共同利用

社会基盤としての高機能暗号とその楕円曲線及び格子による実現

種別	研究集会(II)
研究計画題目	社会基盤としての高機能暗号とその楕円曲線及び格子による実現
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26年9月9日（火）～ 平成26年9月11日（木）
研究分野のキーワード	高機能暗号；属性ベース署名；社会基盤；楕円曲線；格子
目的と期待される成果	1970年前後にCocksらのチーム及びDiffieとHellmanらにより発明された公開鍵暗号は，30年程を経た2003年以降，次のフェーズに大きく移行している．BonehとFranklinが2003年，楕円曲線上のペアリングと呼ばれる双線型写像を本質的に用い，e-mailアドレスなど任意の個人識別情報（ID）を公開鍵に出来る暗号方式（IDベース暗号）を理論的に実現した．その後2004年にはキーワード検索可能な暗号方式（検索可能暗号），また2006年にはアクセス制御可能な暗号方式（属性ベース暗号）等が提案されている．これらの暗号方式は，電子署名方式や認証方式も巻き込み，いわゆる高機能暗号プリミティブ（以下，高機能暗号）として一大研究領域を形成している． 一方，実用に目を転じると，楕円曲線上のペアリング写像の高速実装，また暗号としての安全性が担保されるパラメータファミリの導出といった課題が浮上する．これらの課題に対し，数学の面から，処理アルゴリズムの工夫や評価，またパラメータの選定指針をテーマとする研究が，産学連携も含み活発に行われている．ただし高機能暗号に特化した形での実装については今後の研究開発が待たれている． また別の重要な課題として，これまでの暗号の安全性を根底から揺るがし兼ねない量子計算機の実現後においても安全な暗号方式の確立がある（耐量子暗号）．格子と呼ばれる有限次元ユークリッド空間内の整数係数部分加群について，その基底の選定の仕方と最近ベクトル問題の困難さを活用した暗号方式は，耐量子暗号の有力候補となっている．このため，高機能暗号の理論研究の最前線においては格子が主要な研究対象となっており，しかし理論の難易度の高さから，数学サイドからの貢献が期待されている． このように活発な活動状況ではあるものの，各々の研究領域が深化しているため，社会基盤の要素技術として実用化するのに必要な高機能暗号の課題，また必要な楕円曲線及び格子の理論は，実際には個々の研究者が各々研究しているに留まっている．加えて，これらの交差領域をテーマにした研究集会は，国内において例が無い．これらの事情が，高機能暗号が社会基盤の要素技術として確立されるのに障害となっている． 本応募にて計画する研究集会の目的は，上記の状況にある高機能暗号及び楕円曲線，格子の産学の研究者が各々の専門領域を互いに紹介し，交差領域の理解を深めることにある．成果物には，本研究集会の発表スライドを含めた会議録（冊子）を想定している．会議録のボリュームは，発表1件あたり40スライド程度，計10件程度の発表，1ページ当たり2スライドで，200ページ程度となる．また本研究集会の開催の結果として，高機能暗号を社会基盤の要素技術にするための課題が明らかになり，課題に対し参加者らが動機やアイデアを得るきっかけとなることが期待出来る．会議録にはこれらの結果を盛り込み，会議録を刊行することで関連業界に発信する．

組織委員(研究集会)	穴田　啓晃（公益財団法人九州先端科学技術研究所・研究員）
参加者(短期共同利用)	安田　貴徳（公益財団法人九州先端科学技術研究所・研究員） Xavier DAHAN（公益財団法人九州先端科学技術研究所・特別研究員） 櫻井　幸一（九州大学大学院システム情報科学研究院／公益財団法人九州先端科学技術研究所・教授／情報セキュリティ研究室長）