IETF報告会 (99th プラハ)
暗号関連報告

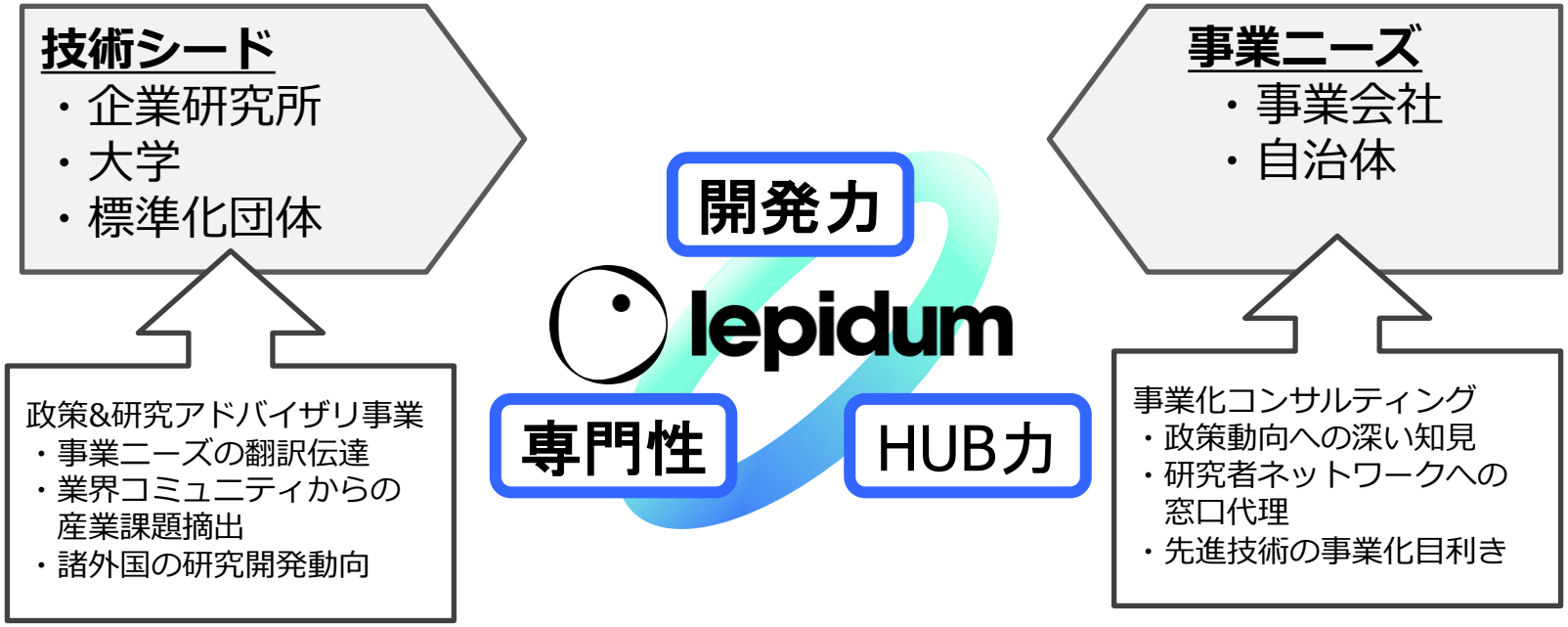
株式会社レピダム
菅野 哲

この人、誰よ？

- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - 株式会社 レピダム
  - ISOC-JP プログラム委員
- どんなことやっていた／やっているの？
  - 学生時代～
    - 暗号製品を売り歩く
    - 暗号ライブラリや暗号関連システム開発
    - 人事部で人材開発
    - 標準化活動
      - RFCを何本か発行
  - 最近は会社に関することは何でも！？

株式会社レピダムって・・・？

「エッジの効いた技術でお客様の事業を加速させる」燃料



具体的な技術領域：

標準化支援、アイデンティティ、プライバシ、認証・認可、情報セキュリティ

目的

- IETF99に参加して感じた暗号技術に関する潮流をご報告します。

- 取り上げるトピックス
  - Post-Quantum Cryptography
  - Non-NIST Approved の利用範囲拡大

IETF99 Agenda

IETF99も毎度のことながら大量のWG/RGがセッションを開催

ART	INT	IRTF	OPS	RTG	SEC	TSV	GEN
avtcore	6lo	cfrg	anima	babel	ace	alto	*iasa20*
capport	6man	gaia	bmwg	bess	acme	dtn	mtgvenue
cbor	6tisch	hrpc	dime	bier	curdle	ippm	
cdni	*banana*	iccrg	dnsop	ccamp	dots	mptcp	
cellar	dhc	icnrg	grow	detnet	i2nsf	nfsv4	
core	dmm	irtfopen	mboned	i2rs	ipsecme	quic	
dcrup	dnssd	maprg	netconf	*ideas*	lamps	rmcat	
dispatch	dprive	nfvrg	netmod	idr	mile	taps	
dmarc	homenet	nmrg	*netslicing*	isis	oauth	tcpm	
httpbis	intarea	nwcrg	opsawg	lisp	saag	tsvarea	
ice	ipwave	panrg	opsec	mpls	sacm	tsvwg	
jmap	lpwan	t2trg	radext	nvo3	secevent		
mmusic	lwig		sidrops	ospf	tls		
modern	ntp		v6ops	pals	tokbind		
netvc	tictoc			pce	trans		
perc				pim			
regext				roll			
rtcweb				rtgarea			
slim				rtgwg			
stir				sfc			
uta				teas			
				trill			

https://datatracker.ietf.org/meeting/99/agenda.html

IETF99 Agenda（暗号的フィルタ）

https://datatracker.ietf.org/meeting/99/agenda.html

暗号技術側面から見た各WG/RGの相関関係

ART Area

SEC Areaで合意された結果を参照しながら標準化を決定している

・各WG　：dcrup, uta etc.,

参照

SEC Area

IETFにおけるセキュリティに関する議論全般を実施している

・全体会合：saag

・各WG　：curdle, lamps, ipsecme etc.,

依頼

技術支援

IRTF

将来的にインターネットで必要となる技術を検討する

・RG　：cfrg

暗号技術が検討されるWG/RG

- 暗号技術の利用などについて方向感だしちゃうぞ
  - saag
    - IETF Security Areaの全体会合
    - セキュリティ全般について議論するセキュリティな人的に参加必須な場所
  - cfrg
    - 将来的にインターネットでの暗号利用や安全性について活動
    - 少し前までは、Non-NIST Approvedなアルゴリズムを検討していたが・・・
- 既存仕様の暗号技術の利用を拡張しちゃうぞ！
  - dcrup
    - DKIMを拡張（現在、RSA-sha256）
  - curdle
    - 古い暗号利用を廃止し、新しい暗号技術を追加
  - lamps
    - 現在、pkix WGやs/mime WGが完了しているが、X509に関する提案が行われているのでそれの受け皿

IETF99における個人的に受けた印象

- 大きな流れとして捉えると・・・

Post-Quantum Cryptography

&

Non-NIST Approved の
利用範囲拡大

Post-Quantum Cryptography（PQC）とは

Post-quantum cryptography

From Wikipedia, the free encyclopedia

Post-quantum cryptography refers to cryptographic algorithms (us
computer. This is not true for the most popular public-key al
with the currently popular algorithms is that their security
logarithm problem or the elliptic-curve discrete logarithm pro
running Shor's algorithm.[1][2] Even though current, publicly
many cryptographers are designing new algorithms to prepa
from academics and industry through the PQCrypto conference series sinc
hosted by the European Telecommunications Standards Institute (ETSI) and the Institu

In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers.[2][7] While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks.[8] Thus post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography. See section on symmetric-key approach below.

Post-quantum cryptography is distinct from quantum cryptography, which refers to using quantum phenomena to achieve secrecy and detect eavesdropping.

Contents [hide]

1 Algorithms
- 1.1 Lattice-based cryptography
- 1.2 Multivariate cryptography
- 1.3 Hash-based cryptography
- 1.4 Code-based cryptography
- 1.5 Supersing

何ベースの
アルゴリズムがいいの？

量子暗号と間違
われることが
多いよね

安全性評価って確立して
るんだっけ？

.wikipedia.org/wiki/Post-quantum_cryptography

cfrgでのPQC

ここ最近、取り扱われるトピックスは定番化されてきている

```
CFRG Agenda
IETF 99 Prague, Czech Republic
July 18, 2017  15:50 - 17:50  Congress Hall I,

Chairs:  Alexey Melnikov and Kenny Paterson

*** PRELIMINARY ***

15:50 CFRG status update from CFRG chairs
      (5 mins; Kenny Paterson)

15:55 Re-keying Mechanisms for Symmetric Keys
      (10 + 10; Stanislav V. Smyshlyaev)
      https://datatracker.ietf.org/doc/draft-irtf-cfrg-re-keying/)

16:15 Verifiable Random Functions
      (10 + 10; Sharon Goldberg)
      https://tools.ietf.org/html/draft-goldbe-vrf-01

16:35 Collective Edwards-Curve Digital Signature Algorithm
      (10 + 10; Bryan Ford)
      https://datatracker.ietf.org/doc/draft-ford-cfrg-cosi/

16:55 The Transition from Classical to Post-Quantum Cryptography
      (5 + 5; Kenny Paterson for Paul Hoffman)
      https://tools.ietf.org/html/draft-hoffman-c2pq-01

17:05 Hash-Based Signatures
      (10 + 5; David McGrew)
      https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/
      See also: http://eprint.iacr.org/2017/349.pdf;  http://eprint.iacr.org/2017/349.pdf; https://github.com/cisco/hash-sigs

17:20 KangarooTwelve
      (10 + 5; Quynh Dang for Beno"t Viguier)
      https://tools.ietf.org/html/draft-viguier-kangarootwelve-00

17:35 Two proposals: ECC mod 8^91 + 5 and DH mod 630(427!+1)+1
      (10 + 5; Andrew Allen for Dan Brown)

17:50 Close of CFRG Meeting
```

: PQC

: Non-NIST Approved

cfrgでのPQC

The Transition from Classical to Post-Quantum Cryptography: draft-hoffman-c2pq

Paul Hoffman, ICANN

具体的なアルゴリズムの話をするのではなく、
量子計算機のことを考慮した移行に備える！

https://datatracker.ietf.org/meeting/99/materials/slides-99-cfrg-the-transition-from-classical-to-post-quantum-cryptography-draft-hoffman-c2pq

cfrgでのPQC

Draftだけで標準化を行うだけでなく実装や評価も推進

Hash-Based Signatures draft-mcgrew-hash-sigs-07

Scott Fluhrer, Mich

IETF 99 Crypto F

What's New

- Updated draft with security tweak
  https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs
- Proof of security
  Further Analysis of a Proposed Hash-Based Signature Standard, Scott Fluhrer, June, 2017, http://eprint.iacr.org/2017/553.pdf
- Comparison with XMSS
  LMS vs XMSS: A comparison of the Stateful Hash-Based Signature Proposed Standards, Panos Kampanakis, Scott Fluhrer, April 2017, http://eprint.iacr.org/2017/349.pdf
- Full-featured C implementation
  https://github.com/cisco/hash-sigs

https://datatracker.ietf.org/meeting/99/materials/slides-99-cfrg-hash-based-signatures-draft-mcgrew-hash-sigs-07

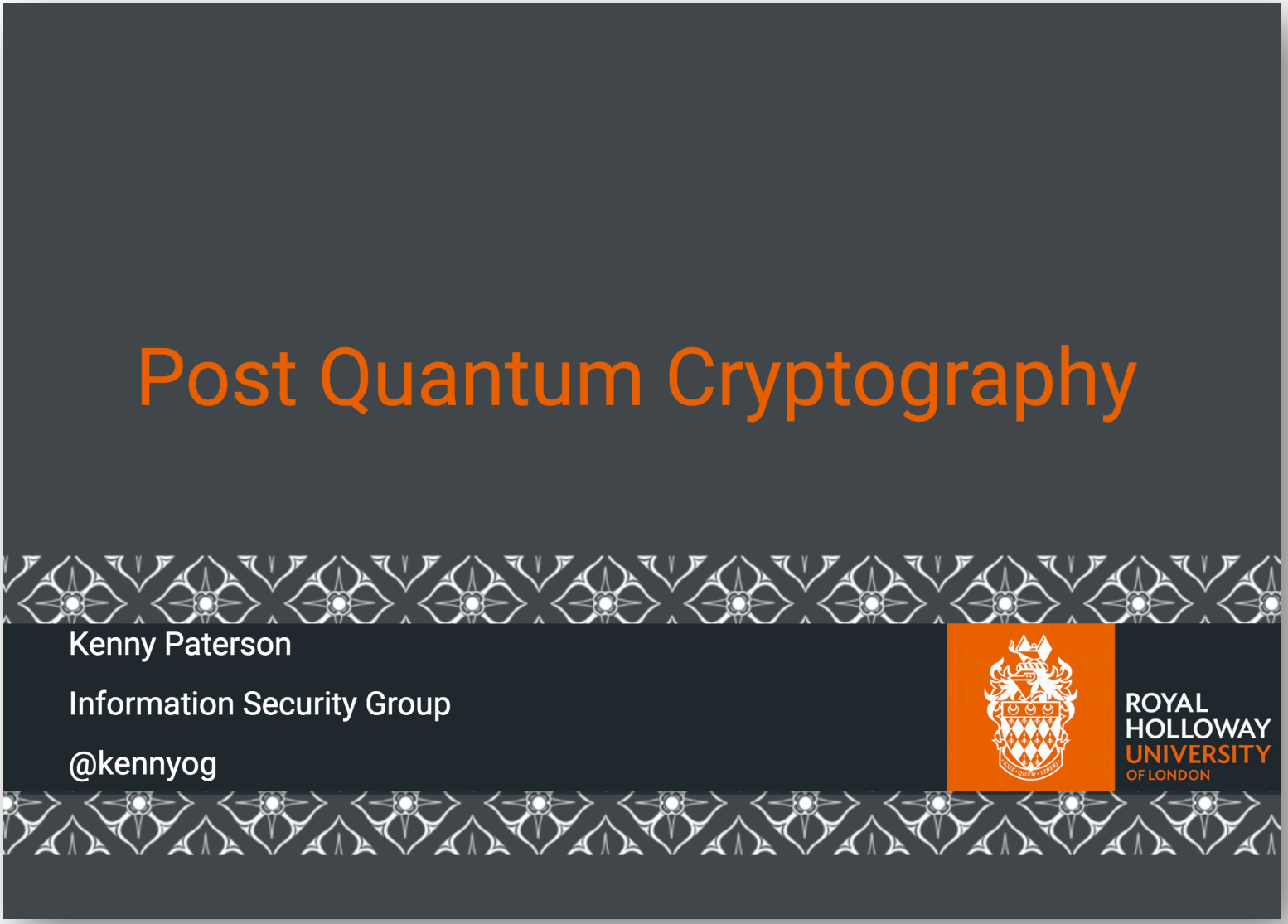
saagでのPQC

agenda

1. WG/BoF Reports and administrivia (10 mins)
2. Invited/offered talks
    1. Post-Quantum Crypto, Kenny Paterson (30 minutes)
    2. Pretty Easy Privacy (pEp), Volker Birk (15 minutes)
    3. Certificate Limitation Profile, Dmitry Belyavsky (5 minutes)
3. open-mic (60 mins)

https://datatracker.ietf.org/meeting/99/materials/slides-99-saag-saag-ietf-99

saagでのPQC



https://datatracker.ietf.org/meeting/99/materials/slides-99-saag-post-quantum-cryptography/

saagでのPQC

- この資料は良かった ╭(・ㅂ・)و ｸﾞｯ！
- 会場ではPQCという話題にも関わらず笑いもw

- 読み物として面白かった！
  - 実例としての危殆化や量子コンピュータの今って？
    - Lifetime of a Hash Algorithm – SHA-1
    - Progress in Quantum Computing
  - NISTによるPQCに関するコンテスト
  - IETFとして何をやるべきか？

参考情報：NIST PQC Contest

Ways Forward – PQC

NIST process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- Deadline for submissions is Nov 30, 2017
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:
  - First conference (Feb. 2018)
  - 12-18 month evaluation period – public and NIST staff.
  - Second conference.
  - (Optional tweaking.)
  - 12-18 month evaluation period.
  - Third conference.
  - Publication of report and portfolio OR decision for further evaluation.

11

https://datatracker.ietf.org/meeting/99/materials/slides-99-saag-post-quantum-cryptography/

ipsecmeでのPQC（1/2)

Agenda

- Agenda bashing, Logistics – Chairs (5min)
- Draft status
  - Finished & Almost finished WG drafts – Chairs (5min)
- Work / other Items
  - Split DNS (10 min)
  - Implicit IV (10 min)
  - Postquantum preshared keys (10min)
  - Hybrid Quantum Safe Key-Exchange (10 min)
  - EC + PQC Ideas (5 min)
  - Minimal G-IKEv2 Implementation (10 min)
  - Responder Initiated IP Address Update in MOBIKE (10 min)
  - Diet-ESP (5 min)

https://datatracker.ietf.org/meeting/99/materials/slides-99-ipsecme-chair-slides

ipsecmeでのPQC （2/2)

- Postquantum preshared keys
  - PSKをPostquantumって話で意味不明（？）だった
  - ノリ的にはワンタイムパッド？的なアレ

- Hybird Quantum Safe Key exchange
  - IKEにおける鍵交換としてPQCを使っちゃうという提案
  - strongSwanでの実装もある
    - https://github.com/post-quantum/strongswan/blob/qske/README.QSKE.md

Name	Number	Key exchange
RLWE 128	1	Diffie-Hellman-like
NewHope 128	2	Diffie-Hellman-like
NTRU EES743EP1	3	KEM
NTRU-Prime 216	4	KEM

IETF99における個人的に受けた印象

- 大きな流れとして捉えると・・・

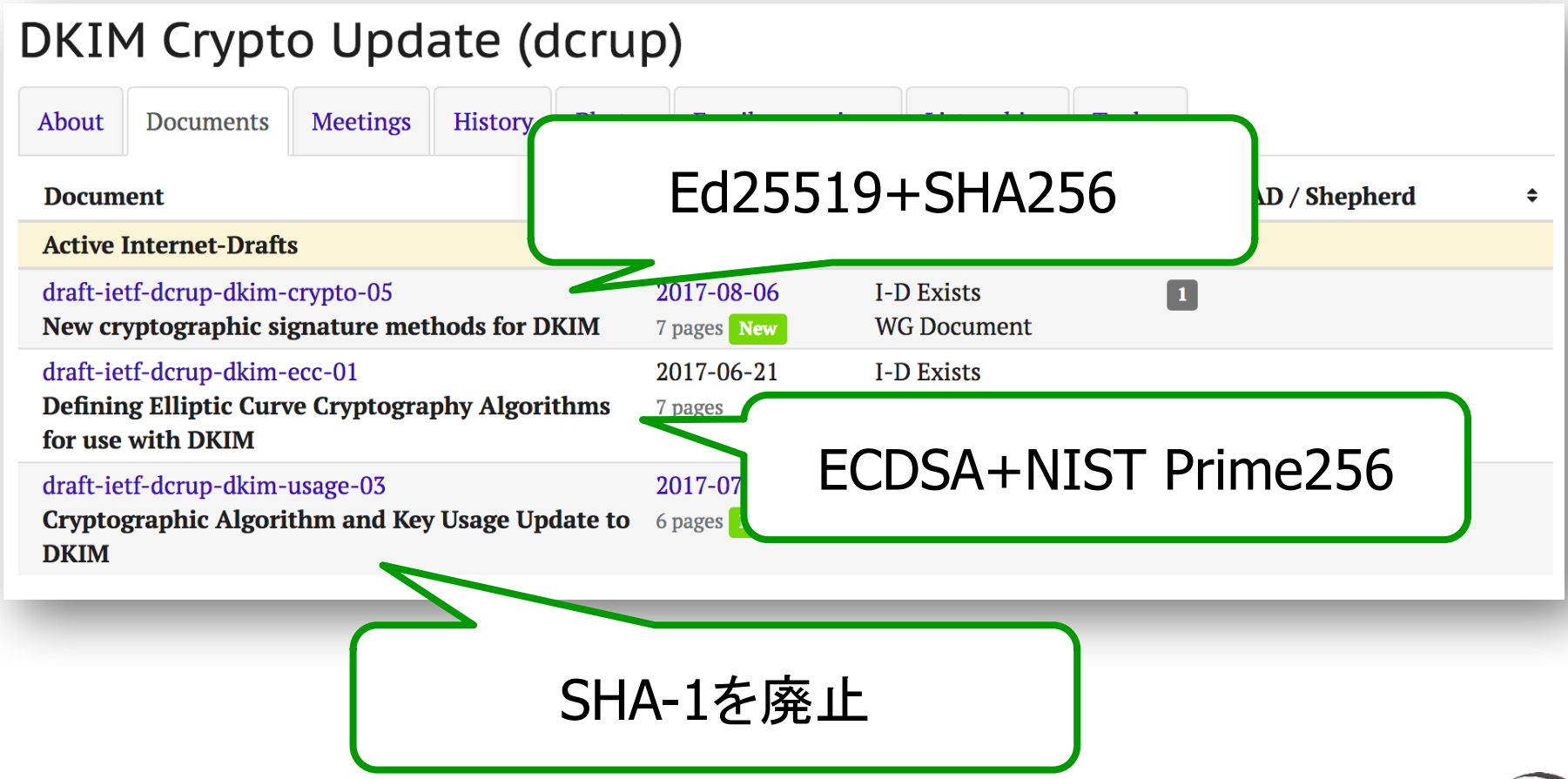
Post-Quantum Cryptography

&

Non-NIST Approved の
利用範囲拡大

dcrupでの動向

2007年5月にRFC4871として標準化されたDKIMをモダンにしちゃおうとするWG



https://datatracker.ietf.org/wg/dcrup/documents/

lampsでの動向

X509とS/MIME向けに可変長出力のSHA-3（SHAKE128およびSHAKE256）を出すよ！っていうお話

SHAKE128/256 and SHAKE256/512 for PKIX and S/MIME

Quynh Dang
Computer Security Division
National Institute of Standards and Technology (NIST)

-**Specifying SHAKE128/256 and SHAKE256/512 for PKIX and S/MIME.**
Supporting reason: Keccak and SHA-3 functions (including all the FIPS 202 and SP 800-185 functions) are the outcome of an open competition, unlike the previous hashing standards. They have a clear design rationale and have been receiving a lot of public cryptanalysis during and after the SHA-3 competition to today. All of that gives great confidence that the SHA-3s are very secure. The SHA3s also have much larger security margins than SHA-2s. In addition, since the design of the SHA3s is very different from SHA-2s (and other ARX-based designs), they offer sane diversity for security. Therefore, the SHA-3s are excellent alternatives to SHA2s.

December 2017: WG adoption of a SHAKE128/256 and SHAKE256/512 draft for PKIX.
December 2017: WG adoption of a SHAKE128/256 and SHAKE256/512 draft for S/MIME.
August 2018: WGLC for the SHAKE128/256 and SHAKE256/512 draft for PKIX.
August 2018: WGLC for the SHAKE128/256 and SHAKE256/512 draft for S/MIME.

https://datatracker.ietf.org/meeting/99/materials/slides-99-lamps-sha3-and-shake-for-pkix-and-smime

curdleでの動向（1/2）

主なRFCで規定された暗号技術の更新に関するステータス共有

WG documents status since IETF98

CMS: (default sent to IESG)
- draft-ietf-curdle-cms-ecdh-new-curves-09
- draft-ietf-curdle-cms-eddsa-signatures-06

Kerberos:
- draft-ietf-curdle-des-des-des-die-die-die-03
- draft-ietf-curdle-gss-keyex

PKIX:
- draft-ietf-curdle-pkix-05
- draft-schaad-curdle-oid-re

WG documents status since IETF98

SSH: (default sent to IESG)
- draft-ietf-curdle-rsa-sha2-09
- draft-ietf-curdle-ssh-curves-05
- draft-ietf-curdle-ssh-dh-group-exchange-04
- draft-ietf-curdle-ssh-ext-info-10
- draft-ietf-curdle-ssh-kex-sha2-08 (WGLC)
- draft-ietf-curdle-ssh-modp-dh-sha2-07

Other:
- draft-ietf-curdle-rc4-die-die-die-00 (WG adoption)

https://datatracker.ietf.org/meeting/99/materials/slides-99-curdle-chair-slides/

curdleでの動向（2/2）

Non-NIST Approvedな暗号技術が様々なプロトコルへ

Where are we ? - Ed*/X*...

	Ed25519/Ed448	X25519/X448	Chacha20Poly1305	AES-GCM	AES-CCM
SSH	Draft-ietf-curdle-ssh-ed25519-00 (TBD)	draft-ietf-curdle-ssh-curves-05	TBD	RFC5647	TBD
DNSSEC	RFC8080 (curdle)				
PKIX	draft-ietf-curdle-pkix-05 draft-schaad-curdle-oid				
CMS	draft-ietf-curdle-cms-ed-signatures-06				
XML					
Kerberos					
JSON	Msg05357 (TBD)				

Where are we ? - Sig/DH/Updates

	New Signature	New DH	Deprecation / Crypto Recommendations
SSH	draft-ietf-curdle-rsa-sha2-09 draft-ietf-curdle-ssh-ext-info-10	draft-ietf-curdle-ssh-modp-dh-sha2-07	draft-ietf-curdle-ssh-dh-group-exchange-04 draft-ietf-curdle-ssh-kex-sha2-08
DNSSEC	NA	NA	draft-arends-dnsop-dnssec-algorithm-update-00 (DNSOP) Draft-wouters-sury-dnsop-algorithm-update-02 (DNSOP)
PKIX	NA	NA	
CMS	NA	NA	
XML			
Kerberos		draft-ietf-curdle-gss-keyex-sha2-02	draft-ietf-curdle-rc4-die-die-die-00
JSON			

https://datatracker.ietf.org/meeting/99/materials/slides-99-curdle-chair-slides/

身近なNon-NIST Approvedアルゴリズム

- 具体的に、どんなアルゴリズム？？

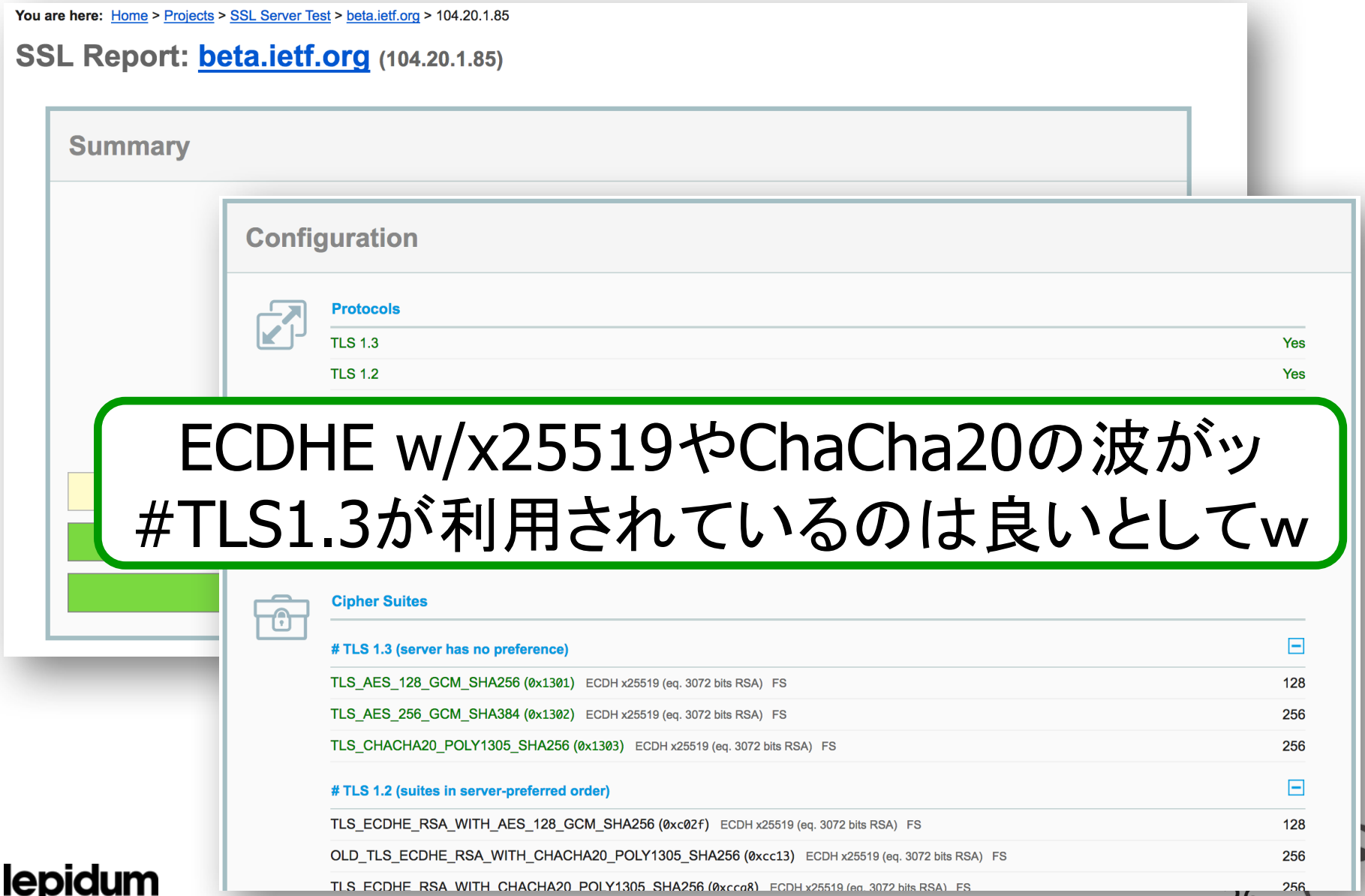
ChaCha20+Poly1305

Ed25519

EdDSA

でも、身の回りで使われてないんでしょ・・・？

例：beta.ietf.org



今後の予想

- ブラウザ系での利用できる環境が急速に整う
  - 利用するモチベーションがあるので暗号ライブラリ側の準備が整う
- 予想される世界として、アメリカ政府は調達する製品等に「Non-NIST Approved」が実装され、利用してしまうかもしれない懸念
  - 気にしないっていう方針？
- 正しく実装されているのかどうかを確認されていない製品等が世界で広がる懸念・・・

まとめ

- IETF99
  - NSA問題からの動きは継続しているため、暗号ネタはちょこちょこ発生
- IETF暗号の潮流および今後の予想
  - Post-Quantum Cryptoが頭一つ分飛び出した？
  - Non-NIST Approvedなアルゴリズムの拡張は続く
- 願いとしては・・・
  - （個人的には）日本から提案を出していきたい

連絡先

- **E-mail**
  - kanno@lepidum.co.jp
- **SNS**
  - Twitter (satorukanno)
  - Facebook (satoru.kanno)
  - Linkedin

お気軽にご連絡ください！