情報処理学会論文誌　Vol. 50　No. 3　1022–1031 (Mar. 2009)

IP マルチキャストを用いた放送型暗号による認証型ライブ映像配信システムの構築と評価

森村吉貴[†1]　上原哲太郎[†2]
侯書会[†1]　美濃導彦[†2]

我々は IP マルチキャスト上の SRTP を用いた鍵配送に放送型暗号を用いたライブ映像配信システムを構築した．一般に認証型のライブ映像配信では，ユーザ鍵の流出と復号映像の流出という問題が残る．我々のシステムは，ユーザ鍵の流出については放送型暗号のユーザ鍵が異なるという特徴を生かし，復号映像については透かしとして映像に ID を埋め込む電子指紋により，それぞれの流出を抑止する．実験では構築したシステム上で帯域資源と計算資源のオーバヘッドを計測し，ライブ映像配信に十分に適用可能であることを示す．

Construction and Evaluation of Live Video Streaming System with Authentication by Broadcast Encryption over IP Multicast

Yoshitaka Morimura,[†1] Tetsutaro Uehara,[†2]
Shuhui Hou[†1] and Michihiko Minoh[†2]

We constructed a live video streaming system over IP Multicast, which uses SRTP and delivers the decryption key with broadcast encryption. Generally, live video streaming with authentication has problems as illegal distribution of user keys and decrypted video. Our system deters user key distribution using characteristics of broadcast encrpytion, which has different user keys by users, and deters decrypted video distribution using digital fingerprint, which embeds user ID into video as watermark. We evaluate overhead of computational resource and network resource on the constructed system and show the system works in realtime for live video streaming.

1. はじめに

今世紀に入り，インターネットにおける映像配信は YouTube に代表されるように急速な普及を見せた．電波放送やケーブルテレビなどの既存の映像配信設備を持たない集団や個人でも，CGM（Consumer Generated Media）として映像による創作活動を活発に行うようになっている．この流れに応じ，地域イベントやサークル活動，教育機関による遠隔教育などを，ネットワークを通じてライブ映像配信することへのニーズが高まっている．たとえば，高校野球の地方大会や人気のストリートミュージシャンのライブなどは，インフラのコストに見合わないため放送局が放送することは少ないが，インターネット上で配信することで数百人から数万人のユーザが視聴することが想定される．実際に，ライブ音声をインターネットラジオとして配信可能なサービスの SHOUTcast では，数百人から数万人のユーザの同時視聴が行われている[1)]．

ライブ映像配信で配信される映像は撮影された被写体に関し，著作権や肖像権など多くの権利を含んでいるため，これらの保護は重要な課題である．著作権保護や肖像権保護を行うためには，権利を持つ映像の配信者の意に沿わない形で映像を利用しようとするユーザを排除しなければならない．また，映像に対する課金制度の構築も重要な課題である．既存の映像配信設備を持たない集団や個人でも容易に映像から対価が得られるようになれば，より活発な創作活動が行われるようになると考えられる．映像に対する課金制度の構築を行うためには，対価を払わずに不法に映像を閲覧しようとするユーザを排除しなければならない．したがって，著作権・肖像権保護や課金制度の構築を行うためには，配信者は閲覧を許可するユーザに対して認証を行い，正しく認証されたユーザのみがライブ映像を閲覧可能なシステムの構築が必要である．このようなシステムを，ここでは**認証型ライブ映像配信**と呼ぶ．

認証型ライブ映像配信において，インターネットのようなオープンな経路を利用する際には，配信経路上で閲覧を許可していないユーザが映像を盗聴するという問題がある．配信側でコンテンツを暗号化し，正しく認証されたユーザにのみ復号を許すことで，この問題は防止することができる．このとき，サーバ側で暗号化に用いる鍵を**サーバ鍵**，正しく認証されたユーザに配布され復号に用いる鍵を**ユーザ鍵**と呼ぶ．

†1 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University
†2 京都大学学術情報メディアセンター
Academic Center for Computing and Media Studies, Kyoto University

© 2009 Information Processing Society of Japan

しかし，認証されたユーザが，ユーザ鍵や復号映像をネットワークを通じて不法に再配布すると，認証されていないユーザがライブ映像を閲覧することができてしまう．この行為をネットワーク映像配信における**海賊行為**という，DVD を代表とする蓄積型の映像に対する YouTube や P2P などを利用した海賊行為はすでに巨大な規模となっていることが判明しており，人気のある配信者が行うライブ配信においても同様の行為が行われることが懸念されている．

このような海賊行為を抑止するためには，ユーザ鍵や復号映像をだれが流出させたかを追跡可能とすることが有効であると考えられる．流出者が追跡可能であれば，その法律的・社会的な責任が問えるようになり，流出者にとって海賊行為が見合わなくなると考えられる．流出者を特定可能とするためには，ユーザ鍵や復号映像がそれぞれユーザごとに異なる ID を持つようにし，それらが流出した際は発信者の持つ ID 情報との照合により流出者が特定できるようにすればよい．本研究は既存の映像放送設備が対象としないような数百人程度から数万人程度までのユーザ数を対象とし，異なるユーザ鍵の配布と映像への ID 情報の挿入を行う認証型ライブ映像配信システムの構築を目標とする．

2. 認証型ライブ映像配信におけるユーザ鍵と復号映像の流出抑止

2.1 想定するサービス

本研究で想定する認証型ライブ映像配信サービスは，以下のようなものである．

サービスにはサービス管理者と映像配信者，および n 人の登録ユーザが存在する．個々の登録ユーザは映像配信者から配信される複数のストリームの中から，視聴契約などにより視聴したいストリームを選択できる．サービス管理者は，映像配信者からユーザ管理に関する委託を受け，ユーザ ID や暗号化・復号に必要な鍵の管理と，海賊ユーザの検出を行う．サービス管理者と映像配信者を分離することで，サービス管理者は複数の映像配信のユーザ管理の集中による効率化が行え，一方映像配信者はユーザ管理の負担が減り映像配信に注力できるという利点がある．サービス全体の流れは次のとおりである．

サービス管理者は，事前に 1 個のサーバ鍵と n 個のユーザ鍵を生成し，対応するユーザ ID とともにサービス DB に記録しておく．また，サーバ鍵を映像配信者へ配布し，サービスへ登録を希望するユーザにユーザ ID とユーザ鍵を配布する．ユーザ ID とユーザ鍵はサービス内で一意であり，サービス内で提供される複数のストリームに対して使用することができる．

映像配信者の映像発信システムは各ストリームの配信開始の前に配信プログラムを各ユーザに提示し視聴に対する希望を把握することにより，事前に視聴許可を与えるユーザを決定しておく．ストリームのライブ配信開始時には，発信システムは暗号化を行ったストリームをユーザに配信する．ライブ映像配信はリアルタイム性が重要な価値を持つため，蓄積型の映像配信と比べ時間的にアクセスが分散せず，同時に多数のユーザの視聴希望を満たす必要がある．したがって，ライブ映像配信には 1 対多の同期的な配信が可能な IP マルチキャストによる配信が適しており，想定するサービスではこれを使用する．ユーザ側の受信システムはネットワークから受信したストリームを自身のユーザ鍵により復号し，ID 情報を映像に挿入する．

ストリームを視聴可能なユーザが海賊行為を行った場合，ユーザ鍵や復号映像がネットワーク上に流出する．サービス管理者は，違法な流出が疑われるネットワーク上に流出したコンテンツを定期的に検証するクローラを用いることで，海賊行為を検出する．クローラはサービス DB 中のユーザ鍵と ID の情報を持ち，ユーザ鍵や復号映像から海賊ユーザを検出し，法的機関にそれを通報する．このようなサービスの概要を**図 1** に示す．

2.2 関 連 研 究

上記のようなシステムにおいては，ユーザごとに異なるユーザ鍵でマルチキャストされたストリームを復号可能な暗号化方式が必要となる．一般的な DES，AES といった共通鍵暗号方式や RSA，ElGamal といった公開鍵暗号方式は 1 対 1 の暗号化を前提とする．1 つの暗号化ストリームを復号できるユーザ鍵は 1 つであり，このような目的にはそぐわない．なぜなら，単純にユーザ数 n の分だけ異なる鍵でストリームを暗号化してマルチキャストする場合，元のストリームの使用帯域に対して n 倍の帯域を使用することとなり，数千人，数万人のユーザ数の場合は帯域資源のオーバヘッドが許容できない水準となるからである．この対策として，ストリーム自体を復号する鍵は全ユーザ共通として，それを配布する際にユーザごとに異なるユーザ鍵によりストリーム用の鍵を 1 対 1 暗号化する方法があげられる．たとえば，地上デジタルテレビ放送などにおいて認証型の配信を実現する B-CAS では各ユーザ共通のスクランブル鍵 K_s とワーク鍵 K_w，ユーザごとに異なるマスタ鍵 K_m の 3 種類の鍵を利用する[2),3)]．K_w は K_m によって暗号化され，各ユーザは復号した K_w を 1 カ月から 1 年程度を目安として保存する．実際のストリームは K_s により暗号化され，K_s は K_w によって暗号化されて配信される．各ユーザは保存した K_w をもとに K_s を復号し，それによりストリームの復号が可能である．しかしながら，この方法はユーザに共通な K_w を長時間保存するため，その流出の恐れが問題となる．K_w の配布を短期的にして使い捨てにしても，鍵長の n 倍の大きさのデータを伝送する必要があり，鍵配布のための帯域

© 2009 Information Processing Society of Japan

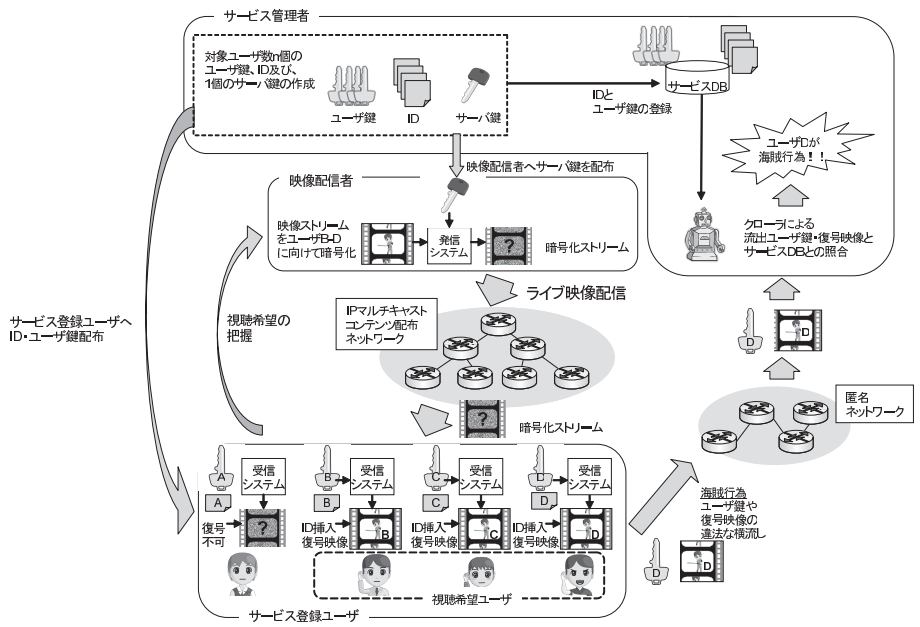

図 1　サービス概要図
Fig. 1　Overview of the service.

のオーバヘッドを生じることとなる．

マルチキャストのような 1 対多に適した暗号方式として，前述の問題を解決する放送型暗号が提案されている[4)–6)]．放送型暗号を用いると，配信者が持つ単一のサーバ鍵で暗号化した単一のストリームをマルチキャスト配信し，それを受信した複数のユーザは自身の持つそれぞれ異なるユーザ鍵によってストリームを復号することができる．したがってこれらの暗号を用いることで異なるユーザ鍵の配布という目標は達成できる．このとき，放送型暗号では暗号化の際のデータ量の増加を O(1) から $O(\sqrt{n})$ 程度に抑えることが可能であり，帯域資源のオーバヘッドを抑制することができる．しかし，放送型暗号の実装に関する文献 7), 8) の報告は一般的な符号列を対象とする暗号化性能単体の評価にとどまっており，暗号化されたストリームを伝送するプロトコルの選択や映像という巨大なデータを暗号化する際の計算資源のオーバヘッドおよび具体的なユーザ数を指定したうえでの帯域資源のオーバヘッドの評価は行っていないため，実際にライブ映像配信に適用した際の実現可能性は未知である．また，放送型暗号をライブ映像配信に適用する際には，鍵の流出を行った海賊ユーザを無効化する仕組みや，リアルタイム性の高い配信プロトコルの選択を考慮しなければならないが，上記の研究ではそのような議論はなされてこなかった．

一方，復号映像の流出を防止するためには，映像信号自身に ID 情報を埋め込む必要がある．このような利用者の識別を目的としてコンテンツ自身に ID 情報を埋め込む手法は，電子指紋と呼ばれる[9)]．対象が画像もしくは映像の場合，画質に影響なく電子指紋を挿入するために，電子透かしが用いられる．ライブ映像配信に電子透かしを挿入する場合，高いリアルタイム性を持つ電子透かしが要求されるので，そのような方式の提案がいくつかなされている[10),11)] が，いずれも発信側でユーザごとにユーザ ID を埋め込むことを想定している．マルチキャストの場合サーバ側ではユーザごとに異なる透かしの挿入は不可能であるため，ユーザ側の受信システムにおける挿入が必要となる．そのような透かし挿入の検討は文献 12), 13) でなされているが，具体的な透かし手法は選択されておらず，PC 上でソフトウェアを構築した場合の計算資源の評価がなされていない．文献 14) では映像の復号と電子指紋の挿入を高速かつ結合的に行う手法が検討されているが，暗号化がスクランブル方式で経路上における映像の可視性が高いこと，および指紋挿入後の映像の PSNR が平均して 40 dB を下回り透かしの性能が低いことから本研究では対象外とする．以上からこれまでの方式ではユーザ側では放送型暗号の復号と電子指紋挿入を同時に行うような応用は想定されておらず，そのようなシステムの構築と，そのシステムの計算資源のオーバヘッドの評価が課題としてあげられる．

2.3　ユーザ鍵と復号映像の流出を抑止する認証型ライブ映像配信システム

本研究では，放送型暗号と電子指紋を組み合わせ，ユーザ鍵と復号映像の流出を抑止する認証型ライブ映像配信システムを構築する．この際に，前節の未解決の問題点を解決するため，(i) 放送型暗号の計算資源と具体的なユーザ数を指定したうえでの帯域資源の評価，(ii) リアルタイム性の高いプロトコルの選択，(iii) 海賊ユーザが発見された場合のそのユーザ鍵の動的な無効化，(iv) PC 上のソフトウェアで放送型暗号の復号と電子指紋挿入を同時に行う場合の計算資源の評価の 4 点を行う．

(i)，(iv) については，次節で述べるようなシステムを PC 上で実際に構築したうえで，計算資源・帯域資源のオーバヘッドはライブ配信の要求に対し十分に小さいことを示す．(ii) については，リアルタイム映像配信に適したプロトコルとして，マルチメディアのライブ配信に適した技術である RTP に暗号化機能を組み入れた SRTP[15)] を利用する．SRTP は IP

© 2009 Information Processing Society of Japan

電話の暗号化を対象として活発な利用がなされているが，放送型暗号による映像配信と組み合わせて SRTP を利用する試みは行われておらず，本研究ではそのようなシステムの構築を行う．(iii) については，海賊ユーザが発見された場合にそのユーザ鍵の動的な無効化を行うために，放送型暗号の枠組みを利用してストリームごとに異なるセッション鍵を生成し，さらにそのセッション鍵をストリームの配布中に短期間で定期的に更新する．放送型暗号で生成されたセッション鍵は生成時に有効なユーザ鍵の指定が行えるので，海賊ユーザの特定ができれば更新時にユーザ鍵の動的な無効化を行うことが可能となる．したがって，本研究では SRTP による暗号化プロトコルに放送型暗号によるセッション鍵の動的更新の手続を組み入れることで (iii) を達成する．次章では，このようなシステムの具体的な実現法を述べる．

3. IP マルチキャストを用いた放送型暗号による暗号化と電子指紋の挿入を行う認証型ライブ映像配信システムの構築

放送型暗号システムには，結託攻撃に強い耐性を持つ Boneh らによる放送型暗号[6] を用いることとする．以降，Boneh らの方式を BGW 放送型暗号と呼ぶ．BGW 放送型暗号を用いれば，単一のサーバ鍵から特定の符号列とそれを暗号化したものを生成することができる．ここではこの処理を BGW 暗号化と呼ぶ．暗号化された符号列はユーザ鍵を用いることで復号することが可能で，この処理を BGW 復号と呼ぶ．このとき，特定の符号列は送信者が選択することができないため BGW 暗号化自体は任意の映像ストリームを暗号化することはできない．しかし，BGW 暗号化した特定の文字列をネットワークを通じて配布し受信側でそれを BGW 復号し，発信システムと受信システムがその特定の文字列を共有して既存の共通鍵暗号システムの鍵として用いることで，間接的に任意の映像ストリームを暗号化・復号することが可能である．以降この特定の文字列を**共通鍵**，それを BGW 暗号化したものを**暗号ヘッダ**と呼ぶ．

SRTP は，共通鍵暗号によって暗号化された映像ストリームをリアルタイム配信するのに適したプロトコルとして RFC3711 で規定されている．提案するシステムは，SSH や SSL などの公開鍵暗号を共通鍵交換に利用するプロトコルと同様，共通鍵の安全な鍵配送方式として BGW 暗号方式を用いた鍵の暗号化・配送・復号を行い，映像配信者とユーザが共通鍵を共有したうえで SRTP プロトコルにより高速な共通鍵暗号方式による IP マルチキャスト配信を行う．以下では，提案するシステムの前処理，発信システム，受信システムについて詳細に述べる．

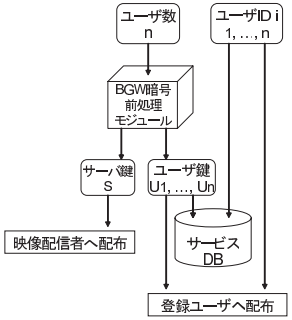

図 2　前処理システム
Fig. 2　Setup system.

提案するシステムにおけるサービス管理者による前処理を**図 2** に示す．サービス管理者は，発信前に前処理としてユーザ数 n を指定し，BGW 暗号前処理モジュールによってサーバ鍵 S およびユーザ鍵 $\{U_i \,|\, i = 1, \ldots, n\}$ を生成し，サーバ鍵 S を映像配信者に配布し，ユーザ ID i とユーザ鍵 U_i を認証されたユーザに配布する．このとき，発信者はユーザ ID i とユーザ鍵 U_i をサービス DB に記録し，認証されたユーザと紐付けておくものとする．

BGW 暗号では 1 度生成したサーバ鍵・ユーザ鍵の組に対し，毎回の映像配信ごとに有効・無効を個々のユーザ鍵ごとに切り換えることが可能である．したがって，サービス管理者はサービス開始時に 1 度サーバ鍵とユーザ鍵を生成すれば，それらを異なる映像配信者たちの複数の映像配信に対して継続的に利用することができる．ユーザ数 n を指定する際には，サービス途中のユーザ数の増加も想定し，サービス開始時の見込ユーザ数より大きい数を作成しておくことが望ましい．本研究の想定するサービスにおいては，数万人の鍵をあらかじめ作成しておけば十分であると考えられる．なぜならば，数十万人の視聴が見込める映像配信は，高コストな電波放送やケーブルテレビ放送などのインフラを利用できるため，提案手法の対象外であるからである．例外的にサービス途中で数十万以上のユーザに対応する必要がある場合は，改めて数十万人のユーザ鍵を作り直して配布しなおし，十分な移行期間を経たうえで有効な鍵を切り換える対応をとる必要がある．

映像配信者の発信システムは映像圧縮モジュール，BGW 暗号化モジュール，SRTP 暗号化モジュールからなる（**図 3**）．映像圧縮モジュールは PC に取り込まれた映像の圧縮符号化を行い映像ストリーム M として出力する．発信システムは有効ユーザ集合 $A \subseteq \{1, \ldots, n\}$ を指定し，BGW 暗号化モジュールによってサーバ鍵 S をもとに共通鍵 K と暗号ヘッダ

© 2009 Information Processing Society of Japan

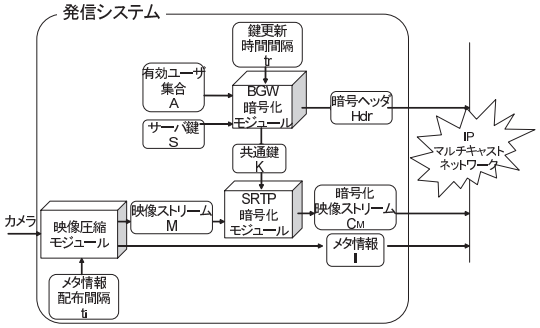

図 3　発信システム
Fig. 3　Transmitting system.

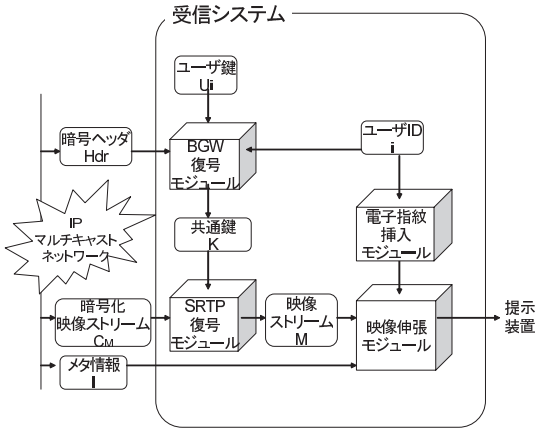

図 4　受信システム
Fig. 4　Receiving system.

Hdr を生成する．次に，SRTP 暗号化モジュールが共通鍵 K を用いて映像ストリーム M を暗号化したうえで RTP 形式に整形した暗号化ストリーム C_M をネットワークに IP マルチキャスト送信する．映像の復号に必要な暗号ヘッダ Hdr や，映像自身の画面サイズやタイトルといったメタ情報 I も同様に IP マルチキャスト送信する．これらの情報はマルチキャストに途中から参加するユーザのことも考慮する必要があるため，一定の配布間隔 t_i で定期的に送信する．

このとき，ライブ映像配信の継続中にユーザが海賊行為を行ってユーザ鍵を流出させる可能性がある．ユーザ ID i を持つユーザの鍵 U_i の流出が検出された場合，そのユーザの鍵を無効化させなければならない．特定ユーザ鍵の無効化を実現するため，発信システムは共通鍵 K と暗号ヘッダ Hdr の定期的な更新を行い，つねに有効ユーザ集合 A の変更が行えるようにする．更新には一定の計算量が必要となるため，リアルタイム配信に影響を及ぼさない範囲で可能な限り短い更新間隔 t_r での更新を行う．

一方，受信システムは BGW 復号モジュール，SRTP 復号モジュール，映像伸長および電子指紋挿入モジュールからなる（**図 4**）．ユーザ ID i を持つユーザの BGW 復号モジュールは定期的に受信する Hdr と，あらかじめ配布された U_i および i をもとに共通鍵 K を復号する．SRTP 受信モジュールは K をもとに，受信した暗号化ストリーム C_M を復号し，映像ストリーム M を出力する．映像伸長および電子指紋挿入モジュールはメタ情報 I と映像ストリーム M から映像を伸長し，同時にユーザ ID i を電子透かしとして挿入する．

このとき受信システムは，共通鍵 K や映像ストリーム M を展開する一時記憶領域がユーザから可読でなく，リバースエンジニアリングなどによる解読などの攻撃がなされても一定期間それに耐えうること（データ難読条件）および放送型暗号の復号から電子指紋の挿入までが一体化されたソフトウェアによりなされること（一体性条件）が満たされていることとする．データ難読条件は既存のソフトウェア難読化手法[16] により可能とすることができる．一体性条件は，図 4 のモジュールをすべて含む一体型のシステムを開発することで可能となる．ユーザがデータ難読条件と一体性条件を満たす最新の受信システムを利用していることは，受信システム中にそのバージョンごとに異なるプレイヤ鍵 K_p を埋め込み，放送型暗号由来の共通鍵 K に加えて K_p によって映像ストリームを暗号化することで保証することができる．プレイヤ鍵 K_p はユーザ鍵 U_i と異なり認証を必要としないので，万が一脆弱性により鍵が流出した場合でも，オンラインアップデートにより脆弱性を修正したソフトウェアごと自動的・同報的に更新することが容易に可能である．

実際の構築にあたり，映像圧縮モジュールと映像伸長モジュールには Windows Media Encoder および Windows Media Player を用い，映像圧縮符号化形式には Windows Media Video 9 形式を用いた．BGW 暗号化モジュールおよび SRTP 暗号化モジュールは，Windows Media Encoder から HTTP により映像ストリームを受け取り SRTP により IP マルチキャスト送信を行う送信プロキシとして実装した．BGW 復号モジュールおよび SRTP 復号モジュールは，SRTP により暗号化ストリームを受け取り，HTTP により Windows Media

© 2009 Information Processing Society of Japan

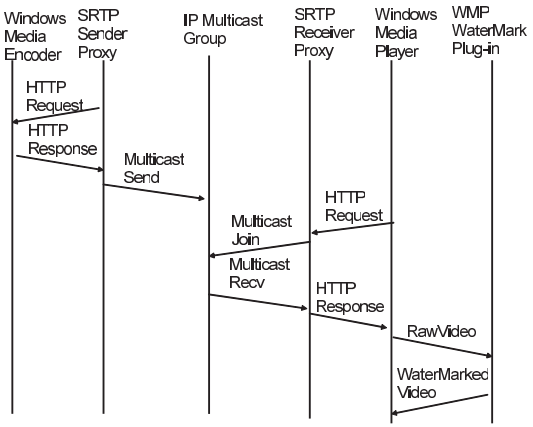

図 5　シーケンス図
Fig. 5　Sequence figure.

Player に出力する受信プロキシとして動作する．SRTP による共通鍵暗号化の暗号方式には広く普及している AES を用いた．また，映像伸長モジュールの電子指紋挿入は Windows Media Player のプラグインとして開発した．受信者による映像の配信要求開始から閲覧開始までのシーケンスを**図 5** に示す．また，電子透かしの挿入には，PC 上でリアルタイムにソフトウェアによる透かしの挿入が可能な C4 Technology 社（現 SBI ネットシステムズ社）の M5 透かし方式[⋆1]を用いた．今回の構築では受信システムがデータ難読条件，一体化条件を完全に満たすまでには至っておらず，プレイヤ鍵 K_p の追加も行っていないが，計算資源と帯域資源のオーバヘッドはこれらの条件と独立であると考えられるため，その計測と評価を行うことが可能である．次章では，構築したシステムの評価実験を行い提案するシステムがライブ映像配信に十分に適用可能であることを示す．

4. 評 価 実 験

提案システムを PC 上に構築し，計算資源と帯域資源の使用状況を評価する実験を行った．ライブ映像発信システム・受信システムの構築には，それぞれ 2006 年度に個人向けの小売店で入手した PC を用いた．これらの PC は，Xeon 2.8 GHz デュアル CPU と 2 GB のメモリを搭載している．現在は CPU のマルチコア化により，これと同程度の計算能力を持つ PC が容易に入手可能である．OS は Windows XP SP2 を用いた．対象とするユーザ数 n は数百人程度から数万人程度とし，比較的大規模な IP マルチキャストにも対応可能なシステムを想定している．

⋆1 http://sbins.co.jp/introduction/digital_watermarking/index.html，M5 方式は共同研究による提供．

図 6　映像例
Fig. 6　Example of video.

表 1　フレームあたり SRTP 暗号化時間の平均
Table 1　Average of STRP encryption time per frame.

	2 M	1 M	500 k
送信 (sec)	0.000031	0.000009	0.000002
受信 (sec)	0.000056	0.000027	0.000020

ライブ映像の撮影には Logitech Qcam 4000 Pro を用いた（**図 6**）．撮影された大きさ QVGA（320 × 240），毎秒 30 フレームの映像を，Windows Media Video 形式で圧縮した．このとき，圧縮映像の構造の最小単位である GOP（Group Of Picture）の時間長は，Windows Media Encoder で設定可能な最小値の 1 (sec) とした．

まず，SRTP 暗号化モジュールおよび SRTP 復号モジュールの計算資源の評価を行った．圧縮後のビットレートが 2 Mbps，1 Mbps，500 Kbps における，SRTP 暗号化モジュール・復号モジュールそれぞれの，1 フレームの映像データの処理に必要な CPU 使用時間を 5 分間計測し平均を算出したところ，**表 1** のようになった．

SRTP はすべての映像ストリームを暗号化するので，秒間 30 フレームの映像のリアルタイム処理を行うためには映像 1 フレームあたりの計算時間が $\frac{1}{30}$ (sec) を超えない必要があ

© 2009 Information Processing Society of Japan

表 2　共通鍵 K の暗号化，復号にかかる時間 t_K^{gen}，t_K^{res} の平均値，標準偏差，最大値，最小値
Table 2　Average, standard deviation, maximum and minimum value of encryption t_K^{gen} and decryption time t_K^{res} for common key K.

	平均値	標準偏差	最大値	最小値
t_K^{gen} (sec)	0.0419	0.0073	0.0781	0.0312
t_K^{dec} (sec)	0.0363	0.0079	0.0937	0.0156

表 3　フレームあたり電子指紋挿入時間の平均
Table 3　Average time of fingerprint insertion per frame.

	2 M	1 M	500 k
挿入時間 (sec)	0.0137	0.0133	0.0125

る．表 1 の結果，送受信時の 1 フレームあたりの処理時間は $\frac{1}{30}$ (sec) の 1%にも満たないため，単体では十分にリアルタイム処理が可能であるといえる．

次に，BGW 暗号化モジュール・復号モジュールの共通鍵の BGW 暗号化・BGW 復号に必要な計算資源の評価を行った．BGW 暗号化・復号で計算量が大きいのはペアリング計算[17] と整数群のべき乗計算である．用いたペアリング計算は Pentium III のマシンで 10–100 (msec) 程度で計算できることが報告されている[8]．べき乗計算は binary algorithm により指数 n に対して $O(\log n)$ で計算できることが知られているが，用いる底が 10^{76} 程度，指数が 10^{47} 程度とともに巨大で計算機の通常の整数演算の範囲に収まらないため，定性的な評価が難しい．したがって，今回は実機による計算時間の評価を行った．BGW 暗号化・復号に要した CPU 使用時間 t_K^{gen}，t_K^{res} を 100 回計算を繰り返して行い，平均値・標準偏差・最大値，最小値を算出したところ，結果は**表 2** のとおりであった．BGW 放送型暗号に基づく手法では，BGW 暗号化・BGW 復号に要する時間はユーザ数 n とは関係なく一定である．

また，電子指紋の挿入モジュールが電子指紋の挿入に要した CPU 使用時間は**表 3** のとおりであった．このとき対象フレームは QVGA 毎フレームであり，電子透かしの強度は設定可能な強度のうち最強の 5 とした．上記処理のうち，SRTP による暗号化・復号および電子指紋の挿入に比べ，放送暗号モジュールの共通鍵の BGW 暗号化・復号には比較的大きな時間がかかるため，処理をフレームの暗号化処理のバックグラウンドで行う必要がある．両処理をあわせて CPU を使いきるとフレーム落ちなどの処理落ちを引き起こすため，リアルタイム性を保持するためには共通鍵の更新間隔 t_r を大きめに設定する必要がある．

表 4　共通鍵 K の更新間隔 t_r に対し，送信システム，受信システムそれぞれが必要とする下限
Table 4　Minimum value required by transmitting system and receiving system for updating interval t_r of common key K.

	2 M	1 M	500 k
送信 (sec)	0.042	0.042	0.042
受信 (sec)	0.021	0.022	0.023

CPU 使用時間を基準に考えると，発信システムでは 1 つの鍵の生成に必要な CPU 時間を t_K^{gen} (sec)，1 フレームの暗号化に必要な時間が t_{enc} とすると，以下の式を満たす必要がある．

$$\frac{t_K^{gen}}{t_r} \times \frac{1}{30} + t_{enc} < \frac{1}{30} \tag{1}$$

また，受信システムでは鍵の BGW 復号に必要な CPU 時間を t_K^{res} (sec)，1 フレームの復号に必要な時間が t_{dec}，1 フレームの電子指紋挿入に必要な時間 t_f とすると，以下の式を満たす必要がある．

$$\frac{t_K^{res}}{t_r} \times \frac{1}{30} + t_{dec} + t_f < \frac{1}{30} \tag{2}$$

送受信の両方で処理落ちを防ぐためには，t_r は式 (1)，(2) をともに満たす必要がある．2 Mbps，1 Mbps，500 Kbps の映像ストリームにおいて表 1，表 2，表 3 の結果を式 (1)，(2) に代入した場合，送信，受信の双方が必要とする t_r の下限は**表 4** のようになった．表 4 より，映像ストリームのビットレートにかかわらず送信側の方が長い更新間隔を必要としており，実験環境では t_r を 0.042 (sec) 以上にすればよいことが分かる．ただし，映像の圧縮や伸長は GOP の時間長を単位として行われるため，実際の更新間隔はこの条件を満たしかつ GOP の時間長の整数倍とすることが妥当である．本実験では GOP の時間長が 1 (sec) であるため，更新間隔 t_r を 1 (sec) として配信実験を行った．なお，表 1，表 3 の両結果より，STRP 暗号化にかかる時間と電子指紋挿入時間が実験の 2 倍かかる場合でも各々の処理はリアルタイム処理が可能であることが分かる．さらに表 2 の放送鍵があわせて実験の 2 倍かかる場合には更新間隔 t_r は 0.084 (sec) 以上にすればよい．よって，PC の計算能力が実験に用いたものの半分程度であっても，更新間隔が 1 (sec) であれば全体として十分にリアルタイム処理が可能であるといえる．

また，送信・受信のシステム全体を通じた遅延時間とリアルタイム性を評価するため，提案手法を適用せずに Windows Media Player から直接 Windows Media Encoder に接続し

© 2009 Information Processing Society of Japan

表 5　提案手法非適用時・適用時の映像の撮影から表示までの遅延 D_{conv}，D_{prop} の平均値，標準偏差，最大値，最小値

Table 5　Average, standard deviation, maximum and minimum value of D_{conv}, D_{prop}, that are delay time between capturing and displaying video when not applying and applying proposing method.

	平均値	標準偏差	最大値	最小値
D_{conv} (sec)	5.386	0.037	5.498	5.336
D_{prop} (sec)	5.604	0.034	5.669	5.532

た場合と，提案手法を適用したシステムのそれぞれに対し映像の撮影から表示までの遅延時間 D_{conv} と D_{prop} を計測する実験を行った．遅延時間の計測は次のような方法で行った．まず，受信システムのディスプレイに msec 単位で時刻を表示する時計を表示し，それを送信システムで撮影したものを受信システムのディスプレイに表示する．1 分ごとに受信システムのディスプレイ表示内容をキャプチャし，前者と後者の時計の時刻の差を求めることで，システム全体を通じた遅延時間が計測できる．このようにして 20 分間に 20 回計測した D_{conv} と D_{prop} の平均値，標準偏差，最大値，最小値を**表 5** に示す．このとき，D_{prop} の平均値の D_{conv} の平均値に対する増加率は 4%程度であり，構築したシステムによる遅延の増加は許容できる範囲であるといえる．またこの実験中，CPU 使用率は 100%に達しておらず処理能力に余裕を残しており，かつ D_{prop} の標準偏差は D_{conv} と同程度であり安定していることから，送信・受信システムは十分にリアルタイム性を保って動作したと考えることができる．また，D_{prop} の最大値と最小値は平均時間からみて $\pm\frac{2}{30}$ (sec) 程度に収まるため，送信プロキシ・受信プロキシのバッファサイズは数フレーム分を確保すればよいと考えられる．

また，電子指紋挿入にともなう画質劣化，および透かしの圧縮耐性の評価を行うため，電子指紋挿入後の PSNR と，伸長した透かし入り映像を 2 Mbps，1 Mbps，500 Kbps それぞれに再圧縮を行った際の指紋検出率を**図 7** に示す．利用した電子透かしモジュールでは透かし強度を 5 段階に設定可能であり，強度を強くするほど圧縮耐性は強まるが画質が劣化する．これらはトレードオフの関係にあるため，ここでは各透かし強度に対し (PSNR ∗ 検出率) を評価関数としこれを最大化する強度を用いることとする．図 7 のデータにこの評価関数を適用した結果，2 Mbps，1 Mbps，500 Kbps いずれの圧縮率においても透かし強度 2 が最良と判断されるため，本実験ではこれを強度として用いた．ただし，受信側の計算機環境が非力である場合，電子指紋の挿入対象はすべてのフレームではなく確率的に選択されたフレームにせざるをえない．計算機環境の非力さは，CPU 使用率と使用時間を計測すること

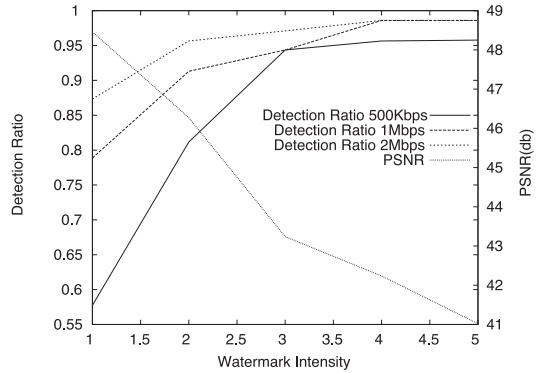

図 7　透かし強度変化に対する PSNR および指紋検出率の変化

Fig. 7　PSNR and detection ratio of fingerprint for fingerpting intention.

とで求められる．1 フレームの処理にかかる時間は CPU 使用時間で求められる一方，1 フレームの表示時間に対する CPU 割当て時間は $\frac{1}{30}$ (sec) に CPU 使用率をかけて求められるため，前者を後者で割ることで処理能力の不足率が求まる．不足率が 1 を超える場合，その割合だけフレームを間引くことになる．このような場合，電子指紋の挿入されたフレーム数の減少により検出力は弱くなるため，電子指紋の強度を上げ，処理能力の不足率の逆数と検出率の積を，間引きが必要でない場合の検出率に相応させることが考えられる．

次に，帯域資源に対するオーバヘッドの評価を行う．提案システムの適用が使用帯域に与える影響として IP マルチキャスト用のメタ情報 I のデータ量 D_I (bit)，および暗号ヘッダ Hdr の配送による鍵のデータ量 D^n_{Hdr}(bit) がある．暗号ヘッダのデータ量 D^n_{Hdr} はユーザ数 n によって変化する．メタ情報および暗号ヘッダの配布間隔 t_i (sec) に対し，使用帯域に与える影響 ΔB は以下の式となる．

$$\Delta B = (D_I + D^n_{Hdr})/t_i \tag{3}$$

提案システムにおいて，$n = 560$，5600，56000 の場合に D_I，D_{Hdr} と t_i の関係を求めたところ**図 8** のようになった．たとえば $n = 5600$ の場合，1 Mbps のストリームに対し使用帯域の増加を 10%以内に抑えたい場合，t_i を 0.51 (sec) 以上に設定することで条件を満たす使用帯域の設定が可能となる．本実験では，共通鍵 K の更新時間と同様，GOP の時間長の整数倍となるよう配布間隔 t_i を 1 (sec) として配信実験を行った．

© 2009 Information Processing Society of Japan

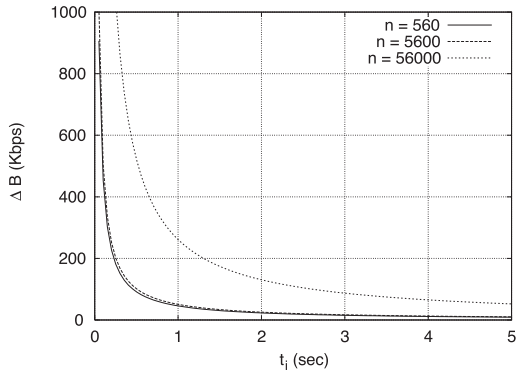

図 8　$n = 560$, 5600, 56000 のときのメタ情報および暗号ヘッダの配布間隔 t_i に対する使用帯域の増加 ΔB
Fig. 8　Bandwidth increse ΔB for for distribution interval t_i of meta information and encryption header for $n = 560$, 5600, 56000.

5. おわりに

我々は IP マルチキャスト上の SRTP を用いた鍵配送に放送型暗号を用いた認証型ライブ映像配信システムを，ソフトウェアによる実装で構築した．実験では個人向けの小売店で入手可能な PC 上でソフトウェアを動作させ，数百人から数万人のユーザ数を想定し，帯域資源と計算資源のオーバヘッドを計測した．結果，共通鍵の更新間隔とメタ情報および暗号ヘッダの配布間隔を 1 (sec) に設定することで，処理落ちがなくかつ帯域増加を 10%以内に抑え，ライブ映像配信に十分に適用可能なことを示した．今後は構築したシステムを実際にライブ映像配信を希望するユーザに利用してもらい，リアルタイム性や画質に関する主観的な評価を行う予定である．ライブ映像配信のアプリケーションとしては，遠隔教育のための講義映像配信などを想定している．

参　考　文　献

1) Nullsoft: SHOUTCast Free internet radio.
available from http://www.shoutcast.com (accessed 2008-06-06)
2) 電波産業会：ARIB STD-B25 デジタル放送におけるアクセス制御方式.
入手先 http://www.arib.or.jp/english/html/overview/doc/2-STD/B25v5_0.pdf (参照 2008-09-18)
3) 山田　宰，映像情報メディア学会：デジタル放送ハンドブック，オーム社 (2003).
4) Fiat, A. and Naor, M.: Broadcast Encryption, *Proc. Crypto '93*, pp.480–491, Springer (1993).
5) 光成滋生，渡辺秀行，吉田真紀，境　隆一，笠原正雄：楕円曲線上のペアリングを用いた不正者追跡法の拡張，情報処理研究報告，CSEC，Vol.2002, No.68, pp.261–266 (2002).
6) Boneh, D., Gentry, C. and Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, *Proc. Crypto '05*, pp.258–275, Springer (2005).
7) Amberker, B.B., Koulgi, P. and Nirmala, M.: Some Implementation Issues in the Fiat-Naor Broadcast Encryption Schemes, *Proc. ADCOM 2006*, pp.634–635 (2006).
8) Lynn, B.: The Pairing-Based Cryptography Library Benchmarks. available from http://crypto.stanford.edu/pbc/times.html (accessed 2008-06-06)
9) Liu, K.J.R., Trappe, W., Wang, Z.J., Wu, M. and Zhao, H.: *Multimedia Fingerprinting Forensics for Traitor Tracing*, Hindawi Publishing Corporation (2005).
10) Echizen, I., Tanimoto, K., Yamada, T., Daninaka, M., Tezuka, S. and Yoshiura, H.: PC-based Real-time Watermark Embedding System with Standard, *Proc. SMC2006*, pp.267–271 (2006).
11) Kim, K., Lee, H., Im, D. and Lee, H.: Practical, Real-Time, and Robust Watermarking on the Spatial Domain for High-Definition Video Contents, *IEICE Trans. Inf. & Syst.*, Vol.E91-D, No.5, pp.1359–1368 (2008).
12) Lee, J. and Yoon, K.: The System Integration of DRM and Fingerprinting, *Proc. ICACT 2006*, pp.2180–2183 (2006).
13) 山田隆亮，吉浦　裕，越前　功，小川一人，室田逸郎，大竹　剛，合志清一：放送コンテンツの著作権保護における電子透かしの利用方法，映像情報メディア学会誌，Vol.57, No.9, pp.1157–1167 (2003).
14) Kundur, D. and Karthik, K.: Video Fingerprinting and Encryption Principles for Digital Rights Management, *Proc. IEEE*, Vol.92, No.6, pp.918–932 (2004).
15) Baugher, M., McGrew, D., Naslund, M., et al.: The Secure Real-Time Transport Protocol (SRTP). available from http://www.ietf.org/rfc/rfc3711.txt (accessed 2008-06-06)
16) 門田暁人：ソフトウェアプロテクションの技術動向（前編）：ソフトウェア単体での耐タンパー化技術，情報処理，Vol.57, No.4, pp.431–437 (2005).
17) Lynn, B.: On the Implementation of Pairing-Based Cryptosystems, PhD Thesis, Stanford University, Stanford (2007).

(平成 20 年 6 月 10 日受付)
(平成 20 年 12 月 5 日採録)

© 2009 Information Processing Society of Japan

森村　吉貴（学生会員）

平成 16 年京都大学工学部情報工学科卒業．平成 18 年同大学大学院情報学研究科修士課程修了．現在，同大学院情報学研究科博士後期課程在学中．映像の自動撮影およびネットワーク配信関係の研究に従事．IEEE，電子情報通信学会各会員．

上原哲太郎（正会員）

平成 2 年京都大学工学部情報工学科卒業．平成 7 年同大学大学院博士課程研究指導認定退学．同年同大学院工学研究科助手，平成 8 年和歌山大学システム工学部講師，平成 15 年京都大学大学院工学研究科附属情報センター助教授，平成 18 年同大学術情報メディアセンター助教授．システム管理，情報セキュリティ関係の研究に従事．京都大学博士（工学）．IEEE，電気学会，電子情報通信学会，日本ソフトウェア科学会，情報ネットワーク法学会，CIEC 各会員．

侯　　書会（学生会員）

平成 10 年北京科学技術大学講師．平成 16 年京都大学大学院情報学研究科博士後期課程入学，現在在学中．電子透かし，電子指紋，暗号関係の研究に従事．

美濃　導彦（正会員）

昭和 53 年京都大学工学部情報工学科卒業．昭和 58 年同大学大学院博士課程修了．同年同大学工学部助手，昭和 62〜63 年マサチューセッツ州立大学客員研究員，平成元年京都大学工学部附属高度情報開発実験施設助教授，平成 7 年同教授，平成 9 年京都大学総合情報メディアセンター教授，平成 14 年京都大学学術情報メディアセンター教授．画像処理，人工知能，知的コミュニケーション関係の研究に従事．工学博士．IEEE，ACM，電子情報通信学会，画像電子学会，日本ロボット学会各会員．

© 2009 Information Processing Society of Japan