コンテンツ配信における不正者追跡技術

Traitor Tracing in Content Distribution

松下　達之　吉田　琢也　秋山　浩一郎　今井　秀樹
■ MATSUSHITA Tatsuyuki　■ YOSHIDA Takuya　■ AKIYAMA Koichiro　■ IMAI Hideki

放送型有料コンテンツ配信では，コンテンツ配信者は音楽や映画などのデジタルコンテンツを暗号化して同報配信し，サービス加入者はあらかじめ与えられた復号鍵を用いて暗号化コンテンツを復号し視聴する。このようなコンテンツ配信における不正行為として，悪意のある加入者が復号鍵を非加入者へ横流しすることにより，非加入者が海賊版デコーダを用いて不正に視聴することが挙げられる。この不正行為に対する抑止力として，不正者追跡技術が研究されている。

東芝は，中央大学及び独立行政法人 産業技術総合研究所（以下，産総研と略記）と共同で，送信オーバヘッド(注1)を抑えつつ，不正者の追跡を妨げようとする巧妙な海賊版デコーダを不正者が作成したとしても，不正者を特定できる方式を開発した。

In content distribution, a broadcaster encrypts and then broadcasts digital contents (e.g., movies) to subscribers. The subscribers decrypt the encrypted contents and play them using their decryption devices (decoders), which contain their decryption keys. In this application, malicious subscribers (known as "traitors") may redistribute their decryption keys to nonsubscribers. This allows nonsubscribers with a pirate decoder to gain illegal access to the content. Traitor tracing has been extensively studied as a deterrent to such piracy.

Toshiba, jointly with Chuo University and the National Institute of Advanced Industrial Science and Technology, has developed a traitor tracing scheme in which the pirate decoder can be traced back to at least one of the traitors, even if the pirate decoder does not respond any further when it detects itself being examined, while maintaining the transmission overhead at an efficient level.

1　まえがき

近年，情報のデジタル化に伴い，様々な形態のデジタルコンテンツの配信が盛んに行われている。それとともに，コンテンツに対する著作権侵害が深刻な問題となっている。コンテンツに対する著作権が保護されていない場合，コンテンツの制作者や配信者は大きな損害を被ることになる。このことは，魅力あるコンテンツの制作や流通の妨げとなり，その結果，消費者が魅力あるコンテンツを享受できなくなってしまう。

このような問題を解決するため，東芝は，中央大学及び産総研と共同で，効率的な送信オーバヘッドと高い追跡能力を両立させた不正者追跡方式を開発した。

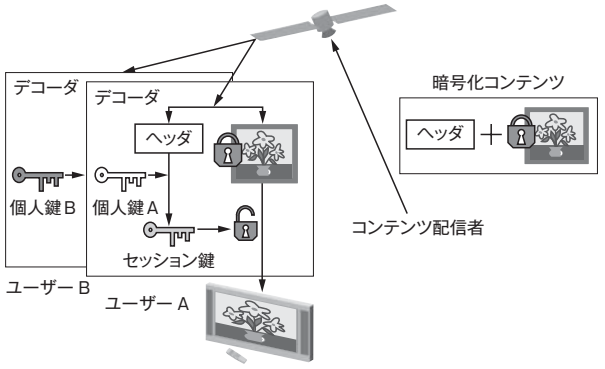

図1. コンテンツ配信システム — ユーザーは，個人鍵を用いてヘッダを復号し，その復号結果であるセッション鍵を用いて暗号化コンテンツを復号する。
Content distribution system

2　コンテンツ配信と不正行為

2.1　コンテンツ配信システム

コンテンツ配信の概要とその不正行為について述べる。

コンテンツ配信システムのモデルを**図1**に示す。コンテンツ配信者は，各加入者（以下，ユーザーと記す）に固有の復号鍵である個人鍵をあらかじめ与えておく。個人鍵はデコーダ，例えば，セットトップボックス(注2)などに格納される。コンテンツをユーザーにだけ利用可能にさせるため，コンテンツ配信者は，コンテンツを暗号化して配信する。暗号化の典型的な例として，まずコンテンツを暗号化し，次にその際に用いた暗号化鍵（セッション鍵）を各ユーザーの個人鍵だけで復号できるように配信用鍵を用いて暗号化する，という2段階の暗号化がある。この場合，セッション鍵を暗号化したもの（ヘッダ）が限定受信情報となっている。コンテンツ配信者は，ヘッダと暗号化されたコンテンツを同報配信する。ユーザーは，ヘッダ

（注1）　送信処理効率を低下させる付帯負荷で，ここでは暗号化通信を行うために帯域に掛かる負荷。
（注2）　放送信号を受信して既存のテレビで視聴可能な信号に変換する装置。

をデコーダに入力してセッション鍵を復号し，更にセッション鍵を用いて暗号化されたコンテンツを復号する。このようなシステムの具体的な応用先として，ペイパービューテレビ(注3)やパッケージメディアによるコンテンツ配布などのアプリケーションが挙げられる。

2.2 想定される不正行為

このようなシステムにおいては，悪意のあるユーザー（以下，不正者と記す）が自分の個人鍵を横流しすることにより，海賊版デコーダを構成して非ユーザーにコンテンツを不正に利用させることが考えられる。この不正行為への対策として，不正者追跡技術[1]が研究されている。

海賊版デコーダが出現した場合に，その作成に加担した不正者が特定されるため，不正者追跡方式の存在は不正行為への抑止力となる。不正者が一人の場合，個人鍵は各ユーザーに固有であるので，入手した海賊版デコーダの中身を調べることにより不正者を特定できるが，複数の不正者が結託する場合，このような単純な方法では不正者の特定は困難となる。更に，海賊版デコーダが耐タンパ(注4)化され，内部解析が困難な場合も想定される。この場合，海賊版デコーダへの入出力だけを観測することにより不正者を特定する，ブラックボックス追跡が必要となる。ブラックボックス追跡は，海賊版デコーダに埋め込まれた個人鍵を直接取り出す必要がなく，海賊版デコーダの実装形態に制限を設けないという意味で，より強力な不正者追跡が可能となり，望ましい性質である。

その他の不正行為として，不正者が復号したコンテンツ自身を再配布することが挙げられる。この対策としては電子透かし技術[2]が知られている。一見，海賊版デコーダの問題は対策を講じるほどではないと感じられるかもしれないが，例えば，ケーブルテレビにおいて深刻な問題となり，業界の被害額は数千万円に上るとも言われている[3]。ここでは，海賊版デコーダ問題の対抗策である不正者追跡技術について述べる。

3 不正者追跡技術

不正者追跡技術の概要と従来方式について述べる。

3.1 概要

不正者追跡の流れを**図2**に示す。まず，海賊版デコーダを入手する。例えば，営利目的の場合など，海賊版デコーダは大量に密売されるので，その入手はそれほど難しくないと思われる。次に，入手した海賊版デコーダに対して，次に述べる検査を繰り返すことにより不正者を特定する。

ここで説明する追跡方法は，海賊版デコーダをブラックボックスとして扱い，不正者を特定するものである（**図3**）。初めに，容疑者を想定し，その容疑者だけが復号不可能で，残りのユーザーは復号可能なヘッダを作成し，海賊版デコーダに入力する。海賊版デコーダがそのヘッダを復号した場合は追跡すべき不正者が容疑者集合に含まれていない，逆にヘッダを復号しなかった場合は容疑者集合に含まれている，ということがわかる。この検査をすべての容疑者集合に対して行うことにより不正者が特定される。例えば，ユーザー1及び2だけが復号不可能なヘッダを入力したときに海賊版デコーダが正しい出力をし，ユーザー1，2，及び3だけが復号不可能なヘッダを入力したときに海賊版デコーダが誤った出力をした場合，ユーザー3が不正者であるとわかる。

ブラックボックス追跡後，特定された不正者により横流しされた個人鍵，つまり海賊版デコーダの無効化を行う。ここでは，大量に出回っていると予想される海賊版デコーダを回収する必要はなく，ヘッダの構成法を工夫することにより，すべての特定された海賊版デコーダを排除できる。

3.2 関連する従来方式

不正者追跡方式はその構成により分類すると，組合せ論的な構成[1]，木構造を用いた構成[4]，代数的な構成[5], [6], [7]，ペアリングを用いた構成[8], [9]，又はそれらの組合せが挙げられる。通常，組合せ論的な構成より代数的な構成のほうがヘッダサイズや個人鍵サイズの観点において優れている。しかし，ユーザー側の計算負荷など，ほかの観点から見ると優劣が逆転す

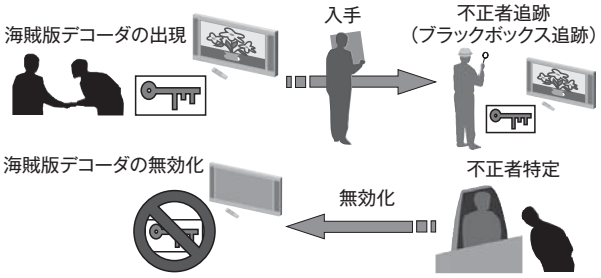

図2. 不正者追跡の流れ — 追跡者は，入手した海賊版デコーダを検査して不正者を特定する。

General flow of traitor tracing

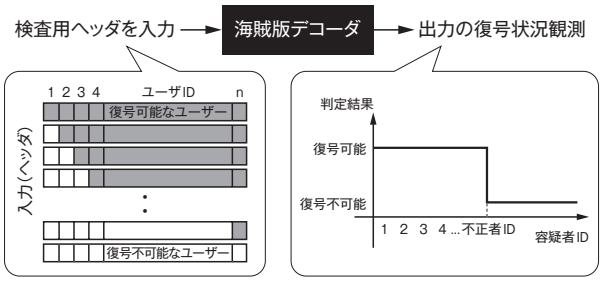

図3. ブラックボックス追跡 — 復号不可能であるユーザーを一人ずつ増やして検査する。

Black-box tracing

（注3） 視聴した分だけ料金を支払うテレビ放送システム。
（注4） 内部解析や改変に対する防御機能。

る場合があり，どの構成が最良であるかは一概には言えない。開発した方式は，代数的な構成と木構造を用いた構成の組合せである。

配信用鍵の公開可能性はシステム拡張性に影響する。配信用鍵が秘密である，言い換えるとコンテンツ配信用ヘッダの作成に秘密情報が必要である場合，同一システムを複数のコンテンツ配信者が利用する際には，配信者間でその秘密を共有する必要があり，配信者数が増えるにつれて秘密漏えいのリスクが高まる。一方，配信用鍵を公開してもシステムの安全性に影響を与えない，言いかえるとコンテンツ配信用ヘッダ作成に秘密情報が不要である場合，そのようなリスクは生じず，配信者側の拡張性があり望ましい。配信用鍵が秘密である方式[1), (4)]においても，ヘッダ生成に用いる共通鍵暗号を公開鍵暗号に置き換えることで，配信用鍵を公開できる。配信用鍵が公開である方式のなかで，検査用ヘッダの作成には秘密情報を必要とする方式[9), (10)]もある。

それに対し，検査用ヘッダ作成にも秘密情報が不要な方式[8)]が提案されている。ただし，この方式では不正者を特定するために信頼できる第三者による秘密の処理が必要である。検査用ヘッダ作成に秘密情報が不要であることは，複数の追跡者に追跡を委託できるため，追跡者側の拡張性があり望ましい。開発した方式では，コンテンツ配信用ヘッダ，検査用ヘッダともに公開情報だけから作成できる。

3.3 従来方式の問題点

ブラックボックス追跡を行うにあたって，検査用ヘッダの入力から追跡の意図を読み取って不正者の割出しを妨げようとする海賊版デコーダを想定する。このような海賊版デコーダに対するブラックボックス追跡方式として，開発した方式のほかに従来方式[7), (9), (11)]が知られている。

文献(7)の方式は，ヘッダサイズがk（kは最大結託人数を表す）にだけ比例し，個人鍵サイズが一定である非常に効率的な方式である。しかし，前述の巧妙な海賊版デコーダを想定するとき，この方式では，何らかの方法により事前に容疑者がk人以下に絞り込まれていなければ不正者を特定できないという問題がある。文献(11)の方式では，この絞込みが不要で，かつヘッダサイズを$O(n^{1/2})$とすることが可能である。ここで，Oはオーダーを，nは全ユーザー数を表す。しかし，不正者を正しく特定する確率とヘッダサイズがトレードオフの関係にあるという問題がある。また，文献(9)の方式では，前述の両方の問題を解決し，ヘッダサイズが$O(n^{1/2})$であるブラックボックス追跡方式が示されている。この方式は，結託人数に依らず安全性が保たれ，また，セッション鍵の復号に要する計算負荷が一定であるという優れた性能を持っている。

開発した方式においても，前述の両問題を解決している。文献(9)の方式との違いは，k人以下の結託に対して安全性を保ち，ヘッダサイズを$O(k+\log(n/k))$に削減した点である。

4 開発した不正者追跡方式

当社は，中央大学及び産総研と共同で，公開鍵暗号技術をベースにした不正者追跡方式の開発を行った[12)]。その方式の概要と，安全性及び効率性について以下に述べる。

4.1 概要

開発したブラックボックス追跡方式の概要を**図4**に示し，以下に述べる。

(1) 鍵生成　信頼できる第三者が個人鍵を生成し，各ユーザーへ秘密に配布する。個人鍵はデコーダに格納される。開発した方式ではユーザー集合を木構造化している（**図5**）。ユーザー部分集合をリーフ（葉）とし，各ノード（節）に鍵生成多項式を割り当て，リーフ，親ノード，及び祖先ノードに割り当てられた鍵生成多項式にユーザーID（IDentification）を代入して得られる値を，個人鍵としてそれぞれユーザーに与える。

(2) 暗号化　コンテンツ配信者は，まずセッション鍵を暗号化し，次にヘッダを同報配信する。一般に，コンテンツ暗号化には共通鍵暗号を単純に用いるため，不正者追

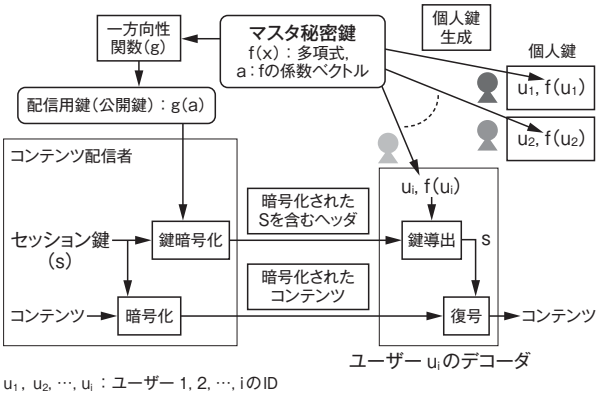

図4．開発方式の概要 — マスタ秘密鍵である鍵生成多項式を生成し，それに基づいて公開鍵と各ユーザーの個人鍵を割り当てる。この公開鍵を用いて作成されたヘッダは，各ユーザーの個人鍵で復号可能となる。

Outline of newly developed scheme for traitor tracing

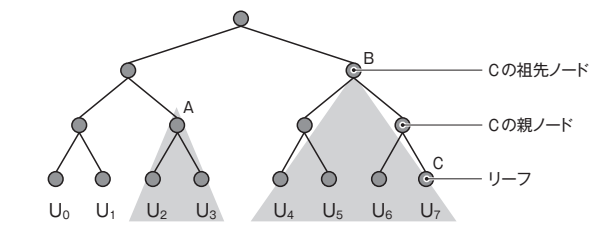

図5．木構造の例 — U_0, …, U_7は全ユーザー集合を分割した部分集合であり，木構造に基づいてヘッダを構成することにより，ヘッダサイズの削減が達成される。

Tree-structured chart of client aggregation

跡方式を考える際にはヘッダの構成に焦点が当てられる。図5に示すように，集合U_2とU_3に属するユーザーだけが復号できるヘッダを作成する際にはノードAに割り当てた鍵生成多項式に対応する公開鍵を用い，集合U_4からU_7に属するユーザーへのヘッダ作成にはノードBに対応する公開鍵を用いる，といった具合にヘッダを作成する。

(3) 復号　　ユーザー側は，受信したヘッダをデコーダへ入力し，セッション鍵を計算する。得られたセッション鍵を用いて暗号化コンテンツを復号する。

(4) ブラックボックス追跡　　海賊版デコーダが押収されたとする。追跡者は，検査用ヘッダを海賊版デコーダに入力し，正しく復号されたか否かを観測する。その出力結果に基づき，不正者を特定する。

4.2 安全性

開発した方式は，計算量的な仮定（Decision Diffie-Hellman問題の困難性）の下での数学的な証明により，以下に述べる安全性が保証される。

(1) セッション鍵の秘匿性　　ヘッダが与えられたとき，非ユーザー（盗聴者）がそのヘッダに対応するセッション鍵を計算できる確率は非常に低い。

(2) ブラックボックス追跡の可能性　　たかだかk人の不正者によって海賊版デコーダが作成されたとき，海賊版デコーダの入出力を観測することだけで，少なくとも一人の不正者を非常に高い確率で正しく特定できる。

4.3 効率性

開発した方式は，**表1**に示すように，文献(9)の方式と大差のない個人鍵サイズで，ヘッダサイズの削減が達成されている。

一方，この方式では，セッション鍵の復号に要する計算負荷が最大結託人数に比例してしまう。これは，パソコンなど計算能力の高い機器では問題ないが，民生機器など比較的計算能力の低い機器に対して，更に効率よくする必要があると考える。

表1. 全ユーザー数 (n)=10^6の場合のヘッダサイズ削減例

Reduction in header size by newly developed method in case of n = 10^6 compared with conventional method

最大結託人数	開発方式（192ビットだ円曲線を想定）		Boneh-Sahai-Waters方式[9]（ペアリング計算可能な1,024ビット巡回群を想定）	
	ヘッダサイズ（Kバイト）	個人鍵サイズ（バイト）	ヘッダサイズ（Mバイト）	個人鍵サイズ（バイト）
k=100	19.6	318.9	1.3	256
k=500	94.5	263.2	1.3	256
k=1,000	188.1	239.2	1.3	256

5 あとがき

効率的な送信オーバヘッドと高い追跡能力を両立させた，不正者追跡方式を開発した。不正行為を法律だけで取り締まるのではなく，技術的な対策を講じておくことも重要である。このような技術的抑止力の存在は，コンテンツ供給者側に安心感を与え，コンテンツ流通を促進すると考えられる。

今後は，実用化を目指し，ユーザー側の計算負荷の小さい不正者追跡技術の開発を行う予定である。

文　献

(1) Chor, B., et al. "Tracing Traitors," CRYPTO'94, Springer-Verlag, 1994, p.257－270.
(2) Cox, I. J., et al. "A Secure, Robust Watermark for Multimedia," IH'96, Springer-Verlag p.185－206.
(3) 日本経済新聞. CATV“ただ見”横行. 2004年10月17日朝刊.
(4) Naor, D., et al. "Revocation and Tracing Schemes for Stateless Receivers," CRYPTO 2001, Springer-Verlag, 2001, p.41－62.
(5) Kurosawa, K., et al. "Optimum Traitor Tracing and Asymmetric Schemes," EUROCRYPT'98, Springer-Verlag, 1998, p.145－157.
(6) Boneh, D., et al. "An Efficient Public Key Traitor Tracing Scheme," CRYPTO'99, Springer-Verlag, 1999, p.338－353.
(7) Kurosawa, K., et al. "Linear Code Implies Public-Key Traitor Tracing," PKC 2002, Springer-Verlag, 2002, p.172－187.
(8) Chabanne, H., et al. "Public Traceability in Traitor Tracing Schemes," EUROCRYPT 2005, Springer-Verlag, 2005, p.542－558.
(9) Boneh, D., et al. "Fully Collusion Resistant Traitor Tracing With Short Ciphertexts and Private Keys," EUROCRYPT 2006, Springer-Verlag, 2006, p.573－592.
(10) Kiayias, A., et al. "Traitor Tracing with Constant Transmission Rate," EUROCRYPT 2002, Springer-Verlag, 2002, p.450－465.
(11) Kiayias, A., et al. "On Crafty Pirates and Foxy Tracers," Security and Privacy in Digital Rights Management: Revised Papers from the ACM CCS-8 Workshop DRM 2001, Springer-Verlag, 2002, p.22－39.
(12) Matsushita, T., et al. "Hierarchical Key Assignment for Black-Box Tracing with Efficient Ciphertext Size," ICICS 2006, Springer-Verlag, 2006, p.92－111.

松下　達之　MATSUSHITA Tatsuyuki, Ph. D.
研究開発センター　コンピュータ・ネットワークラボラトリー，博士（情報理工学）。情報セキュリティ（特に著作権保護）技術の研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.

吉田　琢也　YOSHIDA Takuya, D. Eng.
東芝ソリューション（株）IT技術研究所 研究開発担当主任，工博。情報セキュリティ技術の基礎研究及び応用開発に従事。
Toshiba Solutions Corp.

秋山　浩一郎　AKIYAMA Koichiro, D. Eng.
研究開発センター　コンピュータ・ネットワークラボラトリー主任研究員，工博。セキュリティ技術の研究開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.

今井　秀樹　IMAI Hideki, D. Eng.
中央大学理工学部教授，独立行政法人 産業技術総合研究所 情報セキュリティ研究センター長，東京大学名誉教授，工博。日本学術会議会員。IEEE，電子情報通信学会，IACR各フェロー。
Faculty of Science and Engineering, Chuo University.