@takehara3586

1. 暗号化
2. CCWG (Congestion Control Working Group)

暗号化:モチベーション

- 今回の事前議題でも一番多かった話題
  - CEDEC 2023 でもかなり盛り上がった
- ゲーム業界的モチベーション
  - ゲームのリアルタイム通信に最適化された暗号化モジュールを使いたい
  - QUICから暗号化を切り離したい
    - 期限切れではあるが過去提案はあった
      - https://datatracker.ietf.org/doc/html/draft-banks-quic-disable-encryption

暗号化: tls WG

- The SSLKEYLOGFILE Format for TLS
  - TLSの復号に用いる SSLKEYLOGFILE のフォーマット提案仕様 (ASnoKaze blog)
- TLS 1.2 is in Feature Freeze
  - 緊急のセキュリティパッチ以外はTLS 1.2の仕様追加をフリーズしようという提案

暗号化: Areion

IETF117 Hackathon: 超低遅延暗号 Areion

GMO CYBER SECURITY IERAE

- 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

https://www.isoc.jp/files/IETF117-report-mtg_hackathon-pqc_sakemi.pdf より

暗号化: Areionのゲームへの適用

- ゲームは小さいサイズのデータを高頻度で送る
  - 従来の暗号化やハッシュアルゴリズムでは一定のブロックサイズが必要で無駄がある
- Areionは特に短いメッセージ(最大2KB)の処理に効率的な暗号化
  - 最小サイズは未記載

https://eprint.iacr.org/2023/794 より

暗号化: Areion実装

- IETF 117 で OpenSSL 実装を実施
  - areion-openssl
- IETF 118 では QUIC, WebRTC 実装を実施
  - https://wiki.ietf.org/en/meeting/118/hackathon
- 関連
  - 新しい暗号を組み込んだQUICを動かそう (その1) ～低遅延性が必要なインターネットプロトコルを求めて - 探索編 -

暗号化: Aerionリンク集

- 論文：Areion: Highly-Efficient Permutations and Its Applications
- GitHub：low-latency-crypto-areion
- OpenSSL 実装：areion-openssl
- draft：Ultra-Low Latency Cryptography Areion

https://www.isoc.jp/files/IETF117-report-mtg_hackathon-pqc_sakemi.pdf より

CCWG: CCGWとは？

- Congestion Control Working Groupの略
- 2023/6/26 に新設
  - IETF では 117 から議論
  - IETF 115/116 では CONGRESS BOF として活動
- RFC5033の改定が目的の一つ
  - Specifying New Congestion Control Algorithms
- その他輻輳制御の課題の解決や新しいアルゴリズムの検討等、輻輳制御に関する広範な話題を取り扱う

CCWG: モチベーション

- 現代の複雑なネットワーク環境では輻輳制御があった方が遅延に有利なケースもあり得る
  - UDPであっても輻輳制御が必要なケース
  - 勿論逆に足かせになる場合もある
- ゲームのリアルタイム通信において輻輳制御が語られることはあまりない
  - 一般的にもリアルタイム通信における輻輳制御が語られることはあまりなかった
  - IETF 118 の CCWG では何点か話題に！

CCWG: Non-standard algorithms #35 (の議論からの抜粋)

リアルタイム通信がベストエフォートに比べて遅い(帯域を使わない)べきであるかどうかの議論

- 帯域幅を最大化しようとする輻輳制御はリアルタイム通信の遅延を増加させる原因となりえる
  - RenoやCubicといった伝統的な輻輳制御最大化を目指すアルゴリズムとは区別して考えるべき
  - 遅延感知型の輻輳制御が重要になる
- AQM（Active Queue Management）の適切な配置と設定が重要

CCWG: Containing the Cambrian Explosion in QUIC Congestion Control

- 各QUIC実装の輻輳制御の性能とConformance（遵守率）の比較
  - Conformance:標準(カーネル)実装との一致率
- あくまで目的は各実装のConformanceとパフォーマンスの比較
  - リアルタイム通信の場合はどうというような比較はないが、Deep BufferにおいてConformanceの乖離が目立つ等、不公平性を引き起こす可能性については言及