特集論文

クラウド向き関数型暗号技術の進展

高島克幸* 坂上 勉***
酒井康行** 松田 規***
内藤祐介*** 森 拓海***

Recent Progresses of Functional Encryption Technology for Cloud

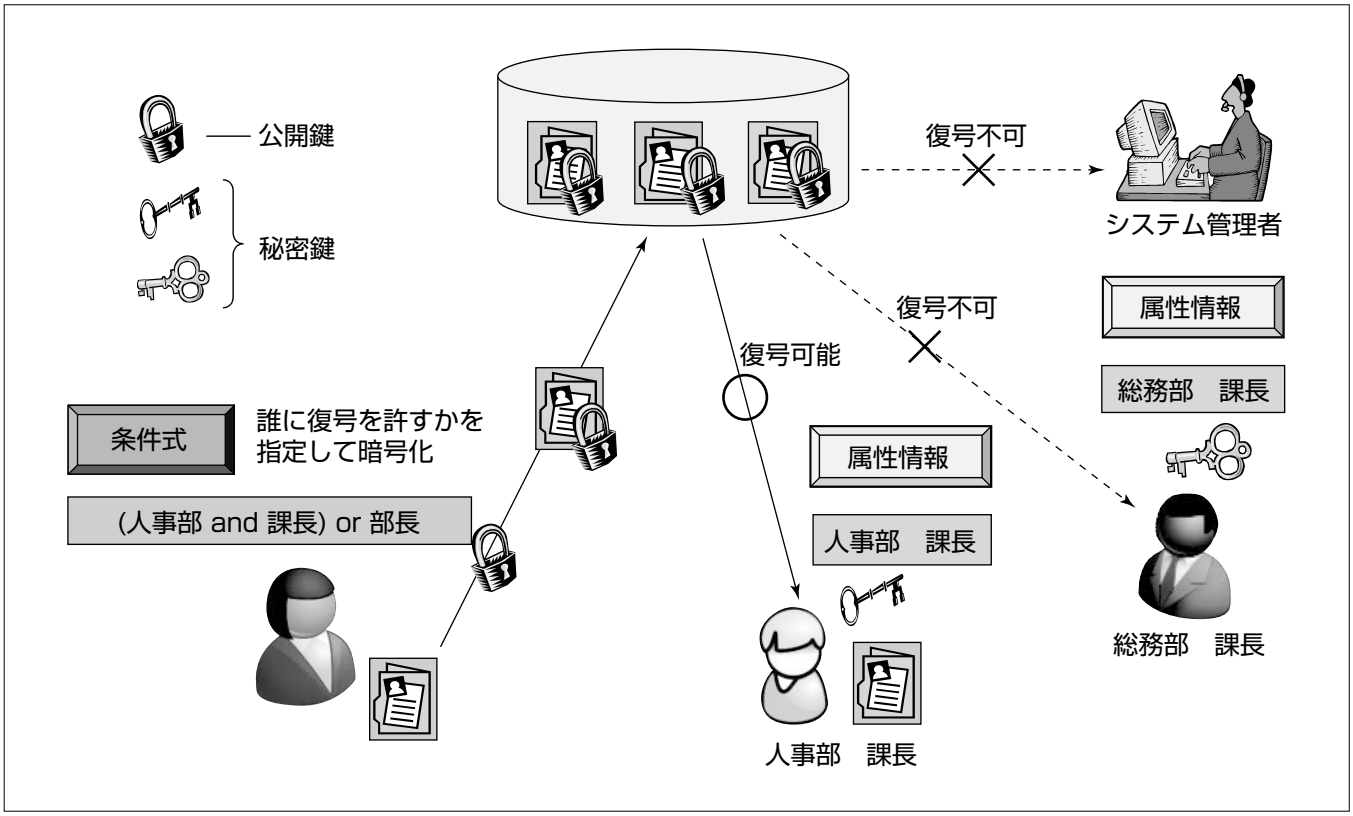
Katsuyuki Takashima, Yasuyuki Sakai, Yusuke Naito, Tsutomu Sakagami, Nori Matsuda, Takumi Mori

要 旨

クラウドコンピューティング(以下“クラウド”という。)環境におけるネットワークサーバ上の不正操作などの情報漏洩(ろうえい)リスクを払拭する関数型暗号方式を，三菱電機は，日本電信電話㈱と共同で開発して，2010年7月に発表した。それを用いると，保管場所のアクセス制御に依存せずに，安全なデータ保管が実現できる。この関数型暗号方式は，復号鍵に“所属・役職”などの属性を埋め込むことができ，暗号化する際に，復号できる人・グループを，その人の“所属・役職”で指定できる特長を持ち，クラウド環境での高機密データ保存に適する。

2010年発表の従来方式では，実用的な性能確保，安全性改善，機能・利便性向上などが課題であった。今回，当社と日本電信電話㈱は，従来のアルゴリズムを改良し，効率性，安全性，機能性の各性質を改善した。それらの改善は互いに関連してなされているので，まとめて本稿で述べる。

効率面では，情報を守る乱数を減らしても安全性を落とさずに，処理性能が改善した関数型暗号アルゴリズムを開発した。安全性の面では，検索キーワードを漏洩することなく検索が行える検索可能暗号用途で，これまで厳密に安全性を証明できなかった場合でも，初めて厳密な数学的安全性が証明された方式設計に成功した。そして，機能面の向上としては，自身の属性を証明できるデジタル認証・署名方式(属性ベース署名)も提案し，属性ベース署名を，関数型暗号方式と組み合わせることで，秘匿・認証を全て個人の属性に基づいて行う暗号通信システムを実現可能にした。また，各属性を管轄する鍵発行センターが相互に通信せずに鍵発行できる分散型鍵発行システムも構築して，関数型暗号と属性ベース署名の利便性を高めた。



クラウド向き関数型暗号アルゴリズム

関数型暗号を利用して機密情報管理システムを構築する場合，暗号化を行う際に，誰に復号を許すかを属性の条件式(例えば，(人事部 and 課長 or 部長))で表し，それによって暗号化する。その条件式を満たす人事部課長は，自身の復号鍵を用いて復号できるが，条件式を満たさない総務部課長は，自身の復号鍵を用いては，復号することができない。

*情報技術総合研究所(博士(情報学)) **同研究所(博士(工学)) ***同研究所

1. まえがき

ICT(Information and Communication Technology)社会の進展は目覚ましく，近年では，クラウドを始めとするネットワークの新しい高度な利用形態が普及してきた。しかし，そのような利用形態では，プライバシー情報や機密性の高いデータをサーバ側に渡して処理を行うため，新たなセキュリティ上の課題が生じる。ネットワークのセキュリティを保証するために現在では共通鍵暗号と公開鍵暗号が広く利用されているが，上記のような新しいネットワーク利用形態でのセキュリティ課題を解決するためには，より先進的な暗号が必要とされるようになった。共通鍵暗号や公開鍵暗号を更に発展させた先進的な暗号として，暗号化-復号のメカニズムの中に高度なロジック(論理)を組み込むことができる関数型暗号の開発に取り組んできた。

2. クラウド向き関数型暗号アルゴリズム

2010年7月に当社と日本電信電話㈱(以下“我々”という。)は，双線型写像ベクトル空間という数学的手法を開拓することで，暗号化-復号メカニズムの中のロジックとして現時点で考え得る最も一般的な機能を持つ関数型暗号の開発に世界で初めて(注1)成功した[1][2]。その特長を次に述べる。

(注1) 2010年7月28日現在，当社調べ

2.1 最も一般的なロジックの実現

数年前から世界中で関数型暗号を目指した研究が活発に行われてきたが，今回開発した関数型暗号方式では，従来開発されてきた暗号方式の機能を全て特殊例として包含する最も一般的な機能を実現できる。これは，AND，OR，NOT，しきい値ゲートによって構成される関係式を全て含む理論上最も広いクラスになっている。中でも特筆すべきことは，従来の方式の機能には含まれていなかったNOTゲートが使えるようになったことである。これによって，属性情報の変更などにも柔軟かつ簡便に対応可能なデータベース管理をクラウド上で実現することができる。

2.2 多様な利用形態への対応

関数型暗号では，暗号文と復号鍵に様々なパラメータを導入することで暗号化－復号のロジックを規定するが，そこでは，属性情報とそれに対する条件式が，それぞれ暗号文，又は復号鍵のパラメータとなる。我々が開発した関数型暗号方式では，①“復号鍵に属性情報，暗号文に条件式”の形態も，②“暗号文に属性情報，復号鍵に条件式”の形態も可能であり，様々な利用形態に対応することが可能となった[1]。①の形態を利用することで，データごとにきめ細かくアクセス条件(開示範囲)が設定された暗号データをクラウド上で管理して，そこで設定されたアクセス条件を満足する属性情報を持つ利用者のみがそのデータを復号・閲覧できるような機能提供が可能になる。企業における機密情報管理システムや公的機関による個人情報データベース管理などの応用がある。要旨の図は，企業における機密情報管理システムでの利用イメージを表している。管理する機密文書ごとに誰に復号を許すかを属性情報の条件式で表し，その文書をその条件式とともに暗号化してクラウド上で管理する。その条件式を満足する属性情報を持つ社員がその文書を復号する際には，その社員の(属性情報に応じた)復号鍵を用いて復号し閲覧する。要旨の図では，人事部の課長が，その属性情報に応じた復号鍵を用いて，クラウド上にある暗号化機密情報を入手，復号して閲覧可能となる状況を表している。

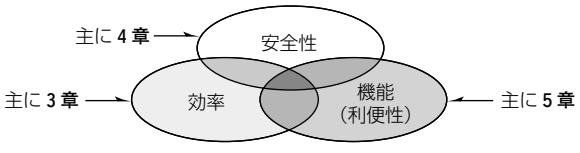


図1．最近の技術進展

2.3 最近の技術進展

参考文献(1)(2)で提案してきた関数型暗号方式を基礎として，最近の参考文献(3)(4)(5)(6)で，安全性・効率性・機能性の各性質が進展したことを述べたが，それらは複合して発展しており，関連させて概観する(**図1**)。

3. データサイズと復号時間削減への取組み

これまでは指定外の人が復号できないよう，多くの乱数を使用し伝達したい情報を守っていたので，暗号化，復号処理に時間が掛かり，その実用的な性能確保が課題であった。参考文献(3)では，情報を守る乱数を減らしても安全性を落とさずに，暗号文サイズと復号処理性能を改善した関数型暗号アルゴリズムを開発した(**図2**)。

条件式に論理演算を10個扱えれば，通常の属性指定に十分であるが，その場合に復号時間が従来の1/4となり，通常の属性指定で十分な性能確保ができることを確認した。また，内積演算を条件式にする暗号化方式の場合，復号時の演算効率を(漸近的に)大きく改善できた。これは，これまで提案してきた方式でのマスター公開鍵・秘密鍵を特殊な疎行列に基づいて生成することで達成した。安全性証明を行い，安全性を落とさずに高性能を達成した。

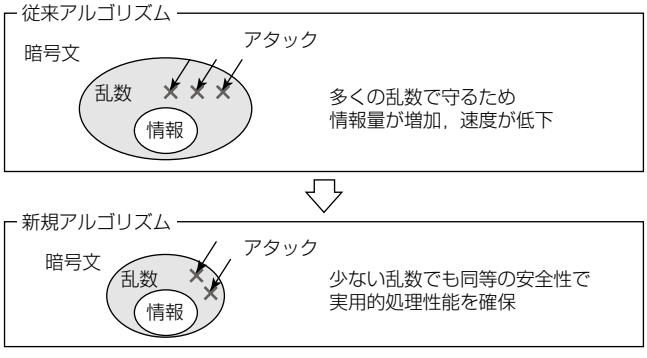


図2．高速関数型暗号の設計ポイント

4. 検索可能暗号への応用での安全性向上

情報を暗号化したまま検索が可能な暗号は，検索可能暗号と呼ばれて，世界中で研究が進められている。我々の関数型暗号方式は，検索可能暗号機能の実現にも応用できる。クラウド環境では，例えば，医療情報など機密性の高い情報が保管されており，それらは高いプライバシー（秘匿性）を必要とする。また，その情報を医師や製薬会社間で適切に共有できれば，より高い医療サービスを実現できるようになり，その際，検索機能は情報共有を促進してデータベースの有用性を高める重要な要素技術である。

特に，より先進的な検索機能として，通常よく使用されるキーワードマッチングで検索対象を絞り込んでいく（AND検索）だけでなく，キーワード情報に対する任意の条件式で検索（AND，OR条件式検索）できて，秘匿安全性が証明された検索可能暗号方式が望まれている。そのような機能は，参考文献(2)の関数型暗号方式を用いれば実現できたが，その方式を含めて，これまで提案された検索可能暗号は全て“弱い安全性”しか達成できていなかった。我々は，2012年４月に，“より強い安全性”を達成する検索可能暗号方式を世界で初めて(注2)提案した(4)。従来の検索可能暗号では，暗号文に埋め込まれたキーワード情報が，秘密鍵に埋め込まれた条件式を満たさない場合には，その秘密鍵で，暗号文に対して検索処理を施しても，条件式が満たされないという事実以外に，キーワード情報に関する余分な情報は一切漏れないことが保証されていた。しかし，暗号文に埋め込まれたキーワード情報が，秘密鍵に埋め込まれた条件式を満たす場合には，そのような保証を与えることができなかった。我々は，参考文献(4)で，その場合にも秘匿性が証明された方式を提案した。

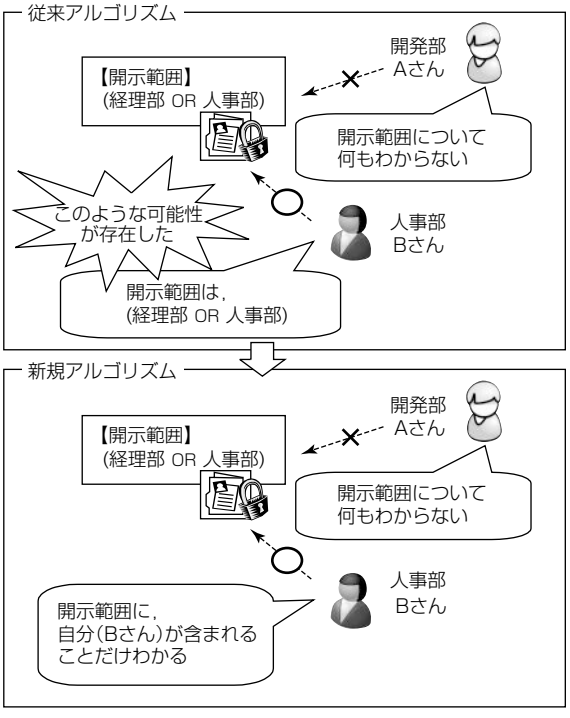


図３．開示範囲に対し強い安全性を持つ関数型暗号

その検索可能暗号によって，**図３**で示すように，情報開示範囲に対して強い安全性を満たす関数型暗号も実現できる。**図３**では，（経理部 OR 人事部）という開示範囲も秘匿した暗号文に対し，開発部Aさんと人事部Bさんがアクセスした時を表している。従来方式では，開示範囲に含まれないAさんに情報を一切漏らさないことが保証されていたが，開示範囲に含まれるBさんに，開示範囲が（経理部 OR 人事部）であることが全て漏洩する可能性があった。しかし，経理部に開示されていることを秘匿したい場合も考えられ，そこでは，余計な情報漏洩は回避すべきだが，そのリスクは拭い去れなかった。参考文献(4)の方式では，そのリスクは全くなくなり，**図３**では，Bさんは，開示範囲に自分（Bさん）が含まれることだけ分かる。

（注２） 2012年４月18日現在，当社調べ

5. 機能（利便性）向上への取組み

5.1 属性ベース署名

データの出所を保証するデジタル署名技術は，現在のインターネット環境で，なくてはならない技術の一つとなっている。その一方，署名に付随して，各ユーザーの行動履歴が明らかになってしまうことで，ユーザーに対する情報のコントロールが知らないうちになされてしまう“プライバシー侵害”も大きな問題となっている。従来のデジタル署名では，署名を施す署名生成鍵と，署名を検証する署名検証鍵が一対一に対応しており，この問題を根本から解消することができなかった。我々は，今回，属性情報とそれに関する条件式を用いることで，署名生成鍵と署名検証鍵の間の対応を，署名者が柔軟に決定できるようにして，上記のプライバシー侵害問題を解消した。

属性ベース署名は，例えば，自分が三菱電機社員であることを身元保証とした署名を行ったり，人事部員であることを身元保証とした署名を行うことができるもので，それによって，自身のプライバシー（匿名性）を守りつつ，一定の身元保証がされた署名付与が可能になる。そして，署名作成の都度，その匿名性の度合いを自分で決定して署名が行えること，及びその匿名範囲指定を属性情報を用いて行えることという特長は，実用上有用である。我々は，NOT条件も使用可能で，従来法に比べて効率的，そして安全性証明可能な属性ベース署名を提案した(5)。

関数型暗号では，暗号化データ送信者がその開示範囲を属性に関する条件式で指定できる。そして，属性ベース署名では，データ受信者がそのデータ認証を属性条件式の形で，検証できる。つまり，この２つの暗号技術によって，属性に基づいたデータ送受信を適切に行うことができ，クラウド環境への関数型暗号技術の適用を更に進めることが

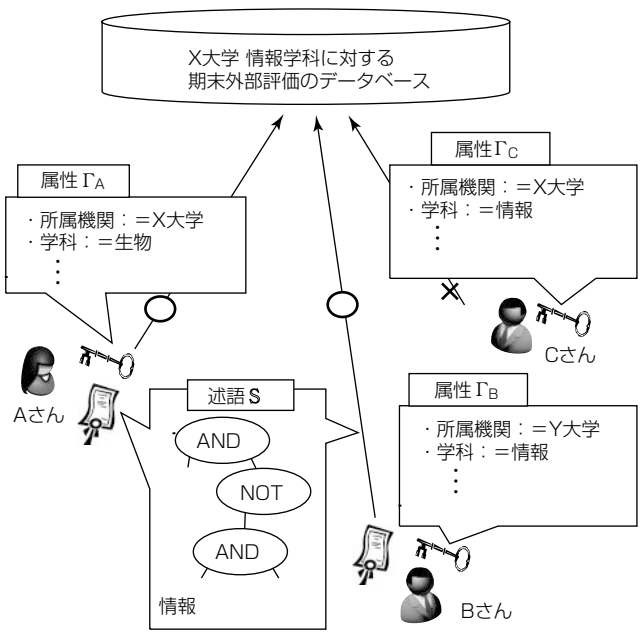


図 4．匿名評価(アンケート)への属性ベース署名の応用

できる。

例えば，各ユーザーは，社員証IC カードのような個人属性を形作る秘密情報(及びそれを格納した媒体)を用いて，様々なデータの認証を行う。例えば，X大学に属するAさんの属性情報が，“所属機関＝X大学，所属学科＝生物，ポジション＝ポスドク，年齢＝30，性別＝女性…”で与えられている場合を考える。彼女は，その属性情報が満たす任意の条件式で匿名性をコントロールして，署名を作成できる。例えば，“条件式＝(所属機関＝X大学) AND (所属学科＝生物)”といった条件式を用いて，自分の身元保証を行うことができる。**図 4** では，X大学情報学科に対する期末外部評価を投稿する際に匿名で署名を行う場合を示している。情報学科所属以外の人のみが許されるアンケート調査であるので，Aさん及びBさんは評価結果を正当に投稿できるが，CさんはX大学情報学科に所属しているので，評価結果を投稿できない。このように匿名での投稿を署名付きで行うことができるのが，属性ベース署名方式のメリットである。

5.2　分散型複数鍵発行センタ方式

実際に，関数型暗号や属性ベース署名を使用する際には，個人の属性秘密鍵は，各管轄機関から発行してもらう属性証明書と密接に関連している場合が多い。例えば，勤務先からの在籍証明，警察からの運転免許，役所からの住民票に対応して，各属性秘密鍵が各機関から発行されて，それらが一まとまりとなって，個人の属性秘密鍵となる。その属性秘密鍵が，暗号・署名システムでの個人の権限を表すので，この鍵発行手続きを安全に行うことは大変重要である。

これまでは，安全性確保のために，信頼できる第三者機関と各鍵発行センターの間に事前秘匿通信が不可欠であった。しかし，参考文献(6)では，そのような事前通信が不要

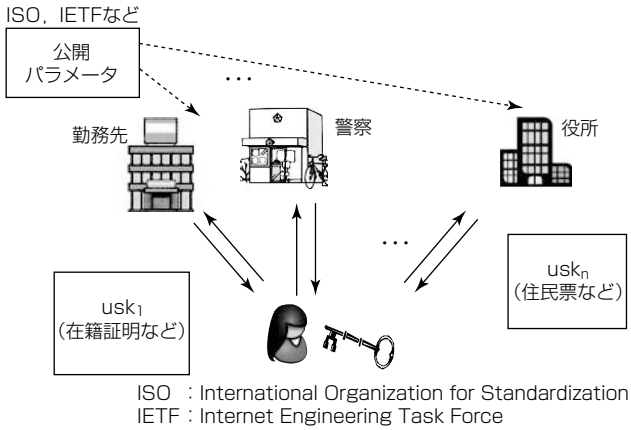


図 5．分散型複数鍵発行センター方式

で，複数機関が安全に鍵発行できるシステムを提案した。その応用範囲は広く，関数型暗号方式にも属性ベース署名方式にも適用可能である(**図 5**)。

6. む　す　び

関数型暗号方式技術の最近の進展を概観した。今後も，効率性，安全性，機能性の各側面で改良を加え，実用化に寄与していく。

参 考 文 献

(1) 日本電信電話㈱，三菱電機㈱：クラウド時代の高度なセキュリティ対策を実現する新世代暗号方式を開発(2010)
http://www.mitsubishielectric.co.jp/news/2010/0728.pdf

(2) Okamoto，T. and Takashima，K.：Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption，CRYPTO（2010）
http://eprint.iacr.org/2010/563

(3) Okamoto，T. and Takashima，K.：Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption，CANS（2011）
http://eprint.iacr.org/2011/648

(4) Okamoto，T. and Takashima，K.：Adaptively Attribute-Hiding（Hierarchical）Inner Product Encryption，EUROCRYPT（2012）
http://eprint.iacr.org/2011/543

(5) Okamoto，T. and Takashima，K.：Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model，PKC（2011）
http://eprint.iacr.org/2011/700

(6) Okamoto，T. and Takashima，K.：Decentralized Attribute-Based Signatures，ePrint（2011）
http://eprint.iacr.org/2011/701