様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　２　日現在

機関番号：　３２６５７
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１６０

研究課題名（和文）時限Certificateless暗号の構成法の研究

研究課題名（英文）Study on Timed-Release Certificateless Encryption

研究代表者
齊藤　泰一（SAITO, TAIICHI）

東京電機大学・工学部・教授

研究者番号：２０３８５４８８

交付決定額（研究期間全体）：（直接経費）　　1,200,000円

研究成果の概要（和文）：Timed-Release暗号は、送信者が設定した時刻のより後の時刻にのみ、受信者が暗号文を復号できるメカニズムである。本研究では、このメカニズムを備えるCertificateless暗号である時限Certificateless暗号の概念と安全性を定義した。さらにその安全性を満たす時限Certificateless暗号の一般的構成法を示した。

研究成果の概要（英文）：Timed-Release Encrtption(TRE) is an encryption mechanism that allows a reciever
to decrypt a ciphertext only after the time that a sender designates. We proposed a notion of certificateless encryption scheme with TRE encryption mechanism, Timed-Release Certificateless Encryption(TRCLE), and defined its security model. Moreover we presented a secure generic construction of TRCLE.

研究分野：　情報セキュリティ

キーワード：　時限Certificateless暗号　Certificateless暗号　Identity-Based暗号　公開鍵暗号　one-time署名

１．研究開始当初の背景

Timed-Release 暗号 (Timed-Release Encryption、 TRE) は暗号文を復号できる時刻を暗号化の際に指定できる暗号方式である。応用としては、 ネットワークを利用した新作コンテンツの配信、オンライン試験における問題配布など、受信者の復号時刻が重要な意味を持つものがある。TRE に関しては様々な研究が行われており、そのほとんどは、公開鍵暗号 (Public-Key Encryption :PKE) に TRE の機能を持たせた公開鍵型 Timed-Release 暗号 (Timed-Release PublicKey Encryption :TRPKE) に関するものである。しかし TRPKE は、PKE と同じく、暗号化するために受信者の公開鍵を事前に入手する必要がある。そのため、認証局等の公開鍵の正当性を保証する機関が必要である。それに対し ID ベース暗号 (Identity-Based Encryption :IBE) に TRE の機能を持たせた、時限式 ID ベース暗号 (Timed-Release Identity-Based Encryption :TRIBE) が我々によって提案された①。 TRIBE では IBE と同じく公開鍵として受信者の識別子 ID(メールアドレスなど) を用いるため、公開鍵の事前入手・認証が不要である。

しかし，時刻鍵がブロードキャストされた後は、ユーザの秘密鍵を生成する鍵生成センタ (Key Generation Center :KGC) が全ユーザの暗号文を復号することが可能であるという安全性上の問題があった。つまり、KGC はすべてのユーザの秘密鍵を生成することができるという大きな権限を持つという問題があった。

２．研究の目的

上記のような問題を解決するため、次のような目的で技術開発を行った。

（１）KGC に対する安全性：ID ベース暗号系における KGC への権限の集中の問題を解決するため Certificateless 暗号系の研究がされている。Certificateless 暗号系においては、KGC はユーザの秘密鍵の代わりに部分秘密鍵とよばれるデータを生成する。ユーザは受け取った部分秘密鍵を元に自分の秘密鍵を生成する。Certificateless 暗号系は、KGC は部分秘密鍵を生成することができるが、それを元にしてユーザによって作られた秘密鍵の情報は得ることができないという安全性が求められる。

（２）Multiple Encryption に基づく一般的構成法：ID ベース暗号系である TRIBE に関する研究の構成法は Dodis と Katz による ″Chosen-Ciphertext Security of Multiple Encryption″②の Multiple Encryption の構成方法を用いて２つの ID ベース暗号を組み合わせるものだった。これら構成方法の時限 Certificateless 暗号への拡張を目標とする。

３．研究の方法

（１）時限 Certificateless 暗号の安全性定義

まず時限 Certificateless 暗号 (Timed-Release Certificateless Encryption :TRCLE)とその安全性の定義を行う。 TRCLE では、 KGC、時刻サーバ (Time-Server :TS)、ユーザ (受信者)、アウトサイダ (公開鍵をすりかえようとする第三者) の不正に対する安全性を定義する。特に、不正な KGC に対する安全性を定義することにより、KGC への権限の集中の問題を解決できる TRCLE の性質を明らかにする。

（２）時限 Certificateless 暗号の構成法

Dodis,Katz の Multiple Encryption の構成方法を応用した TRCLE の構成方法を提案する。また、基礎と構成要素としては、ID ベース暗号、公開鍵暗号、Certificateless 暗号などを想定している。なるべく少ない構成要素・仮定から構成できる構成法を提案する。

４．研究成果

（１）時限 Certificateless 暗号の安全性定義

時限 Certificateless 暗号(Timed-Release Certificateless Encryption: TRCLE) のエンティティは鍵生成センター (Key Generation Center :KGC)、時刻サーバ (Time-Server :TS)、送信者、受信者から構成される。TRCLE は、 CLE と同じく CA が不要であり、 KGC は部分秘密鍵と呼ばれる秘密鍵の一部分のみを生成し、最終的な秘密鍵はユーザ自身が生成する。TRCLE では部分秘密鍵と秘密鍵、時刻鍵の３つの鍵が揃ったときにのみ、復号できる必要がある。KGC は、部分秘密鍵という、暗号文の復号に用いる鍵の一部を ID から生成し各受信者に配布する。TS は時刻鍵という時刻に対応する鍵を生成し、システム全体にブロードキャストする。送信者は、受信者の ID,公開鍵、復号を許可する時刻情報を用いて平文を暗号化する。受信者は、部分秘密鍵、受信者のみが知っている秘密鍵、時刻鍵を用いて暗号文を復号する。

また、TRCLE では認証局が存在しないため、外部者による公開鍵のすり替えが起こることが想定できる。そのため、以下の４つのエンティティに対する安全性を定義する。

KGC に対する安全性：任意の部分秘密鍵が利用できても、ID に対応する秘密情報なしでは暗号文からメッセージの情報を得ることができない

TS に対する安全性：任意の時刻鍵を利用できても，ユーザ秘密鍵無しでは暗号文からメッセージの情報を得ることができない

受信者に対する安全性：ユーザ秘密鍵を持っていても，時刻鍵無しでは暗号文からメッセージの情報を得ることができない

外部者に対する安全性： 公開鍵のすり替えを行っても、TS からブロードキャストされる時刻鍵だけでは暗号文からメッセージの情報を得ることができない (外部者には公開鍵

のすり替えを許す)

KGC に対する安全性については、攻撃者に TS の秘密鍵を与えるという強い安全性を定義とした。そのため、TS に対する安全性は KGC に対する安全性から導かれる。

（２）Multiple Encryption に基づく一般的構成法

提案する TRCLE の構成法は１種類の公開鍵暗号方式、２種類の ID ベース暗号、１種類の one-time 署名の組み合わせである。KGC は ID ベース暗号の鍵生成アルゴリズムを用いて、ID から部分秘密鍵を生成する。送信者は公開鍵暗号の鍵生成アルゴリズムを用いて、公開鍵を秘密鍵を生成し、その秘密鍵と部分秘密鍵の組を TRCLE の秘密鍵とし、その公開鍵を TRCLE の公開鍵とする。また、TS は時刻 t において、ID ベース暗号の鍵生成アルゴリズムを用いて、t に対する時刻鍵を生成する。

送信者は、まず、one-time 署名、署名鍵と検証鍵を生成する。次に、ビット毎排他的論理和を取ると平文になるようなランダムなビット列を３つ生成する。１つ目のビット列と検証鍵の連結を、受信者の ID に基づき ID ベース暗号で暗号化する。２つ目のビット列と検証鍵の連結を、復号させたい時刻を ID として ID ベース暗号で暗号化する。３つ目のビット列と検証鍵の連結を、公開鍵暗号で暗号化する。そして、２つの ID ベース暗号の暗号文と１つの公開鍵暗号の暗号文の連結に対し、one-time 署名を生成する。TRCLE の暗号文は、３つの暗号文と受信者 ID と復号させたい時刻 t と、one-time 署名の検証鍵と、one-time 署名データの組である。

受信者は、TRCLE の暗号文を手に入れたら、まず、one-time 署名の検証鍵を用いて、one-time 署名データが、２つの ID ベース暗号の暗号文と１つの公開鍵暗号の暗号文の連結に対する署名になっていることを検証する。次に、１つ目の ID ベース暗号の秘密鍵により１つ目の暗号文を復号し、１つ目のビット列と one-time 署名の検証鍵を取り出す。次に、２つ目の ID ベース暗号の秘密鍵である時刻 t に対する時刻鍵により２つ目の暗号文を復号し、２つ目のビット列と one-time 署名の検証鍵を取り出す。次に、公開鍵暗号の秘密鍵により、公開鍵暗号の暗号文を復号し、３つ目のビット列と one-time 署名の検証鍵を取り出す。それぞれの one-time 署名の検証鍵が一致したならば、３つのビット列のビット毎排他的論理和を取り、そのビット列を平文として出力する。

このように構成した TRCLE は、公開鍵暗号が選択暗号文攻撃に対する識別不可能性を持ち、one-time 署名が選択文書攻撃に対する強存在的偽造困難性を持つならば、不正な KGC に対しても与えられた暗号文から平文の情報が漏れないことが証明できた。そして、この不正な KGC に対する安全性から不正な TS に対する安全性も証明できる。

また、TS が利用する２つ目の ID ベース暗号が選択暗号文攻撃および適応的 ID 攻撃に対して識別不可能性を持ち、one-time 署名が選択文書攻撃に対する強存在的偽造困難性を持つならば、不正な受信者に対しても与えられた暗号文から平文の情報が漏れないことが証明できた。

そして、KGC が利用する１つ目の ID ベース暗号が選択暗号文攻撃および適応的 ID 攻撃に対して識別不可能性を持ち、one-time 署名が選択文書攻撃に対する強存在的偽造困難性を持つならば、公開鍵のすり替えが可能な外部者に対しても与えられた暗号文から平文の情報が漏れないことが証明できた。

これらの証明はすべて標準モデルでおこなわれた。１つ目の ID ベース暗号と２つ目の ID ベース暗号で、同じ方式を用いると、依拠する安全性を少なくすることができる。

KGC に対する安全性について、その概要を述べる。１つめのチャレンジャーは２つの ID ベース暗号の公開パラメータとマスター秘密鍵が与えられる。そのため、TRCLE のゲームにおいては KGC と TS に関するクエリに対して全て答えることができる。さらにチャレンジャーは、公開鍵暗号の選択暗号文攻撃の環境で識別不可能性を破るゲームでの攻撃者をシミュレートしようとする。攻撃者からの公開鍵要求のいずれかにランダムに、このゲームで与えられる公開鍵をセットする。それ以外の公開鍵要求には、チャレンジャーが自分で公開鍵と秘密鍵の生成を行い、生成した公開鍵をセットする。公開鍵暗号のゲームで与えられた公開鍵を用いてチャレンジ暗号文を作ることになったと仮定する。TRCLE のゲームのチャレンジで２つの平文が与えられたとき、２つのランダムビット列を作り、それらと平文それぞれのビット毎排他的論理和を取る。チャレンジャーは自分で生成した one-time 署名の検証鍵をそれぞれに連結して、公開鍵暗号のゲームのチャレンジャーに２つの平文とし渡し、チャレンジ暗号文を得る。それと、上の２つのランダムビット列と検証鍵を連結して２つの ID ベース暗号で暗号化したものに対して、one-time 署名を生成すると、それらは正しい TRCLE の暗号文になっているため、TRCLE のチャレンジ暗号文として出力できる。ここまでのシミュレーションで、one-time 署名の偽造が起こらなければ完全にシミュレートができるため、TRCLE の KGC に対する安全性は公開鍵暗号の選択暗号文攻撃に対する識別不可能性に帰着される。

具体的な方式としては、２つ ID ベース暗号では decisional Bilinear Diffie-Hellman 仮定に基づく Waters の方式③を用い、公開鍵暗号としては Cramer-Shoup 暗号を用いるのが効率的である。ただし、Cramer-Shoup 暗号を Waters の方式の定義体の乗法群上で構成すると、安全性の根拠である decision Diffie-Hellman 仮定が破られてしまう可能性がある。

提案した TRCLE では one-time 署名を用いている。例えば Waters の方式を用いて暗号文が２つの点と１つの座標を表すため 2048*5 ビットであるとする。Lamport の one-time 署名を SHA-256 で構成するとすると、署名長は 256*2048*5 ビットになってしまう。他の one-time 署名もデータ量に関しては、効率的ではない。one-time 署名の代わりに、通常のディジタル署名を用いることは今後検討する価値がある。

<引用文献>
①押切 徹、齊藤 泰一、時限式 ID ベース暗号、情報処理学会論文誌、Vol.55、 No.9、2014、1964-1970
②Dodis, Y.、Katz, J.、Chosen-Ciphertext Security of Multiple Encryption、Lecture Notes in Computer Science、Vol.3378, 2005、188-209
③Waters, B.、 Efficient Identity-based Encryption Without Random Oracles 、EUROCRYPT'05、Lecture Notes in Computer Science、Vol.3494 2005、114-127

５．主な発表論文等
〔雑誌論文〕（計２件）
① Toru Oshikiri 、 Taiichi Saito 、Timed-Release Certificateless Encryption、International Journal of Advanced Computer Science and Applications (IJACSA)、査読有、Vol.6、 Issue 2、2015、
DOI ： 10.14569/IJACSA.2015.060239
② Toru Oshikiri 、 Taiichi Saito 、Timed-Release Hierarchical Identity-Based Encryption、International Journal of Advanced Computer Science and Applications (IJACSA)、査読有、Vol.5、Issue 11、2014、
DOI ： 10.14569/IJACSA.2014.051125

〔学会発表〕（計２件）
① 押切徹、齊藤泰一、ID ベース型 Timed-Release 暗号、The 10th IEEE Tokyo Young Researchers Workshop、A-1、2013
② 押切徹、齊藤泰一、Timed-Release Certificateless 暗号、コンピュータセキュリティシンポジウム 2013、 CSS2013-1C2-1、2013

６．研究組織
(1)研究代表者
齊藤泰一（SAITO TAIICHI）
東京電機大学・工学部・教授
研究者番号：20385488
(2)研究分担者
なし
(3)連携研究者
なし
(4)研究協力者
押切徹（OSHIKIRI TORU）