秘密情報を“安全に”分散管理する技術

秘密情報を“安全に”分散管理する方法として，しきい値暗号という技術が存在する．安全性を保ったまま効率的に演算が可能なしきい値暗号の構成方法を研究の対象とし，それを実現するRSA方式のしきい値暗号を考案した．なお，本研究は横浜国立大学大学院 環境情報研究院 四方 順司助教授との共同研究により実施した．

石原 武（いしはら たける）　青野 博（あおの ひろし）　本郷 節之（ほんごう さだゆき）

1. まえがき

昨今の移動端末は，i-mode FeliCaの電子マネーをはじめとする重要なデータを扱うようになってきた．データは，ICカード内に入れたら安全，というわけではなく，“いかに安全に取り出すか”が重要である．例えばPINコードによる認証を行って取り出す場合，安全性はICカードではなくPINコード自体でしか保てない．PINコードは手軽ではあるが，安全性に限界があるため，最近では銀行のATMでもPINコードよりも安全な認証方法を取り入れている例もある．このような背景から，安全性を証明できるような情報の管理方法に注目が集まっている．

安全な情報管理方法の1つとして秘密情報を分割して保存する秘密分散法[1][2]がある．例えば保護者から子供に家の電子キーを渡すような場合，秘密分散法を用いると，いくつかの所持品に電子キーの分割したデータを持たせて安全性を高めるといったことができる．しかしながら従来の秘密分散法では，秘密情報の量に比例して分割後のデータも増えてしまい，安全性をより高めるためのICカードとの併用に制約を与えてしまう．また，分割したデータをいかに届けるかといった問題も存在する．そこで，これらの課題を解決するため秘密分散法の一種である，しきい値暗号[3]～[6]に関する検討を行った．しきい値暗号では，分散鍵と呼ばれる一定長のデータのみを秘密にしておけば十分であり，分散鍵を所持品にあらかじめ分散しておくことで秘密分散法の問題を解決できる．

本研究は，分散管理の基礎技術となるしきい値暗号について安全性を確保しつつ，計算や通信の効率性を高めることを目的に進めてきた．その結果，いくつかの成果を得ることができたが，そのうち本稿では研究の主目的であったRSA（Rivest-Shamir-Adleman）方式[7]のしきい値暗号について述べる．提案方式は文献[8]での仮定を基にしているものの，RSAを基にした方式としては，世界で初めて安全性が証明されたしきい値暗号である．

2. 既存技術とその課題

2.1 しきい値暗号

しきい値暗号は例えば**図1**のように利用される．図1は保護者から子供に渡した家の電子キーの使い方を示している．まず，保護者は電子キーを暗号化し，暗号文を作成する．次に，同一の暗号文を子供の携帯端末とバック内のICカードにそれぞれ送信する．ICカードは内部にある分散鍵と呼ばれる秘密情報を用いて部分復号情報を作成する．子供は部分復号情報を集めることにより電子キーを復号できる．図1では分散鍵の数を2，復号に必要な部分復号情報の数も2としたが，分散鍵および復号に必要な部分復号情報の数は，それぞれ任意に選べるため柔軟性が高い．

しきい値暗号の動作原理のイメージを，**図2**を用いて説明する．利用者は公開鍵を用いて平文（図1での家の電子キーに相当）の暗号化（図2で平文を鍵付きの箱にしまうことに相当）を行い，暗号文を計算する．暗号化は公開鍵を用いることにより誰でも可能であるが，復号は分散鍵を用いて初めて行える．しきい値暗号では，分散鍵を用いて暗号文を解読すると平文が変形した形で出てくるように工夫されている．この出力されたデータを部分復号情報という．分散鍵を巧妙に細工しているため，部分復号情報1つでは平文が原形をとどめないほど変形した状態であり，平文に関する情報が手に入らない．しかし，部分復号情報を2つ集めることにより平文が復元できる．この巧妙な細工はShamir法[2]を用いることにより可能となる．

2.2 課題

しきい値暗号の検討すべき課題として，安全性と計算や通信の効率化に着目した．また，利便性，利用環境（安全

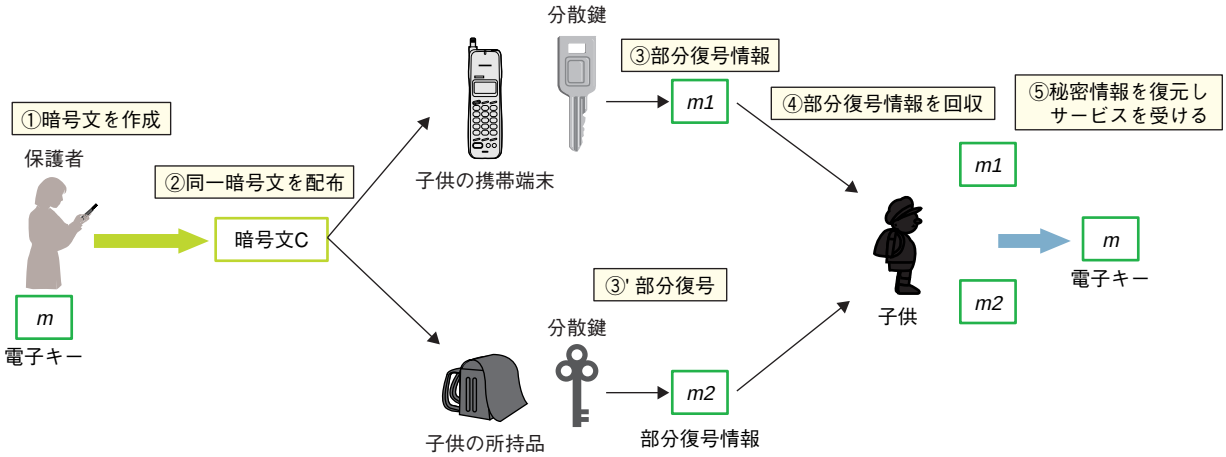


図1　しきい値暗号の利用方法

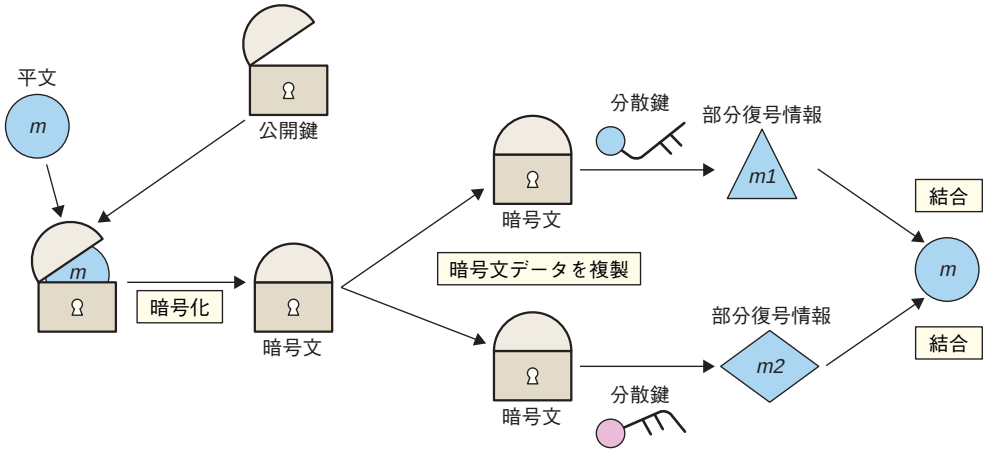


図2　しきい値暗号のイメージ

な通信路をどの程度仮定するか，第三者機関をどの程度信頼してよいか）なども検討する必要があるが，本研究では，基礎となるしきい値暗号そのものの安全性と，計算や通信の効率に的を絞って検討することとした．特に計算の効率については，携帯端末でも十分に実現可能な方式を目指した．安全性についてはこれまでの多数の研究と同様に，安全であることを主張するための仮定の妥当性，および選択暗号文攻撃*1という攻撃が行われても安全性が保てるかどうか，という2点について検討した．さまざまなアプリケーションにおいて暗号を用いる場合には，選択暗号文攻撃に対しても安全でなければならないことが知られており，この攻撃に対しても情報が全く漏れないような安全な方式を目指した．

しきい値暗号は秘密分散法の一種であるが，公開鍵暗号の一種としても知られている．公開鍵暗号にはいくつかの代表的な方式があるが，その中でも一番よく使われているのがRSAと呼ばれる方式であり，実装の仕方を工夫することにより暗号化の速度が他の方式と比較して早くなる．また鍵のサイズ，通信量において他の方式と比較しても十分実用的であり，移動端末でも実現可能である．しかしながら，公開鍵暗号方式のRSA方式を基に単純にしきい値暗号を構成した場合には，選択暗号文攻撃に対して安全性が保障されず，安全なRSA方式のしきい値暗号は存在しなかった．そこで，選択暗号文攻撃に対して安全性を証明できるRSA方式のしきい値暗号の考案を目指し，研究を行った．

2.3　提案方式の基となった公開鍵暗号方式

今回提案する方式は，公開鍵暗号における方式[9]を基に構成を行った．まず，公開鍵暗号の動作原理のイメージを，**図3**を用いて説明する．利用者は，公開鍵を用いて平文を暗号化する．ここでの公開鍵は，しきい値暗号における公開鍵と同様である．しきい値暗号と違って復号のための鍵は1つしかないために容易に復号が行える反面，復号鍵を奪われると暗号文を復号できないばかりか，復号鍵を不正に入手した人に暗号文の復号結果を知られてしまう面がある．

次に，公開鍵暗号における選択暗号文攻撃のイメージを説明する．選択暗号文攻撃において攻撃者は暗号文とよく似たデータ（以下，“暗号文もどき”と呼ぶ）を復号させることを試みる．暗号文もどきは攻撃者にとって都合が良

＊1　選択暗号文攻撃：攻撃者が解読を目的とする暗号文以外の，任意の暗号文の復号結果を得られる解読攻撃．

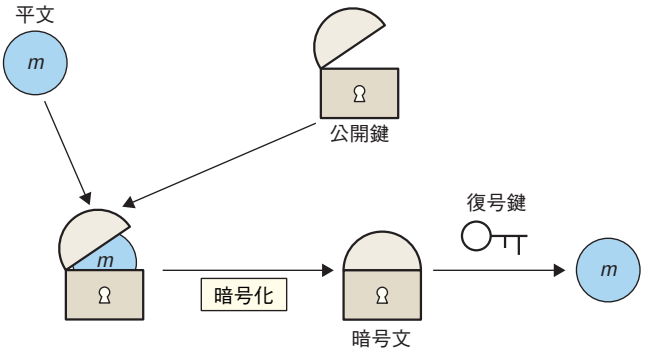


図3　公開鍵暗号のイメージ

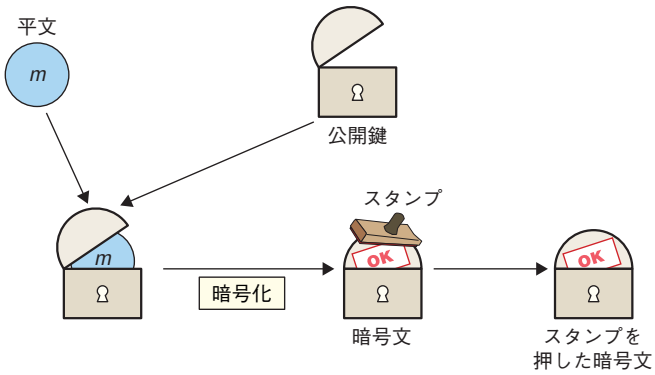


図4　安全性を保障する工夫

いように加工されている可能性があり，暗号文もどきを復号してしまうと攻撃者に復号鍵の情報を与えてしまう可能性がある．このようなことが無いように，暗号文もどきではないことを確認した後に，暗号文を復号することが重要である．しかし，暗号文もどきを見ただけでは暗号文であるか暗号文もどきであるのか一般には区別できないため，暗号文もどきを復号してしまう可能性があり，問題となる．選択暗号文攻撃に対する安全性を保障するための一手法としてスタンプを用いた工夫[9]について，**図4**を用いて説明する．文献[9]では公開鍵に細工を行い，暗号文もどきにはスタンプを押せないようにしている．このときスタンプが押されていないものは，復号しなければ安全性が確保できる．ここで暗号文もどきに対してスタンプを押すことは，未解の数学的な難問を解くことに相当し[10]，スタンプが押してあれば暗号文もどきでないことを保障している．

3. 提案方式

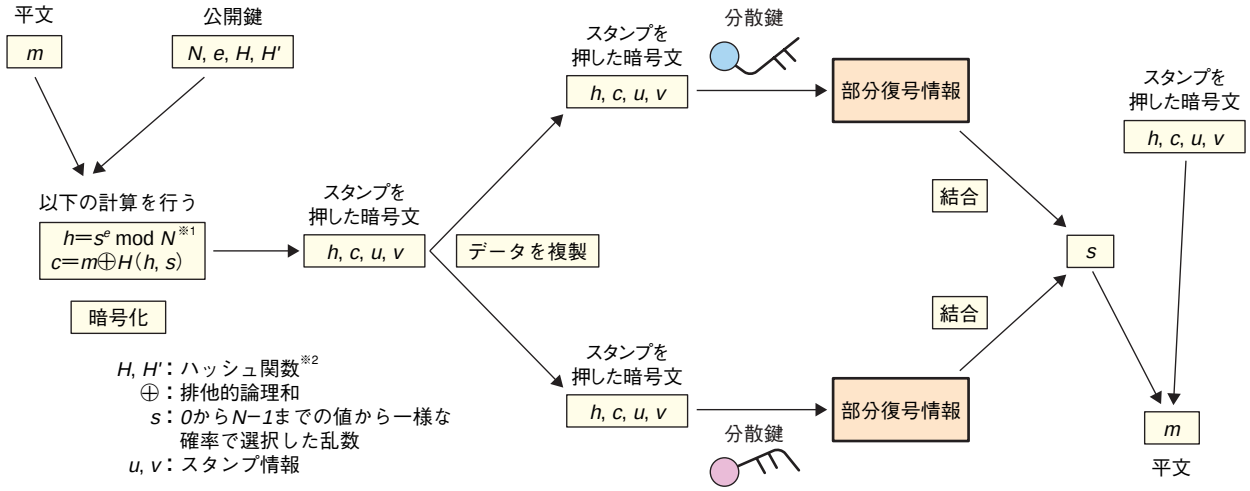
本研究では，上記のスタンプを用いる手法をしきい値暗号に適用しただけでなく，同手法よりも暗号文もどきか否かの判断条件がより厳しい新しい手法を提案した．厳しい条件を設定した要因は，しきい値暗号において平文そのものではなく中身を変形させた部分復号情報を取り出されるため，攻撃者に都合の良い暗号文の種類が増加することが分かったからである[11]．しきい値暗号において，攻撃者にとって都合の良い暗号文すべてにスタンプが押せないようにしていることが，RSA方式のしきい値暗号を作成する際のポイントである．この条件を無視してスタンプを押すことはやはり未解の数学的な難問を解くことに相当し，不可能であることが証明されている[10]．

今回提案する方式のデータの流れを**図5**に示す．鍵生成は，相異なる強い素数[*2] p, qを選択，$N=pq$を計算，さらに素数eを選択する．ここで，暗号化においてh, cの計算が暗号化に相当し，u, vを計算することがスタンプを押すことに相当している（u, vの作成方法は文献[10]とおおよそ同様である）．暗号文の復号はそれぞれ，「検証」，「部分復号」，「結合」という3つのプロセスに分かれている．まず，スタンプがきちんと押されているか検証し，正しく押してあれば正しい暗号文であると判定，これにより，正しい暗号文であることが確認できた場合にのみ部分復号を行う．最後に部分復号情報を結合して平文を復元する．部分復号および結合の方法は文献[5]とほぼ同様のため詳細は割愛する．

本方式と文献[9]との主な違いを簡単に紹介する．暗号文もどきのデータ（h', c', u', v'）に対して$u=u'$が成立する場合，選択暗号文攻撃の特徴から復号結果が攻撃者に与えられる．本方式ではH'の入力を文献[9]よりも増やして$u=u'$の成立をより難しくしていることが，文献[9]の方式に比べて厳しい条件の下でしかスタンプを押せないようにしていることに相当する．

提案方式の利点は以下のとおりである．まず，安全性については他の既存のしきい値暗号と同様に選択暗号文攻撃に対して全く情報が洩れず非常に安全性が高い．また，安全性の根拠となる仮定については，より妥当な仮定ほど安全性が高まることが知られている．そこで，本共同研究では決定問題[*3]の困難性と呼ばれる，他の多くのしきい値暗号で用いている仮定よりもより妥当な仮定に安全性の根拠をおいた方式を検討した．安全性に関する証明は文献[11]にて紹介されているため詳細は割愛する．次に効率に関する利点を述べる．提案方式は，RSA方式に基づいていることから，暗号化の計算量は他のしきい値暗号方式と比べても小さく抑えることができる．通信量，暗号文のサイズ，各移動端末が持つ分散鍵のサイズについても，それぞれ既存方式のなかで最も効率が良い方式と同程度である．また，既存の技術との親和性が高いという点でも優れている．

＊2　強い素数：素数pが強い素数であるとは，$p=2p'+1$なるp'も素数となることをいう．
＊3　決定問題：回答方法が記述式の問題のこと．答えの候補が与えられたとき，その正誤を判定する判定問題に比べて一般的に難しい．



※1　$x \bmod N$：xをNで割った余りを表す．
※2　ハッシュ関数：入力から一定長のデータを出力する一方向性関数．代表的なものにSHA-1がある．

図5　提案方式の流れ図

なお，提案方式は部分復号に関して比較した場合，最も効率が良い文献[6]の方式より計算量が増加するが，分散情報の数が少なければその差は小さく，通常の利用範囲ではあまり問題ではないと考えられる．

4. あとがき

本研究では安全性が証明されたRSA方式のしきい値暗号を考案した．この考案したしきい値暗号を用いることによって，移動端末において安全に秘密情報の分散管理を行うことが可能となる．今後は文献[8]での仮定を用いずとも安全性を証明できるような方式を考えていく予定である．

文　献

[1] G. Blakely:“Safeguarding cryptographic keys,”Afips 1979 Nat. Computer Conf., Vol. 48, Afips Press, pp. 313-317, 1979.
[2] A. Shamir:“How to Share a Secret,”Commun. ACM, Vol. 22, No. 11, pp. 612-613, 1979.
[3] Y. Desmedt:“Society and Group Oriented Cryptography: A New Concept,”In Crypto87, LNCS 293, Springer-Verlag, pp. 120-127, 1987.
[4] P. A. Fouque and D. Pointcheval:“Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks,”ASIACRYPT2001, LNCS 2248, Springer-Verlag, pp. 351-368, 2001.
[5] V. Shoup:“Practical Threshold Signatures,”EUROCRYPT 2000, LNCS 1807, Springer-Verlag, pp. 207-220, 2000.
[6] V. Shoup and R. Gennaro:“Securing Threshold Cryptosystems against Chosen Ciphertext Attack,”Journal of Cryptology, Vol. 15, No. 2, pp. 75-96, 2002.
[7] R. L. Rivest, A. Shamir and L. M. Adleman:“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,”Commun. ACM , Vol. 21, No. 2, 1978.
[8] Y. Tsiounis and M. Yung:“On the Security of ElGamal Based Encryption,”PKC1998, LNCS 1431, Springer-Verlag, pp. 117-134, 1998.
[9] M. Abe:“Securing ‘Encryption + Proof of Knowledge’ in the Random Oracle Model,”CT-RSA (The Cryptographer’s Track at the RSA Conference) 2002, LNCS 2271, Springer-Verlag, pp. 277-289, 2002.
[10] L. C. Guillou and J.-J. Quisquater:“A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Trasmission and Memory,”EUROCRYPT 1988, LNCS 330, Springer-Verlag, pp. 123-128, 1988.
[11] 石原武，青野博，本郷節之，四方順司：“証明可能安全性をもつしきい値暗号の構成法について,”信学技報，Vol. 105，No. 51，ISEC2005-1 (2005-5)，pp. 1-8，2005.

用 語 一 覧

RSA：Rivest-Shamir-Adleman