東京大学大学院情報理工学系研究科
数理情報学専攻

数理情報第1研究室紹介

2023年5月20日

数理情報第1研究室メンバ

教授： 高木 剛（代数数理工学、現代暗号理論）
学部担当講義　大学院担当講義

講師： 高安 敦（情報理論、現代情報理論）

助教: 相川 勇輔

特任助教: 小貫 啓史

特任研究員: 3名

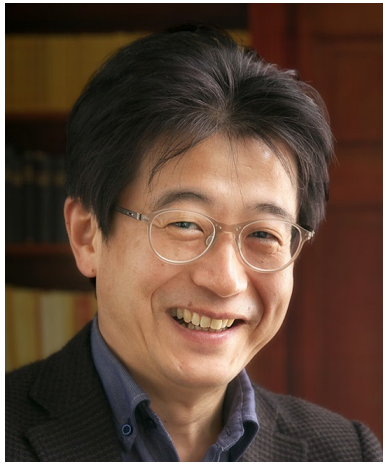
大学院学生(博士課程)

3名　←学振DC1/DC2, SPRING-GX

大学院学生(修士課程)

9名

その他（大学院研究生、留学生）: 数名


高木 剛


高安 敦

現代社会と暗号技術

昔の暗号

限られた人だけが使う特殊技術

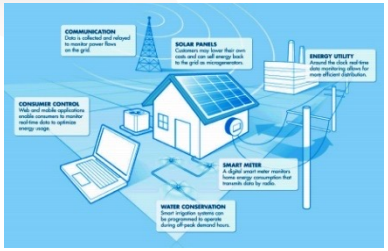
現代の暗号

電子政府

個人認証、プライバシー保護

電子決済、仮想通貨

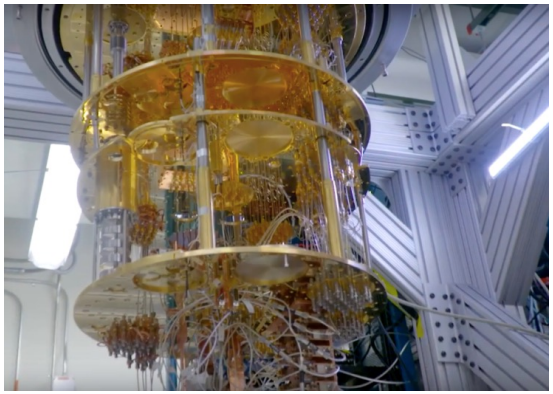
著作権保護、コピー防止



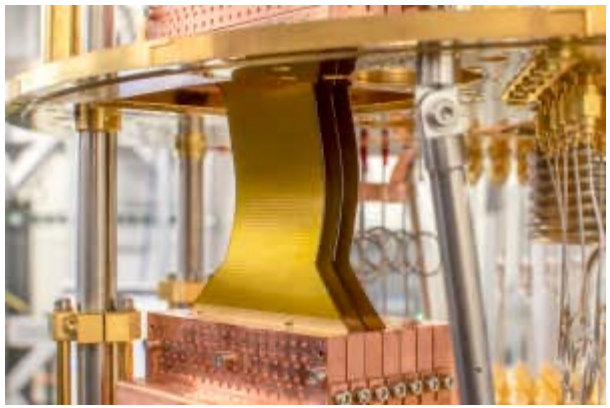
電気自動車、スマートグリッド

暗号は現代社会に無くてはならない技術

量子クラウド IBM Q



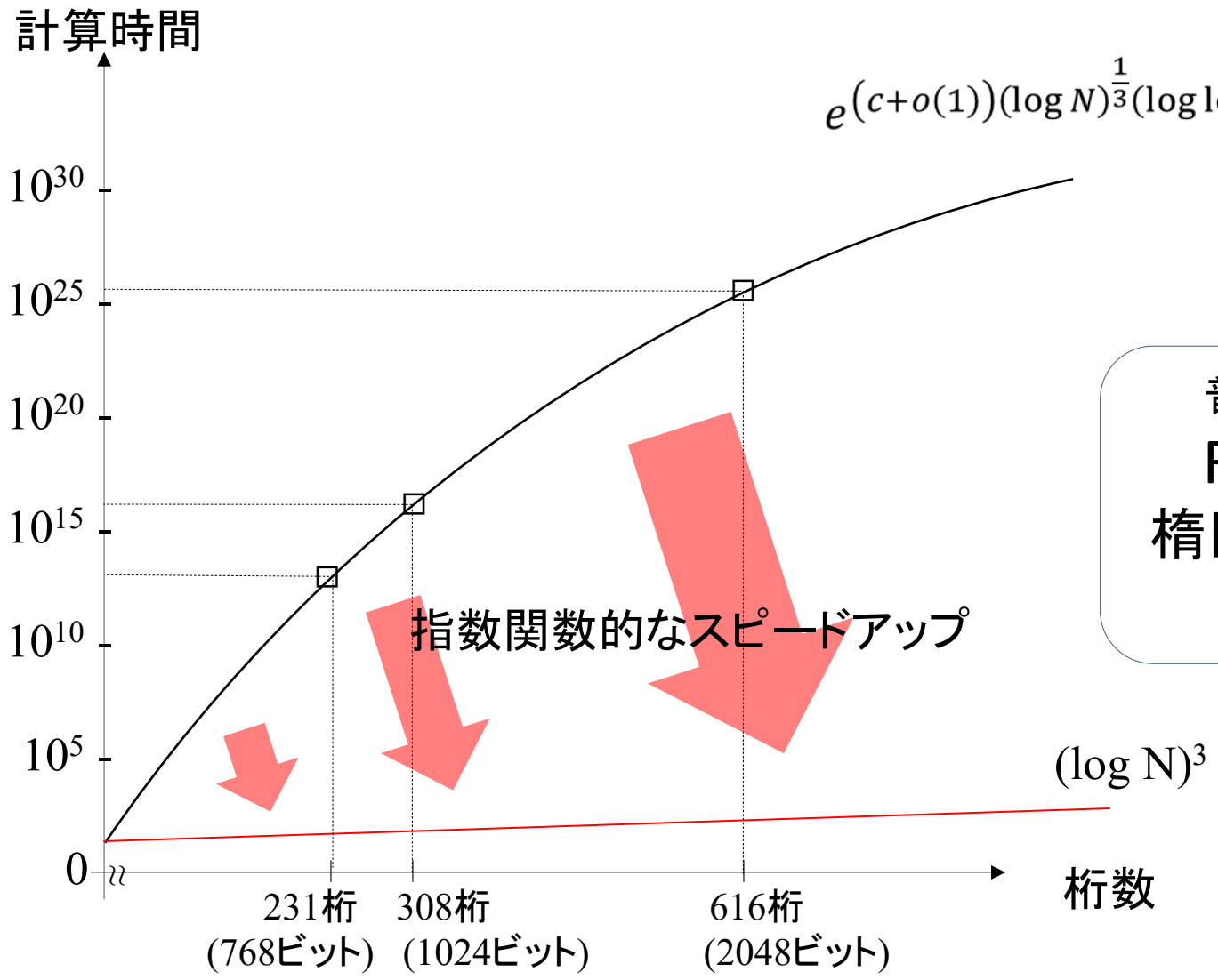
https://www.research.ibm.com/ibm-q/ より転載



IBM Quantum Roadmap
1,121 qubits (2023)
433 qubits (2022)
127 qubits (2021)
65 qubits (2020)

量子超越性

量子コンピュータによる素因数分解



普及している
RSA暗号
楕円曲線暗号
危殆化

ポスト量子暗号
(Post-Quantum Cryptography)

米国標準技術研究所NISTによるPQC標準化計画

http://csrc.nist.gov/groups/ST/post-quantum-crypto/

利用される数学問題

- 格子暗号 (Lattice-based cryptography)
- 符号暗号 (Code-based cryptography)
- 多変数多項式暗号 (Multivariate polynomial cryptography)
- ハッシュ関数署名 (Hash-based signature)
- 同種写像暗号 (Isogeny-based cryptography)

多変数多項式暗号

有限体GF(q)上の n変数の m個の
2次多項式の共通解を求める問題。

$$\begin{cases} f_1(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1 \\ f_2(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m \end{cases}$$

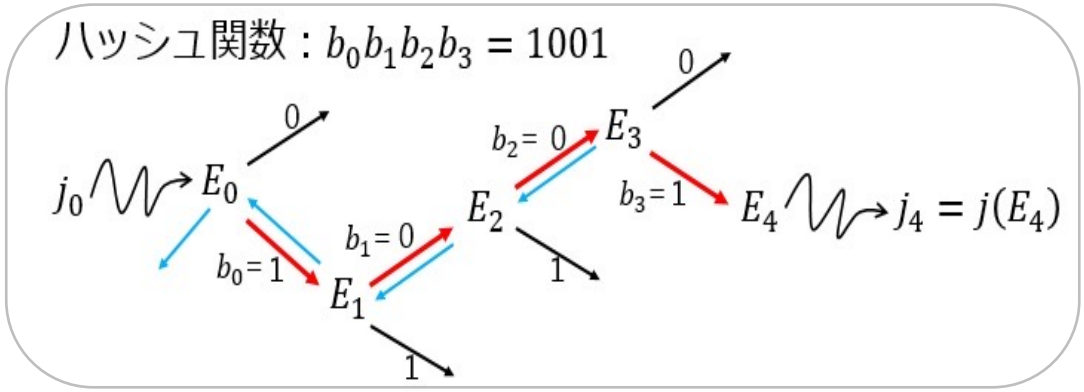
この問題はNP困難であることが知られている。

本研究室では新しい多変数多項式署名QR-UOV を開発した。

Furue, Ikematsu, Kiyomura, Takagi, "A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV“, Aisacrypt 2021.

ラマヌジャングラフによる暗号

・楕円曲線同種写像による暗号方式



暗号に適した数学構造
- ランダムウォーク
- 急速攪拌性
- 素数分布

☆IND-CPA安全性を有する公開鍵暗号SiGamalを発表した。

Scheme	SIDH	CSIDH	SETA	SiGamal
Hash function	Use	Use	Not use	**Not use**
Security	IND-CPA	IND-CPA	OW-CPA	**IND-CPA**
Assumption	SSDDH	CSSDDH	RCSSI	P-CSSDDH

Tomoki Moriya, Hiroshi Onuki, Tsuyoshi Takagi, “SiGamal: A Supersingular Isogeny-based PKE and its Application to a PRF,” ASIACRYPT 2020, LNCS 12492, pp.551–580, 2020.

格子暗号

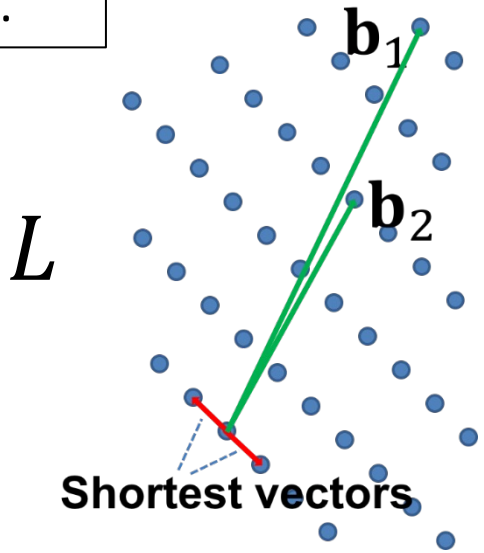
1次独立なベクトル $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ の整数係数の線形和全体

格子 $L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{t=1}^{n} x_t \mathbf{b}_t, x_t \in \mathbb{Z}\}$.

ユークリッドノルム $\mathbf{v} \in \mathbb{R}^m$, $\|\mathbf{v}\| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$, where
$\mathbf{v} \cdot \mathbf{w} = \sum_{i=1}^{m} v_i w_i$ for $\mathbf{v} = (v_1, \ldots, v_m)$, $\mathbf{w} = (w_1, \ldots, w_m)$.

Shortest Vector Problem (SVP)
Input: 格子Lの基底 $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$
Output: 非零の最短ベクトル

NP困難な問題として暗号で利用



本研究室では格子暗号の安全性評価の研究を進めている。

Uemura, Fukushima, Kiyomoto, Kudo, Takagi, “Shortest Vectors in Lattices of Bai-Galbraith’s Embedding Attack on the LWR Problem”, IWSEC 2021.

共同研究先

- 民間企業

NTT研究所

KDDI研究所

東芝研究開発センター

三菱電機研究所

NHK放送技術研究所

- 公的機関

情報通信研究機構

産業技術総合研究所

- 大型研究プロジェクト

JST CREST 暗号数理