事後評価報告書

１．研究課題名：「安全で効率的なデータアクセス制御システムの設計及びそれに適した新たな暗号技術の創出に関する研究」

２．研究代表者名：

２－１．日本側研究代表者：（独）産業技術総合研究所　情報セキュリティ研究センター
花岡　悟一郎　研究員

２－２．米国側研究代表者：コロンビア大学　コンピューター科学部
Keromytis, Angelos 准教授

総合評価： 優

３．研究交流実施内容及び成果：

本共同研究は、コロンビア大学および産業技術総合研究所（以下、産総研）において、理論と実用性に関する双方の知見を生かし、これまでになかった高度な安全性と効率性を同時に実現するデータアクセス制御技術、およびその要素技術を創出することを目的としている。

これまでコロンビア大学の研究グループでは、Dual Receiver 暗号方式と名付けられた独自の技術を開発し、それが安全で効率的なデータアクセス制御に有用であることを示している。

一方、産総研の研究グループでは、現在広く研究がなされておりデータアクセス制御システムを構築するための強力な要素技術としても注目されている。ID ベース暗号について、その厳密な安全性証明手法や効率の良い構成法の提案など、先駆的な研究を行ってきた実積がある。

両者はこれまでにも国際会議などの機会を利用して密な交流を持ちながら有益な情報交換を行ってきた経緯を持っており、これをベースに両者それぞれ次のような成果を挙げている。

①日本側の成果

（ア） Dual Receiver 暗号を任意の ID ベース KEM から一般的に構成することが可能であることを示し、その手法を用いることで実際にさまざまな性質をもつ Dual Receiver 暗号の設計を行った。特に、ランダムオラクルに依存しない初めての方式や、素因数分解タイプの問題の困難性仮定に基づく初めての方式も実現している。

（イ） 基盤的理論の掘り下げも深く行われており、その知見を積極的に活用することで上記（ア）の成果も得られている。

②相手国側の成果

（ア）　産総研側の研究について、Dual Receiver 暗号やネットワークセキュリティ全般に関する独自の知見に基づく助言を提供することで、同研究に大きく貢献した。

（イ）　（ア）の研究と並行しながら、実装を強く意識した別の視点から安全なデータアクセス技術の創出に取り組んでいる。特に、産総研側を実際に訪問し意見を求めながら研究を進めることで、攻撃者の侵入を自動的に排除するソフトウエアの設計指針について明らかにしている。

４．事後評価結果

４－１．総合評価

DoS 攻撃の対策でアドホックに設計されたため、必要とされる性質や設計の方法論が不明であった Dual Receiver 暗号の数学的性質を明らかにして Dual Receiver 暗号と ID ベース暗号技術を融合した新たな技術を創出すべく活動した。日米研究者のレベルは研究開始時点で既に高く、本研究の実施により、更に飛躍的に発展したとの印象は受け難いが、学生を含め若手研究も研究チームに加わっており、本研究遂行によって、数名の若手研究者が育っている点は高く評価される。

研究討論は日米相互でそれぞれ２回ずつ実施され、またワークショップ・セミナーは当初の計画通り計 3 回実施されている。

今後は、実運用システムの実装に関する深い知見を有する米国研究チームと、理論と実用の面から独創的な成果を出していくことが期待できる。

４－２．研究交流の有効性

主体的に研究を行った者のみを著者とする暗号研究分野の慣習に従うとのことで、残念ながら共著論文は存在していないが、日本研究チームによって数多くの論文がまとめられている。コロンビア大学で既に提案されていた Dual Receiver 暗号について理論的考察を深めている点で研究交流の有効性が認められる。

人材交流の面でも、日米双方とも若手研究者がチームに加わっており、本事業が相互の研究者に刺激を与えたであろうことが期待できる。例えば、1 名の大学院学生が研究交流によって得られた成果を国際会議で発表するなどの成果が達成されている。

また、外国人大学院修士学生が育っているほか、本研究に携わっていた 3 名の博士課程日本人学生が産総研の研究員に採用されており、人材の育成は十分になされている。

また、実運用システムの実装に関する深い知見を有する米国研究チームと、ID ベース暗号を中心に暗号理論に関する深い知見を有する日本研究チームとの協力により、研究遂行の段階で内容をともなった研究交流がなされており、持続的な発展の可能性は期待される。

４－３．当初目標の達成度

学生を含め若手研究者も研究チームに加わっており、研究体制は適切であったと考えられる。研究討論は合計 4 回日米相互で実施され、相互派遣、相互交流が活発に行われていた。本研究に関わるワークショップも７０名程度の参加者を集めて行われるなど、内容をともなった研究会開催が計画通り行われたと判断される。相互に研究交流の成果が得られるように、周到な準備をしていたことが認められる。