Information Sciences 422 (2018) 177–187

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A new scale-invariant homomorphic encryption scheme

Jinsu Kim[a], Sungwook Kim[a], Jae Hong Seo[b,*]

[a] *Security Team, Software R&D Center, Samsung Electronics, Republic of Korea*
[b] *Department of Mathematics, Myongji University, Republic of Korea*

ARTICLE INFO

Article history:
Received 25 May 2016
Revised 20 June 2017
Accepted 3 September 2017
Available online 5 September 2017

Keywords:
Fully homomorphic encryption
Unknown message space
Scale-invariant
Integer-based

ABSTRACT

We propose a new fully homomorphic encryption over the integers. The proposed scheme is not only efficient in the sense that it enables scale-invariant multiplications, but it also has an interesting property, which is that all evaluations over encrypted messages can be performed with only partial information about the underlying message space. For example, it can be public that the message space $\mathcal{M}$ is a set of positive integers less than some integer g, but the exact value of g will be provably hidden from all public information under a reasonable assumption. We call this property, informally, *message space hidability*. Such message space hidability has an immediate and interesting application, namely, homomorphic commitment to large integers.

1. Introduction

A fully homomorphic encryption (FHE) scheme enables anyone who has the public key to compute either addition or multiplication over encrypted messages. Since Gentry's first realization of an FHE scheme using ideal lattices [1], there have been improvements in terms of efficiency and diversity in the underlying assumptions. There are several different frameworks used for the FHE design, which are categorized according to the underlying hard problems such as learning with errors (LWE) [2], Ring-LWE [3], and approximate common divisors (ACD) [4]. In this paper, we focus mainly on integer-based constructions. As for the other categories of FHE schemes, we give a brief survey in Section 1.1.

The first integer-based FHE scheme under the approximate common divisor assumption was proposed by van Dijk, Gentry, Halevi, and Vaikuntanathan (DGHV) [5]. There have been several subsequent works that have improved the efficiency of the DGHV-FHE scheme [6,7,8,9,10]. In this paper, we propose a new fully homomorphic encryption over the integers. The proposed scheme is efficient not only in the sense that it enables scale-invariant multiplications, but it also has an interesting property, which is that all evaluations over encrypted messages can be performed with only partial information about the underlying message space. For example, it can be public that the message space $\mathcal{M}$ is a set of positive integers less than some integer g, but the exact value of g will be provably hidden from all public information under a reasonable assumption. We call this property, informally, *message space hidability*.

We begin by pointing out that any existing integer-based scale-invariant fully homomorphic scheme should include a description of the message space. More precisely, the message space is $\mathbb{Z}_g$ for some integer g, and in all previous integer-based homomorphic schemes it has been necessary to know at least the integer g in order to perform an encryption algorithm or evaluation algorithm.

[*] Corresponding author.
E-mail addresses: jinsu86.kim@samsung.com (J. Kim), sw14.kim@samsung.com (S. Kim), jaehongseo@mju.ac.kr, jhsbhs@gmail.com (J.H. Seo).

http://dx.doi.org/10.1016/j.ins.2017.09.012
0020-0255/© 2017 Elsevier Inc. All rights reserved.

Table 1
Comparison of integer-based HE schemes.

	Schemes	CT	PK	Message space
DGHV	DGHV10 [5]	$\tilde{O}(\lambda^5)$	$\tilde{O}(\lambda^{10})$	unknown
	CNT12a [7]	$\tilde{O}(\lambda^5)$	$\tilde{O}(\lambda^5)$	unknown
	CNT12b [7]	$\tilde{O}(L^2\lambda^3)$	$\tilde{O}(L^3\lambda^4)$	known
	batch [8]	$\tilde{O}(\lambda^5)$	$\tilde{O}(n\lambda^7)$	unknown
Scale-inv.	CLT14a [9]	$\tilde{O}(L^2\lambda^3)$	$\tilde{O}(L^3\lambda^4)$	known
	CLT14b [9]	$\tilde{O}(L^2\lambda^3)$	$\tilde{O}(nL^3\lambda^4)$	known
	CS15 [10]	$\tilde{O}(L^2\lambda^3)$	$\tilde{O}(L^5\lambda^7)$	unknown
Ours	non-batch	$\tilde{O}(L^2\lambda^3)$	$\tilde{O}(L^3\lambda^4)$	unknown
	batch	$\tilde{O}(L^2\lambda^3)$	$\tilde{O}(nL^3\lambda^4)$	unknown

λ: security parameter, n: number of slots in batch, L: multiplicative depth,
CNT12a: Compressed pk scheme in [7], CNT12b: Modulus-switching scheme in [7],
CLT14a: Non-batch version scheme in [9], CLT14b: Batch version scheme in [9],
CS15: Scheme in [10] with exponentially large message space. Note that scheme with small message space in [10] achieves quasi-linear complexities, but it cannot achieve message space hidability.

Fortunately, we find that the recent scale-invariant fully homomorphic encryption (SIFHE) scheme of Cheon and Stehlé [10] can be modified to have message space hidability. However, the methodology used in the Cheon–Stehlé (CS) SIFHE scheme inherently requires a large public key, in particular a large multiplication key. Roughly speaking, the heart of the idea in CS-SIFHE is to minimize the empty space in *approximate common divisor (ACD)* instances, which is reserved for handling increases in errors. Therefore, to minimize the increase in errors for multiplication, multiplication in the CS-SIFHE scheme is carried out by bit operations and additions over ciphertexts. This multiplication procedure in the CS-SIFHE scheme consists of two steps: Given two ciphertexts, first, bitwise-decompose each ciphertext and compute their tensor product. Second, compute the inner product of the result and the multiplication key. Therefore, for a ciphertext consisting of γ bits, the size of the multiplication key depends on γ^2. Roughly speaking again, the size γ of the ciphertext is determined by the complexity of the lattice attack, that is, $\gamma = \omega((\eta-\rho)^2 \log\lambda)$, where $\eta - \rho$ is the size of the empty space reserved for the increase in errors in the ciphertext. For a small message space, it is sufficient to set $\eta - \rho = O(\log\lambda)$, with the result that the CS-SIFHE scheme achieves very short ciphertexts for a binary message space. However, for an exponentially large message space, $\eta - \rho$ should be larger than the bit size of the message space, that is, $\eta - \rho = O(\lambda)$, in which case there is no advantage over other integer-based schemes [7,9]. Therefore, for large message spaces, CS-SIFHE is not a state-of-the-art scheme. We compare size complexities and properties among integer-based (batch) homomorphic encryption [denoted (B)HE] schemes in Table 1. As for the computational cost, there are no notable differences between the integer-based schemes. In particular, all computation processes in key generation, encryption, decryption, and evaluation are very similar in the scale-invariant schemes. (The main difference among scale-invariant integer-based schemes is the form and distribution of encryptions in public keys.) In the table, we say message space $\mathbb{Z}_g$ is unknown if g is not required in public algorithm procedures, and is required only in the procedures for key generation and decryption. In the first row of the table, we consider the compressed form of ACD instances [7] in public keys except for the original DGHV.

We argue that the message space hidability property has an immediate and interesting application: homomorphic commitment to large integers. Note that message space hidability can be defined similarly for non-homomorphic encryption schemes or commitment schemes. It is well known that a fully homomorphic encryption scheme can be used as a homomorphic commitment scheme. This has interesting applications, e.g., short zero-knowledge arguments for circuit satisfiability. Furthermore, a commitment scheme with message space hidability (e.g., Fujisaki–Okamoto [11], Damgård [12]) is used for committing to integers of arbitrary length. Therefore, one can easily expect that homomorphic encryption with message space hidability can be used as a homomorphic commitment scheme for large integers. More precisely, the resulting (homomorphic) commitment scheme can be used for committing large integers since the message space hidability property prevents a user from finding two distinct messages having the same value modulo hidden integer g, where the message space is $\mathbb{Z}_g$. Then, zero-knowledge arguments for integer equations could be a direct application of a homomorphic commitment scheme for integers. We expect that there are many other applications of a message-space-hidable FHE scheme.

1.1. Related works

The first fully homomorphic encryption was proposed by Gentry and is based on ideal lattices [1]. The main breakthrough was to use a *bootstrapping* technique that evaluates the decryption circuit homomorphically to reduce the noise in a ciphertext. After Gentry's breakthrough, many FHEs were proposed to enhance the efficiency. Brakerski and Vaikuntanathan constructed an FHE in a simpler way, based on learning with errors (LWE) [13] and its ring variant [14]; they used the *re-linearization* technique to avoid using ideal lattices. Notably, Brakerski, Gentry, and Vaikuntanathan devised a new