

多変数多項式システムを用いた 安全な暗号技術の研究 (131310002)

研究代表者 安田貴徳

九州先端科学技術研究所

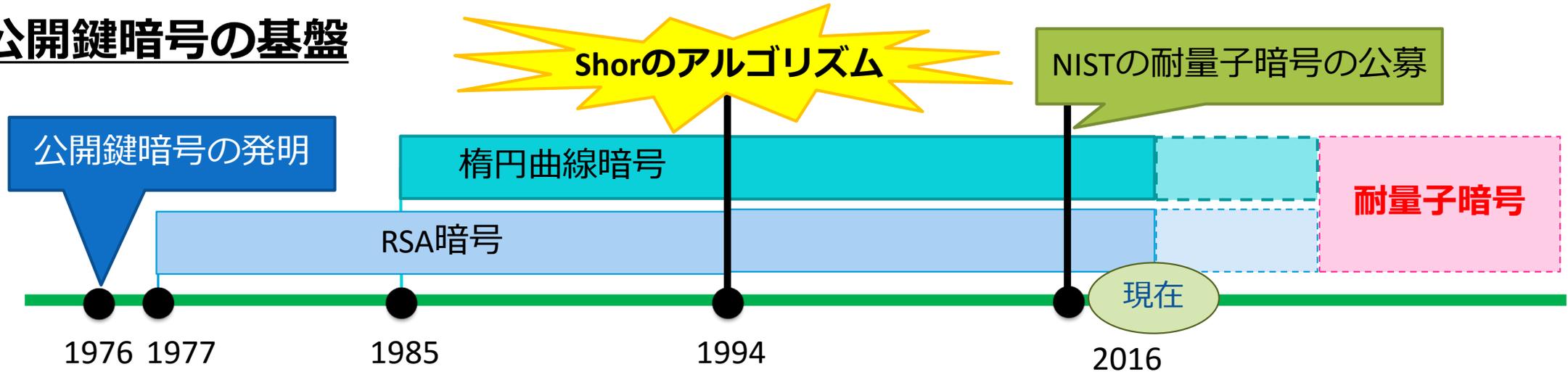
研究分担者

櫻井幸一[†] 高木剛[†] ダハン・グザヴィエ[†] ホアン・ユンジュ[†]

[†]九州先端科学技術研究所

研究開発の目的

公開鍵暗号の基盤



- 量子コンピュータに耐性を持つ次世代暗号（耐量子暗号）の開発が急務
- 耐量子暗号として、多変数多項式公開鍵暗号の実用化の可能性を研究



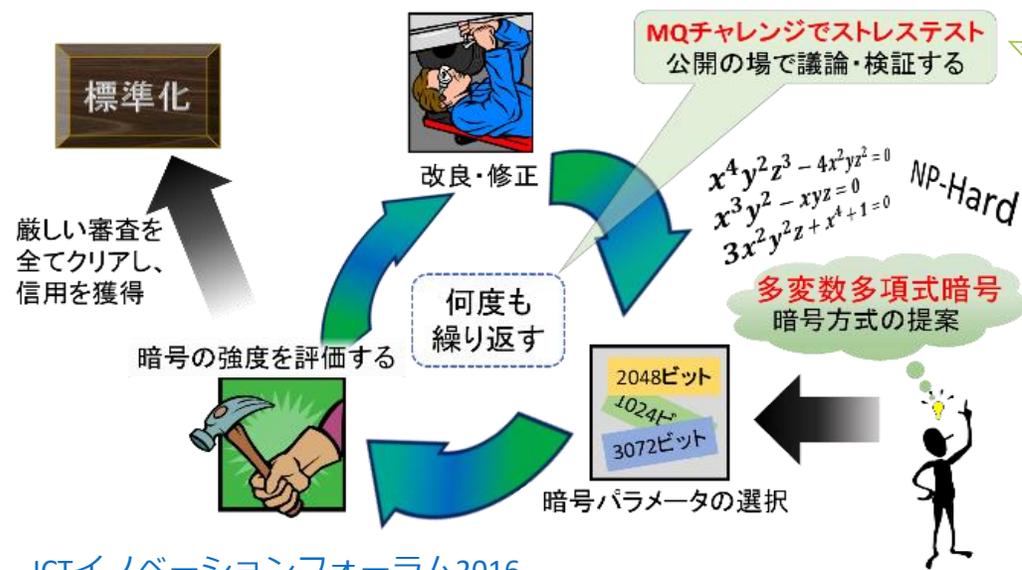
量子コンピュータ研究の発達

- 2011年、「D-wave」の開発
 - 2016年5月、IBMによる5量子ビットの量子コンピュータのオンライン公開
- など...

研究内容と成果 1

多変数多項式公開鍵暗号の安全性の解析

- 理論的解析
 - 攻撃アルゴリズムの解析と計算量の計算
- 実験的解析
 - 公開の解読コンテスト「MQチャレンジ」の開催



Fukuoka MQ Challenge

Submission

Guide for Participants

How to participate

Challenge Format

Download Challenges

Encryption (m=2n)

Type I Type II Type III

Toy examples and answers of n=10, 15, 20

10 15 20

News

2016/03/11 Type V of n=27 and m=18 was solved by Rusydi Makarim, Marc Stevens.

2016/02/29 Type VI of n=27 and m=18 was solved by Rusydi Makarim, Marc Stevens.

2016/02/28 Type V of n=25 and m=17 was solved by Rusydi Makarim, Marc Stevens.

2016/02/25 Type VI of n=25 and m=17 was solved by Rusydi Makarim, Marc Stevens.

2016/02/24 Type V of n=24 and m=16 was solved by Rusydi Makarim, Marc Stevens.

2016/02/24 Type VI of n=24 and m=16 was solved by Rusydi Makarim, Marc Stevens.

more>>

Introduction

Welcome to the Fukuoka MQ challenge project.

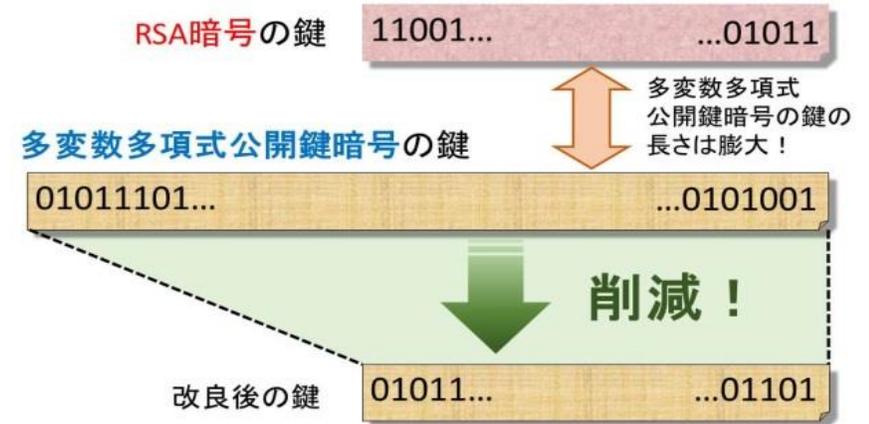
Multivariate (quadratic) polynomial (MQ) problem is the basis of security for potentially post-quantum crypte systems. The hardness of solving MQ problem depends on a number of

現在も実施中のMQチャレンジのホームページ
<https://www.mqchallenge.org/>

研究内容と成果 2

多変数多項式公開鍵暗号の課題の解決と 実用的方式の開発

- これまでの課題
 - 鍵長の削減、暗号方式の開発、効率性の向上など
- 課題の克服方法、新しい方式の開発を行った
 - 鍵長をRSAの約10倍の大きさに抑える方法を開発
 - 新しい暗号方式を提案
 - GPUを用いた多変数多項式計算の効率化
 - 部分復号法の開発



**世界初. ネット配信コンテンツを
一発でプレ視聴・フル視聴！**
～新たな暗号技術を開発～

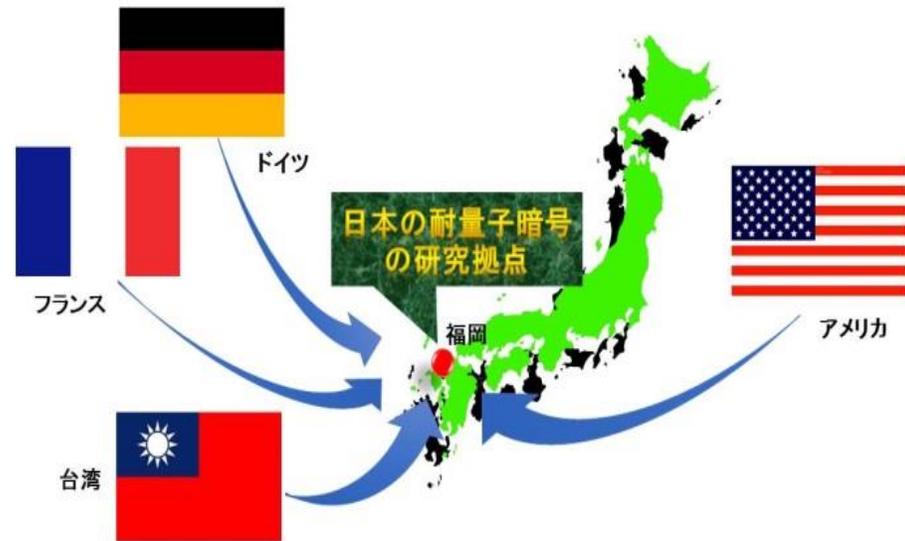
- 従来, 複数暗号の組み合わせ → コンテンツ保護のキー管理がたいへん...
 $R_2: \mathbb{Z}[x_1, x_2]/(x_1^{N_1} - 1, x_2^{N_2} - 1)$
 $R_1: \mathbb{Z}[x_1]/(x_1^{N_1} - 1)$
- 新暗号技術 → ひとつで実現 $\phi_Z: R_2 \rightarrow R_1$
- 一度に全部送信 → 購入キーに応じプレ視聴・フル視聴

研究内容と成果 3

ワークショップと国際会議の開催

- ワークショップ開催 2 回
- 耐量子暗号PQCrypt2016の開催

- NIST(アメリカ国立標準技術研究所)のアナウンス
- ✓ 2017年11月 標準化提案締め切り
 - ✓ 3~5年 解析フェーズ
 - ✓ 2年後 標準化案作成



今後の展開及び取り組み

1. MQチャレンジの継続
 - 新しい投稿、挑戦者
2. 提案方式の標準化
 - より詳細な安全性検証が必要