平成 26 年度研究開発成果概要書

課題名　　：組織間機密通信のための公開鍵システムの研究開発
採択番号　：17201
副題　　：クラウド環境に於ける機密情報・パーソナルデータの保護と利用の両立に向けて

（1）研究開発の目的

組織の機密情報やパーソナルデータの活用と保護の両立を図ること

（2）研究開発期間

平成 25 年度から平成 27 年度（3 年間）

（3）実施機関

中央大学研究開発機構（実施責任者　教授 辻井重男）

（4）研究開発予算（契約額）

総額 156 百万円（平成 27 年度　　49 百万円）
※百万円未満切り上げ

（5）研究開発課題と担当

A-1　組織間機密通信のための暗号方式の開発
A-1-1　基本方式の確立
A-1-1-1　階層型組織への多変数公開鍵暗号方式の確立
A-1-1-2　フラット型組織のための楕円エルガマル暗号及び楕円クラマー・シュープ暗号方式の確立
A-1-1-3　隣接・関連技術との連携・役割分担の確立
A-1-2　社会的背景の考察と利用環境高度化への対応
A-1-2-1　クラウド・ビッグデータの普及拡大による通信内容の高度化と機密・プライバシー保護
A-1-2-2　現代論理学暗号の提案と秘匿検索
A-2　組織間機密通信におけるユースケース、システム構成の検討
A-3　プロトタイプによるフィージビリティ評価
A-3-1　評価対象：暗号方式
A-3-2　評価対象：システムフィージビリティ
A-3-3　評価対象：社会的フィージビリティ

以上，全て中央大学研究開発機構が担当

（6）これまで得られた成果（特許出願や論文発表等）

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	2	2
	その他研究発表	57	41
	プレスリリース・報道	15	9
	展示会	0	0
	標準化提案	0	0

（7）具体的な実施内容と成果

A-1　組織間機密通信のための暗号方式の開発

A-1-1　基本方式の確立

A-1-1-1　階層型組織への多変数公開鍵暗号方式の確立

階層型組織用の組織暗号として提案された方式に於いては、送信側組織と受信側組織で多変数公開鍵暗号によって乱数を共有し、その乱数を使って、送信側組織がTSK 多変数暗号方式によって階層的に復号できるような形で文書を送信する。

この乱数送信に使うための多変数公開鍵暗号方式の安全性を検証したところ、脆弱性が見つかったため、その部分を強化した方式を考案し、論文投稿を行った(査読審査中)。

A-1-1-2　フラット型組織のための楕円エルガマル暗号及び楕円クラマー・シュープ暗号方式の確立

平成 26 年度は、平成 25 年度にプロトタイプ実装を行った組織暗号方式に改良を加えた、改良版組織暗号方式を考案した(特許出願中)。この改良方式は、楕円ElGamal 暗号方式を利用したもので、Cramer-Shoup 暗号方式へ適用することも可能である。

この改良方式ではやはり受信側代表者 A の公開鍵で暗号化された暗号文を、復号することなく代表者 A が受信組織内の担当者 B の公開鍵で暗号化された暗号文へ変換する点は同じである。この手法は、組織外から送られる暗号文を先ず組織のサーバに受けることを前提としたもので、代表者 A(アクセス許可を管理する権限がある)が A の公開鍵で暗号化された暗号文を B の公開鍵による暗号文に変換(再暗号化)するための再暗号化鍵を送り、サーバ(代理人)が再暗号化操作を行うものである。

アクセス許可(再暗号化)の操作では、代表者 A が暗号文のうち平文とは独立した情報のみしか受信しない。また、A の秘密鍵に関する情報は A 以外の者に対しては一切渡す必要が無いため、より高いセキュリティが実現できる。また、再暗号化された暗号文を削除することにより、一度与えたアクセス許可を取り消すことも可能である。また、この方式では、原理的には平文を ElGamal 暗号で暗号化する程度の計算量で再暗号化することが可能であり、高い性能が期待できる。

A-1-1-3　隣接・関連技術との連携・役割分担の確立

上記の代理人再暗号化方式、特に日本で東芝及び NICT などが実用化を提案し特許取得している各方式との比較を行った。主な比較項目は暗号化・復号化・鍵生成の負荷及び信頼できる第三者機関の必要性、セキュリティなどである。以上の調査は平成 27 年度も引き続き実施する。

A-1-2　社会的背景の考察と利用環境高度化への対応

A-1-2-1　クラウド・ビッグデータの普及拡大による通信内容の高度化と機密・プライバシー保護

「組織暗号」の開発の基となった「組織通信のあり方」に関して、歴史を踏まえて４類型に分類した。その結果に基づいて、将来のインターネット社会では組織間通信が重要となり、情報セキュリティに新しい概念を考え、情報通信の階層構造に新しく形式的論理レイヤを提案する論文を発表した。

A-1-2-2　現代論理学暗号の提案と秘匿検索

論理学暗号とはクラウド環境下における組織間通信機能の高度化に寄与する技術である組織間暗号を基盤技術として，論理学暗号に一般文書の論理的正当性，法令文書の法的整合性などの保証を行う技術である。

現代論理学暗号の提案と秘匿検索の処理の流れを概要図に示す。この図は、自然言語による問合せ・回答システムの例であり、自然言語の構造化、論理形式化言語の生成、キーワード秘匿検索、シンボル化等の秘匿処理、ならびに論理演算により現代論理学暗号方式が構成される。このような技術を論文によって提案した。

A-2　組織間機密通信におけるユースケース、システム構成の検討

1. 組織暗号を応用した機密情報配信システムの情報漏えいに対する安全性評価方式の検討

平成 27 年度は、A-1-1-2 で説明している楕円エルガマル暗号を利用した組織暗号応用機密情報配信システムの 3 種の基本構成を例にとり、情報漏えい確率推定式を提案、情報漏えい確率推定式を利用した情報漏えいに関するシステム構成間の比較が有効であることを示した。更に、情報漏えい確率推定式に基づくシステム構成の特徴把握により、情報漏えい対策に特に注力すべき構成要素の特定方法などを示した。

2. 行政で用いる情報システムにおける組織間機密通信システム構成案

A-3 のテーマで構築・評価した、フラット構造向け組織暗号のプロトタイプシステムを使って３つの自治体(新潟県燕市、長野県上伊那郡箕輪町、長野県大町市)で実証実験を行った。ユーザーインターフェース、実行速度、セキュリティなどについて高い評価を受けた。これらの実証実験の概要及び結果は論文にまとめ、日本情報処理学会論文誌へ投稿した(査読中)。

以上の実証実験に協力して頂いた自治体への追加ヒアリングを行い、特にマイナンバー法などの施行などによって行政による個人情報へのアクセスが可能になることへの対策が必要となっていることを痛感し、行政向けに組織暗号とセットで「プライバシー情報の条件つき開示」の方式を提案してゆく方針とした。

A-3　プロトタイプによるフィージビリティ評価

A-3-1　評価対象：暗号方式

今年度実施予定の分は既に平成 25 年度中に前倒しで実施済みである。

A-3-2　評価対象：システムフィージビリティ

フラット構造向け組織暗号の方式について、プロトタイプへ実装することにより、その性能を評価した。また、A-2 の2．で述べたように、所得や資産額、かかった医療費などの値自体は暗号化されたままで、ある基準値を越えているか否か(例：医療費が年間 20 万円以上ならば税控除の対象になる)を知る「プライバシー情報の条件つき開示」機能を行政システムの情報セキュリティ機能として提案することを検討した。この方式は昨年度既に論文発表したものだが、プロトタイプに実装して性能評価を行い、アルゴリズムに工夫を行うことによって暗号化状態処理の性能を向上させた。

A-3-3　評価対象：　社会的フィージビリティ

A-2-1 のテーマで考察した、情報セキュリティの新しい要素として提案する日本語の「論理的整合性」をテーマとして、「ビッグデータ時代の産業・法令日本語情報処理の課題」というタイトルで Melt-UP フォーラムを 2014 年 7 月 30 日（水）に実施した。

また、行政組織及び医療・介護関係者などに向けてユーザー目線で組織暗号の利点を解りやすく解説した配布用パンフレット「組織暗号　利用の手引き」を作成した。この他、リーダー辻井を初めとするメンバーが日本計画行政学会など暗号や情報セキュリティ技術以外が主要分野でないような学会などでの講演、及び日本民間放送連盟など一般向け雑誌への記事執筆により組織暗号の考え方や暗

号による情報保護の必要性を訴えた。

以上