CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会
暗号技術調査ワーキンググループ
（暗号解析評価）
活動報告

主査　高木 剛

東京大学・九州大学

CRYPTREC
Cryptography Research and Evaluation Committees

2017年度 CRYPTREC 体制

本ワーキンググループの目的

- 今日，公開鍵暗号の安全性を支えている
  数学的問題には様々なものが存在する.
- このような数学的問題に関する調査を行うのが，
  本ワーキンググループの主目的である.

主査：高木 剛（東京大学・九州大学）
委員：青木 和麻呂(NTT)
委員：草川 恵太(NTT)
委員：國廣 昇（東京大学）
委員：下山 武司（富士通研究所）
委員：高島 克幸（三菱電機）
委員：安田 貴徳（岡山理科大学）
委員：安田 雅哉（九州大学）

公開鍵暗号の歴史

RSA暗号 (素因数分解問題)

広く普及　楕円曲線暗号 (離散対数問題)

ペアリング暗号 (クラウド時代向けの暗号)

標準化、製品化

ポスト量子暗号 (格子理論, 多変数多項式,符号理論,同種写像)

完全準同型暗号, 多重線形性暗号, 難読化

研究段階

2015～2016年度調査対象

- 下記の項目について，近年の研究動向を調査し，レポートを作成した:
  - 多重線形写像及び難読化
  - 楕円曲線上の離散対数問題に対する指数計算法
  - その他
    - (一般数体篩法の篩処理に関する)予測図の更新
- これらは，CRYPTRECシンポジウム2016にて紹介した.

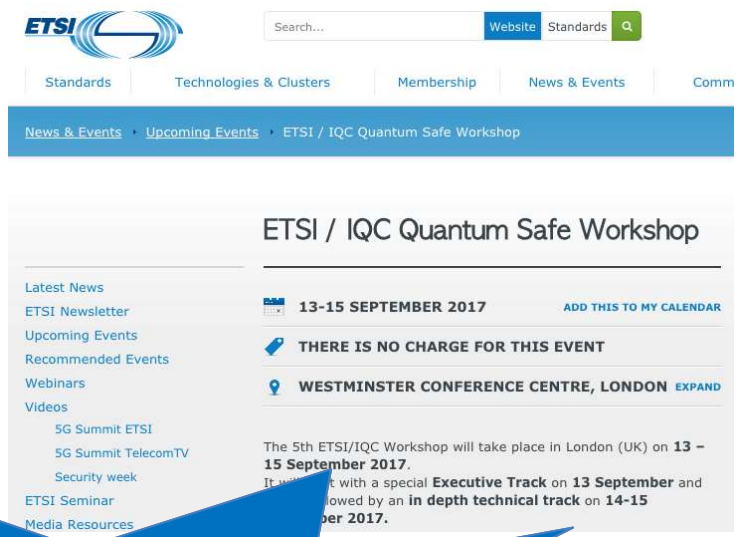
2017～2018年度の活動計画
（耐量子計算機暗号の研究動向調査）

耐量子計算機暗号(PQC)の研究動向調査

- 背景
  - もし十分な規模の量子計算機が実用化されると？
    ⇒RSA 暗号や楕円曲線暗号は安全性を保てない.
  - ある技術者は，今後20年以内に十分な規模の量子計算機が構築されると予想.
  - 現在利用されている暗号は，利用可能になるまで20年近くかかっている.
  - 今から PQC の実用化に取り組む必要がある.

参照（NIST）：https://csrc.nist.gov/projects/post-quantum-cryptography

- 背景（続き）
  - 世界各国の動き
    - 米国（NIST）: PQCの公募を開始（締め切り：11/30）
    - 欧州（ETSI）：PQCの調査を実施 (Workshop 開催など)



国内でもPQCの研究動向を
把握する必要性が高まっている.

PQCの研究動向調査計画

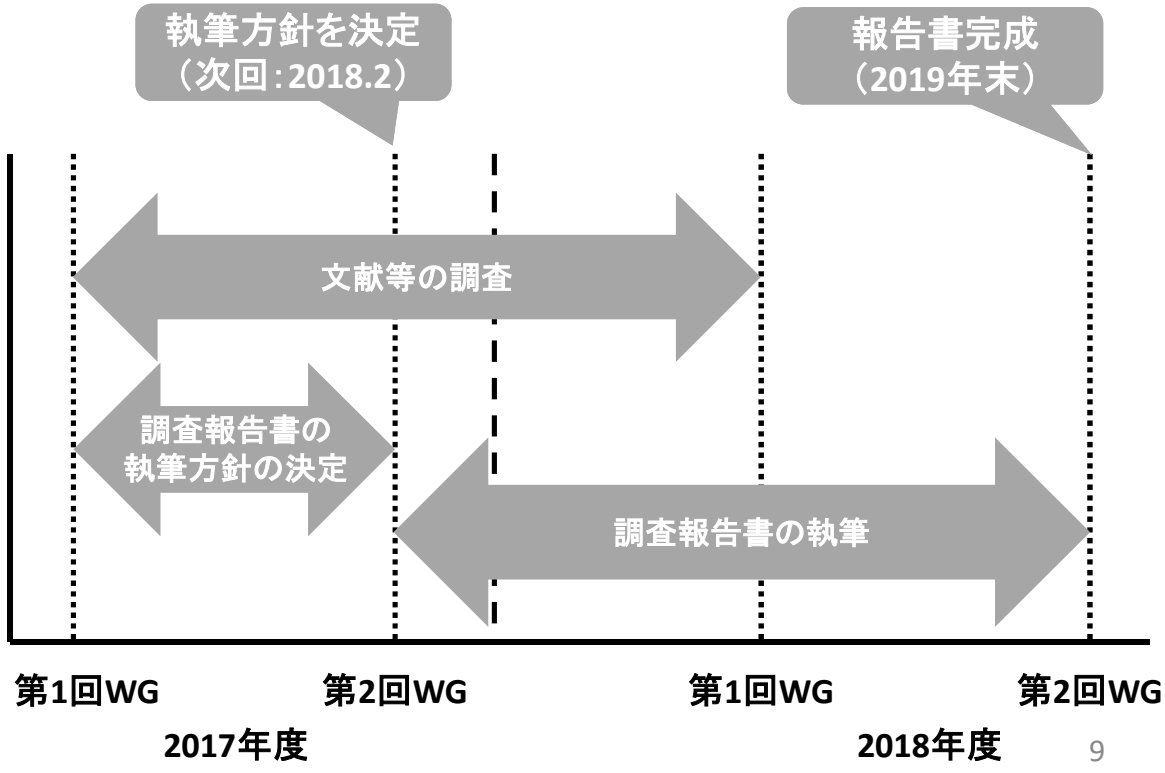
- 活動内容(2017 年度及び 2018 年度)
  - PQCの代表的な四方式について
    三つの機能を中心に調査し, 結果をまとめる.

四つの暗号方式

- 格子暗号
- 多変数公開鍵暗号
- 符号ベース暗号
- 同種写像暗号

三つの機能

- 暗号
- 署名
- 鍵交換



まとめ

- 2017年度及び2018年度の二年間で,
  PQC の研究動向調査を実施する.

- 2017年度は PQC に関する主な研究を把握し,
  調査報告書の執筆方針を決定する.

- 2018年度は調査報告書を作成する.