公開日時が指定されたコンテンツの事前配信において視聴制御と著作権保護を実現するプロトコル（継続）

吉　田　真　紀　　大阪大学大学院情報科学研究科助教

1 研究の背景・目的

近年、ネットワーク通信帯域が大幅に拡大したことや、動画再生機器の性能が格段に向上したことにより、動画配信サービスが盛んになってきた。それに伴いデジタルシネマの家庭向け配信の研究開発が活発に行われている。しかし、映画は公開日時が指定されており、公開日時にアクセスが集中した場合、視聴者への配信が滞る可能性がある。この問題に対して、動画の高圧縮符号化方式や、符号化処理の高速化・並列化などが考えられている。それらの対策に加えて、さらに事前に配信できれば、アクセスが公開日時前に分散され、より多くの人が公開日時に遅延なく視聴できる。つまり、視聴者の満足と配信者の売り上げ増加に繋がる。これは、デジタルシネマという新しいサービスの普及と発展に大きく寄与すると期待できる。一方で、事前に配信することでセキュリティに関して新たな問題が起きる可能性がある。よって、セキュリティに関する十分な検討と、セキュリティを保証する技術の創出が求められる。

本研究では平成 20 年度に、映画のように公開日時が指定されたコンテンツの事前配信を対象とし、コンテンツ配信における一般的な要求と事前配信特有の要求を満たすセキュリティ技術、それを利用したプロトコルの基本設計、大規模な配信環境における有用性・実用性の評価を行った。平成 21 年度では、多様な配信形態の実現に向けたセキュリティ要素技術の創出を目指した。まず、提案技術と他技術の融合に向けた課題発見に努め、その有用性・実用性を評価した。さらに、コンテンツの公開条件として日時だけでなく一般的な条件を指定できるように拡張した。具体的には、公開条件を、日時だけでなく料金を支払った場合というように一般化した。これによって、より細やかな視聴制御や課金体系を実現でき、デジタルシネマのサービスの多様化に貢献できる。

2 研究の成果

2.1 安全かつ効果的な技術融合法の考案

事前配信のためのセキュリティ技術と通常配信のための従来技術の融合によって生じるセキュリティに関する課題を検討する。特に重要な課題として、セキュリティ技術は単独で利用する場合には問題が生じなくとも、他のセキュリティ技術と結合されることで互いに干渉し、安全性に関して新たな問題を生じることが挙げられる。配信に関する技術は現在も発展を続けており、その適用環境も広がり続けている。よって、どのような環境において、どのようなセキュリティ技術と融合（結合）されるかを限定できない。

そこで、任意の利用環境における任意のセキュリティ技術との結合に対処するために、[4]の汎用的結合可能性の理論を用いた。汎用的結合可能性の理論は、これまでのセキュリティ技術の安全性証明理論を集大成するような体系として 2000 年台に入って提案され、大きく発展している理論である。その目的は二つあり、一つは名前の由来となった“どのような環境でどのようなセキュリティ技術と結合されても安全となる(汎用的に結合可能な)”セキュリティ技術の実現であり、もう一つはセキュリティ技術の安全性を統一的な手法で定式化できる枠組みを提供することである。

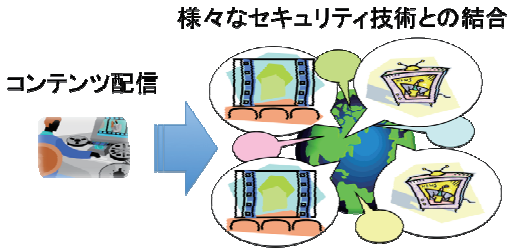

図１　セキュリティ技術の結合の可能性

汎用的結合可能性の理論を用いることで、融合の安全性を定式化し、その安全性を満たす融合法を考案した。また、この課題以外も幅広く検討し、汎用的結合可能性の形式的検証法を提案した。

汎用的結合可能性の形式的検証法：現状最も普及しているネットワークサービスは、オンラインショッピングやネットバンキングである。よって、そこで用いられているセキュリティ技術である公開鍵・秘密鍵型の結合に対処する必要がある。また、近年、電子投票も試験的に運用されており、そこに用いられている公開鍵・秘密鍵型以外の暗号の結合にも対処する必要がある。

本研究では､代表的なセキュリティ技術の汎用的結合可能性を形式的に検証可能とすることを目的とする。形式的検証では、セキュリティ技術とその安全性は記号的に抽象化され、解析される。そのため、基盤技術である記号的モデルを拡張する必要がある。よって、既存のセキュリティ技術を調査し、それらの汎用的結合可能性を記述可能な記号的モデルを提案した。そして、提案した記号的モデルに基づき、検証法を設計した。具体的には、以下の手順で研究を遂行した。

(A) 提案されている暗号技術の調査

現在提案されている暗号技術を調査し，公開鍵・秘密鍵型かそれ以外に分類し、それぞれの特徴と違いについて調べた。現在提案されている暗号技術のほとんどが、[4]で汎用的結合可能性向けに再定義されており、過半数が公開鍵・秘密鍵型以外の暗号技術（コミットメントや紛失通信など）であることが分かった。さらに、それらがどのようなプロトコルにどのように利用されているかを調査し、提案する記号的モデルに必要な記述能力を見定めた。

(B) 汎用的結合可能性向けの記号的モデルの提案

記号的モデルでは、まず調査した暗号技術とそれを利用するプロトコルを記述できるようにする。既存の記号的モデルでの安全性の記述は、プロトコルの種類ごとに発見的であり、手間を要した。それに対して、本研究では汎用的結合可能性の各種概念を記号的モデルに導入することで、汎用的結合可能な安全性と同様の形で記号的な安全性を記述可能にすることを考える。具体的には、本研究グループで提案した[15]の記号的モデルを拡張し，汎用的結合可能性の定義に用いられる各種概念に対応する記号的概念を定義することで、汎用的結合可能性向けの記号的モデルを提案した。提案した記号的モデルでは，(A)で調査したほぼすべての暗号技術が記述可能である。また，ネットワークサービスで必須となる相互認証プロトコルと鍵交換プロトコルのための汎用的に結合可能な安全性に対応する記号的安全性を新たに記述し、共通の方針で記述が可能であることを確認した。これにより,提案した記号的モデルにおける記号的安全性の定義方針の目処が立ち，自動化の可能性がでた．さらに、記号的な安全性のプロトコルの種類によらない共通の記述方針を定め、自動化の目処を立てた。そして､提案モデルで代表的なプロトコルとその安全性を記述できることを確認した。

(C) 任意の暗号技術を利用するプロトコルのための検証法

まず、調査した暗号技術を体系立て、暗号技術の特徴と違いをもとに、公開鍵・秘密鍵型か否かの分類からさらに細分化した。次に，分類した暗号技術ごとに、記号的な記述への変換法を提案した。さらに、それらの暗号技術を利用するプロトコルの記号的な記述への変換法を提案し、鍵交換と相互認証の安全性を記号化し、具体的な検証法を設計した。設計した検証法は、[4]のほぼすべての暗号技術を利用するプロトコルについて、攻撃の漏れがないことを保証できる。

2.2 公開条件の一般化におけるセキュリティ要求の検討

まず、視聴制御のための公開条件にどのような一般化が要求されるかを検討した。そして、それらを特徴づける項目による条件の指定法を策定し、公開条件に関するセキュリティ要求を他技術との融合を想定した上で定式化した。ただし、コンテンツ配信においては、一般的なセキュリティ要求として不正配布の抑止とプライバシー保護、事前配信特有のセキュリティ要求として公開前の不正配布抑止も必須となるため、それらの定式化と矛盾のないように、かつそれぞれの安全性レベルを選択できるように定義した。

コンテンツ配信における一般的な要求（公開後の不正配布抑止、購入履歴の秘匿）：コンテンツ配信における一般的な要求は二つある。一つは公開後に視聴可能となったコンテンツの不正配布抑止である。配信者が不正配布されたコンテンツを発見した場合、 配布した視聴者を特定し、不正を立証したいという要求であり、公開後の不正配布抑止と呼ぶ。もう一つはプライバシー保護に関する要求である。近年プライバシーに対する関心が高まってきており、視聴者が個人情報だけでなく趣味や嗜好がわかる購入履歴を秘匿したいという要求であり、購入履歴の秘匿と呼ぶ。これまでに、公開後の不正配布抑止と購入履歴の秘匿を満たす暗号プロトコルとして、匿名フィンガープリンティング[3] [11] [12] が提案されている。これにより、配信者はコンテンツに視聴者を特定し、不正を立証する情報(特定情報と呼ぶ) を埋め込むことができる。ただし、コンテンツが不正配布されない限り、配信者は特定情報を得ることはできない。

事前配信特有の要求（公開前の不正配布抑止）：事前配信特有の重要な要求として、公開前で視聴できないコ

ンテンツの再配布対策が考えられる。視聴できないコンテンツであっても、再配布されれば、公開後には視聴可能になる。すなわち、事前配信したことにより、不正配布の被害が拡大する。そのため、配信者は公開前に不正配布されたコンテンツを発見した場合､配布した視聴者を特定し、不正を立証したいと考えられる。この要求を公開前の不正配布抑止と呼ぶ。しかし、コンテンツは視聴できない形となっているため、既存の匿名フィンガープリンティング等を用いたとしても､特定情報を抽出できず、購入者を特定し不正を立証できない。すなわち、公開前の不正配布抑止は公開後の不正配布抑止と異なる。そこで昨年度は、事前配信向けに公開前の不正配布抑止の実現方針を考えた。

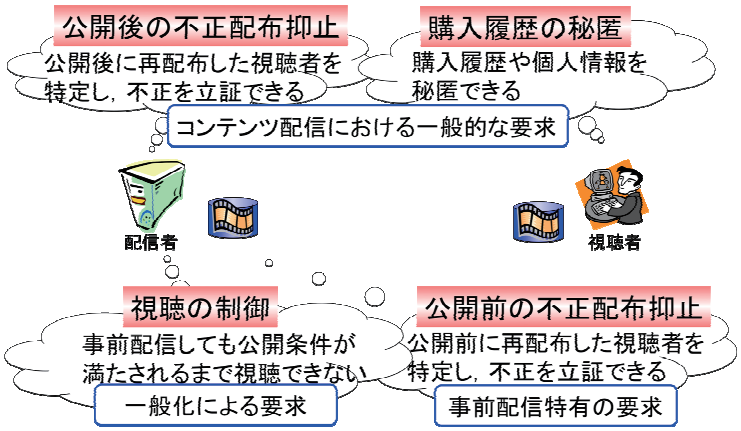

図２　公開条件の一般化におけるセキュリティ要求

一般化による新たな要求（視聴制御）：視聴者がコンテンツを事前に受け取ったとしても、公開条件が満たされない限りは視聴できないが、公開条件が満たされた後は遅延なく視聴できるようにしたいという要求である。昨年度は、公開条件として日時を指定し、その実現のために、日時に基づく暗号技術として、 Timed-release 暗号(あるいはタイムカプセル暗号) [1] [5] [16] [17] を利用した。ここで､[1] [5] [16] [17] の構成法では、時報局と呼ばれる信頼できる機関が放送する正式な時報がなければ復号できないように暗号化できる。復号の際に参加者間の通信は必要なく、効率が良い。本年度は公開条件として、日時に加えて、視聴に最も影響を与える条件である、視聴者の属性（年齢、性別など)、課金体系を考えた。これまでに、属性に基づく暗号プロトコルとして、 属性暗号 [7][8] [9] [14]が提案されており、鍵発行機関と呼ばれる信頼できる機関が属性に応じて発行する鍵がなければ復号できないように暗号化できる。復号の際に参加者間の通信は必要なく、効率が良い。しかし、鍵発行を一度でも受けると、その属性をもつものであれば、何であれ復号できてしまう。他の条件と会わせて利用するために、新たに複合的な実現方針を考える必要がある。

2.3 セキュリティ要求を満たすための設計方針の検討

検討したセキュリティに関する要求を暗号技術によって満たすための方針を検討した。暗号技術は高度な処理を必要とするため、一般にシステムが複雑となり、利便性（配信速度・配信処理）を犠牲にする。よって、有用性・実用性とのトレードオフを考慮し検討した。基本的には、昨年度の設計方針に基づく。

基本方針（公開後の不正配布抑止、購入履歴の秘匿、視聴の制御を満たすための方針）：一般的な匿名フィンガープリンティング[3] [12] を用いた配信では､視聴者は予め生成した特定情報を伏せた形で配信者に送る。配信者はコンテンツと､伏せた形の特定情報から､特定情報が埋め込まれたコンテンツを伏せた形で生成し、視聴者に送る。視聴者は自身だけがもつ情報(視聴補助情報と呼ぶ) を利用し、特定情報が埋め込まれたコンテンツを得る。この過程において、配信者が視聴者の特定情報を知ることはなく、購入履歴の秘匿が満たされる。また、コンテンツに特定情報を埋め込む位置は配信者が選ぶため、視聴者はコンテンツから特定情報を外すことはできない。よって、公開後の不正配布抑止が満たされる。

事前配信において、公開後の不正配布抑止と購入履歴の秘匿を満たすために、匿名フィンガープリンティングと同様に、配信者は特定情報が埋め込まれたコンテンツを伏せた形で生成する。そして、公開条件のうち日時を制御するために、視聴者に送る前に Timed-release 暗号[1] [5] [16] [17] により暗号化する。さらに、視聴者の属性と課金条件に基づく制御をするために、属性暗号[7][8][9][14]により暗号化する。これにより、鍵発行局の属性と課金体系に応じた鍵と、時報局が放送する公開日時の時報がなければ復号できなくなり、視聴の制御が満たされる（図 3 参照)。

公開前の不正配布抑止を満たすための方針：公開前の不正配布抑止を満たすための三つの方針を示す。

（１）**事前解除**：事前解除として、公開条件を満たす前でも配信者が暗号化コンテンツを復号できるようにする。これにより、配信者は埋め込まれた特定情報を抽出し、視聴者を特定し、不正を立証することができる。公開日時前の解除の実現には、暗号化した人であれば、公開日時前でも暗号化コンテンツを復号できるという性質をもつ Timed-release 暗号[5] を利用することで実現できる。ただし、属性暗号ではそのような

性質をもつものがないため、新たに構成する必要がある。

（2）**特定情報露呈**:特定情報露呈として、公開日時前に視聴者が暗号化コンテンツを再配布するためには、自身の特定情報を付けざるを得なくする。具体的には、公開日時に暗号化コンテンツを復号する際には、視聴補助情報と時報だけでなく特定情報もなければ復号できないように暗号化する。これにより、配信者はコンテンツから抽出しなくとも、特定情報を入手でき、不正な視聴者を特定することができる。上述したように、一般的な匿名フィンガープリンティング[3] [12] では、配信者には特定情報がわからないように伏せた形で与えられる。具体的な構成法が示されている匿名フィンガープリンティング[12] において、伏せた形

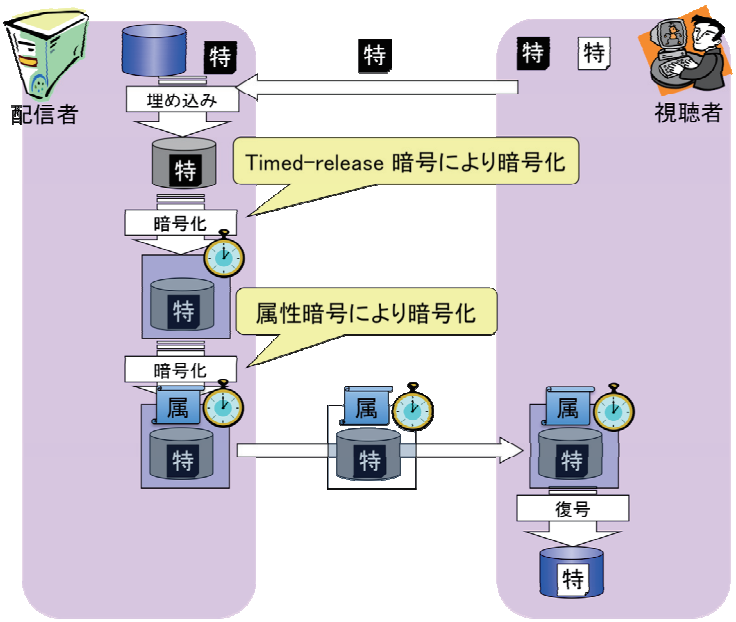

図３　基本となる設計方針

のデータを用いて、特定情報が復号鍵となるように暗号化できると考えられる。そして、この暗号化処理をTimed-release 暗号と属性暗号の暗号化処理の前に行う。よって、公開日時後に暗号化コンテンツを復号する際には、特定情報も必要となる。なお、前に行うことによって、公開日時前に特定情報を用いた復号処理は行えない。

（3）**個人鍵露呈**：個人鍵露呈として、公開日時前に暗号化コンテンツを再配布するためには、視聴者は自身の個人鍵を付けざるを得なくする。具体的には、公開日時後に暗号化コンテンツを復号する際には、時報だけでなく個人鍵もなければ復号できないように暗号化する。これにより、視聴者が不正配布をするためには、なりすましをされる可能性のある個人鍵を配布しなければならなくなり、不正配布に対する抑止力となる。個人鍵露呈の実現には、個人鍵が利用されている[5]の Timed-release 暗号か[3]の匿名フィンガープリンティングを利用すればよいと考えられる。ただし、[5] の Timed-release 暗号では匿名性を満たしていないため、購入履歴の秘匿のための仕組みが新たに必要となる。一方、[3] の匿名フィンガープリンティングでは、個人鍵は署名鍵として利用されている。よって個人鍵(署名鍵) が復号鍵となるような仕組みが新たに必要となるが、例えば、個人鍵で生成された署名を暗号化に用いることができると考えている。そこで、 特定情報露呈と同様に、この暗号化処理を Timed-release 暗号と属性暗号の暗号化処理の前に行う。

提案方針の比較：上述の三つの方針を、配信と特定の効率、不正配布に対する抑止力、一般的な事前配信への拡張性について比較した結果を表１に示す。なお、事前解除が最も自明な方針と考えられるため、事前解除を基準(普通) としている。

（1）**効率**：配信において、特定情報露呈と個人鍵露呈は、それぞれ特定情報と個人鍵がなければ復号できないように暗号化する処理が追加される。一方、事前解除はその処理が追加されないため、配信の効率が良い。ただし、暗号化処理では、大きなデータ(コンテンツ) は対称鍵暗号により暗号化され、その対称鍵を追加された処理で暗号化される。このため、暗号化の対象となるのは対称鍵である。鍵のサイズはコンテンツのサイズと比べるとごくわずかであり、効率に大きな差はないと考えられる。特定において、事前解除はコンテンツから情報を抽出する必要がある。一方、特定情報露呈と個人鍵露呈は、コンテンツに付けられている情報から視聴者を特定できる。そのため、特定情報露呈と個人鍵露呈は特定の効率が良いと考えられる。

（2）**抑止力**：匿名フィンガープリンティングにおける特定情報の抽出の処理には誤りが含まれる可能性がある(ただし，十分小さくできる)。一方、特定情報露呈と個人鍵露呈では、特定情報、もしくは、個人鍵は不正配布コンテンツに付けられているため、抽出する必要がなく誤りが含まれない。このため、特定情報露呈と個人鍵露呈は特定の信頼性が高く、抑止力が強いと考えられる。また、個人鍵はなりすましを可能にする情報であるため、視聴者にとって特定情報よりも配布するリスクが高い。このため、個人鍵露呈は特定情報露呈より、不正配布に対する抑止力が強いと考えられる。よって、個人鍵露呈が最も抑止力が強いと考えられる。

（3）**拡張性**: 事前解除は Timed-release 暗号と属性暗号に依存する方針であるが、特定情報露呈と個人鍵露呈は依存しない。つまり、公開の条件の今後のさらなる拡張が容易と考えられる。このため、特定情報露

呈と個人情報露呈は拡張性が高い。

表１　提案方針の比較

	効率		抑止力	拡張性
	配信	特定		
事前解除	普通	普通	普通	普通
特定情報露呈	少し悪い	良い	強い	高い
個人鍵露呈	少し悪い	良い	最強	高い

以上より、抑止力と拡張性という有用性の観点では特定情報露呈と個人鍵露呈が優れており、効率という実用性の観点では事前解除が優れている。

2.4 セキュリティ要求を満たす暗号技術の創出

考案した三つの方針で実現するためには、事前解除が可能な属性暗号と、コンテンツに付加的な情報（透かし）を埋めこみ、後に抽出するための基盤技術である、電子透かし法を開発することが必須となる。

事前解除が可能な属性暗号：属性暗号では、強固な秘匿性を保証するために暗号化ごとに乱数が生成され利用されている。なお、乱数は暗号化の後に破棄され、復号には利用されない。復号では、属性に対応する秘密鍵を利用する。既存の属性暗号を解析した結果、秘密鍵がなくとも乱数があれば復号できるようになっていることが分かった。よって、事前解除を可能とするために、本来は破棄する乱数を事前解除鍵として利用した。乱数は暗号化の効率を上げるため、小さなサイズとなる。また、乱数を用いた復号は、秘密鍵を用いた復号の途中処理を省くことができ、効率が良いことを確かめることができた。これにより、属性暗号の事前解除を効率よく実現できた。

暗号データへの電子透かし：電子透かしでは、透かしを埋め込む際に、埋込先のコンテンツを微少量だけ変更する。埋込先のコンテンツとして画像・音声・テキストは対象としたものはあったが、暗号データ（鍵、暗号文、署名）を対象としたものは存在しなかった。その主な要因として、暗号データの「微小な」変更の困難さが挙げられる。暗号データは利用する数学的な構造に基づき非常に注意して設計される。その結果、1ビットでも変更されたデータは改ざんとしてみなされ、本来の機能を果たさない。例えば、暗号文であれば復号できず、署名であれば妥当でないと判定される。この問題を解決するために、近年の暗号技術で用いられている数学的な構造、楕円曲線とペアリングに着目する。その数学的な構造は今世紀に暗号技術分野において劇的な発展を可能としたものであり、非常に豊かな性質をもつ。暗号データへの電子透かしの設計の際は、対象とする暗号データの方式は変えること無く、基となる数学的構造のパラメータを適切に選択することによって、透かしを埋め込むことが可能な冗長性をもたせた。これにより、暗号データへの初めての電子透かしを実現することができた。さらに、電子透かしは秘密情報が無い限り除去できないことを保証できている。一方で、誰でも埋め込まれている透かしが確認できるようになっている。このような公開型の透かし確認を実現したのも世界初である。設計では、図４に示すように、暗号データと透かしをベクトルとみなし、透かしの埋め込みはベクトルの加算、透かしの除去はベクトル分解に対応付けている。透かし除去の困難性はベクトル分解の困難さを根拠としているため、利用した数学的構造において、ベクトル分解問題が困難であることを証明した。

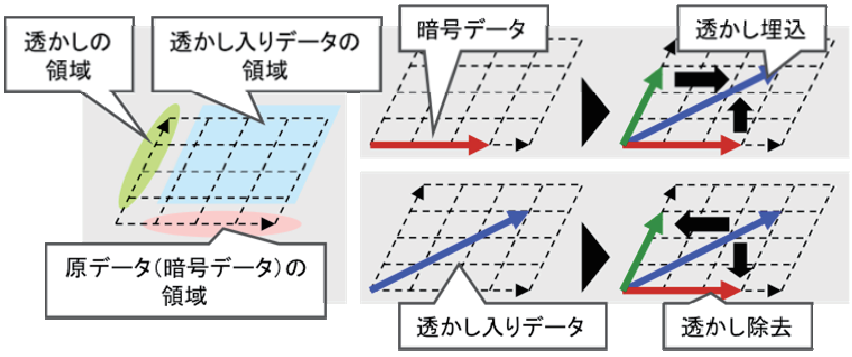

図４　暗号データに対する透かし埋込と秘密情報を用いた透かし除去

2.5 暗号技術を利用した事前配信プロトコルの設計

開発した属性暗号と電子透かし法を基に、考案した三つの方針それぞれに対してプロトコルを設計した。

（1）**事前解除に基づく方式の設計**：方針の考案の際に述べたように、最も効率の良い[3],[12]の匿名フィンガープリンティングと[5]の Timed-release 暗号、そして新たに設計した事前解除が可能な属性暗号を組み合わせることで構成した。

（2）**特定情報露呈に基づく方式の設計**：最も効率の良い匿名フィンガープリンティングのうち、具体的な構成法が示されている[12]の方式を利用して構成した。文献[9] の匿名フィンガープリンティングは、二重使用者の特定が可能な電子コインシステム[2] に基づく。このシステムでは、電子コインの一度目の使用では使用者は特定されないが、複製し、二度目の使用をした場合は特定される。文献[12] の匿名フィンガープリンティングでは、視聴者の登録がコインを引き出すことにあたる。配信では、視聴者が配信者にそのコインを渡し、一度目の使用を行う。そして、コインの二度目の使用を開始するが、使用に関する情報は配信者に渡されず、特定情報として、コンテンツに埋め込まれる。この時、配信者は埋め込まれた特定情報を得られない。ただし、再配布コンテンツが見つかった際、配信者は埋め込まれた特定情報を二度目の使用の情報として用いることができる。これによって、コインを二重使用した視聴者、すなわち、再配布した視聴者を特定できる。ここで、コインが特定情報の伏せた形となっている。本研究では、コインと特定情報の間の関係から、コインを公開暗号化鍵、特定情報を秘密復号鍵とした暗号化方式を構成し、特定情報露呈を実現した。

（3）**個人鍵露呈に基づく方式の設計**：最も効率の良い匿名フィンガープリンティングのうち、個人鍵を用いている [3]の方式を利用して構成した。文献[3]のグループ署名を用いた匿名フィンガープリンティングの配信では、視聴者から配信者へのリクエストはグループ署名における開示機関の公開鍵、視聴者のグループ署名、開示機関の秘密鍵のコミットメントからなる。この開示機関の鍵ペアは視聴者により配信ごとに毎回生成されている。そして、開示機関の秘密鍵は特定情報としてコンテンツに埋め込まれ、視聴者が不正配布したときに、配信者が視聴者をグループ署名の署名者として特定するために利用される。本研究では、グループ署名と個人鍵の関係から、グループ署名を公開暗号化鍵、個人鍵を復号鍵とする暗号化方式を構成し、個人鍵露呈を実現した。

2.6 大規模な配信環境を想定した有用性・実用性の評価

設計したプロトコルの有用性・実用性の評価として、現実的な映画の事前配信状況を想定した上で、利用した暗号技術のパラメータ設定を行い、プロトコルの効率と信頼性を評価した。

効率：効率として、通信量、計算量、メモリ量の増加量を評価した。その際、提案した方式のうち、もっとも自明な方針に従う事前解除方式を基準として、特定情報露呈方式と個人鍵露呈方式における増加量を評価した。増加したのは、配信時の通信量と計算量、視聴者のメモリ量である。まず、通信量の増加は約 400Byte、メモリ量の増加は約 450Byte と、コンテンツのサイズと比べればごくわずかである。また、計算量の増加もごくわずかなサイズに対する暗号化、復号の処理を 1 回だけですむ。よって、両方式は効率の良い事前解除方式から効率をほとんど落とすことなく、それぞれの機能を実現している。なお、特定情報露呈方式と個人鍵露呈方式を比較した場合、それぞれの機能の実現による増加量は同じだが、それ以外については用いる匿名フィンガープリンティングの効率で決まる。通信量、メモリ量については、個人鍵露呈方式の方が特定情報露呈方式より多くなってしまうが、コンテンツのサイズと比べればごくわずかである。また、計算量の差もごくわずかである。すなわち、個人鍵露呈方式は特定情報露呈方式とほぼ同じ効率で，強い不正配布抑止力を実現している。

信頼性：信頼性として提案した三つの方式の安全性を評価した。まず事前解除方式の安全性は、利用する匿名フィンガープリンティングと事前解除が可能な Timed-release 暗号と属性暗号の安全性に帰着できる。帰着先の安全性は十分強いため、事前解除方式は十分な安全性を保証する。次に、特定情報露呈方式と個人鍵露呈方式の安全性は、利用する匿名フィンガープリンティングと事前解除が可能な Timed-release 暗号と属性暗号の安全性に加えて、一般化 ElGamal 暗号の安全性に帰着できた。この暗号の安全性の仮定は最も妥当な仮定の一つであり、近年の多くの暗号プロトコルで安全性の根拠とされている。よって、特定情報露呈方式と個人鍵露呈方式も十分な安全性を保証する。

以上より、プロトコルが大規模な配信規模において十分利用可能な効率と信頼性をもつことを確認できた。

3 研究のまとめ

本研究ではデジタルシネマのような公開日時が指定されたコンテンツの事前配信サービスにおいて、高い安全性と利便性を実現するために、まずセキュリティに関する要求を明確化し、それらを満たすための方針を考案した。そして、必要な基盤技術を開発し、暗号プロトコルを提案し、効率と信頼性を評価した。通常のコンテンツ配信の要求との違いは、視聴の制御と公開日時前の不正配布抑止である。視聴の制御では、公開日時だけでなく、視聴者の属性や課金状況に応じて視聴を制御できるようになっており、デジタルシネマのサービスの多様化に貢献できる。一方、公開日時前の不正配布抑止は、三つの方針（事前解除、特定情報露呈、個人鍵露呈）に基づいている。事前解除は配信の効率が良く、特定情報露呈と個人鍵露呈は特定の効率が良く不正配布に対する抑止力が強い。さらに、不正配布抑止のための基盤技術として、事前解除が可能な属性暗号と暗号データに対する電子透かし法を開発した。そして、三つの設計方針それぞれに対して暗号プロトコルを提案し、現実的な映画の事前配信状況における効率と信頼性を評価し、十分利用可能であることを確認した。よって、本研究の結果はデジタルシネマという新しいサービスの普及と発展に大きく寄与するといえる。

【参考文献】

[1] I. F. Blake and A. C-F. Chan, “Scalable, Server-Passive, User-Anonymous Timed Release Public Key Encryption from Bilinear Pairing,” Proc. ICDCS2005, pp.504–513, 2005.

[2] S. Brands, “Untraceable Off-line Cash in Wallet with Observers,” Crypto’93, LNCS773, pp.302–318, 1994.

[3] J. Camenisch, “Efficient Anonymous Fingerprinting with Group Signatures,” ASIACRYPT2000, LNCS1976, pp.415–428, 2000.

[4] R.Canetti,“Universally Composable Security: A New Paradigm for Cryptographic Protocols,”Cryptology ePrint Archive, Report 2000/067, 2000. FOCS 2001, pp.136- 145, 2001.

[5] A. W. Dent and Q Tang “Revisiting the Security Model for Timed-Release Encryption with Pre-Open Capability” ISC2007, LNCS4779, pp.158–174, 2007.

[6] Y. Frankel, Y. Tsiounis, and M. Yung, “Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash,” ASIACRYPT’96, LNCS1163, pp.286–300, 1996.

[7] V. Goyal , A. Jain, O. Pandey , and A. Sahai . Bounded ciphertext policy attribute based encryption. In ICALP, 2008.

[8] J.Katz, A.Sahai, and B. Waters. “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products,” EUROCRYPT2008, LNCS 4965, pp.146-162, 2008.

[9] J.Li, K.Ren, B.Zhu, and Z.Wan, ″Privacy-aware Attribute-based Encryption with User Accountability ,″ ISC 2009, Pisa, Italy, Sept. 7-9, 2009.

[10] B. Pfitzmann and M. Shunter, “Asymmetric Fingerprinting,” EUROCRYPT’96, LNCS1070, pp.84–95, 1996.

[11] B. Pfitzman and A. -R. Sadeghi, “Coin-based Anonymous Fingerprinting,” EUROCRYPT’99, LNCS1592, pp.150–164, 1999.

[12] B. Pfitzman and A. -R. Sadeghi, “Anonymous Fingerprinting with Direct Non-Repudiation,” ASIACRYPT2000, LNCS1976, pp.401–414, 2000.

[13] R. L. Rivest, A. Shamir, and D. A. Wagner, “Time lock puzzles and timed release Crypto,” In MIT/LCS/TR-684, 1996.

[14] A. Sahai and B. Waters, “Fuzzy Identity-based Encryption,” EUROCRYPT2005, LNCS 3494, pp.457-473, 2005.

[15] M. Yoshida and T. Fujiwara, “Unforgeability Problem for a Class of Protocols Using Signatures,” IEICE Tech. Rep., ISEC98-15, vol.98, no.227, pp.45-52, 1998.

[16] M. Yoshida, S. Mitsunari, and T. Fujiwara, “Time-Capsule Encryption,” IEICE Technical Report, ISEC2004-98, pp.1–5, 2004.

[17] M. Yoshida, S. Mitsunari, and T. Fujiwara, “A Timed-Release Key Management Scheme for Backward Recovery,” ICISC2005, LNCS3935, pp.1-15, 2005.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
公理的安全性の枠組みにおける汎用的結合可能な相互認証と鍵交換の記号的安全性	日本応用数理学会論文誌, 第 20 巻,第 1 号, pp.147-150.	2010. 8
汎用的結合可能な相互認証に対する記号的識別不可能性を用いた記号的基準	2010 年暗号と情報セキュリティシンポジウム予稿集, 2C4-1.	2010. 1
Watermarking Cryptographic Data	The Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2009), A02-02 (CD-ROM) (2009-09).	2009. 9
Improving Capability of Locating Tampered Pixels of Statistical Fragile Watermarking	The 8th International Workshop on Digital Watermarking (IWDW 2009), LNCS 5703, pp.279-293.	2009. 8