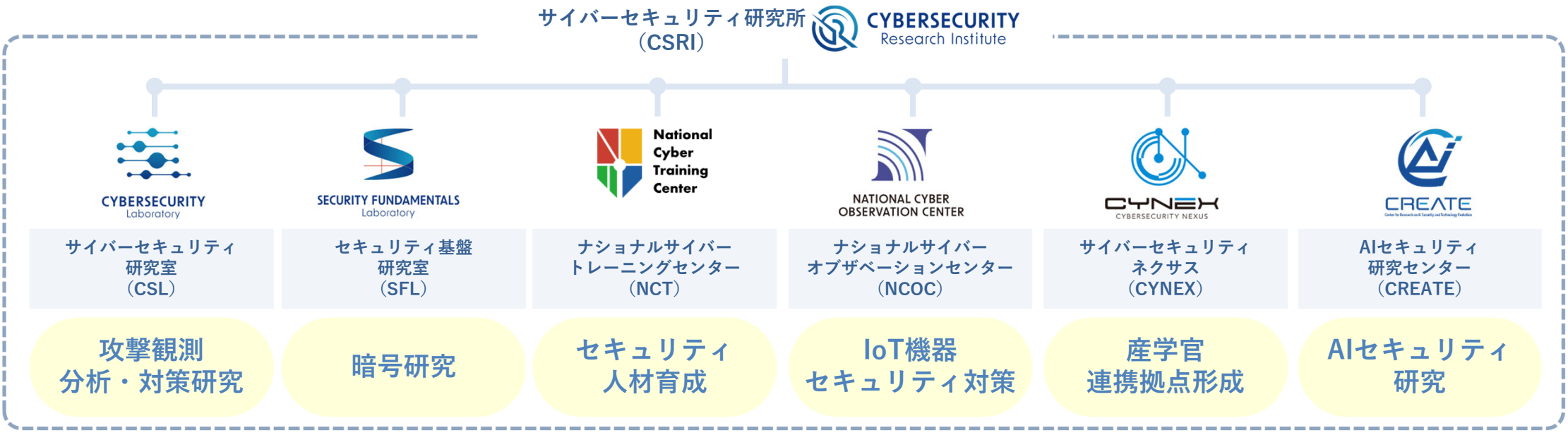
暗号って暗くない？！
明るいインフラ、暗号にお任せあれ

2026年2月14日

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所　セキュリティ基盤研究室
室長　小川一人

サイバーセキュリティ研究所

国立研究開発法人情報通信研究機構（NICT）において戦略的に進めるべき4つの研究領域の一つである『サイバーセキュリティ』に取り組む研究所です。
我々は社会（生命・財産・情報）を守る能力を高める技術について、基礎研究から社会実装、人材育成まで幅広く貢献することでイノベーションを促進していきます。



サイバーセキュリティ研究所

国立研究開発法人情報通信研究機構（NICT）において戦略的に進めるべき4つの研究領域の一つである『サイバーセキュリティ』に取り組む研究所です。
我々は社会（生命・財産・情報）を守る能力を高める技術について、基礎研究から社会実装、人材育成まで幅広く貢献することでイノベーションを促進していきます。

サイバーセキュリティ研究所（CSRI）

CYBERSECURITY Research Institute

SECURITY FUNDAMENTALS Laboratory

セキュリティ基盤研究室（SFL）

暗号研究

CYBERSECURITY Laboratory

サイバーセキュリティ研究室（CSL）

攻撃観測
分析・対策研究

National Cyber Training Center

ナショナルサイバートレーニングセンター（NCT）

セキュリティ
人材育成

NATIONAL CYBER OBSERVATION CENTER

ナショナルサイバーオブザベーションセンター（NCOC）

IoT機器
セキュリティ対策

CYNEX CYBERSECURITY NEXUS

サイバーセキュリティネクサス（CYNEX）

産学官
連携拠点形成

CREATE

AIセキュリティ研究センター（CREATE）

AIセキュリティ
研究

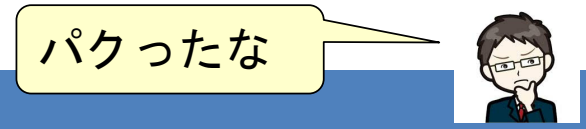
質問

暗号って　「暗い」　ですか？

回答

諸説あります

「暗い」印象：　正しくもあり、間違えでもあります。



“暗号” なぜ、この名前になったか？

暗号が“暗い”と思われる理由　：　文字に “暗” が入っている

なぜ、この漢字になったか？

〇説１（国語大辞典）（Yahoo！知恵袋）(漢字源）(大字源）

◇起源は中国語？ “暗”は“くらい”の意味の他に“ひそかに” という意味

“号”はマーク 二つを足して “暗号 ＝ ひそかなマーク”。

◇日本：1600年頃 “あいことば”

→ 1860年頃 “符号で定めた合図”

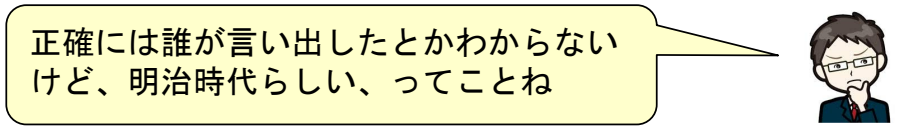
→ 1900年頃 “当事者間で取り決めた符号、または、方法”

〇説２（Google AI）

◇明治時代にcode 、cipherの日本語訳として使われ始めた

〇説３

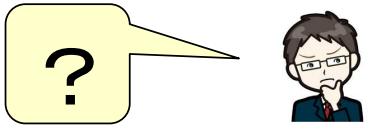
◇・・・



“暗号” を明るくする？

“暗号” を明るくする研究って

何？



“暗号” の役目から考えよう

暗号の役目の例:

攻撃者の悪の手から
- データを保護する
- なりすましを防ぐ
- …

データが保護できる

⇩

データの安全な利活用ができる

⇩

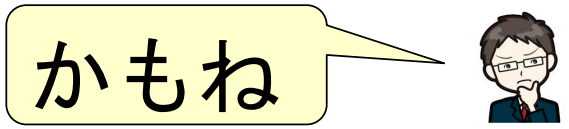
明るいインフラ

⇩

ちゃんとした暗号があれば:
見えてきませんか、暗号が作り出す明るい世界

よく考えて！！

- “暗号”は暗くも明るくもありません。
- “暗号”から思い出されるイメージが **「暗い」**
- “暗号”で明るい世界が導かれれば、イメージが変わる？



NICT
サイバーセキュリティ研究所
セキュリティ基盤研究室
による
明るいインフラ作り

セキュリティ基盤研究室の研究

SECURITY FUNDAMENTALS Laboratory

2021年度～2025年度計画（第５期中長期）

社会の持続的発展において欠くことのできない情報のセキュリティやプライバシーの確保を確かなものとするため、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施し、その安全性評価を行うとともに、安全な情報利活用を推進し、国民生活を支える様々なシステムへの普及を図る。

（ア）安全なデータ利活用技術

データの提供・収集・保管・解析・展開の各段階におけるセキュリティやプライバシーを確保するため、匿名認証や検索可能暗号等のアクセス制御技術、秘匿計算等のプライバシー保護解析技術等の研究開発を行う。これらを用いて組織横断的な連携を含むデータ利活用を促進するとともに、安全なテレワーク等の社会的な課題解決に貢献する。

（イ）量子コンピュータ時代に向けた暗号技術の安全性評価

量子コンピュータ時代に安全に利用できる暗号基盤技術の確立を目指し、耐量子計算機暗号を含む新たな暗号技術及び電子政府システム等において使用される暗号技術の安全性評価に関する研究開発を実施する。具体的には、将来的には耐量子計算機暗号として世界標準となることが予想される格子暗号、多変数公開鍵暗号等や、現在広く使用されているRSA暗号、楕円曲線暗号等の安全性評価について取り組み、世界最先端の評価技術によって国民生活を支える様々なシステムの安全な運用に貢献する。

セキュリティ基盤研究室の研究具体編

本日の紹介内容

☆1　DeepProtectの開発～社会実装

☆2　E2EEの安全性評価

☆3　検索可能暗号の実装

☆4　ロケットでの安全な無線通信

☆5　暗号技術の安全性評価

☆6　CRYPTREC活動

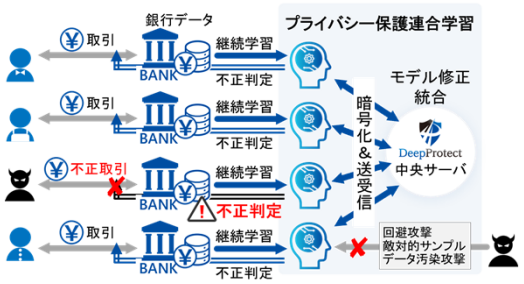
☆7　現代暗号の安全性評価例

☆8　耐量子計算機暗号のエトセトラ

☆9　今後の計画

☆1　DeepProtectの開発～社会実装

- DeepProtectとは：プライバシー保護連合学習技術



➢複数の組織が持つデータセットを互いに秘匿し、プライバシーや機密性をたもったまま共同でディープラーニングを行う技術

具体的な実施内容 ：

◆**DeepProtectをシステムとして開発し社会実装**

金融分野における実証実験ー不正送金検知

医療分野応用への拡大

◆**要素技術の開発**

◆準同型暗号／準同型性のある暗号プロトコル

◆PRIMO、DP-FedELM、PPDT等

☆2　E2EEの安全性評価

- E2EE（End-to-End Encryption）とは

➢エンドユーザとエンドユーザの間で暗号化通信路を作成し、中間に位置するサービスプロバイダであっても、盗聴を不可にする技術

具体的な実施内容 ：脆弱性（なりすまし等の攻撃手法）の発見
◆**Zoom**の安全性評価
　　ーー　SCISイノベーション論文賞
◆**Webex**の安全性評価
◆**Line、Nostr、Rocket.Chat、WhatsApp**
　　ーー　Black Hat USA他トップカンファレンスで採択

☆３　検索可能暗号の実装

- 検索可能暗号とは

➢サービスプロバイダにDBを設置するが、DBの内容、DBへのクエリはユーザが暗号化し、サービスプロバイダには内容がわからないようにする技術

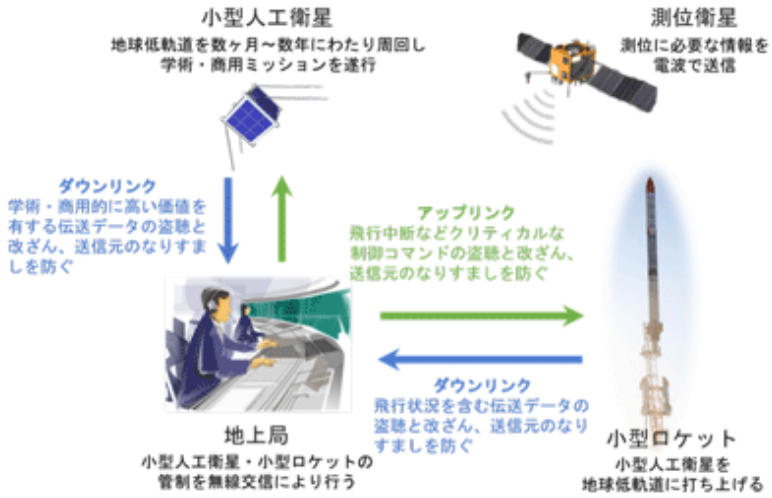
具体的な実施内容
- ◆　暗号化されていても検索可能な検索暗号の開発
- ◆　検索可能暗号とE2EEを応用したシステムの開発
  - ➢　体験版として、一般の方々に試用していただいた
- ◆　放送番組検索への応用
  - ーー　放送型公開鍵暗号検索可能暗号の一般的更生法を提案

☆4　ロケットでの安全な無線通信

SECURITY FUNDAMENTALS Laboratory

- **小型衛星・小型ロケット用の暗号化通信の安全性を確保**
  - ➢ 宇宙空間での通信確保
    - ➢地上とロケット感の伝送データ（資料データ、制御データ）の盗聴、改ざん、なりすまし防止

宇宙線等で装置が一時故障…　　装置が一時故障しても安全



具体的な実施内容

◆　鍵同期方式の開発：　通信にロスが生じた場合の対応
- ➢ プロトタイプ実装にて実用性・有効性を確認

◆　宇宙環境下での暗号回路の堅牢可・高速化
- ➢ 放射線耐性を持つ・実用セキュリティ（形式検証で高速検証）

――　NASA Formal Methos Honorable Mention 受賞

☆5　暗号技術の安全性評価

- 現行暗号方式の評価
  - AES、Camellia等を高速かつ、厳密に評価可能なツール開発
  - HMACの偽造攻撃耐性評価
  - AESの鍵スケジュールの再設計
  - SATソルバーによる暗号技術の厳密な評価手法の提案
  - ・・・

- 耐量子計算機暗号（PQC: Post Quantum Cryptography)の評価
  - 格子暗号評価用　ENUMアルゴリズムによる理論値の再評価
  - 多変数公開鍵暗号UOVの安全性評価
  - ・・・

☆6　CRYPTREC活動

- CRYPTRECとは
- Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。

NICTの具体的な実施内容

◆　NICTはIPA（独立行政法人情報処理推進機構）と共同で
暗号技術評価委員会、暗号技術活用委員会
の事務局として、両委員会を運営する。

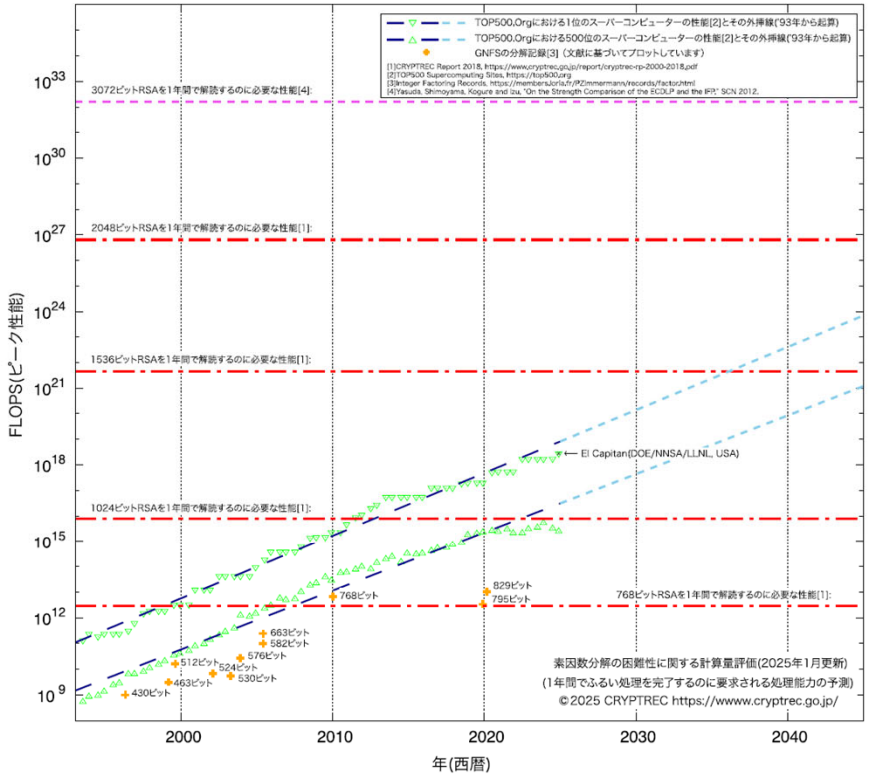
◆詳細

- CRYPTREC暗号リストに掲載されている暗号の監視
- 新規暗号の追加に係る検討
- 新技術等に関する調査及び評価
- CRYPTRECレポートとして活動を報告
https://www.cryptrec.go.jp/eval_cmte.html

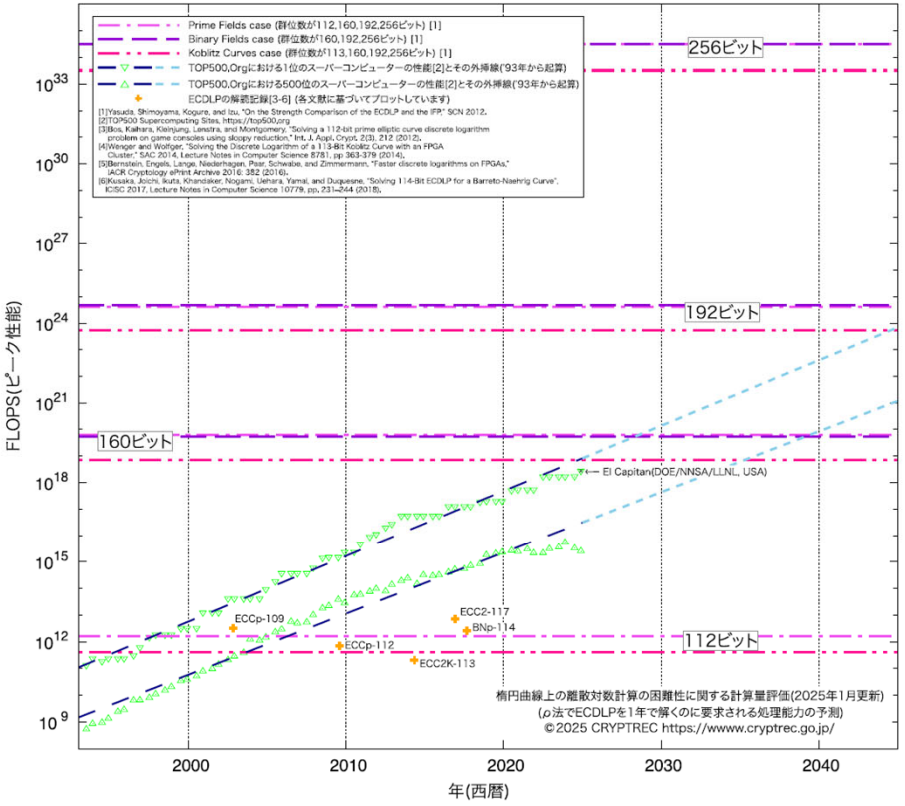
☆7　現代暗号の安全性評価例

SECURITY FUNDAMENTALS Laboratory

RSA等の脆弱性予測に利用



ECDSA等の脆弱性予測に利用



素因数分解の困難性に関する計算量評価

楕円曲線上の離散対数計算に関する計算量評価

☆8　耐量子計算機暗号のエトセトラ

サイバーセキュリティシンポジウム2026

☆8-1　耐量子計算機暗号の安全性評価

☆8-2　そもそもPQCがなぜ騒がれるか

さらに

→ 何が必要だと思いますか？

☆8-3　量子コンピュータの性能はどう？

☆8-1 耐量子計算機暗号の安全性評価

- 耐量子計算機暗号（PQC: Post Quantum Cryptography） の詳細について調査し
  - 調査報告書（2018年度、2022年度、2024年度）
  - ガイドライン（2022年度、2024年度）

  としてCRYPTRECのHPより公開

  https://www.cryptrec.go.jp/tech_reports.html

  https://www.cryptrec.go.jp/tech_guidelines.html

- NISTで標準化されたFIPS-203, 204, 205について
  - 安全性評価
  - 実装性能評価

  関連の活動を開始

☆8-2 そもそもPQCがなぜ騒がれるか

- 量子コンピュータの特性
  - 周期的な構造を発見することが得意
  - Shorが素因数分解や、離散対数問題を効率的に求解することに利用できるアルゴリズム、いわゆる　Shorのアルゴリズム　を開発
- CRYPTREC暗号リストに掲載されている公開鍵暗号方式は、すべて、素因数分解問題、もしくは、離散対数問題にその安全性の根拠を置いている。

＝　量子コンピュータができたら、現在の公開鍵暗号は脆弱化する。

→　PQCを作らなければいけない。

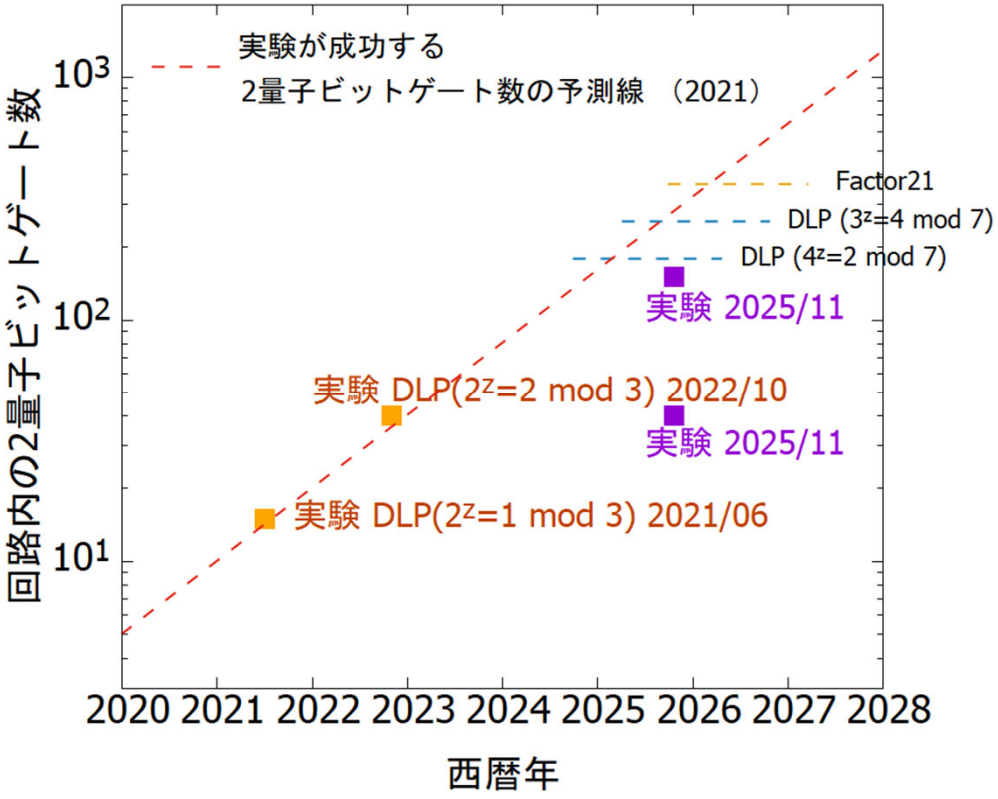
→　世界で使える標準的なPQC方式が必要。

☆8-3 量子コンピュータの性能はどう？

情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員　青野良範

☆8-3 量子コンピュータの性能はどう？

- 量子コンピュータの性能：実装し、試してみました。



実験結果プロット

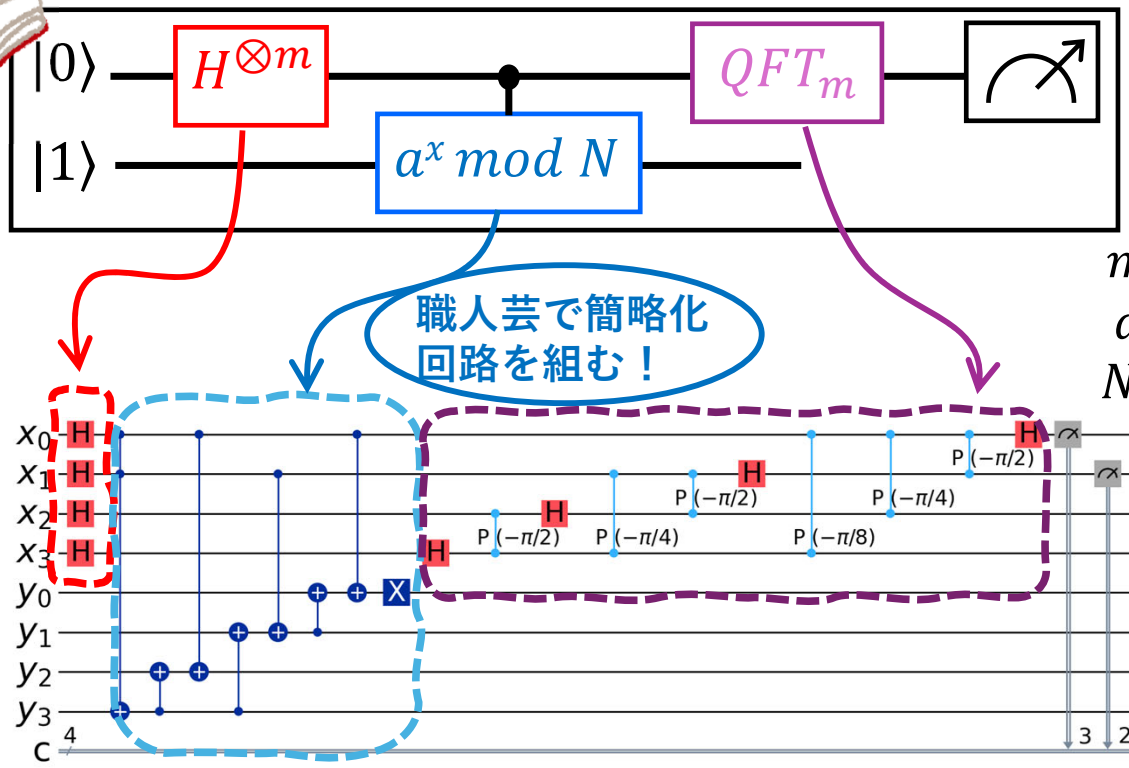
- ■：2021/06,2022/10の実験
  - 離散対数問題
- ■：2025/11の実験
  - 15の素因数分解
  - 離散対数問題

評価を継続
- 現代の公開鍵暗号等の危殆化予測に利用する

☆8-3 15の素因数分解

- 使用した量子コンピュータ ibm_kawasaki@神奈川県川崎市

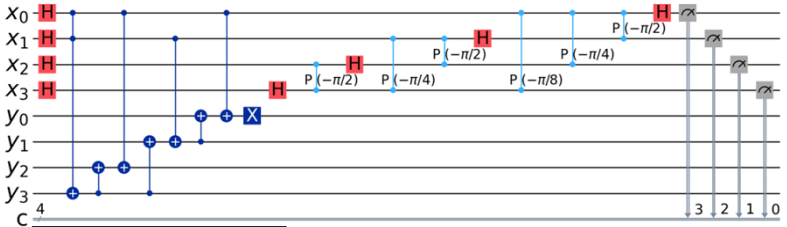
- 教科書に載っているShorの回路



$m = 4$:15のビット数
$a = 2$:職人により選択されたパラメータ
$N = 15$: 素因数分解する数値

論理ゲート数　4　＋　8　＋　10　＝22

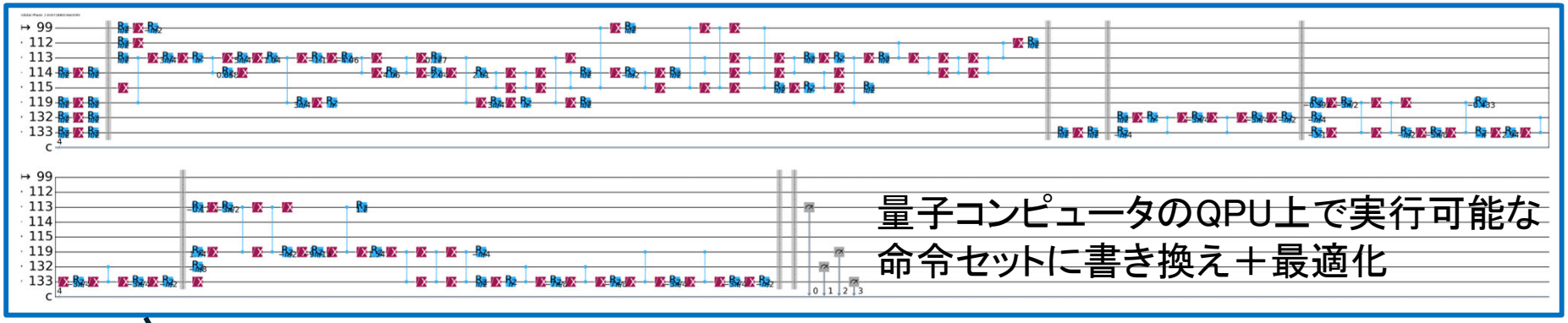
☆8-3 15の素因数分解



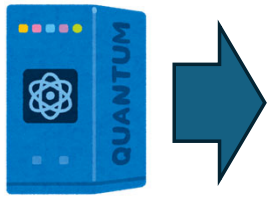
論理量子ゲートによる回路
⇔プログラミングのソースコードに対応

Transpile in laptop

Python命令：
from qiskit.transpiler import generate_preset_pass_manager
generatae_preset_pass_manager(backend=backend, optimization_level=3)



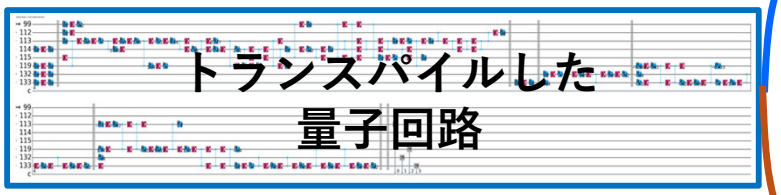
量子コンピュータのQPU上で実行可能な
命令セットに書き換え＋最適化



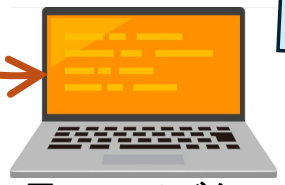
測定結果のビット列が出力される

論理ゲート数154
２ビットゲート数40

☆8-3 実機とシミュレーションの比較

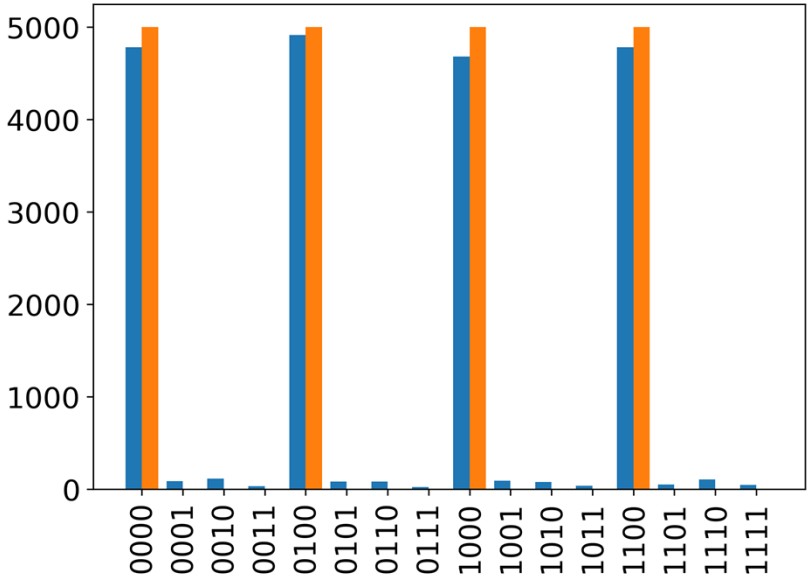


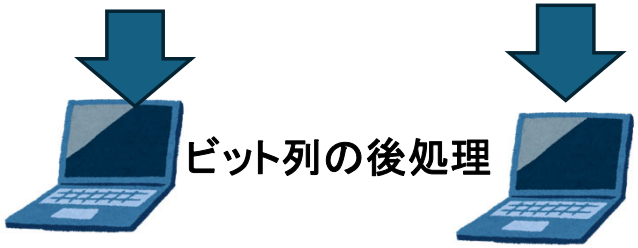
量子コンピュータ



量子ノイズ無し
シミュレーション

ビット列の出力頻度表
（ほとんど誤差がないことに注目！）





ビット列の後処理

素因数分解正解率
$p_{\mathrm{ideal}} = 0.75$

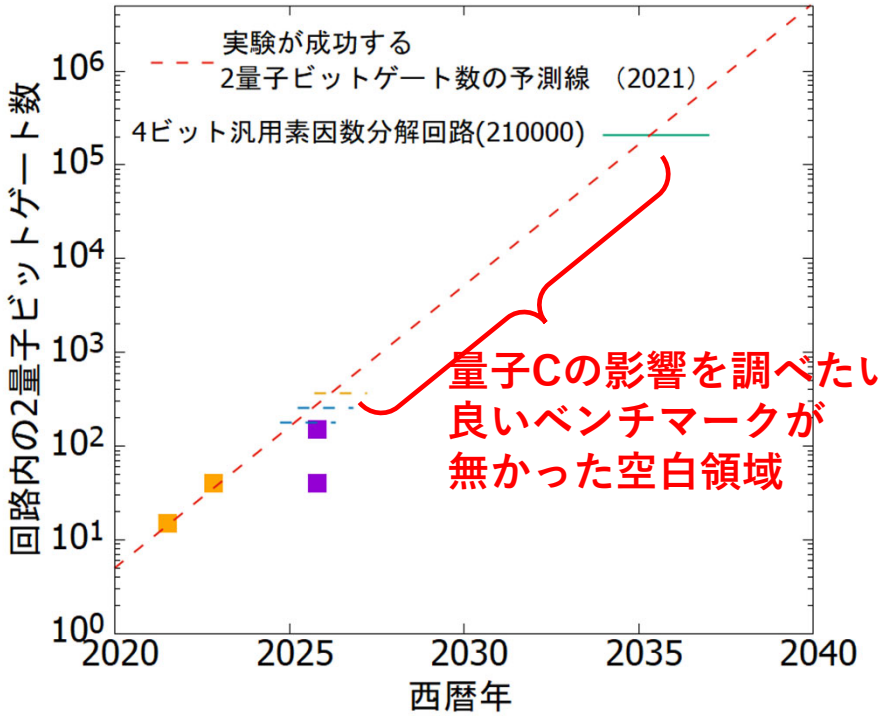
素因数分解正解率
$p_{\mathrm{dev}} = 0.7327$

☆8-3 量子コンピュータ関連研究

- 実験／外部研究結果

★ ibm_kawasakiを用いた実験報告（2025年11月）とプロット

- ○　15の素因数分解（職人が最適化した版）
- △　離散対数問題



- その他

★拡大体$GF(2^n)$上の離散対数問題による
ベンチマーク問題集の提案

- 将来予測のための理論研究の基礎
- 汎用整数演算回路とのギャップを埋める

☆9　今後の計画

2026年度～2030年度計画（第６期中長期）

- まもなく公開予定

☆9　第６期中長期計画

安全なデータ利活用技術

- DeepProtectの医療応用
- 暗号技術の開発

量子コンピュータ時代に向けた暗号技術の安全性評価

- 既存暗号、暗号プロトコル、暗号アプリの安全性評価
- 素因数分解、離散対数問題等の予測図更新
- 量子コンピュータによる演算性能評価

明るいインフラ、明るい世界

暗い暗号
イメージ変わりましたでしょうか。

回答

諸説あります