共同利用

プライバシ保護・分散型管理の次世代暗号技術とこれを支える数理構造

種別	研究集会(II)
研究計画題目	プライバシ保護・分散型管理の次世代暗号技術とこれを支える数理構造
研究代表者	穴田啓晃（公益財団法人九州先端科学技術研究所・情報セキュリティ研究室・研究員）
研究実施期間	平成27年9月1日（火）～ 平成27年9月3日（木）
研究分野のキーワード	クラウド向け暗号，暗号化状態処理，分散型管理，電子通貨
目的と期待される成果	インターネットに留まらず公共インフラそして民間のビジネス活動において，暗号の利用は今日欠かせないものとなった．例えば総務省住民基本台帳サービス，有料道路自動料金収受システム，ネットバンキング等である．これらの社会利用のため，暗号学の研究コミュニティは2010年程まで，主に情報資産の機密性・完全性・可用性の情報セキュリティ三大要件を満足する要素技術の研究を推進してきた． ところがここ5年程，これらの三大要件を超える期待が，暗号に対し高まってきた．この期待を少なくとも二つ挙げることができる．第一は利用者のプライバシ保護，第二は複数の運営者による分散型管理である． 利用者のプライバシ保護は，クラウドコンピューティングによる計算サービスやファイルストレージサービスの普及に動機付けられており，またWeb検索時の匿名化技術なども重要視されている．これらの期待に対し，暗号学は数理構造で応えようとしている．例として，多項式環のイデアルにノイズ相当の値を足し込む暗号化にブートストラップを適用する構造で，完全準同型暗号が発明され（Gentryら，2009年），暗号化状態処理が可能となり，プライバシ保護の解決の糸口が提供されつつある．他，Proof of Storage等の，クラウドに必要とされている技術の活発な研究がある． 複数の運営者による分散型管理は，近年では暗号通貨ビットコインの流行にその期待を見ることができる．そのピア・トゥ・ピアネットワーク上での完全にフラット（どのノードも対等）な取引き管理は，低い手数料による送金サービスを実現する．一方，マルチオーソリティに代表される，複数の運営者が共同で管理する公開鍵暗号の枠組みの研究も盛んである． 本応募で開催を提案する研究集会の目的は，産学官の研究者が，暗号へのこれらの新しい期待に応える最新の研究成果を紹介し，会場の参加者も巻き込み意見交換し，各々貢献しうることを相互理解することにある（「この要素技術／この社会利用のことは誰々に聴けば良い」）．加えて，グラフやネットワークの組み合わせ数学を得意とするインドの研究者，またプライバシ保護に強い中国の研究者を招き，国内の研究者らを刺激して頂く．結果として，期待に応えうる新しい要素技術の研究開発を推進する道筋と課題を共有したい．更に，本研究集会の参加者らがアイデアや動機を得るきっかけを提供し，引いては，暗号とこれを支える数学コミュニティに情報発信するものとしたい．このための成果物として，本研究集会の報告書及び会議録を想定している．
組織委員(研究集会) **参加者(短期共同利用)**	穴田啓晃（公益財団法人九州先端科学技術研究所・研究員） 安田貴徳（公益財団法人九州先端科学技術研究所・研究員） 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） 寺西勇（日本電気株式会社・主任）
成果報告書	【Web公開】成果報告書_共20150015.pdf