共同利用

ネットワークストレージを安全にするための暗号技術とその数学モデリング

種別	一般研究_研究集会(I)
研究計画題目	ネットワークストレージを安全にするための暗号技術とその数学モデリング
研究代表者	Kirill MOROZOV（東京工業大学・数理・計算科学系・特任准教授）
研究実施期間	平成29年6月12日（月）～ 平成29年6月13日（火）
研究分野のキーワード	分散ストレージ，情報セキュリティ，秘密分散法，秘匿計算，数学モデリング
目的と期待される成果	近年のコンピュータシステムとネットワークの急速な発展により，暗号技術の応用の重要性が強調されてきています．機密性と信頼性は共に暗号技術である秘密分散法を使用することで自然に達成されます．また実際に，これら二つの目的のため，秘密分散法はますます広く適用され，加えて効率性が追究されつつあります．例えば米国のIBMによって，また日本のTCSI社やIzumoBASE社によって提供されているクラウドストレージサービスが好例です．別の観点からは，データは格納できるべきのみならず，必要に応じ演算処理できるべきです．例えば，電子決済システムや医療データ処理などが該当します．この課題に対し，安全が保証されたデータ上の検索や計算は，秘匿計算の暗号技術によって実現される可能性があります． 秘密分散法や秘匿計算の技術がより広く受け入れられ実際に利用されるためには，徹底的なセキュリティ評価が必要です．この評価には，厳密な安全性証明と共に，実装システムの数学モデリングが伴われます．特に，以下の方向は，理論的な研究の観点から重要です．効率の向上；すなわち，計算量，通信量，ラウンド数，そしてランダムネスの複雑さ，等の縮小．また，安全性の仮定を弱めること；すなわち，半正直な攻撃者 対 悪意のある攻撃者，計算量的安全性 対 情報理論的な安全性，等．一方，数学的な見地からは，秘密分散法及び秘匿計算の研究開発は，抽象代数学，代数幾何学，マトロイド理論，組み合わせ論，ゲーム理論，情報理論，符号理論の応用を意味します． 本研究集会は（企画が採択されたならば），前回2016年9月5日から7日にかけて開催された秘密分散法の研究集会の成功を推し進めるものとなります．その目的は，データストレージ及び分散データ処理を安全にする秘密分散法，秘匿計算その他の暗号技術の実装例と数学モデリングの知見を共有するために，日本及び海外から産業界と学界の研究者を集めることです．更に，参加者はこれらの暗号技術を実装する際に産業界が直面している実際の問題を検討し，適切な解決案を議論し検討します． 本研究集会は，秘密分散法及び秘匿計算のチュートリアル，最近の結果についての招待講演，またパネル討論を含みます．成果物としては，すべての講演の短い要約及びスライドを含んだ会議録を出版することを計画しています．
組織委員(研究集会) **参加者(短期共同利用)**	Kirill MOROZOV（東京工業大学・数理・計算科学系・特任准教授） 穴田　啓晃（長崎県立大学情報セキュリティ学科・准教授） 須賀　祐治（㈱インターネットイニシアティブ・シニアエンジニア） 櫻井　幸一（公益財団法人九州先端科学技術研究所・研究室長）
成果報告書	【Web公開】成果報告書_共20170021.pdf