匿名性を持つ譲渡禁止電子チケットシステムの提案と評価

甲斐根 功[†] 佐々木 良一[†] 斎藤 泰一[†]

近年，オンライン上でチケットの申請，発行を行う電子チケットシステムに注目が集まっており，電子チケットに関する研究が多く行われている．しかし，現在行われている多くの研究は，譲渡を可能としており，会員制のコンサート，パーティーなどで本人であるかを電子的に確認し，入場を制限する仕組みを持った電子チケットシステムの研究は少ない．そのため，本人であるかどうかを確認するには，チケット内に氏名などを含めた情報を入れておき，人手によって確認する必要があり，人手がかかるうえ，匿名性を保つことが難しい．そこで，これらの問題を解決するための方法として双方向署名と否認不可能署名を用いることにより，匿名性と譲渡禁止を可能とした電子チケットシステムを提案するとともに，プロトタイププログラムを開発し有効性の検証を行った結果についても報告する．

The Proposal and Evaluation of a Transfer Prohibited Electronic Ticket System with Anonymity

Isao Kaine,[†] Ryoichi Sasaki[†] and Taiichi Saito[†]

Attention has been paid on the electronic online ticket system. However, there are few researches to inhibit transfer of the ticket for concert, party etc. One of the considerable methods to inhibit the transfer is to describe the user name in the ticket. In this case, however, it is difficult to keep anonymity. Therefore, we propose the electronic ticket systems that enable anonymity and the transfer prohibition by using an interactive signature and undeniable signature. In addition, we report the evaluation result using the prototype program based on the proposed method.

1. はじめに

近年，インターネットが一般消費者に普及するにつれて，e-コマースなどの消費者を直接対象にした電子商取引サービスが急激に成長している．なかでも，企業・消費者間の取引（Business to Consumer）において，インターネットを介したオンライン上でのコンサートチケットなどの申請，発行を行う電子チケットシステムに注目が集まってきている．なぜならば，電子チケットには以下の利点があるからである．

1) 利用者がチケットセンターまでチケットを取りに行く必要がない．
2) コンサート主催者がどのような属性のユーザが入場したか簡単に把握できる．
3) 電子チケットの偽造が困難である．

現在まで，いろいろな研究[1),2)]，開発[3),4)]が行われてきているが，それら多くの研究は，チケットの譲渡（他人への譲り渡し）を暗黙のうちに前提としている．しかし，会員制のコンサートや，パーティーなどで本人であることを電子的に確認し，本人でないのであれば入場を制限する仕組みを持った電子チケットシステムへのニーズもある．

従来のシステムでも本人確認をするために，チケット内に“氏名”などの情報を入れておき，免許証などを使い人手を使って，入場口で確認することも可能である．しかし，この方式では会場で匿名性を保つことは難しくなる．また，チケットの購入者が自分の秘密鍵で署名をする方式の導入が当然考えられるが，通常のデジタル署名では，コンサート主催者に誰か分かってしまい，この場合も匿名性を維持できない．このように，チケット発行者には，匿名にしなくてもよいが，コンサート主催者には，匿名性を維持したい場合もある．

コンサートなどの会場での匿名性を維持しつつ，チケット購入者本人でないのであれば入場を制限できるようにすることが可能な電子チケットシステムの実現が待たれていた．

本研究の目的は，コンサートなどの会場での匿名性を維持しつつ，チケットを購入した本人でないのであ

† 東京電機大学工学部
School of Engineering, Tokyo Denki University

れば入場を制限できるようにすることにより，チケットの譲渡を抑止できる電子チケットシステムの方式の確立を図るものである．そこで，本研究では，双方向署名と名づけた署名方式と，Chaum によって提案された否認不可能署名方式[5] などを使うことによってこれらを可能とする「匿名性を持つ譲渡禁止チケットシステム」と呼ぶものを提案する[6]．あわせて，プロトタイププログラムを開発し，機能および性能の評価を行ったのでその結果についても報告する．

2. 電子チケットシステム

2.1 従来の電子チケットシステム

電子チケットシステムとはユーザがインターネットを介して，チケット販売会社にチケット購入要求を出し，チケット販売会社はユーザにチケットを電子データで発行するシステムである．

電子チケットシステムでは，以下のエンティティが存在するものとする．

- チケット購入者 A
- チケット販売者
- コンサート主催者

電子チケットシステム購入からチケットをコンサート会場へ持参するまでの流れを**図 1** に示す．

① まず，チケット購入者 A は Web ページなどで名前や住所など必要事項を記入し，チケット販売者にそれらデータを送ることで，購入要求を出す．
② チケット販売会社は，チケット購入者 A が記入したデータを確認し，チケット発行を許可するのであれば，チケット販売者の秘密鍵で電子署名されたチケットを発行し，チケット購入者 A に送信する．
③ 購入者 A は発行されたチケットを IC カードなどに入れてコンサート会場へ持っていく．
④ コンサート会場では，チケット購入者 A が持ってきたチケットの正当性を確認する．現在の電子チケットシステムにおける正当性確認は，一般的に，公開鍵暗号による電子署名が多く用いられている．チケット販売者の公開鍵で電子署名を確認し，複製や，偽造が行われていないことを確認する．確認ができたのであれば本物のチケットとして認め，コンサート会場への入場を認める．

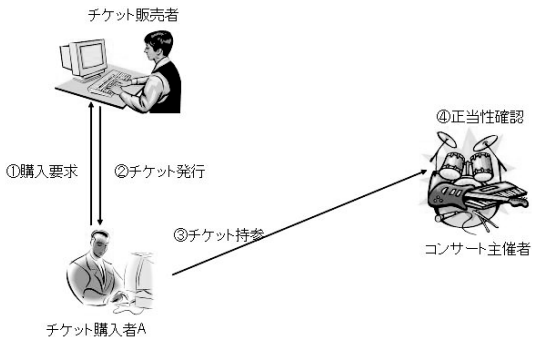

図 1 電子チケットシステム
Fig. 1 Electronic ticket system.

2.2 既存のシステムの問題点

図 2 に示すように，会員制のコンサートやパーティーのように本人であることを確認する必要がある場合には，本人以外は入場を制限する必要がある．しかし，2.1 節で説明した通常の電子チケットシステム（図 1）では，本人確認のための仕組みがなく，譲渡を抑止したい電子チケットシステムには対応できない．

ここで，チケット購入者 A が B に対して発行されたチケットを譲渡する場合を考えてみよう．コンサート会場では，チケットを譲り受けた B が持ってきたチケットの正当性を確認するために，コンサート主催者は，チケット販売者の公開鍵で電子署名を検証し，複製や，偽造が行われていないことを確認する．正当性の確認ができたのであれば，このチケットはチケット購入者 A に対して発行（許可）されたチケットにもかかわらず，本物のチケットとして認められ，チケット発行者によって参加が認められていない B のコンサート会場への入場が認められてしまう．これは，電子チケットそのものには本人確認を行うすべがないので，主催者側が電子チケットの譲渡を防ぐことができないからである．

この解決策として，電子チケット内に “氏名” などの情報を入れておき，免許証などを使い入場口で確認する方法がある．しかし，すでに述べたように，この方法では，確認作業に人手がかかり，時間がかかるうえ，コストもかかり，しかも，人手で確認をするとい

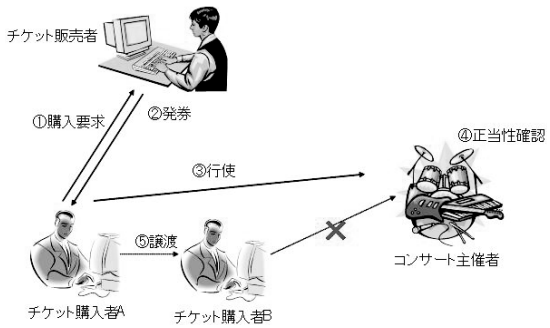

図 2 譲渡禁止電子チケットシステムのイメージ
Fig. 2 Image of transfer prohibited electronic ticket system.

うことは，匿名性が失われてしまうこととなる．また，チケットの購入者が自分の秘密鍵で署名をする方式の導入が当然考えられるが，通常のデジタル署名では，コンサート主催者に誰か分かってしまい，この場合も匿名性を維持できない．しかし，チケット販売者に対し匿名性を維持する必要はないが，コンサート主催者には匿名性を維持したい場合は多いと考えられる．

そこで，本論文では，双方向署名と名づけた署名方式と否認不可能署名などを使うことにより，コンサート主催者に，チケット情報を持っている人が誰であるかは分からないが，確かにチケットを買った本人であることの確認を行えるようにする方式を提案する．

3. 基礎となる署名方式

3.1 双方向署名（Bi-directional Signature）

2.2 節であげた問題点を解決するための方法の 1 つとして**図 3** に示すような双方向署名方式を提案する．

① まず，チケット購入者 A は名前や住所など，必要事項を記入した文書 M を作成し，文書 M に対してチケット購入者 A の秘密鍵 S_A で電子署名 Z を作成する．次に，電子署名 Z と文書 M をチケット販売者に送信する．

② チケット販売者は，文書 M の内容を確認したうえで，電子署名 Z に対してチケット販売者の秘密鍵 S_T で電子署名を行う．なお，チケット購入者 A の公開鍵 P_A が本人のものであることを確認するために，公開鍵証明書などを用いる．

③ この，双方向から署名された電子署名，$S_T(Z)$ を双方向署名と呼ぶ．双方向署名 $S_T(Z)$ と文書 M とのセットをチケット T（$= (S_T(Z) \parallel M)$）とし，チケット購入者 A に送信する．

チケット購入者 A の秘密鍵 S_A で署名された電子署名 Z に対してチケット販売者がさらに署名をする双方向署名を用いることにより，発行されたチケットが誰の所有であるか確認が可能となる．なぜならば，電子署名 Z はチケット購入者 A が持つ秘密鍵 S_A より作成されるため，チケット購入者 A にしか作成できないからである．よって，チケット販売者によって双方向署名されている電子署名 Z が誰によって作られたものであるか確認できるのであれば，発行されたチケットが誰の所有であるかの確認が可能となる．そして，そのことを，チケット販売者が検証していることも第三者に明らかになる．

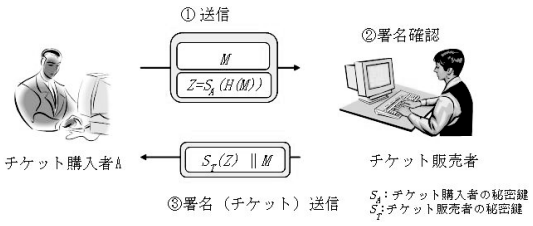

図 3 双方向署名
Fig. 3 Bi-directional signature.

この双方向署名は，チケット発行処理の段階で用いられる．

3.2 否認不可能署名（Undeniable Signature）

否認不可能署名とは Chaum [5] によって提案されている署名方式で，検証時に署名者の秘密鍵が必要となる．つまり，本人の承諾なしでは署名が検証できないことを特徴とする署名方式である．なお，検証が成立したなら，本人が署名したことの否認が不可能になることから否認不可能署名と呼ばれている．

否認不可能署名では，署名者 A が文書 M に対して署名を行う場合，以下のような手順で行われる．この論文で提案するシステムでは，署名者 A がチケット購入者 A に，検証者 B が，チケット販売者や，コンサート主催者に対応する．

① 署名者 A は秘密鍵 S_A，公開鍵 $P_A = g^{S_A} \pmod p$ を作成し，公開鍵を，大きな素数 p と原始要素 g とともに公開する．

② 署名者 A は文書 M に対して秘密鍵 S_A で，たとえば次のようにして署名する．

$$Z = M^{S_A} \pmod p$$

署名者 A が署名を文書 M にしたことの検証を検証者 B が行いたい場合，以下の手順で検証が行われる．

③ 検証者 B は乱数 $r1$，$r2$ を作成し，

$$C = M^{r1} g^{r2} \pmod p$$

を計算し，署名者 A に送信する．

④ 署名者 A は，p より小さい乱数 $r3$ を作成し，

$$S_1 = Cg^{r3} \pmod p$$
$$S_2 = (Cg^{r3})^{S_A} \pmod p$$

を作成し，検証者 B に送る．

⑤ 検証者 B は，$r1$，$r2$ を署名者 A に送る．

⑥ 署名者 A は，$r1$，$r2$ を用いて

$$C' = M^{r1} g^{r2} \pmod p$$

の計算を行い，③ で検証者 B が送った C と同じであるかどうか検証する．

⑦ 正しく検証されたならば，署名者 A は検証者 B に $r3$ を送る．

⑧ 検証者 B は，

$$S_1' = Cg^{r3} \pmod p$$
$$S_2' = (P_A)^{r2+r3} Z^{r1} \pmod p$$

を計算する．

ここで,

$$S_2 = (Cg^{r3})^S A(\mathrm{mod}\ p)$$
$$= (M^{r1}g^{r2}g^{r3})^S A(\mathrm{mod}\ p)$$
(なんとならば $C = M^{r1}g^{r2}\,(\mathrm{mod}\ p)$)
$$= g^{S_A(r2+r3)}(M^{SA})^{r1}(\mathrm{mod}\ p)$$
$$= (P_A)^{(r2+r3)}Z^{r1}(\mathrm{mod}\ p)$$
(なんとならば $P_A = g^{S_A}(\mathrm{mod}\ p), Z = M^{S_A}$ $(\mathrm{mod}\ p)$)

したがって，改ざんやなりすましがなければ，$S_1 = S_1'$ であり，$S_2 = S_2'$ になるはずである．いま，$S_1 = S_1'$ であり，$S_2 = S_2'$ だったとすれば，手順 ④ からも分かるように，検証時に署名者 A の秘密鍵 S_A が必要となるため，署名者 A が許可をしなければ検証ができない仕組みになっている．これは，いい換えると署名者 A がいなければ検証が不可能である．その結果，検証時に署名者 A の公開鍵 P_A に対応する秘密鍵が必ず必要となることと，持っているのは署名者 A のみであるということから，検証が成功したのであれば，検証時にやりとりをしている相手が署名者 A 本人であることが分かる．この特徴を生かし，本人確認を行う．

この方式は，チケット発行処理段階とチケット検証処理段階の両方で用いられる．

4. 匿名性を持つ譲渡禁止チケットシステム

4.1 前提条件

本システムは以下の前提条件の下で提案される．

前提条件 1：公開鍵証明書は信用できる．

前提条件 2：チケット購入者の秘密鍵は IC カードの秘密領域に保管されており，誰も取り出せないものとする．なお，ここで IC カードとしては，通常の，(1) 誰でもがアクセスできるメモリ領域と，(2) 秘密情報などを保管するカードの持ち主しかアクセスできない秘密領域のあるものを使う．

前提条件 3：IC カードは，持ち主が安全に管理し，他の人に貸し出さないものとする．この前提条件は合理的なものであると考えられるが，(1) 1 つの IC カードでいろいろなサービスができるようにしておき，(2) もし，IC カードを他人に貸し出せば，それらのサービスを利用し不正な買い物をされてしまうなどの貸出しのリスクが大きいようにしておけば，より自然なものとなる．

前提条件 4：チケット販売者は個人確認作業が必要であるのでチケット購入者の個人情報を知ってもよいが，コンサート主催者側ではチケット購入者が誰であるかということを知ってはならず，匿名性が維持されなければならない．

前提条件 5：コンサート主催者はチケット販売者を信用している．

4.2 システム概要

4.1 節の前提条件の下，IC カードを用いることと，前章まで説明した，双方向署名，否認不可能署名などの特徴を生かすことにより，匿名性を持ち，譲渡の抑止を可能とした**図 4** に示すような電子チケットシステムを提案する．この方式の基本的アイディアは以下のとおりである．

(1) 双方向署名を，チケット購入者とチケット販売者の間で行う途中で作成される Z の中に，チケットを購入しようとしている人の秘密鍵情報を入れる．

(2) チケット発行段階で双方向署名と否認不可能署名の両方を組み合わせることで，チケット販売者は，チケット情報に「Z の署名者がチケットの購入者であり，公開鍵 P_A に対応する秘密鍵の持ち主である」ことを証明できるようにする．

(3) したがって，チケット販売者を信頼しているコンサート主催者は，公開鍵 P_A の公開鍵証明書などを用いなくても，公開鍵 P_A が確かに，チケット購入者のものであることを知ることができる．しかも，公開鍵 P_A には公開鍵証明書のように，「これが誰のものか」の情報は入っていない．そして，チケット検証段階で否認不可能署名を再度用いることにより，確かにチケットの購入者とチケットの持ち主が同じであることが証明できる．

(4) しかし，コンサート主催者に，公開鍵 P_A そのものは分かるので，考えられる公開鍵証明書を何らかの方法で次々に入手し，公開鍵 P_A と比較することにより，公開鍵 P_A は誰のものであるか分かってしまう可能性がある．そこで，チケット販売者は乱数 R を生成し，チケット購入

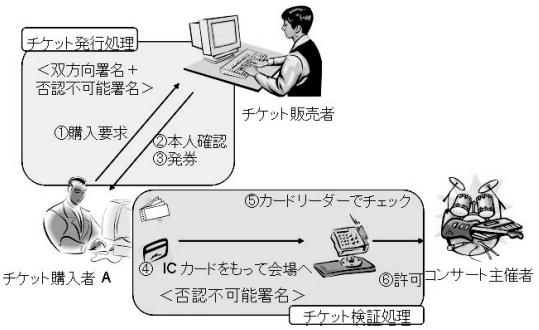

図 4 システム概要
Fig. 4 Overview of system.

者 A の公開鍵 P_A を用いて $(P_A)^R(\mathrm{mod}\ p)$ を計算しこれを送ることでこの問題の解決を図る．

(5) これにより，コンサート主催者に対し，匿名性を維持しつつ，チケット購入者以外のなりすまし入場を防止できるので，結果としてチケットの譲渡が抑止できる．

4.2.1 チケット発行処理

図 4 で述べたシステムにおけるチケット発行処理について**図 5** を用いて説明する．

①-1 最初に，チケット購入者は，名前や住所などの必要事項を記入し，ドキュメント M を作成する．

①-2 チケット購入者 A の秘密鍵 S_A を用いてドキュメント M に対し，たとえば以下のようにして署名を行う．

$Z = H(M)^{S_A}(\mathrm{mod}\ p)$ ここで，

$H(\ )$ はハッシュ関数を表す．

①-3 チケット購入者は作成した (Z, M) をチケット販売者に送信する．

②-1 チケット販売者は M の内容をチェックし，内容的に問題がないならば次の処理を行う．

②-2 チケット販売者は，チケット購入者と協力して ②-2 の以下の過程で否認不可能署名方式を用いて検証を行う．

②-2-i チケット販売者は，最初に，乱数 $r1$ と $r2$ を生成する．

②-2-ii 次に，チケット販売者は，次のようにして C を計算し，それをチケット購入者に送る．

$C = H(M)^{r1}g^{r2}(\mathrm{mod}\ p).$

②-2-iii チケット購入者は乱数 $r3$ を生成し，S_1 と S_2 の計算を次のように行う．

$S_1 = Cg^{r3}(\mathrm{mod}\ p),$

$S_2 = (Cg^{r3})^{S_A}(\mathrm{mod}\ p).$

②-2-iv チケット販売者は $r1$，$r2$ をチケット購入者に送る．

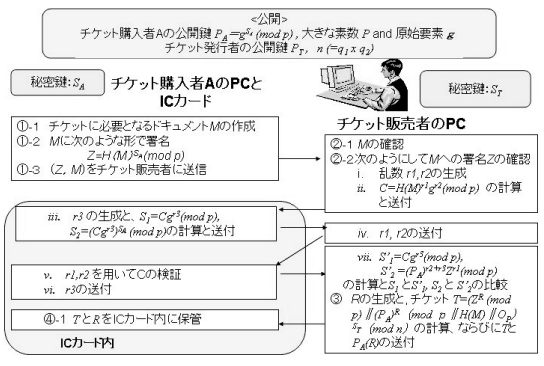

図 5 提案システムにおけるチケット発行処理

Fig. 5 Ticket publishing process of the proposed system.

②-2-v チケット購入者は ②-2-ii で送られた $r1$ と $r2$ を用いて

$C' = H(M)^{r1}g^{r2}(\mathrm{mod}\ p)$

を計算し，②-2-ii で送られた C と同じかどうか検証する．

②-2-vi 正しく検証されたならば，チケット購入者は，$r3$ をチケット販売者に送る．

②-2-vii チケット販売者は $S'1$ と $S'2$ を次のようにして計算する．

$S'_1 = Cg^{r3}(\mathrm{mod}\ p),$

$S'_2 = (P_A)^{r2+r3}Z^{r1}(\mathrm{mod}\ p).$

3.2 節で述べた理由により，改ざんやなりすましがないなら $S_1 = S'_1$ で $S_2 = S'_2$ が成立するはずである．いま，$S_1 = S'_1$ で $S_2 = S'_2$ ならば，チケット購入者 A がチケット発行を要求したのをチケット販売者は知ることができる．ここで，会員でなければ，購入できないようなチケットについては，チケット販売者が会員リストを管理している組織に確認するものとする．なお，ここでの検証処理においては，公開鍵 P_A が確かに本人のものかどうかを確認するためにはチケット購入者 A の公開鍵証明書などを用いればよい．

③ この過程により，本人であることが確認されたら，チケット販売者はチケットを生成し，チケット購入者に送付する．チケットの生成の方式としては，次の 2 つの方式が考えられる．

〈方式 1：基本的な方式〉

チケット購入者 A から送られてきた電子署名 Z，P_A，文書 M より作成された $H(M)$，必要があれば追加するオプション情報 O_P のセットに対して電子署名を行い，電子チケット T を以下のようにして生成する．ここでは，RSA 暗号を用いるものとし，法 n と公開鍵 P_T に対応する秘密鍵 S_T が求められているものとする．

$T = (Z(\mathrm{mod}\ p) \| P_A(\mathrm{mod}\ p) \| H(M) \| O_P)^{S_T}$
$(\mathrm{mod}\ n)$

ここで，オプション情報 O_P とは日時指定や座席指定などの付加情報領域であり，必要であるならばチケット発行会社によって与えられるものである．また，RSA の法 n の長さ $|n|$ は，$2|p|+$ ハッシュ長 $|H(M)|+$ オプション情報長 $|O_P|$ より十分大きいとする．

方式 1 は，双方向署名と否認不可能署名の両方を組み合わせて用いる基本的な方式である．チケット情報はチケット販売者が，「Z の署名者がチケットの購入者であり，公開鍵 P_A に対応する秘密鍵の持ち主である」ことを証明している．したがって，チケット販売

者を信頼しているコンサート主催者は，公開鍵 P_A の公開鍵証明書などを用いなくても，公開鍵 P_A が確かにチケット購入者のものであることを知ることができる．しかも，公開鍵 P_A には公開鍵証明書のように，明示的にこれが誰のものかの情報は入っていない．そして，その後チケット検証段階で否認不可能署名を再度用いることにより，確かにチケットの購入者とチケットの持ち主が同じであることが証明できる．

しかし，コンサート主催者に，公開鍵 P_A そのものは分かるので，考えられる公開鍵証明書を何らかの方法で次々に入手し，公開鍵 P_A と比較することにより，公開鍵 P_A は誰のものであるか分かってしまう可能性がある．そこで，この方式をさらに改良した方式 2 を採用することとした．

〈方式 2：公開鍵 P_A の総当りによるチケット購入者の割出しを防止できる方式〉

チケット発行会社は乱数 R を生成し，チケット購入者 A の公開鍵 P_A を用いて $(P_A)^R(\mathrm{mod}\ p)$ と $Z^R(\mathrm{mod}\ p)$ 計算する．そして，Z^R，文書 M より作成された $H(M)$，必要があれば追加するオプション情報 O_P のセットに対して，電子署名を行い，次のような電子チケット T を生成する．ここでは，RSA 暗号を用いるものとし，方式 1 の場合と同様な，法 n と公開鍵 P_T に対応する秘密鍵 S_T が求められているものとする．

$$T=(Z^R(\mathrm{mod}\ p)\|(P_A)^R(\mathrm{mod}\ p)\|H(M)\,\|\,O_P)^{ST}\ (\mathrm{mod}\ n)$$

この際，$P_A(R)$ も計算し，あわせて送信しておく．

ここで，$(Z^R)^ST = (Z^ST)^R$ の中の Z^ST の部分が，3.1 節で述べた双方向署名 $S_T(Z)$ に対応するものである．

チケット購入者 A の公開鍵 P_A をそのまま用いるのではなく，$(P_A)^R(\mathrm{mod}\ p)$ を用いることにより，コンサート主催者に，P_A を知られなくてすむ．したがって，公開鍵 P_A は誰のものであるか総当り攻撃によりコンサート主催者に知られるのを防止することができる．

④ チケット購入者 A は，送られてきたこれらの電子チケット T を，たとえば IC カード内の通常のメモリ領域に保有する．またチケット購入者は販売会社から送られてきた乱数 $P_A(R)$ から，S_A を用いて R を求めこれを IC カード内の秘密領域に格納する．チケット購入者 A は，これらチケット T を IC カードのメモリ領域，乱数 R，秘密鍵 S_A を IC カードの秘密領域内に持ってコンサート会場へ向かう．

4.2.2 チケット検証処理

④-2 コンサート会場に着いた後，チケット購入者は，IC カード内のチケット情報 $T = (Z^R(\mathrm{mod}\ p)\ \|\ (P_A)^R(\mathrm{mod}\ p)\ \|\ H(M)\ \|\ O_P)^ST(\mathrm{mod}\ n)$ を，カードリーダを経由して，コンサート主催者に示す．

⑤-1 コンサート主催者は，チケット発行者の公開鍵 P_T を用いて T を復号し，$(Z^R(\mathrm{mod}\ p)\ \|\ (P_A)^R(\mathrm{mod}\ p)\ \|\ H(M)\ \|\ O_P)$ を求める．O_P が正しく復号できることが分かれば，信頼するチケット販売者が発行しているものであることを知ることができる．なお，ここで，O_P ではなく，正しく復号できていることを確認するための専用の情報を入れておくことも可能である．

⑤-2 次に，署名 Z（より正確には Z^R）の作成者と，チケットの持ち主が同じであることを検証することを主な目的として，以下の ⑤-2 の処理を行う．

⑤-2-i コンサート主催者は，チケットから得られた O_p をチェックする．もし，O_p の内容に問題がないなら，以下の処理を行う．

⑤-2-ii コンサート主催者は乱数 $r4$，$r5$ を生成する．

⑤-2-iii コンサート主催者は，C を以下のようにして計算し，IC カードリーダを介して，IC カードに送る．

$$C = H(M)^{r4}g^{r5}(\mathrm{mod}\ p)$$

⑤-2-iv IC カードは，IC カード内の R を取り出し，以下のようにして S_3 と S_4 を計算し，それをコンサート主催者に送る．

$$S_3 = Cg^{r6}(\mathrm{mod}\ p)$$
$$S_4 = ((Cg^{r6})^SA)^R(\mathrm{mod}\ p)$$

⑤-2-v コンサート主催者は，$r4$ と $r5$ を IC カードに送る．

⑤-2-vi チケット購入者の IC カードを用いて

$$C' = H(M)^{r4}g^{r5}(\mathrm{mod}\ p)$$

を計算し，⑤-2-iii で送られてきた C と同じかどうかを検証する．

⑤-2-vii 正しく検証できれば，IC カードはカードリーダを経由して $r6$ をコンサート主催者に送る．

⑤-2-viii コンサート主催者は，チケットから取り出した $(P_A)^R$ と Z^R を用いて，S'_3，S'_4 を以下のように計算する．

$$S'_3 = Cg^{r6}(\mathrm{mod}\ p)$$
$$S'_4 = (P_A)^{R(r5+r6)}(Z^R)^{r4}(\mathrm{mod}\ p)$$

ここで，

$$
\begin{aligned}
S_4 &= ((Cg^{r6})^S A)^R \\
&= ((H(M)^{r4} g^{r5} g^{r6})^S A)^R (\mathrm{mod}\ p) \\
&(\text{なんとならば } C = H(M)^{r4} g^{r5} (\mathrm{mod}\ p)) \\
&= g^{S_A R(r5+r6)} ((H(M)^{S_A})^R)^{r4} (\mathrm{mod}\ p) \\
&= (P_A)^{R(r5+r6)} (Z^R)^{r4} (\mathrm{mod}\ p) \\
&(\text{なんとならば } P_A = g^{S_A} (\mathrm{mod}\ p), \\
&Z = H(M)^{S_A} (\mathrm{mod}\ p))
\end{aligned}
$$

したがって，改ざんやなりすましがなければ $S_3 = S'_3$ であり，$S_4 = S'_4$ になるはずである．いま，$S_3 = S'_3$ であり，$S_4 = S'_4$ だったとすれば，4.2 節の基本的アイディアで述べた理由により，否認不可能署名の相手が，公開鍵 P_A に対応する秘密鍵 S_A の持ち主であり，それがチケット購入者であることをチケット販売者が証明していることが分かる．前提条件 5 により，コンサート主催者はチケット販売者を信用しているのでこの結論を受け入れることができる．

ここでは，4.2 節の基本的アイディアで述べたように S_A に対応する P_A がチケット購入者 A のものであることを証明するのに，公開鍵証明書を使用するのではなく，チケット販売者に対するコンサート主催者の信頼を利用している．したがって，個人の識別情報が明示的に出ることはない．しかも，公開鍵 P_A 自体ではなく**図 6** の ⑤ に示すように $(P_A)^R$ をコンサート主催者に渡すようにしているので，すでに述べたように，この情報からチケット購入者が誰か知ることはできない．

また，ここでは，M に氏名などが書かれていたとしても提出するものは $H(M)$ ですむため，文書 M を提出する必要がなく個人情報などが分からない．

以上によって，チケットを購入した本人であることは分かるが，誰であるか具体的には分からず，コンサート主催者に対し，匿名性が保たれることとなる．

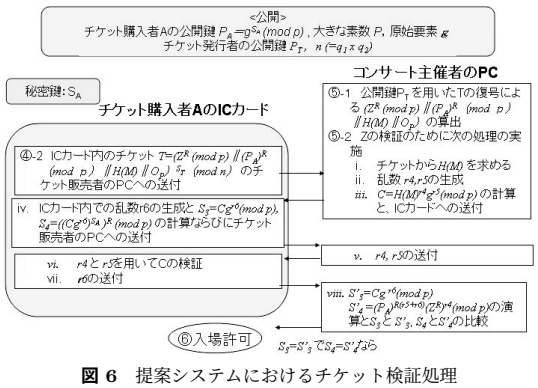

図 6 提案システムにおけるチケット検証処理
Fig. 6 Ticket confirmation process of the proposed system.

4.2.3 計算時間短縮のための検討

4.2.1 項の ③ において，電子チケット T を $T = (Z^R (\mathrm{mod}\ p) \| (P_A)^R (\mathrm{mod}\ p) \| H(M) \| O_P)^{S_T} (\mathrm{mod}\ n)$ とするといった．しかしこのようにするとRSA を使うとして，その法 n の長さ $|n|$ は，$2|p|+$ ハッシュ長 $|H(M)|+$ オプション情報長 $|O_P|$ より十分大きなければならず，T の作成や，その復号に膨大な時間がかかる．

そこで，チケット購入者 A から送られてきた文書 M より作成された $H(M)$，必要があれば追加するオプション情報 O_P のセットに対して D を求める．

$$D = (Z^R (\mathrm{mod}\ p) \| (P_A)^R (\mathrm{mod}\ p) \| H(M) \| O_P)$$

次に，チケット販売者の RSA 暗号の秘密鍵 S_T を用いて，以下のように電子署名を行う．

$$E = H(D)^{S_T} (\mathrm{mod}\ n)$$

この 2 つを電子チケット $T = (D \| E)$ としチケット購入者に送信する．このようにすれば，n は 1,024 ビットぐらいでよく，実際的な計算時間で計算が可能となる．

そして，D のハッシュをとったものと，E を P_T で復号したものが合致すれば，D の改ざんがなされておらず，確かにチケット販売者が署名したことが分かるので，4.2.1 や 4.2.2 項で示した方法と同じ効果を持つことが可能である．

4.3 システムの検討

4.3.1 本人性確認

第三者 B が，チケット購入者 A になりすまし，コンサート会場に入るには，チケット情報 T を知り，秘密鍵 S_A を利用可能にする必要がある．

チケット情報 T は，チケット購入者 A が，自分の IC カードから取り出し，第三者 B に譲渡したり，通信路上を流れるチケット情報 T を第三者 B が入手したりすることにより可能である．

次に，秘密鍵 S_A であるが，チケット購入者 A の IC カードを譲り受けるか，その IC カードから秘密鍵 S_A を取り出せれば利用できる．しかし，前提条件 3 によりチケット購入者 A の IC カードを貸与すればその損害は膨大になる可能性があるのでありえないと仮定できる．また，その IC カードから秘密鍵 S_A を取り出すことはできないと考えうる．

秘密鍵 S_A を用いなければ，否認不可能署名を用いた検証が必ず失敗するため，本人でないと判断でき，コンサートへの入場を制限することが可能となる．したがって，チケットの譲渡を受けても入場できないことから，譲渡が無意味となり，譲渡禁止の機能を持つことができる．

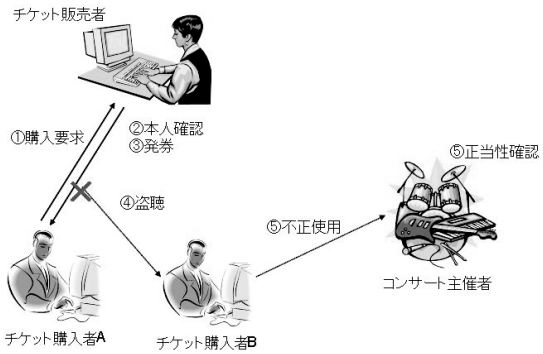

図 7 通信路上による盗聴
Fig. 7 Tapping in network.

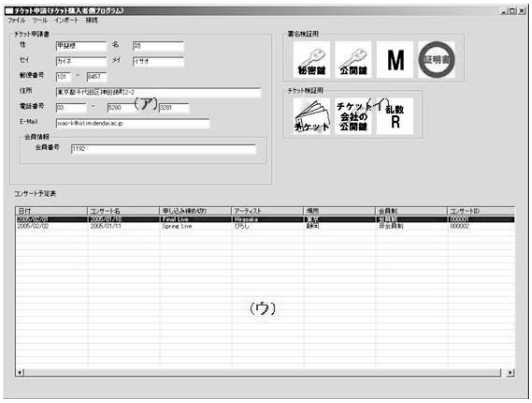

図 8 チケット購入者側プログラムのインタフェース
Fig. 8 Interface of program for ticket purchaser.

4.3.2 匿 名 性

4.2.2 項の最後に示したように，チケット購入者が誰であるか知るための情報である秘密鍵 S_A や，公開鍵 P_A 自体などをコンサート主催者に送ることなしに，チケット購入者と同じ人がコンサート会場に来ていることを検証できるようにしているので，匿名性が失われることはない．

4.3.3 安 全 性

一般的な電子チケットシステムでは，通信路上（**図 7**）での盗聴などによるチケットの複製，偽造などの問題が起こりうる．しかし，本システムでは，通信路上で盗聴され複製が行われた場合であっても，チケット検証処理においてチケット購入者の秘密鍵が必要になるため，検証に失敗する．これによって，盗聴による複製されたチケットでの入場を制限することが可能となる．

5. 実装と評価

前章で提案した方式の有効性と実用性を確認するために，プロトタイププログラムを開発し，実験を行った．

5.1 開 発 環 境

プロトタイププログラムの開発環境は以下のとおりである．

OS：Microsoft Windows XP Professional Version 2002 Service Pack 2
CPU：Intel(R) Pentium(R)4 2.40 GHz
メモリ：504 MB RAM
JAVA：j2sdk1.4.1_05
開発ソフト：Eclipse Platform Version: 2.1.2 Build id: 200311030802 (c) Copyright IBM Corp. and others 2000, 2003. All rights reserved. Visit http://www.eclipse.org/platform
プラグイン：SWT version 3.034

なお，本来は，IC カードを用いることになっているが，開発環境の制約により，USB メモリーカードを用いている．また，基本的に 4.2.1 および 4.2.2 項の方式にそっているが，4.2.3 項の計算時間を短縮する方式を導入している．

5.2 チケット購入者側プログラム

チケット購入者側プログラムとは，チケット購入者がチケット購入を行う際に用いるプログラムである（図 5 の左側）．

チケット購入者側プログラムのインタフェースを**図 8** に示す．

以下に，チケット購入者がチケットを購入する際の処理の流れを示す．

① 図 8（ウ）において，コンサートを選ぶ．
② 図 8（ア）において，名前や住所などの必要事項を記入し文書 M を作成する（図 5 ①-1）．
③ USB メモリ内のチケット購入者の秘密鍵を本プログラムにセットする．
④ 文書 M に対し，チケット購入者の秘密鍵で電子署名する（図 5 ①-2）．
⑤ 電子署名 Z を検証するために必要な鍵がセットされているか図 8（イ）で確認する．
⑥ 電子署名 Z を検証する．
⑦ チケット販売者に接続をし，文書 M，電子署名 Z を送信し，購買要求を出す（図 5 ①-3）．
⑧ チケット販売者より送られてきたチケット T を USB メモリ内のメモリ領域に保存，乱数 R を秘密領域に保存する（図 5 ④）．
⑨ チケット T を検証するために必要な鍵がセットされているか図 8（イ）で確認する．
⑩ チケット T を検証する．
⑪ USB メモリ（IC カード）を持ってコンサート会

場へ行く．

本実装では，開発環境の制約から IC カード内のプログラムは困難であるということから，代わりに USB メモリを使用している．しかし，USB メモリでは内部処理ができない．そのため，本来ならば，図 5 ②-2 における iii，v，vi の計算を IC カードの内部処理によって計算するものであるが，本プロトプログラムでは，プログラム上に秘密鍵を読み込んで．プログラム上で計算している．実際のシステムでは，秘密鍵は，IC カードの秘密領域に保存しておく．IC カードの秘密領域は耐タンパ領域（中が見られない仕組み）であり，ここに保存することにより秘密鍵は IC カードから出ることなく，計算結果のみが出力されるため，安全に保存される．

5.3 チケット販売者側プログラム

チケット販売者側プログラムとは，チケット販売者がチケットを発行する際に用いるプログラムである（図 5 の右側）．チケット発行者側プログラムにおけるインタフェースを**図 9** に示す．

チケット販売者側がチケットを発行する際の処理の流れを以下に示す．

① チケット購入者からチケット購入要求がなされた場合，図 9 のように文書 M が表示され，チケット発行者は内容を確認する（図 5 ②-1）．
② このとき，コンサートが会員制であった場合，会員情報より会員であるかも確認する．
③ 本人か確認するために，否認不可能署名の検証を行う（図 5 ②-2）．
④ オプション情報を作成する（本プログラムでは未実装）（図 5 ③）．
⑤ チケットを発行する（図 5 ③）．

② の処理においては，実際には，会員情報データベースなどにアクセスすることで，会員確認すると考えられる．

また，実際のシステムでは否認不可能署名の処理が必要なため，リアルタイムでの処理が必要となる．しかし，決算処理などがあるため，その場でチケット発行処理を行い，チケットを発行することができない場合もある．この場合は否認不可能署名の検証処理をリアルタイムで行った後，検証が成功したのであれば，チケット T か乱数どちらか一方を送り，決算が終了した後にもう一方を送ることにより，チケット発行処理を終了することで実現できる．

5.4 コンサート会場プログラム

コンサート会場におけるプログラムのインタフェースを**図 10** に示す．

また，コンサート会場での処理の流れを以下に示す．

① チケット購入者が持ってきたチケットを本プログラムに読み込む（図 6 ④-2）．
② チケットをチケット販売者の公開鍵で復号する（図 6 ⑤-1）．
③ チケットの内容を否認不可能署名で検証する（図 6 ⑤-2）．
④ オプション情報を確認（本プログラムでは未実装）（図 6 ⑤-2）．
⑤ 検証が成功したのであれば，入場を許可する（図 6 ⑥）．

本実装では USB メモリを使用しているため内部処理ができない．そのため，本来ならば，図 6 ⑤-2 における iv などの計算を IC カードの内部処理によって計算するものであるが，本プログラムでは，プログラム上に秘密鍵と乱数 R を読み込んで計算している．実際のシステムでは，秘密鍵と乱数 R は，IC カードの秘密領域から出ることなく，計算結果のみが出力される．つまり，秘密鍵と乱数 R は安全に保存され，秘密鍵は漏洩することもなく，また乱数 R が相手に知られることにより公開鍵が復号される心配もない．

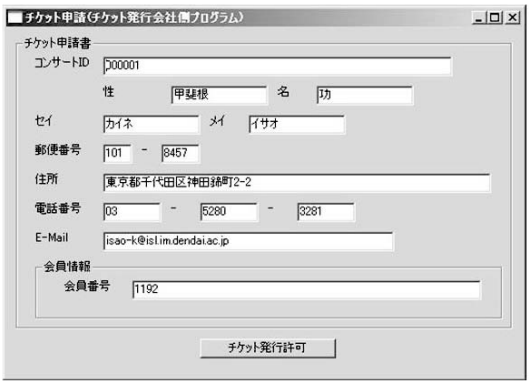

図 9 チケット販売会社側プログラムのインタフェース
Fig. 9 Interface of program for ticket issuing company.

図 10 コンサート会場プログラムのインタフェース
Fig. 10 Interface of program for concert hall entrance.

5.5 実　　験

チケット購入者 A がチケット購入者 B に対して，チケットを譲渡した場合の有効性を示すために実験を行った．

まず，チケット購入者 A とチケット購入者 B の秘密鍵，公開鍵のペアを作成し，**図 11** に示す USB メモリに秘密鍵を格納する．また，チケット購入者の公開鍵は公開されているとし，チケット販売者およびコンサート主催者にも所有させる．

一方，チケット販売会社の秘密鍵，公開鍵のペアを作成する．また，チケット販売者の公開鍵は，公開されているとし，チケット購入者 A，B およびコンサート主催者にも所有させる．ここで，鍵長は 1,024 ビットとなっている．

また，USB メモリ内は，実際の IC カード内と同様に，メモリ領域と秘密領域に分かれており，メモリ領域にチケットを，秘密領域には秘密鍵と乱数 R を保存するものとする（**図 12**）．

(1) チケット要求

チケット購入者 A は，5.2 節で説明したチケット購入者プログラムを用いて，チケット要求処理を行う．

図 11 チケット用 USB メモリ
Fig. 11 USB memory for ticket.

図 12 USB メモリ内部
Fig. 12 Status inside USB memory.

ここでは，チケット購入者 A の USB（チケット購入者 A の秘密鍵）を用いて処理を行う．

(2) チケット発行

チケット販売者は，5.3 節で説明したチケット販売者側プログラムを用いてチケット発行処理を行う．ここで，チケット販売者はチケット購入者 A の否認不可能署名の検証にチケット購入者 A の公開鍵，公開鍵証明書を用いる．否認不可能署名の検証が成功したのであればチケットを発行する．

チケット購入者 A は，発行されたチケット T を USB メモリ内のメモリ領域に格納し，乱数 R を秘密領域に格納する．

(3) チケット検証

コンサート会場では，5.4 節で説明したコンサート会場プログラムを用いてチケット検証を行う．その際，図 11 にあるような 2 種類の USB メモリを用いてそれぞれの検証を行った．

(a) チケット購入者 A の USB（チケット購入者 A の秘密鍵）を用いて検証を行った場合

まず，チケット購入者 A はチケット T を提出し，チケット販売者の公開鍵で復号する．復号されたチケットから，否認不可能署名の検証処理を行う．このとき，チケット購入者 A の秘密鍵を用いて検証処理は行われる．

その結果，正しく検証が行われた（**図 13**）．

(b) チケット購入者 B の USB（チケット購入者 B の秘密鍵）を用いて検証を行った場合

ここでは，チケット購入者 A がチケット購入者に対してチケットを譲渡した場合を考える．まず，チケット購入者 B はチケット T を提出し，チケット販売者の公開鍵で復号する．復号されたチケットから，否認不可能署名の検証処理を行う．このとき，チケット購入者 B の秘密鍵を用いて検証処理が行われる．しかし，チケット T はチケット購入者 A に対して発行されたものであり，チケット購入者 A

図 13 チケット購入者 A の USB メモリによる検証結果
Fig. 13 Verification result for ticket purchaser A.

表 1 譲渡不可能型システムの処理時間（試行回数：100 回）
Table 1 Computation time on transfer inhibited system.

		平均処理時間 [ms]	各セッションの平均処理時間 [ms]
チケット要求	署名時間	52.97	52.97
チケット発行	検証時間	825.33	2,455.58
	発行時間	1,630.25	
チケット検証	正当性確認時間	1,161.87	1,487.50
	本人確認検証時間	325.63	

図 14 チケット購入者 B の USB メモリによる検証結果
Fig. 14 Verification result for ticket purchaser B.

の秘密鍵を持っていないと検証は失敗する．

その結果，検証が失敗する（**図 14**）．

チケット購入者 A の USB メモリ（チケット購入者 A の秘密鍵）では，チケット検証処理は成功するが，チケット購入者 B の USB メモリ（チケット購入者 B の秘密鍵）ではチケット検証処理が失敗していることから，正しくプログラムが動いていることが分かる．また，このことから本プログラムの有効性が示せた．

5.6 処理時間

本プログラムの有効性を 5.5 節で示したが，処理時間がかかってしまったのでは問題である．そこで，実装したプロトタイププログラムを使い処理時間を計測した．ここで使用した鍵長は 5.5 節で使用したものと同一で，それぞれ 1,024 ビットとなっている．その結果を**表 1** に示す．

以上の結果，本来 PC を用いて計算する部分は，数秒以内であり，許容範囲内であることが明確になった．高速化のための工夫をあまりしていない状況でこの値なので，工夫をすればさらに高速化できると考えられる．

しかし，本来，チケット検証の本人確認検証の一部は，IC カードの中で実施するものである．具体的には，4.2.2 節 ⑤-2-iv の

$$S_3 = Cg^{r6} (\mathrm{mod}\ p)$$

$$S_4 = ((Cg^{r6})^S A)^R (\mathrm{mod}\ p)$$

と ⑤-2-vi の

$$C' = H(M)^{r4} g^{r5} (\mathrm{mod}\ p)$$

の計算は IC カードの中で実施すべきものである．1,024 ビット鍵長の RSA 署名は IC カード内で，1 秒以内で計算可能であるといわれている[7]．したがって，これらの計算時間はその数倍だと考えられるが，詳細は今後の課題である．

6. おわりに

本研究では，双方向署名と名づけた署名方式と，Chaum によって提案された否認不可能署名方式[5] を使うことによってこれらを可能とする「匿名性を持つ譲渡禁止チケットシステム」とよぶものを提案した．あわせて，プロトタイププログラムを開発し，機能および性能の評価を行った．

今後は，より効率的な方式の開発を目指すとともに，実際に IC カードを用いた評価実験を行う予定である．

最後に，本論文をまとめるにあたり，いろいろ議論をいただいた本杉洋氏にあつく感謝申し上げる．

参考文献

1) 飯野陽一郎：公開鍵認証基盤に基づく電子チケット，コンピュータセキュリティシンポジウム 2001 論文集，pp.325–330 (2001-11).
2) 三神京子，中村明日香，繁富利恵，小川貴英：匿名譲渡可能なオフライン型電子チケットシステム，情報処理学会研究報告，2004-CSEC-26, pp.367–374 (2004-07).
3) NTT 情報流通プラットフォーム研究所：Flex Ticket (2004/8/18 参照). http://info.isl.ntt.co.jp/flexticket/index_j.html
4) シーフォーテクノロジー：TAS スキーマ (2004/8/18 参照).
http://c4t.jp/corporate/news/press/2003/press_20031125.html
5) Chaum, D.: Zero-Knowlegde Undeniable Signatures, *Proc. Advances in Cryptology CRYPT'90*, pp.458–464, Springer Verlag (1991).
6) 甲斐根功，佐々木良一，斎藤泰一：匿名性を持つ譲渡禁止チケットシステムの提案，コンピュータセキュリティシンポジウム 2004 論文集，pp.331–336 (2004-10).
7) http://www.aladdin.co.jp/etoken/pro_r2.html

(平成 17 年 7 月 15 日受付)
(平成 18 年 4 月 4 日採録)

甲斐根　功

2003 年東京電気大学工学部情報通信工学科卒業後，同大学大学院工学研究科情報通信工学専攻入学．情報セキュリティの研究を行う．2005 年同大学院修了後，株式会社日立情報システムズ入社．

佐々木良一（フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所第 4 部長，セキュリティシステム研究センタ長，主管研究長等を経て 2001 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．2002 年情報処理学会論文賞受賞．2005 年システム制御情報学会産業技術賞受賞．著書に，『インターネットセキュリティ』（オーム社，1996），『インターネットセキュリティ入門』（岩波新書，1999）等．IEEE，電子情報通信学会等の会員．日本セキュリティ・マネージメント学会常任理事，IFIP TC11 日本代表．

斎藤　泰一（正会員）

1989 年早稲田大学理工学部数学科卒業．1991 年同大学大学院理工学研究科修士課程数学専攻修了．同年日本電信電話株式会社へ入社．2001 年中央大学大学院理工学研究科情報工学専攻博士後期課程修了．2004 年より東京電機大学助教授．暗号理論，情報セキュリティの研究に従事．博士（工学）．電子情報通信学会会員．