

耐量子計算機暗号はインターネットに どのような影響をもたらすか - 標準化動向と実装に向けた課題 -

2024年11月20日

菅野 哲

GMOサイバーセキュリティ by イエラエ株式会社

自己紹介

- 名前
 - 菅野 哲 (かんの さとる)
- 所属
 - GMOサイバーセキュリティ by イエラエ株式会社
 - 常務取締役 CTO of Development
- どんなことやっていた／やっているの？
 - 暗号技術と標準化活動
 - 暗号ライブラリや情報セキュリティ関連のシステム開発
 - IETFなどでブロック暗号Camelliaに関する標準化活動
 - 外部活動
 - CRYPTREC 暗号鍵管理ガイダンスWG 委員
 - Trusted Computing Group Invited Expert (2018年10月～)
 - 公正取引委員会 デジタルアナリストとして活動 (2024年5月1日 ～)

菅野パートでのテーマ

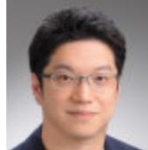
講演者



松本 泰



伊藤 忠彦



菅野 哲

- 松本 泰(JNSA (日本ネットワークセキュリティ協会) フェロー)
- 伊藤 忠彦(セコム株式会社 IS研究所 主任研究員)
- 菅野 哲(GMOサイバーセキュリティ byイエラエ株式会社 常務取締役 CTO of Development)

概要

今日のインターネットのセキュリティは、暗号技術により支えられていると言っても過言ではない状況にあります。しかしながら、量子コンピュータの登場を見据えると、既存の公開鍵暗号から耐量子計算機暗号（PQC）への暗号移行を検討することが必要になりつつあります。インターネットがデジタル社会の基盤として機能していることから、この暗号移行はデジタル社会全体に対して極めて重大な影響を及ぼすものと考えられます。

本セッションでは、過去の暗号アルゴリズム移行についての振り返りや、現在のPQCの状況、IETFなどでのPQCに対応する標準化の動向などから、暗号移行がインターネットに対してどのような影響を与えるのか、そしてどのような課題が生じるのかなどを概説し、今後の暗号移行のあり方を議論します。

トピックス

- 標準化動向
 - NIST、IETFなど
- 実装に向けた課題感
 - PQCの特徴
 - 具体的な事例

<https://internetweek.jp/2024/archives/program/o4>

まず、はじめに

2つの「暗号の2030年問題」とは？

あの大変だった「暗号の2010年問題」対応の悪夢再び....

2つの「暗号の2030年問題」の背景

将来的な「暗号解読の進展」や「計算機環境の変化」を考慮し112bit安全な暗号の移行計画

※ NIST SP 800-57 に記述



1つ目
128bit安全な暗号への移行

CRQCによる現行暗号へのリスクが許容できない

※ **CRQC**: Cryptographically Relevant Quantum Computer / 暗号解読可能な量子計算機



2つ目
PQCへの移行



現行暗号からPQC移行への始まり . . .

- 2022年5月発行されたNSM-10 第3条でPQC移行の大方針
 - → PQCへの移行の期限「2035年」というゴールが設定された

THE WHITE HOUSE

Administration The Record Briefing Room Visit Español MENU

MAY 04, 2022

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

BRIEFING ROOM STATEMENTS AND RELEASES

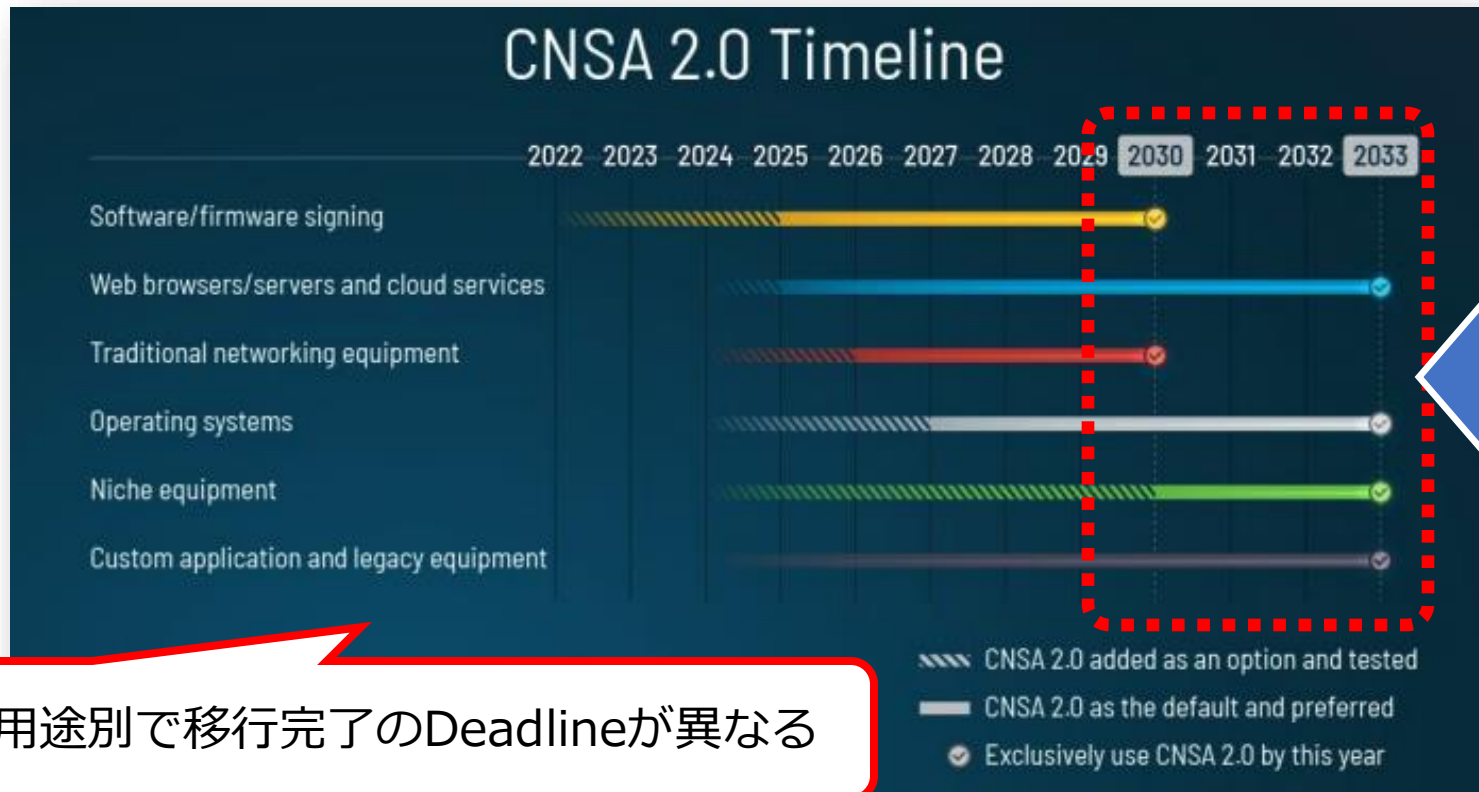
NATIONAL SECURITY MEMORANDUM/NSM-10

Sec. 3. Mitigating the Risks to Encryption. (a) Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC. To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035. Currently, the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA), in their capacity as the National Manager for National Security Systems (National Manager), are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions. The first sets of these standards are expected to be released publicly by 2024.

<https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>

「暗号の2030年問題」であるPQCへの移行の1つの事例

- 2022年9月 NSA が国家安全保障に関する機密情報を守るための暗号 (CNSA) を Ver 2.0に更新 ⇨ CNSA 2.0は耐量子性なアルゴリズムで構成



CNSA: Commercial National Security Algorithm

2030~2033年まで CNSAに完全移行！

<品揃え>

- 公開鍵
CRYSTALS-Dilithium (ML-DSA)
CRYSTAL-Kyber (ML-KEM)
- 共通鍵
AES-256, SHA-384/512
- ソフトウェア等更新
XMSS, LMS

用途別で移行完了のDeadlineが異なる

NSA 「Announcing the Commercial National Security Algorithm Suite 2.0」 より
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMMS_.PDF

標準化動向

NIST PQCコンペティション (1/5)

- 2016年 :
 - NISTがPQCなKEMと署名に関する標準化を発表
- 2017年 :
 - 初期投稿 (64件受理 : KEM 45件 + 署名 19件)
- 2019年 :
 - Round 2 開始 (26方式 : KEM 17件 + 署名 9件)
- 2020年 :
 - Round 3 開始 (7 Finalists, 8 Alternates)

	Finalists	Alternates
KEM	Kyber, NTRU, Saber, Classic McEliece	Bike, FrodoKEM, HQC, NTRUPrime, SIKE
署名	Dilithium, Falcon, Rainbow	GeMSS, Picnic, SPHINCS+

NIST PQCコンペティション (2/5)

- Round 3における評価結果として以下のアルゴリズムを選定

	KEM	署名
Round 3 Selection	CRYSTALS-Kyber	CRYSTALS-Dilithium, Falcon, SPHINCS+

Round 4 Candidates (全てKEM) については最大24ヶ月間の評価を実施予定
この中から少なくとも1つは選定する方針

- Classic McEliece, BIKE, HQC, **SIKE**

選定後に
攻撃が発見...

- 現在、上記に加えて「Additional Digital Signature Schemes」が実施

NISTが発行したPQCに関する標準仕様

- 2024年8月13日 NISTからFIPS 203/204/205 の最終版が遂に公開された

旧名称	新名称	標準仕様名
CRYSTALS-Kyber	ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)	FIPS 203
CRYSTALS-Dilithium	ML-DSA (Module-Lattice-Based Digital Signature Algorithm)	FIPS 204
SPHINCS+	SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)	FIPS 205
FALCON	FN-DSA (FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm)	FIPS 206 ※

※ Draft発行予定：2024年後半

- FIPS 203 ML-KEM (Kyber): <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf>
- FIPS 204 ML-DSA (Dilithium): <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf>
- FIPS 205 SLH-DSA (SPHINCS+): <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf>

NIST PQCコンペティション (3/5)

Additional Signatures の目的として格子ベースでない署名方式を選定したい。また、署名サイズが小さく、署名検証が速い方式を選択したい

- 2022年7月：
 - NISTがAdditional Signaturesの募集を発表
- 2022年8月：
 - 提出要項と評価基準を掲載
- 2023年6月：
 - 最終提出期限
- 2023年7月：
 - 受理されたアルゴリズムを公開

NIST PQCコンペティション (4/5)

- 最終的に**50件**の応募
 - (参考) 2017年に提出された署名は23件
- Round 1の選考結果として**40件**
 - 下記、赤字のアルゴリズムは情報公開後に攻撃が報告...ゴク

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo PROV QR-UOV SNOVA TUOV UOV VOX	3WISE DME-Sign HPPC	Mira MiRitH	RYDE SDitH	PERK	MQOM Biscuit	EagleSign EHTv3 & EHTv4 HAETAE Hawk HuFu Raccoon Squeels	Enhanced pqsigRM Fuleeca LESS MEDS Wave Cross	AIMer Ason-Sign FAEST SPHINCS-alpha	SQIsign	ALTEQ eMLE-Sig 2.0 KAZ-SIGN Preon Xifrat1-Sign.I
7	3	2	2	1	2	7	6	4	1	5
10		7				40				

NIST PQCコンペティション (5/5)

- Round2の選定結果が2024年10月25日に公開
 - Round1 (40件) からRound2の勝者として**14件**が選定
 - Round1選考後に攻撃が発見されたアルゴリズムも敗者復活

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo PROV QR-UOV SNOVA TUOV UOV VOX	3WISE DME-Sign HPPC	Mirath (merger of MIRA/Mi RitH)	RYDE SDitH	PERK	MQOM Biscuit	EagleSign EHTv3 & EHTv4 HAETAE Hawk HuFu Raccoon Squieels	Enhanced pqsigRM Fuleeca LESS MEDS Wave Cross	AIMer Ason-Sign FAEST SPHINCS-alpha	SQIsign	ALTEQ eMLE-Sig-2.0 KAZ-SIGN Preon Xifrat1-Sign.I
4	0	1	2	1	1	1	2	1	1	0
4		5								
14										

諸外国におけるPQCに関する動向

アメリカ以外の諸外国（主にヨーロッパ）の対応状況は以下のとおり

- オーストラリア
 - Australian Signals Directorate (ASD)が2023年にガイダンス” Planning for Post-Quantum Cryptography”の改訂版を公表
- オランダ
 - Nationaal Bureau voor Verbindingsbeveiliging (NBV)が2021年にガイドライン” 「Prepare for the Threat of Quantum Computers”を公表
- ドイツ
 - Bundesamt für Sicherheit in der Informationstechnik (BSI)が2021年にガイドライン” Migration to Post Quantum Cryptography, Recommendations for action by the BSI” を公表
- イギリス
 - National Cyber Security Centre (NCSC)が2020年にホワイトペーパー” Preparing for Quantum-Safe Cryptography”を公表

**各国、アルゴリズムの観点は「NIST選定のPQC中心」
暗号移行の背景や進め方は同様な方針**

IETFとは？ (1/2)

• Internet Engineering Task Force

- インターネットに関する技術の国際標準を策定する組織

1986年1月が
第1回！！

• 理念

- “We reject kings, presidents and voting. We believe in *rough consensus* and *running code*.” David Clark (1992)

• 生産物

- RFC (Request for Comments) を発行
 - インターネットを技術的な側面を支えている

• 活動

- 年3回開催 (3月、7月、11月) で1週間
- 参加者数：1500~2000人
- 参加費：右図参照⇒
- 参加資格：誰でもOK

Onsite Registration Options			
	Super Early	Early	Standard
Week Pass	\$875 USD	\$1095 USD	\$1200 USD
One-Day Pass	\$470 USD	\$590 USD	\$645 USD
Student Pass	\$150 USD	\$150 USD	\$150 USD
Hackathon Only	\$0 USD	\$0 USD	\$0 USD
	Best Available Rate until 27 Jan UTC 23:59	Available until 03 Mar UTC 23:59	Available Anytime

Remote Registration Options			
	Super Early	Early	Standard
Week Pass	\$250 USD	\$310 USD	\$360 USD
One-Day Pass	\$140 USD	\$170 USD	\$200 USD
Student Pass	\$55 USD	\$55 USD	\$55 USD
Hackathon Only	\$0 USD	\$0 USD	\$0 USD
	Best Available Rate until 27 Jan UTC 23:59	Available until 03 Mar UTC 23:59	Available Anytime

<https://registration.ietf.org/122/>

IETFとは？ (2/2)

- IETF/IRTFで主にPQCが関係するWG/RGは以下のとおり (**太字**)

	エリア	代表的なWG
IETF	GEN	gendispatch
	ART	httpbis, satp, mimi, sframe, cbor etc.
	INT	6man, 6lo, drip, dtn etc.
	OPS	dnsop, v6ops, iotops etc.
	RTG	idr, manet, ospf, roll etc.
	SEC	tls, ipsecme, lamps , mls, suit, pquip etc.
	WIT	httpbis, quic, tcpm etc.
IRTF		cfrg , pearg, t2trg, ufmrg etc.

PQC移行を検討

暗号技術を検討

pquip (Post-Quantum Use In Protocols) WG

The screenshot shows the Datatracker website for the Post-Quantum Use In Protocols (pquip) Working Group. The page includes a navigation menu with options like 'About', 'Documents', 'Meetings', 'History', 'Photos', 'Email expansions', and 'List archive'. The main content area is divided into sections: 'WG' (Working Group), 'Personnel', 'Mailing list', and 'Chat'. The 'WG' section provides details such as the name, acronym, area, state, charter, and document dependencies. The 'Personnel' section lists chairs and the area director. The 'Mailing list' section provides the address and archive link. The 'Chat' section provides the room address. Below these sections is the 'Charter for Working Group', which describes the group's purpose and goals. The 'Milestones' section at the bottom lists key events, such as the adoption of an informational document on 'PQC for engineers' in May 2023 and the adoption of a document defining terminology for (hybrid) PQC schemes in April 2023.

WG	Name	Post-Quantum Use In Protocols
	Acronym	pquip
	Area	Security Area (sec)
	State	Active
	Charter	charter-ietf-pquip-01 Approved
	Document dependencies	Show
	Additional resources	GitHub Organization Grand list of WGs and protocols looking at PQC algorithms

Personnel	Chairs	Paul E. Hoffman , Sofia Celi
	Area Director	Roman Danyliw

Mailing list	Address	pqc@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/pqc
	Archive	https://mailarchive.ietf.org/arch/browse/pqc/

Chat	Room address	https://zulip.ietf.org/#narrow/stream/pquip
------	--------------	---

Charter for Working Group

Some IETF protocols rely upon cryptographic mechanisms that are considered secure given today's "classical computers" but would be vulnerable to attacks by a Cryptographically Relevant Quantum Computer (CRQC). These mechanisms rely upon algorithms based on integer factorization or the discrete logarithm problem. Outside of the IETF, active work is underway to develop and validate Post-Quantum Cryptography (PQC) mechanisms that are expected to be resilient to the cryptanalysis capabilities of future CRQCs (e.g., CFRG, US NIST). Select IETF WGs (e.g., LAMPS, TLS, IPSECM, COSE) have already begun standardizing revised protocol behaviors. The focus of Post-Quantum Use in Protocols (PQUIP) WG is to support this growing body of work in the IETF to facilitate the evolution of IETF protocols and document associated operational guidance with respect to PQC.

The WG will provide a standing venue to discuss PQC (operational and engineering) transition issues and experiences to date relevant to work in the IETF. The WG will also provide a venue of last resort to discuss PQC-related issues in IETF protocols that have no associated maintenance WGs. This WG will not update existing protocols, specify new protocols, define new cryptographic mechanisms, or assess whether a given cryptographic mechanism is quantum-resistant.

The WG will document operational and design guidance which supports PQC transition. The general process of elaboration through documentation will be for issues to be identified and discussed on the mailing list, and presentations made at WG meetings. When topics merit more coherent documentation, the WG will adopt documents to capture the information in Internet-Drafts. If the working group consensus is that the material of the Internet-Draft is generally useful for archival purposes, the WG will seek publication of the work items as Informational or Best Current Practices RFCs. At any point, from early discussion of topics through later documentation stages, the WG may identify a more appropriate WG for the matter, and with coordination, dispatch it there.

The output of this WG is expended to inform protocol work and guidance developed by other WGs in the IETF. Consistent with other IETF WGs, this WG will also rely on outside entities (e.g., CFRG) to define and assess new PQC mechanisms.

The IESG is establishing this working group on an experimental basis, and in 2 years, the IESG intends to review it for rechartering to continue or else closure.

Milestones

Date	Milestone	Associated documents
May 2023	WG Adoption of an Informational document on 'PQC for engineers'	
Apr 2023	WG Adoption of an Informational document that defines terminology for (hybrid) PQC schemes	

- PQC移行の問題、IETFでのPQC対応を議論
 - 2023年3月開始
 - PQC移行をサポートするための運用や設計ガイドラインを作成

<https://datatracker.ietf.org/wg/pquip/about/>

pquip WGにおける技術動向

- IETFにおけるPQC移行に向けた初手として、プロトコル設計者や実装者にとって有益となるようなInternet Draft (I-D) を検討
 - どちらのI-Dも粛々とRFC化に向けて進捗

Workgroup: PQUIP
 Internet-Draft: draft-ietf-pquip-pqt-hybrid-terminology-04
 Published: 10 September 2024
 Intended Status: Informational
 Expires: 14 March 2025
 Authors: F. Driscoll, M. Parsons, B. Hale
 UK National Cyber Security Centre, UK National Cyber Security Centre, Naval Postgraduate School

Terminology for Post-Quantum Traditional Hybrid Schemes

Abstract

One aspect of the transition to post-quantum algorithms in cryptographic protocols is the development of hybrid schemes that incorporate both post-quantum and traditional asymmetric algorithms. This document defines terminology for such schemes. It is intended to be used as a reference and, hopefully, to ensure consistency and clarity across different protocols, standards, and organisations.

<https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/>

Workgroup: PQUIP
 Internet-Draft: draft-ietf-pquip-pqc-engineers-06
 Published: 21 October 2024
 Intended Status: Informational
 Expires: 24 April 2025
 Authors: A. Banerjee, T. Reddy, D. Schoinianakis, T. Hollebeek, M. Ounsworth
 Nokia, Nokia, Nokia, DigiCert, Entrust

Post-Quantum Cryptography for Engineers

Abstract

The advent of a Cryptographically Relevant Quantum Computer (CRQC) would render state-of-the-art, traditional public-key algorithms deployed today obsolete, as the mathematical assumptions underpinning their security would no longer hold. To address this, protocols and infrastructure must transition to post-quantum algorithms, which are designed to resist both classical and quantum attacks. This document explains why engineers need to be aware of and understand post-quantum cryptography, detailing the impact of CRQCs on existing systems and the challenges involved in transitioning. Unlike previous cryptographic updates, this shift may require significant protocol redesign due to the unique properties of post-quantum algorithms.

<https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/>

PQUIP WGでの議論 (1/3)

性能、データサイズ
情報あり

NIST PQC Standards

IETF 120-PQUIP
Vancouver Canada, July 22 2024.

- FIPS発表前のNISTによる講演！
 - PQCコンペティションの振り返り
 - 今後の予定など

THE KEMS IN THE 4TH ROUND NIST

Quynh Dang
Cryptographic

Classic McEliece

- NIST is confident in the security
- Smallest ciphertexts, but largest public keys
- We'd like feedback on specific use cases for Classic McEliece

BIKE

- Most competitive performance of 4th round candidates
- We encourage vetting of IND-CCA security

HQC

- Offers strong security assurances and mature decryption failure rate analysis
- Larger public keys and ciphertext sizes than BIKE

~~SIKE~~

- The SIKE team acknowledged that SIKE (and SIDH) are insecure and should not be used

The 4th Round will likely end in the fall of 2024

OTHER UP COMING PQC PUBLICATIONS NIST

- SP 800-208 is being revised, based on industry feedback. How to allow backups for HSMs while minimizing the risk of key reuse.
- SP 800-227 Recommendations for Key Encapsulation Mechanisms is expected to be available for public comments soon after FIPS 203 is finalized and published.
- A draft SP specifies Small SLH-DSA Parameter Sets is expected in Fall 2024.

<https://datatracker.ietf.org/meeting/120/materials/slides-120-pquip-nist-pqc-standards-00>

PQUIP WGでの議論 (2/3)

Post-quantum cryptography migration use cases

[draft-vaira-pquip-pqc-use-cases](#)

PQUIP – IETF 120 – July 23rd 2024

Hendrik Brockhaus
Siemens

John Gray
Entrust

Mike Ounsworth
Entrust

Alex Railean
Siemens

- 「デジタル署名のユースケースにおけるPQC移行」が目的！
 - 適合するアルゴリズムとパラメータの選択支援

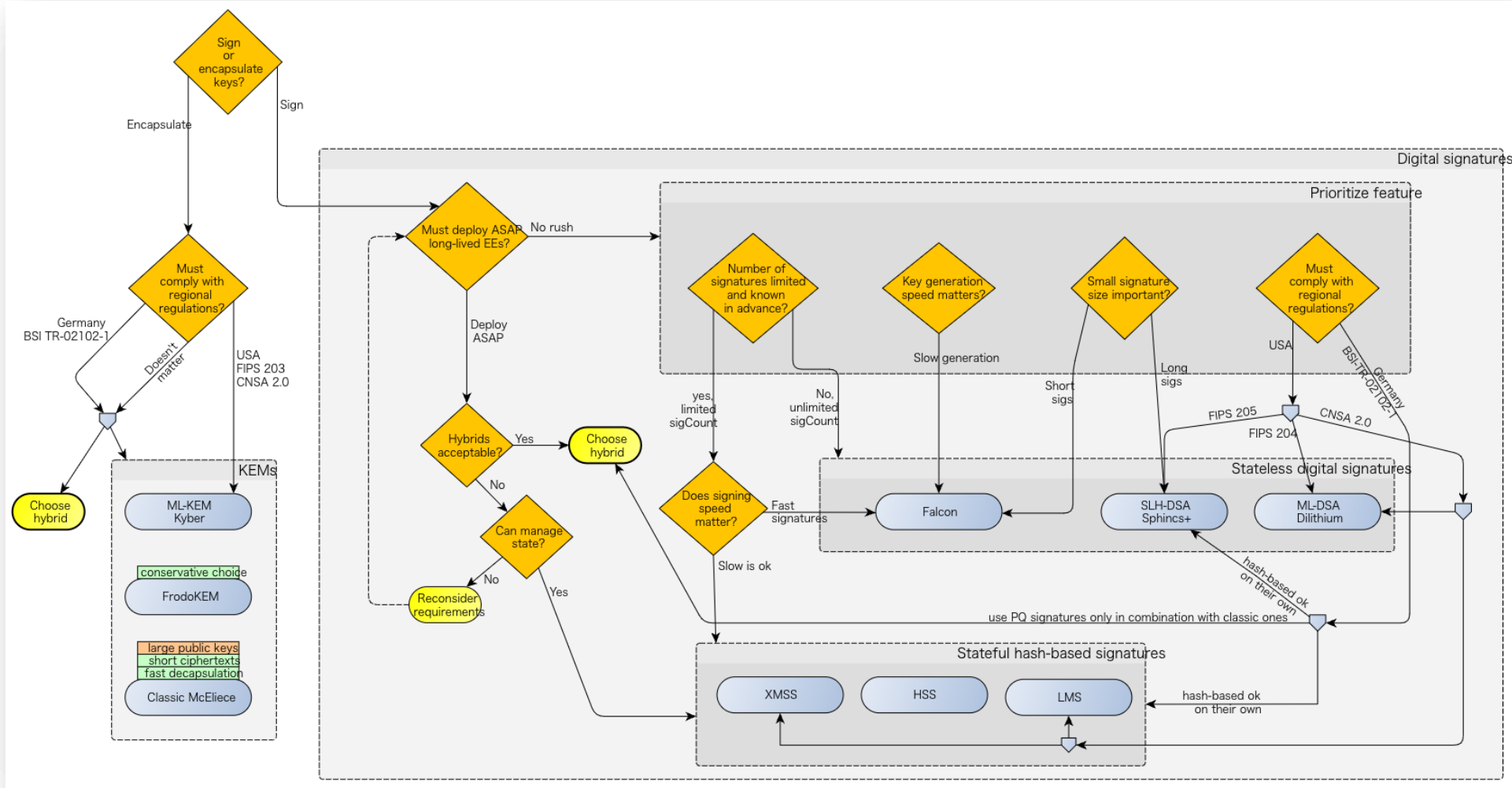
What next? Explore “pessimistic migration”

- Assumption: CRQC-attacks start sooner than standardization or migration is complete. How about tomorrow?
- What can one do today to
 - not be an easy target tomorrow
 - and buy time on Q-day
- Some techniques
 - Wrap legacy communications (e.g., SSH tunnels with NTRU/x25519)
 - Symmetric ciphers with pre-shared keys without handshakes (e.g., shadowsocks)

<https://datatracker.ietf.org/meeting/120/materials/slides-120-pquip-post-quantum-cryptography-migration-use-cases-00>

PQUIP WGでの議論 (3/3)

- 移行先のPQCを決定するための検討フローも検討されている



<https://github.com/avaira77/pq-ietf-usecase/blob/main/decision-tree/pqcrypto-decision-tree.svg>

cfrg (Crypto Forum)

- 将来のインターネットで利用することが期待できる暗号技術を検討
 - Pure PQCやハイブリッド利用について検討

Crypto Forum (cfrg)

About Documents Meetings History Photos Email expansions List archive »

Search

Document ▾ Date ^

Active Internet-Drafts (14 hits)

- [draft-irtf-cfrg-kangarootwelve-15](#) KangarooTwelve and TurboSHAKE 28 pages 2024-11-11
- [draft-irtf-cfrg-det-sigs-with-noise-04](#) Hedged ECDSA and EdDSA Signatures 17 pages 2024-11-11
- [draft-irtf-cfrg-vdaf-13](#) Verifiable Distributed Aggregation Functions 151 pages 2024-11-11
- [draft-fluhrer-lms-more-parm-sets-17](#) Additional Parameter sets for HSS/LMS Hash-Based Signatures 27 pages 2024-10-27
- [draft-irtf-cfrg-aegis-aead-13](#) The AEGIS Family of Authenticated Encryption Algorithms 63 pages 2024-10-27
- [draft-irtf-cfrg-cspace-13](#) CPace, a balanced composable PAKE 96 pages 2024-10-27
- [draft-irtf-cfrg-aead-properties-09](#) Properties of AEAD Algorithms 27 pages 2024-10-27
- [draft-irtf-cfrg-aead-limits-09](#) Usage Limits on AEAD Algorithms 20 pages 2024-10-09
- [draft-irtf-cfrg-partially-blind-rsa-00](#) Partially Blind RSA Signatures 24 pages 2024-09-30
- [draft-irtf-cfrg-opaque-17](#) The OPAQUE Augmented PAKE Protocol 85 pages 2024-09-27
- [draft-irtf-cfrg-bbs-signatures-07](#) The BBS Signature Scheme 117 pages 2024-09-23
- [draft-irtf-cfrg-signature-key-binding-07](#) Key Blinding for Signature Schemes 16 pages 2024-09-23
- [draft-irtf-cfrg-dnhpke-05](#) Deterministic Nonce-less Hybrid Public Key Encryption 40 pages 2024-09-09
- [draft-irtf-cfrg-rsa-guidance-01](#) Implementation Guidance for the PKCS #1 RSA Cryptography Specification 23 pages 2024-09-03

Related Internet-Drafts and RFCs (11 hits)

Document	Pages	Date	Status
draft-connelly-cfrg-xwing-kem-06 X-Wing: general-purpose hybrid post-quantum KEM	34 pages	2024-10-21	I-D Exists
draft-connelly-cfrg-hpke-mlkem-04 ML-KEM for HPKE	9 pages	2024-10-18	I-D Exists
draft-dijkhuis-cfrg-hdkeys-01 Hierarchical Deterministic Keys	24 pages	2024-10-17	I-D Exists
draft-gueron-cfrg-dndkgcm-01 Double Nonce Derive Key AES-GCM (DNDK-GCM)	38 pages	2024-10-17	I-D Exists
draft-sfluhrer-cfrg-ml-kem-security-considerations-01 ML-KEM Security Considerations	10 pages	2024-10-11	I-D Exists
draft-chen-cfrg-vdaf-pine-01 Private Inexpensive Norm Enforcement (PINE) VDAF	17 pages	2024-09-27	I-D Exists
draft-mouris-cfrg-mastic-03 The Mastic VDAF	37 pages	2024-09-27	I-D Exists
draft-harvey-cfrg-ntl-mode-04 Merkle Tree Ladder (MTL) Mode Signatures	53 pages	2024-09-17	I-D Exists 14
draft-harvey-cfrg-ntl-mode-considerations-00 Considerations for Integrating Merkle Tree Ladder (MTL) Mode Signatures into Applications	21 pages	2024-08-22	I-D Exists 1
draft-bradleylundberg-cfrg-arkg-02 The Asynchronous Remote Key Generation (ARKG) algorithm	34 pages	2024-05-27	I-D Exists
draft-westerbaan-cfrg-hpke-xyber768d00-03 X25519Kyber768Draft00 hybrid post-quantum KEM for HPKE	20 pages	2024-05-14	I-D Exists Expires soon

<https://datatracker.ietf.org/rg/cfrg/about/>

CFRGでの議論 (1/2)

- IETF121でFIPSとして公開されたML-KEMの利用に向けた検討が実施
 - 「セキュリティ上の検討事項」や「公開鍵/暗号文サイズの圧縮」について議論
 - 参加者たちも公開鍵/暗号文サイズへの課題意識は興味がある人が多い！

ML-KEM Security Considerations

[draft-sfluhrer-cfrg-ml-kem-security-considerations](#)

Scott Fluhrer, Quynh Dang, John Preuß Mattsson, Kevin Milner, Daniel Shiu
(and anyone else who wants to contribute)

IETF 121, Dublin

1

Kemeleon Encodings

Making ML-KEM public keys and ciphertexts
indistinguishable from random

6 November 2024
IETF121: CFRG

<https://datatracker.ietf.org/meeting/121/materials/slides-121-cfrg-ml-kem-00>

<https://datatracker.ietf.org/meeting/121/materials/slides-121-cfrg-ml-kem-public-key-compression-and-random-encodings-00>

CFRGでの議論 (2/2)

- IETF121でFIPS20Xとして選定されていないFrodoKEMが提案
 - FrodoKEMはML-KEMと比較してシンプルな設計で実装しやすさをアピール
 - 建設的な議論が行われてコメント対応ができれば先に進みそう

FrodoKEM

A simple and conservative KEM from generic lattices

Erdem Alkim Joppe W. Bos Léo Ducas Patrick Longa Ilya Mironov
 Michael Naehrig Valeria Nikolaenko Chris Peikert Ananth Raghunathan Douglas Stebila



FrodoKEM: Introduction

- ❑ FrodoKEM is a quantum-safe IND-CCA2 secure Key Encapsulation Mechanism (KEM) based on the hardness of the plain Learning With Errors (LWE) problem
 - It uses generic, algebraically unstructured lattices
- ❑ It was a **Round 3 alternate** in the NIST PQC standardization process
 - Dropping FrodoKEM was primarily motivated by performance: “In terms of security, Frodo’s conservative design choices are laudable.” (NIST Round 3 Status Report)
- ❑ FrodoKEM has been recommended for use by several European countries (Germany [BSI24], France, Sweden)
- ❑ Ongoing standardization by ISO (started on April’23)
 - To be included as Amendment 2 of ISO/IEC 18033-2 (together with ML-KEM and Classic McEliece)
 - Currently approved for Draft Amendment (DAM), Sept/Oct’24

[BSI24] “BSI – Technical Guideline (Cryptographic Mechanisms: Recommendations and Key Lengths)”, BSI TR-02102-1, version February 2024.

1/11

<https://datatracker.ietf.org/meeting/121/materials/slides-121-cfrg-frodokem-a-simple-and-conservative-kem-from-generic-lattices-00>

PQCの特性を活かしたTLSへのアプローチ

TLS Working Group
Internet-Draft
Intended status: Informational
Expires: 17 October 2024

T. Wiggers
PQShield
S. Celi
Brave Software
P. Schwabe
Radboud University and MPI-SP
D. Stebila
University of Waterloo
N. Sullivan
15 April 2024

KEM-based Authentication for TLS 1.3
draft-celi-wiggers-tls-authkem-03

Abstract

This document gives a construction for a Key Encapsulation Mechanism (KEM)-based authentication mechanism in TLS 1.3. This proposal authenticates peers via a key exchange protocol, using their long-term (KEM) public keys.

<https://datatracker.ietf.org/doc/draft-celi-wiggers-tls-authkem/>

- KEMTLSはTLSのハンドシェイクを改造し、デジタル署名を依存せず、KEMを用いて機密性と認証を実現
- すでにKEMTLSを実装してパフォーマンス評価済み
 - Implementing and Measuring KEMTLS (※)
 - パフォーマンス比較
 - ハンドシェイク：最大38%短縮
 - メモリフットプリントが小さい
 - サーバのCPU負荷を最大90%削減など

※ <https://eprint.iacr.org/2021/1019.pdf>

実装に向けた課題

標準化も順調に進んでるので暗号移行も楽勝？

そうも問屋が卸さない

社会で受容されるに向けて気になる点として・・・

データサイズ

技術としての成熟度

PQCアルゴリズムとデータサイズ比較 (1/2)

現行暗号と比較してデータサイズが**大盛り**へ...

参考：ECDH NIST P256
公開鍵 64byte、秘密鍵 32byte、データ 32byte

カテゴリー	アルゴリズム名	利用する問題	データサイズ (byte)		
			公開鍵	秘密鍵	暗号文/署名
公開鍵暗号 /KEM	CRYSTALS-KYBER	Module-LWE問題 Lattices	800	1,632	760
	BIKE	QC-MDPC符号のSDP Code	1,540	280	1,572
	Classic McEliece	Gappa符号のSDP Code	261,120	6,492	128
	HQC	Quasi-Cycle符号のSDP Code	2,249	40	1,572
デジタル署名	CRYSTALS-DILITHIUM	Module-LWE問題 Lattices	1,312	2,528	2,420
	FALCON	SIS問題 Lattices	897	7,533	666
	SPHINCS+	ハッシュ関数の衝突探索問題 Hash	32	64	7,856

※ **128bit安全相当**を実現した際のデータサイズ
※ 太字・斜体はコンペの勝者

詳細は、PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates
<https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>

PQCアルゴリズムとデータサイズ比較 (2/2)

現行暗号と比較してデータサイズが**特盛**へ...

参考：ECDH NIST P521

公開鍵 132byte、秘密鍵 64byte、データ 66byte

カテゴリー	アルゴリズム名	利用する問題	データサイズ (byte)		
			公開鍵	秘密鍵	暗号文/署名
公開鍵暗号 /KEM	CRYSTALS-KYBER	Module-LWE問題	Lattices 1,568	3,168	1,568
	BIKE	QC-MDPC符号のSDP	Code 5,122	580	5,154
	Classic McEliece	Gappa符号のSDP	Code 1,357,824	14,120	240
	HQC	Quasi-Cycle符号のSDP	Code 7,245	40	14,469
デジタル署名	CRYSTALS-DILITHIUM	Module-LWE問題	Lattices 2,592	4,864	4,595
	FALCON	SIS問題	Lattices 1,793	13,953	1,280
	SPHINCS+	ハッシュ関数の衝突探索問題	Hash 64	128	49,856

※ **256bit安全相当**を実現した際のデータサイズ

※ 太字・斜体はコンペの勝者

詳細は、PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

<https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>

ざっくりとした結論として・・・

PQCの成熟度は**過大評価すべきではない**

- 成熟度の雰囲気
 - 1990年代半ばのRSAの成熟度と同程度 と言われている？！
- 気になる観点
 - アルゴリズム：問題の難易度、評価手法 etc
 - 実装：サイドチャネル攻撃、プロトコルへの統合 etc

成熟度として懸念する事例

- NISTコンペティションで選考されたアルゴリズムでも攻撃がポロポロと発見 → 設計手法や安全性評価が成熟していない？

NIST PQコンペティション (2/5)

GMO CYBER SECURITY IERAE

- Round 3における評価結果として以下のアルゴリズムを選定

	KEM	署名
Round 3 Selection	CRYSTALS-Kyber	CRYSTALS-Dilithium, Falcon, SPHINCS

Round 4 Candidates (全てKEM) については最大24ヶ月間の評価期間。この中から少なくとも1つは選定する方針

- Classic McEliece, BIKE, HQC, **SIKE**

選定後に攻撃が発見...

- 現在、上記に加えて「Additional Digital Signature Scheme」

NIST PQコンペティション (4/5)

GMO CYBER SECURITY IERAE

- 最終的に**50件**の応募
 - (参考) 2017年に提出された署名は23件
- Round 1の選考結果として**40件**
 - 下記、赤字のアルゴリズムは情報公開後に攻撃が報告...ゴクリ

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo PROV QR-UOV SNOVA TUOV UOV VOX	3WISE DME-Sign HPPC	Mira MiRiTH	RYDE SDiTH	PERK	MQOM Biscuit	EagleSign EHTv3 & EHTv4 HAETAE Hawk HuFu Raccoon Squeels	Enhanced pqsigRM Fuleeca LESS MEDS Wave Cross	AIMer Ason-Sign FAEST SPHINCS-alpha	SQIsign	ALTEQ eMLE-Sig 2.0 KAZ-SIGN Preon Xifrat1-Sign.I
7	3	2	2	1	2	7	6	4	1	5
10		7				40				

ざっくりとした結論として・・・

PQCの成熟度は**過大評価すべきではない**

- 成熟度の雰囲気
 - 1990年代半ばのRSAの成熟度と同程度 と言われている？！
- 気になる観点
 - アルゴリズム：問題の難易度、評価手法 etc
 - 実装：サイドチャネル攻撃、プロトコルへの統合 etc

PQCを利用する際に完全に成熟するまで待たずに開始すべし！

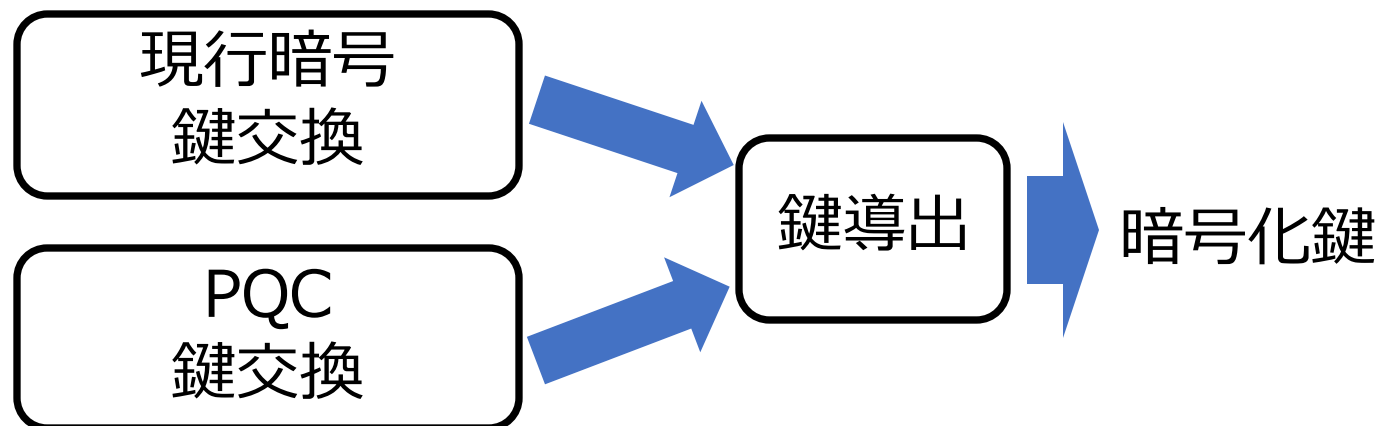
「現行暗号 + PQC」の**ハイブリッド**という解決策

PQC移行における理想と現実

- 理想的には...
 - 想定される脅威（ハーベスト攻撃等）が存在するのでPQCに完全移行だ！
- 現実的には...
 - PQCに対する**新たな攻撃が発見されてしまい暗号方式が危殆化**
 - PQCに関する**実装ノウハウの蓄積不足による脆弱性が生じる** など



- 過渡期だからこそ「**ハイブリッド**」に注目！



ハイブリッドのメリット

- 「現行暗号」か「PQC」が安全であれば、安全な状態を実現
- PQCを実社会運用することができ、課題/問題を抽出

事例：PQC（ハイブリッド）がTLSを破壊！？

Home > News > Security > Google Chrome's new post-quantum cryptography may break TLS connections

Google Chrome's new post-quantum cryptography may break TLS connections

By [Sergiu Gatlan](#) April 28, 2024 10:19 AM 0



Some Google Chrome users report having issues connecting to websites, servers, and firewalls after Chrome 124 was released last week with the new quantum-resistant X25519Kyber768 encapsulation mechanism enabled by default.

Google started testing the post-quantum secure TLS key encapsulation mechanism in August and has now enabled it in the latest Chrome version for all users.

- 2024年4月にリリースされた Chromeで「X25519Kyber768」がデフォルト有効に！
- 原因
 - TLSの適切な実装がなされず、ClientHello Msgのサイズ起因で秘孔を突く
- 影響範囲
 - 複数のベンダー（Fortinet, SonicWall, Palo Alto Networks, AWS など）のセキュリティアプライアンスなど

<https://www.bleepingcomputer.com/news/security/google-chromes-new-post-quantum-cryptography-may-break-tls-connections/>

秘孔を突いたデータ (key share) って？

```
2139 7.161352 10.4.30.133 172.64.155.141 TLSv1.3 756 Client Hello (SNI=chatgpt-async-webps-prod-eastus-5.chatgpt.com)
2140 7.167314 172.64.155.141 10.4.30.133 TCP 66 443 → 63132 [ACK] Seq=1 Ack=2079 Win=65536 Len=0 TSval=200058531 TSecr=2700808640
2141 7.176186 172.64.155.141 10.4.30.133 TLSv1.3 1447 Server Hello, Change Cipher Spec, Application Data
2142 7.176283 10.4.30.133 172.64.155.141 TCP 66 63132 → 443 [ACK] Seq=2079 Ack=1382 Win=130432 Len=0 TSval=2700808656 TSecr=200058534
2143 7.181246 10.4.30.133 172.64.155.141 TLSv1.3 130 Change Cipher Spec, Application Data
2144 7.181496 10.4.30.133 172.64.155.141 TCP 1454 63132 → 443 [ACK] Seq=2143 Ack=1382 Win=131072 Len=1388 TSval=2700808661 TSecr=200058534 [TCP segment of a reassembled PDU]

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 1964
< Extension: Reserved (GREASE) (len=0)
  Type: Reserved (GREASE) (31354)
  Length: 0
  Data: <MISSING>
< Extension: psk_key_exchange_modes (len=2)
  Type: psk_key_exchange_modes (45)
  Length: 2
  PSK Key Exchange Modes Length: 1
  PSK Key Exchange Mode: PSK with (EC)DHE key establishment
< Extension: session_ticket (len=0)
  Type: session_ticket (35)
  Length: 0
  Session Ticket: <MISSING>
< Extension: key_share (len=1263) X25519Kyber768Draft00, x25519
  Type: key_share (51)
  Length: 1263
  Key Share extension
    Client Key Share Length: 1261
    > Key Share Entry: Group: Reserved (GREASE), Key Exchange length: 1
    < Key Share Entry: Group: X25519Kyber768Draft00, Key Exchange length: 1216
      Group: X25519Kyber768Draft00 (25497)
      Key Exchange Length: 1216
      Key Exchange [truncated]: 0c13a46393bbf034eb6951be5e70a6d88fdd808e544
    < Key Share Entry: Group: x25519, Key Exchange length: 32
      Group: x25519 (29)
      Key Exchange Length: 32
      Key Exchange: 15734a2cbbbbcb3a41df639b19af1b61cf6298d66963669111a0aef...
```

0050 13 01 13 02 13 03 c0 2b c0 2f c0 2c c0 30 cc a9+ ./, .0..
0060 cc a8 c0 13 c0 14 00 9c 00 9d 00 2f 00 35 01 00 / .5..
0070 07 ac 7a 7a 00 00 00 2d 00 02 01 01 00 23 00 00zz.....#..
0080 00 33 04 ef 04 ed ea ea 00 01 00 63 99 04 c0 0c [3].....c....
0090 13 a4 63 93 bb f0 34 eb 69 51 be 5e 70 a6 d8 8fc...4. iQ.^p..
00a0 dd 80 8e 54 4a 87 1b e5 57 e7 af f6 42 71 0a b8 ...TJ... W...Bq..
00b0 88 77 31 16 11 6c 33 c5 01 84 85 76 13 5f c7 92 .w1..l3. ...v...
00c0 70 d9 80 9a e5 14 87 6e 44 8b 0a 45 33 19 3c ab p.....n D..E3<..
00d0 eb f5 62 7a 6c 61 7e 7b 59 d5 6c 4f 92 b1 a9 50 ..bzla~{ Y.l0...P
00e0 2c ae af 85 7a a8 74 2d 21 17 83 fc 45 21 a1 99 ,...z-t- !...E!..
00f0 ac 58 51 2f 2d e2 2e fb ea a0 da 2b 82 d5 c0 59 .XQ/-... +...+Y
0100 ec 0a 1c 44 c9 b6 b1 90 3f 5a ac ba bb 85 86 8e ...D... ?Z.....
0110 fb 80 af 70 18 1f 95 ce 97 05 bd 09 80 b8 6b d8 ...p... ..k...
0120 2e c9 5a 71 9a eb 13 b4 4a b9 d5 35 5a ab 69 08 .Zq... J..5Z.i.
0130 7e 10 81 88 89 63 41 e8 53 b5 9c 83 33 6b a9 77 ~...cA. S...3k.w
0140 4c a3 ae 67 24 81 33 5b q... .. L..g\$.3[
0150 7c 64 b2 f4 3e 7e d0 9a .y... ..|d...>...
0160 57 0a 4a d1 c7 09 15 ..|... ..ug.J...
0170 0a 06 21 0d 5e 68 .39... ..!^h
0180 e8 e8 96 26 70 ba =.&... ..&p
0190 5 ca 4a 85 69 80 ae ...~(^.4.J.i..
01a0 12 b6 ec 50 ae c3 e8 e!.C(I... ..P...
01b0 65 2e 25 b7 92 f3 06 1d ?...} @. e.%...
01c0 ac a3 33 34 22 a2 4c b8 *.S.J.: ..34".L.
01d0 62 81 d0 55 3c 4e fa 32 65 60 ce 33 14 0a c4 cc b.U<N:2 e`.3...
01e0 6e ac 28 26 94 d8 40 f1 35 90 c4 09 6f 9d a9 c7 n.{&..@. 5...o...
01f0 f8 5b 63 1a ec ac f6 f0 15 9e 99 ab 37 40 76 5c .[c... ..7@v\
0200 b8 01 d6 82 08 50 fb bd ef 22 35 40 2c cb 74 e5P.. ."5@, .t.
0210 c9 e6 f3 4b 1b 64 c3 ec f0 11 95 b0 99 39 d8 06 ...K.d... ..9...
0220 28 0b 8b b4 a8 58 6b 13 04 2c 69 b7 61 a5 87 92 {...Xk. ,.i.a...
0230 57 bd dd fa af 7d 51 51 b1 e1 8c f4 f0 30 eb 82 W...}QQ ...0..
0240 6f 06 5b 55 6c a6 ad 33 18 5b cc c8 7a 08 fa 71 o.[U].3 .[.z.z.q
0250 1c 0c 12 67 f3 83 59 80 70 cd 29 58 9c 09 5c f6 ...g.Y. p.)X..\
0260 87 a5 88 1c 7a b4 52 0a 0f 11 4a 72 d5 25 f7 80 ...z.R... Jr.*.
0270 15 71 16 95 cd e3 55 9c 96 a4 98 55 74 4b 60 a4 .q...U. ...UtK\
0280 6d a7 cc 2a c1 bd 37 c5 c9 34 8a 8c dd c7 a6 ab m.*.7. .4...
0290 7b 13 1f aa a7 9c 0a 0f 35 c6 15 e3 e1 c6 db ec {..... 5.....
02a0 b2 58 b5 1f 48 61 4d 4e 79 c2 d1 8a b3 df c4 bb .X.HaMN y.....
02b0 37 10 a2 ec f9 be 7c 78 79 aa 65 28 ad 37 c9 3e 7.....|x y.e(.7->
02c0 cc 34 2c a1 40 a7 bb 2f 28 c8 84 5c c0 48 0a 77 .A.T.(.8...H..

鍵交換方式を指定

<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>

実際、どの程度大きいのか？

<現行暗号 X25519での鍵交換>

```

  v Extension: key_share (len=38) x25519
    Type: key_share (51)
    Length: 38
    v Key Share extension
      Client Key Share Length: 36
      > Key Share Entry: Group: x25519, Key Exchange length: 32
  
```

<Hybrid:X25519Kyber728での鍵交換>

```

  v Extension: key_share (len=1263) X25519Kyber768Draft00, x25519
    Type: key_share (51)
    Length: 1263
    v Key Share extension
      Client Key Share Length: 1261
      > Key Share Entry: Group: Reserved (GREASE), Key Exchange length: 1
      > Key Share Entry: Group: X25519Kyber768Draft00, Key Exchange length: 1216
      > Key Share Entry: Group: x25519, Key Exchange length: 32
  
```

33倍以上巨大化！！

結果として

実際のインターネットで利用することで課題を洗い出すことに貢献！

身の回りで利用されるPQC・・・だがしかし

- iOS18よりAppleがプライバシー保護が強化！
 - Live CallerID Lookup等で実装済み

ここで利用されている

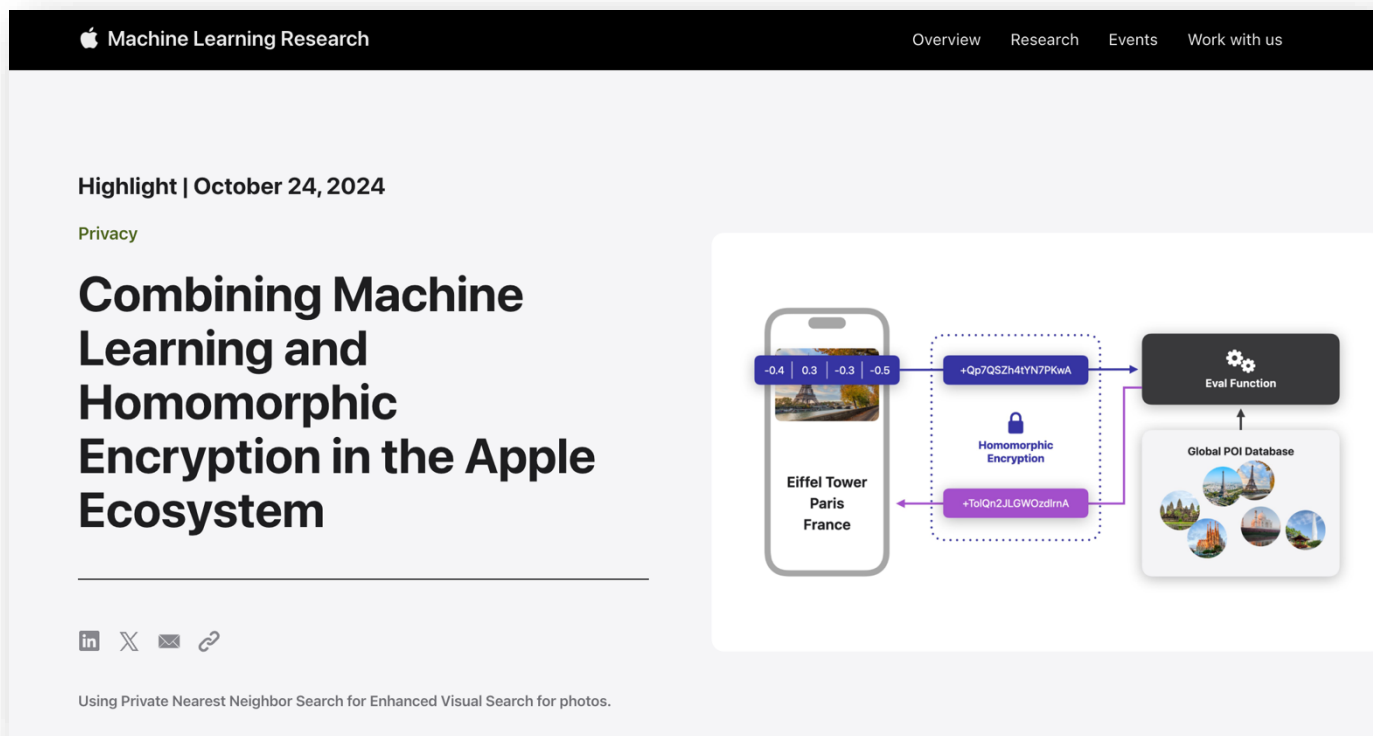
“Homomorphic Encryption” (準同型暗号)

Brakerski/Fan-Vercauteren (BFV)

Ring Learning With Errors (RLWE) 問題を
安全性の根拠とした耐量子暗号 (PQC)

⋮

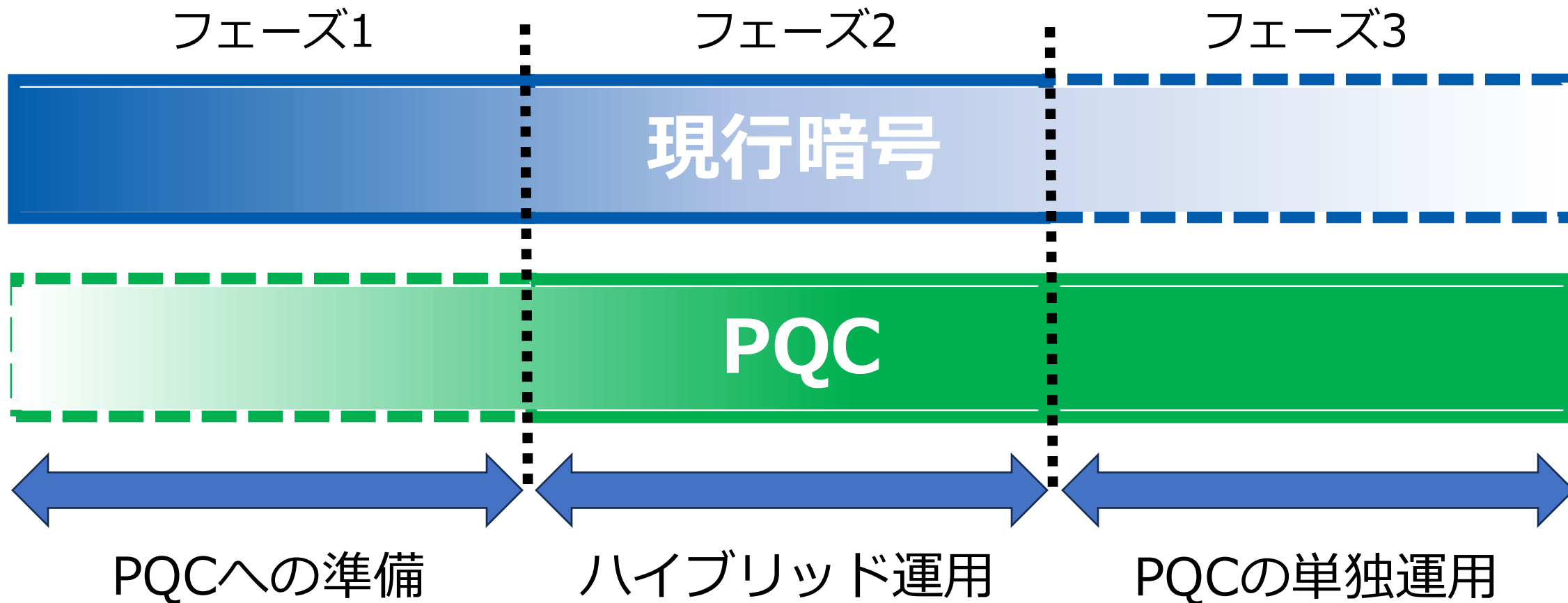
NISTが選定した以外の
PQCもあるから要注意！！



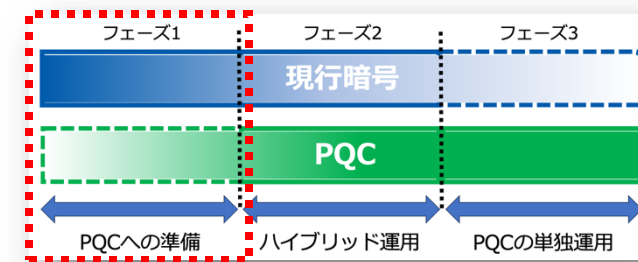
<https://machinelearning.apple.com/research/homomorphic-encryption>

暗号の「2030年問題（PQC）」に向けた暗号移行

- 暗号移行に向けた取り組は3つのフェーズ
 - 最終段階の「フェーズ3」を目指して粛々と準備を進めるのみ



暗号移行計画：フェーズ 1（現在～2024年）



- 基本方針：守備力を上げていこう
 - PQCはメジャーな現行暗号とハイブリッド化は**必須**
 - 寿命の長いデータにはPQCが**推奨**
- ユーザや製品等への影響
 - ハイブリッド利用について、高セキュリティが必要とされるユーザや製品は義務付けられる
 - ライブラリ等の製品はPQC対応を推進
- PQCの選択という観点から自由度
 - （できれば）よく研究され、安定してると期待されるアルゴリズム
 - 例：NIST PQCコンペ Finalistや代替アルゴリズム
 - 一部地域で「FrodoKEM推し」も
 - 望まれる安全性はレベル5

- 暗号移行に関するところに、いつも顔を出す「Crypto Agility」

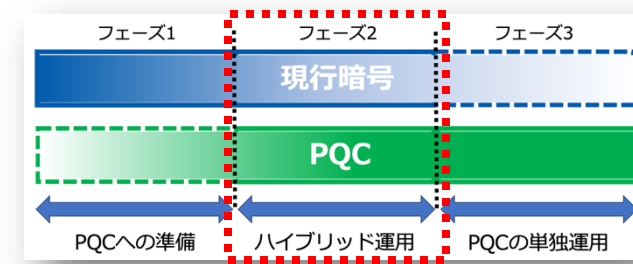
Crypto Agility

暗号

柔軟さ

- ざっくり言うと・・・
 - 対象システムの**ライフタイム中に暗号アルゴリズムを更新できる**状態であること
- Crypto Agilityを活かすためにもう一つ必要なこと
 - やってくる将来の暗号移行に備えて、対象システムの用途や暗号利用を把握するのも大事！
- 実現例：Microsoft CNG (Cryptography:Next Generation)
 - NT 4.0から導入されたCryptoAPIの後継 (Vistaから導入)

暗号移行計画：フェーズ 2（2025年～）

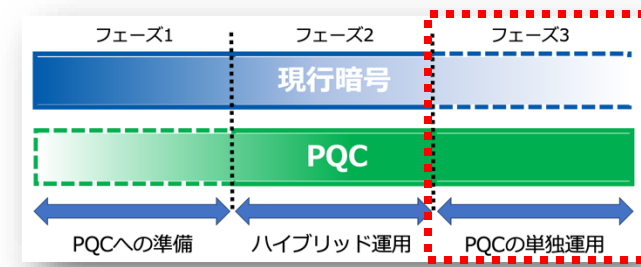


- 基本方針：PQCへの信頼を醸成
 - ハイブリッドは必須！
 - キモチ：現行暗号を保証するためにハイブリッドは重要なまま
 - ユースケースによってはPQCは必須事項へ
- 対応すべきPQCが揃い踏み？！
 - NIST以外にもPQCの基準リストを公開
 - 組織例：仏 ANSSI
 - アルゴリズム例：
 - 格子ベース（KEM）：Crystals-Kyber, FrodoKEM
 - 格子ベース（署名）：Crystals-Dilithium, Falcon
 - ハッシュベース（署名）：XMSS/LMS, SPHINCS+

※ 伝統的にANSSIは革新的な最先端アルゴリズムの排除を避けるために推奨アルゴリズムリストのようなものは提供しないことに注意。
言い換えると推奨はするが排他的なものではない。

https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf

暗号移行計画：フェーズ 3（2030年～）



- 基本方針：PQCの一人立ち
 - ハイブリッドではなく、PQC単体での利用がされ始める
 - 用途選ばず、ほぼ全てのユースケースでPQCが必須となる

まとめ

- 今後のインターネットに大きな影響を与える可能性の高い、耐量子暗号（PQC）に関する「標準化動向」と「実装に向けた課題」をお話しさせていただきました。
 - 暗号の2030年問題
 - NIST/IETFでの標準化動向
 - 実社会に適用しようとした際に気になるPQCの特徴
 - ハイブリッドモード

すべての人にインターネット

GMO