

ホットトピック

ハッカソンレポート（超低遅延暗号） ・ 暗号技術動向

酒見 由美

GMOサイバーセキュリティ by イエラエ
GMO Internet Group Developer Expert

2023年8月28日

自己紹介

- 名前：酒見 由美（暗号のおねえさん）
 - E-mail: yumi.sakemi@gmo-cybersecurity.com
 - Twitter: @ysakemin
- 経歴：
 - 株式会社 富士通研究所（現 富士通株式会社）
 - 株式会社レピダム（現 GMOサイバーセキュリティ byイエラエ）
- 現在のミッション
 - 「インターネット X 先端の暗号技術」で安全かつ便利な世界を目指して活動
 - 先端技術 x UX/UIデザインで「難解な技術をわかりやすく実装」
 - 例：検索可能暗号を適用したチャットサービス/ストレージサービス
 - IETF CFRGでペアリング曲線の標準化活動中

新規サービス開発の
ご相談もぜひ！



- [メイン]IETF117 Hackathonでの活動
 - IETF117 Hackathonの紹介
 - 何をターゲットにしたの？
 - 本活動での成果
- IETF117 暗号技術関連
 - PQC関連のPQUIP WGを中心に

こちらのトピックは当日の諸事情により、
カットとなったため、
スライドのみ情報公開します😊

• IETF117 Hackathon & Security Area / IRTF での暗号技術関連

IETF 117 Meeting Agenda
San Francisco, July 22 - 28, 2023

Agenda | Floor plan | Plaintext

Schedule | Timezone: Meeting | Local | UTC | America - Pacific Time - Los Angeles

Note: IETF agendas are subject to change, up to and during a meeting.

Information about side meeting signups is available on the [side meetings wiki](#). Please see the [meeting page](#) for more information.

Time	Location	Event
2023年7月22日 土曜日		
09:30 - 20:30	Plaza A-B	Hackathon
10:30 - 11:00	Plaza A-B	Hackathon Kickoff
2023年7月23日 日曜日		
09:30 - 16:30	Plaza A-B	Hackathon
14:00 - 16:00	Plaza A-B	Hackathon Results Presentations
18:00 - 20:00	Continental 4	Hot RFC Lightning Talks
2023年7月24日 月曜日		
09:30 - 11:30	Monday Session I	
Golden Gate 7-8	SEC lake	Light Authentication
Golden Gate 6	SEC radest	RADIUS Extension
Continental 8-9	SEC scott	Supply Chain Integrity, Transparency, and Trust
13:00 - 15:00	Monday Session II	
Plaza A	SEC cose	CBOR Object Signing and Encryption
15:30 - 17:00	Monday Session III	
Golden Gate 6	SEC privacypass	Privacy Pass
Continental 4	SEC suit	Software Updates for Internet of Things
17:30 - 18:30	Monday Session IV	
Continental 8-9	SEC acme	Automated Certificate Management Environment
Plaza A	SEC ppm	Privacy Preserving Measurement
18:30 - 19:30	Golden Gate 2-3	Hackdemo Happy Hour
2023年7月25日 火曜日		
09:30 - 11:30	Tuesday Session I	
Plaza A	SEC keytrans	Key Transparency BoF
Plaza A	SEC oauth	Web Authorization Protocol
13:00 - 14:30	Tuesday Session II	
Plaza B	SEC pqqip	Post-Quantum Use In Protocols

Hackthon: 22~23日
セキュリティ・暗号技術関連WG/RG:
27

2023年7月26日 水曜日

15:00 - 16:30 Tuesday Session III

- Continental 6 IRTF cfrg Crypto Forum
- Golden Gate 7-8 SEC jose Javascript Object Signing and Encryption
- Golden Gate 6 SEC teep Trusted Execution Environment Provisioning

17:00 - 18:00 Tuesday Session IV

- Continental 6 SEC secdispatch Security Dispatch

2023年7月27日 木曜日

09:30 - 11:30 Wednesday Session I

- Golden Gate 7-8 SEC oauth Web Authorization Protocol
- Continental 8-9 SEC rats Remote Attestation Procedures

13:00 - 15:00 Wednesday Session II

- Continental 6 SEC tls Transport Layer Security

15:30 - 17:00 Wednesday Session III

- Golden Gate 6 SEC ipsecme IP Security Maintenance and Extensions
- Continental 4-6 IETF plenary IETF Plenary

17:30 - 19:30 Wednesday Session IV

- Continental 5 SEC dtut Detecting Unwanted Location Trackers **BoF**

19:30 - 11:30 Wednesday Session V

- Continental 5 SEC spkts Next Speaker Series
- Continental 5 SEC saag Security Area Open Meeting
- Continental 5 SEC mls Messaging Layer Security

2023年7月28日 金曜日

09:30 - 11:30 Friday Session I

- Continental 5 IRTF pearg Privacy Enhancements and Assessments Research Group
- Continental 4 SEC gnapp Grant Negotiation and Authorization Protocol
- Golden Gate 7-8 SEC oauth Web Authorization Protocol

12:00 - 13:30 Friday Session II

- Continental 4 SEC emu EAP Method Update
- Continental 5 SEC oshl Oblivious HTTP Application Intermediation
- Golden Gate 7-8 SEC openpgp Open Specification for Pretty Good Privacy

IETF 117 Hackathon

IETF117 Hackathonとは？

- 2015年3月開催 IETF92 Dallasからスタート
 - 成果発表として12件程度の規模感
- 開発者と各領域の専門家が協力してIETF標準に対して実用的な実装を加速化させる活動
 - 目的：
 - OSS開発のスピードと協力精神をIETFに注入して標準化活動のスピードと関連性を向上
 - 開発者や若手にIETFに参加してもらい興味を持ってもらう
- 取り扱われているテーマ
 - DNS、FD.io/VPP、HTTP 2.0、NETVC、OpenDaylight、ONAP、RioT、QUIC、TLS 1.3、WebRTC、YANG/NETCONF/RESTCONF など、ほぼすべての IETF 作業領域にわたる幅広いトピック

<https://www.ietf.org/how/runningcode/hackathons/>

IETF117 Hackathonの概要

meeting / 117 / hackathon

IETF 117 Hackathon

[Edit](#) [Edit on GitHub](#)

IETF 117 Hackathon

The Internet Engineering Task Force (IETF) is holding a hackathon to encourage developers and subject matter experts to discuss, collaborate, and develop utilities, ideas, sample code, and solutions that show practical implementations of IETF standards.

When: Saturday - Sunday, 22-23 July 2023

Where: Hilton Union Square, San Francisco, CA, USA

Room: [Plaza A-B, Lobby Level](#)

Sponsored by

Gold Running Code Sponsor Silver Running Code Sponsor Bronze Running Code Sponsor

[Sign up for the Hackathon](#)

<スケジュール>

- ・ 2023年7月22日朝 ~ 23日 昼まで
- ・ 最後に成果報告 (最大3分/pj)あり

<Hackathon概要>

- ・ 参加プロジェクト数: 33
- ・ プロジェクトにはChampionが必須
- ・ 参加数 : **423**名(362 on-site, 61 remote)



<https://wiki.ietf.org/en/meeting/117/hackathon>

IETF117 Hackathon: Road to Champion

- IETF Hackathon で実施したいことがある人はWikiに記入が必要
 - Champion(=発起人)やプロジェクトの概要をWikiに登録
 - なお、Champion以外としても参加可能

Participant Preparation and Prerequisites

Project Teams and Champions

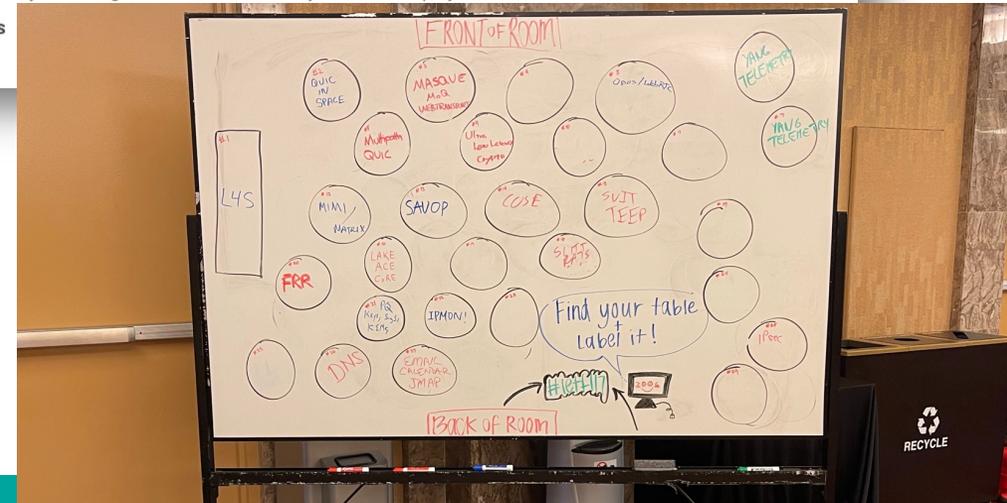
- ▶ Champions are the leads for individual projects in the Hackathon
- ▶ Champions are individuals familiar with a given technology who volunteer to help get others get up and running with that technology
- ▶ Before the Hackathon, champions should:
 - ▶ Add information about your project to the list of [Projects included in Hackathon](#)
 - ▶ Recruit participants from associated working groups, open source projects, etc. Announcing your projects via an email to (hackathon@ietf.org) can be helpful as well.
 - ▶ Specify when and how the project team will meet on the [Team Schedule](#)
- ▶ At the Hackathon, champions should:
 - ▶ Make themselves available to answer questions and help others
 - ▶ Hack on things themselves in their copious free time
- ▶ Additional projects are welcome at any time. For any questions, contact the chairs at (hackathon-chairs@ietf.org)

<https://wiki.ietf.org/en/meeting/117/hackathon>

Ultra-Low Latency Cryptography

- ▶ Champion(s)
 - ▶ Yumi Sakemi (yumi.sakemi@gmo-cybersecurity.com)
 - ▶ Satoru Kanno (satoru.kanno@gmo-cybersecurity.com)
- ▶ Project Info
 - ▶ In future communication technologies such as 6G, there are technical requirements that demand ultra-low latency and high levels of security. So, the purpose of this project is to achieve low-latency and highly secure cryptographic techniques targeting future communication technologies.
 - ▶ At the IETF117 Hackathon, we will take on the challenge of extending OpenSSL with the low-latency cryptographic technique "Areion".
 - ▶ Paper at <https://tches.iacr.org/index.php/TCHES/article/view/10279/9727>
 - ▶ We are currently recruiting collaborators who will join us in this project.
- ▶ Specifications
 - ▶ TBD

超低遅延暗号PJ



- Beyond 5G研究開発促進事業に採択されているため



2022年度評価で
最高ランク「S」を獲得！

国立研究開発法人情報通信研究機構（NICT）のうち、令和4年度新規委託研究の公募（第1回）「Beyond 5G国際共同研究型プログラム」及び採択しました。

(ウ) Beyond 5Gシーズ創出型プログラム

(1) 上空プラットフォームにおけるCPSを活用した動的エリア最適化技術^{※1}

提案者：ソフトバンク株式会社（代表提案者）、学校法人慶應義塾

[概要表示](#)

(2) リアルタイム暗号技術とプライバシー保護への拡張^{※1, ※3}

提案者：兵庫県立大学法人兵庫県立大学（代表提案者）、GMOサイバーセキュリティ byイセラエ株式会社

[概要非表示](#)

概要：センシング機器向けの「リアルタイム暗号化技術」の開発を行う。具体的には、量子計算機による攻撃にも耐性のあるサブナノ級超低遅延暗号を開発する。この技術をセンシング機器に組み込みことで、フィジカル空間で取得したセンシングデータを、超低遅延でサイバー空間に転送可能となり、サイバー空間とフィジカル空間で安全かつシームレスなデータ連携が可能となる。さらに暗号化したままで統計処理や機械学習が可能な秘密計算等とのハイブリッド利用可能な技術に拡張することで、超多数接続においてもプライバシー保護を可能とする。同時に「標準化」と「知財化」を戦略的に進め、2030年までにBeyond 5Gにおけるサービスの高度化に寄与する。

<https://www.nict.go.jp/publicity/topics/2022/08/05-1.html>

- 低遅延暗号が必要な技術背景

- 通信技術の発展により、将来のインターネットで利用される暗号技術への**高い安全性や要件の高度化**

- 低遅延性や高速大容量通信など

- 例

- NIST SP800-38Aのパブリックコメントでの例

- MicrosoftやAmazonから、現行のAES-GCMのような128-bitブロック暗号の利用の限界について示された

- **将来的に192-bitや256-bitブロック暗号の必要性を言及**

- メディア通信向けE2EE通信のメカニズムであるSFrameでは、ハッシュ処理の性能の限界が原因で送信者ごとの認証が提供されていない

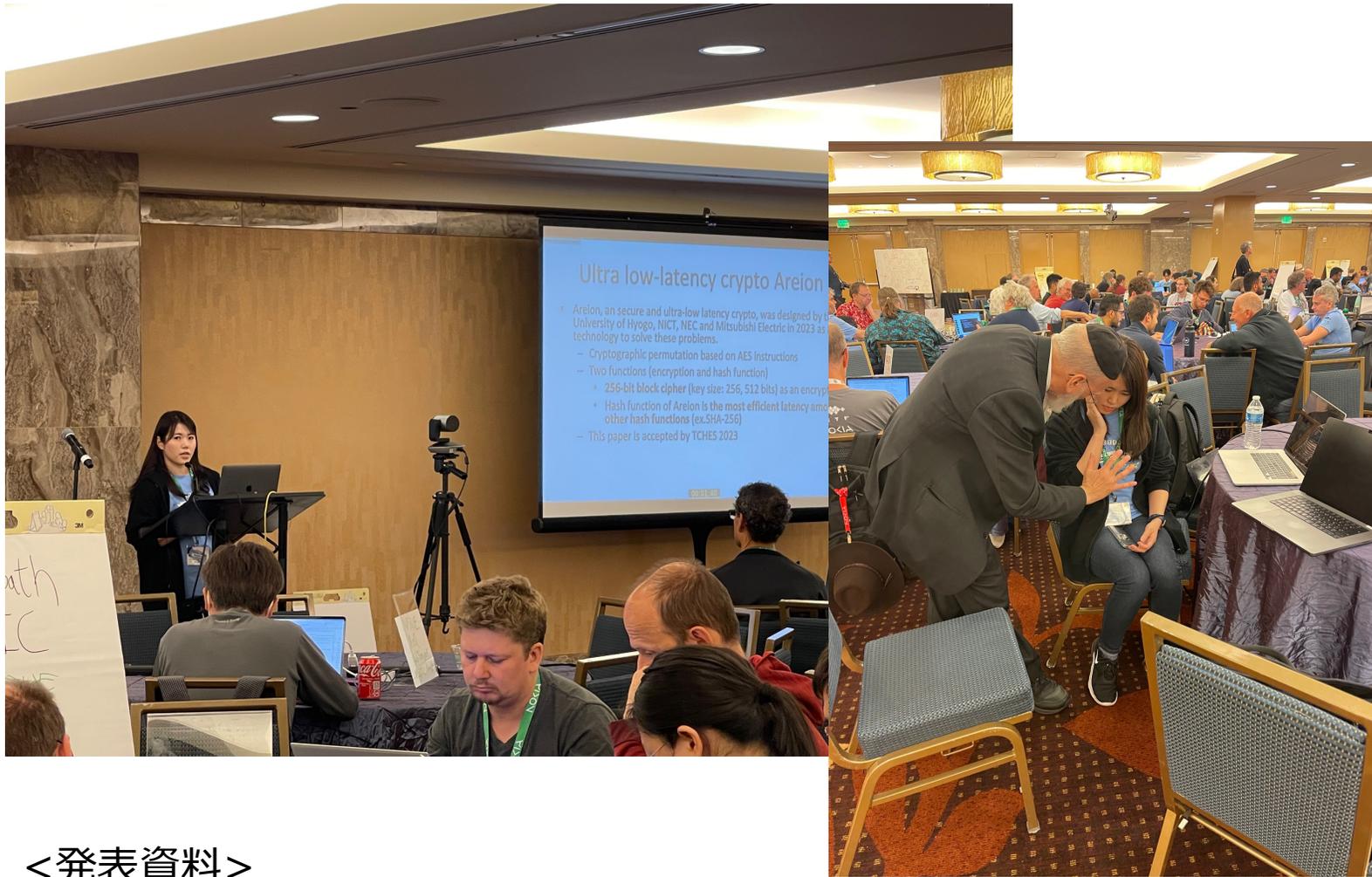
- Internet-Draftのsecurity considerationsにも言及あり

- **低遅延なハッシュ処理を実現する技術が必要**

• 低遅延暗号Areionとは？

- 2023年に兵庫県立大学、NICT、NECおよび三菱電機が共同で開発した安全かつ低遅延な共通鍵暗号技術
 - 暗号業界のトップカンファレンス国際会議 TCHES2023で採録
 - AES命令ベース(AES-NIなど)の暗号的置換アルゴリズム
 - 暗号化とハッシュ化の2つの機能に応用可能
 - 暗号
 - **256-bit ブロック暗号**(256ビット、512ビットの鍵サイズ)
 - ハッシュ
 - 現在主要なSHA256などの他のハッシュ関数と比べて**最速**！
 - 論文での実験結果を参照

- Hackathonでの活動目標
 - Areionを適用したQUICの実現を目標とし、その中間ゴールとしてTLS1.3への適用にチャレンジ
 - TLS1.3の実装物としては、広く利用されているOpenSSLベースのquictlsを採用
- 成果
 - quictlsに用意されているTLS向けサンプルコードを使ってAreionを用いたTLS1.3接続ができることを確認！
 - GitHub :
 - <https://github.com/gmo-ierae/areion-openssl/tree/3.1.0+quic+areion>



• 発表内容

- 新規PJのため、背景からハッカソンの目標、成果などを発表

• 発表後の反応

- 発表直後に質問・コメントがあり、会期中も多数声かけいただいた

• 今後の活動

- 適用先、標準化対象のアルゴリズム選定&実装

- OpenSSL(speed対応)、ハッシュ

<発表資料>

<https://github.com/IETF-Hackathon/ietf117-project-presentations/blob/main/Ultra-Low-Latency-Crypto-Areion.pdf>

IETF 117 暗号技術動向

IETF117での暗号技術動向（概要）

- IETF117でのセキュリティ全般・暗号・プライバシー関連WG/RG
 - BoFやIRTFのRGも含めて、計27WG/RGが開催された
- 暗号プリミティブ関連
 - cfrg
- 耐量子計算機暗号(PQC)移行関連
 - pquip、lampsなど
- プライバシー保護関連
 - privacypass、ppm、peargなど

SEC	acme	cose	dult BoF	emu	gnap	ipsecme	jose	keytrans BoF	lake	lamps	mls	oauth	ohai	openpgp	ppm	pquip	privacypass	radext	rats
	saag	scitt	secdispatch	suit	teep	tls	25WG(Bofを含む)												
IRTF	anrw	cfrg	coinrg	dinrg	gaia	hrpc	iccr	irtfopen	maprg	nmg	pearg	ufmrg							

<https://datatracker.ietf.org/meeting/117/agenda>

- PQUIP (Post-Quantum Use in Protocols)

- 目的

- 現行暗号からPQCへの移行をサポートする運用及び設計のガイダンスの文書化
 - 新しい暗号メカニズムの定義や量子耐性の評価はスコープ外

- 議題の例

- PQC移行に関し、量子計算機が現行システムに与える影響やPQCへの移行の必要性に関するエンジニア向けガイダンスのまとめ方
- 関連するIETFプロトコルでのPQC利用の動向
- IETFプロトコルにおけるPQC関連の問題はなんでも(最終手段の場合)

- 設立時期

- IETF116 (2023年3月)からWGが開催された

が今回 注目した発表

Agenda

- Intro and Note Well (5 min)
- Hybrid terminology document (15 min)
 - draft-ietf-pquip-pqt-hybrid-terminology-00
- PQC for Engineers document (30 min):
 - <https://datatracker.ietf.org/doc/draft-ar-pquip-pqc-engineers>
- Grand list of WGs and protocols looking at PQC algorithms (10 minutes):
 - <https://github.com/ietf-wg-pquip/areas-of-interest/blob/master/README.md>
- Deployment of Post-Quantum Cryptography, Sophie Schmieg (15 minutes)
- LAMPS update on PQC (15 minutes)
- All other WG business



<https://datatracker.ietf.org/meeting/117/materials/slides-117-pquip-chair-slides>

README.md

Protocol-independent algorithm or cryptography specifications

Draft title	Link	Working Group and/or protocol	Topic	Comments
Additional Parameter sets for LMS Hash-Based Signatures	https://datatracker.ietf.org/doc/draft-fluhrer-lms-more-parm-sets/	CFRG	Parameter sets for the LMS signature primitive	
Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)	https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/	CFRG		
Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512	https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-hybrid/	Independent / CFRG	Hybrids of Streamlined NTRU Prime with X25519	
Kyber Post-Quantum KEM	https://datatracker.ietf.org/doc/draft-cfrg-schwabe-kyber/	CFRG	Description of the Kyber algorithm	
Leighton-Micali Hash-Based Signatures	https://www.rfc-editor.org/rfc/rfc8554	CFRG		RFC

• IETFにおけるPQCに関する情報が整理されており非常に重要！

• 観点

- PQCアルゴリズム
- IETFプロトコル内での利用/暗号移行
- PQC対応した際に発生するIETFプロトコルへの改善
- 実装と相互運用テストなど

このGitHubを参照すれば・・・
IETFの**技術/標準化動向が丸わかり！**

資料 : <https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc>

Contents of the draft
(資料のP.3を参照ください)

- Nokiaの技術者が中心に「技術者向けPQC」に関するI-D
- I-Dのコンテンツにあるように幅広くPQCに関する情報が整理される予定
 - 今からPQCを知りたい人には効率的に学べる予感

※関連画像を削除しております

資料 : <https://datatracker.ietf.org/meeting/117/materials/slides-117-pquip-post-quantum-cryptography-for-engineers>

Overview
(資料のP.5を参照ください)

※関連画像を削除しております

動画: https://youtu.be/rIik_BSeKTc?t=3475

資料: <https://datatracker.ietf.org/meeting/117/materials/slides-117-pquip-post-quantum-cryptography-at-google>

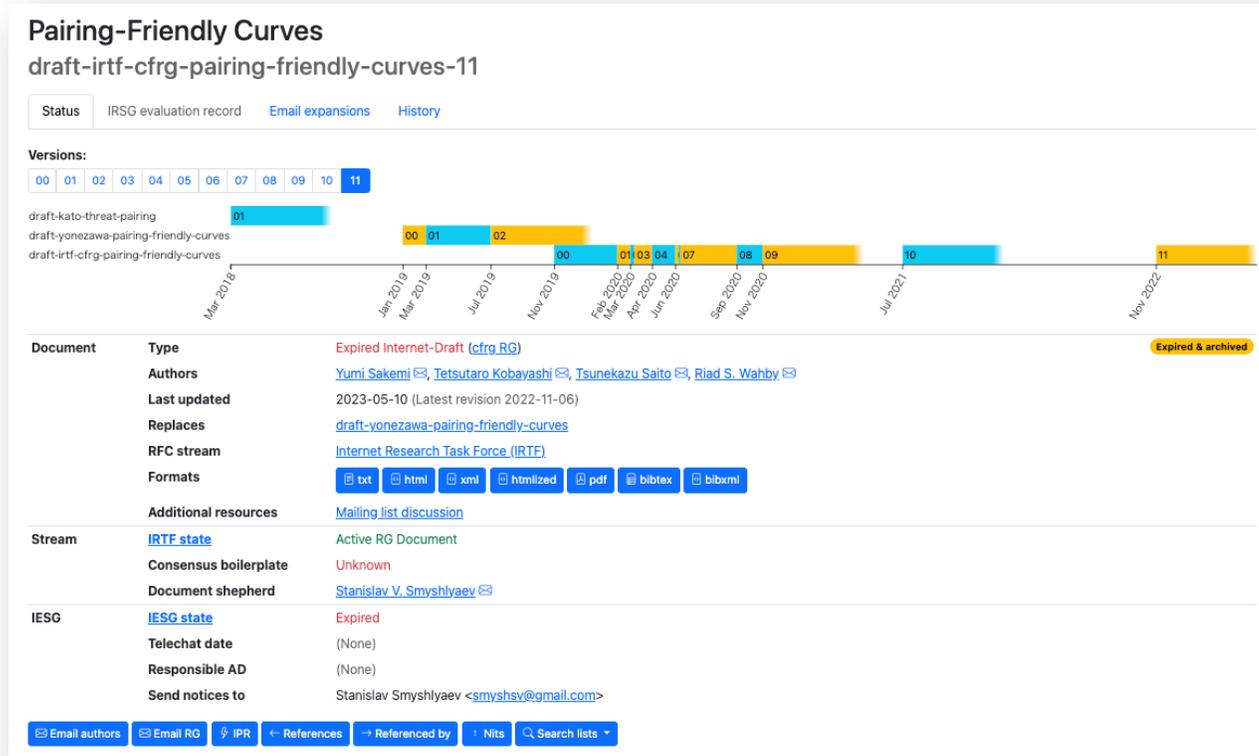
- RPC保護のためのApplication Layer Transport Security (ALTS)のPQC対応に関する話題
 - ALTSは2007年から開発開始、2017年に技術文書が公開

Googleは暗号技術に関する先駆者！ →
ChaCha20関連やNewHopeの実装

※ 興味のある方は発表資料だけだと情報が少ないのでYoutubeの参照を！

やっぱり現地参加っていいよね！な事例

- 会場を歩いていたら仲間が・・・ ✨ ✨ ✨
 - Hackathonでのプレゼンで知名度アップ（？）



- ドキュメントはExpire中
 - さまざまな事情あり(!?)
- Hackthon後の声掛けもあり、こちらのI-Dが前進しそう
- Pairing曲線が大好きなフレンドズには応援してもらいたいです！

<https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/>

これ以外にも現地参加したからこそその成果/効果は多数！

すべての人にインターネット

GMO