1 Cryptography and Homomorphic Encryption

My research focus is in cryptography, which is an area of applied algebra. Specifically, I study a topic called *homomorphic encryption*. Homomorphic encryption describes encryption schemes that allow for addition and multiplication operations to be performed on encrypted messages (called ciphertexts) without needing or leaking any information about the private key or user messages. Furthermore, the operations in the ciphertext space correspond to performing the same operations on the original messages, which can be performed by any third party with knowledge of only the public information. Homomorphic encryption has various modern applications, such as secure cloud computing and private machine learning.

Several modern homomorphic encryption schemes are based on polynomial rings. To best describe our results, we introduce some notation and examples. For a polynomial $\phi(x)$ of degree n and a large positive integer q, define the rings

$$R_n = \mathbb{Z}[x]/(\phi(x)),$$

$$R_{n,q} = \mathbb{Z}_q[x]/(\phi(x)) \cong \mathbb{Z}[x]/(\phi(x), q).$$

We first discuss the underlying hard problem for many homomorphic encryption schemes, called the *ring learning with errors* (RLWE) problem. For a secret $s \in R_{n,q}$, we sample uniform random $a \in R_{n,q}$, sample small random $e \in R_n$, and compute $b := -as + e \mod (\phi(x), q)$. The ordered pair $(a, b) \in R_{n,q}^2$ is called an *RLWE sample*. The Search-RLWE problem is to find s given many RLWE samples. The Decision-RLWE problem is, if given many samples that are either RLWE samples or sampled at uniform random from $R_{n,q}^2$, to decide which distribution the samples are from.

RLWE problems (and several other variations of learning with errors problems) have been shown to be at least as hard as some worst-case lattice problems such as `SVP` or γ-`GapSVP`. These lattice problems form foundations for cryptosystems that are post-quantum secure, meaning that these encryption schemes are secure against attacks by quantum computers. In fact, several finalists in the NIST post-quantum cryptography standardization process are based on these lattice problems.

To form an encryption based on RLWE, we first represent a message as a polynomial $m \in R_{n,t}$ for chosen positive integer parameter $t \geq 2$. We randomly choose a small polynomial $s \in R_n$, which is called our secret key. Then, we sample uniform random $a \in R_{n,q}$, sample small random $e \in R_n$, and compute $b := -as+m+te \mod (\phi(x), q)$. The polynomial pair $(a, b) \in R_{n,q}^2$ forms our ciphertext of m. Observe that $(a, b) \in$

$R_{n,q}^2$ closely resembles an RLWE sample. An adversary with access to only (a, b) will be unable to recover the message m. However, any users with access to both (a, b) and the secret key s will be able to recover m through a process known as *decryption*.

The unique aspect of this encryption process is that this design allows for computation directly in the ciphertext space. For a collection of polynomial pairs of the same format as (a, b) above, there are operations $\boxplus$ and $\boxtimes$ that we can perform between these ciphertexts in $R_{n,q}^2$. These ciphertext operations correspond to addition and multiplication of their respective messages in the message space. However, we require no knowledge of the private information s, m, or e to perform these ciphertext operations. We refer to this computation with ciphertext operations as *homomorphic computation*.

2 Results

Within the outlined encryption process, the term $e \in R_n$ is commonly referred to as a *noise term* or *noise*. When homomorphic computation is performed, the size of our noise term can grow. If noise gets too large, decryption failure can occur, meaning that the message m can no longer be recovered (by anyone, even those with access to the secret key).

In my research, I specifically study the worst-case noise bounds resulting from homomorphic computation. Under the direction of my advisor Dr. Shuhong Gao, I've proved several results which we describe in detail in [1]. Our main result derives and proves parameter conditions which guarantee a predetermined amount of homomorphic computation can always occur, with no probability of decryption failure. This allows for the ability to compute several commonly desired operations homomorphically, such as a standard inner product. We prove these results for 3 prominent homomorphic encryption schemes: the Brakerski-Gentry-Vaikuntanathan (BGV) scheme [2, 3], the Brakerski-Fan-Vercauteren (BFV) scheme [4], and the Cheon-Kim-Kim-Song (CKKS) scheme [5].

3 Current and Future Work

In the CKKS scheme, noise also impacts the precision accuracy of the final decrypted message. Few theoretical studies regarding the impacts of noise on accuracy have been conducted, and none of which give true worst-case bounds or conditions to preserve precision accuracy. The existing studies also do not account for extra error that may occur in implementations either, such as error resulting from floating-point arithmetic. We are currently working to design and prove parameter conditions which not only guarantee homomorphic computation without decryption failure, but also preserve precision accuracy.

Beyond noise analysis, I plan to further study the specific applications of homomorphic encryption in other areas of mathematical cryptography. This includes topics such as zero-knowledge proofs and secure multi-party computation, both of which have natural overlap and common techniques with homomorphic encryption.

4 Additional Topics and Interests

In addition to my main research area of cryptography, I also have research interests in optimization and signal processing. Specifically, I am interested in theoretical results related to the computational complexity of optimization problems used in signal processing.

A famous problem in signal processing is the *compressed sensing* problem, which is the problem of recovering a sparsest solution to a linear system $Ax = b$. Compressed sensing is known to be NP-hard, so several optimization problems have been proposed in order to approximate these sparse solutions. This includes $L_1 - L_2$ minimization, which is the problem of minimizing $\|x\|_1 - \|x\|_2$ subject to $Ax = b$. With the collaboration of Dr. Yuyuan Ouyang, we have proved $L_1 - L_2$ minimization is NP-hard. In addition to my cryptography research, I hope to continue research in the theory of optimization and complexity if given the opportunity.

References

[1] Gao S, Yates K. Leveled Homomorphic Encryption Schemes for Homomorphic Encryption Standard; 2024. Cryptology ePrint Archive, Paper 2024/991. Available from: `https://eprint.iacr.org/2024/991`.

[2] Brakerski Z, Gentry C, Vaikuntanathan V. Fully homomorphic encryption without bootstrapping; 2011. Cryptology ePrint Archive, Report 2011/277. Available from: `https://ia.cr/2011/277`.

[3] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans Comput Theory. 2014 jul;6(3). Available from: `https://doi.org/10.1145/2633600`.

[4] Fan J, Vercauteren F. Somewhat practical fully homomorphic encryption; 2012. `https://ia.cr/2012/144`. Cryptology ePrint Archive, Report 2012/144.

[5] Cheon JH, Kim A, Kim M, Song Y. Homomorphic encryption for arithmetic of approximate numbers. In: Takagi T, Peyrin T, editors. Advances in Cryptology – ASIACRYPT 2017. Cham: Springer International Publishing; 2017. p. 409-37.