LATTICES AND FULLY HOMOMORPHIC ENCRYPTIONS (FHE)

SHUHONG GAO

As distributed computing becomes more and more popular, there is an urgent need to protect privacy of massive sensitive data stored in clouds and blockchains. The traditional encryption schemes can provide privacy protection of data but do not allow performing analytics on encrypted data without decryption first. The Holy-Grail of cryptography is to have a practical encryption scheme that has the following properties: (a) encrypted data can be stored anywhere (e.g. untrusted clouds, or personal computers of hackers), (b) an adversary can use all the available computing techniques but still can not get any information on the original data in reasonable time (say 100 years), and (c) any third party (including cloud servers, hackers and insiders) can perform searching or analytics on the encrypted data to get search results in encrypted form, however, only the data owner (who has the secret decoding key) can decode the encrypted search results. A scheme having all the three properties is called a fully homomorphic encryption (FHE). If (c) is satisfied only for a class of searches (but not all possible searches), then it is called a somewhat homomorphic encryption (SHE). In comparison, traditional cryptosystems (e.g. RSA, AES, etc) have properties (a) and (b), but not (c) which is the most challenging part of an FHE scheme.

The topics of REU are selected from the following:

(1) Understanding the most recent developments on fully homomorphic encryptions;
(2) Studying computational problems in lattices, including LLL lattice reductions, shortest vector problems, learning with errors (LWE) problems;
(3) Applying FHE to solving other problems, for example, secure multi-party computation, practical zero knowledge proof, verifiable computing, etc;
(4) Finding practical solutions for the privacy problem on cryptocurrencies and blockchains.

References

[1] Martin R Albrecht, Rachel Player, and Sam Scott, *On the concrete hardness of learning with errors*, Journal of Mathematical Cryptology **9** (2015), no. 3, 169–203.
[2] Steven D. Galbraith, *Mathematics of public key cryptography*, 1st ed., Cambridge University Press, 2012.
[3] Shuhong Gao, *Efficient fully homomorphic encryption*, 2018. https://eprint.iacr.org/2018/637.
[4] Craig Gentry, *Fully homomorphic encryption using ideal lattices*, STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing, ACM, New York, 2009, pp. 169–178. MR 2780062
[5] Shai Halevi, *Tutorial on homomorphic encryption*, https://shaih.github.io/pubs/he-chapter.pdf (2017).
[6] Vadim Lyubashevsky, Chris Peikert, and Oded Regev, *On ideal lattices and learning with errors over rings*, Advances in cryptology—EUROCRYPT 2010, Lecture Notes in Comput. Sci., vol. 6110, Springer, Berlin, 2010, pp. 1–23. MR 2660480
[7] Oded Regev, *On lattices, learning with errors, random linear codes, and cryptography*, J. ACM **56** (2009), no. 6.