データベースの秘匿検索技術

産業技術総合研究所　情報技術研究部門
高機能暗号研究グループ　縫田　光司

データ検索・マッチング時の情報流出事故を根本的に予防

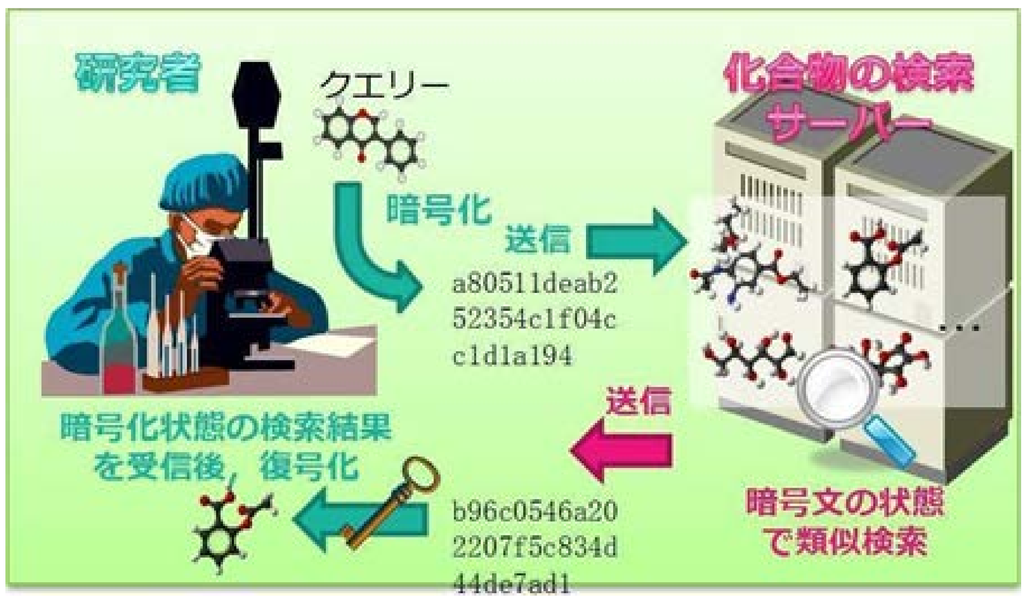
- 何を検索したいかをデータベース側に明かさずにデータ検索を実行できる技術
- 検索結果のみを通知、それ以外の検索内容・データベース情報を相互に秘匿
- 共通データ検索、ゲノム情報検索など多様な検索用途へ対応した技術を開発

研究のねらい

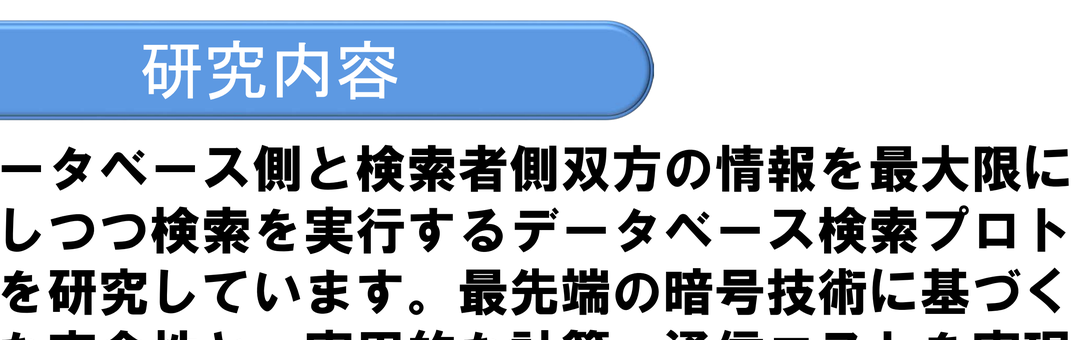
医療情報などのプライバシーに関わる情報や、研究開発に関わる機密性の高い情報について、データベース側に検索内容を開示することなく、また同時に検索者側にも検索結果以外のデータベース情報が開示されない状態での情報検索の実現を目指しています。本研究で開発した技術を用いて産業界や自治体サービス分野等でのデータベース利活用の促進に貢献するため、創薬分野で利用される化合物データベースをはじめ、産業的、学術的、社会的に重要な各種データベースについて秘匿検索を可能とすることによりデータ保有者が安心できる形でデータの分析を行える技術基盤の構築を目指しています。

研究内容

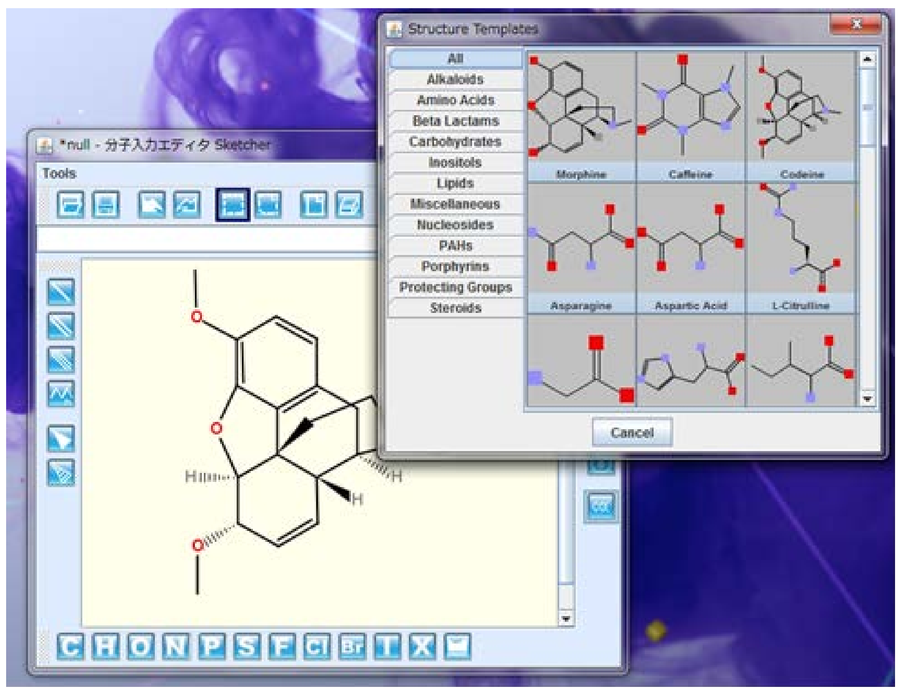
データベース側と検索者側双方の情報を最大限に秘匿しつつ検索を実行するデータベース検索プロトコルを研究しています。最先端の暗号技術に基づく強固な安全性と、実用的な計算・通信コストを実現する効率性の両立を目指しています。特に、データを秘匿しながら情報処理可能な高機能暗号を効率化しつつ上手く組み合わせることで、化合物データベースの類似度秘匿検索、スマートフォン電話帳の共通データ秘匿検索、多次元データの範囲秘匿検索、ゲノム配列情報の最長部分一致秘匿検索といった多様な検索を安全に行うプロトコルを開発しています。



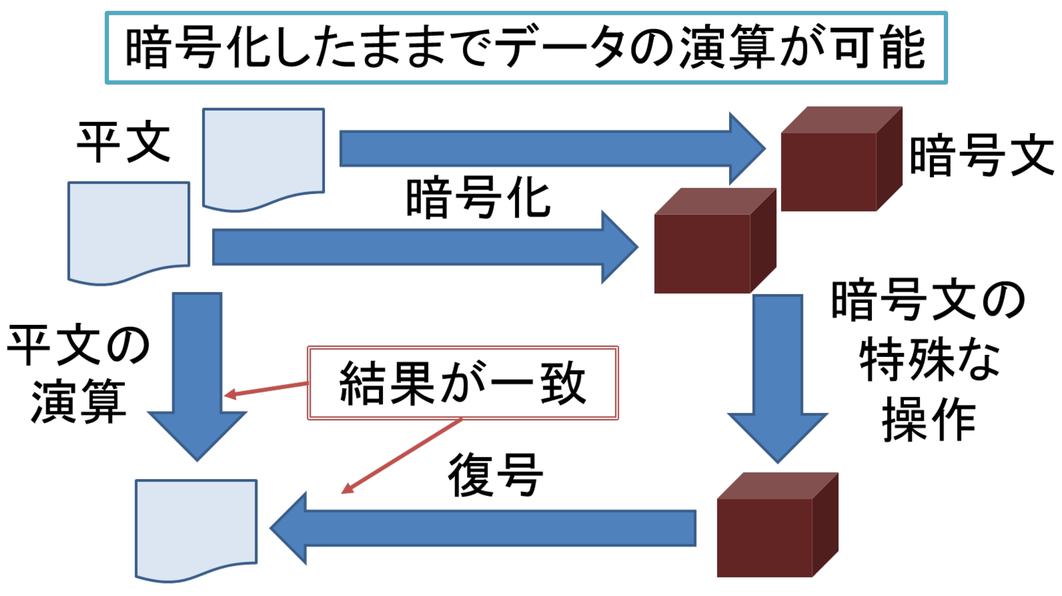
化合物データベースの秘匿検索



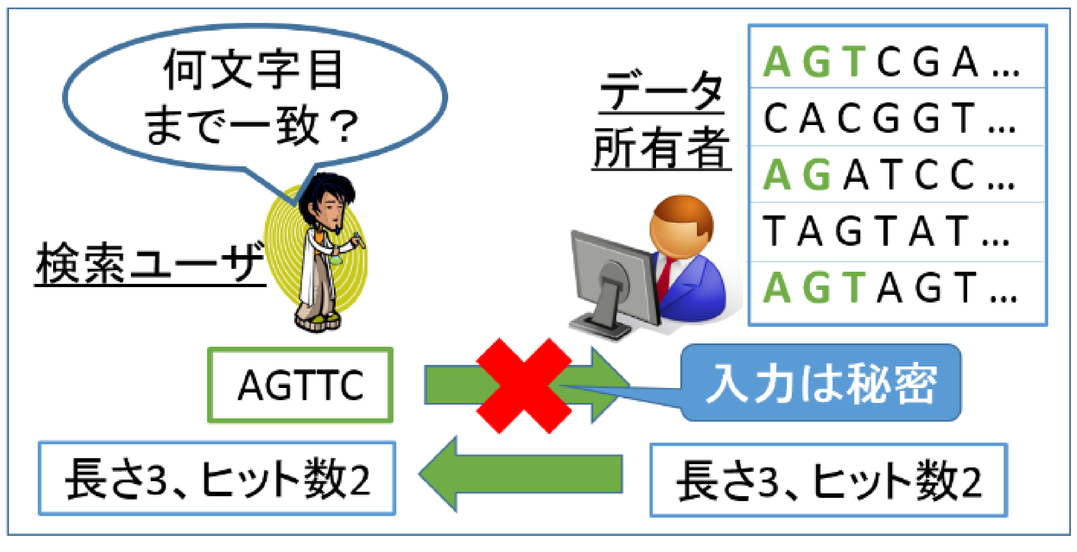
電話帳データの共通部分秘匿検索



実システム適用を想定した実装



構成要素技術の例：準同型暗号



ゲノム配列の最長一致秘匿検索