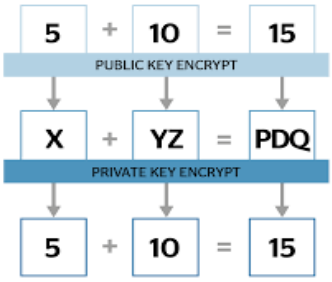
Moder Cryptography

20161190 이민재

1. Introduction

In the past, encryption were simply used to protect data. But modern times, they have been developed to enable many meaningful application. Among the various encryption methods, I would like to introduce homomorphic encryption.

For example, five plus ten equal to fifteen. Five encrypt to X, Ten encrypt to YZ, , Fifthteen is encrypt to PDQ. And then X + YZ equal to PDQ. decrypto to 15. It is same with five plus ten. This computational preservation is expressed in Enc and Dec as follows.



$$Dec\big(Enc(a) + Enc(b)\big) = \mathrm{a} + \mathrm{b}$$

This means that the addition operation is conserved.
So ,homomorphic encryption's characteristics can preserve operations. (In fact, depending on the type of HE scheme, the type of operation preserved or the type of Plaintext that can be received are different.) These can do many things possible so HE apply various field these days.

2. Various types of HE scheme

HE was actually presented in the late thousand nine hundred seventy, but it was difficult to put it into practical use due to a limit on the number of operations. However in two thousand nine, Gentry announced paper about fully homomorphic encryption(FHE), which has no limit on the number of operations. Since then, research on HE has been actively conducted and developed practically. Let's look at the pailier scheme, which is not fully homomorphic encryption, to the most used CKKS scheme recently.

- Paillier (1999)

Paillier invested namely the Composite Residuosity Class Problem, and its applications to public-key cryptography. The method of encryption and decryption algorithm are as follows.

- $Secret\ key \rightarrow sk = (p, q)$
- $Public\ key \rightarrow pk = (n(= pq), g)$
- $Enc(pk, m) \rightarrow c = g^m r^n\ (mod\ n^2)$
- $Dec(sk, c) \rightarrow m = \frac{L(c^\lambda mod n^2)}{L(g^\lambda mod n^2)} mod N$

First, pick two large prime p and q. These are secret key. And n is product of p and q. g is random select from relatively prime with n square. n and g are public key. At encryption. Message m is smaller than n. random r is relatively prime with n. Then, Chiphertext c is g's m square product r's n square mod n square. And decryption. Using Carmichael's theorem. This eqation's result is message m. At this equation L(x) equal x-1/p.

Pailler system advantage is relatively fast than fully homomorphic encryption. But this scheme is somewhat homomorphic encryption. And can't ciphertext multiplication. This scheme only can calcaulate ciphertext addition and constant multiplication at integer. So paillier scheme fits well in scenario where only ciphertext addition and constant multiplication is needed.

- BGV/BFV Scheme (2011)

Brakerski-Gentry-Vaikuntanathan, they present a new approach to fully homomorphic encryption (FHE) that improves performance and bases security on weaker assumptions in 2011. And they improved the speed of BGV then announced BFV in 2012.

- $Secret\ key \rightarrow sk = (s)$
- $Public\ key \rightarrow pk = (a, b(= as + pe))$
- $Enc(pk, m) \rightarrow (c_0, c_1) = (bv + pe_0 + m, av + pe_1)$
- $Dec(sk, c) \rightarrow m = (\big((c_0 - c_1 s) mod\ q\big) mod\ p)$

P is message space, q is ciphertext space. Secret key is s and public key is a,b. b is as+pe. This s in b, can decrypt by delete the value of asv. Encryption function result is c_0 and c1 that is c_0 is $bv + pe_0 + m$, c_1 is $av + pe_1$. Decryption algorithm is $\big((c_0 - c_1 s) mod\ q\big) mod\ p$.

$$c_0 - c_1 s = bv + pe_0 + m - (av + pe_1)s = (as + pe)v + pe_0 + m - (av + pe_1)s$$
$$= asv - asv + m + e(pv + p + ps)$$

So, $\big((c_0 - c_1 s) mod\ q\big) mod\ p = \Big(\big(asv - asv + m + e(pv + p + ps)\big) mod\ q\ \Big) mod\ p = m$

BGV support addition and multiplication operation of two ciphertext. Pros is efficient and can precise calculate at integer. But it can't calculate at decimal and complex number. . So BGV scheme fits well in scenario where precise calculation at integer space is needed.

- FHEW Scheme (2015)

Leo Ducas and Daniele Micciancio present a new method to homomorphically compute simple bit operations, and refresh (bootstrap) the resulting output, which runs on a personal computer in just about half a second.

In particular, when multiplication is performed, noise accumulates. So there is a limit to the operation. However, by using bootstrapping, bring the noise of the ciphertexts back to acceptable levels. In the past, most bootstrapping method based on the Linearization method. This bootstrapping method allows to homomorphically evaluate arbitrary circuits, but it is also the main bottleneck in any practical implementation due to the complexity of homomorphic decryption. FHEW scheme use another bootstrapping method instead of

relinearization. So this scheme's advantage is fast. But it can operate only NAND operation at bit. FHEW can be show good performance in situations where NAND operations in bit are required.

- TFHE Scheme (2016)

Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachene, they make a speed up from FHEW scheme (less than 1 second) to less than 0.1(zero point one) seconds. And also reduce bootstrapping key size 1GB to 24MB preserving the same security levels. FHEW and TFHE use different bootstrapping algorithm. FHEW scheme use Alperin-Sherif-Peikert (AP) and TFHE scheme use Gama-Izabachene-Nguyen-Xie (GINX). FHEW is based on Learning With Error (non-ring) but, TFHE is based on Ring Learning With Error (ring). This is the main algorithmic difference between FHEW and TFHE.

And the reason why TFHE requires binary secrets. While the AP bootstrapping algorithm can be equally applied to secrets of any size, the GINX one is directly applicable only to binary secrets. So TFHE can be show good performance in situations where NAND operations in bit are required.

- CKKS Scheme (2017)

JungHee Cheon, Andrey Kim, Miran Kim, Yongsoo Song, they suggest a method to construct a homomorphic encryption scheme for approximate arithmetic. In real-word there are many data has some errors. When we want to know the average value, it's enough to know the reasonable approximate value rather than the exact value. By approximate arithmetic feature, it improve the speed which is a disadvantage of HE.

It uses a technique called rescalling. Trubcates a ciphertext into a smaller modulus. This occur error. but it treat an encryption noise as part of error occurring during approximate computation. The main idea of this scheme is to handle an encryption noise as part of error occurring during approximate computations.

This scheme's advantage is possible calculate real and complex number quickly. But it can't precise calculation. So, CKKS scheme is suitable for AI fields that deal with vast amounts of data. For example, the following equations required in machine learning can be quickly computed.

– Average of n terms $\{c_i\}$: as a pair $(\sum_{i=1}^{n} c_i)$, where $m = \frac{\sum_{i=1}^{n} c_i}{n}$ is the average.

– Standard deviation: $\sqrt{\frac{\sum_{i=1}^{n}(c_i - m)^2}{n}}$, returned as a pair which is the numerator and denominator of the expression, before taking the square root.

– Logistical regression: $x = \sum_{i=1}^{n} \alpha_i x_i$, where α_i is the weighting constant or regression coeffficient for the variable x_i , and the prediction is $f(x) = \frac{e^x}{1+e^x}$

3. Application of HE in real life

As mentioned earlier, past crypto system's purpose is only protect data. But HE can preserve arithmetic so can apply meaningful applications HE can be applied in many fields. Health care, Cloud service, Ai and Post quantum cryptography and so on.

- Health Care

The existing healthcare industry has not grown significantly due to privacy regulations. Information related to the patient's disease is sensitive so regulated. However, HE can preprocess these data and store it in an encrypted form, and secure computational processing is possible without knowing the contents of the data.

- Cloud Service

Cloud services provide many services based on user information. But adoption of cloud services by consumers and businesses is limited by concerns over the loss of privacy or business value of their private data. But User data can be encrypted using HE and can provide various services without leakage.

And the metabus industry will soon grow very big. I think metabuses Users will also provide sensitive data such as house structure and body information to the cloud service as well as basic information. So HE will become more used in future than now.

- Artificial Intelligence

Artificial intelligence is developing rapidly these days. Machine learning requires a large amount of data. However, due to personal information issues, de-identification data is used. As a result, low performance comes out. To overcome this situation, pure data is encrypted using HE as it is, and machine learning is processed without leaking personal information.

- Post Quantum Cryptography

Cryptographic systems such as Internet banking, e-commerce, and telecommunications are made based on RSA. RSA is a system that uses features that take a very long time to factorize multiple of two large prime numbers. However, there is a shore algorithm that can efficiently factorization, and as quantum computers develop further, RSA will be breaks. Homomorphic encryption is strong against this quantum attack. But understanding this requires the concept of P vs NP.

- Decision problem : The problem that is answer to the question is either true or false.

- Polynomial-time algorithm(efficient algorithm) : Algorithm that has worst time complexity form is n^k.

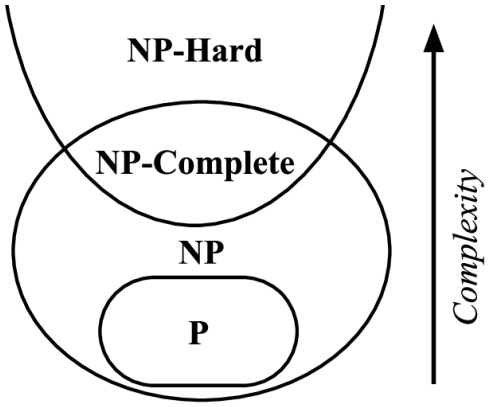
- Deterministic Algorithm : When a particular input comes in, it always goes through the same process and always produces the same result. (Check one by one to see if it is true or false.)

• Nondeterministic Algorithm : lgorithm that derives different results through different processes each time even if the same input is given. (It can be expressed that the correct answer also can be checked in a parallel world or already know the answer load.)

• P : set of problems that can be solved in polynomial time with some deterministic algorithm. (ex) Is a a multiple of b?)

• NP : set of problems that can be solved in polynomial time with some nondeterministic algorithm. (ex) Among the subsets of the set, is there a set in which the sum of elements becomes zero?)

• Reducibility : If there are problem X and Y. When we know the answer of X and does't know the answer of Y. And change Y input to X input form. Then the maked X input get the Y result. Y result change to approximate X result. Then we can solve the X. If these thing possible, we can say the problem is reduciable.



• NP-Hard : For a decision problem Y, if any problem X belonging to NP can be polynomially converted into Y in polynomial time, y is called NP-hard

• NP-complete : If a decision problem belongs to np and is NP-hard, we call it NP-complete.

HE is a lattice-based encryption system. The lattice problem is classified as an NP complete problem. which is a problem that has not been proven to be solved in polynomial time. Since HE is a quantum-resistant encryption, it can be useful for future cryptographic industry.

4. Conclusion

Homomorphic encryption can preserve operations. Existing HE had a limit on the number of operations.(SHE) However, due to A proposed by Gentry in 2009, Fully homomorphic encryption(FHE) without computational restrictions was proposed. Since then, research on HE has been actively conducted and developed practically.

I investigated the characteristics of each scheme. Each scheme had a different form of plaintext and conserved operations. So in the future, I will be able to decide well on which skims to use under some situation.

I also investigated homomorphic encryption use in real life. HE is used in the fileds Health care, Cloud service, Ai and Post quantum cryptography and so on. In particular, HE has quantum-resistatnt characteristics. In order to examine these in detail, I summarized the concepts related to N-NP problem.

When the homomorphic encryption first came out, the computation speed was very slow. So this point make it difficult to put it into practical use. However, in the last 10 years, HE

have achieved a speed improvement of about 10^{10}. Since then, it has begun to be used in real industries. HE is seen as an essential technology in the future.

References

- Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." *International conference on the theory and applications of cryptographic techniques*. Springer, Berlin, Heidelberg, 1999.

- Brakerski, Zvika, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping." *ACM Transactions on Computation Theory (TOCT)* 6.3 (2014): 1-36.

- Ducas, Léo, and Daniele Micciancio. "FHEW: bootstrapping homomorphic encryption in less than a second." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2015.

- Chillotti, Ilaria, et al. "Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds." *international conference on the theory and application of cryptology and information security*. Springer, Berlin, Heidelberg, 2016.

- Cheon, Jung Hee, et al. "Homomorphic encryption for arithmetic of approximate numbers." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Cham, 2017.

- Naehrig, Michael, Kristin Lauter, and Vinod Vaikuntanathan. "Can homomorphic encryption be practical?." *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*. 2011.

- Blog : https://gazelle-and-cs.tistory.com/64