平成 30 年度

修士学位論文

セキュアグループ通話システムの実現に向けた SAS Phone の拡張

An SAS Phone System for Group Voice Communications

1215096　藤田 寛泰

指導教員　清水 明宏

2019 年 1 月 31 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報学コース

要 旨

セキュアグループ通話システムの実現に向けた SAS Phone の拡張

藤田 寛泰

ワークスタイルの多様化を背景にテレワークを実現するための技術として VoIP が注目を集めている．VoIP はインターネットを介した音声通話を提供する技術で，安価にグローバルなコミュニケーションを可能とするためテレワークとの親和性が高い．一方，第三者による盗聴といったセキュリティリスクが懸念されるため TLS などのセキュリティ対策が必須である．TLS は広く普及した技術ではあるが，一般的にセッション中で利用する暗号鍵は固定であるため，暗号解析攻撃により鍵が危殆化する可能性がある．この攻撃への対策として，暗号鍵の更新を考慮した音声通話システム SAS Phone が提案されている．SAS Phone では， 鍵更新に利用する SAS 鍵配送プロトコルの制約によりグループ通話が困難である．

本稿では，SAS グループ鍵配送プロトコルを提案し，小規模グループに適した通話システムとして SAS Phone を拡張する．拡張後の SAS Phone は，グループ通話で求められるセキュリティ要件を満たし，創造会議などの発言権が制御されない会議システムに応用できる．なお，鍵更新処理が QoS に及ぼす影響については明らかになっていない．

キーワード　VoIP, SAS Phone, SAS 鍵更配送プロトコル, グループ通信

Abstract

An SAS Phone System for Group Voice Communications

Hiroyasu FUJITA

VoIP is a promising voice call technology that enables teleworks where we can collaborate with each other regardless of locations. TLS is the most popular security technology and it is used to secure voice calls in VoIP. However, a single encryption key is used and this may bring a vulnerability to cryptographic analysis attacks. Hence, a voice call system called SAS phone is proposed. It is secure against the attack because it provides a key updating mechanism using a SAS key distribution protocol. The protocol, which can be only used for two-party communication, causes SAS Phone to be applied to just two-party calls.

In this paper, a SAS group key distribution protocol is proposed to enable SAS Phone to be used for group calls. The call system achieves security requirements and can be applicable to small size of group calls such as a creative type of conferences. Effectness of key update processing on QoS is not revealed.

key words VoIP, SAS Phone, SAS key exchange protocol, Group communications

目次

目次

図目次

表目次

第 1 章

序論

1.1 背景

近年，ワークスタイルの多様化によりテレワークの実現に向けた，地理的制約や時間的制約にとらわれない遠隔コミュニケーションシステムの必要性が増している．テレワークでは，自宅・サテライトオフィス・本社オフィス等さまざまな場所や時間帯において 2 者間または 3 者以上のグループ間でのコミュニケーションが行われる．

Voice over Internet Protocol (VoIP) は，インターネットを介した音声通話を提供する技術であり，従来の専用線を用いる方法と比較し安価に運用できる点からテレワークとの親和性が高い．一方で，インターネットを利用することで第三者による盗聴のリスクが懸念されるためセキュリティ対策が必須である．

従来的なセキュリティ対策としては，Transport Layer Security (TLS)[1] を用いた VoIP over TLS (VoIPS) がある．TLS は広く普及した技術ではあるが，通信セッション間では暗号鍵は異なるが，同一セッション内では固定である．そのため，セッションが長期化する VoIP アプリケーションなどでは暗号鍵の危殆化が懸念される．実際に，TLS に対する選択型平文攻撃に基づく暗号解析によりメッセージの解読に成功した事例が報告されている [2]．これは，暗号文に存在する共通パターンの捕捉により鍵の特定ができることを示唆するため，セッション内においても鍵更新が重要である．暗号鍵を定期的に更新するメリットとして，暗号文間の依存性を小さくすることで鍵の類推が極めて困難になることと，万が一暗号鍵が漏洩しても影響範囲を限定できることが挙げられる．一方で，デメリットとしては，更新のコストが高い場合にアプリケーションの提供するサービス品質の低下が考えられる．音

声通話のようなリアルタイムなインタラクションを必要とする場合には，鍵更新処理がボトルネックとならないように処理の軽量さが重要となる．

このような背景から，通話セッション内で暗号鍵を更新する仕組みを有する音声通話システム SAS Phone が提案されている [3]．このシステムでは，Simple And Secure password authentication protocol (SAS) [4] に基づく SAS 鍵配送プロトコルを用いて鍵更新を行う．SAS は，公開鍵暗号方式をベースとした手法や類似するワンタイムパスワード認証方式と比較し極めて処理負荷の小さな方式であることから，音声通話における鍵更新に適していると考えられる．しかし，SAS 鍵配送プロトコルは 2 者間でのみ鍵配送が可能なため，SAS Phone ではグループ通話が行えないという問題がある．SAS Phone でグループ通話を実現するには，SAS 鍵配送をグループメンバ間で実行可能なプロトコルとして拡張する必要がある．

そこで本論文では，SAS グループ鍵配送プロトコルを提案しそれを用いることで，セキュアグループ通話システムとして SAS Phone を拡張する．そして，グループ通話に求められるセキュリティ要件に基づき，拡張後の SAS Phone を評価する．

1.2　本論文の構成

本論文は全 6 章で構成される．第 2 章では，従来の SAS Phone を解説し，音声通話システムで求められるセキュリティ要件を定義する．第 3 章では，SAS 鍵配送プロトコルでグループ通信を実現する方法を検討し問題点を明らかにし，第 4 章で，SAS グループ鍵配送プロトコルを提案する．第 5 章では，提案する SAS グループ鍵配送プロトコルを用いた SAS Phone の拡張を行い，第 6 章で結論を述べる．

第 2 章

音声通話システム

本章では，音声通話システムに関する導入として VoIP と SAS Phone について述べる．その後，グループ通話における脅威とセキュリティ要件を述べる．

2.1 VoIP の概要

インターネット回線や LAN のブロードバンド化が進み，異なる通信網を共用する動きがある．その動きの中で，専用回線を用いていた一般電話回線や，内線電話回線を LAN や WAN で用いる動きが出てきた．電話回線を LAN や WAN を用いて実現することを VoIP という．具体的には，音声情報を様々な符号化方式を用いて符号化し，符号化されたデータをパケットとして，IP 網を用いて転送する技術である．VoIP では，専用線を必要としないため一般電話よりも通話料金を安くすることが可能となる．

VoIP の代表的な規格として，国際電気通信連合 (ITU-T) 勧告による規格 VoIP/H.323 や，現在最も注目を集めている VoIP/SIP(Voice over Internet Protocol / Session Initiation Protocol) がある．以下では，VoIP/SIP について述べる．

2.1.1 VoIP / SIP

SIP とは，アプリケーション層を利用した音声，動画，テキストメッセージなどを二者以上でやり取りするためのプロトコルである．主たる機能としてセッションの生成，変更，切断を行う機能がある．

図 2.1 にプロトコルスタックを示す．VoIP/SIP を用いるためには，主に VoIP/SIP 対応

アプリケーション，SIP プロキシが必要となる．次に，図 2.1 に示す，代表的な VoIP/SIP を用いた電話発信から通話終了までのコールフロープロトコルを示す．

まず，発信者 A は，SIP サーバ A に対し，INVITE リクエストメッセージを送信する．INVITE メッセージを受け取った SIP サーバ A は適当な SIP サー バ B に INVITE メッセージを送信する．それと共に，SIP サーバ A は，応答 100 Trying メッセージを発信者 A に送信する．INVITE メッセージを受け取った SIP サーバ B は，着信者 B に対し，INVITE メッセージを送信する．その後，SIP サーバ B は，SIP サーバ A に対し，応答 100 Trying メッセージを送信する．INVITE メッセージを受け取った着信者 B は，SIP サーバ B および SIP サーバ A を経由し，応答 180 Ringing メッセージと応答 200 OK メッセージを送信する．この時点で，発信者 A と，着信者 B は，通話可能状態と なる．次に，発信者 A は，SIP サーバ A および SIP サーバ B を経由し，ACK メッセージを送信し，通話状態となる．その後，通話終了まで音声データを発信者 A および着信者 B 同士で送受信し，再生する．通話終了を行う際，発信者 A もしくは着信者 B が BYE メッセージを他方に送信する．BYE メッセージを受け取ったユーザは，セッション切断メッセージとして，200 OK メッセージを送信し，セッション切断となる．

これらにより，電話発信， 通話状態，通話終了が実現できる．

SIP プロトコル	SDP	SIP	RTP/RTCP
トランスポート層	TCP	UDP	
ネットワーク層	IP		

表 2.1　VoIP / SIP プロトコルスタック

2.1.2　通話セッションのトポロジ

通話開始から終了までのセッションにおける通信方式としては，ユニキャストまたはマルチキャストが利用される．それらを用いて図 2.2 のようなトポロジを形成し通信を行う．これらのトポロジは一種類に限定する必要はなくアプリケーションで選択することができる．

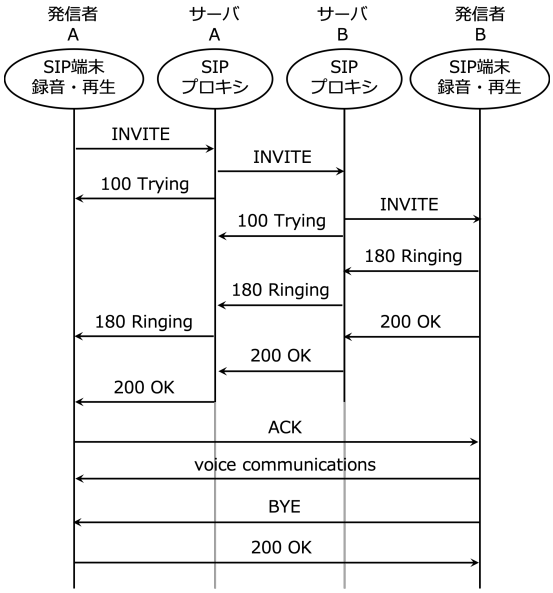

図 2.1　SIP コールフロープロトコル

2 人の参加者の間での通話の場合はユニキャストを選択し，グループ通話のようにグループ全体への送信が必要な場合はマルチキャストを使用する [5]．マルチキャストを行うにはルータの明示的な設定を必要とする場合があり [6]，必ずしも利用できるとは限らない．そのような場合は，ユニキャストとマルチキャストの組み合わせなどが有効である．

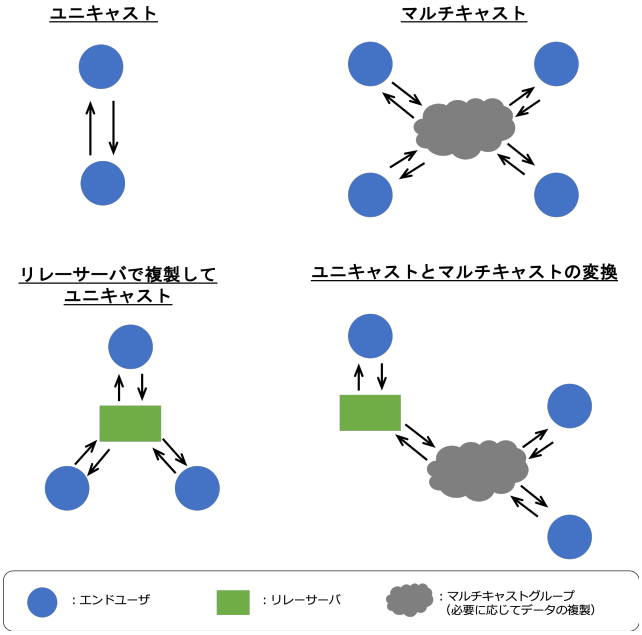

図 2.2　通話セッションのトポロジ

2.2 SAS Phone

SAS Phone は，VoIP アプリケーションの一つであり，鍵の更新を定期的に行うことでセキュアな音声通話を提供することができる．鍵の更新には，SAS 認証を鍵配送に応用した SAS 鍵配送プロトコルを用いることで高速な鍵更新を実現を実現している．以下では，SAS Phone におけるシステム構成およびセットアップフェーズ/音声転送フェーズについて述べる．

2.2.1 システム構成とコールフロー

VoIP における通信では，IP アドレスを用いて通話相手を特定する．しかし，LAN 内の端末の IP アドレスは NAT により隠蔽されていることがあり，LAN 外からの直接的な呼び出しは現実的には困難である．そこで，SAS Phone では図 2.3 のようなシステム構成をとり 2 者間での通話を行う．

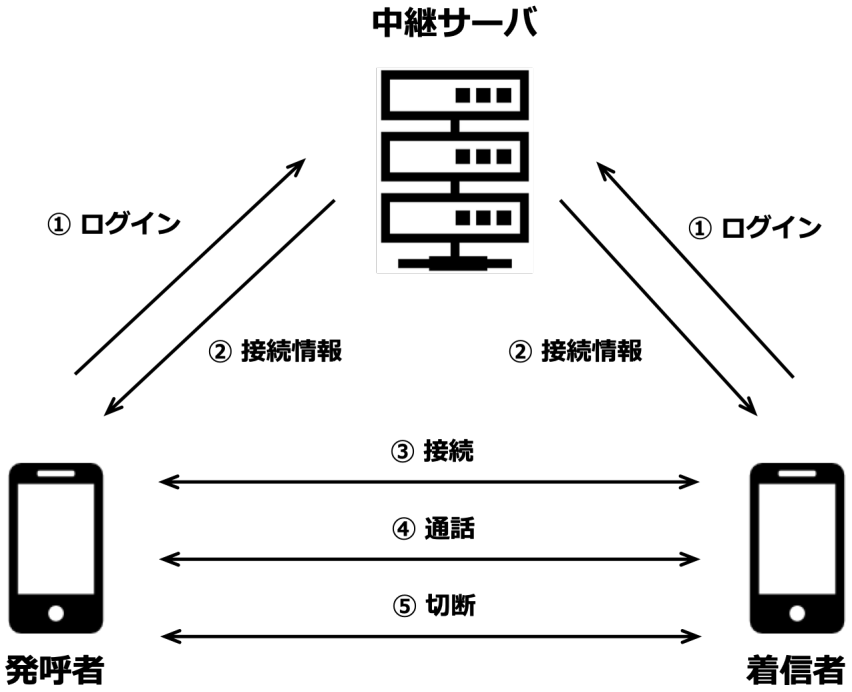

図 2.3 SAS Phone におけるシステム構成およびコールフロー

2.2.2 セットアップフェーズ / 音声転送フェーズ

セットアップフェーズおよび音声転送フェーズをそれぞれ図 2.4，2.5 に示す．セットアップフェーズは，接続開始直後にのみ実行され SAS 認証情報が共有される．SAS 認証情報は SAS 鍵配送にて利用される．一方，音声転送フェーズは，1 ～ 1000[ms] の間で定期的に実行される．このフェーズでは，鍵配送の実行後に共有した暗号鍵を用いて音声データを 2 者間でやり取りする．

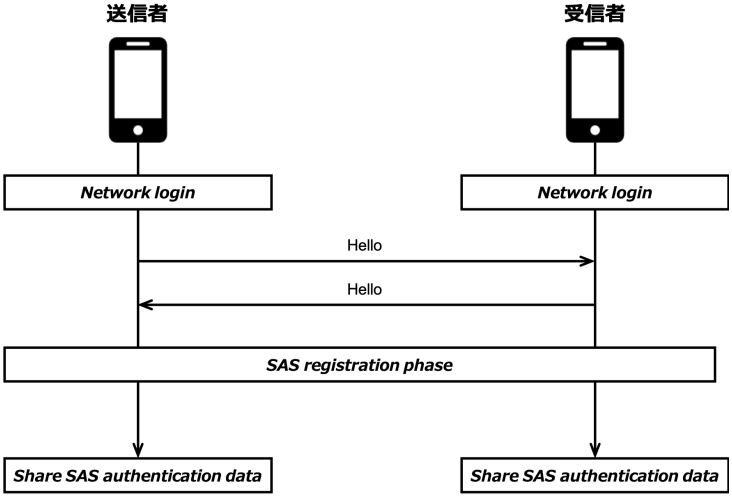

図 2.4 SAS Phone のセットアップフェーズ

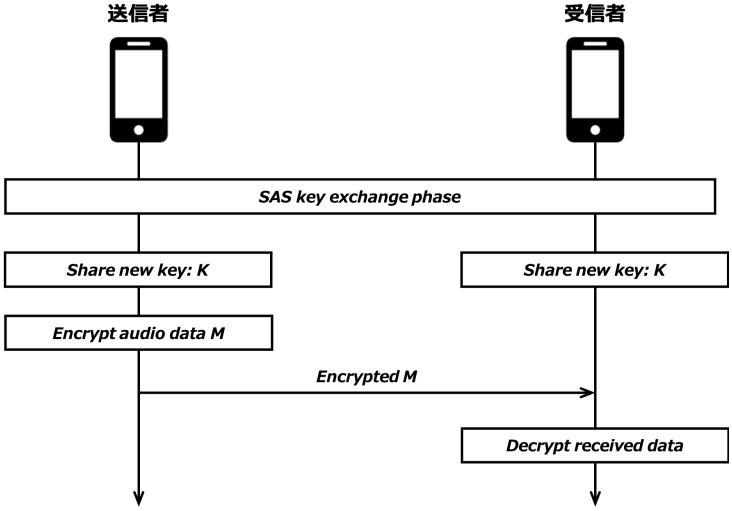

図 2.5 SAS Phone の音声転送フェーズ

2.3　音声通話システムにおけるセキュリティ要件

本節では，セキュアな音声通話システムで必要となるセキュリティ要件を定義する．

2.3.1　音声通話システム全般が満たすべきセキュリティ要件

機密性

通話セッションに参加するメンバのみが通話内容を知ることができる．SAS Phone は，2 者間のみがデータにアクセス可能なためこの要件を満たす．

暗号鍵の更新

通話アプリケーションは，比較的一つのセッションが長期化することから暗号解析攻撃に対する懸念が大きい．この攻撃に対しては，暗号鍵を変更することで耐性を高めることができる．SAS Phone は，定期的な暗号鍵の更新によりこれを満たす．

整合性

エンドユーザ間で適切に暗号鍵の共有ができる．鍵更新を前提にする場合，パケットロス更新後に利用する暗号鍵はメンバ全体で確実に共有している．SAS Phone で用いる SAS 鍵配送では鍵の同期がとれない場合が考えられるためこの要件を満たさない．

鍵更新時の認証

新しい鍵が信頼できるユーザから送信されたかを検証できる．SAS Phone では，鍵配送と認証を提供する SAS 鍵配送プロトコルを用いているためこの要件を満たす．

2.3.2　3 者以上のグループ通話システムが満たすべきセキュリティ要件

前方秘匿性

グループ通話では，セッションの一部にだけ参加を許可されたユーザが存在しうるため，そのユーザが退出した際に，それ以降の通話内容を知りえないことが必要である．

後方秘匿性

前方秘匿性と同様に，一部の通話に参加可能なユーザが途中参加した場合に，それ以前の通話内容を知りえないことが必要である．

可用性

グループから任意のメンバが抜けたたとしても，2 名以上が通話セッションに参加している場合は通話を維持できる．

第 3 章

SAS 鍵配送プロトコル

鍵配送プロトコルは，鍵を正当な通信相手に対して安全に届ける方式である．SAS Phone では，Simple And Secure password authentication protocol (SAS) を鍵配送プロトコルとして応用している．このプロトコルは，排他的論理和やハッシュ関数などの低負荷な処理で構成されていることから，高速な鍵配送が求められるサービスでの応用が期待される．

以下では，SAS 鍵配送プロトコルを構成する登録フェーズ，鍵配送フェーズについて述べる．なお，表記法には表 3.1 を用いる．

表 3.1　用語および記号の定義

“今回認証情報”	ユーザとサーバで共有している情報を指す
“次回認証情報”	ユーザがサーバへ登録する新しい認証情報を指す
i	鍵配送フェーズを区別するための 1 以上の整数値
N_i	擬似乱数．i 回目の鍵配送フェーズにおける今回認証情報作成に用いられる
$+$	加算演算子
$\oplus$	排他的論理和演算子
ID	ユーザを表す識別子
A_C	今回認証情報
A_N	次回認証情報
H	暗号学的ハッシュ関数
KFD	鍵導出関数
EK	KFD によって生成された暗号鍵

3.1　登録フェーズ

登録フェーズは，鍵配送前に一度だけ実行され，情報共有の手段には安全な通信路を必要とする．図 3.1 に登録フェーズを示す.

$User$

1. 乱数 N_1 を生成し，自身の識別子 ID を用いて認証情報 $A_C = X(ID, N_1)$ を計算
2. 安全な経路を用いて ID, A_C をサーバへ送信
3. 初回鍵配送フェーズに備え ID，A_C を保存

$Server$

3. 受信した ID と A_C を保存し，さらに，$A_B = A_C$ としてバックアップ

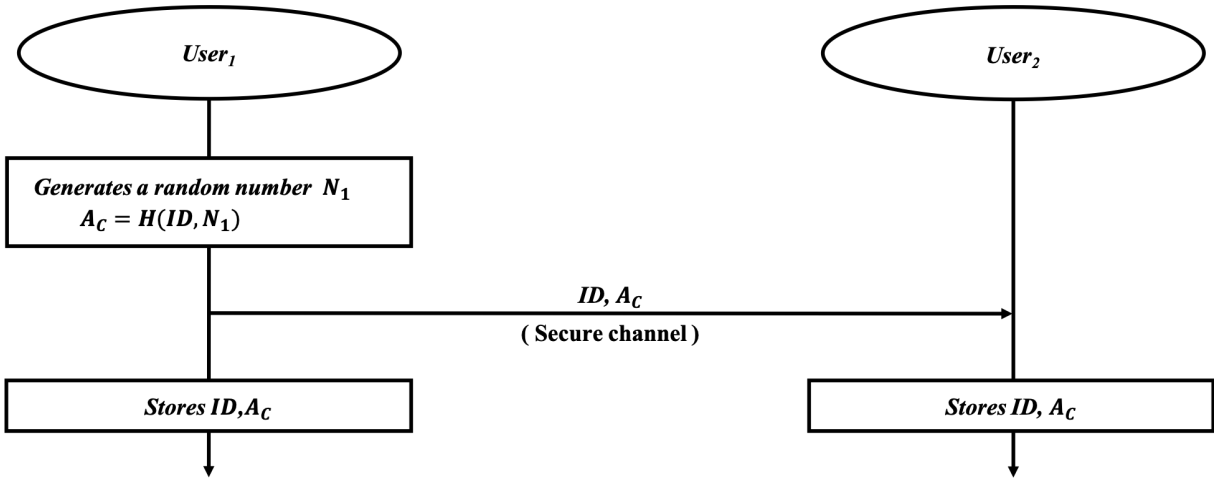

図 3.1　登録フェーズ

3.2　鍵配送フェーズ

このフェーズでは，まず SAS 認証を実行する．その後，2 者間で同一の情報が共有されるためそれを暗号鍵に変換することで鍵配送が完了する．

図 3.2 に第 i 回目の鍵配送フェーズを示す．

$User_1$

1. 乱数 N_{i+1} を生成し，$A_N = H(ID, N_{i+1}))$ および $H(A_N) = H(ID, A_N)$ を計算．
2. 通信データ $\alpha = A_N \bigoplus (H(A_N) + A_C)$，$\beta = H(A_N) \bigoplus A_C$ を計算．
3. 今回認証情報 A_C を 次回認証情報 A_N の値で更新．
4. サーバに，ID，α および β を送信．
5. 次回認証情報 A_N を用いて $EK = KDF(H(A_N))$ とすることで暗号鍵を計算．

$User_2$

6. 受信した β と A_C を使用し，$H(C) = \beta \bigoplus A_C$ を算出．さらに，これと A_C を用い，$A_N = \alpha \bigoplus (H(C) + A_C)$ を算出．
7. $H(A_N)$ と $H(ID, A_N)$ を比較して一致した場合にユーザを認証し以下を実行．一致しなかった場合は，認証不成立で鍵の更新が行われない．
8. 今回認証情報 A_C を 次回認証情報 A_N の値で更新．
9. 次回認証情報 A_N を用いて $EK = KDF(H(A_N))$ により暗号鍵を計算．

3.2　鍵配送フェーズ

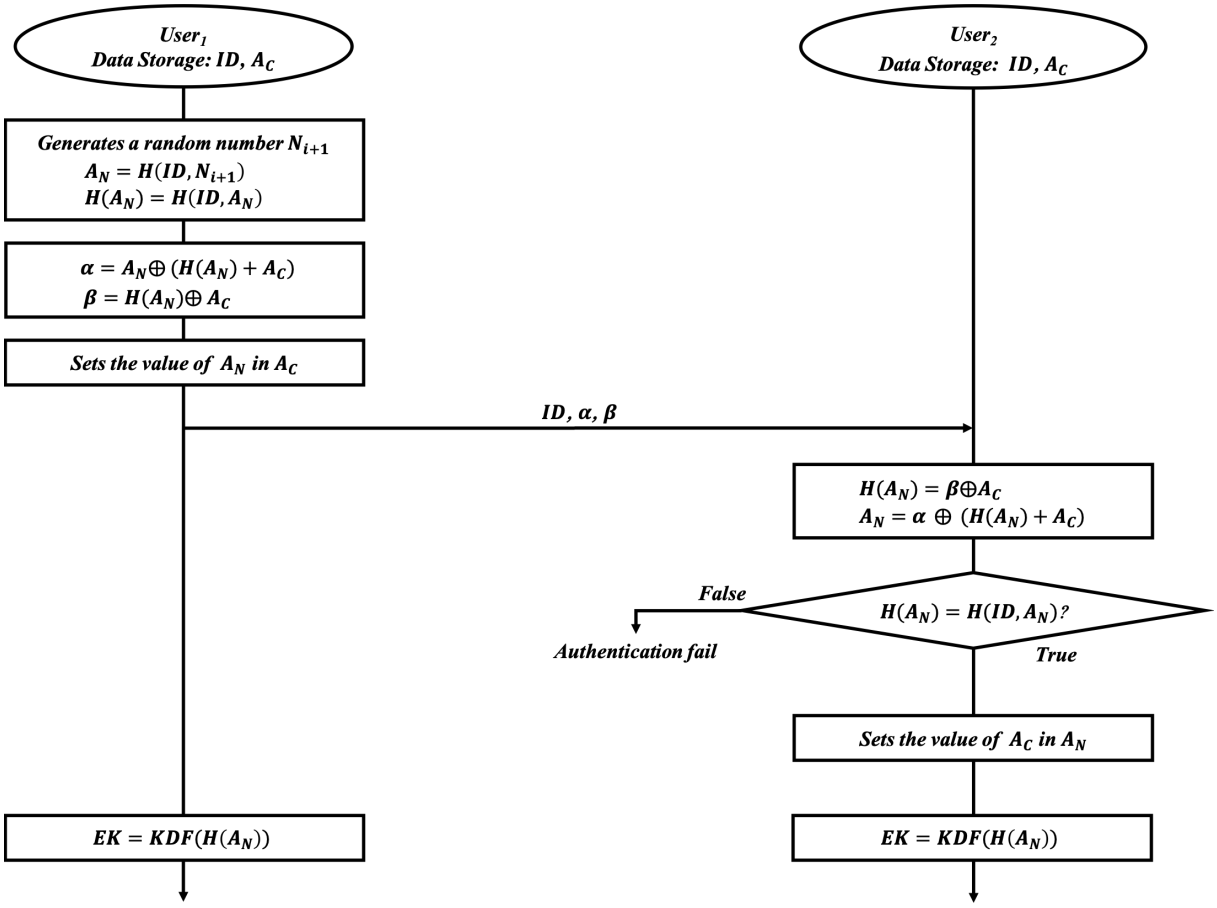

図 3.2　鍵配送フェーズ

3.3　グループ鍵配送の実現に向けた検討

SAS 鍵配送では，2 者間での鍵配送のみを想定しているためグループ間での利用には拡張が必要である．通信経路上では，パケットロスにより同期ズレが生じることで鍵の共有ができない可能性があるため，その対策も合わせて必要となる．

以下では，グループ鍵配送スキームおよび同期ズレを考慮した SAS 鍵配送プロトコルについて述べ，グループ鍵配送プロトコルを示す．さらに，そのプロトコルで懸念される DoS 攻撃について述べる．

3.3.1　グループ鍵配送スキーム

グループ鍵配送を実現する方法としては，ユニキャストまたはマルチキャストを問わず，図 3.3 のようにコントローラを中心として行う方法が考えられる．

一般に，コントローラに依存する鍵管理スキームはそのノードが単一障害点となるが，SAS 鍵配送においては，認証情報 A_C を持つものであれば任意のメンバがコントローラの役割を担うことが可能であるため障害耐性に強いという特徴がある．

そこで，本論では鍵配送スキームとしてコントローラを中心としたものを用いる．

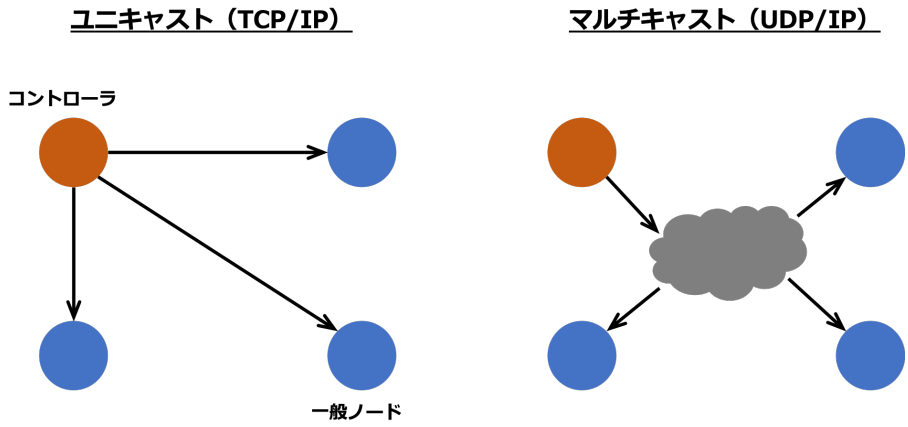

図 3.3　コントローラによるグループ鍵配送スキーム

3.3.2　同期ズレを考慮した SAS 鍵配送プロトコル

SAS Phone で利用する SAS 鍵配送プロトコルでは，通信データが経路上で損失した場合，認証情報の更新を行う側と行わない側が存在することで，互いに所持している情報にズレが生じる場合がある．これを同期ズレと呼ぶ．同期ズレが発生した場合，鍵の共有ができなくなる．

同期ズレへの対策として中原らによる SAS 鍵配送プロトコルが提案されている [7]．中原の方式における鍵配送フェーズを図 3.4 に示す．従来の SAS 鍵配送との違いは次の通りである．

- $User_1$ と $User_2$ のみが知りうる情報を利用して返信

  具体的には，3.2 項のステップ 8 の処理後に，$\gamma = H(ID, H(A_N))$ を返信
- $User_1$ と $User_2$ の認証情報の更新の順番を $User_2$，$User_1$ としている
- $User_2$ は認証情報をバックアップ

  $User_2$ が送信した γ が経路上で損失した場合に，$User_1$ では更新処理が実行されないため同期ズレが生じる．これに対しては，3.2 項のステップ 8 にて，A_C の値を A_B としてバックアップをとることで対処可能である．これにより，$User_2$ は A_N と $A_B = A_C$ の 2 つの情報を持つことになり，$User_1$ 側で更新処理が行われない場合でも A_C を共有しているためその後の鍵配送も行える．

3.3　グループ鍵配送の実現に向けた検討

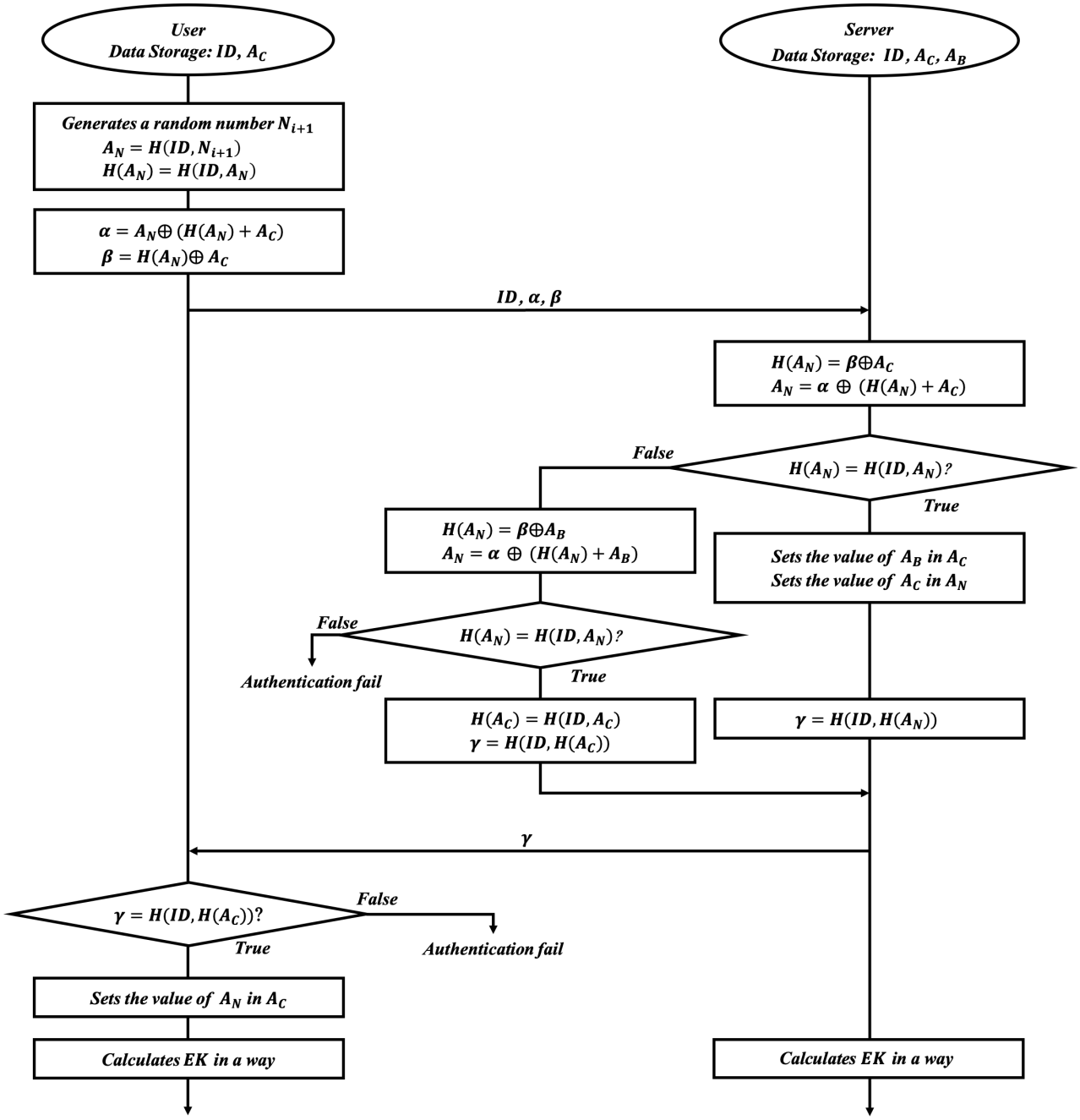

図 3.4　同期ズレに対処した SAS 鍵配送

3.3.3　SAS グループ鍵配送プロトコルに対する DoS 攻撃

中原らの同期ズレを考慮した SAS 鍵配送プロトコルに対してグループ鍵配送スキームを適用した場合の，鍵配送時における通信の概要を図 3.5 に示す．コントローラを起点とし，グループ内のユーザ $User_1$ と $User_2$ に対して，ID, α, β を送信する．さらに，すべてのユーザから γ が返信された場合に認証情報を更新する．これによって，コントローラを含めたすべてユーザ間で共通の鍵を共有できるようになる．

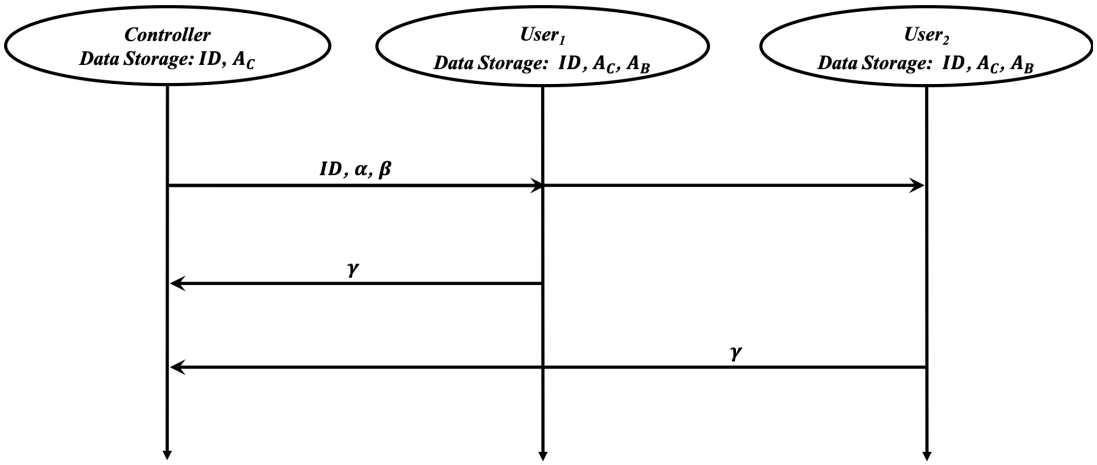

図 3.5　SAS グループ鍵共有の通信フロー

しかし，図 3.6 のように $User_2$ に通信データが届かない場合，攻撃者が，$User_1$ が送信した γ を盗聴し $User_2$ の代わりにそれを送信することで，同期ズレを引き起こすことが可能である．

この問題に対する解決策として，TCP に基づく高信頼な通信が利用できるユニキャスト型のグループ通信を用いる方法が考えられる．TCP は，確認応答 (ACK) が送信先から受信できない場合にパケットを再送する機能を提供する [8]．これにより $User_2$ に通信データを届けることができ，上記で想定した攻撃を実行したとしても同期ズレは起きない．しかし，攻撃者が $User_2$ 宛のパケットを経路上で盗聴した場合に，攻撃者側で不正に作成した ACK によって再送を妨害することが可能である．よって，ユニキャスト型のグループ通信を用いた場合でも同期ズレが起こりうるため別の対策が必要となる．

また，この問題に関連し，コントローラからデータを受信できた $User_1$ が鍵を更新しそれを利用した場合，受信ができなかった $Usre_2$ は $User_1$ から送られてきた暗号化された音声パケットにアクセスできない．そのため，コントローラによる鍵更新の許可を意味するメッセージをユーザ全体に送信する必要がある．ただし，メッセージの不正送信を防止するために，グループメンバのみが知る情報を含める必要がある．

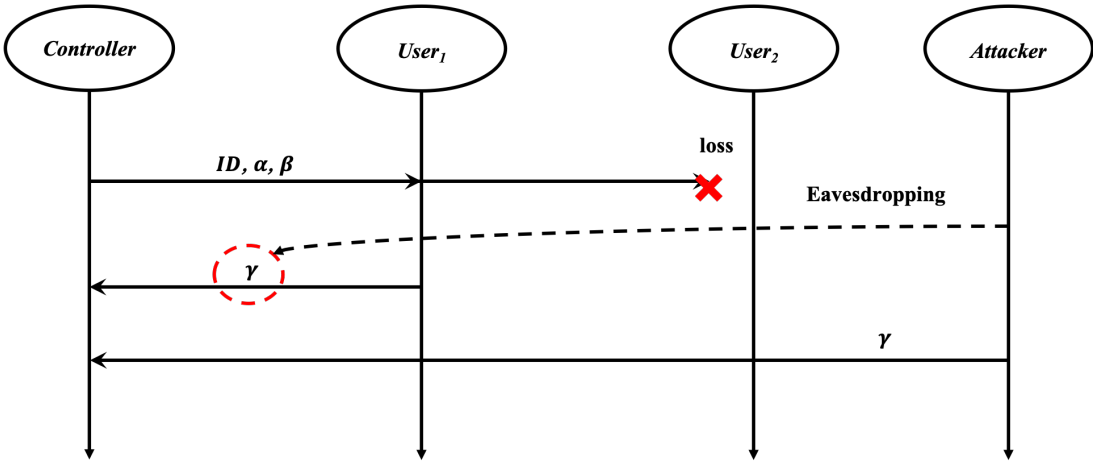

図 3.6　SAS グループ鍵共有プロトコルに対する DoS 攻撃

3.4　まとめ

本節では，SAS Phone でのグループ通話を実現することを目的に， SAS グループ鍵配送プロトコルの検討を行った．これにより，なりすましによる鍵の同期ズレを引き起こす攻撃の存在が明らかになった．次章以降では，この攻撃を Denial of Service (DoS) 攻撃と呼びその対策方法を示す．

第 4 章

SAS グループ鍵配送プロトコルの提案

4.1 目的

3 章では，従来の 2 者間で実行可能な SAS 鍵配送をベースとしてグループ通信に対応した SAS グループ鍵配送プロトコルを検討した．それにより，DoS 攻撃が可能なことが示されたため，グループ外の第三者により意図的にメンバ間で鍵の整合性を満たすことを妨害する可能性がある．本章では， DoS 攻撃に耐性を有する SAS グループ鍵配送プロトコルを提案し，SAS 鍵配送プロトコルのグループ対応化により生じるオーバヘッドを検証する．

4.2 プロトコル概要

SAS グループ鍵配送プロトコルは，コントローラと呼ばれるグループの代表者の制御によりメンバ全体で安全にグループ鍵を共有する方式である．鍵配送の仕組みにワンタイムパスワード認証方式 SAS を利用していることから，高速な鍵配送および鍵の認証が可能である．通信方式にはユニキャストとマルチキャストの両方を用いることが可能である．

DoS 攻撃への対策として，メンバの返信情報 γ を生成する際にその者の識別子を用いる．また，コントローラが一部のメンバから γ を受信できない場合，鍵更新用のメッセージをそのメンバに対して送ることで鍵の整合性の保持を可能とする．

SAS グループ鍵配送プロトコルは，登録フェーズと鍵配送フェーズから構成される．登

録フェーズは，グループを構成する際に一度だけ実行され，鍵配送フェーズはグループ鍵の更新を行う場合に実行される．

以下では，次の前提と表 4.1 の表記に基づき提案プロトコルについて述べる．

- あるメンバは同じグループに所属する他のメンバのグループに対するアクセス権限を適切に検証できる
- 同じグループに所属するメンバ間の利害関係は一致し，DoS 攻撃などの妨害は行わない
- 登録フェーズは何らかの方法を用いて安全かつ確実に行うことができる
- コントローラは，何らかの方法でグループメンバの中から選出される

表 4.1　表記法

M_i	グループ内のメンバ
ID_i	グループ内で一意な M_i を表すメンバ識別子.
M_C	コントローラ．ただし，$M_C \in \{M_i\}_{\forall i}$
ID_C	コントローラを表す識別子．ただし，$ID_C \in \{ID_i\}_{\forall i}$
L	全メンバの識別子を格納するリスト
N_j	擬似乱数．j 回目の鍵配送フェーズにおける今回認証情報の作成に用いられる
A_C, A_N, A_B	それぞれ SAS で用いられる，今回認証情報，次回認証情報，バックアップ用認証情報
H	暗号学的ハッシュ関数
KFD	鍵の生成する鍵導出関数
EK_C	j 回目の鍵配送フェーズで生成される鍵
EK_B	$j-1$ 回目の鍵配送フェーズで生成された鍵のバックアップ

4.2.1　登録フェーズ

登録フェーズは，グループ間で初回認証情報の共有を目的に実行される．まず，グループ全体でメンバ識別子を格納するリスト L を共有する．次に，コントローラは初回認証情報 A_C を生成しメンバへブロードキャストする．その後，L と A_C を保存する．一方，メンバはバックアップ用の認証情報 $A_B = null$ を生成し，L, A_C とともに保存する．グループサイズが 3 としたときの，初期化フェーズを図 4.1 に示す.

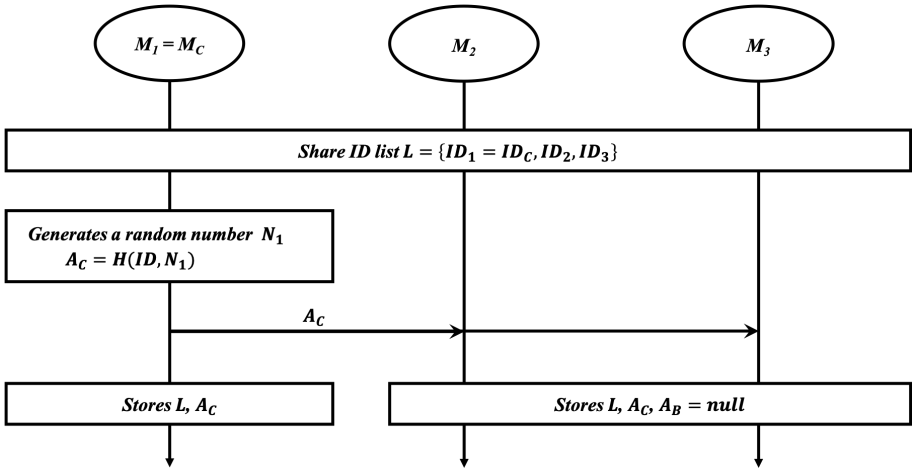

図 4.1　SAS グループ鍵配送プロトコルの登録フェーズ

4.3　鍵配送フェーズ

4.3.1　通信フロー

鍵配送フェーズの通信フローを図 4.2 に示す．コントローラは，ID_C, α, β をブロードキャストする．その後，全てのメンバから返信データ γ を受信し検証に成功した場合に限り，鍵の更新を許可を意味する $update\,message$ をメンバ全体に送信する．$update\,message$ としては，以下のように γ_c を用いることができる．

$$update\ \ message \quad = \quad ID_C, \quad \gamma_C$$

その後，グループ全体で鍵のバックアップと生成を次のように行う．暗号鍵はその鍵配送セッションにおける今回認証情報および次回認証情報を用いて次のように生成する．

$$\begin{aligned} EK_B &= EK_C \\ EK_C &= KDF(ID_1, ..., ID_i, ..., A_C, A_N) \end{aligned}$$

ただし，初回鍵配送フェーズにおいては，EK_B には $null$ をセットする．

パケットロスが発生しない場合，上記の処理によって鍵配送が完了する．鍵のバックアップは，鍵配送後に古い鍵で暗号化されたデータを受信する可能性がある場合などに利用される．パケットロスが発生する場合は，そのデータにより大きく分けて 2 つの処理が行われる．

α, β または，γ_i がロスした場合

コントローラはメンバ M_i からの返信 γ_i を受信できないため，α, β の再送処理を行う．

$update\ message$ がロスした場合

これを受信できなかったメンバ M_i は，鍵配送後に提供される認証やメッセージの暗号化などの暗号サービスと連携することで，そのときに所持する認証情報を利用して鍵を生成する．この状況における M_i の具体的な処理は，5.3.6 項で述べる．

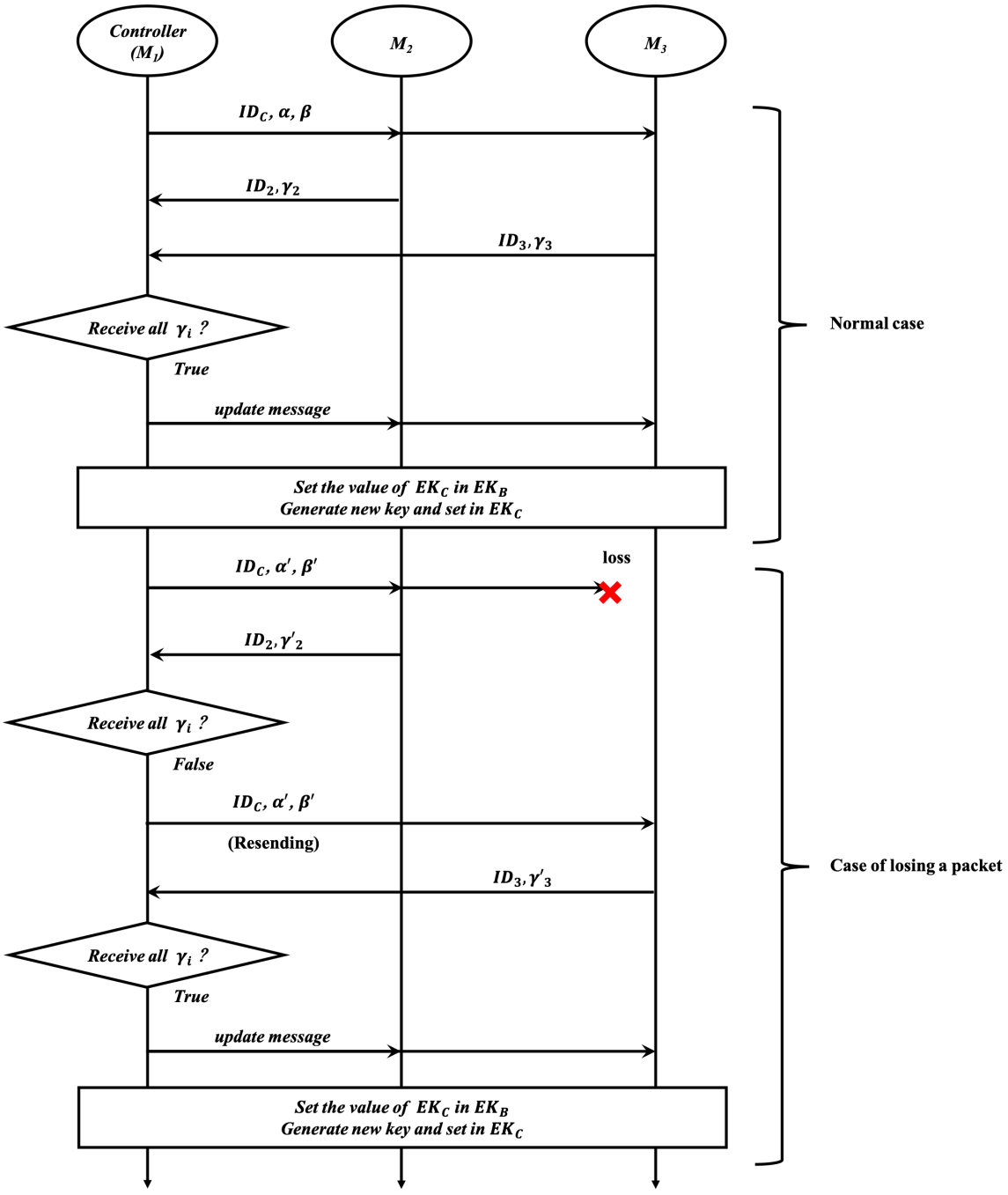

図 4.2　SAS グループ鍵配送プロトコルの鍵配送フェーズの通信フロー

4.3.2 コントローラとメンバの処理詳細

コントローラとメンバ M_i との間で行われる処理の詳細を図 4.3 と以下に示す.

M_C 側

1. 乱数 N_{i+1} を用い $A_N = H(ID_C, N_{i+1}))$ および $H(A_N) = H(ID_C, A_N)$ を計算.
2. 通信データ $\alpha = A_N \bigoplus (H(A_N) + A_C)$, $\beta = H(A_N) \bigoplus A_C$ を計算.

M_i 側

3. 受信した β と A_C を使用し, $H(C) = \beta \bigoplus A_C$ を算出. さらに, これと A_C を用い, $A_N = \alpha \bigoplus (H(C) + A_C)$ を算出.
4. $H(A_N)$ と $H(ID_C, A_N)$ を比較して一致した場合にユーザを認証し以下のステップを実行. 一致しなかった場合はステップ 7 を実行.
5. バックアップ用の認証情報 A_B を A_C の値で, A_C を A_N の値で更新.
6. $\gamma_i = H(ID_i, H(A_N))$ を計算しステップ 10 を実行.
7. ステップ 3 の処理を A_C の代わりに A_B を用いて実行.
8. $H(A_N)$ と $H(ID_C, A_N)$ を比較して一致した場合にユーザを認証し以下を実行. 一致しなかった場合は, 認証失敗として何らかの処理（e.g. α, β の再送）を実行.
9. $\gamma_i = H(ID_i, H(A_C))$ を計算.
10. ID_i, γ_i をコントローラへ送信.

M_C 側

11. 受信した γ_i と自身で計算した $H(ID_i, H(A_C))$ と比較し一致した場合し以下を実行, 認証が成功, 一致しなかった場合は, 認証失敗として何らかの処理を実行.
12. ID_i との鍵配送に成功したことを記録.

M_C/M_i

13. M_C が *update message* を送信後に, EK_C を EK_B としてバックアップし, ID, A_C, A_N を用いて EK_C を新たに生成.

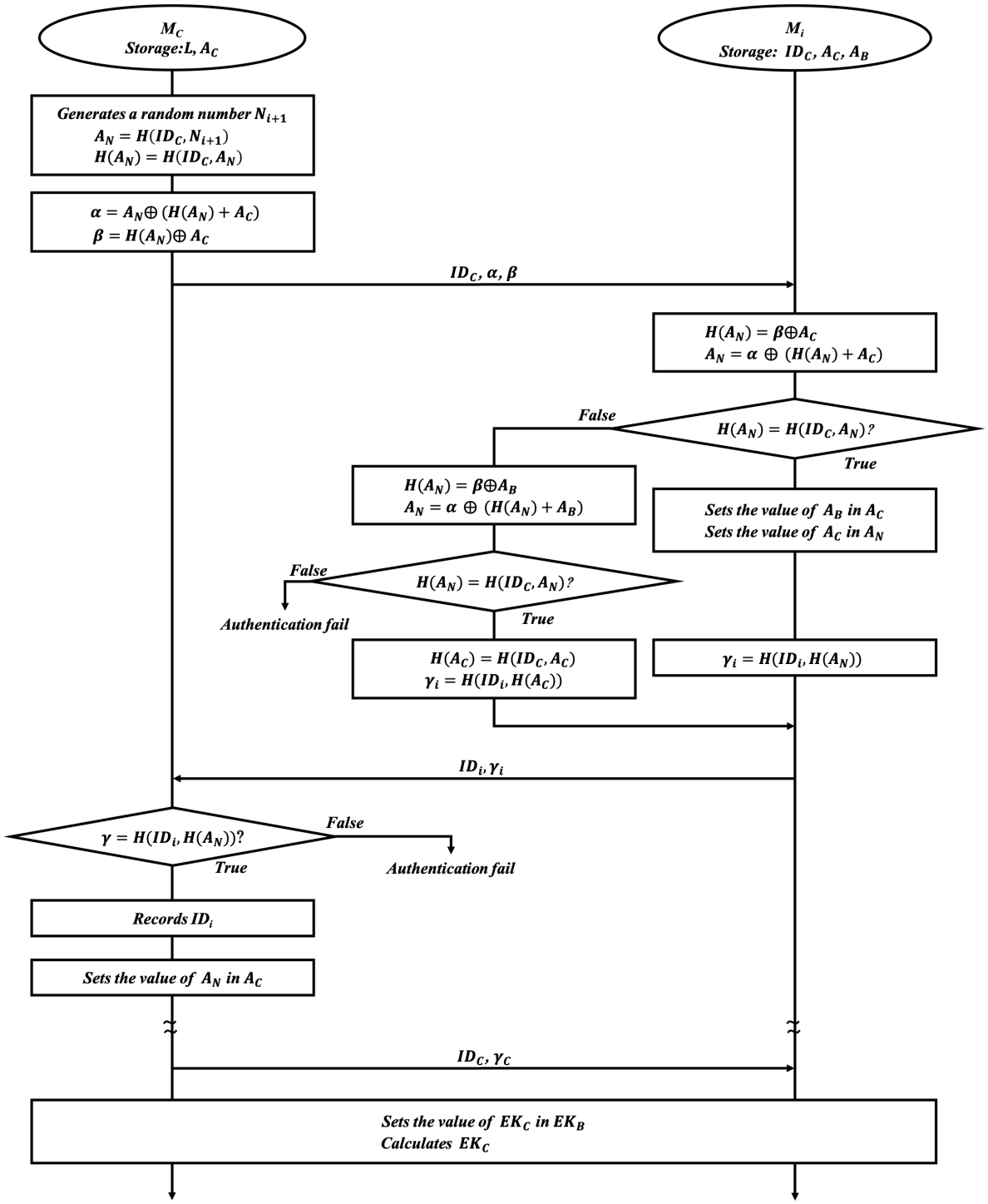

図 4.3　SAS グループ鍵配送プロトコルの鍵配送フェーズ

4.4 評価

4.4.1 DoS 攻撃への耐性評価

SAS グループ鍵配送プロトコルにおける DoS 攻撃は，通信データを再利用することで認証情報の更新を妨害する攻撃である．この攻撃に耐性が無い場合，鍵配送が成立しないため一部のメンバは暗合通信でやり取りされるデータにアクセスできなくなる．

DoS 攻撃に利用できる通信データは次の通りである．

$$
\begin{aligned}
message1: &\quad ID_C, \quad \alpha = B \bigoplus (H(B) + A), \quad \beta = H(B) \bigoplus A \\
message2: &\quad ID_i, \quad \gamma_i = H(ID_i, H(B)) \\
message3: &\quad ID_C, \quad \gamma_C = H(ID_C, H(B))
\end{aligned}
$$

message1，message3 は，コントローラがメンバへ送信するデータ，message2 はメンバがコントローラへ送信するデータを表す．これらのメッセージが経路上で損失した場合に，以下の通り DoS 攻撃が成功する可能性がある．

M_i が message1 を受信できない場合

攻撃者は message2 作成しコントローラへ送信することで攻撃が成功する．このとき，M_i 以外が認証情報を更新する．

M_i が送信した message2 をコントローラが受信できない場合

攻撃者は message3 作成し M_i へ送信することで攻撃が成功する．このとき，M_i のみが認証情報を更新する．

M_i が message3 を受信できない場合

この状況下では，グループ全体で認証情報を共有しているため DoS 攻撃は成功しない．

DoS 攻撃が成功するには，攻撃者が $\gamma_x = H(ID_x, H(B))$ の計算で使われる $H(B)$ を特定する必要がある．しかし，盗聴したデータを用いたとしてもハッシュ関数の原像計算困難性により計算量的に困難であるため，提案プロトコルは DoS 攻撃に対して耐性を有する．

表 4.2 SAS 鍵配送 (KD) と SAS グループ鍵配送 (GKD) のパフォーマンス比較

	メッセージサイズ	内部処理				ストレージ	
		送信回数		ハッシュ関数			
		コントローラ	メンバ	コントローラ	メンバ	コントローラ	メンバ
KD	$l_i + 2l_a$	1	0	2	1	$2l_i + l_a$	
GKD	$(n+1)l_i + (n+3)l_a$	2	1	$n+2$	2	$nl_i + l_a$	$nl_i + 2l_a$

4.4.2 鍵配送フェーズにおけるオーバヘッド比較

既存の SAS 鍵配送プロトコルおよび本稿で提案する SAS グループ鍵配送プロトコルのパフォーマンス比較結果を表 4.2 に示す．ただし，同期ズレは発生しないものとし，n はコントローラを除くグループメンバの数を表し，l_i, l_a はそれぞれ，メンバ識別子と認証情報のデータサイズを表す．メッセージのサイズは，メンバ数に比例することがわかる．ネットワーク別に分けた場合，メンバのネットワークに届くメッセージのサイズは $2l_i + 3l_a$，コントローラのネットワークでは $(n+1)l_i + (n+3)l_a$ となり，コントローラ側のネットワークオーバヘッドはメンバ数に比例する．大規模なグループでは，各メンバからの返信が M_C のネットワークに集中するため，輻輳による通信のオーバヘッドの増加が懸念される．一方，小規模グループの場合は，メンバ識別子や認証情報は数十バイト程度と小さいことから，オーバヘッドによる影響は小さいものと考えられる．

また，SAS グループ鍵配送プロトコルでは，コントローラはマルチキャスト通信を前提としているため，送信回数が 2 回となっている．このパラメータは，ユニキャストの場合ではメンバ数に比例し $n+1$ 回となる．

ハッシュ関数の回数に関しても同様にグループサイズに比例するが，動作周波数 3GHz の CPU では約 0.4 マイクロ秒と高速に実行できることから内部計算のオーバヘッドの増加は通信と比較し影響は小さいと考えられる．

以上より，ネットワーク負荷の懸念から提案プロトコルは小規模グループ間での鍵配送に適している．

第 5 章

SAS Phone の拡張

5.1 概要

前節では，一般的なグループ通信で利用可能な鍵配送方式 SAS グループ鍵配送プロトコルを提案した．本章では，このプロトコルを利用しグループ音声通話を可能とすべく SAS Phone の拡張について述べる．

SAS Phone の拡張にあたり，2.3 項に示した音声通話におけるセキュリティ要件を満たすように，SAS グループ鍵配送プロトコルの初回認証情報の安全な共有方法およびグループメンバの変更を実現する方法を検討する必要がある．そこで，グループ鍵管理方式である Tree-based Group Diffie-Hellman (TGDH) を用いる．TGDH は小規模グループに限定されるが，分散型のグループ鍵管理の仕組みを提供するため機密性・前方秘匿性・後方秘匿性・可用性を満たすことができる．SAS グループ鍵配送と TGDH を組み合わせた鍵更新の仕組みを SAS Phone に適用することでグループ通話を可能とする．

既存の SAS Phone では，鍵更新と音声パケットの転送を逐次的に実行することでセキュアな通話を実現していた．実際の通話時には，パケットロスの影響により鍵配送処理が遅延することが予想され，特にグループ通話の場合は通話品質の低下が懸念される．パケットロスの影響を小さくするために，拡張後の SAS Phone 鍵更新と音声パケットの転送を並列に実行する．

5.2　グループ鍵管理方式の検討

グループ鍵管理方式は，グループメンバの変更を考慮した鍵管理の仕組みを提供するため，2.3 項のセキュリティ要件に示した，前方秘匿性および後方秘匿性を提供できる [9]．グループ鍵管理方式は中央集権型および分散型の 2 つのアーキテクチャに分類され，それぞれの代表的な方式として，Logical Key Hierarchy (LKH) [10] と Tree based Group Diffie-Hellman key management (TGDH) [11] が知られている．これらの方式では，図 5.1 のような鍵木を用いた階層構造で管理する．これは鍵木と呼ばれ，ルートノードはグループ鍵を葉ノードはメンバと 1 対 1 で対応する鍵を表す．各ユーザは葉ノードからルートノードまでの鍵パス上に存在する鍵を保持する．

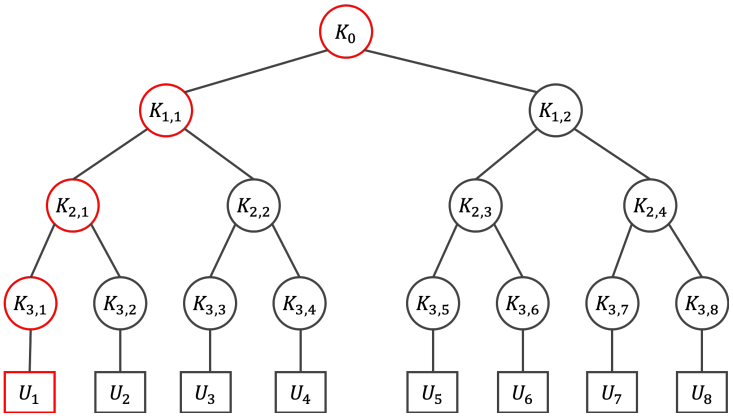

図 5.1　鍵木

LKH は，コントローラを中心にしたグループ鍵管理を提供する方式である．葉ノードはコントローラとユーザ間で確立されるペアワイズ鍵を指す．コントローラは鍵木全体の鍵を保持し，各ユーザはルートノードから自身の葉ノードまでのパスの間に存在する鍵を持つ．新規ユーザの参加や既存メンバの退出時には，コントローラは変更が必要な鍵のみを更新してそれらを下位の鍵で暗号化しメンバへ届ける．操作に要するメッセージの送信数は，参加時で $(\log_d n + 1)$，退出時で 1 となる．ただし，d はノードの次数を表す整数．また，暗号処理コストは，参加/退出時ともに $\mathcal{O}(\log_d n)$ である．

TGDH は，2 者間の Diffi-Hellman 鍵合意プロトコル [12] をグループ鍵管理のために拡

張した方式である．TGDH における鍵木は二分木のみであり，各ノードは秘密鍵と公開可能なブラインド鍵を持つ．各ユーザは，全てのノードのブラインド鍵および鍵パス上の秘密鍵を管理する．それらの鍵は下位から上位ノードに向けて DH プロトコルを利用して計算される．あるユーザ u が参加する際は，まずブラインド鍵をグループ全体にブロードキャストする．他の全メンバは，鍵木中の u の挿入箇所と u の参加を支援するスポンサーを決定する．各ユーザは自身が管理する鍵木中に u の葉ノードおよび中間ノードを挿入し，スポンサーの葉ノードからルートノードまでに存在する秘密鍵およびブラインド鍵を削除する．そして，スポンサーが自身の秘密鍵を再生成し，葉ノードからルートノードまでのブラインド鍵を計算する．その後，計算した全てのブラインド鍵をグループ全体に送信することで，他のメンバはグループ鍵を計算できるようになる．また，u が退出する際は，スポンサーを決定し残るメンバは u に対応する葉ノードを削除する．その後，スポンサーは自身の秘密鍵を生成し葉ノードからルートノードまでのブラインド鍵を計算する．計算結果をメンバ全体にブロードキャストすることで，グループ鍵を全体で共有できる．TGDH における参加/退出操作のメッセージ送信数はそれぞれ，2，1 である．また，べき乗演算のコストは，参加/退出時ともに $\mathcal{O}(\log n)$ である．

両方式を，2.3 項のセキュリティ要件，通信コスト，計算コストの観点で比較した結果を表 5.1 に示す．

表 5.1　LKH と TGDH の比較

前方秘匿性	後方秘匿性	機密性	鍵の認証	可用性	メッセージ数 [1]	計算コスト	グループ規模
Y	Y	Y(N)	N	N(Y)	$(\log_d n + 1)$ / 1	$\mathcal{O}(\log_d n)$	大
Y	Y	Y	N	Y	2 / 1	$\mathcal{O}(\log n)$	小

[1] 順に，参加時と退出時におけるメッセージ送信数を表す．

LKH はコントローラによって鍵管理が行われる．グループメンバの代表者がこれを担う場合は，機密性を満たせるが可用性が満たすことが難しくなる．また，グループメンバ外の信頼できるサーバに委任する場合は，冗長構成を取ることで可用性を満たせるが，サーバ

はデータにアクセスできるため機密性を満たすことができない．そのため，LKH は機密性および可用性の一方のみを提供する．一方，TGDH は，セキュリティ要件を満たすものの，べき乗演算をグループメンバ全員が行わなければならずスマートフォンなどの処理能力が低いデバイスが存在する場合にグループメンバのサイズが限定されてしまう．いずれの方式も鍵の認証は提供しないため，RSA [13] や DSA [14] などの署名方式を用いる必要がある．

これらを総合的に考えて，小規模グループ通話を前提とすれば TGDH を用いる利点が大きいため，SAS Phone の拡張には TGDH に基づくグループ鍵管理方式を用いる．以降では，TGDH で共有するグループ鍵を GK，新規メンバの参加プロトコルを $JOIN$，メンバの退出プロトコルを $LEAVE$ と表記する．

5.3　グループ通話が可能な SAS Phone

5.3.1　前提

本稿で拡張する SAS Phone では，次のことを前提とする．

- 中央サーバはプロトコル通りに正しく動作するが，通話内容に関心がある
- 通話セッションに参加していないものは，通話内容に対するアクセス権限がない
- 通話セッションに参加しているグループメンバは信頼できるが，途中参加または退出する者はアクセス権限の無い通話内容に関心がある

5.3.2　ネットワーク構成

提案方式におけるネットワーク構成は，中央サーバとエンドユーザ間で図 5.2 のようなスター型のトポロジを用いる．中央サーバの役割は，グループメンバ管理・アクセス制御や従来の SAS Phone と同様な呼制御を提供する．また，マルチキャスト通信が困難なユーザが存在する場合は，そのユーザとマルチキャストグループのゲートウェイとしての機能も提供する．通話セッションを確立したユーザは，ユニキャストまたはマルチキャスト通信を利用

して通話を行う．

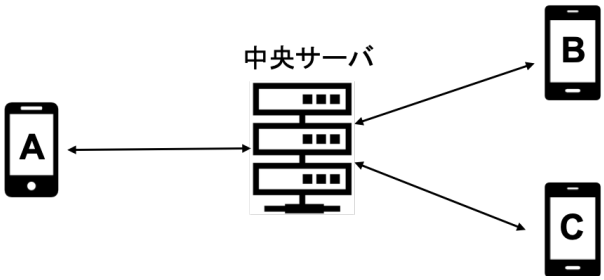

図 5.2　ネットワーク構成

5.3.3　プロトコルスタック

提案手法のプロトコルスタックを図 5.3 に示す．鍵更新は，前節で述べた SAS グループ鍵交換プロトコルを用いて行われる．これを定期的に実行することで音声パケットの暗号鍵が更新される．呼制御では，中央サーバにログインしているグループメンバに対して通話セッションの確立に必要な IP アドレスやポート番号，メディアのコーデック情報など通話セッションの識別に必要な情報を SDP と SIP を用いて提供する．また，音声通話では，暗号化された音声パケットを RTP を用いてエンドユーザ間でやり取りする．暗号処理で用いるのは，Authenticated Encryption with Associcated Data (AEAD) または Authenticated Encryption (AE) と呼ばれる認証付き暗号 [15] である．4.3.1 項で述べたように，SAS グループ鍵配送で update message の受信に失敗したユーザが存在する場合に復号の失敗を検出する必要があり，AEAD を用いることで実現できる．AEAD としては，AES-GCM[16] や ChaCha20-Poly1305[17] などが知られている．

5.3.4　通話セッションの確立と切断

通話セッションは，中央サーバを経由して図 5.4 の通り確立・切断する．まず，メンバは中央サーバへログインし通話を行うグループへのアクセス権を要求する．中央サーバがアクセス権を検証できた場合，通話に必要なセッション情報をメンバへ返信する．メンバは，

<table>
<tr><td colspan="3">鍵更新</td><td colspan="2">呼制御</td><td>音声通信</td></tr>
<tr><td rowspan="3">TGDH</td><td rowspan="3">SAS グループ鍵配送</td><td rowspan="3">鍵生成</td><td rowspan="3">SDP</td><td rowspan="3">SIP</td><td>音声コーデック</td></tr>
<tr><td>AEAD / AE</td></tr>
<tr><td>RTP</td></tr>
<tr><td colspan="3">TCP or UDP</td><td>TCP</td><td colspan="2">UDP</td></tr>
<tr><td colspan="6">IP</td></tr>
</table>

図 5.3　提案方式のプロトコルスタック

セッション情報を用いて通話セッションを有効にする．複数のメンバが通話セションを有効になることで通話セッションが確立する．セッションの切断は， BYE メッセージを相互にやり取りすることで行われる．

5.3.5　SAS グループ鍵配送と TGDH を組み合わせた鍵更新の実現

鍵の更新は，SAS グループ鍵配送プロトコルにおける鍵配送フェーズにより行う．鍵配送フェーズで利用する認証情報の共有は，初期化・参加・退出フェーズにて TGDH を用いて行われる．初期化フェーズは通話セッション開始時に実行される．また参加・退出フェーズは，グループ構成の変更時に実行され，処理は $JOIN$，$LEAVE$ プロトコルに基づく．

図 5.5 に認証情報の共有方法を示す．新規の通話セッションの確立またはメンバ構成の変更が行われるときに，グループ全体で TGDH を用いてグループ鍵 GK を共有する．その後，コントローラが不在の場合はその選出を行う．選出の基準としては，メンバが利用している端末の処理性能などを用いることができる．ここで共有した GK を SAS 初回認証情報として鍵配送フェーズを実行することで鍵の更新が可能となる．

メンバ変更時に実行される $JOIN$，$LEAVE$ プロトコルでは，そのときに共有している暗号鍵 EK_C を用いて EK_B に設定する．

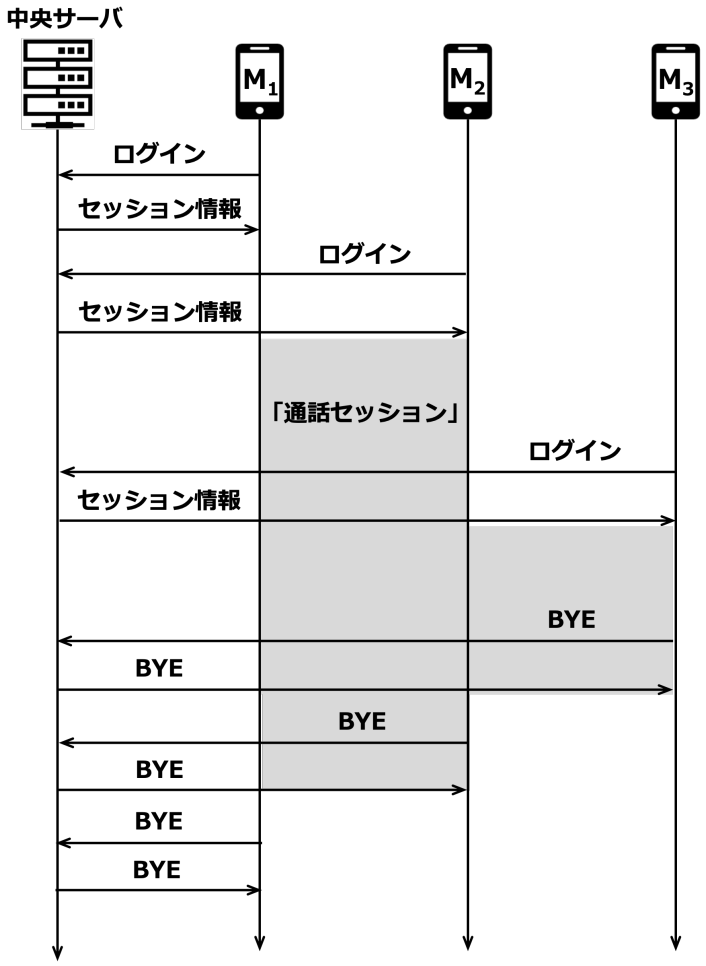

図 5.4　グループ通話対応 SAS Phone のセッション確立

5.3.6　音声転送と鍵更新

提案方式においては，音声転送と鍵更新は並列に処理される．通話セッションが確立すると，音声パケットの暗号化に必要な鍵の共有のために 図 5.6 のように SAS グループ鍵配送プロトコルの初期化フェーズおよび鍵配送フェーズを実行する．鍵配送フェーズが終了することで音声通話が可能となる．

以降は，定期的に鍵配送を実行することで鍵の更新を行う．なお，実行間隔は，鍵配送フェーズの実行に要する時間に依存する．

鍵配送フェーズの実行直後は，暗号化パケットは用いている鍵によって 2 種類が混在する

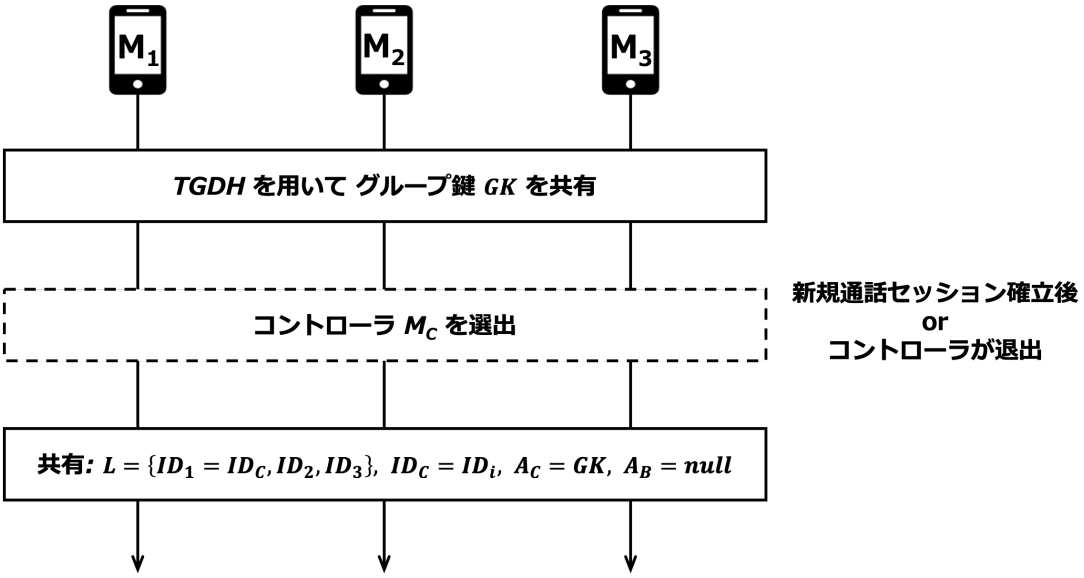

図 5.5　TGDH を用いた認証情報の共有

ことになる．図 5.6 を例に挙げると，EK_C^1，EK_C^2 のいずれかで暗号化されたパケットが存在するということである．鍵配送フェーズ後に受信したパケットは，いずれのメンバも最新の鍵である EK_C^2 で復号を試みる．提案方式で利用する暗号は認証付き暗号であるため，メンバは復号に成功したかどうかを判断できる．もし，失敗した場合は EK_B^2 で試みることで復号が可能である．

鍵配送フェーズにおいて，update message の受信に失敗した場合の対処が必要である．受信に失敗したユーザ M_i は，最新の鍵を持たないため，それを用いた暗号化されたデータ $Enc(D)$ にアクセスできない．しかし，update message が発行された時点でグループ全体で鍵の生成に必要な情報が共有されていることが保証されることから，最新の鍵を計算することは可能である．そこで，$Enc(D)$ の復号を EK_C^j を用いて試み，失敗した場合は最新の鍵を計算して復号を行う．

グループへの参加および退出が発生する場合の音声転送と鍵更新の様子を図 5.7,5.8 に示す．

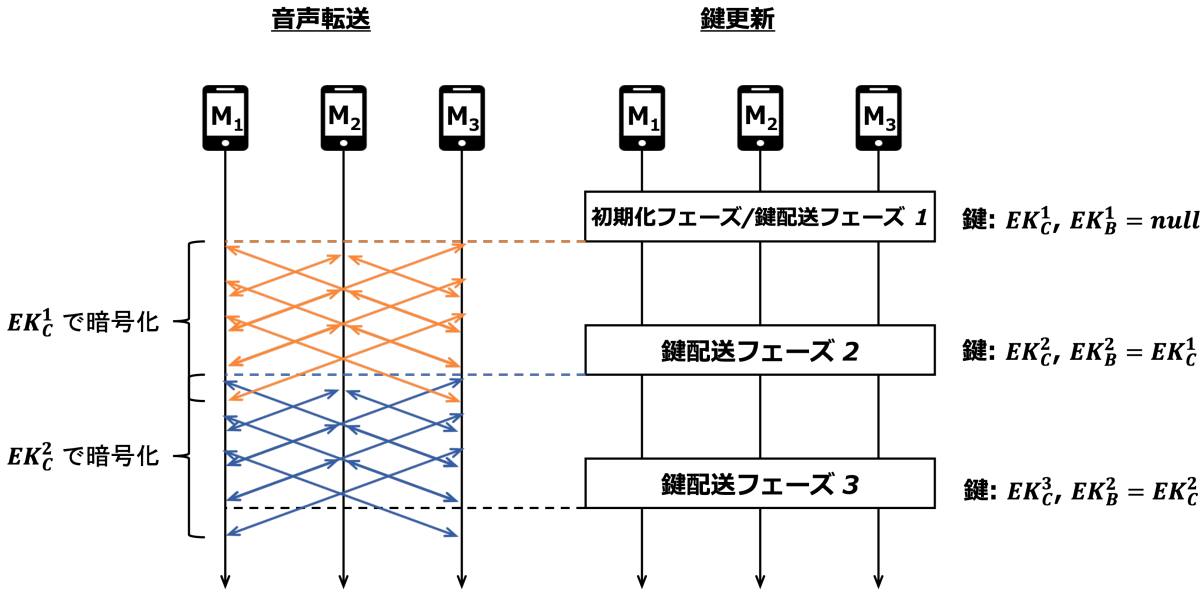

図 5.6　グループ通話対応 SAS Phone の音声転送と鍵更新

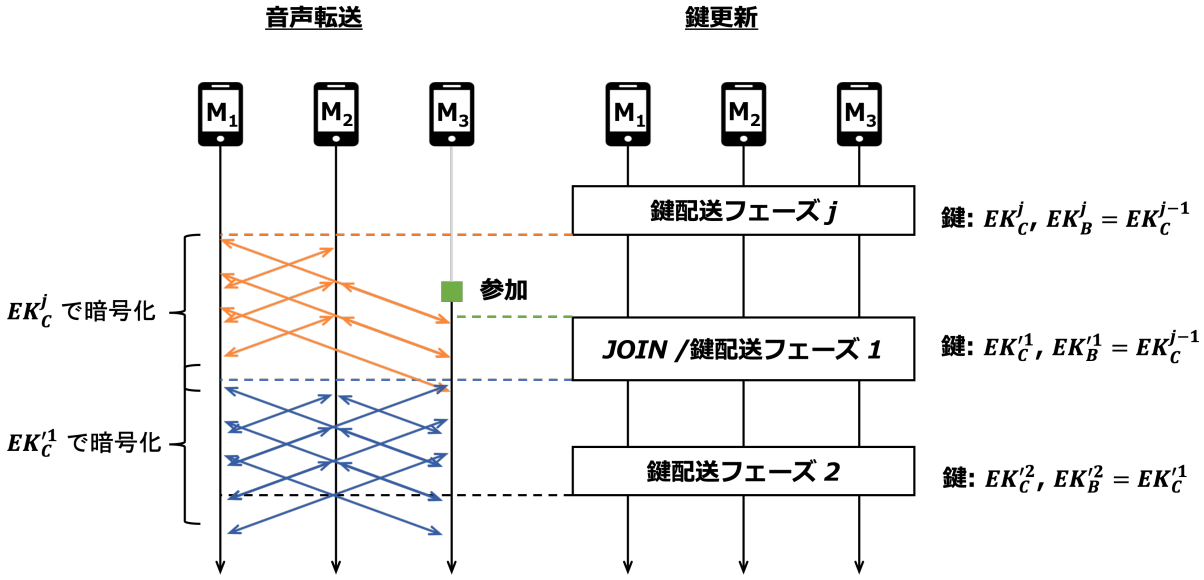

図 5.7　グループ通話対応 SAS Phone での新規メンバ参加時の音声転送と鍵更新

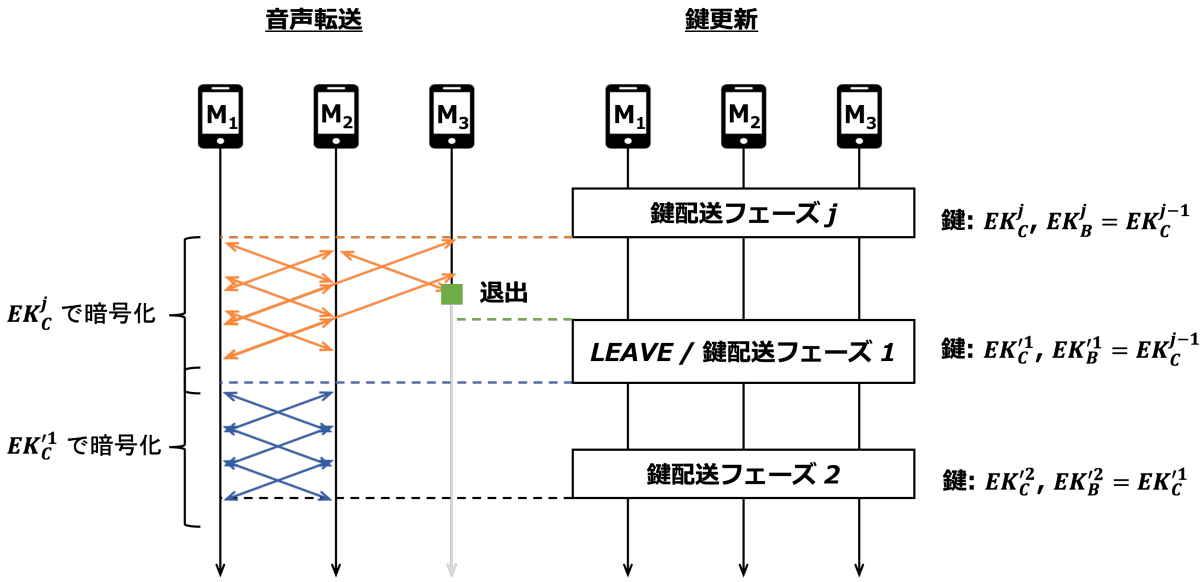

図 5.8　グループ通話対応 SAS Phone でのメンバ退出時の音声転送と鍵更新

5.4　評価

5.5　セキュリティ要件

本節では，SAS Phone がグループ通話に求められる 2.3 節で定義したセキュリティ要件を満たすかどうかを評価する．

機密性

SAS グループ鍵配送プロトコルで利用する認証情報の共有には，分散型グループ鍵管理方式 TGDH を用いる．この TGDH で共有する値は，離散対数問題の困難性を安全性の根拠としてグループメンバしか知り得ない．SAS Phone では，認証や通話セッションの確立に中央サーバを利用するが，TGDH のメンバとしては参加しない．よって，中央サーバを含むグループ外のエンティティは認証情報を得ることができないため，それをもとに計算される暗号鍵で秘匿される通話内容は秘匿される．

暗号鍵の更新

従来の SAS Phone と同様にグループメンバ間で定期的に鍵更新を行えるためこの要件を満たす．

整合性

鍵更新を定期的に行う場合，メンバ全体で鍵の更新が適切に行われない可能性がある．SAS Phone の鍵更新は，DoS 攻撃に耐性を有する SAS グループ鍵配送に基づくためメンバ間で整合性を保つことができる．ただし，TGDH ではパケットロスの影響を考慮していないため，メンバ間で確実に共有するためにはデジタル証明を導入するなどの対策が必要である．

鍵更新時の認証

SAS グループ鍵配送プロトコルは，ワンタイムパスワード認証方式 SAS をベースにするため鍵の更新および認証を提供することが可能である．グループ構成の変更時に実行される TGDH によって認証情報の更新が行われる．このとき，中央サーバが提供する

デジタル署名を利用することで認証が可能である．

前方秘匿性

メンバが退出したとき，残りのメンバ間では新たな認証情報を利用して鍵更新を行うため，一度退出した場合その後の通話内容を知ることができない．

後方秘匿性

メンバがグループに参加するとき，それまでに利用していた認証情報と新規の認証情報の間には関連性がなくなるため，そのメンバは過去の通話内容を知ることができない．

可用性

グループからコントローラ以外のメンバ退出した場合は，その後の鍵更新は正常に行うことができるが，コントローラが抜けた場合も，同様に鍵更新処理を継続できることが必要である．グループ通話に対応した SAS Phone では，TGDH による分散型の認証情報の共有の仕組みを用いるため，新たなコントローラの選出により鍵更新処理を継続することが可能である．

5.6　各種暗号アルゴリズムのパラメータ

セキュリティ強度とは，Xbit の鍵を用いる対称鍵暗号アルゴリズムにおける鍵の総当たりにかかる計算量と説明される．このとき，暗号アルゴリズムは Xbit のセキュリティ強度をもつ．一般に，複数の暗号アルゴリズムを使用する場合の安全性は，最も弱いセキュリティ強度を提供するアルゴリズムおよびその鍵サイズにより決まる [18]．本項では，まず SAS 鍵配送のセキュリティ強度を明らかにし，SAS Phone で利用が予想される暗号アルゴリズムの推奨パラメータサイズを述べる．

SAS 鍵配送における解読を，エンドユーザ間で共有する認証情報 A を特定することと定義する．以下に示す SAS の通信データから，解読は B または $H(B)$ の特定と等価である．

$$
\begin{aligned}
& ID, \\
\alpha \quad &= \quad B \bigoplus (H(B) + A), \\
\beta \quad &= \quad H(B) \bigoplus A
\end{aligned}
$$

これまでに SAS の解読における有効な攻撃は発見されていないため，解読にかかる計算量は $\mathcal{O}(2^n - 2) = \mathcal{O}(2^n)$ となる．よって，セキュリティ強度は認証情報のサイズはに等しい．

NIST によって，暗号アルゴリズムごとに特定のセキュリティ強度を達成するために必要なセキュリティパラメータが示されている．それらと， SAS のセキュリティ強度の検証結果を踏まえ，主要な暗合アルゴリズムのセキュリティパラメータを表 5.2 に示す．NIST では，128bit 以上のセキュリティ強度を満たすパラメータを推奨しているため SAS Phone で利用する暗号アルゴリズムにはそのようなパラメータを用いる必要がある．

表 5.2　セキュリティ強度とパラメータの関係性 (単位: bit)

セキュリティ強度	AES 鍵長	DSA/DH 鍵共有	SAS 認証情報サイズ
128	128	公開鍵=3072, 秘密鍵=256	128
192	192	公開鍵=7680, 秘密鍵=384	192
256	256	公開鍵=15360, 秘密鍵=512	256

5.7　音声通話システムの比較

音声通話システムとして，拡張前後の SAS Phone・LINE・Skype の比較結果を表 5.3 に示す.

従来の SAS Phone では 2 者間通話のみが想定されているが，1 対 1 の通話セッションを多重に確立するフルメッシュ接続を行うことでグループ通話が可能である．グループサイズが N の場合，あるエンドユーザは N-1 個の暗号鍵を持ち，その分だけ送出するパケットが多くなる．そのため，拡張 SAS Phone と比較し輻輳が懸念される.

中・大規模のグループ通話を行うにあたり，エンドユーザが全てのメンバのパケットを処理することは現実的には難しい．そのような規模での通話では，中央サーバによる複数の音声ストリームを一つに集約する音声ミキシングが必要である [19]．この処理では，音声パケットの復号を必要とするため，管理者による通話内容の盗聴が可能である.

グループ通話の用途として，創造会議や定形会議が想定される．創造会議は，テーマに対するアイデアを出し合うことを目的としており，参加者は自由に発言することが求められる．一方，定形会議は，情報共有が目的であり司会者により発言権が決められる．グループ通話で問題になるのが，同時に複数の者が発言することで生じる衝突である．これは，グループ規模が大きくなるほど顕著であることが予想されるため，発言権を制御する必要がある．一方，小規模の場合は，比較的衝突からの復帰が容易であるため発言権の制御は必ずしも必要ではない．よって，規模の大きいグループ通話の場合は利用は定形会議に限られ，小規模の場合は創造会議または定形会議で利用できる.

SAS Phone は，ミキシングを許容しないため小規模通話に限定されるが，創造会議等に適用できる．特に，中央サーバに対する信頼は LINE や Skype に比べて弱いため，内部犯による不正といった脅威に対して安全性が高く，機密情報を扱う可能性がある場合は，他システムと比べ優位性を持つ.

表 5.3　グループ音声通話システムとの比較（N: グループサイズ）

	送出音声パケット数	規模	管理者の盗聴	鍵更新
拡張した SAS Phone	1	数名	不可	有
従来の SAS Phone	N-1	数名	不可	有
LINE	1	∼200 名	可	無
Skype	1	∼250 名	可	無

第 6 章

結論

TLS をベースとした従来型 VoIP システムでは，同一セッションではその長さに依らず 1 つの暗号鍵のみを使うため暗号解析攻撃が脅威である．このような背景から，SAS 鍵配送プロトコルに基づいた定期的な暗号鍵の更新を行う音声通話システム SAS Phone が提案されている．しかし，グループ通話に対応していないため実用性の観点で課題が残っていた．

本稿では，SAS Phone によるグループ通話の実現を目的に，グループ通信環境下で鍵配送を可能とする SAS グループ鍵配送プロトコルを提案した．このプロトコルの評価により，鍵の同期を妨害する DoS 攻撃に対して安全性が示された．また，コントローラが所属するネットワークの負荷がメンバサイズに比例して増加するため，小規模ネットワークに適していることが明らかになった．

SAS グループ鍵配送プロトコルを用いて小規模向けセキュアグループ通話システムとして SAS Phone の拡張を行った．評価結果から，グループ通話に求められる要件を満たすことが明らかになった．しかし，鍵更新処理が音声通話の QoS に及ぼす影響に関する検証が不十分である．そのため今後の課題として，音声通話システムとして SAS Phone を実装し QoS の観点で評価を行うことが挙げられる．

謝辞

本研究の御助言をいただきました高知工科大 清水明宏教授に感謝いたします．香港理工大学への訪問や情報セキュリティEXPOでの営業を経験させていただきました．

本研究の副査を担当していただいた高知工科大 敷田幹文教授，植田和憲講師に深くお礼申し上げます．懇切丁寧な研究指導をして頂き自身の研究を深く考えることができました．また，敷田教授は私を含む清水研究室の修士2年生全員を副査をしてくださいました．研究室に訪問するなどしてくださいました．我々に対するお気遣大変うれしく存じます．

高知工科大 吉田真一 准教授に心より感謝致します．修士セミナにおいて私を含む研究室メンバ4名にアドバイスをいただきました．吉田准教授は副査ではありませんでしたが，我々の研究をより良くしようという思いが非常に伝わり，大変感激したのを覚えております．また研究室のサーバ管理についてご相談に親身にのってくださったり，研究指導に関する有益な情報をご教示頂きました．重ねて御礼申し上げます．

高知工科大学 清水研究室の関係者各位に感謝いたします．同期の合田氏・多田氏・安光氏の存在により有意義な2年間を過ごすことができました．研究・講義・就職活動等で困難な場面がありましたが，彼らと協力することで乗り越えられたと思います．今後は別々の道を歩み，互いが進む先に何が待っているかはわかりませんが，物事は「シンプル」に考え「安全」に気をつけながら進んでいきましょう．後輩の修士1年 高橋氏は，彼自身が忙しいにもかかわらず，学部生の指導や手伝いを必要以上にしていただきました．彼の後輩に対する優しさに敬意を表します．就職活動と修士研究が無事に終えられるよう祈っています．また，学部生の後輩には私の力不足で十分な指導ができなかったこと申し訳ありません．君たちの今後の活躍を祈っております．

最後に，大学生活の6年間を支えてくださった祖父母と叔母に感謝申し上げます．

参考文献

[1] T. Dierks and E. Rescorla, “Request for comments 5246: The Transport Layer Security (TLS) Protocol Version 1.2,” IETF, https://tools.ietf.org/html/rfc5246, August 2008.

[2] G. V. Bard, “A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL,” IEEE International Conference on Security and Cryptography, INSTICC Press, 2006.

[3] 幸地勇明, 中野勇貴, 小野豊, 清水明宏, “携帯端末向けセキュア VoIP システムの提案,” 信学技報, vol. 111, no. 286, LOIS2011-48, pp. 135-140, 2011 年 11 月.

[4] T. Tsuji and A. Shimizu, “A One-Time Password Authentication Method for Low Spec Machines and on Internet Protocols,” IEICE Trans. COMMUN, vol. E87-B, no.6, pp. 1594—1600, 2004.

[5] C. Perkins, 小川晃通（訳）, “マスタリング TCP/IP RTP 編,” オーム社, 2004.

[6] シスコシステムズ合同会社, “Catalyst 3750 スイッチソフトウェアコンフィギュレーションガイド Cisco IOS Release 12.1(19)EA1: IP マルチキャストルーティングの設定,” https://www.cisco.com/c/ja_jp/td/docs/sw/lanswt-access/cat3750swt/cg/001/j-cat3750-scg/33-swmcast.html,（最終検索日：2019 年 1 月 13 日）.

[7] 中原知也, 辻貴介, 清水明宏, “SAS-2 認証方式の同期問題に関する検討,” 電子情報通信学会技術研究報告, OIS, vol.104, no.714, pp.83-87, 2005.

[8] 竹下隆史, 村山公保, 荒井透, 苅田幸雄, “マスタリング TCP/IP 入門編,” オーム社, 2012.

[9] R. BARSKAR and M. CHAWLA, “A Survey on Efficient Group Key Management Schemes in Wireless Networks,” Indian Journal of Science and Technology, 2016.

[10] C. K. Wong, M. G. Gouda, and S. S. Lam, “Secure Group Communications Using Key Graphs,” IEEE/ACM Trans. Networking, vol.8, no.1, pp.16-30, 2000.

[11] Y. Kim, A. Perrig, and G. Tsudik, “Group key agreement efficient in communication,”IEEE transactions on computers, 53(7), 905-921, 2004.

[12] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol.IT-22, No.6, pp.644-654, Nov, 1976.

[13] B. Kaliski, J. Jonsson, and A. Rusch, “Request for comments 8017: PKCS #1: RSA Cryptography Specifications Version 2.2,” IETF, https://tools.ietf.org/html/rfc8017, November 2016.

[14] T. Pornin, “Request for comments 6979: Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA),” IETF, https://tools.ietf.org/html/rfc6979, August, 2013.

[15] M. Bellare, and C. Namprempre, “Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm,” In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 531-545, 2000.

[16] J. Salowey, A. Choudhury, and D. McGrew, “Request for comments 5288: AES Galois Counter Mode (GCM) Cipher Suites for TLS,” IETF, https://tools.ietf.org/html/rfc5288, July 2008.

[17] Y. Nir, and A. Langley, “Request for comments 7539: ChaCha20 and Poly1305 for IETF Protocols,” IETF, https://tools.ietf.org/html/rfc7539, July 2015.

[18] E. Barker , “Recommendation for Key Management Part1 General,” NIST Special Publication 800-57 Part 1 Revision 4, http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4, January, 2016.

[19] 大島浩太, 安藤公彦, 但馬康宏, 寺田松昭, “IP Telephony におけるクライアント依存性を排除した多者間通話サービス,” 情報処理学会論文誌 Vol.45 No.10 pp.2344-2353,

2004.