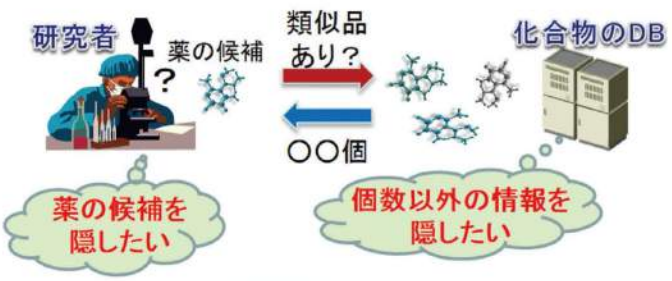
# 生命情報工学を支援する暗号技術の開発

縫田 光司
（アルゴリズムチーム 主任研究員）

生命情報工学の分野では、名称の通り生命現象にまつわる様々な情報を扱います。それらのうち、一般に未公表で価値の高い情報や、人々のプライバシーにかかわる情報については、取扱いの効率性だけでなく安全性も同時に重視する必要があります。CBRCでは、2011年から産総研セキュアシステム研究部門と連携して、最新の暗号技術に基づき、生命情報工学分野における情報・プライバシー保護技術を研究開発しています。

例えば、創薬に用いられる化合物データベースの検索について、検索を行うユーザ側とデータベース側双方の情報を秘密にしながら、必要な検索結果のみをユーザに返答する「秘匿検索技術」を開発しました。新薬の候補となる化合物を研究者（ユーザ）が既存の化合物データベースから探す際、「どのような化合物を探しているか」は新薬開発における極秘事項であり、データベース保有者にすら教えたくありません。現状では解決策の一つとして、ユーザが化合物データベースを丸ごと購入して手元で密かに検索する手段がとられています。しかし、必要な化合物情報を含んでいるか定かでない高価なデータベースの購入はためらわれますし、一方でデータベース自体も貴重なため、データベース保有者としては購入前のユーザに対してデータベースを自由に「試し読み」させるわけにもいきません。

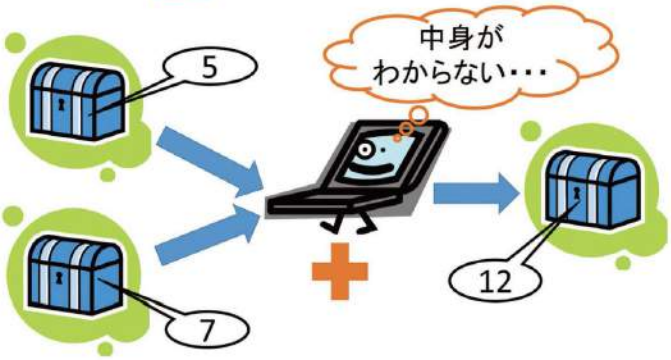
このユーザとデータベース保有者の間のジレンマを解消するため、探している化合物とデータベースの中身をともに秘密にしたまま、「目的の化合物の情報がデータベースにどのくらい含まれているか」だけをユーザに返答できる特殊なデータベース検索プロトコルを開発しました（図1）。




【図1】化合物データベースの秘匿検索技術

この成果については情報セキュリティ分野で国内有数の研究会議「コンピュータセキュリティシンポジウム2013」で優秀デモンストレーション賞を受賞するなど、生命情報工学分野だけでなく情報セキュリティ分野からも重要性が認められています。

上述の化合物データベース秘匿検索技術では、構成要素として「準同型暗号」を用いています。準同型暗号とは、足し算、掛け算など予め定められた種類のデータ操作について、データを暗号化して秘密に保ったままの状態で演算を行う機能を持つ暗号技術です（図2）。




【図2】足し算のできる準同型暗号の模式図

私自身は元々数学者であり生命情報工学の専門家ではありませんが、こうした暗号的な要素技術の開発や、プロトコルの数学的安全性評価などで上記の研究に携わっています。この4月より装いを新たにしたCBRCの研究ミッションの一つであるゲノム情報の利活用と保護の両立についても、これまでに培った数学と暗号の知見を基に貢献していきます。

大学院生の頃はいわゆる純粋数学（群論と組合せ論）を専攻していました。産総研に入ってからは暗号の研究をしつつ、そこで見つけた数学の問題に取り組んでいました。今年度からはCBRCの一員として、生命情報工学分野の研究に貢献しつつ、また新たな数学の問題を見つけられたらいいな、と思います。