# 松浦研究室

## 暗号と情報セキュリティ

情報・エレクトロニクス系部門

情報セキュリティ

情報理工学系研究科 電子情報学専攻

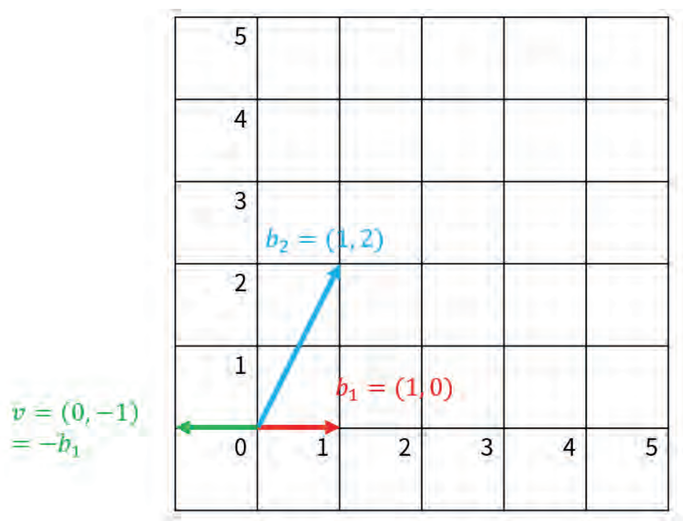
http://kmlab.iis.u-tokyo.ac.jp/

## 耐量子計算機暗号を実現する数学

暗号通信で多く用いられている公開鍵暗号方式の安全性は、素因数分解や離散対数問題の計算困難性によるものである。しかし、量子コンピュータの技術の進歩により、将来的にこれらの問題が高速に解かれる可能性がある。そこで、量子コンピュータでも解読されない暗号（**耐量子計算機暗号**）の実現が期待される。

- **Learning With Errors（LWE）**

  耐量子計算機暗号でしばしば用いられる数学的問題の一つ
  誤差つきの連立方程式を解く問題
  **最短ベクトル問題**と呼ばれる格子問題に帰着される

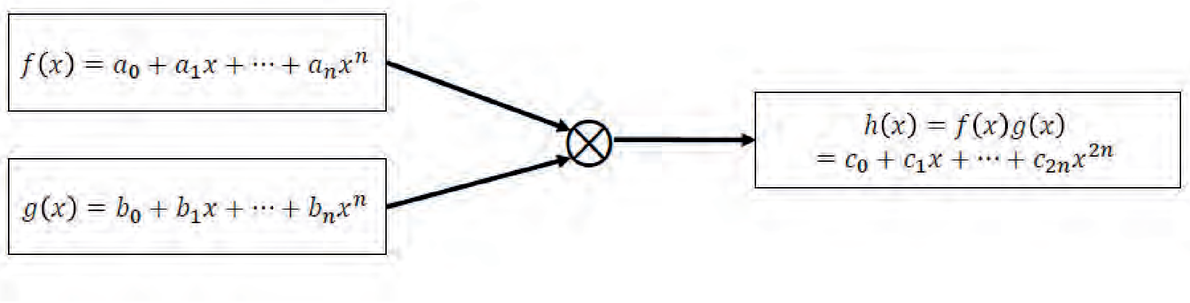



- **LWE の高速計算**

  - NTT（Number Theorem Transform）

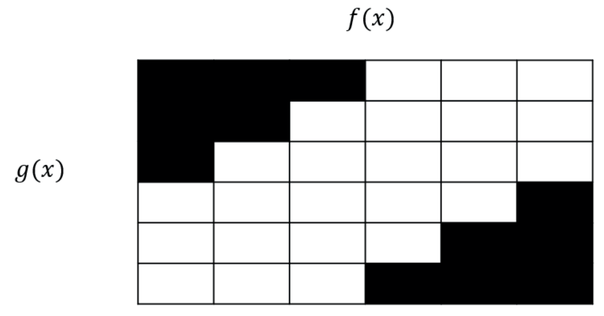
    LWE で必要となる、多項式の乗算を
    高速に行う手法
    愚直にやれば $O(n^2)$ かかる
    多項式乗算を、離散フーリエ変換の
    応用により、 $O(n \log n)$ で実現する

    並列計算などを用いた計算の高速化に
    取り組んでいる




  - 中間積計算

    近年になって、中間積（Middle-product）と呼ばれる演算を
    用いた方式の LWE も提案されている [1]
    高速な演算を実現しつつ、安全性も担保される利点がある
    NTT や、Karatsuba 法を活用した高速な中間積計算に
    取り組んでいる




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