暗号技術の地殻変動：古典的暗号から耐量子暗号へ

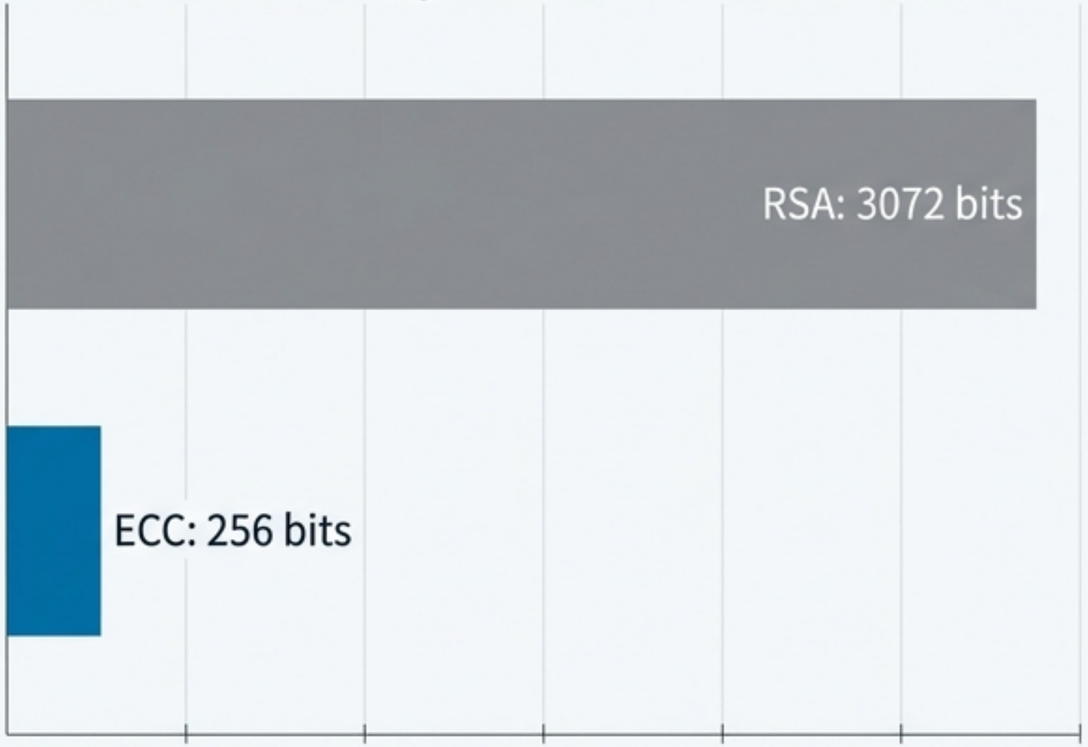
デジタル世界の基盤を再構築する、性能と安全性の新たなトレードオフを理解する

NotebookLM

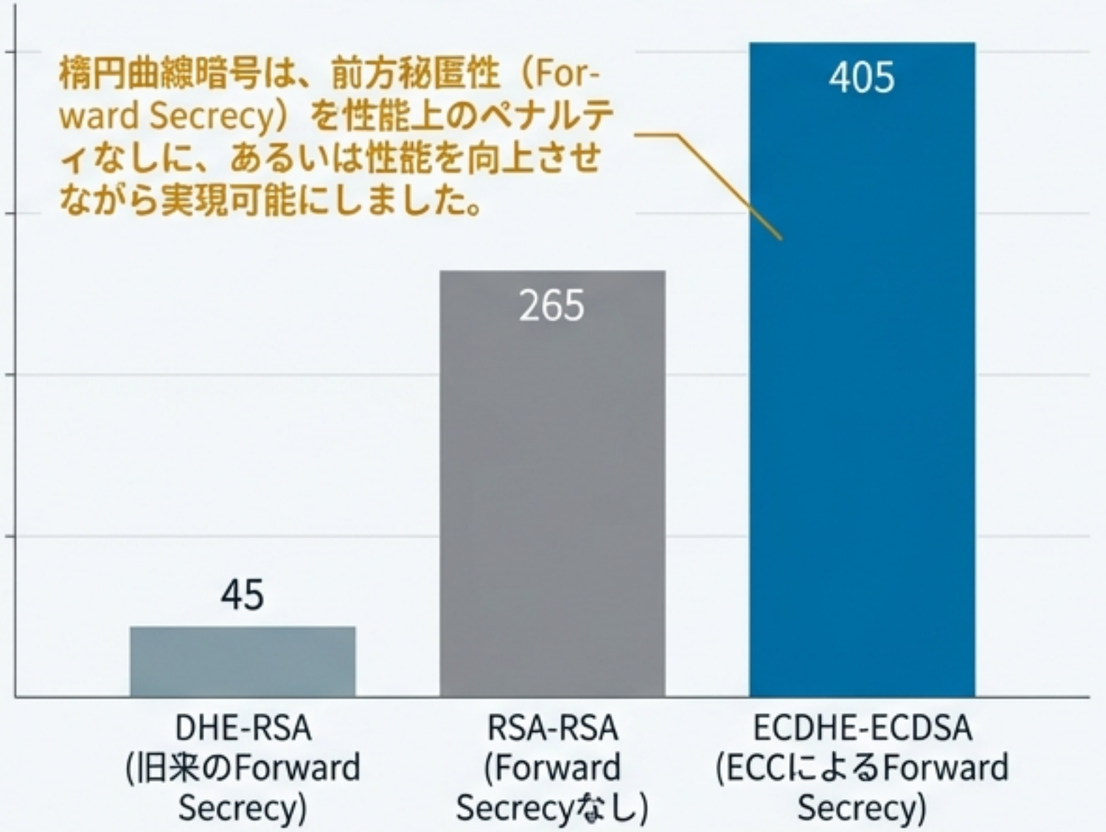
現代の暗号基盤：なぜ世界は楕円曲線暗号(ECC)を選択したのか

ECCは、RSAと同等以上の安全性をはるかに小さな鍵長で実現し、劇的な性能向上をもたらしました。これは、効率性を求めた結果としての最初の大きな地殻変動でした。

セキュリティ対鍵長（Security vs. Key Size）



性能へのインパクト（Performance Impact）



NotebookLM

迫り来る地殻変動：量子の脅威が現在の公開鍵暗号を破壊する

Core Threat: Shor's Algorithm (ショアのアルゴリズム)

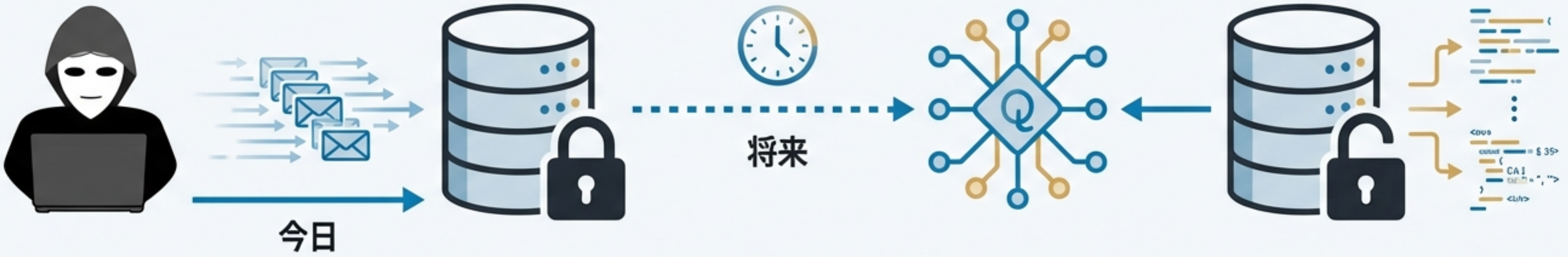
大規模な量子コンピュータは、素因数分解と離散対数問題を多項式時間で解くことができます。
これにより、RSAとECCを含む、現在広く配備されている公開鍵暗号システムの安全性が根底から覆されます。

Immediate Urgency: "Harvest Now, Decrypt Later" Attack

この攻撃シナリオでは、敵対者は今日暗号化されたデータを収集・保存し、将来的に量子コンピュータが利用可能になったた時点で解読します。

長期的な機密性を必要とするデータにとって、量子の脅威は「将来の問題」ではなく「現在のリスク」です。

「今収穫し、後で解読する」攻撃



NotebookLM

新たな基盤の設計図：NISTによる耐量子暗号の標準化プロセス

A Multi-Year Global Effort (数年にわたる世界的な取り組み)

米国国立標準技術研究所(NIST)は、量子コンピュータによる攻撃に耐えうる新しい公開鍵暗号アルゴリズムを標準化するため、2016年に公募を開始しました。
世界中の暗号研究コミュニティが参加し、数ラウンドにわたる厳格な評価と分析が行われました。

Process Timeline & Key Milestones (プロセスのタイムラインと主要マイルストーン)

The Result: A New Foundation (成果：新たな基盤)

2024年8月、NISTは最初の3つの耐量子暗号標準を最終版として公開しました。

FIPS 203
(ML-KEM / Kyber)

FIPS 204
(ML-DSA / Dilithium)

FIPS 205
(SLH-DSA / SPHINCS+)

NotebookLM

新たな標準の主役：CRYSTALS-KyberとDilithium

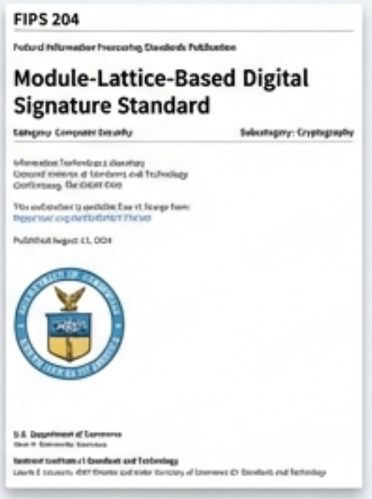
FIPS 203: ML-KEM (CRYSTALS-Kyber)


FIPS 203

Module-Lattice-Based
Key-Encapsulation Mechanism Standard

- **用途:** 鍵カプセル化メカニズム (Key Encapsulation Mechanism - KEM)
- 安全な通信チャネルを確立するための鍵共有に使用されます。(換される統遡 Diffie-Hellman 和 ECDH.)
- **数学的基盤:** Module Learning With Errors (MLWE)
- **主な特徴:** 様々なプラットフォームで良好な性能を発揮します。

FIPS 204: ML-DSA (CRYSTALS-Dilithium)


FIPS 204

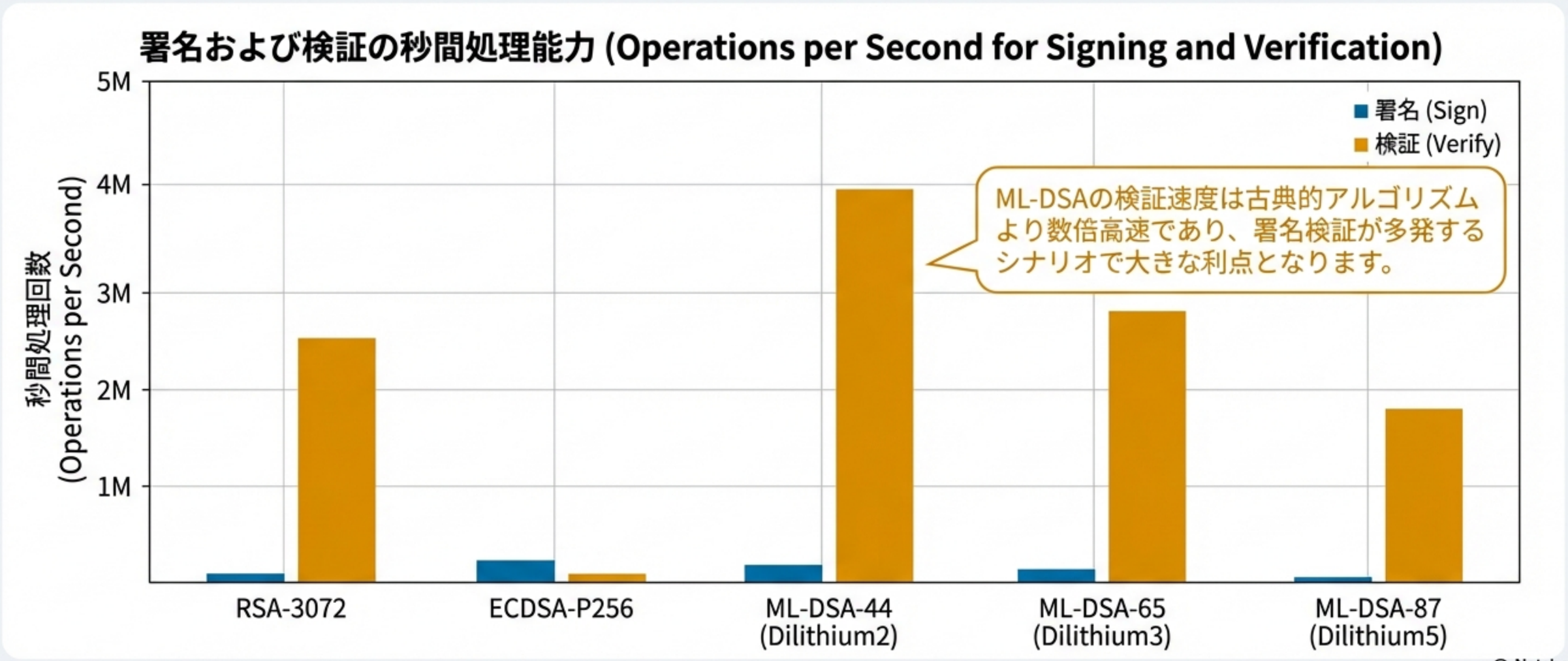
Module-Lattice-Based Digital
Signature Standard

- **用途:** デジタル署名アルゴリズム
- データの完全性と認証を保証するために使用されます。(撰撑される統繙の癈 RSA 和 ECDSA.)
- **数学的基盤:** Fiat-Shamir with Lattices
- **主な特徴:** 良好な性能と、比較的小さな公開鍵・署名サイズを持ち、汎用的なアプリケーションに適しています。

NotebookLM

新たなトレードオフ (1) 速度：PQC署名は驚くほど高速

耐量子性への移行は、必ずしも計算速度の犠牲を意味しません。ML-DSA (Dilithium)は、多くのユースケースでECDSAやRSAを凌駕する性能を示します。

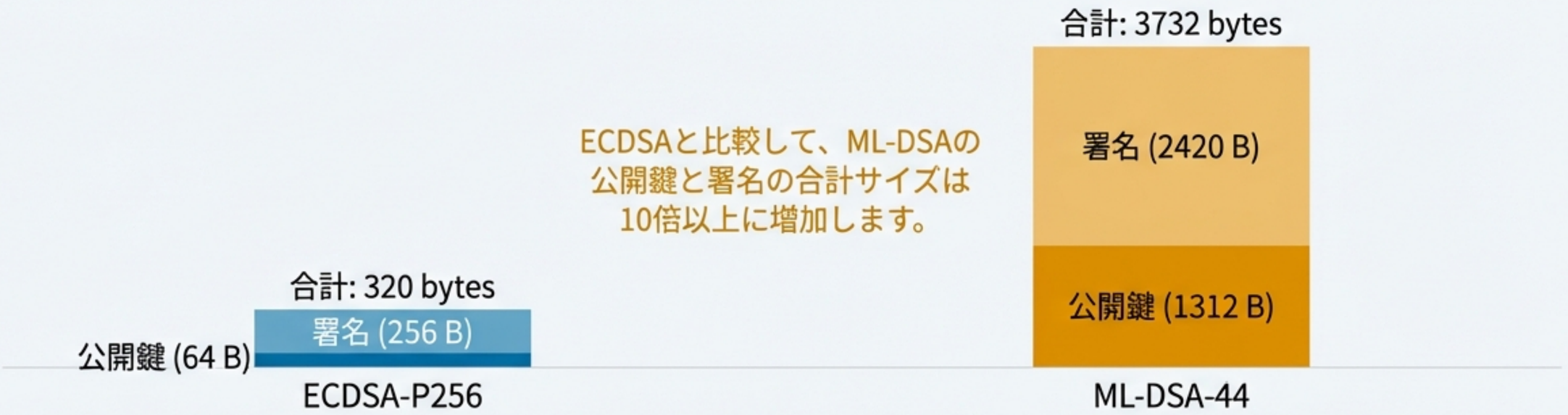


NotebookLM

新たなトレードオフ (2) サイズ：鍵と署名の増大が新たな課題を生む

耐量子暗号の最大のトレードオフは、データサイズの大幅な増加です。これはネットワークプロトコルやストレージに直接的な影響を与えます。

アルゴリズム	セキュリティレベル	公開鍵	署名	合計 (PK + Sig)
ECDSA-P256	Classical-128	64 bytes	256 bytes	**320 bytes**
ML-DSA-44 (Dilithium2)	PQC Category 2	1312 bytes	2420 bytes	**3732 bytes**
比較		**～20倍 (x20)**	**～9.5倍 (x9.5)**	**～11.5倍 (x11.5)**

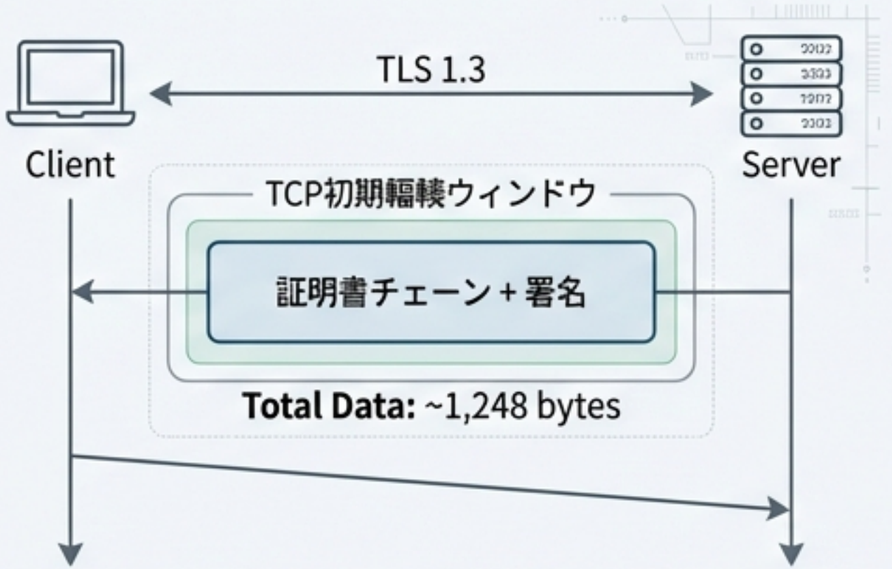


NotebookLM

プロトコルへの影響：PQCがTLSハンドシェイクをどう変えるか

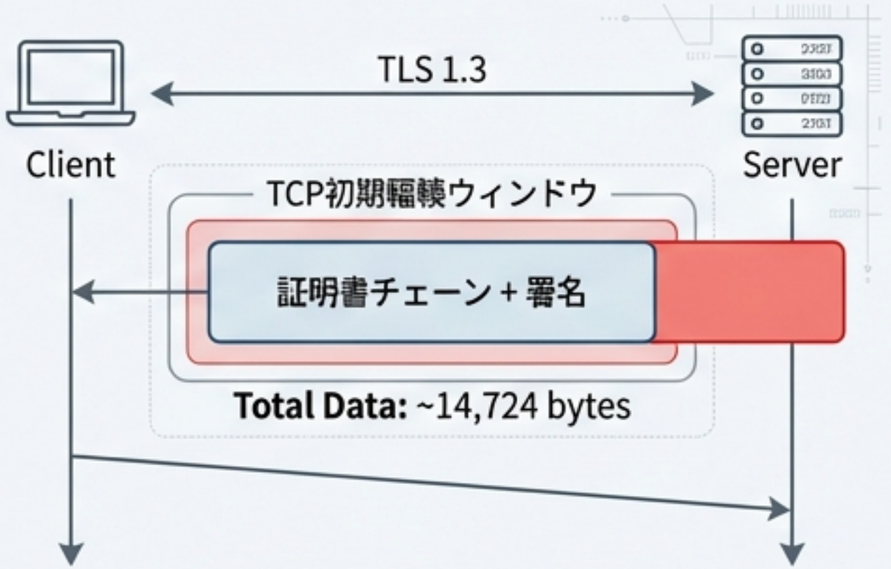
PQCの鍵と証明書のサイズは、TLSのようなレイテンシに敏感なプロトコルに直接影響を与え、コネクション確立を遅延させる可能性があります。

Classical Handshake (ECDSA)



TCP初期輻輳ウィンドウ (~14,600 bytes) 内に収まる
(Fits within the TCP Initial Congestion Window)

PQC Handshake (ML-DSA)



TCP初期輻輳ウィンドウを超える
(Exceeds the TCP Initial Congestion Window)

この超過により、ハンドシェイクを完了するためにもう1回のネットワークラウンドトリップ(RTT)が必要となり、ウェブページの読み込みが遅くなる可能性があります。

NotebookLM

未来への道筋：暗号アジリティを確保し、段階的な移行を計画する

The Mandate (政府の方針)

> 米国国家安全保障覚書(NSM-10)より：「量子リスクの大部分を2035年までに実現可能な限り緩和することを目標とする。」


MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

移行ロードマップ (Migration Roadmap)

1. インベントリ作成 (Create Inventory)
Identify all systems and applications using quantum-vulnerable cryptography.

2. 優先順位付け (Prioritize)
Assess risk based on data sensitivity and system criticality.

3. 計画と準備 (Plan & Prepare)
Develop a migration strategy, engage vendors, and test new algorithms.

4. 移行と検証 (Migrate & Validate)
Transition systems, potentially using hybrid schemes as a bridge, and validate their operation.

戦略的目標：暗号アジリティ

「プロトコル、アプリケーション、ソフトウェア、ハードウェア、インフラ内で、暗号スキームを置き換え、適応させるために必要な能力」

暗号アジリティは、将来の暗号移行を迅速かつ低コストで実現するための鍵となります。

NotebookLM

暗号の地殻変動は既に始まっている。
課題はもはや理論ではなく、実装にある。

- 我々は、量子コンピュータの脅威からデジタル資産を保護するために、不可欠な暗号移行に直面しています。
- 新たなNIST標準は、驚くべき計算性能を提供しますが、その代償としてデータサイズが大幅に増加します。
- この新しいトレードオフは、プロトコルの最適化、インフラの更新、そしてアプリケーションの再設計を要求する、新たなエンジニアリング上の課題を提起します。

標準はここにあり、移行のタイムラインは設定されています。
今こそ、自組織の暗号インベントリを把握し、移行計画を開始する時です。

NotebookLM