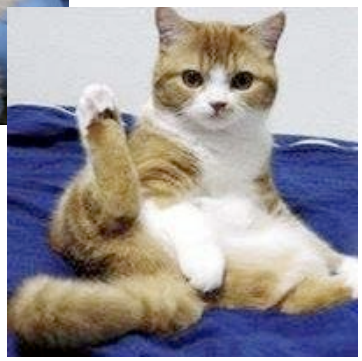
IETF90 報告会
TLS とUTA WG 関連

ちょっとTCPINCもあるよ

2014年8月25日

菅野　哲（かんの　さとる）

この登壇者は何者・・・？



- **名前**
  - 菅野 哲（かんの さとる）
- **所属**
  - NTTソフトウェア 株式会社
    - 最近では技術職ではないという噂
    - マーケティングやプロモーションがメイン業務
- **その他の所属**
  - CELLOS事務局
  - ISOC Japan Chapter（Program Committee）
  - MIT-KIT Japan Chapter（窓口？）

この講演での話題

TLS & UTA WG

と

暗号技術関連

IETFでなぜこんなに暗号技術の話するのか？

IETF88において

Pervasive Surveillance

を大きく取り上げた

政府への不信感の高まり

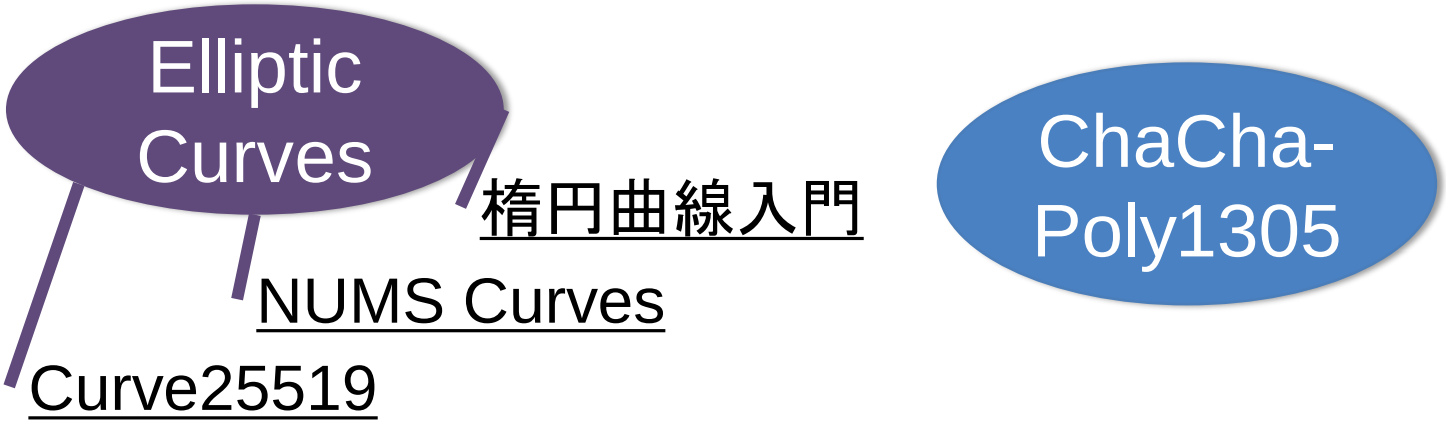
PSの明確化！

暗号技術で対抗

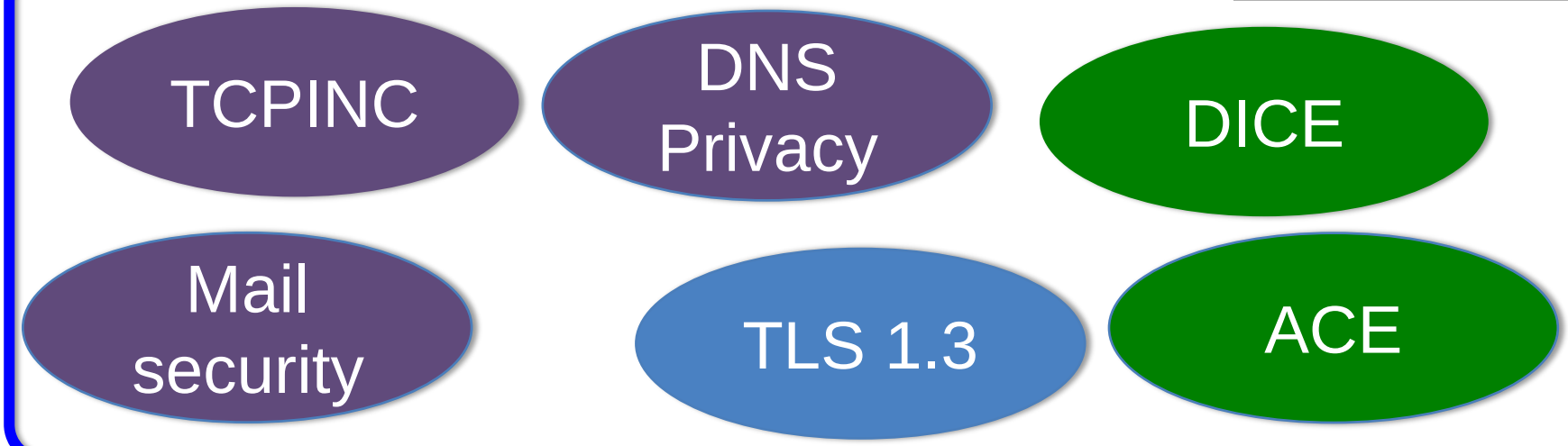
IETF90
セキュリティエリア

IETF90 セキュリティ全体の外観

暗号プリミティブ



プロトコル関連



TLS WG

- **TLS（Transport Layer Security）WGとは？**
  - TLSに関する仕様検討やメンテナンスを行う

- **今回のTLS WGは？**
  - Interimを含めて**3回**の会議を開催！
    - やっぱり **TLS 1.3** がアツイ！
    - 既存攻撃への対策
    - 暗号技術関連
      - **楕円曲線暗号**周辺をどうする？！
      - 毎度おなじみ**ChaCha20+Poly1305**

TLS WG: Agenda

Sunday July 20, 2014 (TLS Interim Meeting)
Mozilla Toronto
Toronto, ON, Canada

10:00 - 10:15 Administrivia (Chairs)
10:15 - 11:45 1RTT Handshake Flow (EKR)
11:45 - 13:00 Lunch
13:00 - 14:00 Renegotiation/rekey/client au
14:00 - 14:30 Content Type Encryption (DKG)
14:30 - 14:45 Break
14:45 - 15:30 SNI encryption (DKG)
15:30 - 16:00 Triple-Handshake (TBD)

Agenda

Monday July 21, 2014 (IETF 90 TLS Meeting - Session 1)
Fairmont Royal York - Ontario C
Toronto, ON, Canada

Blue sheets/scribes/etc. (chairs)
WG Document Status (chairs)
ECC to Standards Track/MTI (all)
ChaCha/Poly1305 (AGL)
SCSV/Downgrade (AGL)

Agenda

Thursday July 24, 2014 (IETF 90 TLS Meting - Session 2)
Fairmont Royal York - Ontario C

17:30 - 17:35 Blue sheets/scribes/etc. (chairs)
17:35 - 18:00 New curves:
Report from CFRG (CFRG Chairs)
Discussion
18:00 - 18:15 Named DH Groups (DKG)
18:15 - 18:30 Hardware Crypto Considerations (MSJ)

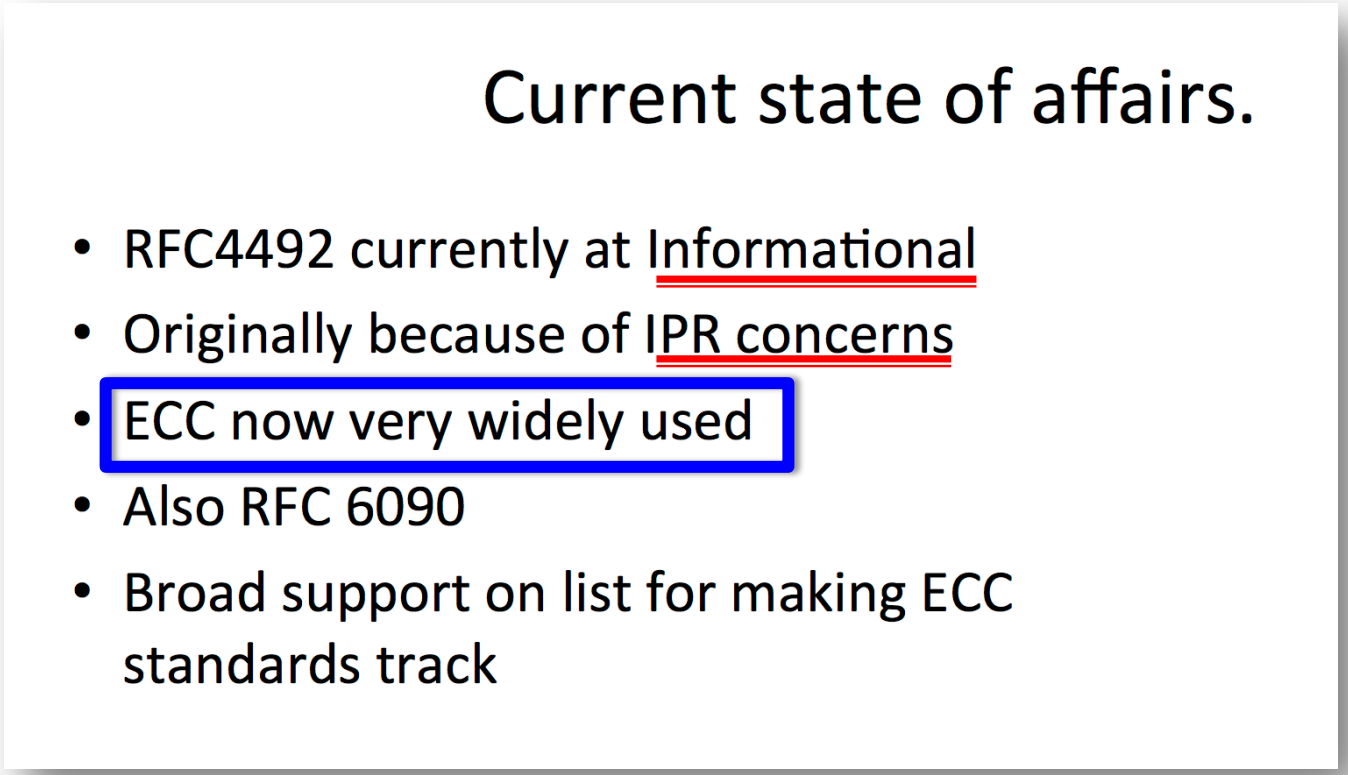
http://www.ietf.org/proceedings/90/slides/slides-90-tls-1.pdf

TLS WG: TLS 1.3での決まったこと＆課題

- **決まったこと**
  - Compressionのサポート削除
  - Static RSAおよびStatic DHによる鍵交換のサポート削除
    - (Perfect) Forward Secrecy の実現
  - Authenticated-Encryption with Associated-Data (AEAD) のサポート
- **課題**
  - ハンドシェイク全体への署名を行うか？
  - TLS1.2以前への互換性をどうするか？
  - Triple Handshake攻撃への対策を反映するか？

TLS WG: ECC to Standards Track / MTI

注目を集めている楕円曲線暗号の現状は・・・



http://www.ietf.org/proceedings/90/slides/slides-90-tls-3.pdf

TLS WG: ECC to Standards Track / MTI

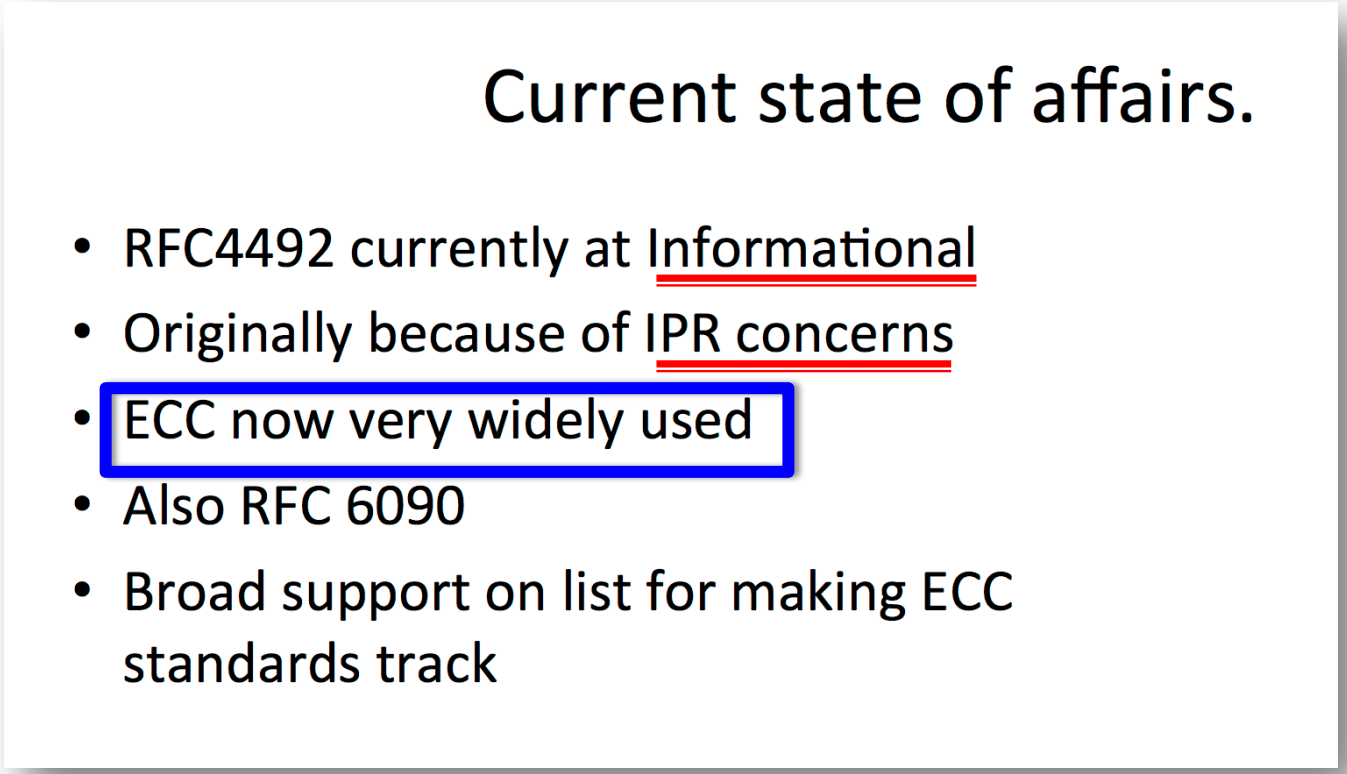
疑問：楕円曲線暗号って本当に使われてるの？？

Browser: Firefox 31.0

結論：案外・・・**使われてる**（かもしれない）

TLS WG: ECC to Standards Track / MTI

注目を集めている楕円曲線暗号の現状は･･･



TLS1.2を含めてRFC4492bisを執筆！

http://www.ietf.org/proceedings/90/slides/slides-90-tls-3.pdf

TLS WG: まとめ

- TLS 1.3という鈍行列車は加速するか？
  - ErkがTLS WGのco-chairを退任したので注力されて加速するかも？！
  - 今後に期待！！
- 楕円曲線周辺の話題
  - CFRGから楕円曲線としての要件が提示
    - **Curve25519**と**NUMS Curve**の一騎打ち？！
- ChaCha20+Poly1305の動向
  - 今後も続きそうな気も・・・

UTA WG

- UTA（Using TLS in Applications）WGとは？
  - TLSプロトコルによりアプリケーションのプロトコルを保護する
  - **アプリケーションエリア**のWG

- **主に議論していることは・・・**
  - ***TLS Attacks and BCP***の検討

UTA WG: TLS-BCP

TLS BCP: Last Revision

- Clarified that specific TLS-using protocols may have stricter requirements
- Changed TLS 1.0 from MAY to SHOULD NOT
  - But may still fallback to TLS 1.0 (unfortunately)
- Added discussion of "optional TLS" and HSTS
- Recommended use of the Signature Algorithm and Renegotiation Info extensions
- Use of a strong cipher for a resumption ticket: changed SHOULD to MUST
- Added an informational discussion of certificate revocation, but no recommendations

今回の議論の結果：TLS1.0へのfallbackは許容

http://www.ietf.org/proceedings/90/slides/slides-90-uta-2.pdf

UTA WG: TLS-BCP

つぶらな瞳でTLS-BCPのCipher suiteを眺めてみる・・・

Recommendations for Secure Use of TLS and DTLS

http://tools.ietf.org/html/draft-ietf-uta-tls-bcp-01

Given the foregoing considerations, implementation of the following cipher suites is RECOMMENDED (see [RFC5289] for details):

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

} fallbackでき・・・ない

感触としてTLS1.2のCiphersuiteだけはツライ

UTA WG: TLS-BCP

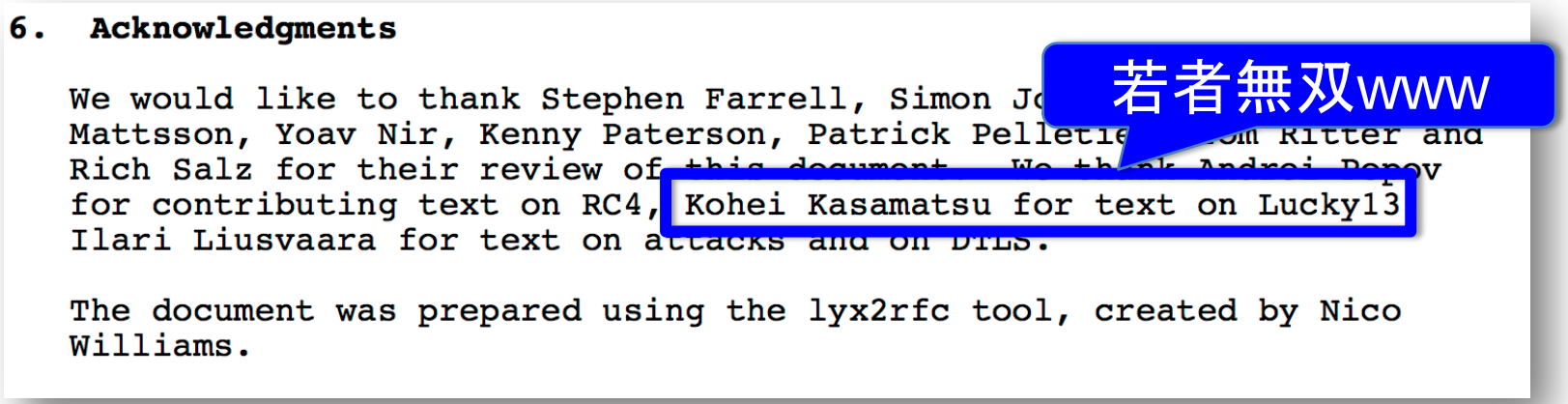
- **検討されているCiphersuiteを見ると・・・**
  - 採用した暗号アルゴリズムが危殆化した際の移行に支障が？！
    - 具体的に言うと
      - ✓ アルゴリズムの選択肢がない
        - 例：共通鍵 AESのみ
      - ✓ 問題発生時の対処フローがない 等・・・

Ciphersuiteの構成部品に関する
選択肢について議論を持ちかけているなう！

UTA WG: まとめ

- TLS-BCPのRFC化をWG Chairは急いでいるけどもう少しじっくり見直した方が良いかなぁ
  - 安全性だけに注力していると相互運用性に支障がでそう
- TLS-Attacksはだいたい議論は収束しそう

おまけ：Summarizing Current Attacks on TLS and DTLS



6. Acknowledgments

We would like to thank Stephen Farrell, Simon Jo
Mattsson, Yoav Nir, Kenny Paterson, Patrick Pelletie
Rich Salz for their review of this document. We thank Andrei Popov
for contributing text on RC4, Kohei Kasamatsu for text on Lucky13
Ilari Liusvaara for text on attacks and on DTLS.

The document was prepared using the lyx2rfc tool, created by Nico
Williams.

若者無双www

https://datatracker.ietf.org/doc/draft-ietf-uta-tls-attacks/

TCPINC WG

- **TCPINC WGとは？**
  - TCPレイヤにおけるデータの機密性および完全性を提供するTCP extensionを規定する
  - **トランスポートエリア**のWG

- **TCP extensionの要件**
  - **相手認証を考えない**
  - **上位レイヤに影響は与えない**
  - **コネクション毎にForward secrecy を満たす**
  - **NAT/Firewallを通過できる**
  - **小さいオーバヘッド**
  - **手動による環境設定を必要としない**

TCPINC WG: 謎の期待感Ɪ

Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: January 22, 2015

A. Bittau
D. Boneh
M. Hamburg
Stanford University
M. Handley
University College London
D. Mazieres
Q. Slack
Stanford University
July 21, 2014

Cryptographic protection of TCP Streams (tcpcrypt)
draft-bittau-tcpinc-01.txt

Abstract

This document presents tcpcrypt, a TCP extension for cryptographically protecting TCP segments. Tcpcrypt maintains the confidentiality of data transmitted in TCP segments against a passive eavesdropper. It protects connections against denial-of-service attacks involving desynchronizing of sequence numbers, and when enabled, against forged RST segments. Finally, applications that perform authentication can obtain end-to-end confidentiality and integrity guarantees by tying authentication to tcpcrypt Session ID values.

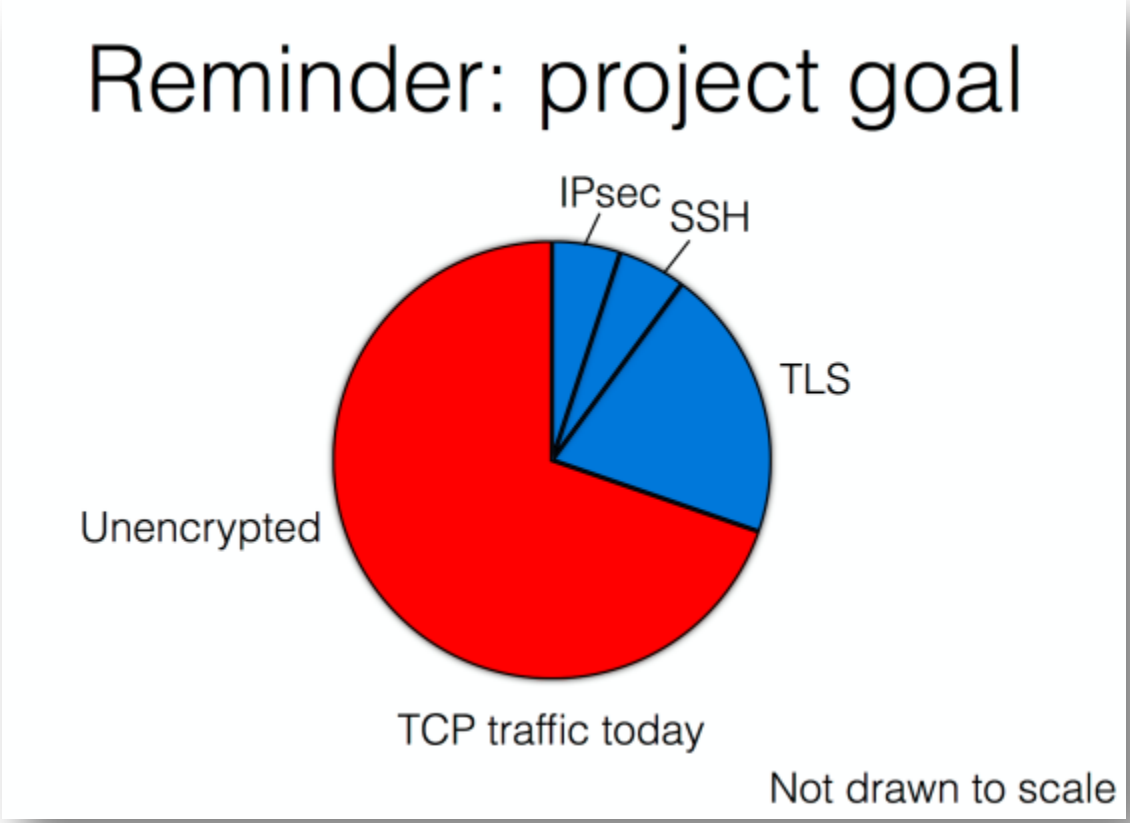
The extension defines two new TCP options, CRYPT and MAC, which are

connections per second.

効率的なIBE（ID Based Encryption）を実現した
Prof. Dan Bonehが関係しているのでテンション⬆□

TCPINC WG: tcpcrypt

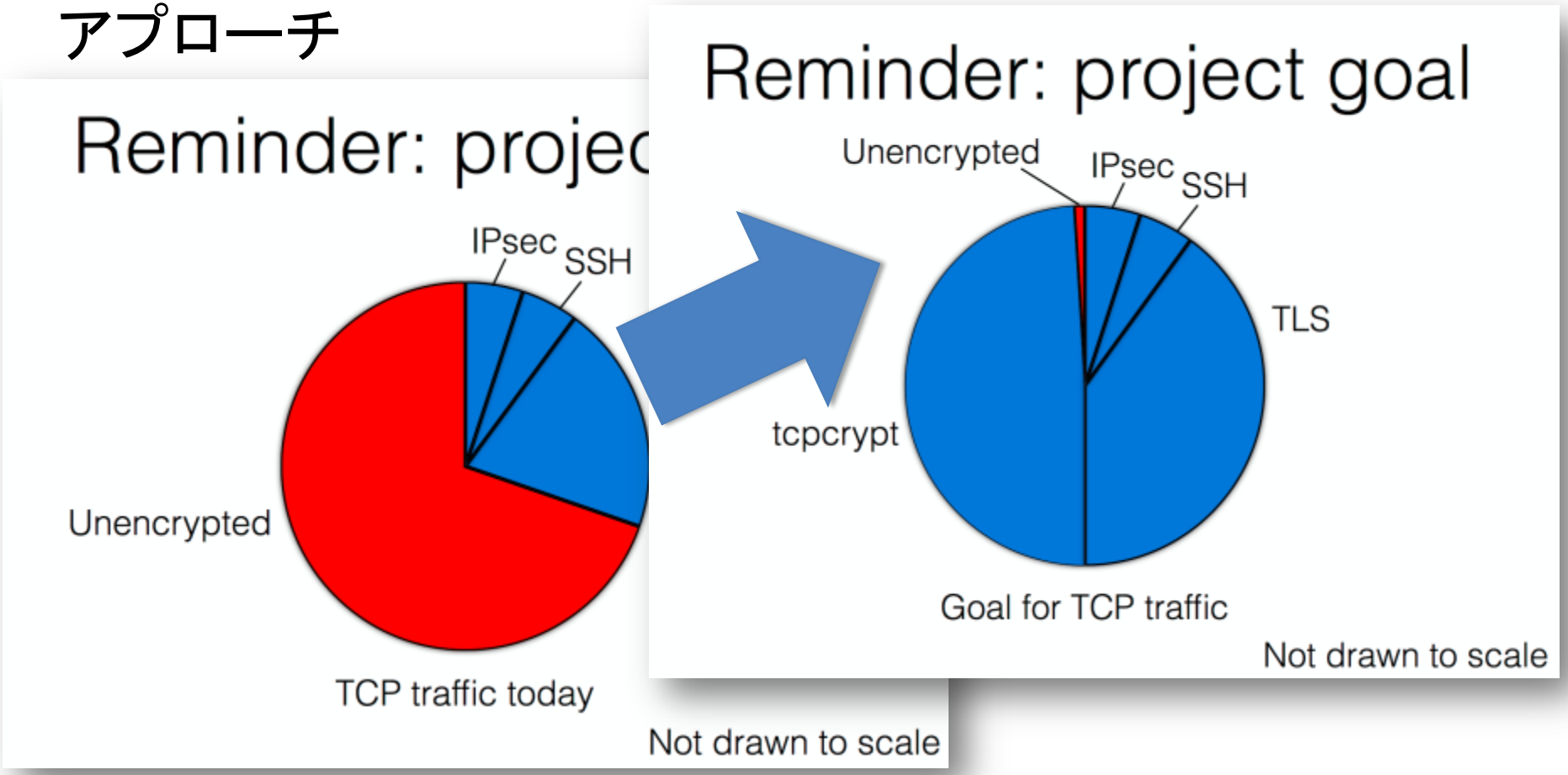
TCP通信を全部暗号化しちゃえば良いよね？というアプローチ



http://www.ietf.org/proceedings/90/slides/slides-90-tcpinc-2.pdf

TCPINC WG: tcpcrypt

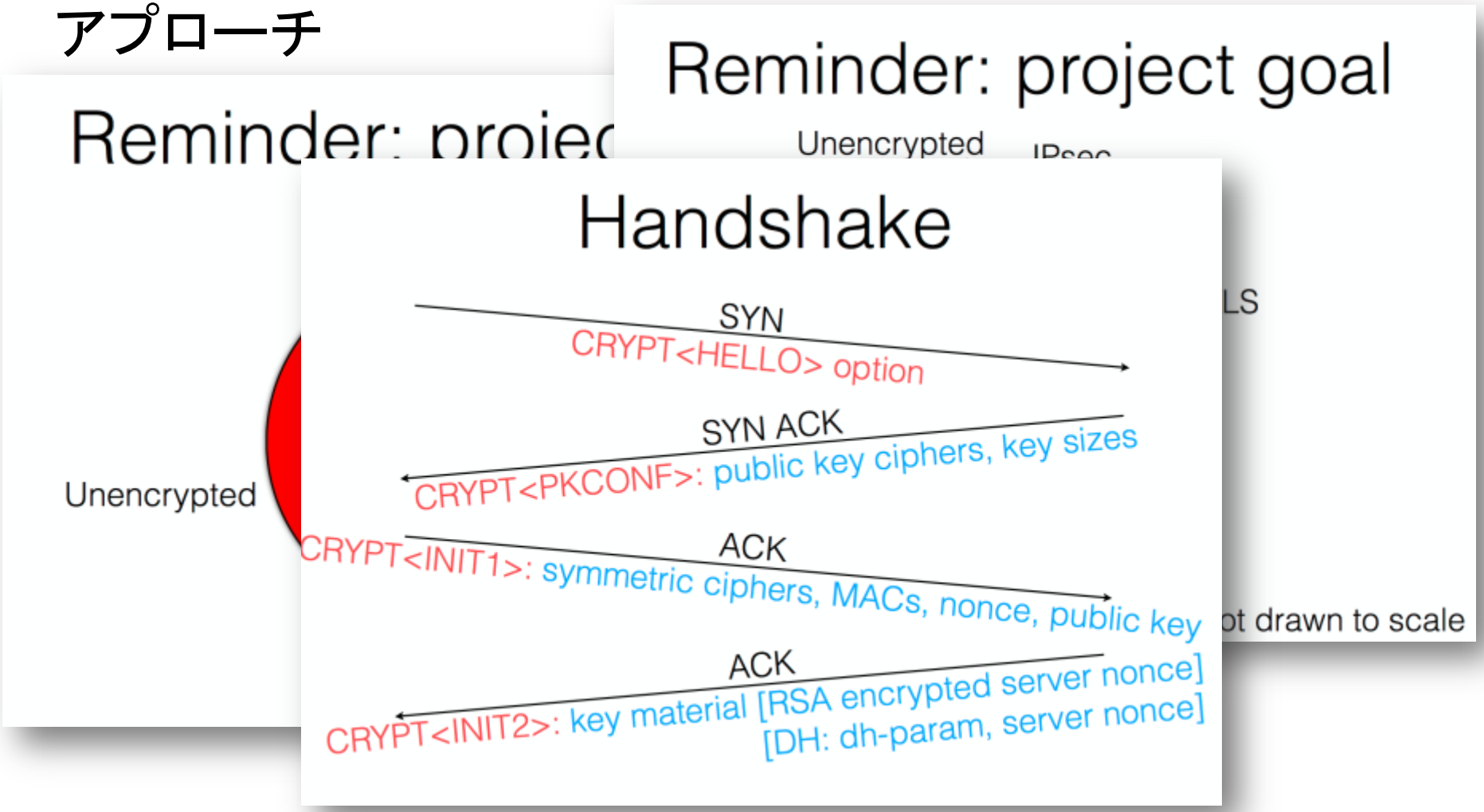
TCP通信を全部暗号化しちゃえば良いよね？というアプローチ



http://www.ietf.org/proceedings/90/slides/slides-90-tcpinc-2.pdf

TCPINC WG: tcpcrypt

TCP通信を全部暗号化しちゃえば良いよね？というアプローチ



http://www.ietf.org/proceedings/90/slides/slides-90-tcpinc-2.pdf

TCPINC WG: まとめ

- トランスポートエリアのWGということもあり，ノーマークでIETF90では参加できなかった．．．

  orz…

  - 技術としてはPervasive Surveillance対策としては強力！
  - 次回は参加しようと心に誓う？
- 参考情報
  - https://datatracker.ietf.org/wg/tcpinc/charter/

暗号技術関連: 楕円曲線の選定

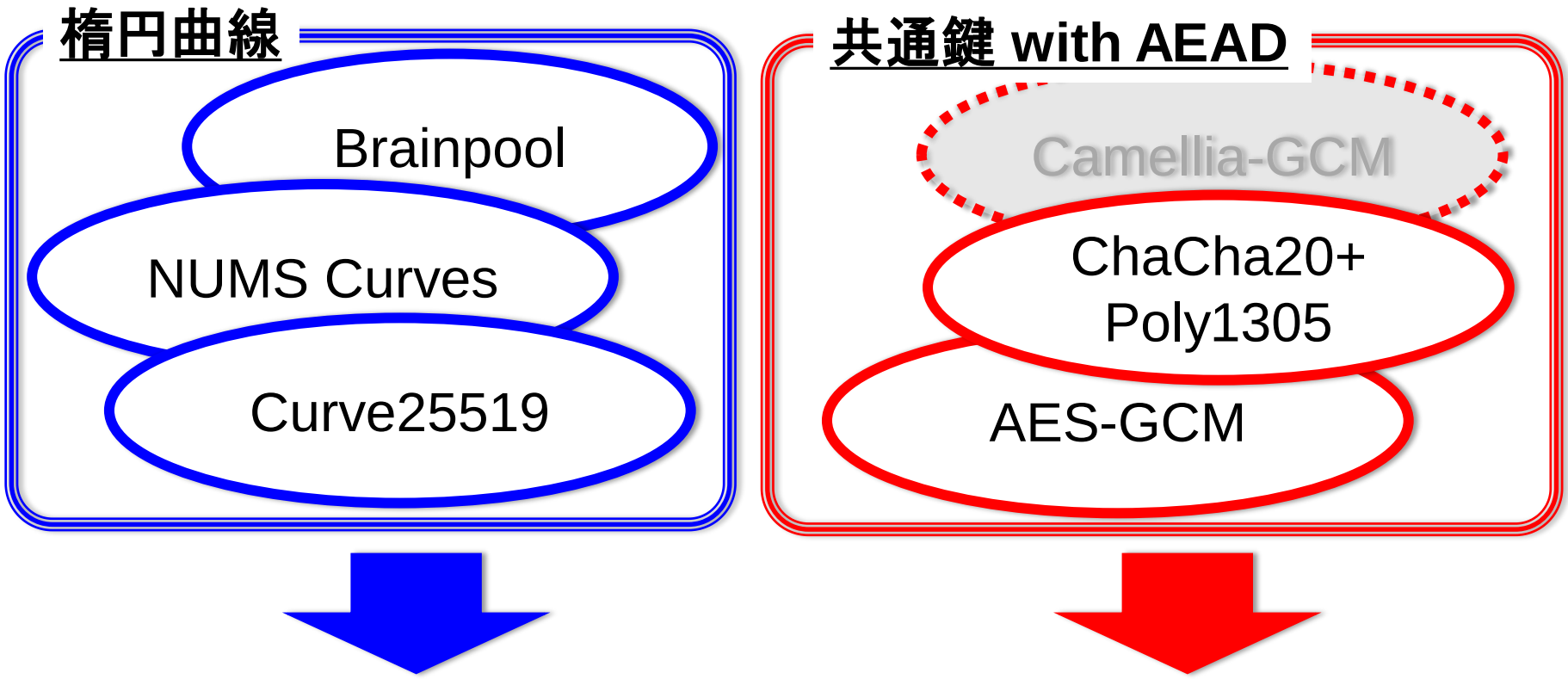
- **楕円曲線の選定**
  - **Curve25519**の独壇場か･･･と思われたが **NUMS Curve**@ Microsoftの提案
    - 若干 Brainpoolは忘れられてたり･･･
  - CFRGとして安全な楕円曲線の要求仕様（基準）をTLS WGに提示
    - どんな要件か知りたい人！
      - JPNICさんメルマガ臨時号 “**第90回IETF報告 [第3弾]暗号技術に関する動向**”を参照
      - https://www.nic.ad.jp/ja/mailmagazine/backnumber/2014/

最近のIETFの動向を見ていて．．．

気になること

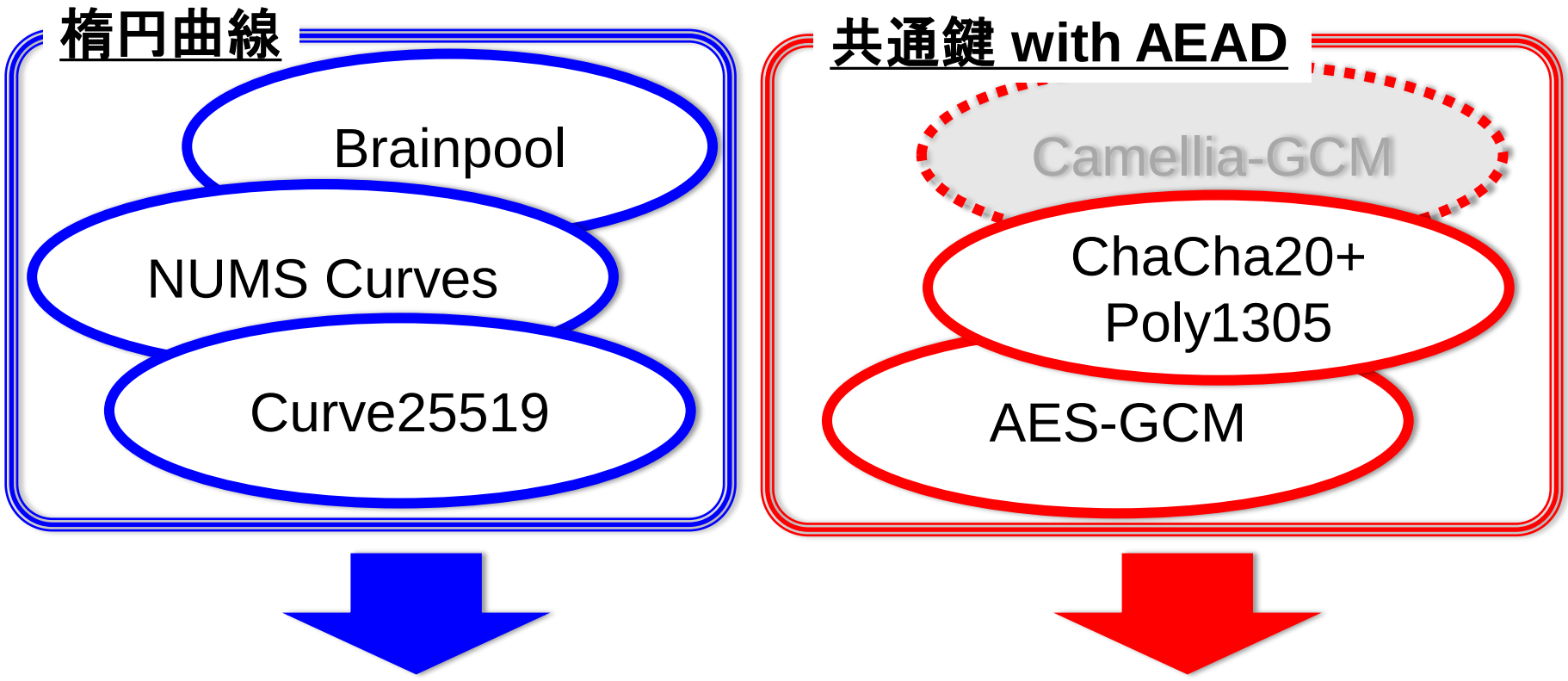
がある

TLSを安全にするためにめっちゃ議論してる・・・



TLS_{鍵交換}_{署名}_WITH_{共通鍵}_{鍵長}
_{暗号利用モード}_{MAC}

TLSを安全にするためにめっちゃ議論してる・・・



TLS_**ECDHE_ECDSA**_WITH_**ChaCha20_Poly1305**

DJB...

あれ？ なんか不思議な気分・・・

まとめ

- 暗号技術の需要が高まるという***異常事態***！
- Pervasive Surveillance対策が気になりすぎて様々なプロトコルで暗号化を導入してしまい最適化は考えていないのかなぁ・・・

- 今後の懸念・・・
  - 現在，IETFで推されているアルゴリズムは**広く評価されていない**ことが多い
  - **暗号プロトコルが増加**しまくっているけど，仕様検討の段階で**安全性を評価**しきれるのか？

連絡先

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

お気軽にご連絡ください！