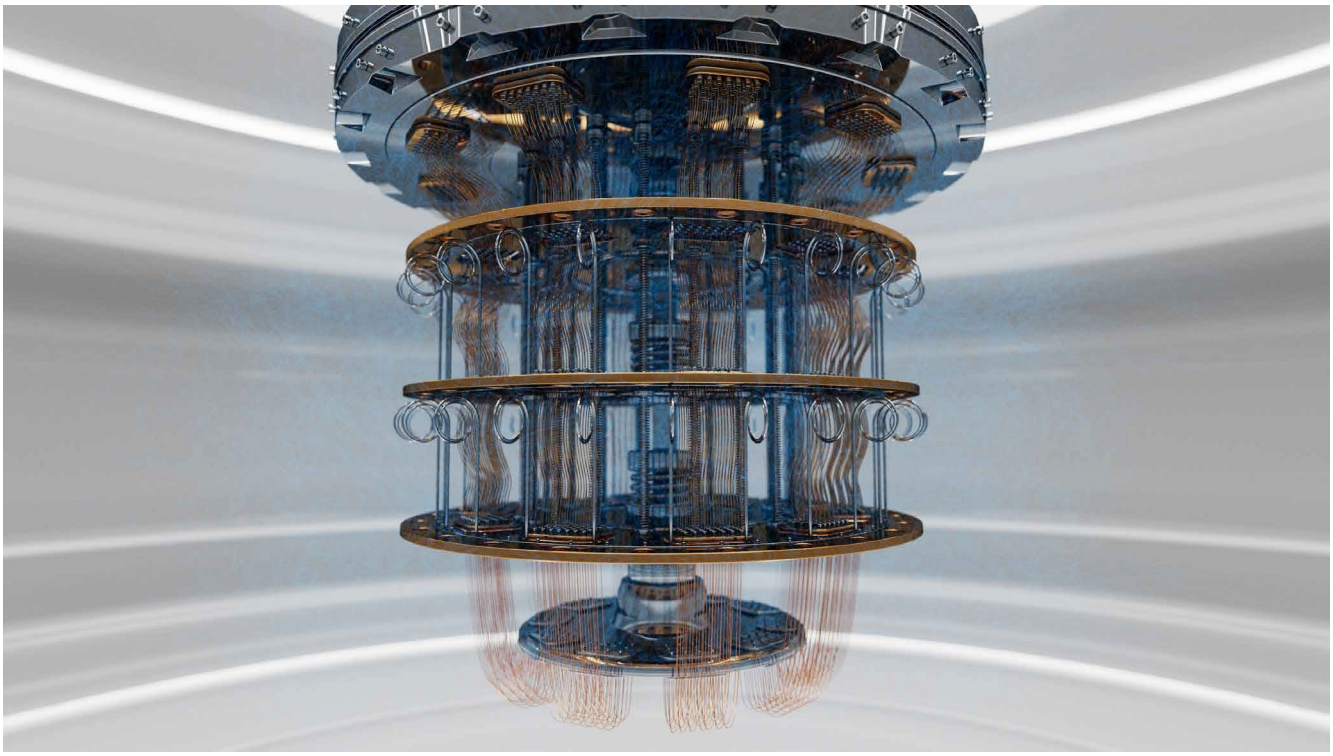
ポスト量子暗号への移行に向けた組込みデバイスの課題

NXPポスト量子暗号チーム



目次

ホワイト・ペーパー
ポスト量子暗号

概要

デジタル・ランドスケープの進化に伴い、量子コンピューティングの実用化への期待から、特に暗号化の分野において機会と課題の両方が提示されています。従来型コンピュータからの攻撃に耐えられるよう設計された従来の暗号化アルゴリズムは、強力な量子コンピューティングの前では脆弱化する可能性があります。現在のテクノロジ領域に不可欠な要素となっている組込みデバイスは、ポスト量子暗号（Post-Quantum Cryptography: PQC）ソリューションの導入にあたり、特別な移行上の課題に直面しています。

このホワイト・ペーパーでは、組込みデバイスへのPQCの実装に向けた移行上の課題について解説します。具体的には、演算能力、メモリ、消費エネルギーなどのリソースに制約があるという、組込みデバイスに固有の性質によって課される制限について見ていきます。さらに、今後登場するPQC標準のほか、耐量子アルゴリズムへの移行に関連する統合上の複雑さや性能面のトレードオフについても検討します。主な検討事項には、サイドチャネル攻撃やフォルト攻撃に対するセキュリティ保証を維持しながら演算オーバーヘッドを最小限に抑える、メモリを意識した効率的な実装のニーズも含まれます。これにより、リソースに制約のあるデバイスに向けた専用ハードウェア・ソリューションのニーズが明確になります。

組込みデバイスでのポスト量子暗号への移行を最終的に成功させるには、暗号研究、ハードウェア設計、ソフトウェア開発、システム統合を含む、多分野にわたるアプローチが必要になります。NXPは、これらの課題に先回りして対処することで、量子コンピューティングがもたらす新たな脅威に対し、組込みシステムのレジリエンスを確保するための道を切り開いています。

デジタル社会でのセキュリティ

コンピュータが日常生活に欠かせないものとなった世の中で、何世代にもわたる人々が育ってきました。この現代において、サイバーセキュリティは信頼を築くための重要な土台の1つです。セキュリティは、当たり前の機能と思われがちです。高度暗号化標準（Advanced Encryption Standard: AES）[(1)]などの、いわゆる対称鍵アルゴリズムは、暗号化にも復号化にも同じ鍵を使用する手法で、通常はデータを効率的に暗号化するために使用されます。一方、公開鍵アルゴリズムは公開鍵と秘密鍵で構成され、対称鍵の交換やデジタル署名の生成に使用できます。現在利用されている公開鍵アルゴリズムの例としては、RSA（名前の由来は発明者のRon Rivest、Adi Shamir、Leonard Adleman）と楕円曲線暗号（Elliptic Curve Cryptography: ECC）[(2)]が挙げられます。あまり知られていないかもしれませんが、誰もがこれらの暗号化標準を1日に数十回、多ければ数百回も使用して、インターネットの閲覧、オンライン決済、キャッシュカード決済を行ったり、スマートフォンで好きなメッセージング・アプリからメッセージを送信したりしています。

コンピューティングの新たな枠組み

一方で、量子コンピューティングの実用化の見込みは、コンピューティングとセキュリティの原則に根本的な変化をもたらすきっかけになります。量子コンピュータは、重ね合わせやもつれなどの量子力学特性を利用し、量子ゲートによって量子ビット（いわゆる「Qubit」）を操作します。Qubitの利用は、1998年に行われた2つの物理Qubitで動作する量子アルゴリズム[(3)]の最初の実験から、2023年12月にIBMによって実証された1,121個のQubitの使用例[(4)]に至るまで、緩やかながら着実な進歩を遂げています。しかし、Qubitの使用量の推移は、この話の前置きにすぎません。現在の研究の重点は、高レート量子誤り訂正の実現という目標へと移っています。IBMのロードマップには、2020年代末までに「200個のQubitによって1億個のゲートを実行できる量子システム」を実現するという見込みが示されています[(5)]。

そうした商業上の予測が、リスク評価に使用できる政府のガイドラインでも支持されています。たとえば、ドイツ連邦情報技術安全局（German Federal Office for Information Information Security: BSI）は、「2030年代初めに暗号関連量子コンピュータが利用可能になる」と予想しています[(6)]。大型で安定した汎用量子コンピュータには、製造可能な最強のスーパーコンピュータでも手に負えない、複雑な計算を実行できる見込みがあります。このような汎用量子コンピュータは、材料科学や製薬といった現在は難易度の高い多くの分野で、より迅速にソリューションを見つけられる可能性を秘めています。ただし、それ以外に、現在利用しているセキュリティ・ソリューションの基盤を揺るがすような、あまり前向きではない影響も生じます。

1994年まで遡ると、マサチューセッツ工科大学（Massachusetts Institute of Technology: MIT）のPeter Shor[(7)]が、現在使用されている大部分の公開鍵暗号システムのセキュリティを弱体化させる量子アルゴリズムを発表しています。また、1996年にコンピュータ・サイエンティストのLov Grover[(8)]によって開発された量子アルゴリズムは、対称暗号とハッシュ関数によるセキュリティに大きな影響を及ぼす可能性があります。つまり、現在使用されている暗号鍵や現在暗号化されているデータは、量子コンピュータが現実のものになれば、いつでも侵害される可能性があるということです。

ポスト量子暗号

現存する量子コンピューティング・デバイスはわずかですが、イノベーションは急速に進んでいます。社会への大規模な影響という潜在的脅威を受け、量子コンピュータを使用した攻撃に対する安全性が期待される、新しい暗号化アルゴリズムや標準の開発への取り組みが、広範囲に展開されています。

考えられる今後の道筋の1つが、量子力学の原則に基づいて暗号化手法と暗号化プロトコルを構築することです。この場合、必ずしも量子コンピュータの使用を考慮する必要はありません（QKDに関する補足記事を参照）。

もう1つの道筋は、「耐量子暗号」や「ポスト量子暗号(PQC)」と総称されている手法です。PQCでは、従来型コンピュータと量子コンピュータの両方の攻撃に耐えられるセキュリティ・ソリューションの構築を試みますが、これに量子対応のデバイスは必要ありません。PQCは、現在の世の中ですでに利用されている、すべてのコンピュータ、IoTデバイス、スマートカードで実行できるよう設計されています。

最初のPQC標準

2016年には、「暗号の終末」の可能性に備えるとともに、世界中の特に優秀な開発者に安全かつ効率的なPQCソリューションのための標準の開発を促す目的で、米国国立標準技術研究所（National Institute of Standards and Technology: NIST）が提案公募を実施しました。その約1年後、鍵交換とデジタル署名を可能にする鍵カプセル化メカニズム（Key Encapsulation Mechanism: KEM）という暗号化機能について、69件の「完全かつ適切」な提案が寄せられました。そのうち6件のKEM提案に、NXPのセキュリティ・エキスパートが共著者として含まれていました。

量子鍵配送 (QKD)

量子メカニズムの構成要素を使用したプロトコルとして最も有力な例の1つが、量子鍵配送（Quantum Key Distribution: QKD）です。QKDでは、光ファイバー・リンク上で光子などの量子粒子を交換することにより、2者間に証明可能安全性を有したリンクが確立されます。このような「量子暗号」は、既存の手法に新たな防御層をもたらす可能性があります。ただし、EUのさまざまな政府機関が結論付けたとおり、「現在の固有の制限により、QKDは現時点でいくつかの特定分野のユース・ケースにのみ実際に使用できます。現時点で従来の鍵合意方式が使用されている大部分のユース・ケースには、QKDを実際に使用することはできません。さらに、セキュリティの観点から見て、QKDはまだ十分に成熟していません」[9]。

3回にわたる選考の末、69件の提案は2020年の時点で15件まで絞られました。最後まで残った15件には、NXPが関与する6件の提案のうち5件が含まれていました。2022年7月、約6年にわたる選考プロセスの最後に、NISTはポスト量子暗号の標準化の取り組みにおける最初の勝者を発表しました。NXPが共著者となったCRYSTALS-Kyber案が、同コンペのKEM部門で唯一の勝者となり、ML-KEMという名称で標準化される予定です。ML-KEMは格子ベースの提案であり、その優れた性能、扱いやすい鍵サイズ、およびNISTが信頼する持続的なセキュリティ能力を理由に選ばれました[10]。以下の表にまとめられているとおり、この成果の一環として3つのPQC署名アルゴリズムが標準化される予定です。3つ目のPQC署名アルゴリズムのFALCON（FN-DSAとして標準化される予定）は、NISTが今後リリースする予定であるため、表には記載されていません。

Type	Submission name	Standard name	Standard document
Key Encapsulation Mechanism (KEM)	CRYSTALS-Kyber	ML-KEM	FIPS-203: Module-Lattice-Based Key-Encapsulation Mechanism Standard[10]
Digital signature	CRYSTALS-Dilithium	ML-DSA	FIPS-204: Module-Lattice-Based Digital Signature Standard[11]
Digital signature	SPHINCS+	SLH-DSA	FIPS-205: Stateless Hash-Based Digital Signature Standard[12]

2024年のNISTによる最初のPQC標準の発表をもって、この取り組みの初期段階は終わりを告げ、新たな拡大フェーズへと突入しています。国際標準化機構（International Organization for Standardization: ISO）はアルゴリズム・リストの拡張の評価を進めており、韓国は独自のPQCアルゴリズムを標準化する予定です[13]。中国を含むその他の国も、同様の措置を取ることが予想されます。

PQC署名のポートフォリオを多様化させるために、NISTは最近になって追加の提案公募を実施しました。第2回の候補は、2024年中に発表される見込みです[14]。これらは、いずれもアルゴリズム・レベルでの取り組みですが、必要な取り組みは他にもあります。さまざまなユース・ケース向けのプロトコル標準を更新することが必要になるでしょう。これらの多様な取り組みが、量子による脅威に対抗できる環境への、大規模な移行の出発点となります。

今後登場するFIPS標準は、初めて標準化されるPQCアルゴリズムではありません。NIST SP 800-208[15]には、2つのステートフルなハッシュベースの署名方式、Leighton-Micali署名（Leighton-Micali Signatures: LMS）と拡張マークル署名方式（eXtended Merkle Signature Scheme: XMSS）のためのパラメータ・セットが定義されています。LMSとXMSSはステートフルであるため、署名を作成するエンティティが状態の維持と同期を行う必要があります。そのため、ファームウェア/ソフトウェア署名のユース・ケースに、より適した署名方式となっています。

ポスト量子暗号への移行

PQCへのデバイスとシステムの移行には、応用研究、エンジニアリング、標準化への多大な取り組みが必要です。最近の量子コンピューティング分野における進歩と、このように大規模な移行に要する時間を考慮すると、今すぐPQCへの移行準備を始めることが極めて重要になります。

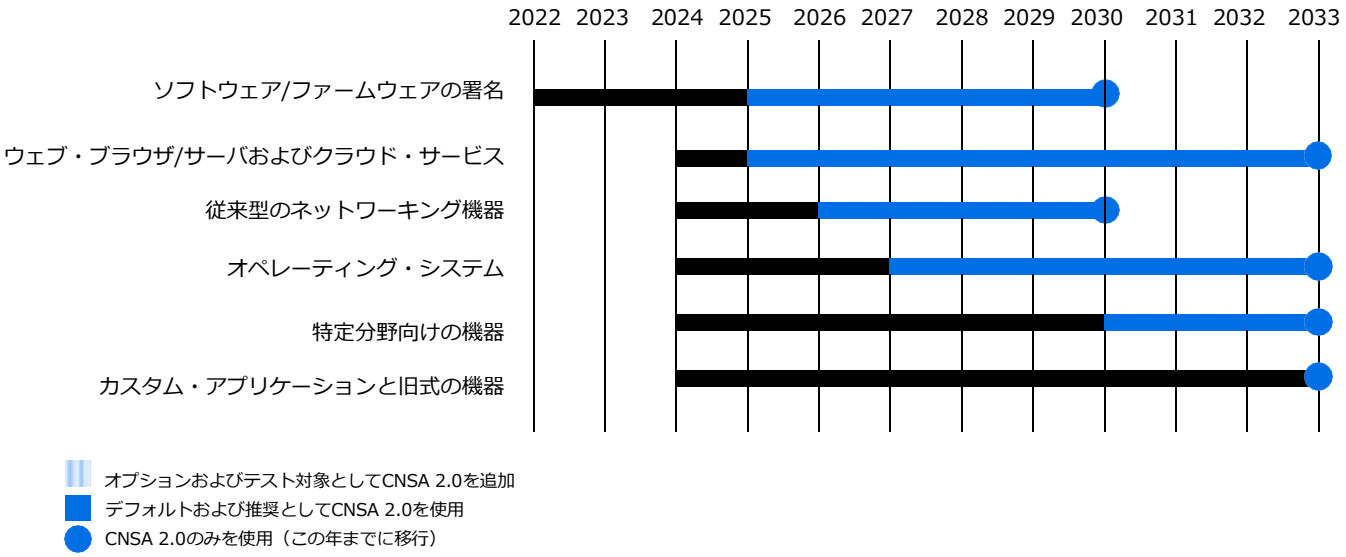
対処すべき主な課題は2つあります。第一に、機密性を保護する必要があります。つまり、今後転送されるデータは耐量子アルゴリズムによって保護し、将来の復号化、つまりは「Store now, decrypt later（保存しておいて後で復号）」と呼ばれる攻撃を防ぐことが必要です。第二に、耐量子認証を使用する必要があります。これを使用すれば、将来の攻撃者がシステムに不正にアクセスして、ファームウェアを変更したり置き換えたりすることはできなくなります。これら2種類の耐量子セキュリティ・メカニズムを導入しておかないと、将来開始される暗号関連量子コンピュータ (CRQC) を使用した量子攻撃のリスクに、データやデバイスがさらされることになります。

組込み分野では、現在利用されている多くのデバイスが長い寿命を有しているため、データを保持、処理、交換するデバイスについての検討も必要になります。デバイスのメーカーは、今後施行されるサイバー・レジリエンス法案 (CRA)[16]などの法律に従い、そのようなデバイスの信頼性と安全性を、デバイスの寿命全体を通して確保する必要があります。デバイスで実行されるファームウェアは信頼できるものであることが必要で、それはファームウェアやソフトウェアに適用される更新についても同様です。通常はデジタル署名を使用して、セキュア・ブート動作中にファームウェアが純正かどうかをチェックしたり、信頼できるソースから安全な更新プログラムを受信しているかどうかをチェックしたりします。このような署名は、ソフトウェアが悪意のある第三者によって変更されていないか確認することにより、完全性の保護にも役立ちます。将来の攻撃者がCRQCを使用して従来型のデジタル署名を偽造できた場合、その攻撃者は独自のソフトウェアをロードすることでデバイスを制御できるため、結果としてセキュリティと安全性の問題が生じます。このような理由から、デジタル署名のセキュアな実装は、一部のステークホルダーにとっては鍵の確立や「Store now, decrypt later」の脅威と同様、あるいはそれ以上に重要なものとなります。

移行にあたっては、最も貴重な資産の保護やデバイスのセキュリティの補強に使用される暗号の移行を最優先に位置付けながら、エコシステムのメンバーにとってのリスクが反映されるような移行方法を採用することも必要です。各国の機関や国際機関は移行の義務化に向けた戦略とスケジュールの策定を進めており、複数の市場に事業を展開しているステークホルダーにとっては要件の競合につながる可能性があります。米国の国家安全保障システム（National Security Systems: NSS）とそれに関連する資産の場合、商用国家安全保障アルゴリズム・スイート（Commercial National Security Algorithm Suite: CNSA）2.0には、連邦情報処理標準（Federal Information Processing Standards: FIPS）の認証を取得した製品やデバイスの移行のカットオフ・ポイントに対して、厳格な制限が設けられています[17]。

その他の機関も同様のスケジュールを定めていますが、アルゴリズムの優先傾向がわずかに異なります。たとえば、ANSSI（フランス）とBSI（ドイツ）は、NIST　PQC標準のサポートを重視してきましたが、標準化済みPQCアルゴリズムのリストを拡大することにも関心を示しています。

米国国家安全保障システム (NSS) の要件に対するCNSA 2.0のスケジュール



移行に向けた組込みデバイスの課題

システムやアプリケーションを安全な方法で更新するのは、簡単なことではありません。ソフトウェア・ソリューションにも同じことが言えますが、特定のハードウェア・アクセラレーションに依存するシステムの場合は、はるかに困難になります。性能に影響が及んだり、移行が相互運用性に作用したりする可能性があるほか、サービスの継続性が失われることもあります。リソースに制約のある組込みデバイスの場合、影響はさらに大きくなります。追加のメモリを頻繁に割り当てることができるサーバとは異なり、制約のあるデバイスは限られた容量のメモリしか使用できません。同様に、安全性に優れたクラウド・アプリケーションは、分離されたリモート・マシンで運用されることが多いですが、組込みデバイスの場合は、タイミングやその他のサイドチャネル情報が、悪意のあるエンティティによる悪用から保護される保証はありません。本節では、これらの課題の一部を詳しく説明していきます。

ポスト量子暗号に関するハードウェアの制約

暗号関数用のハードウェア・アクセラレーションは、現在のチップ設計の中核を担っています。

ハードウェア・アクセラレーションは、AESのような対称関数やSHA-2/SHA-3のようなハッシュ関数に使用されるだけでなく、ECCやRSAなどの公開鍵暗号にも使用されます。ハードウェア・アクセラレーションにより、暗号関数や暗号プロトコルの実行が過度に遅くなることを防げるので、性能要件を満たしながらデバイスの安全性を保てます。

ポスト量子暗号向けのハードウェア・アクセラレーションは、まだ初期段階にあります。ハッシュ計算を高速化する暗号化ハードウェアは、ML-DSA、ML-KEM、SLH-DSAなどの方式に再利用できます。ML-DSAとML-KEMでは、それに加えて専用のアクセラレーションを利用できます。専用のPQCハードウェアの設計、開発、生産は、何年にも及ぶことの多い長期的なプロセスです。　NXPのPQCチームは、既存のECC/RSAアクセラレーションをPQC向けに再利用する取り組みを主導してきました(18)。しかし、専用のPQCハードウェア・コプロセッサを実現可能な段階で導入するのが、状況としては理想的です。

ハードウェアに関するもう1つの懸念がメモリです。不揮発性メモリの場合は、暗号鍵のストレージ要件の拡大を考慮に入れる必要があります。たとえばECCの鍵表現に必要なのは、たったの32バイトですが、PQCには桁違いに大きな容量のメモリが必要になる可能性があります。

Scheme	Quantum-Safe?	Public Key (bytes)	Secret Key (bytes)
ECC-256	X	~32	~32
RSA-3072	X	~384	~768
ML-KEM-768	√	1184	*1216
ML-DSA-65	√	1952	4000

* ML-KEMの秘密鍵には、暗号文の復号化に必要な1216バイトが含まれるほか、1184バイトのカプセル化鍵も必要です。公開カプセル化鍵が復号化用の1216バイトとともに保存されない場合、秘密鍵の全長は2400バイトとなります。

しかし、組込みデバイスには、さらに大きな課題があります。それは、ポスト量子暗号に、場合によっては現在の暗号よりも多くの作業メモリ（RAM）と、長期にわたる保存が必要になることです。ECCは数KiBのメモリだけで実装できますが[19]、ML-DSAの高速実装に要するメモリは優に50 KiBに達します[20]。ノートPCやサーバのような、より大型のデバイスの場合、通常は自由に使用できる数ギガバイトのRAMがあるため、この点は問題になりません。しかし、組込みデバイスの場合は話が違います。アクセス・カード、パスポート、センシングに使用されるセキュア・マイクロコントローラには、16 KiBや、さらに少ない8 KiBのRAMしか搭載されていない場合があります。
NXPは、組込みデバイスでのPQCを可能にするソリューションに率先して取り組んでいます。最も見込みのあるアプローチの1つが、PQC方式の低フットプリント実装の研究に関連するものです[21][22]。これらの取り組みは、性能への影響が最小限になるまでメモリ使用量を削減することを目標としています。その他の研究には、一般的なPQCのユース・ケースに対する既存ハードウェアの活用の実現可能性調査[23]があり、すでに移行が可能な領域を示すことを目的としています。

多数の標準

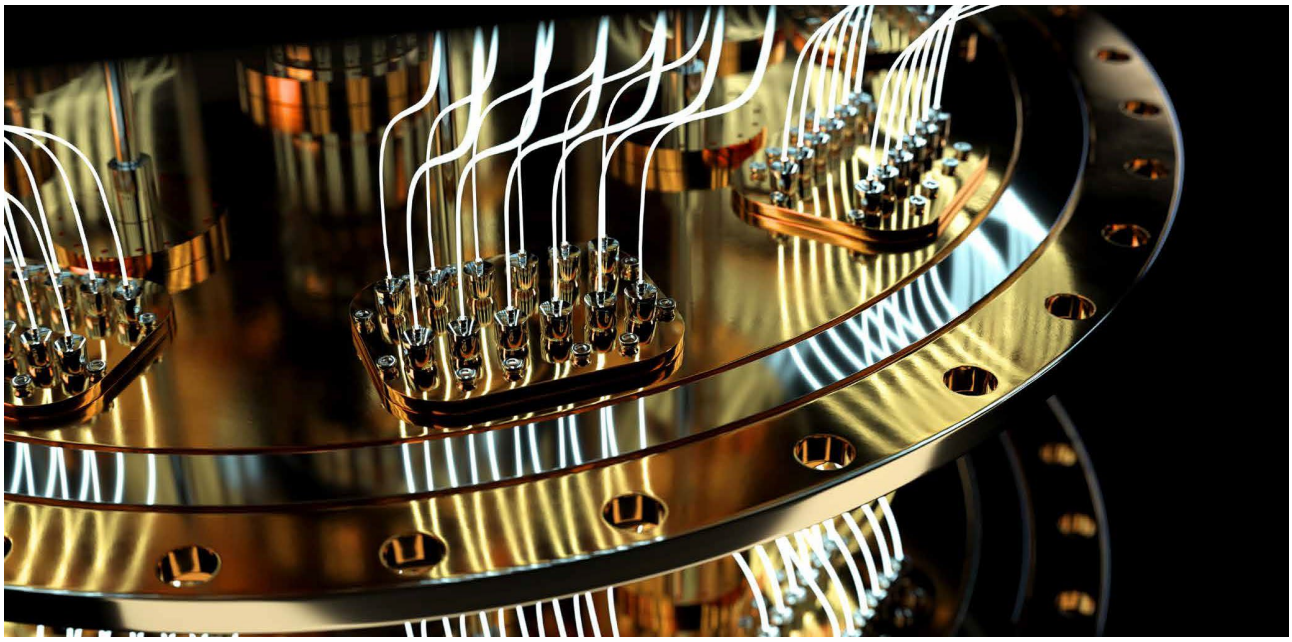
現在の暗号を単一のPQC方式に更新するだけでも、組込みデバイスの（ハードウェア）要件に大きな影響が及ぶことになります。しかし現実には、鍵の確立とデジタル署名に複数のPQC標準で対応することになる可能性が高いため、そのようなデバイスでは、おそらく複数のPQC標準をサポートすることが必要になります。

それだけではありません。組込みデバイスは通常、さまざまなユース・ケースやシナリオ向けに使用されます。ML-DSAの方が適したユース・ケースに使用されるデバイスもあれば、SLH-DSAや、NIST SP 800-208に定義されている、XMSS/LMSなどのステートフルなハッシュベースの方式の方が適したユース・ケースに使用されるデバイスもあります。さらに、これらのデバイスは、NISTから発行されたものとは異なるガイドラインや標準を使用する国で販売される可能性もあります。冒頭で触れたように、ヨーロッパとアジアでは、標準化が見込まれている方式が異なります。さまざまな市場や規制に対応できるような単一のチップを設計するには、鍵を保存するためのストレージ領域をより多く確保し、複数の暗号化アルゴリズムをサポートできるようにコード・サイズを拡大する必要があります。もちろん再利用可能なものもありますが、現在の暗号に比べてアルゴリズム数は大幅に増えます。

この課題は、より上位の標準が存在することで、さらに複雑化します。多くのユース・ケースでは、暗号プリミティブを直接使用せずに、暗号化プロトコルを介して使用します。たとえば、他のデバイスとの通信はトランスポート層セキュリティ（Transport Layer Security: TLS）を使用して行われ、チップ内部の通信は通常、セキュア・チャネル・プロトコル（Secure Channel Protocol: SCP）などの別のプロトコルで保護されます。ベンダー間の相互運用性を確保するために、上位のプロトコルがさまざまな標準化団体によって標準化されています。

PQCへの移行後も相互運用性を維持するには、これらの標準を更新する必要があります。こうしたプロセスは、何年もかかる可能性があることに加え、さまざまな標準化団体が同じアルゴリズムを選択する保証もありません。組込みデバイスで複数の上位プロトコルをサポートしなければならない場合、グローバルにサポートされているKEMと署名のすべてに十分な領域を割り当てられない可能性があります。その場合は、開発者が優先順位を決めなければなりません。

NXPは、こうした課題への対処を支援するために、世界のデジタルおよび組込みインフラストラクチャを保護する標準や、そのプロトコルを標準化しているコンソーシアムに



積極的に貢献しています。その対象は、Connectivity Standards Alliance (CSA)、Global Platform、GSM Association (GSMA)、Internet Engineering Task Force (IETF) など、さまざまです。標準間の統一性をできる限り高めることを推奨し、プロトコルの更新時に組込みを重視した選択をすることにより、できるだけ多くの組込みデバイスで、そのプロトコルを実現可能かつ有効化しやすいものに最大限維持できるよう支援しています。

最後に、以下の節でも解説しますが、今後開発するチップでは、ハードウェア・サポートとソフトウェア・サポート間のトレードオフを適切に考慮する必要があります。設計開始の段階から、セキュリティ、性能、柔軟性のバランスに配慮して設計することが必要です。そうすることで、将来のプロトコル更新が大幅に実装しやすくなります。

物理的な攻撃からの保護

ほとんどのアプリケーションで、セキュリティ・システムのユーザーは入力値を送信して出力値を確認することができますが、暗号化アルゴリズムによって使用される秘密鍵などの内部値についての情報は得られません。

しかし、組込みデバイスなどの物理的なシステムで暗号を実装および導入する場合、そのような想定は、もはや妥当とは言えません[24]。というのも、暗号実装の実行時間など、システムの物理的特性を測定することで、秘密情報を推測できるからです。アルゴリズムの実行時間が秘密鍵の値に依存している場合は、実行時間が変動することがあり、そのタイミングの差によって秘密鍵についての情報が明らかになる可能性があります。デバイスの物理的特性を測定しながら秘密情報を処理するというこのコンセプトは、サイドチャネル分析という用語で形式化されています。このような分析には、タイミング動作に加えて、消費電力や電磁放射などの他の情報源も使用できます。また、フォルト注入攻撃と呼ばれる手法により、暗号化演算を積極的に妨害して機密情報を回収することもできます。

物理的な脅威は、重大かつ現実的な問題です。危険にさらされているシステムに暗号化方式を実装するには、専用の対抗策が必要です。そのような対策を導入すれば、通常はメモリ要件や性能に関して大きなオーバーヘッドが課されることになりますが、攻撃が成功した場合に生じるコストと影響は、それを上回ります。現在の標準化された公開鍵暗号の場合、徐々に強力になる物理的攻撃からの保護を効率的に達成する方法は確立されています。PQCの場合、そのような専用の保護というテーマは、まだ活発に研究されている段階です。

従来型公開鍵暗号の高保証実装の先駆者として、NXPは今後標準化される暗号化方式に適した対抗策の開発と最適化にも貢献しています[25] [26]。NXPには、この分野の主要な学術研究者とともに研究に取り組む暗号およびセキュリティ関連のエキスパートが数多く在籍しています。この取り組みには、幅広い対抗策を確保するための、新たなサイドチャネル攻撃やフォルト攻撃の調査も含まれるため[27] [28]、NXPはこの終わりのない戦いにおいて一歩先を進み続けることができます。

組込みデバイスの更新性

大型デバイスよりも厳しい組込みデバイスのもう1つの制限が、その更新性です。リソースやコネクティビティに制限があるため、一部の組込みデバイスは出荷後に更新することができません。この点は、特にアクセス・トークンなどの制約付きデバイスに当てはまります。さらに、デバイスに更新メカニズムが用意されていたとしても、製造時に組み込まれたハードウェア・アクセラレーション、フラッシュ・メモリ、RAMに限られます。また、更新メカニズム自体が、耐PQではない可能性もあります。その場合、PQCの更新は実現できないかもしれません。これを防ぐには、現在のデバイスでPQCを実行できるようにする必要がありますが、それも前の節で触れた課題によって困難になる可能性があります。

PQCへの移行や、デバイスにすでに実装されている非対称暗号の更新を計画する場合、その意思決定プロセスには多くの情報が投入され、そのプロセスからさまざまな結果が得られます。場合によっては、転送されるデータが比較的短命で価値も低いため、CRQCを所持していたとしても、そのデータを入手するために行う攻撃のコストに見合わない可能性もあります。そのようなユース・ケースは、移行計画では優先度の低いケースと見なされ、攻撃が成功した場合に署名能力が得られるルート証明書など、より無防備な資産に高い優先度が与えられます。攻撃にさらされた場合のリスクが大きいほど、移行計画での優先度が高くなります。

その他には、システムに関与するエンティティの数が限られるケースもあります。そのようなケースでは、（耐PQの）対称鍵の事前共有[29]が、ポスト量子セキュリティにつながる実現可能な道のりになるでしょう。

脅威が現れる前にその影響を軽減するには、以下で解説する暗号の俊敏性と、セキュリティやリスクに関する長期的思考が効果的です。

実用的な移行ソリューション

この節では、さまざまな方法で公開鍵暗号を使用する、PQCへの移行に向けたいくつかのアプローチについて説明します。重要なのは、これらのアプローチをシステム・レベルで検討することです。アルゴリズムとプロトコルは、標準化されて製品やデバイスに組み込まれた後、より広範囲のソリューションと連携することになります。すべてのリンクやエンドポイントは、個々のコンポーネントではなく、システムに対してどのようにセキュリティ特性を付与するかという観点から評価する必要があります。

ハイブリッド・ポスト量子暗号

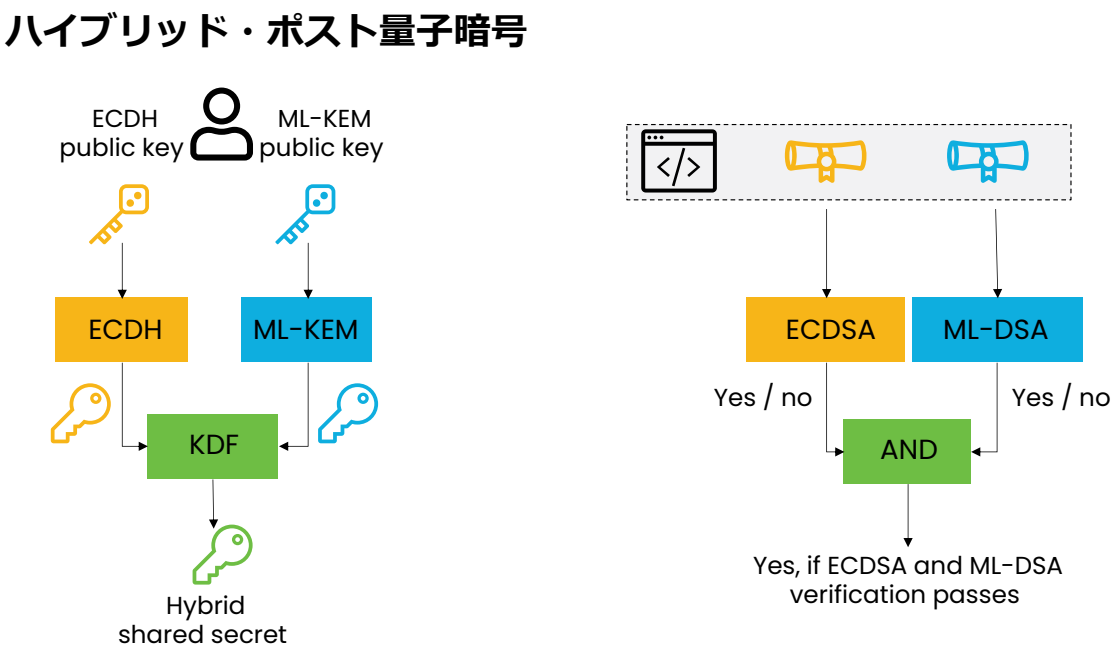
ハイブリッドPQCとは、従来の方式とPQC方式を組み合わせたものです。このアプローチの背景には、従来の方式がCRQCによって侵害されたとしても、PQC方式でセキュリティを確保できるという根拠があります。反対に、CRQCがまだ実用化されていない段階で、PQC方式が予期しない標準的な攻撃によって侵害された場合は、従来の方式でセキュリティを確保できます。ドイツのBSI[30]やフランスのANSSI[31]をはじめ多くの国家機関がハイブリッド・アプローチを推奨しています。従来のアルゴリズムの実行によって生じるオーバーヘッドは、PQCアルゴリズムを実行する場合に比べて、比較的わずかで済みます。そのためハイブリッドPQCは、リスクを分散できる実用的なソリューションとして認識されています。

ハイブリッドPQCは、実際には以下のような方法で実現することになります。

- ML-KEM（または別のPQC KEM）と、楕円曲線ディフィー・ヘルマン（Elliptic-curve Diffie-Hellman: ECDH）などの従来の鍵交換方式の組み合わせは、鍵導出関数（KDF）を使用してML-KEM交換とECDH交換から導出した共有秘密を組み合わせることによって実現します。この結果、両方の方式のセキュリティを組み合わせた共有秘密が得られます。
- ML-DSA（または別のPQC署名方式）と、楕円曲線デジタル署名（Elliptic Curve Digital Signature: ECDSA）やRSA署名などの従来の署名方式の組み合わせは、ML-KEMと従来の鍵交換システムの組み合わせよりもシンプルです。必要なのは、両方の方式でメッセージに署名し、両方の署名を検証者に送信することだけです。検証者が両方の署名を検証し、どちらの署名も有効な場合にのみメッセージを受け入れることが、極めて重要な手順となります。

相互運用性

多くのデバイスやユース・ケースにとってPQCへの移行は必須ですが、セキュリティと性能を維持することも必要です。ただし、移行の重要な側面の1つに、相互運用性の維持があります。相互運用性は、デジタル環境を機能させるのに役立ち、多数のデバイスやアプリケーション間でのシームレスな通信と情報共有を可能にします。相互運用性は、現在は多くの暗号化方式、通信プロトコル、デジタル証明書でサポートされています。主な例がIETFで行われている取り組みで、ML-KEM[32]およびML-DSA[33]向けのアルゴリズム識別子のインターネット・ドラフトや、TLS 1.3[34]でのハイブリッド鍵交換に関する提案などが挙げられます。



ポスト量子暗号への移行に関するコンソーシアム

NXPは、NISTの国立サイバーセキュリティ・センター・オブ・エクセレンス（National Cybersecurity Center of Excellence: NCCoE）によって設立された、Migration to Post-Quantum Cryptographyプロジェクト・コンソーシアムのメンバーです。このコンソーシアムの目標は、ポスト量子アルゴリズムへの移行に伴う問題についての認識を促すとともに、ベンダーやインテグレーター向けのベスト・プラクティスを開発することであり、暗号の発見、相互運用性、暗号の俊敏性に重点が置かれています[34]。

暗号の俊敏性

暗号の俊敏性とは、システムの暗号セキュリティを簡単かつ信頼性と安全性に優れたシンプルな方法で更新できる、すべてのメカニズムや実装手法のことです。そのような変更やアップグレードが行われたことをユーザーに気付かれることさえなく実施するのが理想的です。更新は、従来の方式とPQC方式の両方で将来の攻撃を軽減するのに役立ちます。暗号の俊敏性の対象となるのは、特定の方式から別の方式への移行だけではありません。パラメータ・セットに関する柔軟性のほか、実装の更新や、サイドチャネルまたはフォルト注入攻撃への対抗策の更新も含まれます。

暗号の俊敏性は必須事項のようにも思えますが、実現にかかるコストは依然として高く、リソースに制約のあるデバイスの場合はなおさらです。さらに、一定の柔軟性を追加し、より頻繁かつ場合によっては大幅なシステムまたはデバイスの更新を行えるようにすると、脆弱性が高まる可能性もあります。すべての更新が信頼できるソースから要求されるようにすること、またセキュリティのダウングレードは許可しないことが不可欠になります。このプロセスは、ハードウェアによる信頼の基点で保護できます。

まとめと展望

ポスト量子暗号への移行には、リソースに制約のある組込みデバイスにとって大きな課題が伴いますが、デジタル・インフラストラクチャのセキュリティとレジリエンスを確保するために、先を見越した対策を講じることが不可欠です。NXPは、初期の設計段階から暗号の俊敏性を考慮することに努めています。これは、組込み分野におけるポスト量子暗号の課題を克服し、耐量子暗号ソリューションの新時代を迎え入れるうえで、極めて重要なステップです。ハードウェアの制約、サイドチャネルからの保護、更新性などの問題に対処することで、NXPは、ポスト量子時代の組込みデバイスのために効率的かつ安全なデジタル化された未来を切り開いています。

References

[1] NIST; FIPS 197, Advanced Encryption Standard (AES) https://csrc.nist.gov/pubs/fips/197/final

[2] NIST; FIPS 186-5 Digital Signature Standard (DSS) https://csrc.nist.gov/pubs/fips/186-5/final

[3] Chuang, Gershenfeld, Kubinec; Experimental Implementation of Fast Quantum Searching. In: Phys. Rev. Lett. 80, 3408, 1998 https://doi.org/10.1103%2FPhysRevLett.80.3408

[4] https://www.ibm.com/quantum/blog/quantum-roadmap-2033

[5] https://www.ibm.com/roadmaps/quantum/2029/

[6] BSI; BT-Drucksache 19/26340 https://dserver.bundestag.de/btd/19/263/1926340.pdf

[7] Shor; Algorithms for quantum computation: discrete logarithms and factoring. In: FOCS 1994 https://doi.org/10.1137%2FS0097539795293172

[8] Grover; A fast quantum mechanical algorithm for database search. In: STOC 1996 https://doi.org/10.1145%2F237814.237866

[9] Position Paper on Quantum Key Distribution by French Cybersecurity Agency (ANSSI), German Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces. Jan. 2024 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

[10] NIST; FIPS-203, Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/ipd

[11] NIST; FIPS-204, Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/ipd

[12] NIST; FIPS-205, Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/ipd

[13] https://www.kpqc.or.kr/

[14] https://csrc.nist.gov/Projects/pqc-dig-sig/standardization

[15] NIST; SP800-208, Recommendation for Stateful Hash-Based Signature Schemes https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

[16] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[17] NSA; CNSA 2.0 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[18] Bos, Renes, van Vredendaal; Post-Quantum Cryptography with Contemporary: Co-Processors Beyond Kronecker, Schönhage-Strassen & Nussbaumer. In: USENIX 2022 https://www.usenix.org/conference/usenixsecurity22/presentation/bos

[19] Fujii, Aranha; Curve25519 for the Cortex-M4 and beyond. In: LatinCrypt 2017 https://doi.org/10.1007/978-3-030-25283-0_6

[20] Abdulrahman, Hwang, Kannwischer, Sprenkels; Faster Kyber and Dilithium on the Cortex-M4. In: ACNS 2022 https://doi.org/10.1007/978-3-031-09234-3_42

[21] Bos, Renes, Sprenkels; Dilithium for Memory Constrained Devices. In: AFRICACRYPT 2022 https://doi.org/10.1007/978-3-031-17433-9_10

[22] Bos, Bronchain, Custers, Renes, Verbakel, van Vredendaal; Enabling FrodoKEM on embedded devices. In: CHES 2023 https://doi.org/10.46586/tches.v2023.i3.74-96

[23] Bos, Carlson, Renes, Rotaru, Sprenkels, Waters; Post-Quantum Secure Boot on Vehicle Network Processors. In: escar 2022 https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/year/2022/docId/9372

[24] Kocher; Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: CRYPTO 1996 https://doi.org/10.1007/3-540-68697-5_9

[25] Bos, Gourjon, Renes, Schneider, van Vredendaal; Masking Kyber: First- and Higher-Order Implementations. In: TCHES 2021 https://doi.org/10.46586/tches.v2021.i4.173-214

[26] Azouaoui, Bronchain, Cassiers, Hoffmann, Kuzovkova, Renes, Schneider, Schönauer, Standaert, van Vredendaal; Protecting Dilithium against Leakage: Revisited Sensitivity Analysis and Improved Implementations. In: TCHES 2023 https://doi.org/10.46586/tches.v2023.i4.58-79

[27] ElGhamrawy, Azouaoui, Bronchain, Renes, Schneider, Schönauer, Seker, van Vredendaal; From MLWE to RLWE: A Differential Fault Attack on Randomized & Deterministic Dilithium. In: TCHES 2023 https://doi.org/10.46586/tches.v2023.i4.262-286

[28] Bronchain, Azouaoui, ElGhamrawy, Renes, Schneider; Exploiting Small-Norm Polynomial Multiplication with Physical Attacks Application to CRYSTALS-Dilithium. In: TCHES 2024 https://doi.org/10.46586/tches.v2024.i2.359-383

[29] NSA; Symmetric Key Management Requirements Annex v2.1 https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/Symmetric%20Key%20Management%20Requirements%20v2_1.pdf

[30] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626

[31] https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

[32] https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/

[33] https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/

[34] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[35] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

How to reach us

Website:
www.nxp.com/pqc

Whitepaper:
The Emergence of Post-Quantum Cryptography

Blogs:
A Brief Outlook on the Migration to Post-Quantum Cryptography

Conservative Post-Quantum Security with FrodoKEM

Protecting Post-Quantum Cryptography Against Side-Channel Attacks

Standardization of Post-Quantum Cryptography

NXP Stands at the Forefront of Post-Quantum Cryptography

Post-Quantum Cryptography: Physical Attacks and Countermeasures

Prepare for the Quantum Breakthrough with Post-Quantum Cryptography

The Emergence of Post-Quantum Cryptography

Joppe Bos

Joppe W. Bos is a Technical Director and cryptographer at the Competence Center Crypto & Security (CCC&S) in the CTO organization at NXP Semiconductors. Based in Belgium, he is the technical lead of the Post-Quantum Cryptography team, and has authored over 20 patents and 50 academic papers. He is the co-editor of the IACR Cryptology ePrint Archive.

Christine Cloostermans

Christine Cloostermans is a principal cryptographer at the Competence Center for Cryptography and Security (CCC&S) in the CTO organization at NXP Semiconductors. She acquired her doctorate from TU Eindhoven on topics related to lattice-based cryptography. Christine is a co-author on 10+ scientific publications, and has given many public presentations in the area of post-quantum cryptography. Beyond PQC, she is active in multiple standardization efforts, including IEC 62443 for the Industrial domain, ISO 18013 for the mobile driver's license, and the Access Control Working Group of the Connectivity Standards Alliance.

Melissa Azouaoui

Melissa Azouaoui is a senior cryptographer at the Competence Center for Cryptography and Security (CCC&S) in the CTO organization at NXP Semiconductors. She completed her PhD in 2021 at UCLouvain in Belgium, and NXP in Germany with a focus on side-channel countermeasures and evaluations for symmetric and asymmetric cryptography. Melissa is a member of the Post-Quantum Cryptography team and her work at NXP includes side-channel and fault injection attacks and countermeasures, with a particular focus on lattice and hash-based cryptography.

Gareth Thomas Davies

Gareth T. Davies is a senior cryptographer at the Competence Center for Cryptography and Security (CCC&S) in the CTO organization at NXP Semiconductors. Gareth is a member of the Post-Quantum Cryptography team and works on various topics including protocol analysis, authentication schemes and standardization.

詳細情報：nxp.jp/pqc

ドキュメント番号：POSTQUANCOMPWPA4 REV 0