情報数学分野

情報数学分野においては，代数系や離散数学等の様々な数理構造の研究を基盤として，「情報」に関わる素材を対象とした数学を通して，広い意味での情報学を深く理解するための基礎理論の構築およびその応用研究を行っている．以下に，具体的な研究内容の一例を紹介する．

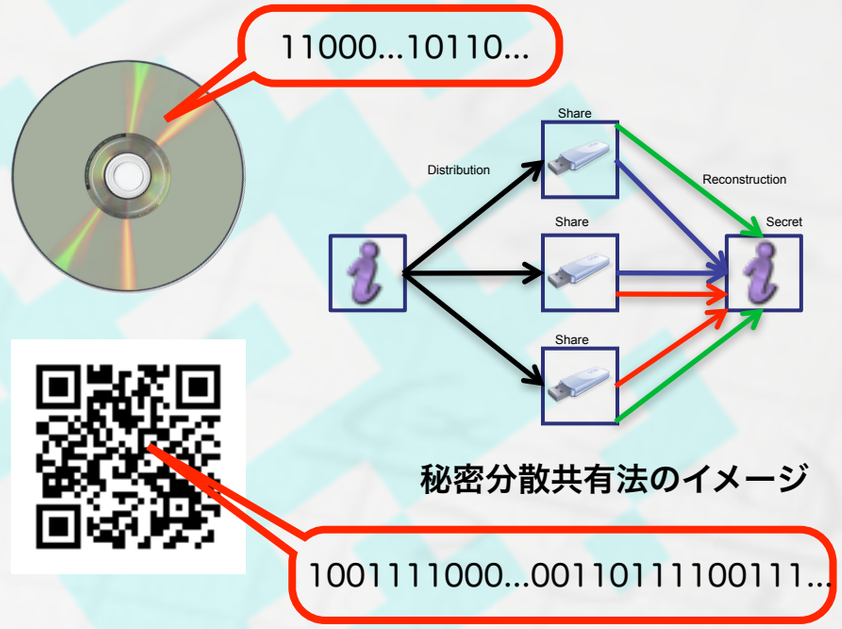
■ 数学の情報通信・情報セキュリティ分野へ応用研究

今後の超高度情報化社会を見据えてた場合に，大規模な情報通信や量子コンピュータの脅威に耐えうる通信技術や暗号技術が必要とされる．そこで，本研究室では主に以下の研究を実施している．

① CD・DVD等の記憶装置や2次元バーコード等にも幅広く利用されている，デジタル情報を伝送・記録する際に生じる誤りを数学的に訂正するための**誤り訂正符号**についての新たな符号の構成や復号アルゴリズムの検討

② クラウドコンピューティングやビットコイン・ブロックチェーン等での秘密保持技術として期待されている**耐量子計算機暗号**と言われている次世代の暗号システムや**秘密分散共有法**についての行列や格子と言われる数学構造を利用した暗号の構成，組合せ数学を用いた分散処理の考察や安全性の検討

キーワード：符号，暗号，秘密分散法，アルゴリズム



秘密分散共有法のイメージ

■ グラフの分割問題とビッグデータのクラスタリングに関する研究

SNSなどのソーシャルメディアの急速な普及に伴い，大量かつ多様なデータ，いわゆる**ビッグデータ**を効率良く高速に処理する技術が現代社会では必要とされている．特に，そのような構造を解析するために，データ構造の中から特定の有用な部分構造を切り出す手法（**クラスタリング抽出**）の研究が重要な課題の１つとなっている．そこで，本研究室では，正則性の高い構造へのグラフ（図形）の分割問題に対する解の存在性やアルゴリズムについて考察することで，クラスタリング抽出への応用研究を実施している．

また，閉路や道の構造へのグラフの分割問題から，通信網におけるグループネットワークの構成や巡回セールスマン問題などの経路最適化への応用研究も実施している．

キーワード：グラフの分割，ビッグデータ，クラスタリング，通信網，経路最適化