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

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、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、セキュリティに関する要求を満たすことを目的とする。コンテンツ配信における一般的な要求として、視聴者のプライバシーの保護と、公開後に視聴可能となったコンテンツの不正配布抑止が挙げられる。本研究ではさらに、事前配信特有の要求を検討する。必須の要求として視聴の制御が挙げられるが、これ以外にも、視聴者のプライバシーやコンテンツの不正配布に関するセキュリティを事前配信の状況に応じて検討する。そして、それらの要求を全て満たすためのセキュリティ技術を確立し、プロトコルを設計する。また、大規模な配信環境を想定し、有用性・実用性を評価する。

2 研究の成果

2.1 事前配信において満たすべきセキュリティ要求の明確化

公開日時よりも前にコンテンツを配信することによって生じるセキュリティに関する要求を検討した。セキュリティに関する要求として､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が考えられる。

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] [8] [9] 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（視聴の制御、公開前の不正配布抑止）：事前配信特有の要求として自明なものは視聴の制御である。視聴者がコンテンツを事前に受け取ったとしても、公開日時前は視聴できないが、公開日時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。これまでに、日時に基づく暗号プロトコルとして、Timed-release 暗号(あるいはタイムカプセル暗号) [1] [5] [10] [11] [12] が提案されている。特に、[1] [5] [11] [12] 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。さらに、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、新たに公開前の不正配布抑止の実現方針を考える必要がある。

2.2 セキュリティ要求を満たすための複数かつ多角的な方針の考案

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。

コンテンツ配信における一般的な要求は、匿名フィンガープリンティングと同様に満たすことができると考えられる。よって、本研究では事前配信特有の要求も満たす匿名フィンガープリンティング、すなわち、コンテンツ事前配信のための匿名フィンガープリンティングを実現することを考えた。視聴の制御は日時に基づくため、[1] [5] [11] [12] の Timed-release 暗号の方針に従う。その上で，公開前の不正配布抑止を満たすための実現方針を三つ提案した。

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] [9] を用いた配信では、図 1 に示すように、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。ただし、図 2 に示すように、視聴時刻の制御を満たすために、視聴者に送る前に Timed-release 暗号[1] [5] [11] [12] により暗号化する。これにより、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、視聴時刻の制御が満たされる。

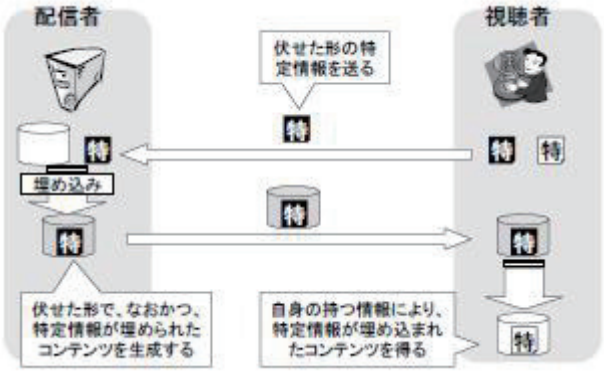

図 1　匿名フィンガープリンティング

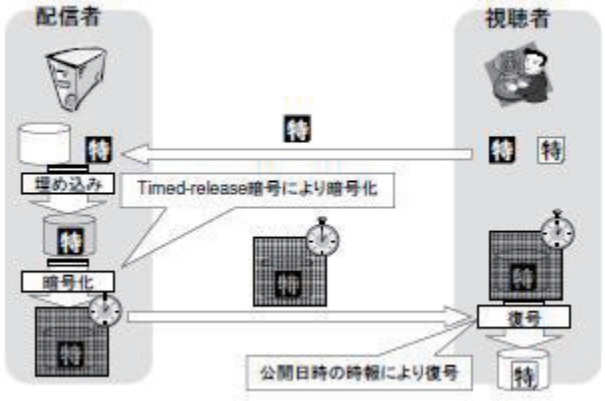

図 2　公開前の不正配布抑止、購入履歴の秘匿、視聴の制御を満たすための基本方針

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、公開日時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。事前解除の実現には、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。

（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] [9] 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[9] において、伏せた形のデータを用いて、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 暗号の暗号化処理の前に行う(図 3 参照) 。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 暗号の暗号化処理の前に行う(図 4 参照) 。

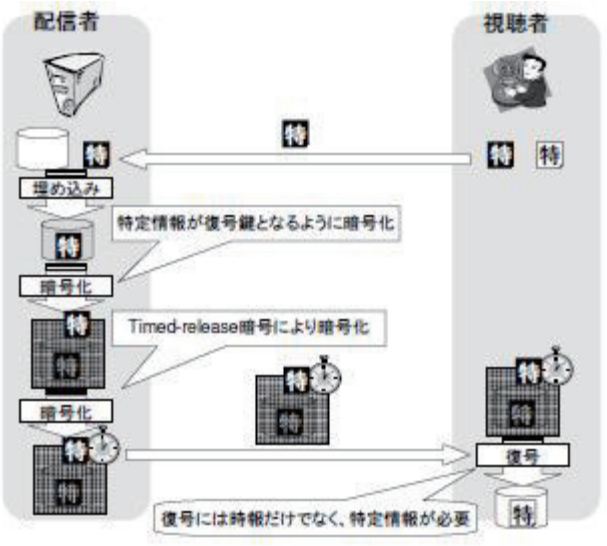

図 3　特定情報露呈

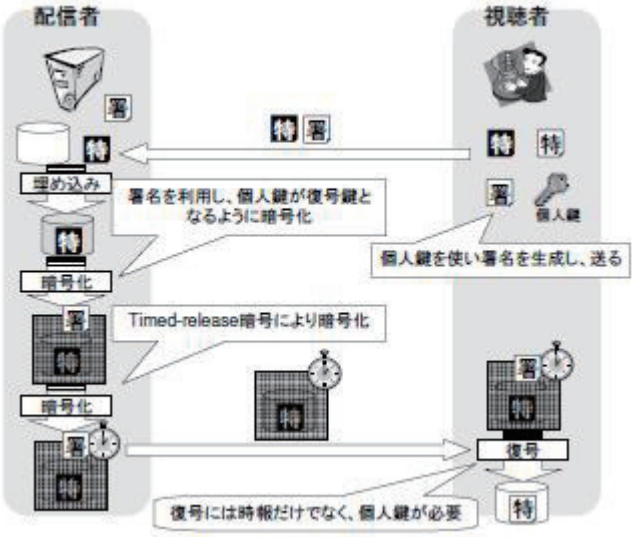

図 4　個人鍵露呈

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、公開の条件が、時刻を含めた一般的な条件である事前配信への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。

2.3 考案方針を実現するための基盤となる暗号技術の創出

考案した三つの方針で実現するためには、コンテンツに情報を埋めこみ、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。取り出した情報に誤りがあった場合、不正配布元の誤認につながり、サービス全体の信用を落とすこととなる。よって、誤り確率が最小であることを理論的に保証する最適な電子透かし法の開発を行った。

電子透かし法の埋め込み先・埋め込み法には様々なものがある。透かしの埋め込み先としては，輝度値などの画素空間と DCT 係数・DWT 係数などの周波数空間がある。また、埋め込み法の種類としては、加法埋め込み、乗法埋め込み、非線形埋め込みがある。本研究では、より一般的な埋め込み先である周波数空間、より効率のよい加法埋め込みを対象とした。周波数空間のうち DWT 係数は他の周波数空間に比べて埋め込みによる画質の劣化が小さく、異なる攻撃に対しても柔軟に対応できるという点で電子透かし法に適していることが知られている。そこで、DWT 係数を埋め込み先として選んだ。一方、加法埋め込みに従う代表的な方式としてパッチワーク法とランダム透かし法が挙げられるが、従来研究ではいずれの方式が良いかを比較していない。そこで、本研究では両方式について、最適な抽出法を仮説検定に基づき設計し、その誤り確率を理論的・実験的に比較した。その結果、ランダム透かし法の誤り確率が小さいことが確認できた。そこで、埋め込み法としてランダム透かし法を選び、最適な電子透かし法を設計した。

2.4 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、[5]の Timed-release 暗号を最も効率の良い[3],[9]の匿名フィンガープリンティングと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[9]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[9] 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。

2.5 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、提案した三つの方式のうち、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１回ですむ。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、視聴時刻の制御と公開日時前の不正配布抑止も満たすことである。本研究では、視聴時刻の制御を満たすために、Timed-release 暗号を利用した。一方、公開日時前の不正配布抑止を満たすための方針として三つ（事前解除、特定情報露呈、個人鍵露呈）を提案し比較した。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、最適な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] D. Chaum, J. H. Evertse, and J. van de Graaf, “An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations,” EUROCRYPT’87, LNCS304, pp. 127–141, 1984.
[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] B. Pfitzmann and M. Shunter, “Asymmetric Fingerprinting,” EUROCRYPT’96, LNCS1070, pp. 84–95, 1996.
[8] B. Pfitzman and A. -R. Sadeghi, “Coin-based Anonymous Fingerprinting,” EUROCRYPT’99, LNCS1592, pp. 150–164, 1999.
[9] B. Pfitzman and A. -R. Sadeghi, “Anonymous Fingerprinting with Direct Non-Repudiation,” ASIACRYPT2000, LNCS1976, pp. 401–414, 2000.
[10] R. L. Rivest, A. Shamir, and D. A. Wagner, “Time lock puzzles and timed release Crypto,” In MIT/LCS/TR-684, 1996.
[11] M. Yoshida, S. Mitsunari, and T. Fujiwara, “Time-Capsule Encryption,” IEICE Technical Report, ISEC2004-98, pp. 1–5, 2004.
[12] 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
Expiration-dated Fingerprinting	Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008), 147-150	2008. 8
Anonymous Fingerprinting for Predelivery of Contents	Proceedings of the 11th International Conference on Information Security and Cryptography (ICISC2008), LNCS 5461, 134-151	2008. 12
DWT 係数に対する加法電子透かし法とパッチワーク法の性能比較	2009 年暗号と情報セキュリティシンポジウム予稿集, 1D1-5	2009. 1
コンテンツ事前配信における不正配布抑止力の強い匿名フィンガープリンティング	2009 年暗号と情報セキュリティシンポジウム予稿集, 1B2-3	2009. 1