推薦論文

送信者に認証機能を付加したブロードキャスト暗号とその応用

金沢史明[†] 岡本健[†]
猪俣敦夫[††] 岡本栄司[†]

ブロードキャスト暗号とは，多数のユーザが存在する中で，送信者が選択したユーザのみに対し，ブロードキャストチャネルを通して安全かつ効率的にデータを配布する技術であり，有料放送など著作物の配信に有効である．本稿では，送信者が自身の秘密鍵を用いて暗号文を生成することにより，受信者が送信者の本人認証とメッセージ認証を行うことができる方式を提案する．さらに，提案方式を応用し，1-out-of-n 署名と検証者指定署名の特徴をあわせた署名方式が構築できることを示す．両方式は，いずれも暗号文や署名のサイズが n に依存せず固定長となり，チャネルの帯域が制限された環境に適している．

Broadcast Encryption with Sender Authentication and its Application

Fumiaki Kanazawa,[†] Takeshi Okamoto,[†] Atsuo Inomata[††]
and Eiji Okamoto[†]

Broadcast Encryption allows a sender to distribute digital data securely and efficiently, through a broadcast channel to selected users. This technology enables us to distribute digital contents such as pay-TV. In our scheme, a sender encrypts data using his private key. This allows the receiver to authenticate the sender and the message. Furthermore, we consider the efficient signature scheme combining both functions of 1-out-of-n signatures and designated-verifier signatures.

1. はじめに

近年，音楽や画像，映像など，著作物のデジタル化技術が発展したことにより，衛星放送などの放送型通信サービスが急速に普及しつつある．総務省によると，日本における有料衛星放送（WOWOW，スカイパーフェク TV!）の契約件数の合計は，2005 年 12 月の時点で 643 万件に達した[22]．これは NHK の放送受信契約件数[17] の約 17%，衛星契約件数 1,247 万件の約 52%を占める．これらの割合は年々増加しており，今後も契約件数は増えていくことが予想される．衛星放送がここまで普及した背景には，主要な衛星放送のすべてがデジタル放送であるということから多チャネル化に進んでいるという情勢がある．結果として，放送される番組は膨大な数になっている．

一方，デジタル情報はコピーが容易であることから，新しい問題が発生している．すなわち，インターネットなども含め，放送されたデジタルコンテンツの著作権が侵害されるという事件が多発しており，深刻な社会問題になっている．衛星放送では，商業的な理由から料金を支払う者のみが視聴などのサービス利用を許され，料金を支払わない者はサービスを利用できないといったシステムが求められる．ただし，消費者は自由に契約，解約，再契約できる必要があるため，サービス利用の権限をどのようにして動的に，かつ効率良く与えるかが，消費者の利便性に深くかかわり，結果としてシステムにおける大切な要件となる．

ブロードキャスト暗号[3),8)] は，こうしたサービスに適した暗号方式であり，Berkovits や Fiat らによって提案された．この暗号方式では，送信者が指定したメンバは暗号文を復号することができるが，それ以外の

† 筑波大学大学院システム情報工学研究科リスク工学専攻
Department of Risk Engineering, Graduate School of Systems and Information Engineering, University of Tsukuba
†† 独立行政法人科学技術振興機構
Japan Science and Technology Agency

本論文の内容は 2005 年 10 月のコンピュータセキュリティシンポジウムにて報告され，CSEC 研究会前主査により情報処理学会論文誌への掲載が推薦された論文である．

メンバは復号することができない．従来の暗号（データ守秘）方式は送信者と受信者が 1 対 1 であるが，この方式は 1 対多の暗号方式である点が異なっている．

2005 年，Boneh らによって，stateless receiver（秘密鍵の更新機能を持たない受信者）に適したブロードキャスト暗号[4] が提案された．以降，本方式を BGW 方式と称す．BGW 方式は，暗号文サイズと秘密鍵サイズに関し，優れた性能を有する．

前述の衛星放送では，送信者の身元を示すため，送信メッセージに対し署名機能を付加することが望ましい．しかしながら，BGW 方式は暗号方式であるため，署名機能を有していない．このことは，送信者と送信データの正当性が保証されない（相手認証およびメッセージ認証の不備）ということを意味する．また，単純に署名機能を付加しただけでは，鍵管理や伝送量などの点で，送信時におけるオーバヘッドが増大する．

本稿では，新しいブロードキャスト暗号方式を提案する．これは，BGW 方式を改良した方式であり，前述の問題点を解決することができる．提案方式は，送信者が認証子（署名）生成時に秘密鍵を明示的に使用し，署名生成と暗号化処理を同時に行う方式である．このため，BGW 方式に対し単純に署名機能を付加した場合に比べ，鍵管理や伝送量という点で優れている．また，BGW 方式の利点も引き継いでいる．

加えて，提案方式を応用した新しい匿名署名方式についても提案する．この署名方式は，1-out-of-n 署名[1),20)] と検証者指定署名[11),16)] を組み合わせた方式であり，署名者匿名性や検証者限定性などの性質を有する．暗号方式と電子署名方式は，いずれも落し戸付き一方向性関数を用いた公開鍵暗号系であり，両者は双対性を持つことが知られている．本研究では，提案方式（認証機能付きブロードキャスト暗号）と匿名署名方式（検証者指定型 1-out-of-n 署名）との双対性に注目し，両者の変換可能性について検討した．双対性については，Kiayias らや岡本らに既存研究[13),19)] がある．しかし，認証機能付きブロードキャスト暗号から検証者指定型 1-out-of-n 署名へ変換が可能であることを明示的に示したのは，本研究が初めてであり，本研究の主要な成果の 1 つである．提案する匿名署名方式は，署名長がシステムの加入者の数に関係なく固定サイズであり，現在求められている安全性を考慮しても 1,004 bit で構成可能という優れた特徴を持つ．本方式は，署名者匿名性と検証者限定性といった性質を有するため，より安全な内部告発者の保護[1),20)] が達成できる．

以下，本稿の構成を述べる．2 章では，本稿で必要な知識を述べる．3 章では，ブロードキャスト暗号について述べる．4 章では，既存方式である BGW 方式[4)] を紹介する．5 章では，本稿の提案方式であるブロードキャスト暗号について述べる．6 章では，提案方式の応用として匿名署名方式を提案する．双方の提案方式について，7 章では性能評価を行い，8 章では安全性の考察を行う．最後に 9 章で本稿をまとめる．

2. 準　　備

各表記と安全性の根拠となる問題を定義する．

2.1 表　　記

各表記を以下のように定義する．

$\mathcal{N}$ ：システム内の全ユーザの集合（$|\mathcal{N}| = N$）
$\mathcal{S}$ ：復号を許可するユーザの集合（$|\mathcal{S}| = n$）
$\mathcal{R}$ ：復号を許可しないユーザの集合（$|\mathcal{R}| = r$）
p, q ：q が $p-1$ を割り切るような大きな素数
$\mathbb{G}_1$ ：素数 q を位数とする有限加法群
$\mathbb{G}_2$ ：素数 q を位数とする有限乗法群（$\mathbb{G}_2 \subset \mathbb{Z}_p^*$）
$\hat{e}(\cdot,\cdot)$：ペアリング（双線形写像）（$\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$）
$H(\cdot)$ ：ハッシュ関数（$\{0,1\}^* \to \mathbb{Z}_q$）
P ：$\mathbb{G}_1$ の生成元

2.2 ペアリングに基づく問題

BGW 方式[4)] は，以下の問題に基づいている．

定義 1（Bilinear Diffie-Hellman Exponent 問題）. $\alpha \in \mathbb{Z}_q$，$N \in \mathbb{N}$，$T \in \mathbb{G}_1$ とする．N-BDHE 問題とは，任意のベクトル $(T, P, \alpha P, \alpha^2 P, \cdots, \alpha^N P, \alpha^{N+2} P, \cdots, \alpha^{2N} P)$ が与えられたとき，$e(P,T)^{\alpha^{N+1}}$ を求める問題である．

ここで，与えられたベクトルに $\alpha^{N+1} P$ が抜けていることに注意されたい．

3. ブロードキャスト暗号

ブロードキャスト暗号方式の目的は，送信者が選択したユーザのみに，メッセージを安全に送信することである．本章では，その概要について述べる．

3.1 関 連 研 究

ブロードキャスト暗号方式は，特定の者のみが送信する共通鍵タイプと任意の者が送信する公開鍵タイプの 2 種類に分類できる．

共通鍵ブロードキャスト暗号[2),9),10),18)]　システム管理者などの特定の者のみが送信を行う方式である．送信者は，ユーザと共有する秘密鍵を用いてメッセージを暗号化する．送信者は制限されるが，比較的高速な暗号化・復号が可能となる．

公開鍵ブロードキャスト暗号[4),7)]　任意のユーザが送信を行う方式である．システム管理者は，公開鍵

と秘密鍵を生成し，秘密鍵を各ユーザに配布する．送信者は，選択したユーザに応じた公開鍵を用いてメッセージを暗号化する．一般の公開鍵暗号と同様，暗号化・復号にコストがかかる方式が多い．

代表的な共通鍵方式として，Naor らが提案した Complete Subtree（CS）方式と Subset Difference（SD）方式[18] があげられる．双方とも木構造を用いてユーザや鍵を管理する木構造鍵管理方式に則しており，CS 方式はヘッダサイズに関して，SD 方式は秘密鍵サイズに関して良い性能と有する．さらに，層化した木構造に SD 方式を適用した Halevy らの Layered SD（LSD）方式[10]，完全多分木に CS 方式を適用した Asano の方式[2]，SD 方式の鍵導出を改良し秘密鍵サイズをさらに削減した Goodrich らの Stratified SD（SSD）方式[9] があげられる．

また公開鍵方式として，Naor らは CS 方式・SD 方式の公開鍵版[18] を提案したが，これらの方式は公開鍵の数が莫大であり，各ユーザの鍵保管量も非常に多く現実的でない．現実的な方式として，Dodis らが，CS 方式は ID ベース暗号を参考に，SD 方式と LSD 方式は階層的 ID ベース暗号を参考に，公開鍵方式へ拡張した方式[7] がある．

BGW 方式は公開鍵ブロードキャスト暗号に分類される．木構造鍵管理方式に則していないが，秘密鍵サイズ，ヘッダサイズの双方ともシステム内のユーザ数 N に依存せず，固定サイズとなる優れた性能を有する．

3.2 モデル

共通鍵方式と公開鍵方式の双方とも，以下のようにモデル化することができる．

初期化・鍵生成フェーズ 初期段階において，システム管理者はセキュリティパラメータから各ユーザの秘密鍵と公開情報を生成する．ユーザ秘密鍵を各ユーザにそれぞれ秘密通信で配布し，公開情報を各ユーザがつねに取得できる状態にする．

暗号化フェーズ 送信者は，セッション鍵と呼ばれる共通鍵暗号の鍵を生成し，その鍵でメッセージを暗号化する．次に，復号を許可するユーザを選択し，そのユーザのみが各自の秘密鍵で復号できるようにセッション鍵を暗号化する．暗号化セッション鍵をまとめたものはヘッダと呼ばれる．送信する暗号文はヘッダと暗号化メッセージで構成される．

復号フェーズ 復号を許可されたユーザは，受信したヘッダの中から自分が復号可能な暗号化セッション鍵を見つけ，初期に配布された秘密鍵で復号する．復号で得られたセッション鍵で暗号化メッセージを復号する．

表 1 既存方式の性能
Table 1 Performance of previous works.

	秘密鍵サイズ	ヘッダサイズ
CS [18]	$O(\log N)$	$r \log \frac{N}{r}$
SD [18]	$O(\log^2 N)$	$2r-1$
Basic LSD [10]	$O(\log^{1.5} N)$	$4r-2$
SSD [9]	$O(\log N)$	$k(2r-1)$
Asano [2]	$O(1)$	$r(\log_a \frac{N}{r}+1)$
公開鍵 SD [7]	$O(\log^3 N)$	$\log N(2r-1)$
BGW [4]	$O(1)$	$O(1)$

SSD 方式は木構造内の層数が k の場合．
Asano 方式は a 分木の場合．

3.3 望まれる性質

ブロードキャスト暗号は，秘密鍵のサイズ，ヘッダのサイズ，暗号化・復号時における計算コストの 3 点から性能評価が行われる．**表 1** に代表的な既存方式の性能を示す．

秘密鍵のサイズ BGW 法が提案される以前においても，秘密鍵サイズが固定長となる方式が存在していた．こうしたユーザの記憶容量を考慮した方式のほとんどが，公開情報や関数を利用して，1 つの秘密鍵から状況に応じた秘密鍵を導出する方式である．代表的な方式は Asano 方式で，RSA 問題に基づいている．

ヘッダのサイズ 1 章では暗号文全体のサイズと述べた．ブロードキャスト暗号の方式によって変化するのはヘッダのサイズのみであり，暗号化メッセージのサイズはメッセージの暗号化に用いる共通鍵暗号方式のみの影響を受ける．BGW 法が提案される以前においても，ブロードキャストチャネルの伝送容量に配慮した方式が存在していた．その代表といえる SD 方式のヘッダサイズは，復号を許可しないユーザ数 r に依存する．

暗号化・復号時における計算コスト 計算コストの大部分は鍵導出にかかるコストである．家電製品などユーザの計算能力に制限のある場合には，考慮する必要がある．表 1 に記載していないが，CS 方式は鍵導出が不必要であり，計算コストは一番小さい．数学的性質を利用した Asano 方式・公開鍵 SD 方式・BGW 方式は，比較的コストが大きい．

ただし，秘密鍵サイズとヘッダサイズは互いにトレードオフの関係にあり，すでに述べた方式も含め，そのバランスが考慮された方式が数多く提案されている．

4. BGW 方式[4]

Boneh らが提案した BGW 方式は，任意のユーザが暗号化可能な方式，すなわち公開鍵ブロードキャス

ト暗号の一種である．

4.1 プロトコル

初期化・鍵生成

(1) 乱数 $\alpha \in \mathbb{Z}_q$ を生成．

(2) $P_i = \alpha^i P$ を計算（$i = 1, 2, \cdots, N, N+2, \cdots, 2N$）．

(3) 乱数 $\gamma \in \mathbb{Z}_q$ を生成し，$Q = \gamma P$ を計算．

(4) ユーザ $i \in \{1, \cdots, N\}$ の秘密鍵 $D_i = \gamma P_i$ を計算（すなわち $D_i = \alpha^i Q$ である）．

(5) 各ユーザの秘密鍵 $\{D_1, \cdots, D_N\}$ と，公開情報 $PK = (P, P_1, \cdots, P_N, P_{N+2}, \cdots, P_{2N}, Q) \in \mathbb{G}_1^{2N+1}$ を出力．

暗号化

(1) 乱数 $t \in \mathbb{Z}_q$ を生成し，セッション鍵 $K = g^t \bmod p$ を計算（$g = \hat{e}(P_N, P_1)$ を利用）．

(2) ヘッダ Hdr を以下のように計算．

$$Hdr = \left(tP,\, t\left(Q + \sum_{j \in \mathcal{S}} P_{N+1-j} \right) \right).$$

(3) メッセージ M を鍵 K で暗号化し，暗号化メッセージ C_M を生成（任意の共通鍵暗号系を利用）．

(4) Hdr と C_M を出力．

復号

$Hdr = (C_0, C_1)$ とする．

(1) ユーザ $i \in \mathcal{S}$ は，秘密鍵 $D_i \in \mathbb{G}_1$ を利用し，C_M の復号鍵 K を以下のように導出．

$$K = \frac{\hat{e}(P_i, C_1)}{\hat{e}\left(D_i + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}, C_0 \right)} \bmod p.$$

(2) 鍵 K で C_M を復号し，復号されたメッセージ M を出力．

ここで，復号アルゴリズムにおいて，K が正確に導出されることを以下に示す．

$$\begin{aligned} K &= \frac{\hat{e}(P_i, C_1)}{\hat{e}\left(D_i + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}, C_0 \right)} \\ &= \frac{\hat{e}\left(P_i, t\left(Q + \sum_{j \in \mathcal{S}} P_{N+1-j} \right) \right)}{\hat{e}\left(\alpha^i Q + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}, tP \right)} \\ &= \frac{\hat{e}\left(P_i, t\left(Q + P_{N+1-i} + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j} \right) \right)}{\hat{e}\left(\alpha^i Q + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}, tP \right)} \\ &= \frac{\hat{e}(P, P)^{t\alpha^{N+1}} \cdot \hat{e}\left(P_i, t\left(Q + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j} \right) \right)}{\hat{e}\left(\alpha^i \left(Q + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j} \right), tP \right)} \\ &= \frac{g^t \cdot \hat{e}\left(P_i, t\left(Q + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j} \right) \right)}{\hat{e}\left(t\left(Q + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j} \right), P_i \right)} \\ &= g^t. \end{aligned}$$

BGW 方式は，以下の 2 つの点で優れている．

ユーザ秘密鍵のサイズ ユーザ i の秘密鍵は D_i であり，各ユーザは $\mathbb{G}_1$ の元を 1 つ持つ必要がある．よって，秘密鍵は D_i（$i = 1, \cdots, N$）であり，サイズは全ユーザ数 N に影響されず，固定サイズとなる．

ヘッダのサイズ ヘッダは (C_0, C_1) であり，送信者と受信者は $\mathbb{G}_1$ の元を 2 つやりとりする必要がある．よって，ヘッダサイズは全ユーザ数 N と送信者が選択したユーザ数 n のいずれにも影響されず，固定サイズとなる．

4.2 送信者に対する認証機能の不備

BGW 方式は公開鍵ブロードキャスト暗号であるため，任意の者が送信可能であり，公開情報 PK のみを用いて暗号文を生成することができる．暗号化の際に送信者 a のみが知りうる情報（秘密鍵など）は必要ないため，生成された暗号文から送信者を特定することが困難である．このため，復号を行うユーザ $i \in \mathcal{S}$ は，暗号文の送信元が a なのか区別できない．つまり，ユーザは送信者の本人認証を行うことができず，送信者 a は身元が保証されないこととなる．

送信者 a がこの暗号文を生成したことを証明する場合，暗号化の際に a のみが知りうる情報を利用する必要がある．解決手段として，単純に BGW 方式に既存の署名方式と組み合わせることが考えられる．しかし，署名のサイズが短い short signature 方式[5] は離散対数問題に基づいた方式であるため，N-BDHE 問題に基づいている BGW 方式とは秘密鍵の型が異なる．

すなわち，BGW 方式では公開鍵 $Y \in \mathbb{G}_1$ に対応する秘密鍵 $X \in \mathbb{G}_1$ が $X = \gamma Y$ であるが，short signature 方式では秘密鍵 $x \in \mathbb{Z}_q$ に対応する公開鍵 $Y \in \mathbb{G}_1$ は $Y = xP$ である．よって，short signature 方式と BGW 方式を単純に組み合わせると，秘密鍵のサイズや公開情報のサイズが基本方式の約 2 倍となるなど，効率が悪くなる．

5. 提案方式

提案方式である送信者に認証機能を付加したブロードキャスト暗号は，メッセージの正当性と送信者の正当性を保証する方式である．

5.1 構成手法

提案方式の要件は 3.3 節の要件をすべて受け継いでいる．さらに，基本方式の要件に加え，送信者の認証機能を持つことが提案方式の要件となる．

送信者認証機能 受信したデータから，受信者は送信者の本人認証が可能である．また，送信者は他人に成りすますことができない．

この機能を付加するために，ヘッダ Hdr 中の Q の代わりに，送信者の秘密鍵 D_a（$= \alpha^a Q$）を用いる．また，成りすまし対策として，t が送信者 a によって生成されたことを受信者に証明する必要がある．そこで，送信者 a はヘッダの中に t の知識を有する証明として認証子 (e, y) を加える．

5.2 モデル

提案方式は，送信者の認証機能を備えているため，3.2 節の基本モデルとは異なり，以下のようになる．

初期化・鍵生成フェーズ 初期段階において，システム管理者はセキュリティパラメータからユーザの秘密鍵と公開情報を生成する．生成した秘密鍵を各ユーザに配布し，公開情報を各ユーザがつねに取得可能な状態にする．具体的には，システム内のユーザ数 N を考慮し，各ユーザの秘密鍵 $\{D_1, \cdots, D_N\}$，公開情報 PK を生成する．生成した秘密鍵 D_i をユーザ i にそれぞれ配布する．

認証子生成・暗号化フェーズ 送信者は，復号を許可するユーザを選択し，初期に配布された秘密鍵を用いてメッセージを暗号化する．さらに暗号鍵に関する情報（ヘッダ）を生成する．暗号化されたメッセージは，復号を許可されたユーザのみが導出可能な鍵で復号可能である．具体的には，送信者 $a \in \mathcal{N}$ は復号を許可するユーザ集合 $\mathcal{S}$ を選択し，公開情報 PK，秘密鍵 D_a を用いてメッセージ M を暗号化し，暗号化メッセージ C_M と認証子を含んだヘッダ Hdr を生成する．

検証・復号フェーズ 復号を許可されたユーザは，初期に配布された秘密鍵とヘッダから送信者の検証を行う．検証に成功した場合，秘密鍵とヘッダから復号鍵（セッション鍵）を導出し，暗号化メッセージを復号する．具体的には，ユーザ $i \in \mathcal{S}$ は，復号許可ユーザ集合 $\mathcal{S}$，公開情報 PK，秘密鍵 D_i を用いて，ヘッダ Hdr から，送信者が a であるかを検証する．検証に成功した場合，$\mathcal{S}$，PK，D_i を用いて，Hdr から復号鍵を導出し，暗号化メッセージ C_M を復号する．

5.3 ペアリングに基づく問題

提案方式の安全性を考察するために，以下のような問題を定義する．

定義 2（拡張 Bilinear Diffie-Hellman Exponent 問題）. $\alpha \in \mathbb{Z}_q$，$N \in \mathbb{N}$，$T \in \mathbb{G}_1$ とする．拡張 N-BDHE 問題とは，任意のベクトル $(T, \alpha^{-(N-1)}P, \cdots, \alpha^{-1}P, P, \alpha P, \alpha^2 P, \cdots, \alpha^N P, \alpha^{N+2}P, \cdots, \alpha^{2N}P)$ が与えられたとき，$e(P,T)^{\alpha^{N+1}}$ を求める問題である．

ここで，与えられたベクトルに $\alpha^{N+1}P$ が抜けていることに注意されたい．また，拡張 N-BDHE 問題は，N-BDHE 問題のベクトルに，$\alpha^{-(N-1)}P$, $\alpha^{-(N-2)}P, \cdots, \alpha^{-1}P$ を追加したものである．このため，帰着関係として，N-BDHE 問題から拡張 N-BDHE 問題が解けるが，その逆が解けるとは限らない．

5.4 プロトコル

初期化・鍵生成

(1) 乱数 $\alpha \in \mathbb{Z}_q$ を生成．

(2) $P_i = \alpha^i P$ を計算（$i = -(N-1), \cdots, -2, -1, 1, 2, \cdots, N, N+2, \cdots, 2N$）．

(3) 乱数 $\gamma \in \mathbb{Z}_q$ を生成し，$Q = \gamma P$ を計算．

(4) ユーザ $i \in \{1, \cdots, N\}$ の秘密鍵 $D_i = \gamma P_i$ を計算．

(5) 各ユーザの署名鍵 $\{D_1, \cdots, D_N\}$ と，公開情報 $PK = (P, P_{-(N-1)}, \cdots, P_{-1}, P_1, \cdots, P_N, P_{N+2}, \cdots, P_{2N}, Q) \in \mathbb{G}_1^{3N}$ を出力．

暗号化

(1) 送信者 a は，乱数 $t \in \mathbb{Z}_q$ を生成し，セッション鍵 $K = g^t \bmod p$ を計算．

(2) 乱数 $r \in \mathbb{Z}_q$ を生成し，$u = g^r \bmod p$ を計算．

(3) $e = H(u)$ を計算．

(4) $y = r - et \bmod q$ を計算．

(5) ヘッダ Hdr を以下のように計算（e と y は送信者とメッセージの認証子）．

$$Hdr = \left(tP, t\left(D_a + \sum_{j \in \mathcal{S}} P_{N+1+a-j} \right), e, y \right).$$

(6) メッセージ M を鍵 K で暗号化し，暗号化メッセージ C_M を生成（任意の共通鍵暗号系を利用）．

(7) Hdr と C_M を出力．

検証・復号

$Hdr = (C_0, C_1, e, y)$ とする．

(1) ユーザ $i \in \mathcal{S}$ は秘密鍵 $D_i \in \mathbb{G}_1$ を利用し，C_M の復号鍵 K を以下のように導出．

$$K = \frac{\hat{e}(P_{i-a}, C_1)}{\hat{e}\left(D_i + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}, C_0 \right)} \bmod p.$$

(2) $u' = g^y K^e \bmod p$ を計算.
(3) もし，$e = H(u')$ が成り立つならば (4) へ進む．成り立たなければ，送信者 a の認証が失敗した旨を出力.
(4) 鍵 K で C_M を復号し，復号されたメッセージ M を出力.

復号・検証アルゴリズムにおいて，K が正確に導出されることを以下に示す．ただし，BGW 方式と重複する部分は省略する．

$$\begin{aligned} K &= \frac{\hat{e}(P_{i-a}, C_1)}{\hat{e}\Big(D_i + \sum_{\substack{j\in\mathcal{S}\\ j\neq i}} P_{N+1-j+i}, C_0\Big)} \\ &= \frac{\hat{e}\big(\alpha^{i-a}P, t\big(D_a + \sum_{j\in\mathcal{S}} P_{N+1+a-j}\big)\big)}{\hat{e}\Big(\alpha^i Q + \sum_{\substack{j\in\mathcal{S}\\ j\neq i}} P_{N+1-j+i}, tP\Big)} \\ &= \frac{\hat{e}\big(P_i, \alpha^{-a}t\big(\alpha^a Q + \alpha^a \sum_{j\in\mathcal{S}} P_{N+1-j}\big)\big)}{\hat{e}\Big(\alpha^i Q + \sum_{\substack{j\in\mathcal{S}\\ j\neq i}} P_{N+1-j+i}, tP\Big)} \\ &= \frac{\hat{e}\big(P_i, t\big(Q + \sum_{j\in\mathcal{S}} P_{N+1-j}\big)\big)}{\hat{e}\Big(\alpha^i Q + \sum_{\substack{j\in\mathcal{S}\\ j\neq i}} P_{N+1-j+i}, tP\Big)} \\ &= g^t. \end{aligned}$$

6. 検証者指定型 1-out-of-n 署名

5 章の提案方式の応用として，リング署名[20] の一種である 1-out-of-n 署名[1] と検証者指定署名[11] の機能をあわせた署名方式を提案する．この署名方式は，提案するブロードキャスト暗号の手順を逆に実行することで実現され，署名のサイズはユーザ数 n に依存しない．署名者の匿名性と検証者の制限を必要とする状況に適している．

6.1 関 連 研 究

6.1.1 1-out-of-n 署名方式[1),20)]

1-out-of-n 署名方式とは，n 人の集合 $\mathcal{S}$ に属する 1 人以上が署名を生成し，検証者は $\mathcal{S}$ 内のだれかが署名したことは検証できるが，だれが署名したかは特定できない方式である．代表的な方式として，Rivest らのリング署名方式[20]，Abe らの方式[1] があげられる．

署名者は，選択した集合 $\mathcal{S}$ に属するユーザの意思にかかわらず，$\mathcal{S}$ を名義とする署名を生成する．検証者は，$\mathcal{S}$ 名義の署名としての正当性は検証できるが，署名者個人の特定はできない．そのため，署名者は選択した各ユーザに対して，署名した責任を均等に分散させることが可能となる．署名者の匿名性を確保しているため，内部告発者の保護に大きく寄与している．1-out-of-n 署名の概要を以下に述べる．

初期化・鍵生成フェーズ 初期段階において，各ユーザは公開鍵と秘密鍵を生成する（システム管理者が各ユーザの秘密鍵を生成し，秘密通信で配布する形式でも可）.

署名生成フェーズ 署名者は，署名者集合 $\mathcal{S}$ を選択し，署名者自身の秘密鍵と $\mathcal{S}$ に属するユーザの公開鍵から，$\mathcal{S}$ の署名 σ を生成する.

署名検証フェーズ 署名検証者は，署名者集合 $\mathcal{S}$ に属するユーザの公開鍵から，署名 σ の正当性を検証する.

6.1.2 検証者指定署名方式[11),16)]

検証者指定署名方式とは，署名者が指定した者のみに署名を検証する能力を与える方式である．代表的な方式として，Jakobsson らの方式[11] や Laguillaumie らの複数検証者指定署名方式[16] があげられる．

署名者は，検証能力を与えるユーザ v を指定し，v のみが検証可能な署名を生成する．検証者 v は署名を検証できるが，v 以外のユーザは署名の正当性を検証できない．また，検証者 v は第三者に対して署名者がだれであるかを納得させることが不可能である．すなわち，指定した検証者 v 以外のユーザが，v の秘密鍵を用いて署名者の検証を行ったとしても，実際の署名者は否認することが可能である．既存方式には，v が v 自身を指定して署名した可能性，すなわち自作自演の可能性を残すことによって，実際の署名者の否認する余地を残す方式がある．自作自演の可能性がある場合，第三者は，実際の署名者が署名したのか，指定された検証者による自作自演なのかを判断することができない．検証者指定署名の概要を以下に述べる．

初期化・鍵生成フェーズ 1-out-of-n 署名と同じ.

署名生成フェーズ 署名者は，指定する検証者 v を選択し，署名者自身の秘密鍵とユーザ v の公開鍵から，ユーザ v のみが検証可能な署名を生成する.

署名検証フェーズ 検証者 v は，v 自身の秘密鍵と署名者の公開鍵から，署名の正当性を検証する.

6.2 ブロードキャスト暗号から匿名認証への変換

提案する署名方式は，先に提案したブロードキャスト暗号に対して，双対性に関する変換を施すことで構築される．以下に，双対性と変換手法について説明する.

データ守秘暗号方式と電子署名方式の双対性 公開鍵暗号において，ユーザ u に対する暗号文は，任意の者が生成可能であり，ユーザ u のみが復号可能である．また，電子署名において，あるメッセージに対する u の署名は，u のみが生成可能であり，任意の者が検証可能である．すなわち，任意の者が暗号化能力と署名検証能力を持ち，u の

みが復号能力と署名生成能力を持つ．これは，プロトコルの観点から考慮して，公開鍵暗号と電子署名の手順が互いに逆となっており，双方の間に双対性が存在することを示している．

こうした双対性を利用した研究として，Kiayiasらや岡本らの手法[13),19)]があげられる．しかし，5章で提案した送信者の認証機能を持つブロードキャスト暗号と，本章で提案するような署名者の匿名性を持つ機能と検証者を指定する機能をあわせ持った署名方式の双対性を利用した研究は，今回が初めてとなる．

提案方式と匿名署名の双対性 本章で提案する署名方式は，5章において提案したブロードキャスト暗号に対して変換を施したものである．

BGW方式などの公開鍵ブロードキャスト暗号において，ユーザ集合 $\mathcal{S}$ に対する暗号文は，任意の者が生成可能であり，各ユーザ $i \in \mathcal{S}$ のみが復号可能である．これに双対性に関する変換を施せば，あるメッセージに対するユーザ集合 $\mathcal{S}$ の署名が，各ユーザ $i \in \mathcal{S}$ のみが生成可能であり，任意の者が検証可能となるような署名方式が構成できる．すなわち，生成された署名は $\mathcal{S}$ に属するユーザであればだれでも生成可能なため，署名者が $\mathcal{S}$ に属するかどうかのみを検証可能であり，署名者個人の特定は不可能である．

さらに，5章の提案方式は，送信者の認証機能を付加した公開鍵ブロードキャスト暗号であるため，送信者が a であることを示す暗号文は a のみが生成可能である．この方式に変換を施せば，ユーザ a のみが検証可能である1-out-of-n 署名方式が構成できる．署名者の匿名性を持つ機能と検証者を指定する機能をあわせ持った署名方式を実現が可能となる．

6.3 求められる安全性

一般の署名方式の要件に加え，1-out-of-n といった匿名性と検証者指定の両方を考察する必要があり，以下のような要件を満たす必要がある．

署名者匿名性 ユーザ集合 $\mathcal{S}$ に属するだれかが生成した署名は，署名者が $\mathcal{S}$ に属することのみ検証可能であり，署名者個人を特定することは不可能である．

検証者限定性 署名者が指定したユーザのみが署名を検証することが可能である．たとえ，指定されないユーザが結託しても検証することは不可能である．

なお，検証者指定署名の要件であった第三者による署名者検証不可能性は，提案する署名方式の要件に含めないこととする．含める必要がある場合の解決策については，本章の最後で述べる．

6.4 モ デ ル

提案する署名方式は，1-out-of-n 署名と検証者指定署名を融合して，次のようにモデル化することができる．

初期化・鍵生成フェーズ 5章の提案方式と同じ．

署名生成フェーズ 署名者は，巻き添えにするユーザと署名検証能力を与える1ユーザを選択し，メッセージの署名を生成する．生成された署名は，真の署名者と巻き添えユーザをあわせたうちの1人が署名したことを証明する．具体的には，署名者 $i \in \mathcal{N}$ は，署名者候補の集合 $\mathcal{S}$ と署名検証能力を与える検証者 a を選択し，秘密鍵 D_i と公開情報 PK を用いて，メッセージ M の署名 σ を生成する．ただし，集合 $\mathcal{S}$ は巻き添えユーザの集合に署名者 i を加えたものである．

署名検証フェーズ 署名検証者は自分の署名検証能力を確認し，署名が $\mathcal{S}$ 名義のものであるかを検証する．具体的には，検証者 a は，署名者候補の集合 $\mathcal{S}$ と秘密鍵 D_a，公開情報 PK から，自分の署名検証能力を確認する．確認に成功した場合，署名 σ が $\mathcal{S}$ に属するユーザの署名であるか検証する．

ここで，署名生成フェーズで指定する検証者の公開鍵を用い，署名検証フェーズで検証者自身の秘密鍵を用いることによって検証者限定性を満たすことを目指す．

6.5 プロトコル

実際の署名者 $i \in \mathcal{S}$ が生成する乱数 t を集合 $\mathcal{S}$ の秘密鍵，指定された検証者 a のみが導出できる g^t を公開鍵とし，巡回群 $\langle g \rangle = \mathbb{G}_2$ 上のSchnorr署名に適用した．今回の方式は，知識の証明のためにSchnorr署名を用いたが，ほかにも離散対数問題に基づいているDSA署名やElGamal署名の方式を用いてもよい．

初期化・鍵生成 5章の提案方式と同じである．

署名生成 送信者 i はユーザ a のみを検証者に指定する．

(1) 乱数 $t, k \in \mathbb{Z}_q$ を生成し，X_0 と X_1 を以下のように計算．

$$X_0 = tP_{i-a} + kP_{-a},$$

$$X_1 = t\left(D_i + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}\right) + k\left(Q + \sum_{j \in \mathcal{S}} P_{N+1-j}\right).$$

(2) 乱数 $r \in \mathbb{Z}_q$ を生成し，$u = g^r \bmod p$ を計算 ($g = \hat{e}(P_N, P_1)$ を利用).
(3) メッセージ M に対し，$e = H(u||M)$ を計算.
(4) $y = r - et \bmod q$ を計算.
(5) 署名 $\sigma = (X_0, X_1, e, y)$ を出力.

署名検証

(1) 次の K' を計算.

$$K' = \frac{\hat{e}\left(X_0, D_a + \sum_{j \in \mathcal{S}} P_{N+1+a-j}\right)}{\hat{e}(X_1, P)} \bmod p.$$

(2) $u' = g^y K'^e \bmod p$ を計算.
(3) もし，$e = H(u'||M)$ が成り立つならば署名の正当性を受諾する旨を，そうでなければを棄却する旨を出力.

検証アルゴリズムにおいて，正当な署名 σ が受諾されることを示す.

$$\begin{aligned} u' &= g^y K'^e \\ &= g^y \cdot \left\{ \frac{\hat{e}\left(X_0, D_a + \sum_{j \in \mathcal{S}} P_{N+1+a-j}\right)}{\hat{e}(X_1, P)} \right\}^e \\ &= g^y \cdot \hat{e}(P, tP_{N+1})^e \\ &= g^y (g^t)^e = g^{r-et} g^{et} = g^r = u. \end{aligned}$$

よって，$H(u'||M) = H(u||M) = e$ が成り立つため，σ は受諾される.

署名者の匿名性を保持するため，乱数として t 以外に k を用いている．もし k を用いずに $X_0 = tP_{i-a}$ とした場合，検証者 a は，

$$\hat{e}(X_0, P_{N+1+a-i}) = K'.$$

を実行することにより，真の署名者 $i \in \mathcal{S}$ を特定可能である.

また，6.3 節で述べた，第三者による署名者検証不可能性を必要とする場合について考える．提案した署名方式において，署名者は指定する検証者を $\mathcal{S}$ に含めることができない．署名検証の際に P_{n+1} を必要とするためである．この解決策として，初期段階においてユーザの 2 倍分の秘密鍵を生成し，1 ユーザに署名用と検証用の 2 つの秘密鍵を配布することを提案する．秘密鍵サイズと公開情報のサイズが 2 倍となるが，署名者が指定検証者を $\mathcal{S}$ に含める場合でも，検証の際に P_{n+1} を必要とすることはない．こうして，指定する検証者が署名者に成りすました可能性を作り出すことで，実際の署名者に匿名性を付与できる.

7. 性能評価

3.3 節で述べた 3 つの基準と公開情報のサイズに関して，提案方式の性能評価を行う．前半では，5 章で提案した送信者に本人認証機能を付加したブロードキャスト暗号方式について，後半では，6 章で提案した 1-out-of-n 署名の機能と検証者指定署名の機能をあわせた署名方式について述べる.

なお，**表 2** と**表 3** は以下の条件における値である．$|p| = 1{,}026$，$|q| = 160$，$\mathbb{G}_1$ は楕円曲線上に定義される加法群とする．$(x, y) \in \mathbb{G}_1$ のサイズは 342 bit ($|x| = |y| = 171$) とし，加算とべき倍算は Jacobian 座標系[6] で計算する．$\mathbb{G}_1$ 上のべき倍算と $\mathbb{G}_2$ 上のべき乗算は binary 法[14] を利用し，ペアリング演算は Kobayashi らの sliding window Miller 法[15] を利用する．さらに，1M を $\mathbb{Z}_p^*$ 上における乗算 1 回分のコストと定義する.

7.1 ブロードキャスト暗号

各ユーザの秘密鍵のサイズ，ヘッダサイズ，公開情報サイズ，暗号化・復号時における負荷の 4 点から評価する．表 2 において，単純に BGW 方式と既存署名方式を組み合わせた方式と提案方式の性能比較を示した．本節に限り，BGW 方式と Schnorr 署名[21] を組み合わせた方式を a 方式，BGW 方式と short signature 方式[5] を組み合わせた方式を b 方式と呼ぶこととする.

秘密鍵のサイズ 提案方式では，BGW 方式と同様に，ユーザの秘密鍵は $\mathbb{G}_1$ の元 1 個分である．全体的なサイズは全ユーザ数 N に影響されず，固定サイズである．BGW 方式と既存署名方式を組み合わせると，それぞれの秘密鍵が必要となるため，サイズが比較的大きくなる．表 2 の 342 bit は十分に実用的である.

ヘッダのサイズ 提案方式のヘッダは $\mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{Z}_q \times \mathbb{Z}_q$ の元である．全体的なサイズは，全ユーザ数 N と送信者が選択したユーザ数 s のいずれにも影響されず，固定サイズである．提案方式は Schorr 署名の考え方を取り入れているため，Schnorr 署名を単純に用いた a 方式とヘッダサイズが同じである．b 方式は，署名長が短い short signature を用いたため，ヘッダ全体も比較的小さい．しかし，表 2 における提案方式の 1,004 bit は，十分に実用的だといえる.

公開情報のサイズ BGW 方式は公開情報のサイズが $\mathbb{G}_1$ の元 $2N + 1$ 個分であるのに対し，提案方式は $3N$ 個分である．すなわち，提案方式は BGW 方式と比較して約 1.5 倍の情報公開が必要であり，全ユーザ数 N に比例する．しかし，BGW 方式と既存署名方式を組み合わせると，それぞれの公開鍵が必要となるため，提案方式よりサイズが大

表 2 提案方式の性能評価（ブロードキャスト暗号）
Table 2 Performance of proposed broadcast encryption scheme.

	(a)	(b)	提案方式
秘密鍵サイズ (bit)	502	502	342
ヘッダサイズ (bit)	1,004	855	1,004
公開情報サイズ (bit)	$1{,}710N + 342$	$1{,}026N + 342$	$1{,}026N$
暗号化・認証子生成 (M)	$645.8 + 0.3n$	$571.6 + 0.3n$	$645.8 + 0.3n$
検証・復号 (M)	$1{,}289.7 + 0.3n$	$1{,}694.5 + 0.3n$	$1{,}289.7 + 0.3n$

(a) BGW 方式 + Schnorr 署名方式[21)]
(b) BGW 方式 + short signature 方式[5)]

表 3 提案方式の性能評価（検証者指定型 1-out-of-n 署名）
Table 3 Performance of proposed signature scheme.

	提案方式
秘密鍵サイズ (bit)	342
署名サイズ (bit)	1,004
公開情報サイズ (bit)	$1{,}026N$
署名生成 (M)	$626.8 + 0.6n$
署名検証 (M)	$1{,}290.0 + 0.3n$

きくなる．

暗号化・復号時における負荷 暗号化にかかる計算量は，$\mathbb{G}_1$ 上の加算が n 回とべき倍算が 2 回，$\mathbb{G}_2$ 上の乗算が 1 回とべき乗算が 2 回となる．検証・復号にかかる計算量は，$\mathbb{G}_1$ 上の加算が $n-1$ 回，$\mathbb{G}_2$ 上の乗算が 2 回とべき乗算が 2 回，ペアリング演算が 2 回となる．双方とも送信者が選択したユーザ数に比例する．

表 2 において，ユーザ数に関わる変数を持つ項目について考える．提案方式と b 方式の公開情報サイズが $1{,}026N$ bit であるのに対し，a 方式はその 1.6 倍以上である．$1{,}026N$ bit は，$N = 50{,}000$ で約 6.12 MB，$N = 1{,}000{,}000$ で約 122 MB となる．公開情報はオンラインで取得可能な場合，Boneh らが文献 4) において主張する上限 $N = 50{,}000$ は，本方式においても適したユーザ数と考えられる．メモリカードなどで公開情報を配布することを考慮する場合，ユーザ数を 100 万とすれば，128 MB のメモリカードで配布可能である．

7.2 検証者指定型 1-out-of-n 署名

各ユーザの秘密鍵のサイズ，署名のサイズ，署名生成・検証時における負荷の 3 点から評価する．表 3 において，提案方式の性能評価を示す．

秘密鍵のサイズ ユーザの秘密鍵は，BGW 方式と同じく，$\mathbb{G}_1$ の元 1 個分である．全ユーザ数 N に影響されず，固定サイズである．

署名のサイズ 署名のサイズは $\mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{Z}_q \times \mathbb{Z}_q$ の元である．全ユーザ数と署名者が選択したユーザ数のいずれにも影響されず，固定サイズである．

公開情報のサイズ 公開情報のサイズは，$\mathbb{G}_1$ の元 $3N$ 個分である．すなわち，提案方式は BGW 方式の約 1.5 倍の情報公開が必要であり，全ユーザ数 N に比例する．

署名生成・検証時における負荷 署名生成にかかる計算量は，$\mathbb{G}_1$ 上の加算が $2n-1$ 回とべき倍算が 4 回，$\mathbb{G}_2$ 上の乗算が 1 回とべき乗算が 1 回となる．検証にかかる計算量は，$\mathbb{G}_1$ 上の加算が n 回，$\mathbb{G}_2$ 上の乗算が 2 回とべき乗算が 2 回，ペアリング演算が 2 回となる．双方とも，署名者が選択したユーザ数に比例する．

表 3 において，提案方式の公開情報サイズは $1{,}026N$ bit である．7.1 節同様，公開情報はオンラインで取得可能な場合，Boneh らが主張する上限 $N = 50{,}000$ は，本方式においても適したユーザ数と考えられる．5 万のユーザを抱える環境として企業などがあげられる．メモリカードなどで公開情報を配布することを考慮する場合，ユーザ数を 100 万とすれば，128 MB のメモリカードで配布可能である．100 万規模のユーザをかかえる環境として，都道府県などの地方自治体内が各世帯に端末を置くような場合が考えられる．

8. 安 全 性

提案方式の安全性を考察する．前半では，5 章で提案したブロードキャスト暗号方式における，データ守秘機能の結託耐性と認証子偽造不可能性について述べる．後半では，6 章で提案した署名方式における，署名偽造不可能性，署名者匿名性，検証者限定性について述べる．

8.1 ブロードキャスト暗号

結託耐性 ユーザ $h \in \mathcal{R}$ が，結託したとしても，ユーザ $i \in \mathcal{S}$ の秘密鍵 D_i を用いることなく，セッション鍵 $K = \hat{e}(P_{N+1}, tP)$ を導出することが不可能であることを示す．ただし，送信者 a が生成するヘッダを $Hdr = (C_0, C_1, e, y)$，公開情報を PK とする．

まず，送信者が a であることを考慮せずに，C_0，PK から K を導出することは，N-BDHE 問題

を解くこととなるため，いかなるユーザも困難である．

C_0，C_1，PK，D_h から K を導出する場合，ユーザ $h \in \mathcal{R}$ は以下の 2 つの計算を実行する必要がある．

(1) C_1 と $W \in PK$ から，K を含むような $\hat{e}(C_1, W)$ を生成．

(2) $\hat{e}(C_1, W)$ から K 以外の部分を除去．

$i \in \mathcal{S}$ に対して $W = P_{i-a}$ としたとき，

$$\begin{aligned}&\hat{e}(C_1, P_{i-a})\\ &= \hat{e}\big(t\big(D_a + \textstyle\sum_{j\in\mathcal{S}} P_{N+1+a-j}\big), P_{i-a}\big)\\ &= \hat{e}\Big(D_i + \textstyle\sum_{\substack{j\in\mathcal{S}\\ j\neq i}} P_{N+1+i-j}, tP\Big)\cdot K,\end{aligned}$$

となり，(1) を実行することができる．次に K 以外を除去する必要がある．h の秘密鍵 D_h から秘密鍵 D_i を導出するには，P_{i-h} から α^{i-h} を求める必要があるが，これは離散対数問題を解くことになり，困難である．すなわち，$h \in \mathcal{R}$ が結託した場合において，(1) を実行した後に (2) を実行することはできない．逆に，$h \in \mathcal{R}$ が (2) を実行可能なように W を設定する場合，(1) を実行することができない．よって，離散対数問題と N-BDHE 問題に基づき，$h \in \mathcal{R}$ の結託によってセッション鍵 K を導出することは不可能である．

認証子偽造不可能性 送信者 a の秘密鍵 D_a を用いることなく，検証者（受信者）に送信者が a であると納得させる認証子を生成することが不可能であることを示す．

前項で述べたように，送信者 a 以外の秘密鍵から D_a を導出することや，送信者が a であることを考慮せずにセッション鍵 $K = g^t$ を導出することは，困難である．

さらに，a が生成したセッション鍵のみを入手し，異なるメッセージの暗号化に使用する場合を考える．認証子 (e, y) を偽造するには，セッション鍵 $K = g^t$ から乱数 t を求める必要がある．これは離散対数問題を解くこととなるため困難である．よって，離散対数問題と N-BDHE 問題に基づき，秘密鍵 D_a を用いなければ，メッセージの送信者が a であることを検証者に納得させる認証子を生成することができない．

8.2 検証者指定型 1-out-of-n 署名

署名偽造不可能性 ユーザ $i \in \mathcal{S}$ の秘密鍵 D_i を用いることなく，$\mathcal{S}$ 名義の署名を生成することが不可能であることを示す．

署名者 $h \notin \mathcal{S}$ が $\mathcal{S}$ のユーザに成りすます場合を考える．検証者 a は，$\mathcal{S}$ の公開鍵 $K' = g^t$ を以下の式で導出する．

$$K' = \frac{\hat{e}\big(X_0, D_a + \sum_{j\in\mathcal{S}} P_{N+1+a-j}\big)}{\hat{e}(X_1, P)} \bmod p.$$

すなわち正確に K' を導出させるために，h は上記を満たす (X_0, X_1) を生成する必要がある．ここで，$\hat{e}(X_1, P)$ に K'_{-1} を含ませるような X_1 を生成することは N-BDHE 問題を解くこととなるため困難である．よって，以下の条件を満たす (X_0, X_1) を生成することとなる．

(1) $Y_0 = D_a + \sum_{j\in\mathcal{S}} P_{N+1+a-j}$ に対し，$\hat{e}(X_0, Y_0)$ が K' を含むような X_0．

(2) $\hat{e}(X_0, Y_0)/\hat{e}(X_1, P) = K'$ を満たす，h の秘密鍵 D_h と PK のみから生成した X_1．

前節と同様に，署名者 h の秘密鍵 D_h から，ユーザ $i \in \mathcal{S}$ の秘密鍵 D_i を生成することは困難である．D_i を持たない h は，(1) を満たすように X_0 を生成すると，(2) を満たす X_1 を生成することができない．逆に，(2) を考慮して X_1 を生成すると，(1) を満たす X_0 を生成できない．

また，h が $\mathcal{S}$ の公開鍵 K' のみを入手し，異なるメッセージの署名生成に使用する場合を考える．(e, y) を偽造するには，公開鍵 $K' = g^t$ から乱数 t を求める必要があり，これは困難である．よって，離散対数問題に基づき，ユーザ $i \in \mathcal{S}$ の秘密鍵 D_i を用いなければ，$\mathcal{S}$ 名義の署名を生成することが不可能である．

署名者匿名性 署名者 $i \in \mathcal{S}$ が生成した署名から，第三者が署名者個人を特定することが不可能であることを示す．

検証者が，署名 $\sigma = (X_0, X_1, e, y)$ から i を求めることを考える．検証者が X_0 や X_1 から t や k を求めることは，離散対数問題を解くこととなるため，困難である．よって，乱数 t が係数である項，すなわち X_0 の P_{i-a} や X_1 の $D_i + \sum_{\substack{j\in\mathcal{S}\\ j\neq i}} P_{N+1-j+i}$ は，乱数 k が係数である項と分離させることができない．また，6.5 節に述べたように，乱数として t 以外に k を用いたことで匿名性を保持している．X_0 と X_1 の双方が乱数 k を含んでいるため，鍵 K' と比較することで署名者を特定することは困難である．

ゆえに，(X_0, X_1, e, y) から i を求めることは困難である．

検証者限定性 署名者 $i \in \mathcal{S}$ が指定した検証者 a の秘密鍵 D_a を用いることなく，署名を検証することが不可能であることを示す．

検証者 a 以外の秘密鍵から D_a を導出することや，X_0 や X_1 から乱数 t を求めることは困難である．よって，乱数 t を求めることなく指定され者以外の秘密鍵と PK のみから K' を求めることは N-BDHE 問題を解くこととなるため困難である．検証者 $h \in \mathcal{N}$ が，$\mathcal{S}$ の公開鍵 $K' = g^t$ を求めることを考える．以下の式において，乱数 γ を含む項は X_1 内にあるため，$Y_0 = D_h + Y_0'$ とする．ただし Y_0' と Y_1 は PK から導出されるものとする．

$$\frac{\hat{e}(X_0, Y_0)}{\hat{e}(X_1, Y_1)}$$

$$= \frac{\hat{e}(tP_{i-a}, D_h + Y_0')}{\hat{e}\Big(t\Big(D_i + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}\Big), Y_1\Big)}$$

$$\cdot \frac{\hat{e}(kP_{-a}, D_h + Y_0')}{\hat{e}\big(k\big(Q + \sum_{j \in \mathcal{S}} P_{N+1-j}\big), Y_1\big)}.$$

$K' = g^t$ に乱数 k が含まれていないことから，

$$\frac{\hat{e}(kP_{-a}, D_h + Y_0')}{\hat{e}\big(k\big(Q + \sum_{j \in \mathcal{S}} P_{N+1-j}\big), Y_1\big)} = 1$$

$$\frac{\hat{e}(k(Q + \alpha^{-h} Y_0'), P_{h-a})}{\hat{e}\big(k\big(Q + \sum_{j \in \mathcal{S}} P_{N+1-j}\big), Y_1\big)} = 1.$$

乱数 γ を含む項（Q）を考慮すると，$Y_1 = P_{h-a}$，$Y_0' = \sum_{j \in \mathcal{S}} P_{N+1+h-j}$ となる．これより，

$$\frac{\hat{e}(X_0, Y_0)}{\hat{e}(X_1, Y_1)}$$

$$= \frac{\hat{e}\big(tP_{i-a}, D_h + \sum_{j \in \mathcal{S}} P_{N+1+h-j}\big)}{\hat{e}\Big(t\Big(D_i + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1-j+i}\Big), P_{h-a}\Big)} \cdot 1$$

$$= \frac{\hat{e}\big(D_{h+i-a} + \sum_{j \in \mathcal{S}} P_{N+1+h-j+i-a}, tP\big)}{\hat{e}\Big(D_{h+i-a} + \sum_{\substack{j \in \mathcal{S} \\ j \neq i}} P_{N+1+h-j+i-a}, tP\Big)}$$

$$= \hat{e}(P_{N+1+h-a}, tP).$$

ゆえに検証者 a のみが，$\mathcal{S}$ の公開鍵 $K' = g^t$ を導出することができる．秘密鍵 D_a を持たない者は，署名検証をすることが不可能である．

9. ま と め

本稿では，送信者に認証機能を付加したブロードキャスト暗号方式を提案した．提案方式は，BGW 方式と署名を単純に組み合わせるのではなく，暗号化の際に送信者の秘密鍵を利用する方式である．また，ユーザ秘密鍵のサイズとヘッダのサイズのいずれも固定サイズであり，ユーザ数に影響されない．送信者の本人認証を行うため，BGW 方式をそのまま使用する場合より，ユーザは暗号化されたデータに対して信頼を持つことができる．特に，暗号化されたデータがコンピュータウイルスである場合など，ユーザが復号後に被害をこうむる可能性を考慮すると，送信元確認の重要性が非常に大きいことが分かる．

また，提案方式を応用し，1-out-of-n 署名と検証者指定署名の両機能を持った署名方式を提案した．さらに，署名のサイズが n に依存しないことが示された．本方式は，署名者の指定したユーザのみが署名者の所属を特定可能であり，署名者個人の特定は困難である．この特徴は，アンケートや内部告発など，署名者の匿名性と検証者の限定が求められるシステムに有効であると考えられる．

参 考 文 献

1) Abe, M., Ohkubo, M. and Suzuki, K.: 1-out-of-n Signatures from a Variety of Keys, *Advances in Cryptology—Asiacrypt 2002*, LNCS, Vol.2501, pp.415–432, Springer-Verlag (2002).
2) Asano, T.: A Revocation Scheme with Minimal Storage at Receivers, *Advances in Cryptology—Asiacrypt 2002*, LNCS, Vol.2501, pp.433–450, Springer-Verlag (2002).
3) Berkovits, S.: How to Broadcast a Secret, *Advances in Cryptology—Eurocrypt '91*, LNCS, Vol.547, pp.535–541, Springer-Verlag (1991).
4) Boneh, D., Gentry, C. and Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, *Advances in Cryptology—CRYPTO 2005*, LNCS, Vol.3621, pp.258–275, Springer-Verlag (2005).
5) Boneh, D., Lynn, B. and Shacham, H.: Short Signatures from the Weil Pairing, *Advances in Cryptology—Asiacrypt 2001*, LNCS, Vol.2248, pp.514–532, Springer-Verlag (2001).
6) Cohen, H., Miyaji, A., Ono, T.: Efficient Elliptic Curve Exponentiation Using Mixed Coordinates, *Advances in Cryptology—Asiacrypt '98*, LNCS, Vol.1514, pp.51–65, Springer-Verlag (1998).
7) Dodis, Y. and Fazio, N.: Public Key Broadcast Encryption for Stateless Receivers, *Proc. ACM DRM 2002*, LNCS, Vol.2696, pp.61–80, Springer-Verlag (2002).
8) Fiat, A. and Naor, M.: Broadcast Encryption, *Advances in Cryptology—CRYPTO '93*, LNCS, Vol.773, pp.480–491, Springer-Verlag (1994).
9) Goodrich, M.T., Sun, J.Z. and Tamassia, R.: Efficient Tree-Based Revocation in Groups of Low-State Devices, *Advances in Cryptology—CRYPTO 2004*, LNCS, Vol.3152, pp.511–527, Springer-Verlag (2004).

10) Halevy, D. and Shamir, A.: The LSD Broadcast Encryption Scheme, *Advances in Cryptology—CRYPTO 2002*, LNCS, Vol.2442, pp.47–60, Springer-Verlag (2002).
11) Jakobsson, M., Sako, K. and Impagliazzo, R.: Designated Verifier Proofs and Their Applications, *Advances in Cryptology—Eurocrypt '96*, LNCS, Vol.1070, pp.143–154, Springer-Verlag (1996).
12) 金沢史明, 岡本 健, 猪俣敦夫, 岡本栄司：送信者に認証機能を付加したブロードキャスト暗号, コンピュータセキュリティシンポジウム（CSS2005）論文集, pp.349–354 (2005).
13) Kiayias, A. and Yung, M.: Extracting Group Signatures from Traitor Tracing Schemes, *Advances in Cryptology—Eurocrypt 2003*, LNCS, Vol.2656, pp.630–648, Springer-Verlag (2003).
14) Knuth, D.E.: *Seminumerical Algorithms, The Art of Computer Programming, 3rd ed.*, Vol.2, Addison-Wesley (1998).
15) Kobayashi, T., Aoki, K. and Imai, H.: Efficient Algorithms for Tate Pairing, *IEICE Trans. Fundamentals*, Vol.E89-A, No.1, pp.134–143 (2006).
16) Laguillaumie, F. and Vergnaud, D.: Multi-designated Verifiers Signatures, *Information and Communications Security—ICICS 2004*, LNCS, Vol.3269, pp.495–507, Springer-Verlag (2004).
17) NHK インターネット営業センター：受信契約件数一覧（月別・全国計）. http://www.nhk.or.jp/eigyo/know/jyushinryo.html
18) Naor, D., Naor, M. and Lotspiech, J.: Revocation and Tracing Scheme for Stateless Receivers, *Advances in Cryptology—CRYPTO 2001*, LNCS, Vol.2139, pp.41–62, Springer-Verlag (2001).
19) 岡本 健, 岡本栄司：署名長が固定された 1-out-of-n 署名, コンピュータセキュリティシンポジウム（CSS2005）論文集, pp.223–228 (2005).
20) Rivest, R.L., Shamir, A. and Tauman, Y.: How to Leak a Secret, *Advances in Cryptology—Asiacrypt 2001*, LNCS, Vol.2248, pp.552–565, Springer-Verlag (2001).
21) Schnorr, C.P.: Efficient Signature Generation by Smart Cards, *J. Cryptology*, Vol.4, No.3, pp.161–174 (1991).
22) 総務省情報通信統計データベース：民間衛星放送の有料放送契約数. http://www.johotsusintokei.soumu.go.jp/field/data/gt030103.xls

(平成 18 年 4 月 26 日受付)
(平成 18 年 9 月 14 日採録)

推 薦 文

Boneh らによって提案されているブロードキャスト暗号 BGW 方式の問題点である送信者の身元確認を，送信者の秘密鍵をヘッダ中に組み入れることで実現し，ブロードキャスト暗号に本人認証機能を追加している．さらに，提案方式を応用し，1-out-of-n 署名と検証者指定署名の両機能を持った署名方式を提案している．この方式は署名長が n に依存しないものであり，帯域制限のある環境下で非常に有効であると思われる．信頼性と実用性，完成度が高いので，論文として推薦する．

（コンピュータセキュリティ研究会
前主査 村山優子）

金沢 史明（学生会員）

2003 年東京理科大学理学部応用数学科卒業．2005 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．現在，筑波大学大学院システム情報工学研究科博士後期課程在学中．暗号，情報セキュリティに関する研究に従事．電子情報通信学会，IEEE，ACM 各会員．

岡本 健（正会員）

2002 年北陸先端科学技術大学院大学博士後期課程修了．博士（情報科学）．同年東京電機大学理工学部情報科学科助手．その後 2003 年より筑波大学大学院システム情報工学研究科講師，現在に至る．情報セキュリティ，暗号とその応用に関する研究に従事．著書に『科学大辞典第 2 版』（丸善出版：分担執筆），『Linux ハンドブック』（オライリージャパン：共訳）等．

猪俣　敦夫（正会員）

2002 年北陸先端科学技術大学院大学博士後期課程修了．博士（情報科学）．同年日本テレコム（株）情報通信研究所入社．その後 2004 年より独立行政法人科学技術振興機構研究員，現在に至る．DWDM 光多重伝送，ネットワークセキュリティ，暗号とその応用に関する研究に従事．電子情報通信学会，教育システム情報学会各会員．訳書に『Linux セキュリティ大全』（ピアソン），『Linux ハンドブック』（オライリー）等．

岡本　栄司（フェロー）

1978 年東京工業大学大学院電子専攻博士課程修了．工学博士．同年 NEC 中央研究所入社．その後，北陸先端科学技術大学院大学，東邦大学を経て，2002 年より筑波大学大学院システム情報工学研究科教授，現在に至る．1990 年電子情報通信学会論文賞，1993 年本会ベストオーサ賞受賞．2003 年電子情報通信学会フェロー，2004 年本会フェロー．著書に『暗号理論入門』（共立出版），『電子マネー』（岩波書店）等．