研究課題別事後評価結果

１．研究課題名：　安全な秘匿化データ処理を実現する汎用依頼計算技術

２．研究代表者名及び主たる研究参加者名（研究機関名・職名は研究参加期間終了時点）

研究代表者

花岡　悟一郎（産業技術総合研究所サイバーフィジカルセキュリティ研究センター　研究チーム長）

主たる共同研究者

浅井　潔（東京大学大学院新学術領域創成科学研究科　教授）

３．事後評価結果

○評点：

A+　期待を超える十分な成果が得られている

○総合評価コメント：

秘匿統計処理、秘匿マッチングでその普及のボトルネックとなっていた高速演算・スケーラビリティおよび汎用化を目指し､暗号理論と応用分野の実装の２グループがそれぞれの方面から研究を実施した。

効率的なレベル２準同型暗号の提案とその高速実装やユーザの無効化と追跡可能性を両立させて高機能な暗号、計算負荷がそれほど必要でない計算機能制限可能疑似ランダム関数の開発など暗号理論の研究として数々の成果を上げた。また分散データの保護に必要なノイズを抑えたマルチパーティ計算の開発など暗号技術の応用にも取り組んだ。これらの成果はトップ会議にも採択され高く評価されている。また、さまざまなマルチパーティ計算に使われる手法を統合して扱うことのできる「MAYBE フレームワーク」を提案し、目標である秘匿化計算の汎用化に向けて確実な進展を達成した。

要素技術の研究開発と並行して産業応用に耐えるソフトウェア整備を含めて当該技術の普及という大きな目標に挑戦して欲しい。