Information Sciences 310 (2015) 149–162

Contents lists available at ScienceDirect

Information Sciences

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

CRT-based fully homomorphic encryption over the integers

Jung Hee Cheon [a,*], Jinsu Kim [a], Moon Sung Lee [a], Aaram Yun [b]

[a] Department of Mathematical Sciences, Seoul National University, Republic of Korea
[b] School of Electrical and Computer Engineering, Ulsan National Institute of Science and Technology, Republic of Korea

ARTICLE INFO

Article history:
Received 18 August 2014
Received in revised form 21 February 2015
Accepted 10 March 2015
Available online 18 March 2015

2010 MSC:
94A60
94A15
14G50

Keywords:
Privacy homomorphism
Chinese remainder theorem
Homomorphic encryption
Approximate gcd
DGHV

ABSTRACT

In 1978, Rivest, Adleman and Dertouzos introduced the basic concept of privacy homomorphism that allows computation on encrypted data without decryption. It was an interesting work whose idea precedes the recent development of fully homomorphic encryption, although actual example schemes proposed in the paper are all susceptible to simple known-plaintext attacks.

In this paper, we revisit one of their proposals, in particular the third scheme which is based on the Chinese Remainder Theorem and is ring homomorphic. It is known that only a single pair of known plaintext/ciphertext is needed to break this scheme. However, by exploiting the standard technique to insert an error to a message before encryption, we can cope with this problem. We present a secure modification of their proposal by showing that the proposed scheme is fully homomorphic and secure against the chosen plaintext attacks under the approximate GCD assumption and the sparse subset sum assumption when the message space is restricted to $\mathbb{Z}_2^k$.

Interestingly, the proposed scheme can be regarded as a generalization of the DGHV scheme with larger plaintext space. Our scheme has $\widetilde{O}(\lambda^5)$ ciphertext expansion overhead while the DGHV has $\widetilde{O}(\lambda^8)$ for the security parameter λ. When restricted to the homomorphic encryption scheme with depth of $O(\log\lambda)$, the overhead is reduced to $\widetilde{O}(\lambda)$. Our scheme can be used in applications requiring a large message space $\mathbb{Z}_Q$ for $\log Q = O(\lambda^4)$, or SIMD style operations on $\mathbb{Z}_Q^k$ for $\log Q = O(\lambda),\ k = O(\lambda^3)$, with $\widetilde{O}(\lambda^5)$ ciphertext size as in the DGHV.

1. Introduction

The concept of computation on encrypted data without decryption was firstly introduced in 1978 by Rivest, Adleman and Detourzos [24]. They defined a *privacy homomorphism* to be an encryption $\mathbf{Enc}: \mathcal{P} \to \mathcal{C}$ which permits computation of $\mathbf{Enc}(m_1 * m_2)$ from $\mathbf{Enc}(m_1),\ \mathbf{Enc}(m_2)$ for an algebraic operation $*$ on $\mathcal{P}$, without revealing m_1 and m_2. They presented five examples, but one of them was essentially RSA encryption supporting multiplication only, and the rest of them were insecure against known plaintext attack [3].

One of the examples given in [24] is as follows. Let $p,\ q$ be large primes and $n = pq$. The plaintext space is $\mathbb{Z}_n$ and the ciphertext space is $\mathbb{Z}_p \times \mathbb{Z}_q$. An encryption of a message $m \in \mathbb{Z}_n$ is $(m \bmod p, m \bmod q)$ and the decryption is done using the Chinese Remainder Theorem (CRT). This cryptosystem supports modular addition and multiplication. Unfortunately, it

* Corresponding author.
E-mail addresses: jhcheon@snu.ac.kr (J.H. Cheon), kjs2002@snu.ac.kr (J. Kim), moolee@snu.ac.kr (M.S. Lee), aaramyun@unist.ac.kr (A. Yun).

http://dx.doi.org/10.1016/j.ins.2015.03.019
0020-0255/

is shown that this scheme is insecure under the known plaintext attack [3]. In fact, we have $p|\gcd(m-c_1,n)$ and $q|\gcd(m-c_2,n)$ when $\mathbf{Enc}(m)=(c_1,c_2)$. Later, Domingo-Ferrer proposed two variants of this scheme using additional secret key elements, but they are also broken under known plaintext attacks [28,8].

In this paper, we revisit this particular scheme, and present a secure variant of it. To avoid known plaintext attacks to which previous variants were susceptible, we consider adding small random 'errors' to plaintexts, as in the recent fully homomorphic encryption schemes.

1.1. Basic idea

We denote by a mod p the unique integer in $(-\frac{p}{2},\frac{p}{2}]$ that is congruent to a modulo p, and by $\mathrm{CRT}_{(p_0,\ldots,p_k)}(m_0,\ldots,m_k)$ the unique integer in $\left(-\frac{\prod_i p_i}{2},\frac{\prod_i p_i}{2}\right]$ which is congruent to m_i modulo p_i for all i. Our basic symmetric encryption scheme is as follows:

- **KeyGen**$(\lambda,\{Q_i\})$: Given security parameter λ and relatively small pairwise coprime integers Q_i $(i=1,\ldots,k)$, choose large pairwise coprime integers p_i $(i=0,\ldots,k)$ and let $n=\prod_{i=0}^{k}p_i$. Output the secret key $sk=(p_0,\ldots,p_k)$ and the public parameter $pp=(n,Q_1,\ldots,Q_k)$. The message space is $\mathbb{Z}_Q$ for $Q=\prod_{i=1}^{k}Q_i$.
- **Enc**(sk,m): Output $c=\mathrm{CRT}_{(p_0,\ldots,p_k)}(e,m_1+e_1Q_1,\ldots,m_k+e_kQ_k)$ where $m_i=m \bmod Q_i$ for all i,e is a random integer in $(-p_0/2,p_0/2]$ and $e_1,\cdots,e_k$ are ρ-bit random integers.
- **Dec**(sk,c): Output
$$m=\mathrm{CRT}_{(Q_1,\ldots,Q_k)}(d_1,\ldots,d_k),$$
where $d_i=(c \bmod p_i)\bmod Q_i$ for all i.

Since the CRT is a ring isomorphism from $\prod_i\mathbb{Z}_{p_i}$ to $\mathbb{Z}_n$ with respect to modular addition and multiplication, **Dec** is also ring homomorphic. However, to ensure correct decryption of a ciphertext, the size of e_i and Q_i must be sufficiently smaller than that of p_i.

This scheme is a symmetric key encryption scheme which permits bounded number of modular additions and multiplications. We can convert this scheme to a somewhat homomorphic public key encryption scheme by publishing many encryptions of zero and encryptions of k elementary elements $E_i=\mathrm{CRT}_{(Q_1,\ldots,Q_i,\ldots,Q_k)}(0,\ldots,1,\ldots,0)$.

We reduce the security of our Somewhat Homomorphic Encryption (SWHE) scheme to a decisional version of Approximate GCD problem (DACD). Approximate GCD (ACD) problem is to find p given many multiples of p with some errors (i.e. $x_i=pq_i+e_i$). Note that the ACD assumption was used to prove the security of the DGHV scheme [13], and another decisional version of the approximate GCD assumption which is slightly different from ours was used to prove the security of a more efficient variant of DGHV by Coron et al. [12].

In fact, our scheme can be regarded as a generalization of the DGHV scheme, but with larger plaintext space. Moreover, our scheme can be extended to a Fully Homomorphic Encryption (FHE) through bootstrapping and squashing the decryption circuit as in [14,13], when $Q_1=\ldots=Q_k=2$ (see Section 5.1). In Section 5.2, we also show how we may do the bootstrapping when Q_i's are sufficiently large.

Let λ be the security parameter. The ciphertext size of our SWHE scheme is $\widetilde{O}(\lambda^5)$ as in the DGHV scheme. While the plaintext size of the DGHV is $O(\lambda)$, that of ours is $O(\lambda^4)$ for $O(\lambda)$-bit $Q_1,\ldots,Q_k$ with $k=O(\lambda^3)$. Consequently, our scheme reduces the overheads (ratio of ciphertext computation and plaintext computation) from $\widetilde{O}(\lambda^4)$ to $\widetilde{O}(\lambda)$. For the case that the message space is $\mathbb{Z}_2^k$, the overhead is reduced from $\widetilde{O}(\lambda^8)$ to $\widetilde{O}(\lambda^5)$ for $k=O(\lambda^3)$.

Our scheme has an advantage over [18] in applications requiring larger message space. When dealing with arithmetic on $\mathbb{Z}_Q$ for $\log Q=O(\lambda^4)$, our SWHE scheme can support $O(\lambda)$ multiplications with many additions. One of the important applications of homomorphic encryption schemes is to securely evaluate a multivariate polynomial over integers. Our scheme is an attractive choice for evaluating a polynomial of degree $O(\lambda)$ with inputs $\Omega(\lambda^2)$. Also our scheme can be used in the applications requiring SIMD style operations in k copies of $\mathbb{Z}_Q$ for $\log Q=\lambda,\ k=O(\lambda^3)$.

1.2. Related work

In 2009, Gentry [14,15] introduced the first fully homomorphic encryption scheme based on ideal lattices which supports arbitrarily many additions and multiplications on encrypted bits. His breakthrough paper drew an explosive interest and lead numerous researches in this area [13,11,12,17,27,25,26,18,2,1]. Gentry's scheme and its variants [14,15,27,25] are based on hard problems on ideal lattices. Another class of schemes [13,11,12] relies on the approximate GCD problem. The message space of these schemes is $\mathbb{Z}_2$, so the overhead is rather high due to the large ciphertext expansion ratio. Our scheme improves their efficiency. Recent schemes based on the learning with error (LWE) or the ring-LWE are more efficient and accomplish polylogarithmic overhead for wide enough arithmetic circuits on $\mathbb{Z}_p$ for $p=poly(\lambda)$. For more information on related work, we refer to [19].