平成 25 年度 委託研究

課題 172

組織間機密通信のための公開鍵システムの研究開発

研究計画書

独立行政法人
情報通信研究機構

１．研究開発課題

『組織間機密通信のための公開鍵システムの研究開発』

２．研究開発の目的

近年、ネットワークを介した情報流通が各種業務において一般的に行われるようになっている。これらの情報流通においては、その情報を受け取る権利のない人に対しては情報が秘匿されるなどのセキュリティ確保が必要であり、暗号技術を始めとした各種のセキュリティ技術の研究が行われており、その結果として安全性が確認された暗号技術が広く使われている。

一方で、現実の業務における組織間の情報流通の形態を考えた場合、既存の暗号技術では対応できない状況が存在する。組織間で情報流通を行う場合、その情報は情報提供先において情報へのアクセス権に応じて情報の暗号化を行う必要があるが、この情報に対するアクセス権は、一般的に情報の性質によって規定される。例えば、企業から自治体に情報を送信する場合、税金に関する情報を送信する場合と、社会保険に関する情報を送信する場合では、その情報を復号してよい人は異なる。しかし、この企業では自治体における実際の担当者がわからないため、どの鍵で暗号化してよいかわからない。そのため、担当組織にひも付いた公開鍵で暗号化することになる。一方で受信する組織（自治体）においては、個々の情報に応じて実際に情報にアクセスして良い担当者を指定する必要がある。これは、個別の情報に応じて担当者を柔軟に変更することを可能にしたり、担当者の人事異動等に柔軟に対応できるようにする必要があるためである。

上記のように、現実の業務形態を考慮したとき、情報を暗号化する送信者は実際に情報を復号する受信者を知らないまま暗号化を行い、受信者側の組織で実際の復号を行う受信者を再設定する形式の暗号技術が必要となる。

本研究開発では、公的研究機関である機構が実施する研究開発の成果により我が国におけるネットワークのセキュリティが確保されることが求められていることから、上記のような新しい運用モデルに適した公開鍵暗号システムについて、現実の組織間での機密通信を行う際の性能的なフィージビリティの検証を行うことを主目的とし、この目的を達成するために CRYPTREC 等で行われる評価に適う数学的な証明可能安全性と、現実的な組織規模で運用可能な処理性能を有する方式を確立する。また、本研究開発成果に、機構の自主研究が実施する暗号技術の評価に関する知見や、様々なセキュリティ要求に対応できるセキュリティアーキテクチャを連携させることで、組織間を流通する情報の安全性確保と、情報流通形態の高度化に対応した暗号技術の実現に貢献することも視野に入れたものとする。

３．採択件数、研究開発期間及び予算

採択件数：1 件

研究開発期間：契約締結日から平成２７年度までの３年間。

予算：平成２５年度は総額５５百万円を上限とする。なお、平成２６年度以降は対前年度比で 6%削減した金額を上限として提案を行うこと。（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

４．研究開発の到達目標

１）組織間機密通信のための暗号方式の確立

＜前提条件＞

従来の暗号技術とは異なる、組織間機密通信のための安全性評価のためのモデルを確立するとともに、その実現方式を検討し、数学的な安全性証明を付与すること。ここでの組織間機密通信に必要な要件としては、情報を送信する組織には受信組織において復号を行う担当者は不明であり、情報を受信する組織において改めて受信できる担当者を設定、あるいは限定できるようにすること。

＜実施要件＞

（１）組織間機密通信のための暗号方式の設計

前提条件に示した組織間機密通信を実現するための暗号方式（鍵生成・管理、暗号化、復号できる担当者の設定、復号の各アルゴリズム）を設計すること。その際には、（２）において数学的に厳密な安全性証明が付けられるように、システムモデルと安全性モデルの定義を行うこと。

（２）組織間機密通信のための安全性評価の実施

（１）で定義したシステムモデルと安全性モデルに従い、数学的な安全性証明を付与すること。この安全性証明については、査読付き国際会議において、第三者から正当性の確認を受けること。

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

＜前提条件＞

組織間機密通信は、情報の送信者にとって、情報の受信者が所属する組織の内部構成が不明であることが前提条件である。また、受信者が所属する組織では、情報の復号を行うことができる担当者を設定する管理者が存在する。

さらに、復号ができる担当者は、個別の情報に応じてその都度設定することが可能である。また、担当者の候補は、人事異動等に対応できるように柔軟に変更できる。

＜実施要件＞

前提条件に述べた組織間機密間通信が現実に使われる状況を調査、整理し、システムモデル、ユースケースとしてとりまとめること。その上で、具体的なユースケース（例：公的サービス）を提案書に記載し、そのユースケースに沿ったシステムモデル、運用モデルに沿った研究を行うこと。その際に、送信側の組織、受信側の組織のユーザ数や組織の構造、組織間機密通信の運用手続き、暗号処理が用いられる場所、性能要件を明らかにすること。

３）プロトタイプによるフィージビリティ評価

＜前提条件＞

組織間機密通信を実現する暗号技術は、従来の暗号技術に加えて、復号できる担当者の担当者の変更など、新しい機能と運用手順が加わっている。これらの機能と運用手順によって生じる、計算機上の処理のオーバーヘッド、および運用におけるオーバーヘッドを現実の業務を妨げない範囲に抑える必要がある。そのため、提案技術が十分な実用性と運用の可能性を有していることを本件研究項目によって確認する。この際、２）で洗い上げたユースケースと性能条件を満たす必要がある。

＜実施要件＞

１）で提案した方式について、２）で設定したユースケースとシステム構成に応じて、処理性能と運用のオーバーヘッドを明らかにすること。このオーバーヘッドが、実際の業務において許容できない範囲にあるときには、１）の研究にフィードバックを行い改良を図るか、許容できるようになる運用条件を示すこと。

５．研究開発の運営管理及び評価について

研究開発に当たっては、機構の自主研究との連携を図ること。

平成２７年度に終了評価を行う。また、研究開発終了後に追跡評価を行う場合がある。

６．参考

（１）研究課題設定の背景及びその必要性

現在、機構の自主研究では、ネットワークセキュリティ技術に関して、「サイバーセキュリティ」、「セキュリティアーキテクチャ」、「セキュリティ基盤」の 3 つの研究開発を柱に、三位一体として国民誰もが安心・安全に情報通信を行うことができるように、社会が必要とする研究開発を進めている。

特に、「セキュリティアーキテクチャ」の研究開発では、モバイル、クラウド、新世代ネットワークを含めた、セキュアネットワークの最適構成技術と設計・評価技術を確立し、安全なネットワークを提供することを目指している。

近年、ネットワーク上を流通する情報のセキュリティの確保、プライバシの保護のニーズは高まっており、暗号技術を含めて様々な技術が提案されている。一方で、情報流通の形態は複雑化しており、暗号技術が本来有する情報に対するアクセス制御という機能についても、復号を行う人を柔軟に設定できる暗号技術が求められている。例えば、関数型暗号[1]のように、復号権限をある条件に従って設定可能な暗号技術の研究が近年大きく進んでいる。これらの技術は、主にクラウドを通じた情報流通において活用されることが期待されている。また、クラウドでの情報に対するアクセス制御を柔軟に再設定することができる技術として、代理再暗号化技術[2]があるが、この技術は復号権限に関数型暗号のような構造を設定することは出来ない。

しかし、現実の組織における情報の秘匿の運用を考えた場合、送信先の組織の構造を知ることは困難であり、その場合、組織間で正しいアクセス制御の構造を設定することはできない。この場合、受信者の組織で管理者を置き、管理者が受信側の組織の事情に応じたアクセス制御を再設定する必要がある。このような運用は、関数暗号や代理再暗号化だけでは実現することができない。そのため、組織間機密通信に対応した、処理性能、運用の両面で実用的な新たな暗号方式が必要である。

また、関数型暗号などは、理論的研究成果は数多く提案されているが、現実のユースケースに対応した形での実証は現在のところ不十分である。これらの高機能暗号技術は、現実のユースケースにおける有効性実証が重要であり、本研究開発においてもこの有効性検証が必要である。

（２）本研究開発による情報流通の高度化に対応したセキュリティの向上

（１）で述べたような課題に対応した暗号技術を構築することにより、組織間のセキュアな情報流通を実施するための基盤技術を確立するとともに、フィージビリティ評価と改良により、実用的な暗号技術の構築を行うことができる。また、組織構造が柔軟に変化するシステムにおいて、セキュリティとプライバシ保護への国民の要求の複雑化へ対応可能な技術の確立することが

できる。

また、本研究開発では、性能面でのフィージビリティ検証に重点を置いており、近い将来の電子政府、公共団体、民間企業などにおいて運用可能な高機能暗号技術の実現を目指す。

（３）本課題と機構の自主研究の関係

「セキュリティアーキテクチャ」の研究開発では、ICT の利用方法に応じたセキュリティ要求を、様々なセキュリティ技術を過不足無く満足させる方法を研究している。特に、組織間をまたがる場合の情報の秘匿性は、ネットワーク間連携が盛んになる今後の ICT 環境において重要なセキュリティ要求であり、この要求の実現技術を NICT 発のセキュリティアーキテクチャに組み込むことは必須である。

また、「セキュリティ基盤」の研究開発では、長期利用可能暗号の研究として有望な暗号理論である「多変数公開鍵暗号」について、安全な暗号アルゴリズムの設計と設計のための評価技術の研究を行っている。組織暗号は多変数公開鍵暗号をベースに作られており、本委託研究により実際のシステム運用を考慮した技術課題が抽出でき、その結果としてセキュリティ基盤研究室に置ける評価の精度を向上させることができる。

参考文献

[1] 高橋，星野，小林，山本剛，山本具，宮澤，吉田，冨士，横森，永井，”関数型暗号:実装の現在と実用化への展望,”暗号と情報セキュリティシンポジウム（SCIS2012）1B1-3, 2012 年 2 月，金沢.

[2] 川合，松田，花岡，国廣，“代理人再暗号化方式の安全性について,” 暗号と情報セキュリティシンポジウム（SCIS2012）3A3-1, 2012 年 2 月，金沢.