An Additively Homomorphic Encryption over Large Message Space

Hu Chen, State Key Laboratory of Integrated Service Networks, Xidian University, Shanxi, Xi’an, China
Yupu Hu, State Key Laboratory of Integrated Service Networks, Xidian University, Shanxi, Xi’an, China
Zhizhu Lian, State Key Laboratory of Integrated Service Networks, Xidian University, Shanxi, Xi’an, China
Huiwen Jia, State Key Laboratory of Integrated Service Networks, Xidian University, Shanxi, Xi’an, China
Xu An Wang, State Key Laboratory of Integrated Service Networks, Xidian University, Shanxi, Xi’an, China

ABSTRACT

Fully homomorphic encryption schemes available are not efficient enough to be practical, and a number of real-world applications require only that a homomorphic encryption scheme is somewhat homomorphic, even additively homomorphic and has much larger message space for efficiency. An additively homomorphic encryption scheme based heavily on Smart-Vercauteren encryption scheme (SV10 scheme, PKC 2010) is put forward, where both schemes each work with two ideals I and J. As a contribution of independent interest, a two-element representation of the ideal I is given and proven by factoring prime numbers in a number field. This two-element representation serves as the public key. The authors’ scheme allows working over much larger message space than that of SV10 scheme by selecting the ideal I with larger decryption radius to generate public/private key pair; instead of choosing the ideal J as done in the SV10 scheme. The correctness and security of the scheme are shown, followed by setting parameters and computational results. The results indicate that this construction has much larger message space than SV10 scheme.

Keywords: Bounded Distance Decoding Problem, Fully Homomorphic Encryption, Lattice-Based Public Key Cryptosystem, Polynomial Coset Problem

DOI: 10.4018/IJITWE.2015070106
1. INTRODUCTION

Several exciting advances for lattice-based public key cryptosystem have been made, including predicate encryptions (Gorbunov, 2015a), the schemes of candidate multilinear maps (Garg, 2013a; Gentry, 2015; Coron, 2013a; Coron, 2015) and their applications (Garg, 2013b; Sahai, 2014), and homomorphic constructions (Gorbunov, 2015b; Gentry, 2009a). Particularly, homomorphic encryption (HE) is such an encryption where the output of the ring operations on the ciphertext space can be decrypted as the output of the corresponding ring operations on the plaintext space. It can be used for secure function evaluation, but the major application is homomorphic service, which is in such a scene. A user needs to obtain the output of the ring-operations on the plaintext space, and he wants to do nothing but decryption. The server implements homomorphic operations on the ciphertext space. That is, the server is given corresponding ciphertexts of input plaintexts, and computes the corresponding ciphertext of the output plaintext. Then the server sends this ciphertext to the user. The user then decrypts this ciphertext to obtain the original output plaintext. If an HE scheme can compute any function of the ciphertexts, then it is known as a Fully Homomorphic Encryption (FHE) scheme. Otherwise, it is referred to as a Somewhat Homomorphic Encryption (SHE) scheme. Recent years have witnessed several exciting advances for FHE, since the breakthrough work of Gentry (Gentry, 2009a; Gentry, 2009b). Smart and Vercauteren presented a novel FHE at PKC 2010 (Smart, 2010) (SV10 scheme for short), in which ciphertexts are integers rather than vectors. Another earliest scheme for FHE over the integers was presented by Dijk et al. (Dijk, 2010) at Eurocrypt 2010. The schemes above that follow Gentry’s blueprint have fairly poor performance. Without using the squashing step, the schemes in (Gentry, 2011a; Brakerski, 2011) begin to make the differences from Gentry’s blueprint for FHE. As shown in (Brakerski, 2011), the authors introduced new way of dimension-modulus reduction to control noise and thus to construct an FHE scheme based on the learning with error (LWE) problem. Soon after, Brakerski et al. (Brakerski, 2012b) made good use of modulus switching technique to obtain an FHE scheme without bootstrapping. Subsequently, the authors of (Brakerski, 2012a; Coron, 2014) gave several FHE schemes without modulus switching. At Crypto 2013 Gentry et al. (Gentry, 2013) used the approximate eigenvector method for building FHE scheme, which has no evaluation keys. This makes their scheme asymptotically faster and helps them construct the first identity-based FHE scheme. As a key technology for achieving FHE, faster bootstrapping is also explored in (Alperin-Sheriff, 2014; Ducas, 2015).

To increase the efficiency of FHE, the authors of (Smart, 2010) mentioned that their scheme can be adapted to support single-instruction multiple-data (SIMD) style operations, instead of operations on single bit messages. They in (Smart, 2011) described a ciphertext-packing technique based on polynomial Chinese Remainder Theorem (CRT), and Gentry et al. (Gentry, 2012) used that technique to achieve a nearly optimal homomorphic evaluation (up to polylogarithic factors). Most recently, the authors in (Chen, 2015) provided a scheme using double batch for RLWE-based FHE.

However, the above-mentioned FHE schemes are not efficient enough to be practical partly because bootstrapping is rather expensive and partly because ciphertext expansion is very large. A case in point shown in (Coron, 2013b) is that using FHE supporting bit operations homomorphic evaluates these functions with very large integer inputs. Lauter et al. (Lauter, 2011) therefore suggested that for many applications (say, private information retrieval), it suffices to have an SHE system which computes many additions and a small number of multiplications on ciphertexts. Hence, it is interesting to construct an SHE scheme over large message space.
The Contribution of Information Science Through Intellectual Property to Innovation in the Brazilian Health Sector

Characterizing the IT Artefact through Plato's Ontology: Performance Measurement Systems in the Web 3.0 Era