平成 27 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

（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確立
　A-1-1　基本方式の確立
　A-1-1-1　階層型組織のための多変数公開鍵暗号方式
　　（MPKC: Multivariate Public Key Cryptosystem）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　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：「社会的利用フィージビリティ」

（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	1	1
	外国出願	0	0
外部発表	研究論文	4	2
	その他研究発表	94	37
	プレスリリース・報道	18	3
	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確立

A-1-1　基本方式の確立

A-1-1-1　階層型組織のための多変数公開鍵暗号方式
（MPKC: Multivariate Public Key Cryptosystem）の確立

素因数分解の困難性に依拠する多変数公開鍵暗号方式を提案し、2012 年国際会議 SCC で発表した方式を改良した。また、量子コンピュータに対しても安全な多変数公開鍵暗号方式を提案し、電子情報通信学会、情報セキュリティ研究会（ISEC）で発表し、国際会議に投稿した。

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

楕円 ElGamal 暗号を利用して、暗号文書を復号せず暗号文のまま別の鍵で暗号化できる方式を提案した。また、提案時に考えられていた方式の欠点である、「転送者の作業マシンがアタックされると平文の盗まれる可能性がある脆弱性」の対策を考えて特許出願し、また論文発表も行った。

A-1-1-3　隣接・関連技術との連携・役割分担の確立

属性ベース暗号、関数型暗号、代理人再暗号化を含む公開鍵システム全般に対する暗号技術の整理、技術動向の調査を実施した。

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

マイナンバーの運用などによって普及する組織通信に要請される価値観について考察し、個人通信、公共放送、交流サイトに加えて、組織通信を通信・放送の４類型に１つに位置づけた。

組織通信におけるコンプライアンス検証の概念を明確化しその技術要素を明らかにした。また、法令構造の特徴を考慮すると、最近進歩の著しい定理証明技術である SMT(Satisifiability Modulo Theories)ソルバーによるコンプライアンス自動検証の可能性の高いことを示した。

A-1-2-2　論理学暗号の提案と秘匿検索

秘匿検索方式における概念、ならびに社会的必要性、貢献性を検討し、実現に必要とされる技術的内容を分析し、方式を検討した。

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

自治体組織および医療・介護組織への組織暗号紹介および実証実験を通じた調査活動により、①「医療・介護分野」及び②「税と社会保障分野」のユースケースについて、個人情報・医療情報の安全な利活用のための組織暗号適用システム構成を提案した。

また、転送・復号制御および証跡確保に関する組織内暗号化情報流通マネジメント機能の実現性に関し検討を実施した。また、楕円エルガマル暗号ベースの組織暗号応用機密情報配信システム実装者向けに、この２つのシステムモデルに対する組織暗号の適切かつ有効な実装のための実践規範（ガイドライン）を作成した。

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」

多変数公開鍵方式を利用した方式、ならびに、フラット型組織用組織暗号として、楕円曲線 ElGamal 方式を利用した方式について、プロトタイプ作成、ならびに性能評価を行った。

A-3-2　評価対象：「システムフィージビリティ」

医療・介護の現場でも組織暗号の実用化に対する意見・評価を把握すべく、６か所の医療・介護

機関との意見交換を実施、その中で１か所の医療機関で組織暗号実証実験を実施した。

A-3-3　評価対象：「社会的利用フィージビリティ」

平成 26 年度に引き続き、2 自治体、及び 1 医療機関で実証実験を実施した。26 年度同様、実証実験を行った場では参加者からの意見や評価の集約を行っている。

講演会 MELT up フォーラム（暗号とその社会的利用フォーラム）を開催し、組織通信、組織暗号に関する活動紹介・意見交換を実施した。