# 共同利用

## 安全・安心社会基盤構築のための代数構造

| | |
|---|---|
| **種別** | 研究集会(I) |
| **研究計画題目** | 安全・安心社会基盤構築のための代数構造 |
| **研究代表者** | 四方 義啓（名古屋大学・名誉教授） |
| **研究実施期間** | 平成25年8月26日（月）～ 平成25年8月30日（金） |
| **研究分野のキーワード** | 暗号、コンピュータセキュリティ、情報フロー, アクセス制御、ガロア理論、束、ガロア接続, 形式的概念分析 |
| **目的と期待される成果** | 公開鍵暗号は、有限群の構造を巧みに利用して、ネットワーク社会の安全性と信頼性確保に不可欠な基盤技術となっている。共通鍵暗号においても、DESの後継である国際標準ブロック暗号AESでは、拡大体の理論を用いて効率的実装を可能にしている。このように暗号の設計では、群や拡大体の理論が積極的に利用されている。<br>もう一つの代数構造である束も、アクセス制御に応用されている(研究としては、公開鍵暗号の発明よりも古いことに注意)。束におけるガロア理論のアナロジーとして、ガロア接続がある。<br>ソフトウエア工学では、形式検証において、このガロア接続も活用されている。最近では、ビッグデータの解析にも有効ということでさらに期待される。ようは、ランダムなデータの解析は、膨大な処理が必要になるが、その中の順序のある（部分）構造（ガロア接続）があれば、その処理を効率化できるというもの。<br><br>代数構造は、符号や暗号で基本的な役割を演じており、すでに多くの研究集会や国際会議も活発である。また、束(lattice)もコンピュータセキュリティへの現実応用理論がある。秘密分散では、マトロイドを用いて記述される成果も多く、離散数学の一分野を形成している。<br><br>しかし、こうした具体的産業応用をもつ代数構造を研究している研究者は互いに独立・分散している状況にある。<br>この共同利用研究集会では、産学の暗号とセキュリティ、数理学研究者が、代数構造の応用を議論する。暗号理論は、日本では世界レベルの研究者を多数かかえるが、ガロア接続をもちいたアクセス制御の設計と解析を行っている研究者は、国内ではほとんどいない状況、この方面の活性化を目的とする。<br>特に、ガロア接続をはじめ形式的概念分析のアクセス制御への応用は、まだ研究の歴史が浅く、計算論的解析も課題となっており、本研究集会を通じて数理学者と計算機科学者との交流討論の機会を得たい。<br>また、本研究集会の予稿集出版、ひいては拡張充実版を教科書として、この分野の研究者の参入のきっかけとしたい。 |
| **組織委員(研究集会)**<br>**参加者(短期共同利用)** | 櫻井幸一（九州大学　大学院システム情報科学研究院・教授）<br>安田 貴徳（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）<br>四方 義啓（名古屋大学・名誉教授）<br>Xavier DAHAN（九州大学システム情報科学研究院・特任助教） |