Master Thesis Topics in Secure, Ultra-Reliable, Low-Latency Communication

Our research interests lie in the applications of lattices and codes, where we are particularly interested in working with these special, symmetrical, and friendly mathematical structures. Coding theory and lattices can be applied to efficient alternatives of information transmission, distributed information systems, security, and cryptography, to name a few. Currently, the research topics we are interested in are as follows.

Coding for Physical Layer Security (PLS) in Beyond 5G (B5G)/6G Wireless Communication Systems

With the advent of quantum computers, PLS, which only utilizes the resources at the physical layers of the transmission parties and provides *information-theoretically unbreakable security*, has been recognized as an appealing technique for safeguarding confidential data in B5G/6G wireless communication systems recently. Such communication systems use information-theoretic approaches to guarantee unconditional data security, i.e., they are secure against an adversary without any limitation of computational resources. Previous works on PLS are mainly based on non-constructive random-coding arguments to establish theoretic results. Such results indicate that finding a coding scheme that transmits the highest amount of secure information is possible. Still, the practical usefulness of such a non-constructive approach is very little. The construction of practical codes for physical layer security deserves much more attention in real-world applications. Unfortunately, existing PLS coding solutions cannot meet the stringent latency and reliability requirements for short-packet communication since most previous works on PLS only provide impractical solutions for secure communication schemes under the assumption that an arbitrarily large coding block length can be used. We are currently interested in developing practical and efficient information-theoretically secure and reliable communication schemes against eavesdropping attacks using information theory and coding techniques. We aim to design **finite-length polar and lattice code-based** security coding schemes to ensure ultra-reliable and low-latency communication between the authorized parties while preventing an adversarial eavesdropper from learning the transmitted messages.

Security Analysis of Lattice-based Cryptography

The central computational problem in lattice-based cryptography is the *shortest vector problem (SVP)*: Given a lattice basis, the goal of the problem is to find the shortest non-zero vector in the lattice generated by the given basis. Recently, a simple and novel approach to showing the hardness of a variant of the approximate SVP problem has been proposed using a family of lattices generated via *Construction A* from *Reed-Solomon codes*. We are interested in investigating this presented analysis approach and improving the hardness results by considering different constructions of lattices from other classes of codes.

Lattice decoding

Finding the closest lattice point to a given real vector is hard when the dimension increases (the reason why this problem is also used to design cryptosystems), and we can call such a process lattice decoding. For some well-known lattices, efficient decoding algorithms can be derived due to their special structure, and this is the case for lattices constructed from linear codes. The idea here is to improve the lattice decoding by using characteristics from the codes.

Background Requirements

A strong background in algebra, discrete mathematics, and probability is required. Intermediate programming skills are also essential for verifying the theoretical findings. Please do not hesitate to contact us for further information.

Contact Details

- Dr. Øyvind Ytrehus, `oyvindy@simula.no`
- Dr. Hsuan-Yin Lin, `lin@simula.no`
  web: `http://hsuanyin-lin.com/main.html`