様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２９年９月７日現在

機関番号：１３３０１
研究種目：基盤研究（Ｃ）
研究期間：　2010～2012
課題番号：22560360
研究課題名（和文）　条件付き暗号技術の仕組みの解明

研究課題名（英文）　Study on the cryptographic Techniques with Conditions

研究代表者　満保　雅浩
（MAMBO　MASAHIRO）
金沢大学・電子情報学系・教授
研究者番号：60251972

研究成果の概要（和文）：

多様な特性を持つ暗号技術の研究開発の重要性が高まっている。そこで、従来の暗号技術を包含する、与えられた条件が成立した場合にのみ処理が実現される、条件付き暗号技術について研究を行った。特に、サインディクリプションと呼ぶ、署名生成を復号条件とする暗号方式について、概念の創出と定義付け、及び、具体的な構成方法の提案などの議論を行った。また、検索機能付き暗号の条件についても記述能力を向上させる方法などについて考察を行った。

研究成果の概要（英文）：

The importance of research and development of cryptographic techniques with variety of properties has been increasing. In this paper, we have studied cryptographic techniques with conditions, which can be processed only if its associated condition is fulfilled. In particular, we have focused on a new scheme called signdecryption, in which a decryptor needs to create a signature in order to execute decryption. We have introduced such a notion, made its definition and showed its concrete and generalized constructions. Moreover, we have studied methods to improve the condition of searchable encryption schemes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,000,000	300,000	1,300,000
2011 年度	1,000,000	300,000	1,300,000
2012 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,000,000	900,000	3,900,000

研究分野：暗号理論
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：条件付き暗号、サインディクリプション

１．研究開始当初の背景

暗号技術の社会での利用の拡大と情報セキュリティに求められる技術自体への社会の要請の多様化に伴い、多様な特性を持つ暗号技術の研究開発の重要性が高まっている。特に、近年、事前に設定された条件が満たされた場合にのみ処理が実行される条件付き暗号技術に注目が集まっている。条件付き暗号技術は様々な場面で活用していくことができる潜在的な能力がある技術と捉えられ、基礎となる暗号技術の高機能化を実現することができる。

現在までにも、生体情報から得られる ID 情報を復号鍵に活用することにつながる、一定誤差範囲内の ID 情報であるという条件が満たされるならば復号が実行されるファジー型の ID に基づく暗号、メッセージへのアクセス管理につながる、属性を条件とする属性に基づく暗号、クラウドなどに保管された暗号文から守秘性を保ちながら必要なもののみを取り出すことにつながる、暗号文に付加された検索用の情報を条件文とする検索機能付き暗号などが実現されている。このように、設定できる条件が増えてきているものの、設定できる条件も限られており、取り組まなければならない課題も多いという状況にあった。

２．研究の目的

従来の暗号技術を包含する、与えられた条件が成立した場合にのみ処理が実現される、条件付き暗号技術について研究を行う。特に、より多様な場面で活用することができるように、条件付き暗号の機能を拡張する方法について検討を行う。

活用する具体的な場面として、ディジタルコンテンツの流通が挙げられる。ディジタルコンテンツの流通では、ディジタルコンテンツ販売者はユーザがディジタルコンテンツの使用条件へ合意したことを保証したいという要求がある。更に、もし、その合意がない場合は、ディジタルコンテンツへのアクセスを制限したいという要求もある。これらの要求を満たすような条件付き暗号技術を考案する。

また、その他にも、暗号化メールの検索が挙げられる。暗号化された複数のメールの中から、特定のキーワードを含むといった特定の条件を満たすものを取りだしてくることができるような条件付き暗号について考察する。

３．研究の方法

本研究では、以下の 3 つの観点から、条件付き暗号技術の仕組みの解明を行う。

(1) 条件の設定方法や実現方法の妥当性の研究

条件付き暗号技術では条件の付け方が重要な役割を果たすため、条件の設定方法やその実現方法の妥当性について研究を行う。

(2) 署名生成を条件とする暗号方式に関する研究

暗号文の復号者がディジタル署名を生成した場合に復号が成功する暗号方式の構成を行い、解決すべき課題などについて考察を行う。ディジタル署名は署名者だけが生成できるように構成されているため、暗号文の生成者は、どのような値になるか分からないディジタル署名が生成されたことを検証しつつ、ディジタル署名が正しければ復号が行われるように暗号文（およびその復号処理）を構成しなくてはいけない。

ディジタルコンテンツの購入者が暗号化されたディジタルコンテンツにアクセスしようとしたとしても、コンテンツ使用条件に署名しない限り復号できず、ディジタルコンテンツ自体を入手できないようにすることにより、ディジタルコンテンツの使用条件に対する合意をディジタル署名により得つつ、ディジタルコンテンツへのアクセス制限を暗号化により行うことを目指す。

(3) 検索機能付き暗号に関する研究

検索機能付き暗号は検索可能暗号とも呼ばれ、暗号文に検索用の情報を付加することにより、暗号文の中身であるメッセージが検索条件を満たしたものであるか否かを判定する。検索条件がキーワードとの一致として与えられるのではなく、大小比較、部分集合検索や範囲検索などのような形で与えられるものとして、隠れベクトル暗号方式がある。隠れベクトル暗号方式により暗号化された文書の属性を暗号文の属性と、検索したい属性のことを検索クエリの属性という。この隠

れベクトル暗号方式の安全性について考察すると共に、安全性が保たれる方式の構成を目指す。

４．研究成果

(1) 条件の設定方法や実現方法の妥当性の研究

既存の条件付き暗号技術についての調査研究を進めていく過程で、一部の条件付き暗号技術において、条件の付け方が十分でない場合があった。

暗号における条件は、属性暗号や述語暗号、さらには、それらを包含する概念である関数暗号において復号を実現するための条件として与えられ、検索可能暗号のような暗号形態では復号対象となる暗号文を抽出するための条件として与えられる。検索可能暗号においては、条件に関わる情報が暗号文に付加される。メッセージのみならず、このように付加された情報の中身なども漏洩しないように、条件が構成される必要がある。例えば隠れベクトル暗号においては、暗号文の属性と検索クエリの属性の両方が秘匿されることが必要であり、メッセージ自体の暗号化に加えて、付加された情報および検索クエリからメッセージに関する情報が漏れないように条件設定を行う必要がある。この条件に汎用性を出すために、任意の文字に置き換え可能なワイルドカードの使用を許すなどにより、条件の記述能力を高めた場合、その過程で、新しい攻撃の可能性が生まれ、設定した条件に抜けが生じる恐れがある。このような事例について考察を行った。

(2) 署名生成を条件とする暗号方式に関する研究

暗号文の復号者がディジタル署名を生成し、そのディジタル署名が正しければ復号が行われるような暗号文およびその復号処理を構成する方式をサインディクリプション方式と呼び、以下の研究を行った。

まず、サインディクリプション方式に求められる要素技術とそれらの関係についての仕組みを示すと共に、Boneh-Franklin ID ベース暗号方式と Boneh-Lynn-Shacham 署名方式を組み合わせることにより、具体的な構成方法の一例を示した。

Naor は ID ベース暗号方式からディジタル署名方式を構成できるという考察を行っている。この考察は、ID ベース暗号方式のマスター秘密鍵を署名者の秘密鍵および ID をメッセージとみなすことにより、ID を有する利用者が信頼のおけるセンターから入手する ID ベース暗号の秘密鍵がメッセージに対するディジタル署名として活用可能であるというものである。このディジタル署名の検証には、任意のメッセージに対して ID ベース暗号の暗号化を行った後に、ディジタル署名として機能する秘密鍵を用いて正しく復号できるかを確認する。Naor による ID ベース暗号方式からディジタル署名方式を構成するこの方法は、Naor 変換と呼ばれる。

Gentry は Naor 変換を公開鍵の非自明な証明書の発行に活用しており、この Gentry のアプローチは証明書ベース暗号方式と呼ばれる。証明書ベース暗号方式では、認証局が更新された公開鍵にディジタル署名を付けた上で復号鍵を受信者に渡していたときのみ受信者が復号できる。この手続きが行われていないと受信者が復号できないため、送信者は暗号化を行ったときに、受信者が復号できるかを知らない。このため、発行される公開鍵は非自明なものとなる。

本研究で考案した方式は、Gentry 証明書ベース暗号方式のアプローチを採用しているが、Gentry が構成した具体的な方式と以下のような相違点が存在する。まず、Gentry 証明書ベース暗号方式では更新された公開鍵に対して署名が施されるが、サインディクリプション方式では、受信者によって署名を施されるメッセージを送信者が選択することができる。また、Gentry 証明書ベース暗号方式では認証局のディジタル署名と受信者のディジタル署名の両方に関連付けられた秘密情報を作成するために複数のディジタル署名を一つのディジタル署名に集約することができる Boneh-Gentry-Lynn-Shacham 集約署名方式が用いられているが、当初、具体的な構成方式の一つとして考案した BasicSigndecrypt では、集約機能は必要ないため、単に、Boneh-Lynn-Shacham 署名方式が用いられる。

次に、サインディクリプション方式に求められる要素技術とそれらの関係についての仕組みを再考察した。これは一般的な構成方法が知られていないなどの解決すべき課題が残されていたためである。再考察により、サインディクリプション処理の出力において署名を明示的に出力する必要がないような定義を採用しているなど、条件付けという観点において必ずしも十分なものになっていないことが判明した。このため、サインディクリプション処理の出力において署名を

明示的に出力することを含めて、どのような条件が必要となるかということについて検討を行った。

また、上記の構成方法が具体的な構成方法の一例を示しているのみであったため、より一般的な構成要素として一般の ID ベース暗号を組み合わせることにより、サインディクリプション方式全体を構成する方法について考察した。その際、構成要素である ID ベース暗号に必要となる条件を含めて考察を行った。

更に、この一般的な構成に基づいて、Waters ID ベース暗号方式とそれから変換された署名方式を用いて具体的な構成方法の一例も示した。Waters ID ベース暗号およびそれから変換された署名方式では、復号者もしくは署名者は自己の秘密情報として、ある底の値を乱数でべき乗計算した値を使用する仕組みになっている。Waters ID ベース暗号とその変換された署名方式を用いて構成した具体的方式では、この性質を活用することにより、復号処理において署名生成を回避する行為を難しくしている。

一方、サインディクリプション方式での復号の制約を緩めた方式としてセミ・サインディクリプション方式を取り上げ、セミ・サインディクリプション方式の有用性について議論を行った。また、セミ・サインディクリプションに該当する具体的な方式を示し、復号の制約がどのように緩められているのかを確認した。

著者の知る限り、以上のような枠組みを議論した既存研究は存在せず、新しい着眼点に基づいた成果といえる。

(3) 検索機能付き暗号に関する研究

既存方式に存在した検索クエリ中のワイルドカードが漏洩するという問題について、新たにワイルドカード秘匿を定義した。そして、Iovino らの方式を参考に、合成数位数の群上で定義される双線形写像を用いることで、検索クエリ中のワイルドカードの守秘性を保障する方式を構成し、この構成方式がワイルドカード秘匿を満たすことを示した。また、メッセージ自体の守秘性などその他の性質も満たすことを示した。

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 1 件）
① 秋山浩岐，<u>満保雅浩</u>，岡本栄司，検索クエリ中のワイルドカードを秘匿する隠れベクトル暗号システム，査読有，情報処理学会論文誌，Vol.52，pp.2662-2673，2011.

〔学会発表〕（計 2 件）
① <u>満保雅浩</u>，条件付き暗号の機能拡張に関する考察，2012 年暗号と情報セキュリティシンポジウム，2012 年 2 月 1 日，金沢エクセルホテル東急（石川県）.

② <u>満保雅浩</u>，サインディクリプション方式の構成法について，コンピュータセキュリティシンポジウム 2012，2012 年 10 月 31 日，くにびきメッセ（島根県）.

〔産業財産権〕
○出願状況（計 1 件）

名称：公開鍵暗号システム、送信装置、受信装置、公開鍵暗号方式、プログラム、及び記録媒体
発明者：満保雅浩
権利者：満保雅浩
種類：特許
番号：特許第 6057150 号
登録年月日：2016 年 12 月 16 日
国内外の別：国内

６．研究組織
(1)研究代表者
満保　雅浩（MAMBO　MASAHIRO）
金沢大学・電子情報学系・教授
研究者番号：60251972

(2)研究分担者
なし

(3)連携研究者
なし