3-3-3　エンドツーエンド暗号化に対する安全性評価
3-3-3　Security Analysis of End-to-End Encryption

伊藤 竜馬
ITO Ryoma

新型コロナウイルス感染症の世界的流行に伴い、ビデオ会議システムの利用が世界中で拡大した。また、ユーザのプライバシーを保護するための技術であるエンドツーエンド暗号化（E2EE: End-to-End Encryption）の必要性も高まり、多くのビデオ会議システムで E2EE が導入されるようになった。セキュリティ基盤研究室は兵庫県立大学と NEC との共同研究により、主要なビデオ会議システムに導入される E2EE に対して安全性評価を実施した。本稿では、主要なビデオ会議アプリケーションの 1 つである Zoom の E2EE、そしてオーディオ・ビデオ製品向け E2EE フレームワークである SFrame に対する安全性評価の結果を紹介する。

The global spread of the COVID-19 pandemic significantly increased the use of video conferencing systems. Furthermore, extensive surveillance disclosures, most notably by Edward Snowden, have highlighted the importance of end-to-end encryption (E2EE) for protecting users' privacy and data integrity across various communication platforms. Consequently, many video conferencing systems implemented E2EE during the pandemic. In collaboration with the University of Hyogo and NEC, we have conducted an in-depth analysis of the E2EE protocols used in major video conferencing systems. This paper summarizes our cryptanalysis findings on E2EE implementations in Zoom and SFrame, a framework for E2EE in major audio/video applications.

1　まえがき

エンドツーエンド暗号化（E2EE: End-to-End Encryption）とは、通信相手との間でのみメッセージの正常な送受信が可能であり、情報通信サービスの提供者であってもメッセージの盗聴、改ざん等が技術的に不可能な暗号技術のことである（図 1 左）。2013 年 3 月に発生したエドワード・スノーデン氏の暴露事件で明らかになったように、インターネットを介した通信では国家規模の大規模な監視活動が行われている危険性がある。このような背景の下、サービス利用者のプライバシーを保護する技術として E2EE が注目され始めた。

2024 年 4 月現在、E2EE はメッセージングアプリケーションやビデオ会議システムなどの様々な情報通信サービスに導入されている。しかしながら、その安全性は必ずしも十分ではない場合が多く散見される。例えば、東アジアで幅広く利用されているメッセージングアプリケーションの LINE では、Letter Sealing と呼ばれる E2EE の暗号プリミティブや暗号プロトコルを悪用することで、メッセージの完全性が保証されないという脆弱性（ぜいじゃく）が 2018 年に指摘された [1]。その他、E2EE の安全性評価に関する議論、特に脆弱性の指摘が活発に行われている [2]–[7]。以上より、情報通信サービスに導入されている E2EE の安全性評価を行い、求められる安全性要件が確保されているかを検証することは重要である。

新型コロナウイルス感染症の世界的流行に伴ってビデオ会議システムの活用が世界中に拡大したことにより、主要なビデオ会議システムに対して E2EE を導入することが検討され始めた。例えば、Zoom では 2020 年 5 月に E2EE の導入計画が発表され、その仕様がホワイトペーパー [8] として公開された。また、2020 年 5 月に、リアルタイム通信が要求されるビデオ会議システムなどで効率的に E2EE を実現するためのフレームワークである SFrame の仕様が IETF のインターネットドラフト [9] として公開され、Cisco Webex、Google Duo、Jitsi Meet などに導入された。これらのビデオ会議システムに導入される E2EE に対し、兵庫県立大学と NEC との共同研究で安全性評価を行い、プライバシー保護レベルが確保されているかを検証した。Zoom の E2EE に対する安全性評価結果を **2** で、SFrame に対する安全性評価結果を **3** で概説する（図 1 右）。

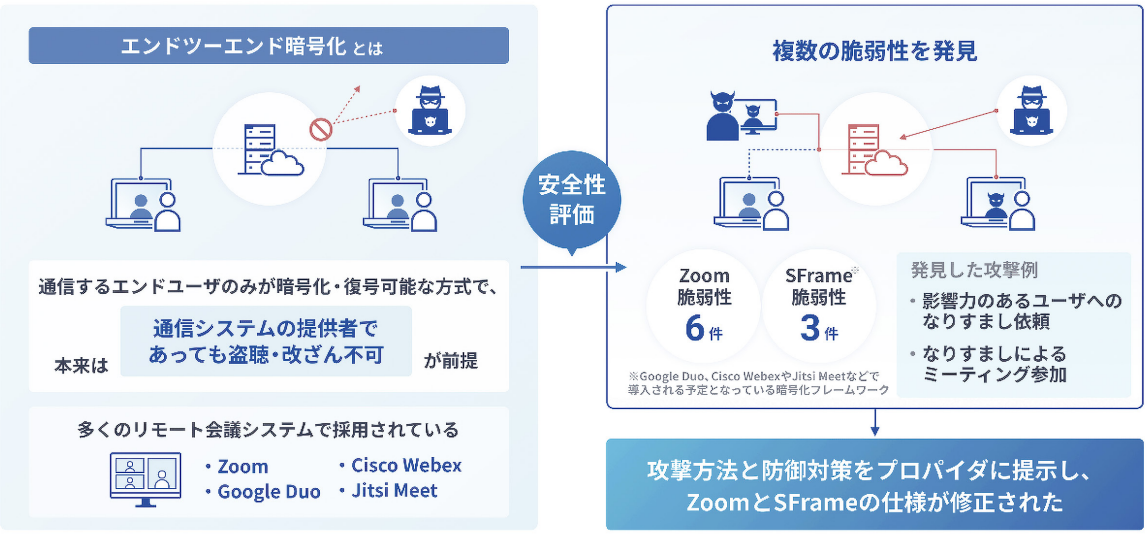

図 1　Zoom や Webex 等で導入されているエンドツーエンド暗号化技術の評価

2　Zoom の E2EE に対する安全性評価

我々はホワイトペーパーのバージョン 2.3.1 に記載された仕様に対して安全性評価を実施した [12]–[15]。本章では我々の安全性評価によって発見した複数の脆弱性、そしてこれらの脆弱性に起因する攻撃手法とその対策手法について概説する。2024 年 4 月時点において、ホワイトペーパーの最新バージョンは 4.3 であり、我々の評価結果の一部が反映されていることを確認している。また、紙面の都合上、仕様の詳細については文献 [8] を、攻撃者モデルや安全性要件の詳細については文献 [12]–[15] を参照されたい。

2.1　任意の会議参加者へのなりすまし攻撃

Zoom でのビデオ会議において、音声、動画、共有資料などのデータは AES-GCM と呼ばれる認証暗号方式で暗号化される。AES-GCM による暗号化では、データの機密性と完全性を保証するものの、エンティティ認証の機能がないために真正性を保証しない。この特徴を悪用することで、悪意ある会議参加者が別の任意の会議参加者になりすました上で、任意のデータを送信することが可能となる。

この攻撃が成立する根本的な原因は、ビデオ会議中におけるエンティティ認証が欠如していることにある。このため、対策手法の一案としては、全てのデータに対して署名技術を適用することが挙げられる。ただし、ホワイトペーパー [8] によると、パフォーマンスと否認防止の観点で署名技術の導入が今後の課題となっている。

2.2　任意の Zoom ユーザへのなりすまし攻撃

正当な会議参加者であるかを検証するために、会議開始前に各ユーザ間で相互認証が行われる。この際、認証用データとして、Zoom サーバから送信されるデータと各会議固有の掲示板を経由して各ユーザ間で共有されるデータが使用される。なお、Zoom サーバと会議参加者は掲示板へ自由にアクセスできるという特徴がある。つまり、インサイダー（悪意のあるサーバ管理者）と悪意のある会議参加者は、過去のビデオ会議で使用された認証用データを収集し、再利用することが可能となる。

ホワイトペーパー [8] によると、悪意のある会議参加者はインサイダーと結託することによって別の会議参加者へのなりすましが可能であると明記されており、このような攻撃は仕様上の制約事項となっている。一方で、我々の安全性評価では、Zoom のセキュリティチームが想定するよりも強力な攻撃が実行可能であることを指摘した。具体的には、次のとおりである。

- インサイダーが悪意のある会議参加者と結託する場合、会議参加者だけでなく、会議に招待されていない任意の Zoom ユーザへのなりすましが可能である。
- 会議参加者と結託することなく、インサイダーは会議に招待されていない任意のユーザへのなりすましが可能である。

この攻撃が成立する根本的な原因は、全ての認証用データがインサイダーによって再利用可能ということにある。このため、対策手法の一案としては、認証用データに時間情報（例えば、会議開始時間など）を含め、時間情報の整合性チェックを実施することが挙げられる。

2.3　共有デバイス上の別ユーザへのなりすまし攻撃

Zoom アプリケーションを起動するためのデバイスを複数のユーザ間で共有している状況を想定する。この時、アウトサイダー（共有デバイス上の悪意あるユーザ）は、インサイダーと結託することで共有デバイス上の別ユーザ（被害者）へのなりすましが可能となる。

各ユーザは相互認証で使用する秘密鍵を暗号化し、共有デバイス上のローカルストレージに保存するとともに、その復号鍵を Zoom サーバ上で保存する。ここで、インサイダーとアウトサイダーが結託し、インサイダーがアウトサイダーに被害者の復号鍵を提供することを考える。この時、アウトサイダーは提供された復号鍵で被害者の秘密鍵を復号できるため、被害者になりすまして相互認証を行い、ビデオ会議に参加することが可能となる。

この攻撃が成立する根本的な原因は、Zoom サーバが復号鍵を管理していることにある。このため、対策手法の一案としては、復号鍵の管理を信頼できる第三者機関に委託する、又は秘密分散法を利用して復号鍵のシェアを複数サーバに分散保管することが挙げられる。

2.4　ナンスの再利用に基づく偽造攻撃

会議中のデータ暗号化に使用される AES-GCM では、誤ってナンス（Nonce）が再利用された場合、暗号文から認証鍵を容易に復元できることが知られている [16]–[18]。ホワイトペーパー [8] によると、ナンスはカウンタ機能を用いて生成されると明記されているが、ソフトウェア更新時にインサイダーがトラップドアを仕掛け、ナンスが再利用されるよう改変される可能性も否めない。この場合、既存手法 [16]–[18] に基づく偽造攻撃が成立する。

この攻撃が成立する根本的な原因は、ナンスの再利用に対して脆弱な認証暗号方式を採用していることにある。このため、対策手法の一案としては、ナンスの再利用に対して安全な認証暗号方式を採用することが挙げられる。

2.5　サービス拒否攻撃

2.2 で述べたように、認証用データの一部は掲示板を経由して共有されるとともに、インサイダーは掲示板への自由なアクセスが可能である。つまり、インサイダーは掲示板を経由する認証用データを別のデータに差し替えることが可能である。

掲示板を経由する認証用データの一部とは、各ユーザが生成する鍵交換用の公開鍵と認証用データに対する署名である。ユーザ間で署名を検証し合うことで相互認証が成立するため、認証用データ又は署名に誤りがある場合、ユーザ認証が成立せず、対象となる会議参加者（被害者）が会議に参加できなくなる。このような特徴を悪用し、インサイダーは被害者のユーザ認証が成立する前に、掲示板にアップロードされた公開鍵又は署名を別の異なるデータに差し替えることで、被害者の会議参加を意図的に拒否することが可能となる。

この攻撃が成立する根本的な原因は、インサイダーが掲示板にアクセスできることにある。このため、対策手法の一案としては、掲示板の管理を信頼できる第三者機関に委託することが挙げられる。

2.6　情報開示

我々の安全性評価結果については、2020 年 11 月 16 日に脆弱性報告プラットフォーム HackerOne を通じて Zoom のセキュリティチームに連絡済みであり、論文として公開する許可も得ている。セキュリティチームと議論した結果、本稿で示した攻撃は全て実現し得ることを確認している。その後、2020 年 12 月 15 日に、ホワイトペーパーのバージョンが 2.3.1 から 3 に更新されたことを確認した。

3　E2EE フレームワーク SFrame に対する安全性評価

我々は初期のインターネットドラフト（draft-omara-sframe-01）に記載された仕様に対して安全性評価を実施した [15][19]–[21]。本章では我々の安全性評価によって発見した複数の脆弱性、そしてこれらの脆弱性に起因する攻撃手法とその対策手法について概説する。2024 年 4 月時点において、最新のインターネットドラフトは draft-ietf-sframe-enc-09 であり、我々の評価結果の一部が反映されていることを確認している。また、紙面の都合上、仕様の詳細については文献 [9] を、攻撃者モデルや安全性要件の詳細については文献 [15][19]–[21] を参照されたい。

3.1　SFrame で使用する認証暗号方式の安全性

SFrame では、認証暗号方式として AES-GCM 又は AES-CM-HMAC を採用している。AES-GCM の鍵長は 128 又は 256 ビットであり、タグ長は指定されていない。一方、AES-CM-HMAC とは AES-CTR と HMAC-SHA256 の一般的構成であり、その鍵長は 128 ビット、タグ長は 4 又は 8 バイトに限定されている。

これらの認証暗号方式は証明可能安全性を有しているものの、SFrame では一般的な安全性証明にて想定されている使用方法とは異なる方法で認証暗号方式を

取り扱っているため、既存の安全性証明をもってSFrameで使用する認証暗号方式が安全であるとは言えない状況であった。

我々の評価の結果、SFrameで使用する場合に限り、これらの認証暗号方式が安全であることを明らかにした。しかし、これらの認証暗号方式をSFrame以外で使用する場合には安全性が損なわれる危険性があり、特にAES-CM-HMACのタグ生成アルゴリズムについて改善の余地があったため、その解決案を提示した。詳細は、文献[19]–[21]を参照されたい。

3.2　短いタグ長を指定したAES-CM-HMACに対する偽造攻撃

一般的に、ビデオ会議における音声、動画、共有資料などのデータは、全ての会議参加者間で共有された秘密鍵（共有鍵）を使用して暗号化される。つまり、会議参加者の中に悪意のある攻撃者が存在する場合、この攻撃者は共有鍵を保有しているため、任意のデータに対して暗号化と復号が可能である。この特徴を悪用することで、悪意のある会議参加者は、短いタグ長を指定したAES-CM-HMACに対し、現実的な計算量で偽造攻撃が実行可能となる。

例えば、4バイトのタグ長が指定されたAES-CM-HMACを使用する場合について考える。悪意のある会議参加者は共有鍵を使用して任意のデータから正しい暗号文･タグのペアを自由に生成できるため、2^{32}通りの暗号文・タグのペアを保存した事前計算テーブルを準備することが可能である。この準備段階をオフラインフェーズと呼ぶ。オフラインフェーズが完了したのち、オンラインフェーズとして次の手順を実行する。

1. ある会議参加者から送信されたデータを傍受する。この際、データに含まれる暗号文・タグのペアを(C, T)とする。
2. 攻撃者は事前計算テーブルから$T^* = T$かつ$C^* \neq C$となるような(C^*, T^*)を探索する。
3. 該当するペアが事前計算テーブルに存在する場合、傍受したデータ内のCをC^*に差し替え、他の会議参加者に送信する。

暗号文を差し替えてもタグの値が変化しないため、偽造されたデータの受信者は問題なくタグ検証に成功する。なお、SFrameでは署名機能が導入されているものの、データ全体ではなくタグに対して署名を計算するため、署名検証にも問題なく成功する。ある特定の条件下にて、このような偽造攻撃は100 %の確率で成立する。なお、8バイトのタグ長を指定した場合でも同様に偽造攻撃が成立する。詳細は、文献[19]–[21]を参照されたい。

この攻撃が成立する根本的な原因は、AES-CM-HMACの使用時に4又は8バイトのタグ長しか指定できないことにある。このため、対策手法の一案としては、AES-CM-HMACで長いタグ長（例えば、16バイト）をサポートすることが挙げられる。なお、長いタグ長を指定したAES-CM-HMACの安全性については、文献[19]–[21]で証明済みである。

3.3　AES-GCMに対する偽造攻撃

3.2で紹介した偽造攻撃は、E2EEで使用される認証暗号への汎用的な攻撃であり、オフラインフェーズにおける計算量はタグ長に依存する。一方で、AES-GCMの場合はオフラインフェーズを実行する必要が無く、タグ長に依存しない偽造攻撃が可能となる。この偽造攻撃においても、会議参加者の中に悪意のある攻撃者が存在することを仮定する。つまり、この攻撃者は共有鍵を保有している。

16バイトのタグ長を指定したAES-GCMの場合で具体例を示す。12バイトのナンスN、1ブロック（16バイト）の認証データA、2ブロックの平文$M = (M_1, M_2)$で構成される入力(N, A, M)に対し、AES-GCMでは次のように計算し、暗号文$C = (C_1, C_2)$とタグTを出力する。

$$C_1 = E_K(N \| 2_{32}) \oplus M_1, \tag{1}$$

$$C_2 = E_K(N \| 3_{32}) \oplus M_2, \tag{2}$$

$$T = A \cdot L^4 \oplus C_1 \cdot L^3 \oplus C_2 \cdot L^2 \oplus \mathrm{len}(A, C) \cdot L \oplus E_K(N \| 1_{32}). \tag{3}$$

ここで、E_Kは共有鍵Kを使用したAESでの暗号化関数、$\|$は結合、$\oplus$は排他的論理和、$\cdot$はガロア体上の乗算、$\mathrm{len}(A, C)$はAとCの合計ビット長、$L = E_K(0)$は認証鍵、i_{32}は非負整数iの32ビット値を表す。

攻撃者は秘密鍵Kを知っているため、$L = E_K(0)$を容易に計算できる。最初に、攻撃者は任意のナンスN'と任意の1ブロック分の認証データA'を選択する。次に、選択したN'と偽造した平文ブロックM_1'から、式(1)に従ってC_1'を計算する。最後に、式(3)を変換し、以下の等式が成り立つようにC_2'とT'を決定する。

$$C_2' \cdot L^2 = T' \oplus A' \cdot L^4 \oplus C_1' \cdot L^3 \oplus \mathrm{len}(A', C') \cdot L \oplus E_K(N' \| 1_{32}). \tag{4}$$

ここで、攻撃者がT'にTを代入すると、攻撃者によって偽造されたデータには偽造前と同じタグ$T = T'$が含まれることとなるため、**3.2**の偽造攻撃と同様、タグ検証と署名検証が問題なく成功する。なお、この具体例の場合、M_1'を任意の平文に偽造できるが、M_2'を任意

の平文に偽造できないことに注意が必要である。

この攻撃が成立する根本的な原因は、AES-GCM のタグ生成アルゴリズムが線形性を有していること、そしてデータ全体ではなくタグに対して署名を計算していることにある。このため、対策手法の一案としては、HFC [22] のような認証暗号方式を採用すること、又はタグではなくデータ全体に対して署名を計算することが挙げられる。このような対策手法の有効性については文献 [21] で議論しているため、その詳細は文献 [21] を参照されたい。

3.4　短いタグ長を指定した AES-GCM に対する認証鍵回復攻撃

3.1 で説明したように、AES-GCM の使用において 4 又は 8 バイトのような短いタグ長を指定することも可能である。この場合、前節の偽造攻撃に加え、アウトサイダー（悪意のある任意のユーザ）による認証鍵回復攻撃のリスクを考慮する必要がある。なお、認証鍵が導出できる場合、アウトサイダーによる偽造攻撃が実行可能となる。

この攻撃の実行可能性については、Ferguson によって初めて指摘された [17]。さらに、Mattoson と Westerlund が Ferguson の研究を発展させ、攻撃に必要な計算量の厳密な評価を実施した [23]。文献 [23] によると、文献 [24] で定められている制約事項を厳守する場合、例えば 4 バイトのタグ長を指定する AES-GCM への認証鍵回復攻撃は、少なくとも 2^{61} の計算量が必要であると明記されている。しかしながら、この制約事項を厳守しない場合、タグ長を t とすると、認証鍵は 2^t で復元可能となる。つまり、4 バイトのタグ長を指定する場合、認証鍵回復攻撃は 2^{32} という現実的な計算量で実行可能となる。

インターネットドラフト [9] にはこのような制約事項について明記されていない。また、開発者による SFrame 実装 [25]、Cisco Webex における SFrame 実装 [26]、Jitsi Meet における SFrame 実装 [27] のソースコードが公開されているが、文献 [19]–[21] 執筆時点でこのような制約事項が適用されていないことを確認している。このため、対策手法の一案としては、文献 [24] で定められている制約事項を仕様書に明記することが挙げられる。その上で、SFrame を導入する各開発者は、このような制約事項を厳守して実装する必要がある。

3.5　情報開示

我々の安全性評価結果については、2021 年 3 月にメールとビデオ会議を通じて SFrame の設計者に報告済みであり、論文として公開する許可も得ている。SFrame の設計者と議論を重ねた結果、本稿で示した攻撃については全て実現し得ることを確認している。我々の脆弱性報告を受け、設計者は署名メカニズムの削除とタグ生成メカニズムの強化を速やかに実施し、2021 年 3 月 29 日にインターネットドラフトを draft-omara-sframe-02 に更新した。

4　むすび

本稿では、Zoom の E2EE と SFrame に対する安全性評価の研究を紹介した。

Zoom の E2EE に対し、ホワイトペーパーのバージョン 2.3.1 [8] に基づき安全性評価を実施し、Zoom が想定するよりも強力な攻撃が実行可能であることを示した。特に、インサイダーが悪意のある攻撃者と結託した場合、インサイダーは会議参加者にのみなりすましが可能であると想定していたが、我々の安全性評価においてインサイダーは任意のユーザになりすましが可能であることを明らかにした。

SFrame に対し、インターネットドラフトの draft-omara-sframe-01 [9] に基づき安全性評価を実施し、E2EE に対する汎用的な攻撃としての偽造攻撃が現実的な計算量で実行可能であることを示した。特に、SFrame では悪意のある会議参加者からの偽造攻撃を防ぐために各ユーザ固有の署名を添付しているが、データ全体ではなくタグのみに対する署名を計算した場合、汎用的な偽造攻撃を防ぐことができない場合があることを明らかにした。

ビデオ会議システムに導入される E2EE はまだ発展途上の技術であり、本稿執筆時点（2024 年 4 月末）において、Zoom の E2EE に関するホワイトペーパーや SFrame に関するインターネットドラフトは定期的に更新されている状況である。これらの技術が今後も幅広く利用されることを考えると、これらの E2EE に対する安全性評価は継続的かつ活発に行われるべきである。このような観点から、我々の研究がビデオ会議システムにおける E2EE の発展に貢献できることを信じている。また、メッセージングアプリケーションやビデオ会議システムに限らず、クラウドストレージ、パスワードマネージャー、SNS アプリケーション、IoT 機器など、様々なアプリケーション・製品に E2EE が導入されるようになってきている。このような観点から、我々の E2EE に対する安全性評価の知見を持ってこれらの E2EE に対する安全性評価を実施し、国民生活を支える様々なシステムの安全な運用に貢献していくことが今後の継続的な課題となる。

【参考文献】

1 T. Isobe and K. Minematsu, “Breaking Message Integrity of an End-to-End Encryption Scheme of LINE,” Proceedings of the ESORICS 2018, LNCS, vol.11099, pp.249–268, Springer, 2018.
2 C. Garman, M. Green, G. Kaptchuk, I. Miers, and M. Rushanan, “Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage,” Proceedings of the the 25th Usenix Security Symposium, pp.655–672, Usenix Association, 2016.
3 P. Rosler, C. Mainka, and J. Schwenk, “More is less: On the End-to-End Security of Group Chat in Signal, WhatsApp, and Threema,” Proceedings of the 2017 IEEE European Symposium on Security and Privacy, pp.415–429, IEEE Computer Society, 2017.
4 M. R. Albrecht, L. Marekova, K. G. Paterson, and I. Stepanovs, “Four Attacks and a Proof for Telegram,” Proceedings of the 2022 IEEE Symposium on Security and Privacy, pp.87–106, IEEE Computer Society, 2022.
5 T. von Arx and K. G. Paterson, “On the Cryptographic Fragility of the Telegram Ecosystem,” Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, pp.328–341, 2023.
6 M. R. Albrecht, S. Celi, B. Dowling, and D. Jones, “Practically-Exploitable Cryptographic Vulnerabilities in Matrix,” Proceedings of the 2023 IEEE Symposium on Security and Privacy, pp.1419–1436, IEEE Computer Society, 2023.
7 M. R. Albrecht, M. Backendal, D. Coppola, and K. G. Paterson, “Share with Care: Breaking E2EE in Nextcloud,” Proceedings of the 2024 IEEE European Symposium on Security and Privacy, to appear, IEEE Computer Society, 2024.
8 J. Blum, S. Booth, O. Gal, M. Krohn, J. Len, K. Lyons, A. Mercedone, M. Maxim, M. E. Mou, J. O’Connor, M. Steele, M. Green, L. Kissner, and A. Stamos, “E2E Encryption for Zoom Meetings - Version 2.3.1,” 2020. https://github.com/zoom/zoom-e2e-whitepaper/blob/master/archive/zoom_e2e_v2_3_1.pdf
9 E. Omara, J. Uberti, A. Gouaillard, and S. Murillo, “Secure Frame (SFrame),” https://datatracker.ietf.org/doc/html/draft-omara-sframe-01, 2020
10 Nostr, “A decentralized social network with a chance of working,” https://nostr.com
11 https://www.forbes.com/sites/digital-assets/2023/05/30/bitcoin-social-network-nostr-creator-fiatjaf-/?sh=43c40c1711c0
12 五十部孝典, 伊藤竜馬, “Zoom のエンドツーエンド暗号化に対する安全性評価,” Proceedings of the SCIS 2021, 3B3-1, 2021.
13 Takanori Isobe and Ryoma Ito, “Security Analysis of End-to-End Encryption for Zoom Meetings,” Proceedings of the ACISP 2021, LNCS, vol.13083, pp.234–253, Springer, 2021.
14 Takanori Isobe and Ryoma Ito, “Security Analysis of End-to-End Encryption for Zoom Meetings,” IEEE Access, vol.9, pp.90677–90689, 2021.
15 Takanori Isobe, Ryoma Ito, and Kazuhiko Minematsu, “Cryptanalysis on End-to-End Encryption Schemes of Communication Tools and Its Research Trend,” Journal of Information Processing, vol.31, pp.523–536, 2023.
16 D. A. McGrew and J. Viega, “The Security and Performance of the Galois/Counter Mode of Operation (Full Version),” IACR Cryptology ePrint Archive, 2004/193, 2004.
17 N. Ferguson, “Authentication Weaknesses in GCM,” the Comments on the Choice Between CWC or GCM to NIST, 2005.
18 A. Joux, “Authentication Failures in NIST Version of GCM,” the Comments on the Draft GCM Specification to NIST, 2006.
19 五十部孝典, 伊藤竜馬, 峯松一彦, “エンドツーエンド暗号化 SFrame に対する安全性評価,” Proceedings of the CSS 2021, 2E3-3, 2021.
20 Takanori Isobe, Ryoma Ito, and Kazuhiko Minematsu, “Security Analysis of SFrame,” Proceedings of the ESORICS 2021, LNCS, vol.12973, pp.127–146, Springer, 2021.
21 Takanori Isobe, Ryoma Ito, and Kazuhiko Minematsu, “Security Analysis of SFrame,” IACR Cryptology ePrint Archive, 2021/424, 2021.
22 Y. Dodis, P. Grubbs, T. Ristenpart, and J. Woodage, “Fast Message Franking: From Invisible Salamanders to Encryptment,” Proceedings of the CRYPTO 2018, LNCS, vol.10991, pp.155–186, Springer, 2018.
23 J. Mattsson and M. Westerlund, “Authentication Key Recovery on Galois/Counter Mode (GCM),” Proceedings of the ASIACRYPT 2016, LNCS, vol.9646, pp.127–143, Springer, 2016.
24 M. Dworkin, “Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality,” NIST SP 800-38C, 2007.
25 https://github.com/medooze/sframe
26 https://github.com/cisco/sframe
27 https://github.com/jitsi/lib-jitsi-meet/

伊藤 竜馬（いとう りょうま）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
共通鍵暗号の解析・設計、実際のシステムに対する安全性評価

【受賞歴】
2023年　Journal of Information Processing, Specially Selected Paper certificate, IPSJ
2023年　情報処理学会 2022年度山下記念研究賞
2022年　電子情報通信学会 SCIS 2021 イノベーション論文賞