *and a pair of computable functions* $n(\cdot)$ *and* $m(\cdot)$, *satisfying the following conditions:*

- ***(Functionality preserved under puncturing.)*** *For every PPT adversary $\mathcal{A}$ such that $\mathcal{A}(1^\lambda)$ outputs a set $S \subseteq \{0,1\}^{n(\lambda)}$, then for all $x \in \{0,1\}^{n(\lambda)}$ where $x \notin S$, we have that:*

$$\Pr\left[\mathsf{Eval}(K,x) = \mathsf{Eval}(K_S,x) : K \leftarrow \mathsf{Key}(1^\lambda), K_S = \mathsf{Puncture}(K,S)\right] = 1.$$

- ***(Pseudorandom at punctured points.)*** *For every PPT adversary $(\mathcal{A}_1, \mathcal{A}_2)$ such that $\mathcal{A}_1(1^\lambda)$ outputs a set $S \subseteq \{0,1\}^{n(\lambda)}$ and any $x \in S$, consider an experiment where $K \leftarrow \mathsf{Key}(1^\lambda)$ and $K_S = \mathsf{Puncture}(K,S)$. Then we have*

$$|\Pr[\mathcal{A}_2(K_S,x,\mathsf{Eval}(K,x)) = 1] - \Pr[\mathcal{A}_2(K_S,x,U_{m(\lambda)}) = 1]| \leq negl(\lambda),$$

where $U_{m(\lambda)}$ denotes the uniform distribution over $m(\lambda)$ bits.

Review of PIO based multi-key IBFHE proposed by Canetti et al. (2017)

In PKC 2017, Canetti et al. (2017) constructed a multi-key IBFHE scheme from statistical trapdoor encryption, PIO, and puncturable PRF. Their key ideas are borrowed from works of Canetti et al. (2015) and Dodis et al. (2016). Firstly, they constructed a tag-puncturable additively homomorphic encryption scheme. For homomorphic computations, they use the method in (Dodis et al. 2016). Concretely, assume C is an algebraic circuit with n input, they first split every ciphertext into n ciphertexts corresponding to n identities. For an addition gate, they carry out n homomorphic additions and obtain n ciphertexts. For a multiplication gate, they first execute n^2 homomorphic computations obtaining $2n^2$ ciphertexts and then execute n homomorphic computations obtaining n ciphertexts. Finally, at the output gate, they combine the resulting n ciphertexts to obtain the final ciphertext. The identity corresponding to the final ciphertext is XOR of n identities in the input, i.e. $\mathbf{id_{eval}} = \bigoplus \mathbf{id_i}$. There is a problem arising here. We give an attack in the following to show that this scheme is not secure.

Attack Our attack is as follows:

1. The adversary $\mathcal{A}$ queries a secret key of one identity sk_α for some identity id_α.
2. $\mathcal{A}$ receives the challenge ciphertext ct^* which encrypts m_b under identity id^*.
3. $\mathcal{A}$ computes a ciphertext ct_m of some message m under identity $id_\beta \triangleq id_\alpha \oplus id^*$.
4. $\mathcal{A}$ homomorphicly adds ct_m with ct^* and obtains a ciphertext ct^{**} which encrypts $m + m_b$ under identity $id_\beta \oplus id^* = id_\alpha$.
5. $\mathcal{A}$ decrypts ct^{**} using sk_α and obtains message $m + m_b$.
6. $\mathcal{A}$ obtains the challenge plaintext m_b by subtracting m from the above message.
7. $\mathcal{A}$ compares m_b with m_0, m_1 and obtains the value of b with probability 1.

To resist the above attack, we use the idea of randomization. In particular, for every gate of the circuit, we set the identity of the output ciphertext to be a random identity. In this case, after the adversary $\mathcal{A}$ performs some computation on the challenge ciphertext ct^*, the identity corresponding to the final ciphertext will be completely random, hence the probability that it is same as some identity id_α for which $\mathcal{A}$ has queried corresponding secret key of one identity sk_α is negligible.

We think there is a mistake in their security proof which exists in the last step of Proof of Claim 3. Concretely, we think the two games G_3 and G_4 are not indistinguishable, because when taking a ciphertext with tag $(id^*, i-1)$ as input, the two obfuscations in G_3 will output the encryptions of 0, but in G_4 they will output "abort".

Besides the above security flaw, their scheme also has the following two drawbacks:

1. The secret key of one identity is an obfuscation of some decryption circuit, which is very large;
2. For a circuit with n inputs consisting of addition gates and multiplication gates, the numbers of computation for each addition gate and multiplication gate in their scheme are n and $n^2 + n$ respectively, which are very inefficient.

In the following section, we propose our Multi-key IBFHE scheme, which eliminates the above drawbacks.

Our multi-key IBFHE from trapdoor encryption and PIO

- $\mathsf{Setup}(1^\lambda)$: Let E be a trapdoor encryption scheme. Assume the message space $\mathcal{M}$ and identity space $\mathcal{ID}$ of our multi-key IBFHE are a ring and $\{0,1\}^k$, respectively. Assume E has the same message space $\mathcal{M}$. Let $pi\mathcal{O}$ be a PIO scheme and $\mathcal{F}$ be a puncturable PRF.

  Sample a PRF key K. Let $P_{map}[K]$ be the following program:

  1. K is hardwired, take input $id \in \{0,1\}^k$;
  2. Compute $r_{id} = \mathcal{F}_K(id)$;
  3. Compute $(pk_{id}, sk_{id}) = \mathrm{E.Gen}(1^\lambda, r_{id})$;
  4. Output pk_{id}.

  Let $P_{add}[K]$ and $P_{mult}[K]$ be the following probabilistic programs:

  1. K is hardwired into both, both take inputs $(id_1, ct_1), (id_2, ct_2) \in \{0,1\}^k \times \mathsf{E}.\mathcal{CT}$;
  2. Compute $(pk_{id_i}, sk_{id_i}) = \mathrm{E.Gen}(1^\lambda, \mathcal{F}_K(id_i))$ for $i = 1, 2$;

3. Compute $m_i = \mathrm{E.Dec}(sk_{id_i}, ct_i)$ for $i = 1, 2$;
4. Sample $r \leftarrow \{0,1\}^k$ and set $id_{out} = r$, compute $(pk_{id_{out}}, sk_{id_{out}}) = \mathrm{E.Gen}(1^\lambda, \mathcal{F}_K(id_{out}))$
5. Now the programs differ:
   $\underline{P_{add}[K]}$: Draw $ct_{out} \leftarrow \mathrm{E.Enc}(pk_{id_{out}}, m_1 + m_2)$, output (id_{out}, ct_{out}).
   $\underline{P_{mult}[K]}$: Draw $ct_{out} \leftarrow \mathrm{E.Enc}(pk_{id_{out}}, m_1 \times m_2)$, output (id_{out}, ct_{out}).

Let $\mathcal{O}_{map}[K] \leftarrow pi\mathcal{O}(P_{map}[K])$, $\mathcal{O}_{add}[K] \leftarrow pi\mathcal{O}(P_{add}[K])$ and $\mathcal{O}_{mult}[K] \leftarrow pi\mathcal{O}(P_{mult}[K])$. Set $msk = K$ and $mpk = (\mathcal{O}_{map}[K], \mathcal{O}_{add}[K], \mathcal{O}_{mult}[K])$.

- $\mathsf{KeyGen}(msk, id)$: Parse $msk = K$. Compute $(pk_{id}, sk_{id}) = \mathrm{E.Gen}(1^\lambda, \mathcal{F}_K(id))$ and output sk_{id}.
- $\mathsf{Enc}(mpk, id, m)$: Parse $mpk = (\mathcal{O}_{map}[K], \mathcal{O}_{add}[K], \mathcal{O}_{mult}[K])$, compute $pk_{id} = \mathcal{O}_{map}[K](id)$. Draw $ct_{id} \leftarrow \mathrm{E.Enc}(pk_{id}, m)$ and output (id, ct_{id}).
- $\mathsf{Dec}(sk_{id}, id, ct_{id})$: Output $m = \mathrm{E.Dec}(sk_{id}, ct_{id})$.
- $\mathsf{Eval}(mpk, (id_1, ct_1), ..., (id_t, ct_t), C)$: Parse $mpk = (\mathcal{O}_{map}[K], \mathcal{O}_{add}[K], \mathcal{O}_{mult}[K])$, view C as an algebraic circuit consisting of addition gates g_+ and multiplication gates $g_\times$ over the message space $\mathcal{M}$. We process the circuit gate by gate, let u, v be encryption of the input values of some gate. For an addition gate g_+, evaluate g_+ homomorhpically by computing $w = \mathcal{O}_{add}[K](u, v)$; For a multiplication gate $g_\times$, evaluate $g_\times$ homomorhpically by computing $w = \mathcal{O}_{mult}[K](u, v)$.

Lemma 2 *If* E *is a trapdoor encryption scheme, $pi\mathcal{O}$ is a PIO scheme and $\mathcal{F}$ is a puncturable PRF, then the above scheme is a multi-key IBFHE scheme which is fully compact and unleveled.*

Proof Correctness and homomorphic correctness follow immediately from correctness of E and $pi\mathcal{O}$.

For security, we show that for any PPT adversary $\mathcal{A}$, its chance of winning the multi-key IBFHE selective security game for random identities is at most $1/2 + \mathrm{negl}$. We use a hybrid argument.

Game 0: This is the original multi-key IBFHE selective security game for random identities.

1. $\mathcal{C}$ draws $id^* \leftarrow \{0,1\}^k$ and $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda)$, sends mpk to $\mathcal{A}$.
2. $\mathcal{A}$ makes queries to an oracle $\mathcal{O}$ defined by $\mathcal{O}(id) = \begin{cases} \mathsf{KeyGen}(msk, id), & \text{if } id \neq id^*; \\ \perp, & \text{otherwise.} \end{cases}$
3. $\mathcal{A}$ chooses two messages $m_0, m_1 \in \mathcal{M}$ and sends them to the challenger $\mathcal{C}$.
4. $\mathcal{C}$ uniformly samples a bit $b \leftarrow \{0,1\}$, and returns $ct^* \leftarrow \mathsf{Enc}(mpk, id^*, m_b)$.
5. $\mathcal{A}$ outputs a guess bit b' and wins if $b' = b$.

Game 1: This is the same as Game 0 except for the following changes. $\mathcal{C}$ computes $K^* \leftarrow \mathsf{PRF.Puncture}(K, id^*)$ and answer secret key queries using K^* instead of K.

The adversary cannot detect any difference between Game 0 and Game 1, since for all $id \neq id^*$ it holds that $\mathcal{F}_K(id) = \mathcal{F}_{K^*}(id)$.

Game 2: This is the same as Game 1 except that we make the following changes to $P_{add}[K]$ and $P_{mult}[K]$:

1. Replace K with K^*. id^* and $\mathcal{F}_K(id^*)$ is also hardwired.
2. In step 2, if $id_i = id^*$, then use $\mathcal{F}_K(id^*)$ instead of $\mathcal{F}_{K^*}(id_i)$; In step 4, if $id_{out} = id^*$, then use $\mathcal{F}_K(id^*)$ instead of $\mathcal{F}_{K^*}(id_{out})$.

Note that the modified programs is functionally equivalent to $P_{add}[K]$ and $P_{mult}[K]$, and due to the security of PIO, their respective obfuscations are thus computationally indistinguishable. So Game 1 and Game 2 are computationally indistinguishable.

Game 3: This is the same as Game 2 except that we make the following changes to $P_{map}[K]$:

1. Replace K with K^*. id^* and $\mathcal{F}_K(id^*)$ is also hardwired.
2. In step 2, if $id = id^*$, then sample $r \leftarrow \{0,1\}^n$ where $n = |\mathcal{F}_K(id^*)|$, and set $r_{id} = r$.

By the security of the puncturable PRF, we have that the following two distributions are computationally indistinguishable.

$$\{(K^*, id^*, \mathcal{F}_K(id^*))\} \approx \{(K^*, id^*, r) : r \leftarrow \{0,1\}^n\}$$

Due to the security of PIO, it follows that Game 2 and Game 3 are computationally indistinguishable.

Game 4: This is the same as Game 3 except that we make futher changes to $P_{map}[K]$:

1. If $id = id^*$, then output $tpk \leftarrow \mathrm{E.tGen}(1^\lambda)$.

Due to the key-indistinguishability of trapdoor encryption scheme E, the output distributions of the program $P_{map}[K]$ in Game 3 and Game 4 are close, and hence, the security of PIO implies that the obfuscations of the programs are also indistinguishable (even given the punctured key). It follows that Game 3 and Game 4 are computationally indistinguishable.

In Game 4, due to the hiding property in the trapdoor mode of trapdoor encryption scheme E, the success advantage of adversary $\mathcal{A}$ in this Game is negligible. This completes our proof of security. □

In our multi-key IBFHE scheme, secret key of one identity is a normal secret key, which is much smaller than that of Canetti et al.'s scheme; the numbers of computation for each addition gate and multiplication gate are all 1 instead of n and $n^2 + n$ in Canetti et al.'s scheme.

Combining Lemma 2 with Lemma 1 we get the following result immediately.

Theorem 1 *If there exists PIO, a trapdoor encryption scheme, and a puncturable PRF, then there is a CCA1 secure FHE scheme which is fully compact and unleveled.*

Conclusion

In this work, we focus on construction of CCA1 secure FHE schemes. Our starting point is the work of Canetti et al. (2017) who showed that CCA1-secure FHE scheme can be constructed from any multi-key IBFHE scheme. We analysed the multi-key IBFHE scheme from PIO that proposed by Canetti et al. (2017) and showed that their scheme is not secure by giving an attack. We gave a solution to avoid the above attack and redesigned a more succinct and efficient multi-key identity-based FHE scheme. Thus we obtained a more efficient CCA1 secure FHE scheme.

Funding

This work was supported by National Natural Science Foundation of China [grant number 61472414,61772514,61602061], and National Key R&D Program of China (2017YFB1400700).

Authors' contributions

The first author conceived the idea of the study and wrote the paper. All authors discussed the results and revised the manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 20 April 2018 Accepted: 7 September 2018
Published online: 25 September 2018

References

Agrawal S, Boneh D, Boyen X (2010) Efficient lattice (H)IBE in the standard model. In: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera. Springer, Berlin, Heidelberg. pp 553–572. May 30 - June 3, 2010. Proceedings. https://doi.org/10.1007/978-3-642-13190-5_28

Boneh D, Canetti R, Halevi S, Katz J (2007) Chosen-ciphertext security from identity-based encryption. SIAM J Comput 36(5):1301–1328. https://doi.org/10.1137/S009753970544713X

Brakerski Z, Vaikuntanathan V (2011a) Efficient fully homomorphic encryption from (standard) LWE. In: IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011. IEEE Computer Society, Washington. pp 97–106. October 22-25, 2011. https://doi.org/10.1109/FOCS.2011.12

Brakerski Z, Vaikuntanathan V (2011b) Fully homomorphic encryption from ring-lwe and security for key dependent messages. In: Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference,. Springer, Heidelberg. pp 505–524. August 14-18, 2011. Proceedings. https://doi.org/10.1007/978-3-642-22792-9_29

Brakerski Z, Gentry C, Vaikuntanathan V (2012) (leveled) fully homomorphic encryption without bootstrapping. In: Innovations in Theoretical Computer Science - ITCS 2012. ACM, New York. pp 309–325. January 8-10, 2012. http://doi.acm.org/10.1145/2090236.2090262

Brakerski Z (2012) Fully homomorphic encryption without modulus switching from classical gapsvp. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference. Springer, Heidelberg. pp 868–886. August 19-23, 2012. Proceedings. https://doi.org/10.1007/978-3-642-32009-5_50

Brakerski Z, Cash D, Tsabary R, Wee H (2016) Targeted homomorphic attribute-based encryption. In: Theory of Cryptography - 14th International Conference, TCC 2016-B. Springer, Berlin, Heidelberg, Beijing. pp 330–360. October 31 - November 3, 2016, Proceedings, Part II. https://doi.org/10.1007/978-3-662-53644-5_13

Canetti R, Halevi S, Katz J (2004) Chosen-ciphertext security from identity-based encryption. In: Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg. pp 207–222. May 2-6, 2004, Proceedings. https://doi.org/10.1007/978-3-540-24676-3_13

Cramer R, Shoup V (1998) A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference. Springer, Berlin, Heidelberg. pp 13–25. August 23-27, 1998, Proceedings. https://doi.org/10.1007/BFb0055717

Clear M, McGoldrick C (2014) Bootstrappable identity-based fully homomorphic encryption. In: Cryptology and Network Security - 13th International Conference, CANS 2014. Springer, Cham. pp 1–19. October 22-24, 2014. Proceedings. https://doi.org/10.1007/978-3-319-12280-9_1

Canetti R, Lin H, Tessaro S, Vaikuntanathan V (2015) Obfuscation of probabilistic circuits and applications. In: Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015. Springer, Berlin, Heidelberg, Warsaw. pp 468–497. March 23-25, 2015, Proceedings, Part II. https://doi.org/10.1007/978-3-662-46497-7_19

Canetti R, Raghuraman S, Richelson S, Vaikuntanathan V (2017) Chosen-ciphertext secure fully homomorphic encryption. In: Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography. Springer, Berlin, Heidelberg. pp 213–240. March 28-31, 2017, Proceedings, Part II. http://dx.doi.org/10.1007/978-3-662-54388-7_8

Dahab R, Galbraith SD, Morais E (2015) Adaptive key recovery attacks on ntru-based somewhat homomorphic encryption schemes. In: Information Theoretic Security - 8th International Conference, ICITS 2015. Springer, Cham. pp 283–296. May 2-5, 2015. Proceedings. https://doi.org/10.1007/978-3-319-17470-9_17

Dodis Y, Halevi S, Rothblum RD, Wichs D (2016) Spooky encryption and its applications. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference. Springer, Berlin, Heidelberg. pp 93–122. August 14-18, 2016, Proceedings, Part III. https://doi.org/10.1007/978-3-662-53015-3_4

Gentry C (2009a) A fully homomorphic encryption scheme. PhD thesis, Stanford, CA, USA. http://crypto.stanford.edu/craig

Gentry C (2009b) Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. ACM, New York. pp 169–178. May 31 - June 2 2009. https://doi.acm.org/10.1145/1536414.1536440

Gentry C, Halevi S, Smart NP (2012a) Better bootstrapping in fully homomorphic encryption. In: Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography Darmstadt. Springer, Berlin, Heidelberg. pp 1–16. May 21-23, 2012. Proceedings. https://doi.org/10.1007/978-3-642-30057-8_1

Gentry C, Halevi S, Smart NP (2012b) Fully homomorphic encryption with polylog overhead. In: Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg. pp 465–482. April 15-19, 2012. Proceedings. https://doi.org/10.1007/978-3-642-29011-4_28

Gentry C, Sahai A, Waters B (2013) Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference. Springer, Berlin, Heidelberg. pp 75–92. August 18-22, 2013. Proceedings, Part I. https://doi.org/10.1007/978-3-642-40041-4_5

Loftus J, May A, Smart NP, Vercauteren F (2010) On cca-secure fully homomorphic encryption. IACR Cryptol ePrint Arch 2010:560

Lai J, Deng RH, Ma C, Sakurai K, Weng J (2016) CCA-secure keyed-fully homomorphic encryption. In: Public-Key Cryptography - PKC 2016 - 19th, IACR International Conference on Practice and Theory in Public-Key

Cryptography. Springer, Berlin, Heidelberg. pp 70–98. March 6-9, 2016, Proceedings, Part I. http://dx.doi.org/10.1007/978-3-662-49384-7_4

Naor M, Yung M (1990) Public-key cryptosystems provably secure against chosen ciphertext attacks. In: Symposium on Theory of Computing, STOC 1990. ACM, New York. pp 427–437. May 13-17, 1990. http://doi.acm.org/10.1145/100216.100273

Rivest RL, Adleman L, Dertouzos ML (1978) On data banks and privacy homomorphisms. Found Secure Comput 4:169–179

Smart NP, Vercauteren F (2010) Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography. Springer, Berlin, Heidelberg. pp 420–443. May 26-28, 2010. Proceedings. https://doi.org/10.1007/978-3-642-13013-7_25

Smart NP, Vercauteren F (2014) Fully homomorphic SIMD operations. Des. Codes Crypt 71(1):57–81. https://doi.org/10.1007/s10623-012-9720-4. Springer US

Sahai A, Waters B (2014) How to use indistinguishability obfuscation: deniable encryption, and more. In: Symposium on Theory of Computing, STOC 2014, New York. pp 475–484. May 31 - June 03, 2014. http://doi.acm.org/10.1145/2591796.2591825. ACM, New York

van Dijk M, Gentry C, Halevi S, Vaikuntanathan V (2010) Fully homomorphic encryption over the integers. In: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg. pp 24–43. May 30 - June 3, 2010. Proceedings. https://doi.org/10.1007/978-3-642-13190-5_2

Zhang Z, Plantard T, Susilo W (2012) On the CCA-1 security of somewhat homomorphic encryption over the integers. In: Information Security Practice and Experience - 8th International Conference, ISPEC 2012. Springer, Berlin, Heidelberg. pp 353–368. April 9-12, 2012. Proceedings. https://doi.org/10.1007/978-3-642-29101-2_24

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com