GMO CYBER SECURITY IERAE

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う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。

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

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

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

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

1つ目

128bit安全な暗号への移行

2つ目

PQCへの移行

今回は
コチラ！

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

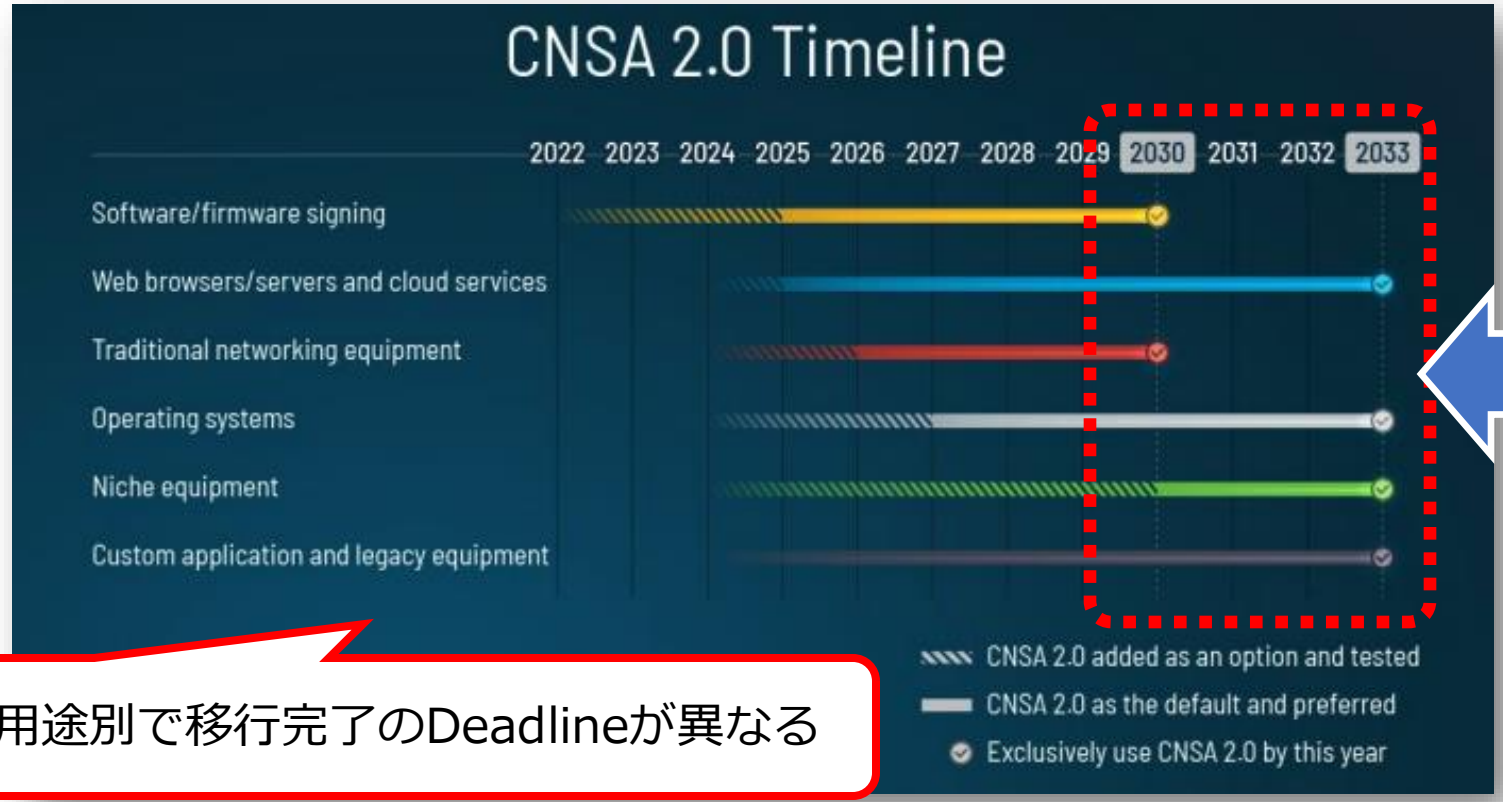
NATIONAL SECURITY MEMORANDUM/NSM-10

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



用途別で移行完了のDeadlineが異なる

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

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_ALGORITHMS_.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~~

- 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…ｺﾞｸﾘ

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 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
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/MiRitH*)	**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

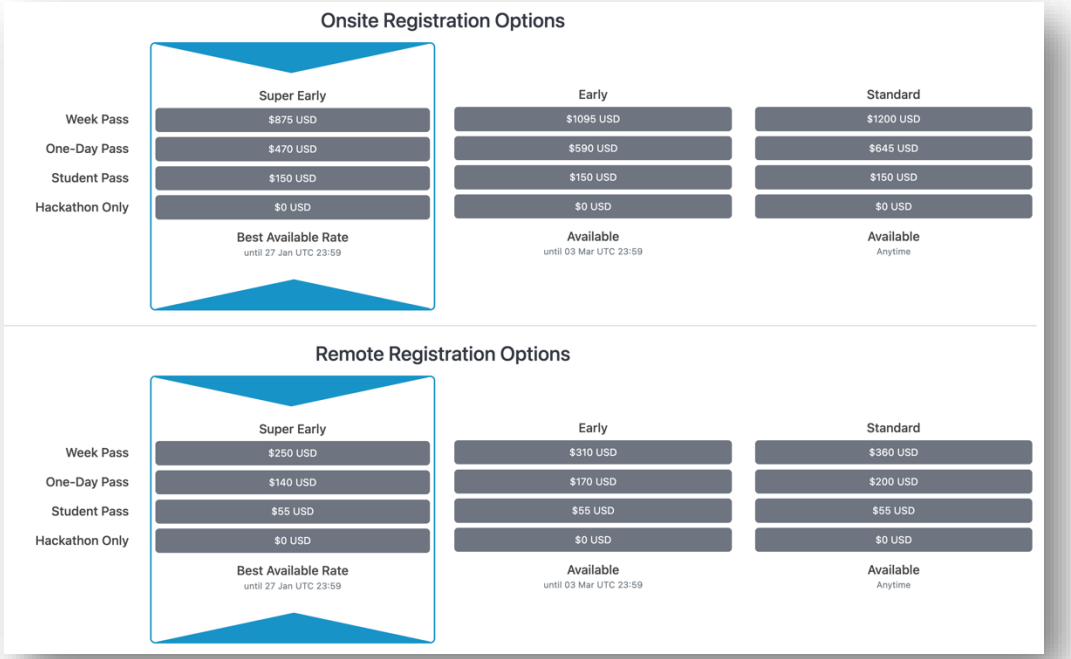
- オーストラリア
  - Australian Signals Directorate (ASD)が2023年にガイダンス” Planning for Post-Quantum Cryptography”の改訂版を公表
- オランダ
  - Nationaal Bureau voor Verbindingsbeveiliging (NBV)が2021年にガイドライン” 「Prepare for the Threat of Quantum Computers”を公表
- ドイツ
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)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）

- **I**nternet **E**ngineering **T**ask **F**orce
  - **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
- 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

1986 年1月が第1回！！



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

IETFとは？（2/2）

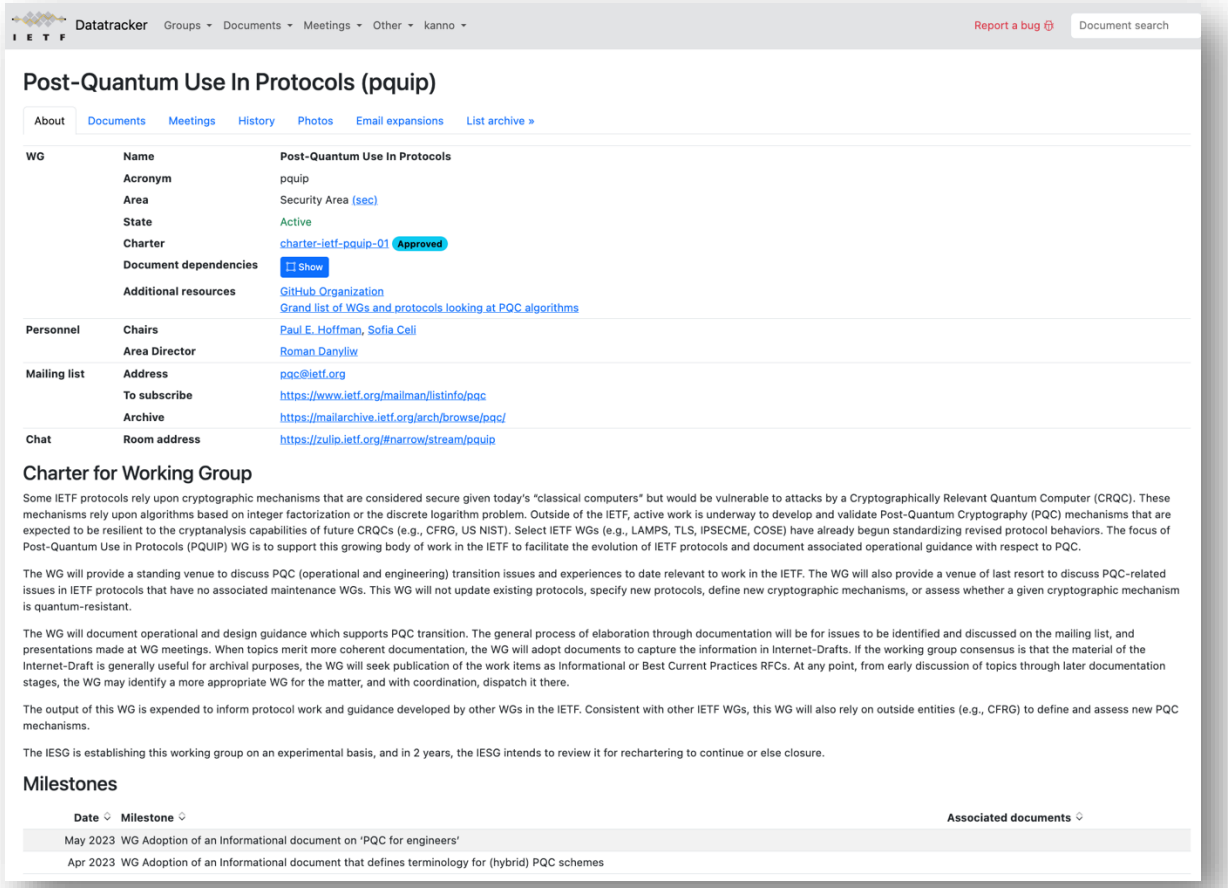
- IETF/IRTFで主にPQCが関係するWG/RGは以下のとおり（**太字**）

	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



Datatracker Groups Documents Meetings Other kanno Report a bug Document search

Post-Quantum Use In Protocols (pquip)

About | Documents | Meetings | History | Photos | Email expansions | List archive »

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, IPSECME, 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	

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

- 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

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*

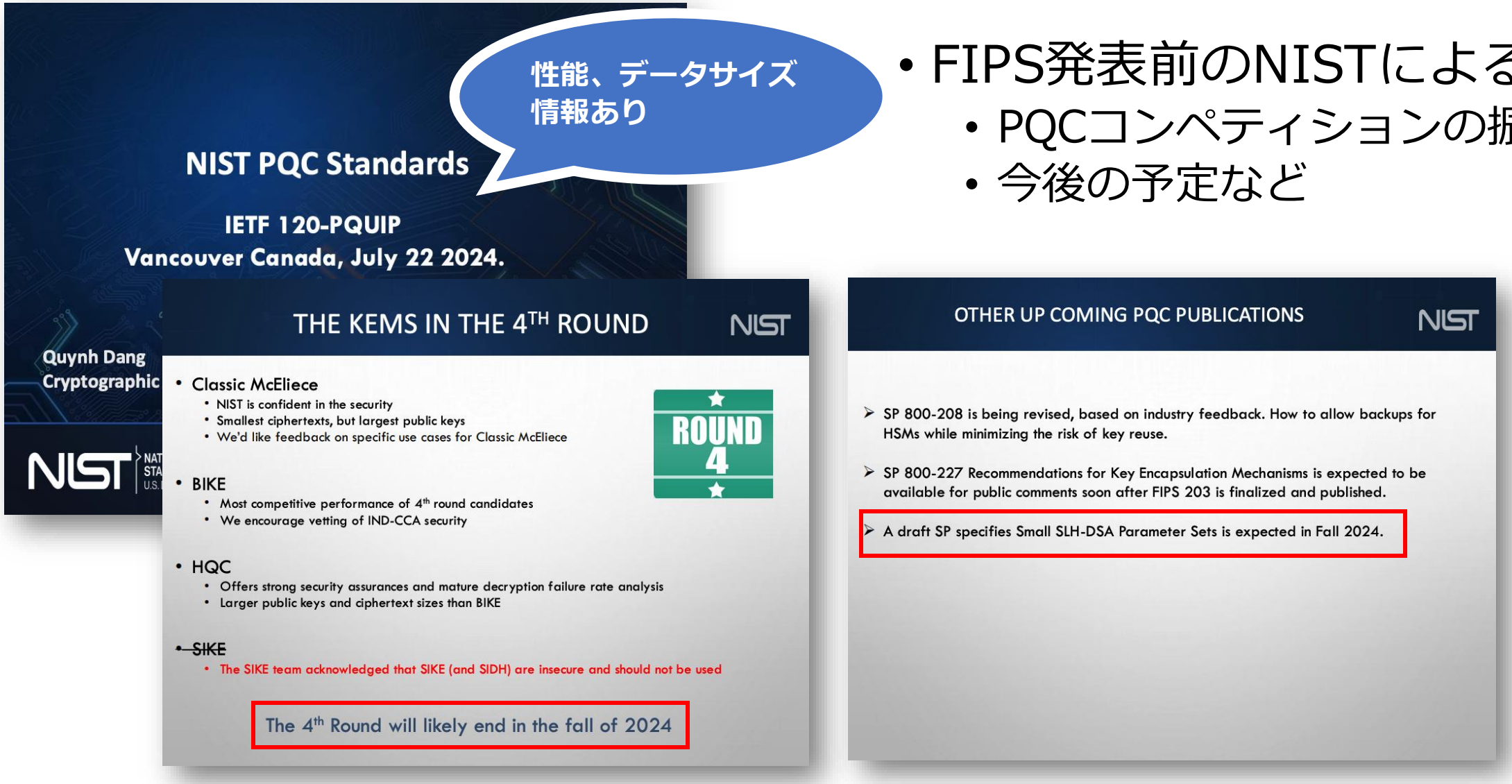
Post-Quantum Cryptography for Engineers

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/

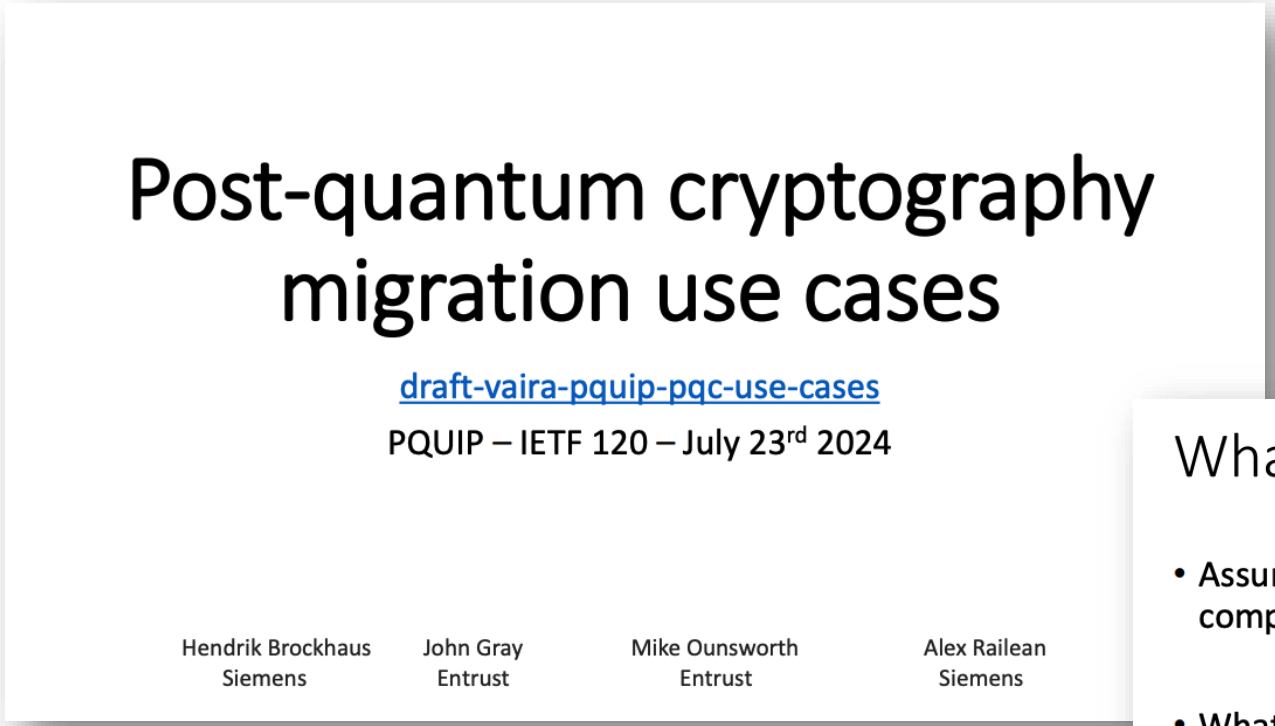
PQUIP WGでの議論（1/3）



- 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

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

PQUIP WGでの議論（2/3）



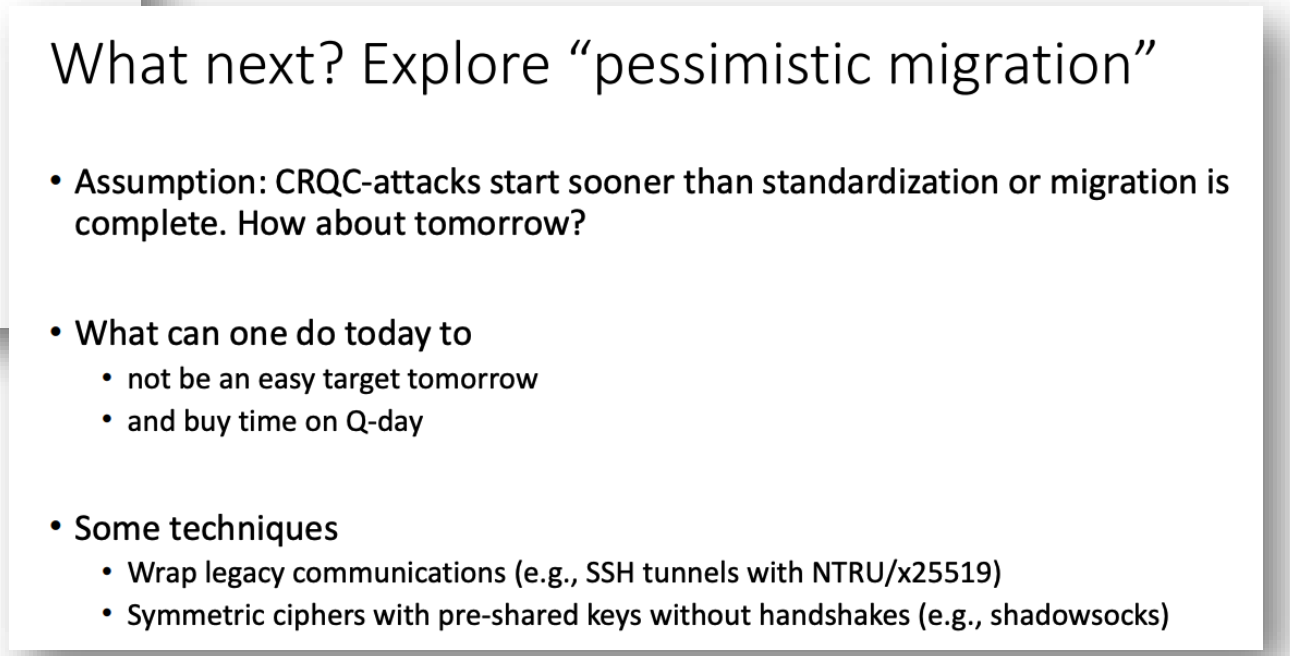
Post-quantum cryptography migration use cases

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



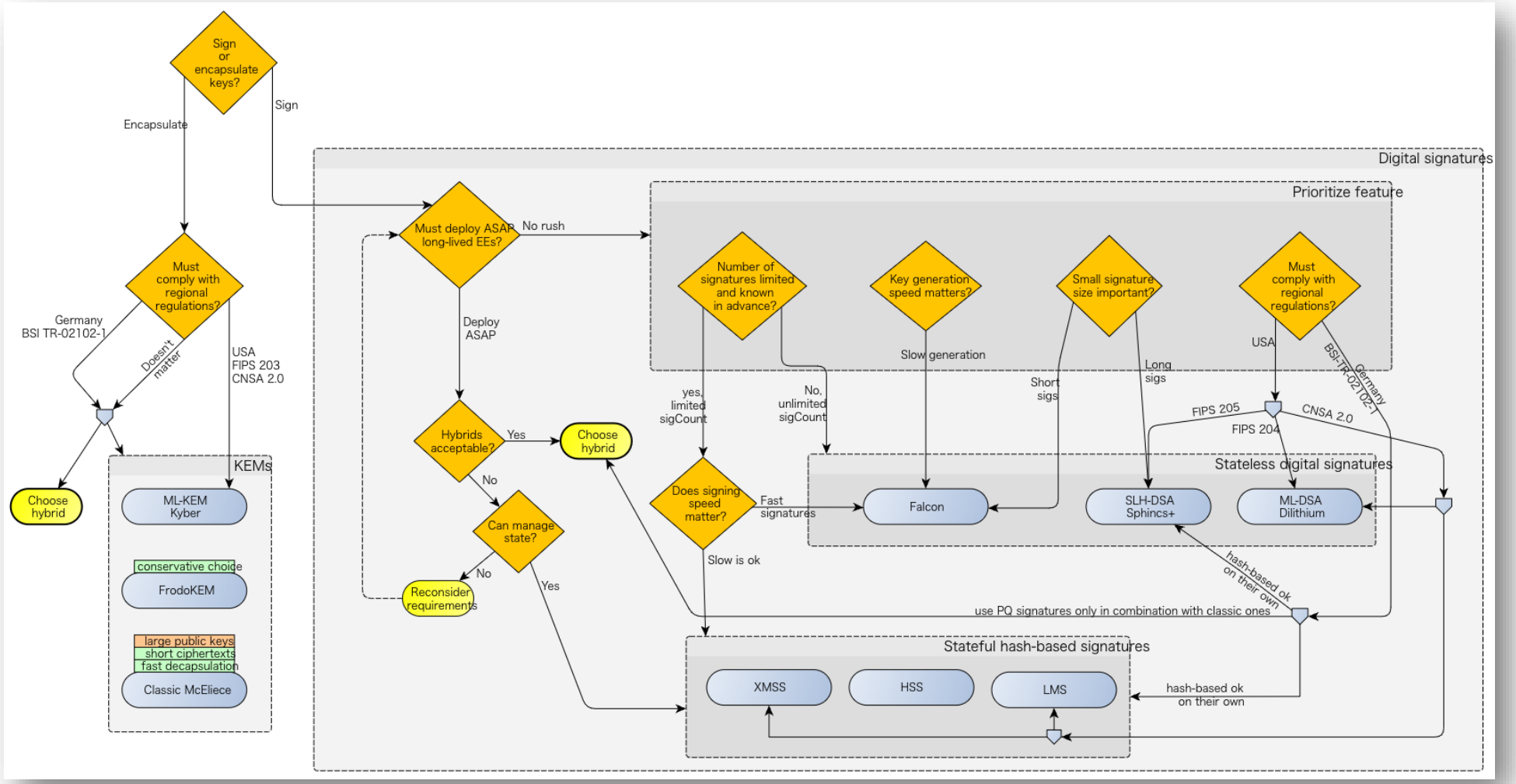
What next? Explore “pessimistic migration”

- 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）

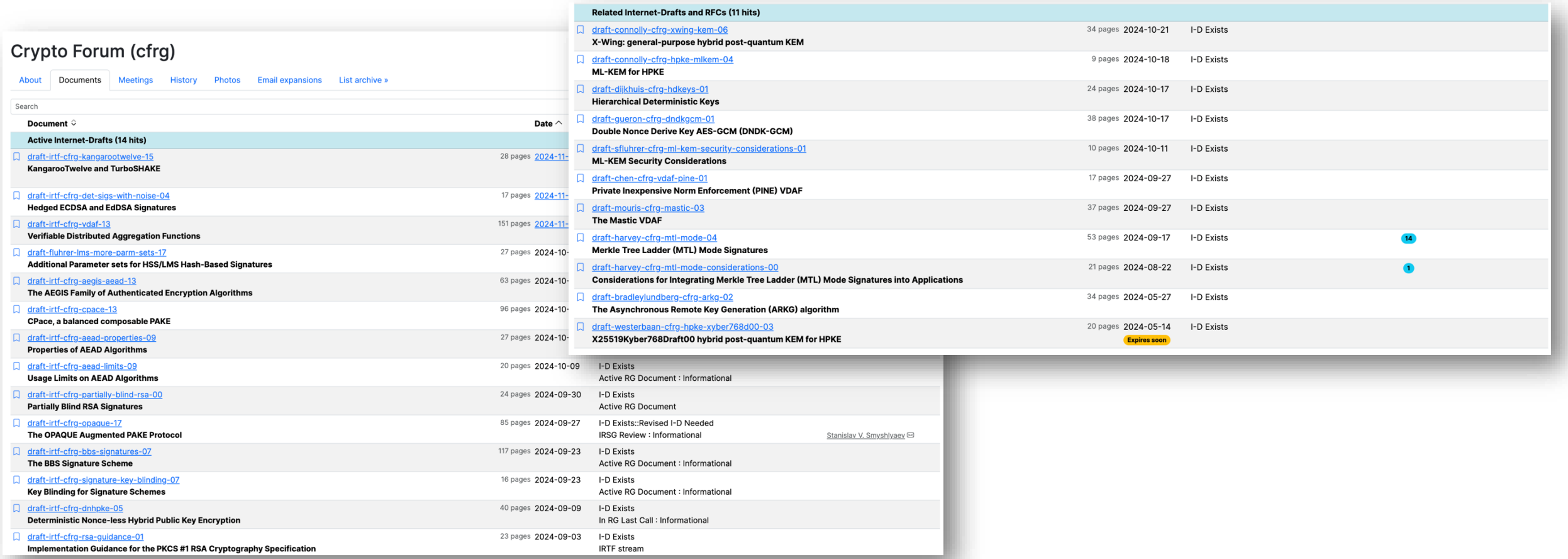
- 移行先のPQCを決定するための検討フローも検討されている



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

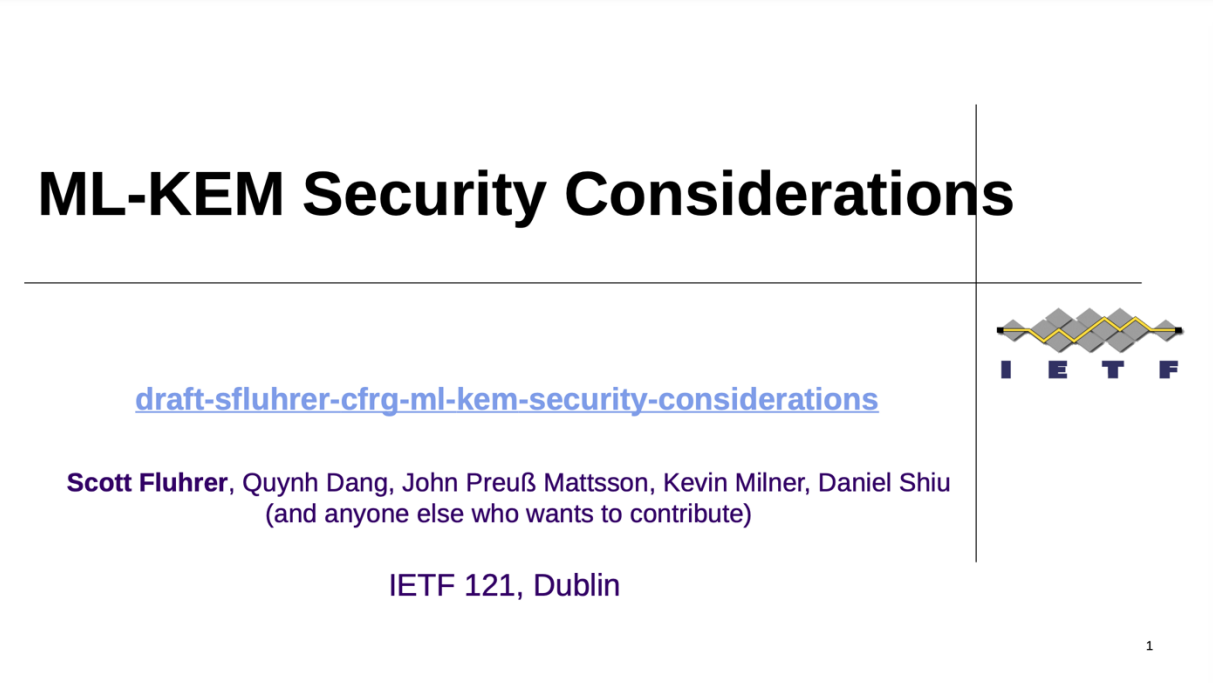
Document	Date		
Active Internet-Drafts (14 hits)			
draft-irtf-cfrg-kangarootwelve-15 **KangarooTwelve and TurboSHAKE**	28 pages	2024-11-	
draft-irtf-cfrg-det-sigs-with-noise-04 **Hedged ECDSA and EdDSA Signatures**	17 pages	2024-11-	
draft-irtf-cfrg-vdaf-13 **Verifiable Distributed Aggregation Functions**	151 pages	2024-11-	
draft-fluhrer-lms-more-parm-sets-17 **Additional Parameter sets for HSS/LMS Hash-Based Signatures**	27 pages	2024-10-	
draft-irtf-cfrg-aegis-aead-13 **The AEGIS Family of Authenticated Encryption Algorithms**	63 pages	2024-10-	
draft-irtf-cfrg-cpace-13 **CPace, a balanced composable PAKE**	96 pages	2024-10-	
draft-irtf-cfrg-aead-properties-09 **Properties of AEAD Algorithms**	27 pages	2024-10-	
draft-irtf-cfrg-aead-limits-09 **Usage Limits on AEAD Algorithms**	20 pages	2024-10-09	I-D Exists Active RG Document : Informational
draft-irtf-cfrg-partially-blind-rsa-00 **Partially Blind RSA Signatures**	24 pages	2024-09-30	I-D Exists Active RG Document
draft-irtf-cfrg-opaque-17 **The OPAQUE Augmented PAKE Protocol**	85 pages	2024-09-27	I-D Exists::Revised I-D Needed IRSG Review : Informational Stanislav V. Smyshlyaev
draft-irtf-cfrg-bbs-signatures-07 **The BBS Signature Scheme**	117 pages	2024-09-23	I-D Exists Active RG Document : Informational
draft-irtf-cfrg-signature-key-blinding-07 **Key Blinding for Signature Schemes**	16 pages	2024-09-23	I-D Exists Active RG Document : Informational
draft-irtf-cfrg-dnhpke-05 **Deterministic Nonce-less Hybrid Public Key Encryption**	40 pages	2024-09-09	I-D Exists In RG Last Call : Informational
draft-irtf-cfrg-rsa-guidance-01 **Implementation Guidance for the PKCS #1 RSA Cryptography Specification**	23 pages	2024-09-03	I-D Exists IRTF stream

Related Internet-Drafts and RFCs (11 hits)				
draft-connolly-cfrg-xwing-kem-06 **X-Wing: general-purpose hybrid post-quantum KEM**	34 pages	2024-10-21	I-D Exists	
draft-connolly-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-mtl-mode-04 **Merkle Tree Ladder (MTL) Mode Signatures**	53 pages	2024-09-17	I-D Exists	14
draft-harvey-cfrg-mtl-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 Expires soon	I-D Exists	

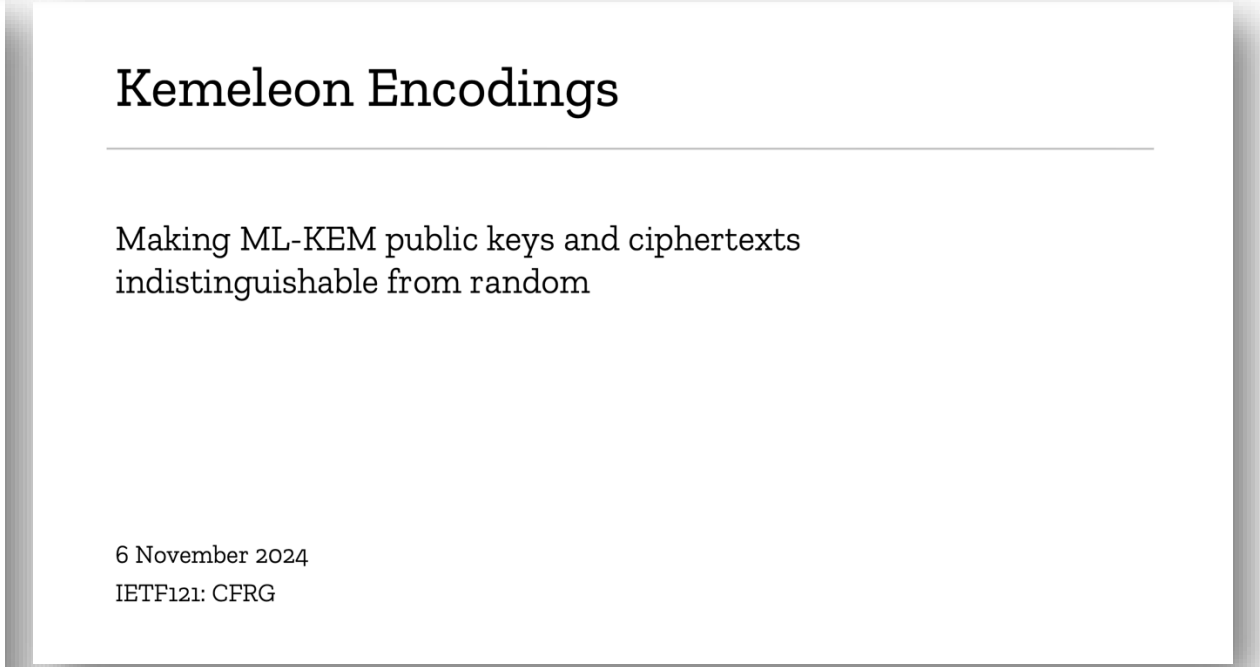
https://datatracker.ietf.org/rg/cfrg/about/

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たちが多い！



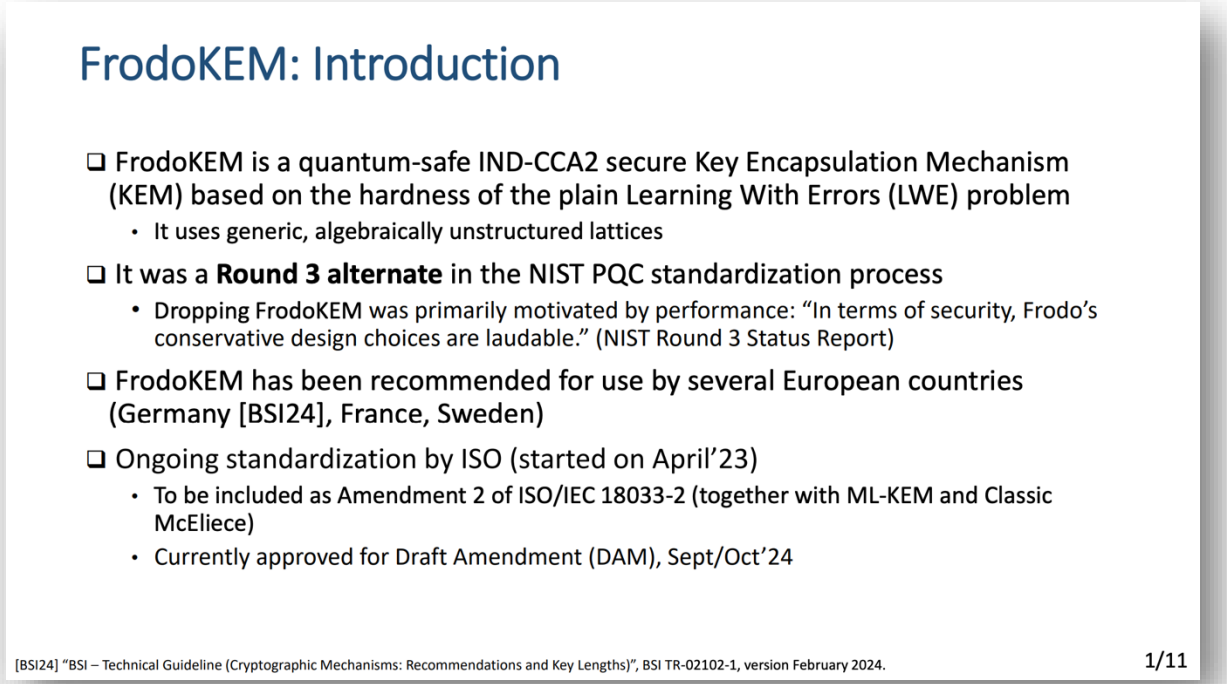
https://datatracker.ietf.org/meeting/121/materials/slides-121-cfrg-ml-kem-00



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

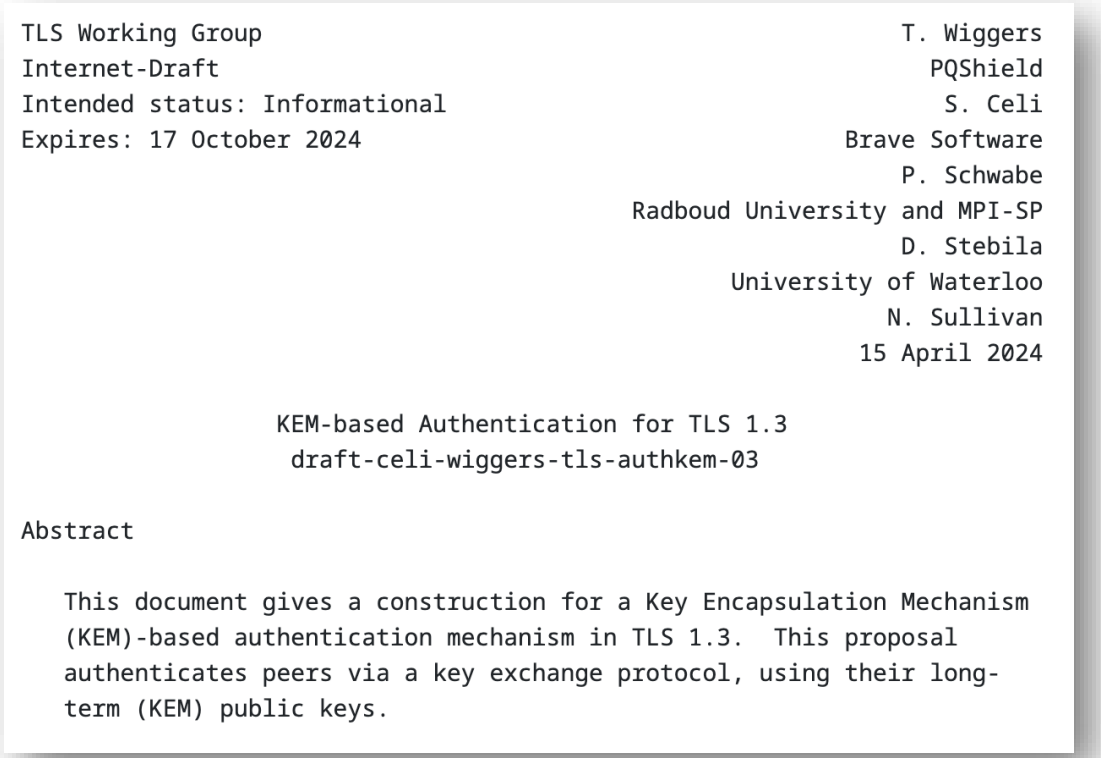
CFRGでの議論（2/2）

- 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



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)

GMO CYBER SECURITY IERAE

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)

GMO CYBER SECURITY IERAE

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

現行暗号と比較したPQCの成熟度って、どう？！

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 PQC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, SPHIN

Round 4 Candidates (全てKEM) については最大24ヶ月間の評
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 PQC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…ｺﾞｸﾘ

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 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
7	3	2	2	1	2	7	6	4	1	5
10		7								
40										

現行暗号と比較したPQCの成熟度って、どう？！

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

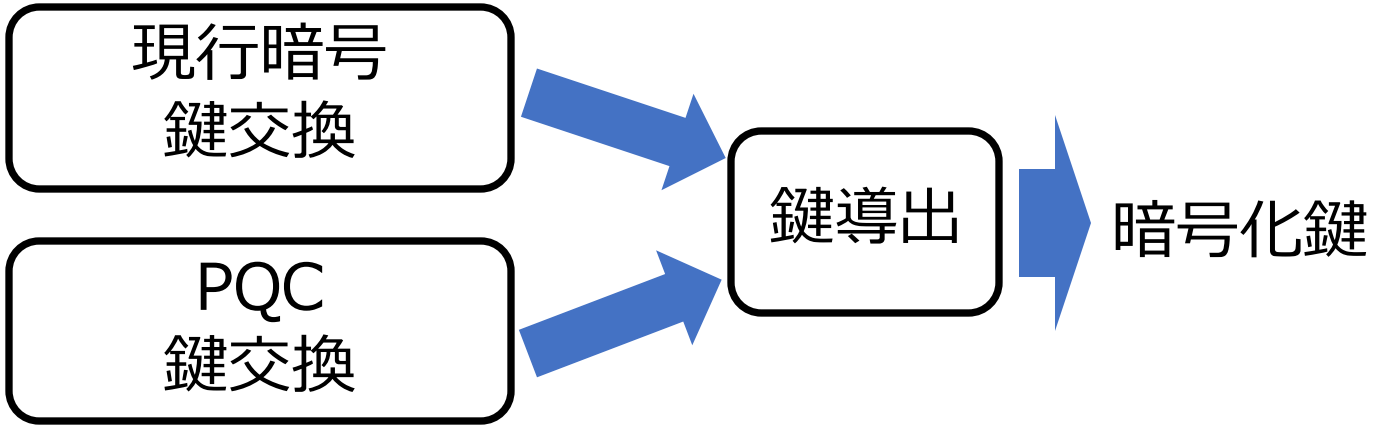
PQCを利用する際に完全に成熟するまで待たずに開始すべし！

「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

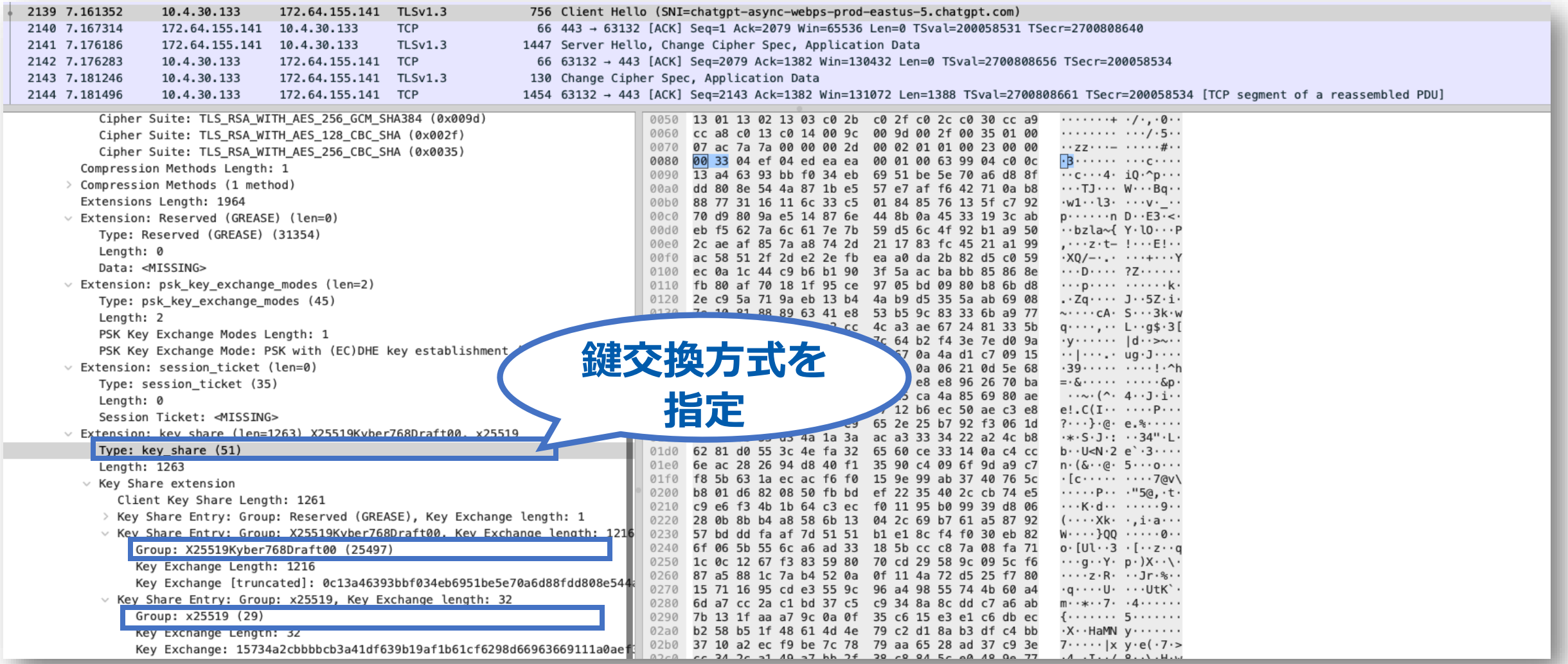
Some Google Chrome users report having issues connecting to websites, servers, and firewalls after Chrome 124 was released last week with the new quantum-resistant X25519Kyber768 encapsulation mechanism enabled by default.

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/

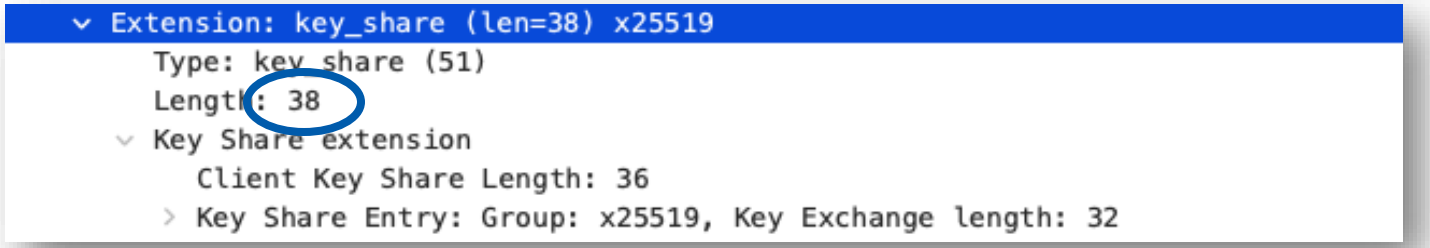
秘孔を突いたデータ (key share) って？



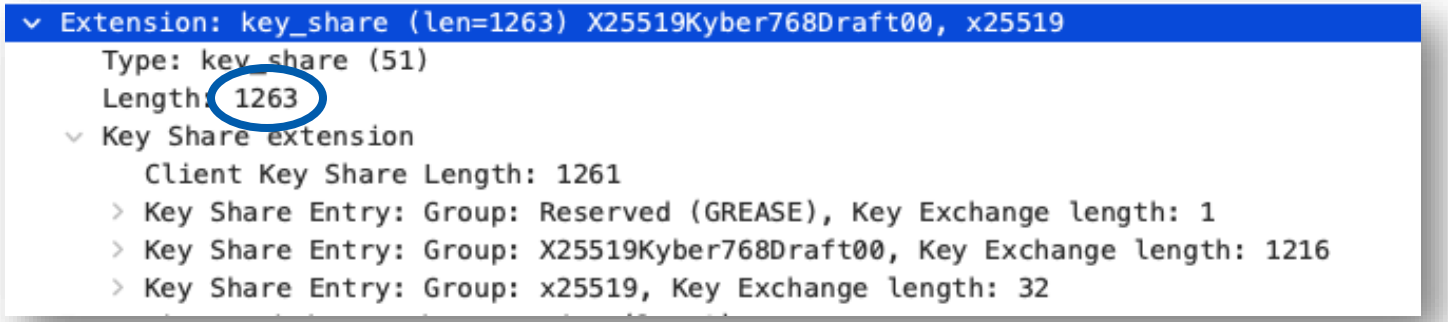
https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

実際、どの程度大きいの？

<現行暗号 X25519での鍵交換>



<Hybrid:X25519Kyber728での鍵交換>

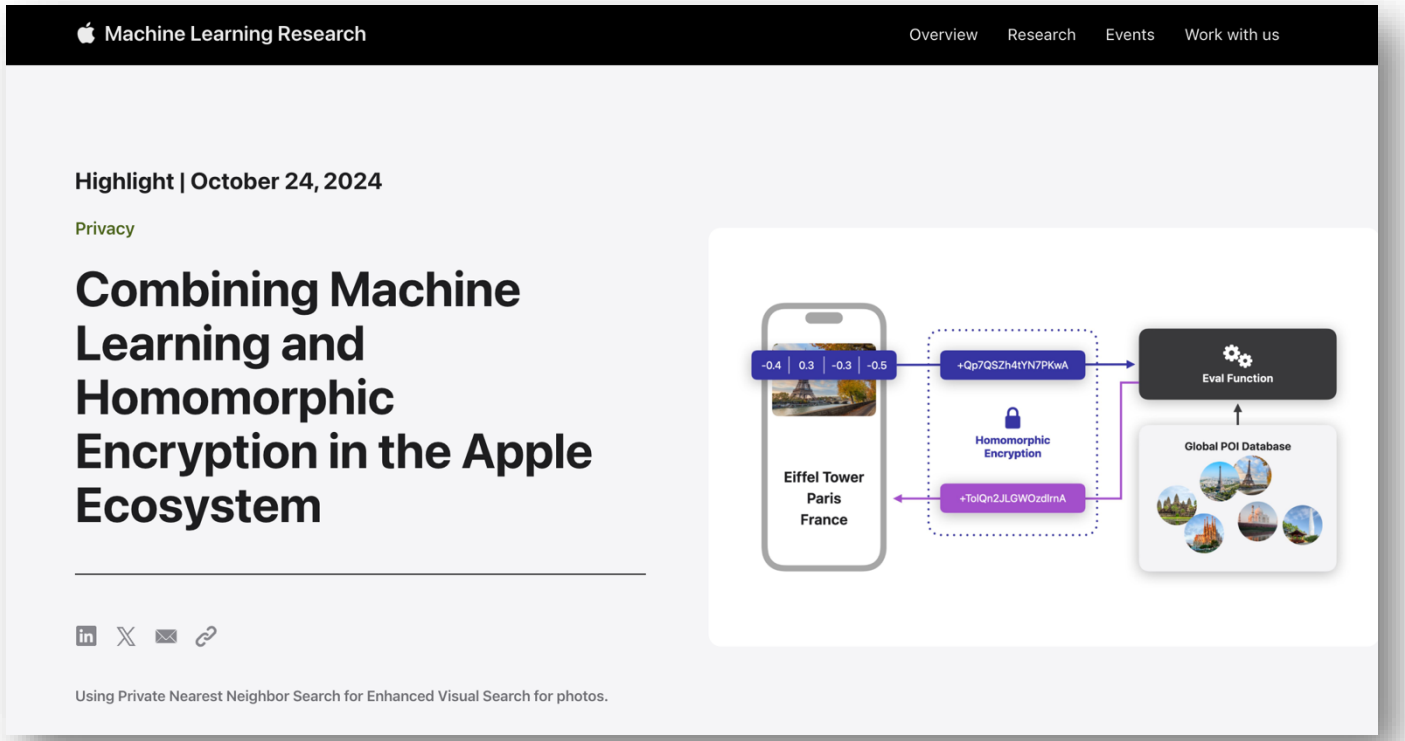


33倍以上巨大化！！

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



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

ここで利用されている

“Homomorphic Encryption”
(準同型暗号)

Brakerski/Fan-Vercauteren (BFV)

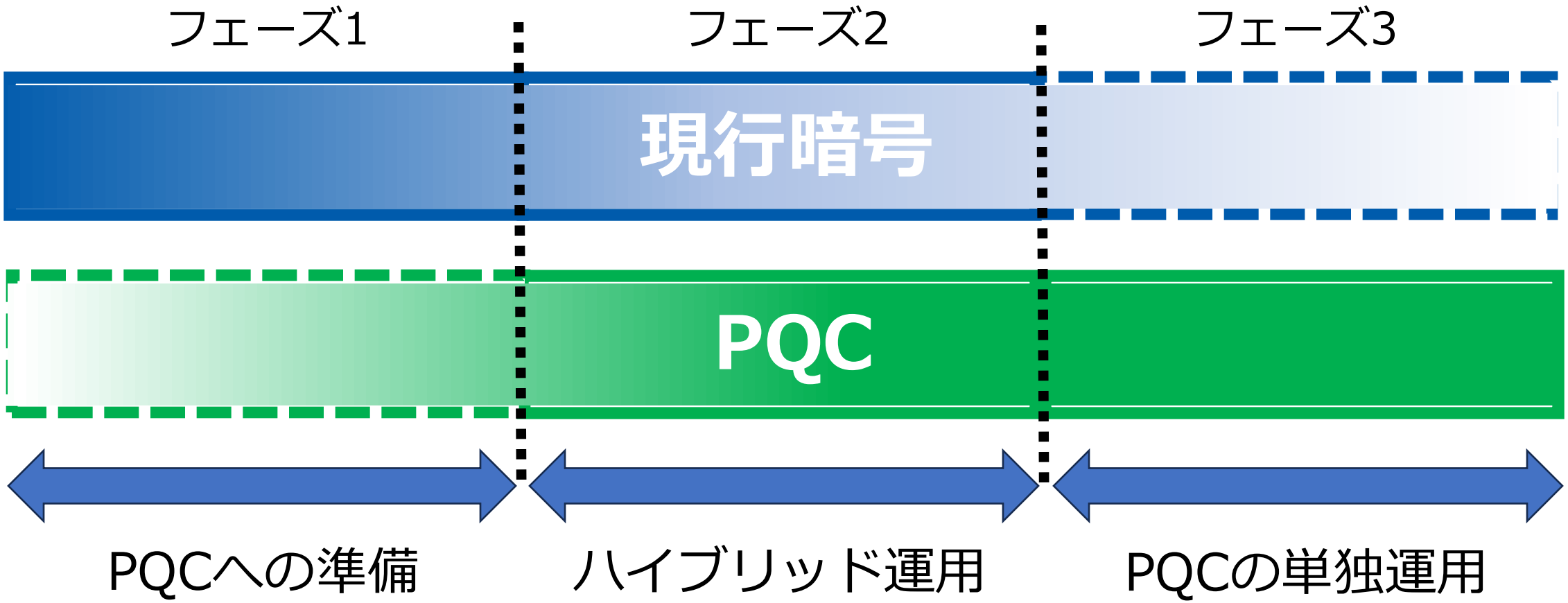
Ring Learning With Errors (RLWE) 問題を安全性の根拠とした**耐量子暗号（PQC）**

⋮

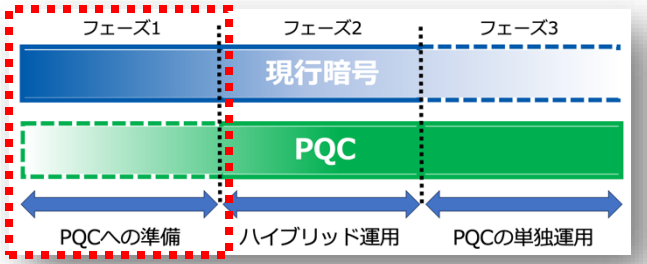
NISTが**選定した以外の**
PQCもあるから要注意！！

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

Crypto Agility

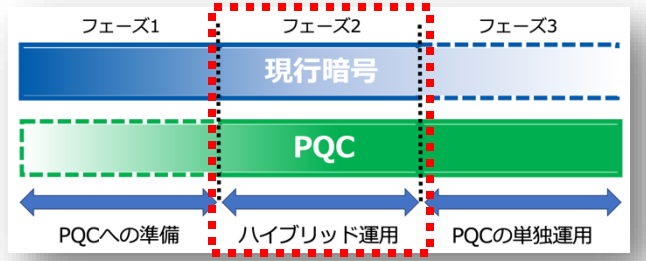
- 暗号移行に関するところに、いつも顔を出す「Crypto Agility」

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～）

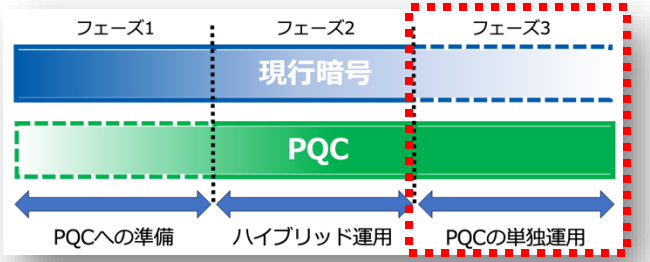


- 基本方針：PQCへの信頼を醸成
  - ハイブリッドは必須！
    - キモチ：現行暗号を保証するためにハイブリッドは重要なまま
  - ユースケースによってはPQCは必須事項へ
- 対応すべきPQCが揃い踏み？！
  - NIST以外にもPQCの基準リストを公開
    - 組織例：仏 ANSSI
    - アルゴリズム例：
      - 格子ベース（KEM）：Crystals-Kyber, FrodoKEM
      - 格子ベース（署名）：Crystals-Dilithium, Falcon
      - ハッシュベース（署名）： XMSS/LMS, SPHINCS+

※ 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