軽量・高速・耐量子計算機暗号（PQC）対応暗号化ソフトウェア

ハードウェア性能の低いIoT機器でも高速・軽量に動作する暗号・認証ソフトウェア技術により安全な社会へ貢献

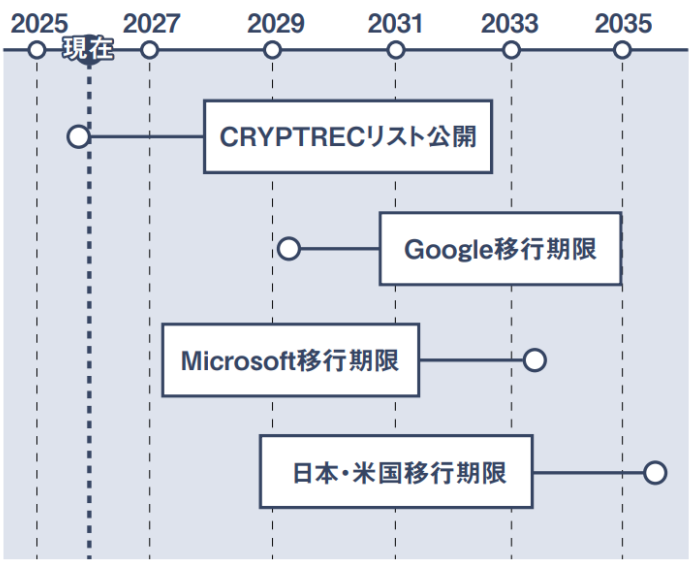
背景・目指す姿

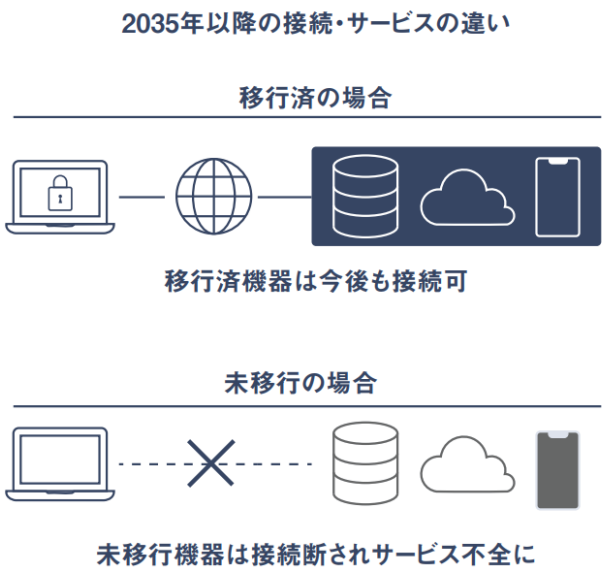
IoTの活用により生産性や利便性の向上が期待されていますが，多種多様な機器がインターネットに繋がることにより，サイバー攻撃の被害増大が懸念されています。サイバー攻撃を防ぐためには、ITだけでなく組み込み機器にも暗号・認証機能を実装することが重要です。

私たちは、軽量・高速でCPU、メモリなどのリソースが限られるIoT機器でも実装可能な、暗号・認証ソフトウェアを開発しています。現在標準化されている従来の暗号アルゴリズムをIoT機器に最適化して展開するとともに、耐量子計算機暗号※（PQC: Post Quantum Cryptography）ソフトウェアの開発も行っています。

各製品への開発を支えた豊富なノウハウを活かし、要望に合わせて必要な暗号アルゴリズムをカプセル化して提供することで、開発リソース効率化、開発期間短縮にも貢献します。

※量子コンピュータでも破れない次世代暗号技術

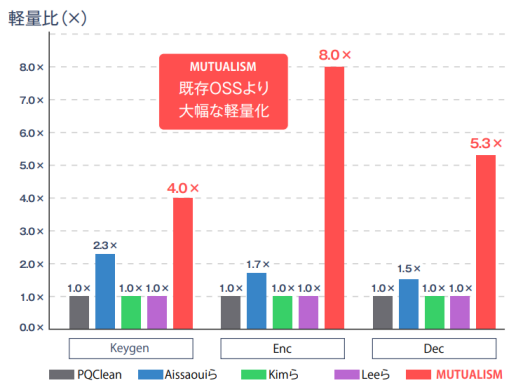




特長

- 世界最小のメモリを実現する独自実装
- 耐量子計算機暗号も対応した暗号化通信の提供
- 組込み向けのセキュア実装で30年の実績

- 軽量・高速
  - 最新規格をIoT機器で実現
  - 最新の政府推奨暗号(EdDSA, AES, SHA3等)をソフトウェアで実現
    - 耐量子計算機暗号(ML-DSA, ML-KEM等)にも対応
    - 脆弱性リスクのあるオープンソース不使用
  - IoT実装可能な軽量・高速な実装
    - 必要メモリ1/10 (OpenSSL比)
    - 高速動作 2~4倍(同上)
    - 低スペックCPUでも動作可能



- 組み込み容易
  - 必要機能をカプセル化
    - お客様ご要望の使用に応じて、必要なアルゴリズム、機能をカプセル化してご提供
    - お客様アプリとAPI接続のみで実装可能
  - 柔軟なカスタマイズ対応可能
    - 各種CPU, OS、メモリ等、様々な実装条件に対応
    - Bluetooth Low Energyなど、IP通信以外の通信方式にも対応
    - OpenSSLの置き換えに対応

- 充実のサポート、搭載実績
  - パナソニック製品での搭載実績
    - 10年以上にわたり、当社IoT機器のセキュリティ開発を支えた実績あり
  - 充実の保守サポート
    - CVE等の脆弱性への対策、更新ライブラリの提供など、製品ライフサイクルにわたる対策も支援可能

ユースケース

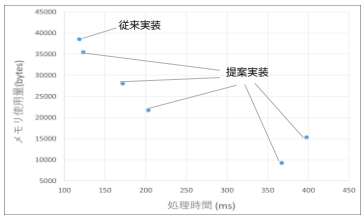
- IoT機器
  メモリやハードウェア容量など資源の限られた機器においても、設計と機能を最適化することで高負荷な暗号技術の導入を実現

コア技術

- 格子ベース暗号におけるメモリの削減

  格子ベース暗号ML-KEM（FIPS203）と ML-DSA（FIPS204）では多数の中間変数が生成されることで負荷が増大しますが、この中間パラメータを逐次生成することでメモリ量を抑えます。

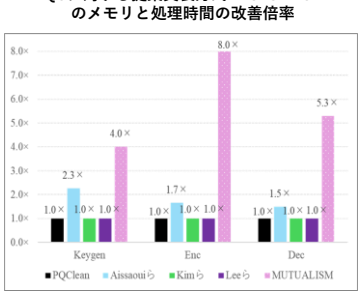
ML-DSAに対する提案実装方式の
メモリ改善結果

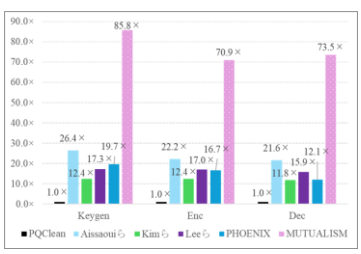


- 符号ベース暗号におけるメモリと処理時間の削減

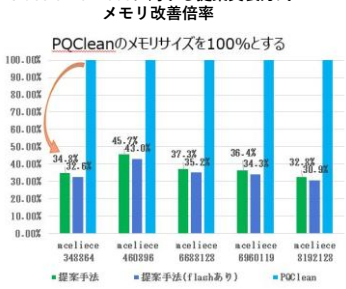
  符号ベース暗号HQCとClassic McElieceでは多項式乗算を含めた誤り訂正の処理が、負荷の大部分を占めます。この処理を新たな乗算方法の提案と関連するメモリの共有化を行いました。これにより、HQCではメモリ量を1/4 から 1/8まで抑え、処理時間を1/70 から 1/85まで抑えます。Classic McElieceではメモリ量を1/3 から1/8 まで抑えます。

HQCに対する提案実装方式”MUTUALISM”
のメモリと処理時間の改善倍率





Classic McElieceに対する提案実装方式の
メモリ改善倍率



関連リンク

- 関連論文

  “Parameterizing Time-Memory Trade-Off for Flexible Implementation of CRYSTALS-Dilithium”, SecITC 2024
  https://link.springer.com/chapter/10.1007/978-3-031-87760-5_14
  2024/11/21
  Yasushi Takahashi, Naohisa Nishida, Yuji Unagami, Saburo Toyonaga, Naoto Yanai, Yasuhiko Ikematsu, Koji Nuida, Masaya Yasuda

  “The Giant Footprint is the Smallest: Low-Footprint Decryption of Classic McEliece”, CSP 2025
  https://ieeexplore.ieee.org/document/11141920
  Cong Liu, Naoto Yanai, Naohisa Nishida, Akira Maruko

  “Giant Footprint Sharing: A Memory-Efficient Decryption Implementation for Classic McEliece”. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 109(3): 271-279
  https://www.jstage.jst.go.jp/article/transfun/E109.A/3/E109.A_2025CIP0010/_article
  2026/03/01
  Cong Liu, Naoto Yanai, Naohisa Nishida, Akira Maruko

  “Parameterizing Time-Memory Trade-off for CRYSTALS-Dilithium and Its Flexible Implementation”, IEICE TRANSACTIONS on Information
  https://www.jstage.jst.go.jp/article/transinf/advpub/0/advpub_2025ICP0007/_article/-char/ja
  2026/06/01
  Yasushi TAKAHASHI, Naohisa NISHIDA, Yuji UNAGAMI, Saburo TOYONAGA, Naoto YANAI, Yasuhiko IKEMATSU, Koji NUIDA, Masaya YASUDA

  “MUTUALISM: Low-Footprint and High-Throughput Software Implementation of HQC for Resource-Constrained Devices”, WiSec 2026 (Accepted.)
  2026/06/30
  Cong Liu, Akira Maruko, Yasushi Takahashi, Naoto Yanai

お問い合わせ窓口

- パナソニック ホールディングス株式会社　DX・CPS本部
  exh.info.phd.dcd@ml.jp.panasonic.com