事後評価報告書

１．研究課題名：暗号技術に基づくプライバシー安全管理システムの研究

２．研究代表者名：

２－１．日本側研究代表者：

岡本栄司（筑波大学大学院システム情報工学研究科教授）

２－２．米国側研究代表者：

Rebecca Wright（スティーブンス工科大学コンピューター科学部准教授）

総合評価：　優

３．研究交流実施内容及び成果：

本研究交流では、情報セキュリティ対策の核となる暗号技術を用いたプライバシー保護方式の研究を行った。

研究交流の実施内容及び成果について以下のとおり各年度を基本にして第1～3期に分類し、主要な取り組みを以下に記載する。

第1期(2004年12月～2005年3月)

最初にプライバシ保護技術に関する問題点について研究調査を行った。具体的には米国チームと連携を取りながら、主にプライバシ保護技術とペアリングにおける現状と解決すべき点について、あぶり出しを行った。ペアリングとは、楕円曲線理論を用いた双線形写像 $e:G_1\times G_2\rightarrow G_T$ のことであり、$e(aP、Q)=e(P、aQ)=e(P、Q)^a$ という性質を満たす。ここで、G_1、G_2、G_T を同じ位数を持つ群であり、a は整数、 $P\in G_1$、 $Q\in G_2$ である。

また、プライバシを考慮した暗号管理システムに関するワークショップを開催し、関係者の基礎知識を固めるとともに、プロジェクトの今後の進め方について打ち合わせを行った。また、日米ワークショップ「重要情報基盤保護(CIIP)」を開催し、プライバシを考慮した暗号管理システムについて国内外からの研究者と意見交換を行った。

これらの取り組みによる成果として、ペアリングを用いた 1-out-of-n 署名を提案した。また、1-out-of-n 署名とブロードキャスト暗号について、双対性が存在することを明示的に示した。双対性に関する関連研究としては、2003年に Kiayas らによってグループ署名と traitor tracing による双対性が示されているが、1-out-of-n 署名とブロードキャスト暗号の双対性について明示的に解析したのは、今回が始めての試みとなる。また、提案方式は署名候補者となる n の数に依存せず、署名長を 800bit 程度の固定サイズで運用できるという利点を有する。これらの研究をさらに推し進めるために、日本側の研究構成員が、米国やオーストラリアなどの研究施設を訪問し、現地の研究者と共同研究や意見交換を行った。

第2期(2006年度)

前期の成果を応用して、1-out-of-n 署名と検証者指定署名を組み合わせた方式について提案した。これは署名者匿名性や検証者限定性などの性質をもっており、鍵管理や伝送量と

いう点で優れている。双対性については、認証付ブロードキャスト暗号と検証者指定署名の対を持つことを解析し、この暗号系の中で暗号から署名へ自由に変換が可能な技術を初めて実現した。

k-out-of-n 署名は、1-out-of-n 署名を一般化したものであるが、1-out-of-n 署名を k-out-of-n 署名に拡張する技術については、2004 年に椎名らにより組み合わせ理論を用いた方式が提案されているが、k と n の値によっては、計算量的な困難性により署名生成が不可能となるなどの問題があった。実用性と安全性を兼ね備えた匿名署名を構築するためには、これらの問題を解決する必要があるため、日本側の研究員が Steven 工科大学を訪問して意見交換を行った。これらの取り組みにより、我々は「多重リング」という手法を用いて k-out-of-n 署名に拡張する方法を提案した。提案方式は、RSA 暗号系、DLP 暗号系、EC-DLP 暗号系など、現在、標準化されている主要な暗号方式のいずれも適用することができ、高い実現可能性をもつ。

第 3 期(2007 年度)

本プロジェクトが主体となって、ペアリングに関する国際会議 “Paring 2007” を東京で開催し、米国をはじめ国内外の研究者と意見交換を行った。この会議において、本プロジェクトの取り組みを明示的に報告することにより、プロジェクトや組織に対する認知度を高めるとともに、提案した匿名署名に関する議論を行った。

また、提案した方式に対し、安全性について厳密な評価を行った。さらに、提案方式の分類、性能評価、応用例などを示した。また、実効性を評価するため、いくつかの方式について実装を行った。最終的に、実装などの方法により匿名署名システムの統合を行い、提案方式が高い有効性を持つことを確認した。

研究成果の今後期待される効果であるが、ペアリングは暗号と組みあわせることにより、有益な運用ができることがわかっている。また、匿名署名を用いた暗号技術の構築は、社会的なニーズが高く、今後、実社会において適用される情報セキュリティ技術と考えられている。本プロジェクトで提案した各種の匿名署名は、いずれもペアリングを用いた方式であり、他の既存方式と比べデータサイズ、計算量の点で効率がよい。このため、今後、産官学連携による取り組みなどにより提案方式を実用化し、運営を行うことが考えられる。

現在、暗号理論分野の主要な国際会議(CRYPTO 等)の約 20%がペアリングに関する研究であると報告されており(参照：CRYPTO2006 Rump Session で発表された調査研究)、ペアリングは、特に暗号・情報セキュリティ分野において大変注目されている研究テーマである。これに関連して、最近は ISO や IEEE のような国際標準化団体において、ペアリングの標準化が精力的に進められている。ペアリングに関する本プロジェクトの成果は、暗号・情報セキュリティ分野の研究において、これからの日本の国際競争力を維持するとともに、いくつかの成果については、国際標準化を見据えた取り組みを目指すことが可能である。

また、最近、ペアリングを用いた研究は、単に暗号方式の提案だけに留まらず、整数論、離散数学、ネットワーク、クラスタリング、情報のアクセシビリティ、更にはマネジメントなど、社会人文科学分野まで含む広範囲に渡っており、実用的および学術的な方面への

波及効果がある。このため、本プロジェクトの成果はこれらの分野において新しい研究テーマを生み出し、従来では想定していなかった新たな波及効果を及ぼすことが期待できる。

４．事後評価結果

４－１．総合評価

研究メンバーの１人である境隆一大阪電気通信大学講師、及び　笠原正雄大阪学院大学教授らによって世界に先駆けて発明されたペアリングによるＩＤベース技術などを軸に、匿名性と安全性の両立を図るという匿名署名に関する研究成果を始め、プロトコル、マネジメントなどの応用研究に至るまで、多くの成果を上げている。しかし、相手国との交流を踏まえた成果であるとは必ずしも判断できない

４－２．研究交流の有効性

新しい知の創造に関し、ペアリングの研究は、これまで理論と応用に分かれて研究されてきたが、本プロジェクトが開催した国際会議「pairing2007」によって、より総合的な観点からの研究が推進された。

人材の育成に関し、上記の国際会議を立ち上げる過程での意見交換を通じて、交流が深まると共に、人材の育成に効果があった。

研究交流の今後に関しては、上記の国際会議が 2008 年度も開催することが決められており、更に、それ以降の毎年開催することを予定している。それによって、米国との研究交流がより活発化され、持続的な発展が期待される。

４－３．当初目標の達成度

ワークショップの開催など計画通り行われた。