様式 C-19

科学研究費補助金研究成果報告書

平成２１年　6月 19 日現在

研究種目：基盤研究（C）
研究期間：2007～2008
課題番号：19500005
研究課題名（和文）　否認不可署名方式の理論的基盤構築に関する研究

研究課題名（英文）　Study on Theoretical Foundation of Undeniable Signature Scheme

研究代表者
黒澤　馨（KUROSAWA KAORU）
茨城大学・工学部・教授
研究者番号：60153409

研究成果の概要：
　否認不可署名方式は、ソフトウエアのライセンス発行、電子現金、電子投票、電子オークション、電子入札など、多くの応用を有する。本研究では、汎用結合安全性（どのように複雑なプロトコルに組み込んでも元の安全性が保たれるという性質）を満たす方式を初めて検討すると共に、発行済みの否認不可署名を通常のデジタル署名に変換することが可能な方式を、標準モデルにおいて始めて開発した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,800,000	540,000	2,340,000
２００８年度	1,600,000	480,000	2,080,000
年度			
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号系

１．研究開始当初の背景

　筆跡鑑定のプロにとっては、与えられたサイン σ が本当にアリスの署名かどうか、検査するのは容易である。一方、素人にとっては、この鑑定は難しい。デジタル情報に対し、万人が筆跡鑑定のプロとなるような方式をデジタル署名方式という。すなわち、平文 m に対するアリスの署名文を σ としたとき、(m, σ)の正当性を誰でも検証できる。これを、万人検証性という。
　これに対し、万人が筆跡鑑定の素人となるような署名方式を否認不可署名方式という。すなわち、万人検証性が成り立たない。その代わり、署名者アリスは、正当な検証者ボブに対してのみ、確認プロトコルを走らせることにより(m, σ)の正当性を証明し、否定プロトコルを走らせることにより(m, σ)の非正当性を証明する。また、(万人検証不可能な) 否認不可署名 σ を発行した後、署名者が何らかの情報を公開することにより、その σ を（万人検証可能な）デジタル署名に変換することが可能な方式を、選択的 convertible 否認不可署名方式という。また、全ての σ をデジタル署名に変換することが可能な方式

を、all convertible 否認不可署名方式という。

否認不可署名方式は、ソフトウエアのライセンス発行など、多くの応用を有する。しかし、デジタル署名方式が幅広く研究されているのに対し、否認不可署名方式の研究は、かなり立ち遅れている。

２．研究の目的

否認不可署名方式における未知の領域をさらに開拓・解明し、基礎理論を拡張・発展させるとともに、新しい応用へ向けての理論的基盤を構築することを目的とする。具体的には、以下の通り。

(1)（従来とは異なる数論的仮定に基づく方式の開発：）素因数分解の困難さ、あるいは離散対数問題の困難さに基づく選択的 convertible 否認不可署名方式を開発する。従来、素因数分解に基づくそのような方式は、ランダムオラクル・モデルにおいてすら全く知られていない。また、離散対数に基づく方式は、標準モデルにおいて知られていない。

(2)（UC 安全性の解明：）最近、Canetti により、マルチパーティプロトコルと親和性の高い 汎用結合安全性（universally composability）(略して UC)という安全性の概念が導入され、活発に研究されている。UC とは、どのように複雑なプロトコルに組み込まれたとしても、元の安全性が維持される、という概念である。本研究では、否認不可署名方式の UC 安全性を定義し、その性質、および実現可能性を解明する。従来、否認不可署名方式に対する UC 安全性は、ほとんど検討されていない。

３．研究の方法

長年の共同研究者であるロンドン大学の Yvo Desmedt 教授らと研究打ち合わせを行う。また、主要な国際会議に出席し、最新の研究成果を収集するとともに、一流の研究者と研究討論を行う。

４．研究成果

本研究では、以下のような成果が得られた。

(1) 否認不可署名方式は、ソフトウエアのライセンス発行、電子現金、電子投票、電子オークション、電子入札など、多くの応用を有する。たとえば、電子入札において、応札者は入札値 m に対する入札者の署名 σ を必要とする。しかし、不正な応札者は、その(m, σ)を競争相手に教えてしまうかもしれない。この場合、σ を否認不可署名とすれば、この相矛盾する問題を容易に解決することができる。

(2) では、安全性が証明されている否認不可署名方式は、上記のように複雑なプロトコルに組み込まれた場合でも、その安全性は保たれるのであろうか。この問題は、その重要性にもかかわらず、従来、研究されていなかった。

(3) 本研究では、まず、否認不可署名方式の汎用結合可能(UC)安全性を定義した。すなわち、この UC 安全性を満たす否認不可署名方式は、どのように複雑なプロトコルに組み込まれた場合でも、その安全性が維持されることが保証される。

(4) 次に、stand alone な setting において、従来の安全性の定義の問題点を指摘するとともに、それを解決する新しい安全性の定義を示した。

(5) さらに、(3)と(4)で示した２つの安全性の定義が等価であることを証明した。この結果は、(有名な Chaum 方式を含む）従来知られている全ての方式は、UC 安全であることを意味している。すなわち、それらは、より複雑なプロトコルに組み込まれたとしても、安全性が維持されることとなる。

(6) 以上の成果は、computer science の分野において、FOCS, STOC と並び最もレベルの高い国際会議の一つである ICALP 2008 に採択されるに至った。

(7) 本研究では、次に、発行済みの否認不可署名を通常のデジタル署名に変換することが可能な方式を、標準モデルにおいて始めて開発した。

(8) RSA 暗号は、現在、最もポピュラーな公開鍵暗号である。したがって、RSA 暗号に基づく否認不可方式の開発は、実用的にも理論的にも、非常に重要である。従来、RSA 否認不可方式は、ランダムオラクルモデルという極度に理想化されたモデルにおいて開発されてきた。報告者らは、Asiacrypt 2006 において、標準モデルにおける方式を初めて提案した。

(9) 本研究では、まず、上記の報告者らの方式は、invisibility という安全性を満たさないことを示した。Invisibility とは、署名文 σ が正しい署名文かどうか全くわからない、という性質である。

(10) 次に、新たな RSA 否認不可方式を示し、その安全性を標準モデルにおいて証明した。偽造不可能性は強 RSA 仮定の下で成り立ち、ivisibility は DNR 仮定の下で成り立つ。

(11) 本方式は、以下のように表される。

(秘密鍵) 大きな素数 p_1, q_1, p_2, q_2、
(公開鍵)
$N_1=p_1q_1, N_2=p_2q_2$, 及びハッシュ関数 H。
ただし、$N_1<N_2$

(平文)　m
(署名生成)
まず、$r \in Z_{N2}$ をランダムに選び、
$y^e = H(m||r^{N2} \bmod N_2) \bmod N_1$
となる素数 e、及び $y \in Z_{N1}$ を求める。
次に、
$t = r^{N2}(1+yN_2) \bmod N_2$
を計算する。最後に、
$\sigma = (e,t)$
を署名文とする。

(確認プロトコル)
入力 m 及び $\sigma=(e,t)$に対し、署名者は、
$y^e = H(m||t \bmod N_2) \bmod N_1$　(1)
$t = r^{N2}(1+yN_2) \bmod N_2$　(2)
となる $r \in Z_{N2}$、$y \in Z_{N1}$ が存在することを零知識証明で証明する。

(否認プロトコル)
入力 m 及び $\sigma=(e,t)$に対し、署名者は、
$y_1^e = H(m||t \bmod N_2) \bmod N_1$
$t = r^{N2}(1+y_2N_2) \bmod N_2$
$y_1 \neq y_2$
となる $r \in Z_{N2}$、$y_1 \in Z_{N1}$、$y_2 \in Z_{N2}$ が存在することを零知識証明で証明する。

(12) 各署名文 σ を通常のデジタル署名に変換することが可能な方式を、選択的 convertible 否認不可署名方式という。また、全ての σ をデジタル署名に変換することが可能な方式を、all convertible 否認不可署名方式という。本研究では、上記の RSA 否認不可方式は、選択的 convertible であり、かつ all convertible であることも示した。

(選択的 conversion)
あるメッセージ m に対する署名文 $\sigma=(e,t)$ を通常のデジタル署名に変換したいとき、署名者は r を公開する。
検証者は、まず、r 及び式(2)から y を計算する。次に、その y が式(1)を満たすことをチェックする。

(ALL conversion)
全ての署名文を通常のデジタル署名に変換したいとき、署名者は p_2, q_2 を公開する。
検証者は、まず、p_2, q_2 及び式(2)から y を計算する。次に、その y が式(1)を満たすかどうかチェックする。

(13)さらに、RSA 否認不可方式の匿名性について検討した。匿名性とは、署名文 σ の発行者が誰なのかわからない、という性質である。RSA 暗号に基づく暗号系においては、公開鍵 N がユーザによって異なるため、匿名性を満たす方式を構成するのは簡単ではない。そこで、従来、２つの方法が提案されている。一つ目の方法は、padding 等により、ある一定の長さになるまで署名文を長くする方法である。２つ目の方法は、乱数をうまく選び直すことにより、署名文の長さをある一定の長さになるまで短くする方法である。しかし、一つ目の方法では、署名文の長さが長くなってしまう。また、二つ目の方法では、計算量が増加してしまう。

(14) 一方、Lenstra は、N の先頭の半分のビットを任意に指定されたビット列となるような N=pq の生成法を示している。ここで、p,q は大きな素数である。

(15) 本研究では、この Lenstra の方法を利用すれば、匿名性を有する RSA 否認不可方式を簡単に実現できることを示した。たとえば、全ユーザが N の先頭の 83 ビットをある指定されたビット列になるように、それぞれの N を Lenstra の方法に従って生成すれば、匿名性について 80 ビット安全性を達成できる。

(16)本 RSA 否認不可方式を設計するツールとして、twin moduli RSA 問題を導入し、強 twin moduli RSA 仮定は単なる RSA 仮定と等価であることを証明した。この成果は、否認不可方式の枠を超え、多くの応用を有するものと期待される。ここで、RSA 仮定とは、(N,e,y)から $y=x^e \bmod N$ となる x を求めることは難しい、という仮定である。twin moduli RSA 問題とは、$(N_1, N_2, e_1, e_2, y_1)$から、$y_1=x^{e1} \bmod N_1$, $y_2=x^{e2} \bmod N_2$ となる y_2 を求めよ、という問題である。強 twin moduli RSA 仮定とは、(z_1, z_2)を質問したときに、$z_1=a^{e1} \bmod N_1$, $z_2=a^{e2} \bmod N_2$ となる a が存在さればそのような a を返してくれるオラクルが存在したとしても、twin moduli RSA 問題は難しい、という仮定である。

(17) 以上の成果は、AfricaCrypt 2009 という国際会議に採択された。また、電子情報通信学会論文誌においても、現在、条件付採択となっている。

(18)最後に、本研究では、離散対数問題に基づく否認不可方式について検討した。離散対数仮定は、RSA 仮定とともに、現在、最もポピュラーな暗号学的仮定である。したがって、離散対数問題に基づく否認不可方式の開発は、実用的にも理論的にも、非常に重要である。

(19)従来、離散対数問題に基づく否認不可方式は、ランダムオラクルモデル及び標準モデルにおいて開発されてきた。しかし、(12)に示したような意味での convertible な方式は、従来、しられていない。

(20)本研究では、標準モデルにおいて、選択

的 conversible かつ all convertible な方式を示し、標準モデルにおける安全性を証明した。提案方式は、そのような性質を有する最初の方式である。また、署名サイズも短く、確認プロトコル、否認プロトコルも非常に効率がよい。安全性は、strong DH 仮定、及び decision linear 仮定の下で証明されている。

(21)本方式は、以下のように表される。

G を位数が素数 q の群、P をその生成元とする。また、$e:G\times G\rightarrow G_T$ を、双線形成を満たすペアリング関数とする。

(秘密鍵) $x, x_1, x_2 \in Z_q$

(公開鍵) $Q=xP$, $Q_1=(1/x_1)P$, $Q_2=(1/x_2)P$,
及びハッシュ関数 H.

(平文) m

(署名生成) まず、$r_1, r_2 \in Z_q$ をランダムに選び、

$$U_1=r_1Q_1,\quad U_2=r_2Q_2 \qquad (3)$$

を計算する。次に、s をランダムに選び、

$$T=1/(x+s)\cdot H(m||U_1||U_2) \qquad (4)$$

$$U_3=(r_1+r_2)P+T \qquad (5)$$

を計算する。最後に、$\sigma=(s, U_1, U_2, U_3)$を署名文とする。

(確認プロトコル)

入力 m 及び$\sigma=(s, U_1, U_2, U_3)$に対し、署名者は、式(3),(4),(5)及び $Q=xP$ を満たす(x,r_1,r_2)が存在することを零知識証明で証明する。

(否認プロトコル)

入力 m 及び$\sigma=(s, U_1, U_2, U_3)$に対し、式(4),(5)が成り立たないので、

$$(x+s)(U_3-(r_1+r_2)P-H(m||U_1||U_2))\neq 0$$

そこで、署名者は、乱数 $r\in Z_q$ を選び、

$$V=r(x+s)(U_3-(r_1+r_2)P-H(m||U_1||U_2))$$

を検証者に送る。次に、定式、式(3)及び $Q=xP$ を満たす(r, x, r_1, r_2)が存在することを零知識証明で証明する。

(All conversion)

全ての署名文を通常のデジタル署名に変換したいとき、署名者は x_1, x_2 を公開する。

検証者は、まず、

$$T=U_3-x_1Q_1-x_2Q_2$$

により、T を求める。次に、

$$e(T, X+sP)=e(H(m||U_1||U_2)), P)$$

が成り立つことをチェックする。

(選択的 conversion)

あるメッセージ m に対する署名文$\sigma=(s, U_1, U_2, U_3)$を通常のデジタル署名に変換したいとき、署名者は、まず、

$$T=U_3-x_1Q_1-x_2Q_2$$

を公開する。次に、

$$P=x_1Q_1,$$

$$P=x_2Q_2$$

$$U_3-T=x_1Q_1+x_2Q_2$$

を満たす(x_1,x_2)が存在することを示す非対話型証明πを公開する。そのような非対話型証明πは、Groth and Sahai の結果を利用し、効率よく構成することができる。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

① Le Trieu Phong, Kaoru Kurosawa and Wakaha Ogata: New RSA-Based (Selectively) Convertible Undeniable Signature Schemes. AfricaCrypt 2009, LNCS 5580, pp.未定(2009) 査読有り

② Kaoru Kurosawa and Jun Furukawa: Universally Composable Undeniable Signature. ICALP (2), LNCS 5126, pp.524-535 (2008) 査読有り

〔学会発表〕（計 1 件）

① Le Trieu Phong, Kaoru Kurosawa and Wakaha Ogata: New RSA-Based (Selectively) Convertible Undeniable Signature Schemes. 2009 年暗号と情報セキュリティシンポジウム (SCIS 2009)、平成 21 年 1 月 22 日、滋賀県大津市大津プリンスホテル

６．研究組織

(1)研究代表者

黒澤 馨 (KUROSAWA KAORU)

茨城大学・工学部・教授

研究者番号：60153409

(2)研究分担者

なし

(3)連携研究者

なし