平成26年度「組織間機密通信のための公開鍵システム」の研究開発 目標・成果と今後の研究計画

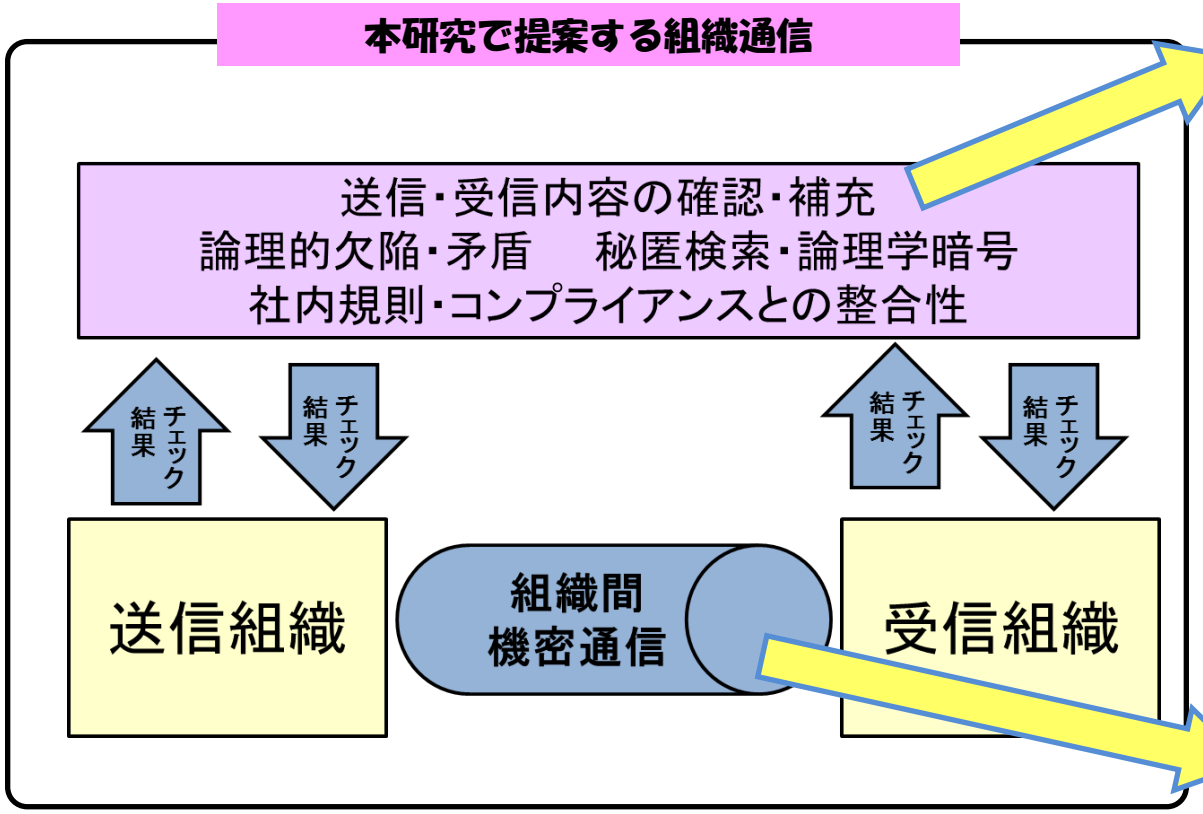
1. 実施機関・研究開発期間・研究開発予算

◆実施機関　　中央大学 (代表研究者)
◆研究開発期間　平成25年～平成27年　　◆研究開発予算　156百万円　(平成26年度55百万円)

2. 研究開発の目標

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

3. 研究開発の成果



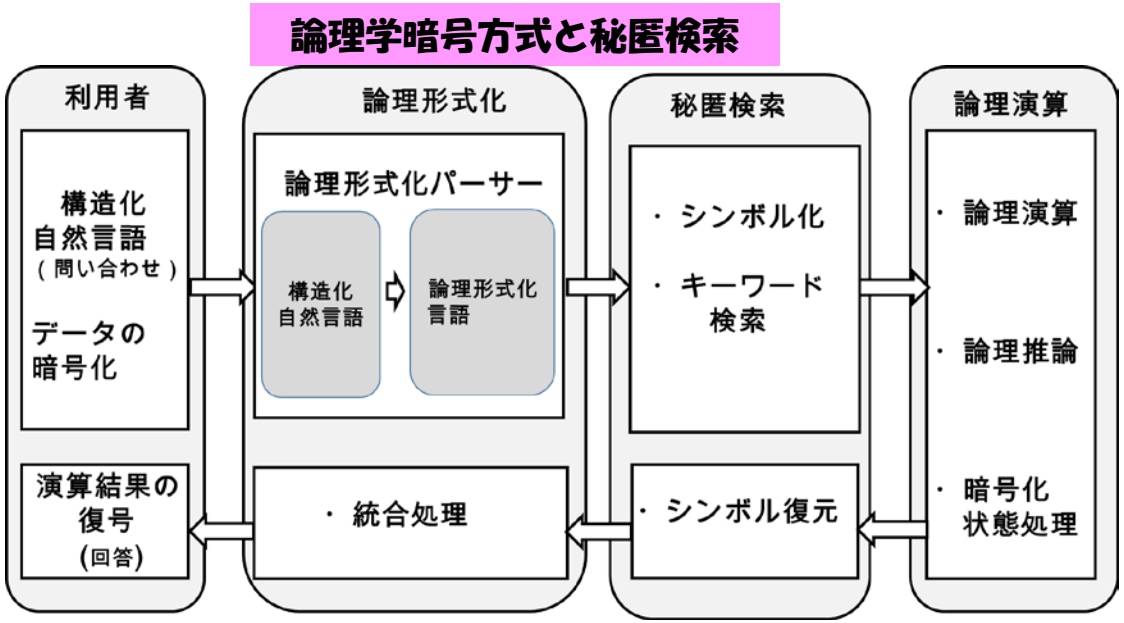
論理学暗号方式の研究開発

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
論理演算

組織暗号方式の研究開発

① 階層型構造向け(MPKCベース)
TSK暗号方式により組織内分配
PQ型暗号方式により乱数を共有

②フラット型構造向け(ElGamalベース)
楕円曲線暗号を応用
コンパクトで柔軟、高効率の方式



4. これまで得られた成果

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース 報道	展示会	標準化提案
組織間機密通信のための公開鍵システムの研究開発	0 （0）	0 （0）	2 （2）	57 （41）	15 （9）	0 （0）	0 （0）

※成果数は累計件数、（ ）内は当該年度の件数です。

（1） 組織暗号の、地方行政組織における実証実験

当プロジェクトで開発された組織暗号方式について、3か所の地方自治体で実証実験を行った。主題は組織暗号のユーザーインターフェース及び実行速度などの使い勝手について、現場の操作者から評価してもらうことであるが、この時同時に、行政職員に対して、以下のような説明会の場を設けている。以下が組織暗号実証実験のアジェンダである：

1. 組織暗号システムを使った実証実験システムのシステム全体、及び操作手順
2. 暗号による情報セキュリティに関する説明
3. 組織暗号の必要となるような行政・介護・社会保障関連の業務例
4. 実証実験

以上のような内容の実証実験を3つの自治体(新潟県燕市役所、長野県大町市役所、長野県上伊那郡箕輪町)で行った。

（2） Melt-up フォーラム「」（主催：中央大学研究開発機構） http://c-faculty.chuo-u.ac.jp/~tsujii/lecture.html

2014年7月30日(水) 於 中央大学駿河台記念館
テーマ 「ビッグデータ時代の産業・法令日本語情報処理の課題」
法律や契約関係など論理性のある文章をつくり論理学的に処理を行うための言語としての「日本語」について様々な角度から論じた。法学部が有名な中央大学のフォーラムにふさわしく、学長を初めとする法律の専門家や、アルゴリズムと言語をつないだ「法令工学」の専門家の講演、及び、情報セキュリティ関係の講演会では珍しく、日本ペンクラブ専務理事を務める作家の吉岡忍氏などからも日本語やその文章に関して非常に深い内容の講演を行って頂いた。
また、東京オリンピックを含めて、東京を初めとする各都市が外国語ネイティヴにとっても暮らし易い国際都市となってゆくために必要な言語・外国語サービスや、そのための日本語処理技術、例えば機械翻訳システムなどの課題について、また特許文書の処理など科学技術関連のニーズなど、幅広い視野からの講演及びパネルディスカッションによる議論が行われた。

5. 今後の研究開発計画

平成26年度は、以前から何らかのつながりのあった自治体に対して直接訴えかけ、行政に使われる情報システムに関して実証実験を「依頼」してとにかくその価値と必要性を実感して貰うことに主眼を置いていたが、年度の後半になって、報道などで取り上げられたこともあり、トップダウンで組織暗号を検討する動きも見られる。平成27年度は、ますます広く実証実験を行って今後の行政のための情報セキュリティと個人情報保護を提案してゆく。

また、当研究室におけるこれまでの研究の蓄積を活用して、個人情報を可能な限り行政の業務担当者に直接アクセスさせずに必要な行政サービスの判断は実行できる(例： 生活保護支給の決定、高額医療費の払い戻しなど)技術を紹介しつつ、行政のマイナンバーや電子自治体への対応のための方式として提案を行う。

行政向けだけでなく、 当初より組織暗号や暗号化状態処理が必要とされていた、医療や介護関連の組織向けにもユーザーニーズを更に調査して把握しながら、実用に耐えるシステムの提案を行う。

組織暗号技術に関しては、楕円曲線暗号を利用した発想に基づき、ElGamal暗号に続いて、より高い水準の安全性が証明されているCramer-Shoup方式に基づいた組織暗号のアルゴリズムを提案し、暗号の専門家も納得させられるだけの安全性の保障を提供する。また、階層型構造向けとして考えられた組織暗号方式である「多変数公開鍵暗号」に関しても新しい効率的な方式を考案し、論文として社会へ提案する。

論理学暗号技術に関しては、今までに論文発表を行った方式をプロトタイプに実装し、評価を行うと共に、当研究ユニットで当初から構想していた組織通信の実現につとめる。