MATSUURA LAB.

Cryptography and Information Security

Department of Informatics and Electronics

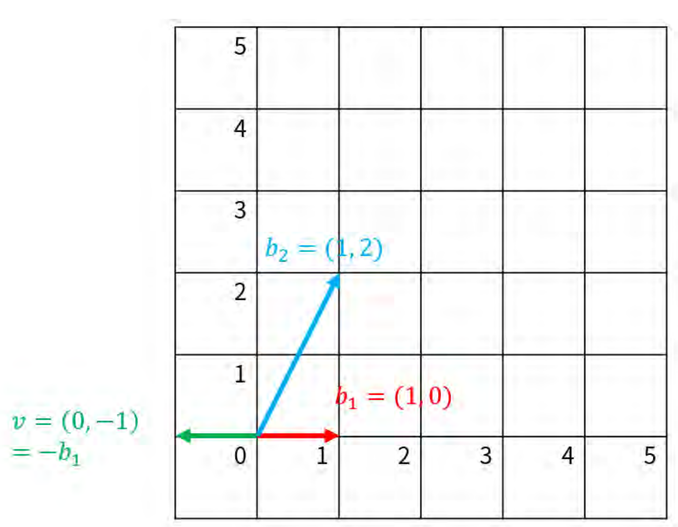
Information Security
Department of Information and Communication Engineering
http://kmlab.iis.u-tokyo.ac.jp/

Math for Post-quantum Cryptography

The security of public key cryptography is derived from the complexity of prime factorization and discrete logarithm problem. However, as the research of quantum computer progresses in the future, these problems might be solved in a short time. Then, as the cryptography scheme that could not be solved even by using quantum computer, **post-quantum cryptography (PQC)** is expected.

- ### Learning With Errors (LWE)

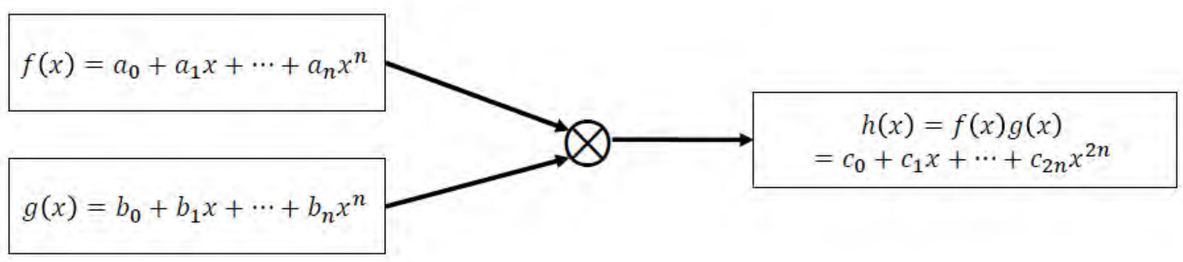
  A mathematical problem often used in PQC
  A problem that solves simultaneous equations with errors
  It is reduced to the lattice problem called Shortest Vector Problem (SVP)



- ### Calculation acceleration of LWE

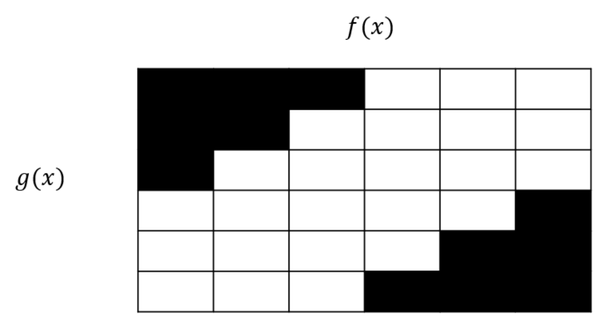
  - #### NTT (Number Theorem Transform)

    NTT is a method that accelerates polynomial multiplication
    Using NTT, polynomial multiplication can be conducted in $O(n \log n)$ times, which is $O(n^2)$ if conducted naively
    We focus on parallel computing to accelerate NTT



  - #### middle product

    Recently, LWE using middle-product is proposed [1]
    It has an advantage of realizing both fast calculation and high security
    We focus on accelerating middle-product using NTT or Karatsuba method



[1]: Guillaume Hanrot, Michel Quercia, and Paul Zimmermann. The middle product algorithm I. Applicable Algebra Engineering, Communication and Computing, 14(6):415–438, 2004.