公開鍵検索可能暗号の拡張

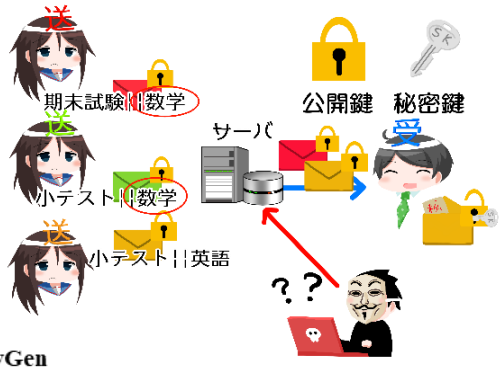
Extension of public key encryption with keyword search

柴山 綸太郎・システム分科会・情報セキュリティ大学院大学

Abstract：Searchable encryption (SE) is an encryption method that allows keyword search without decoding ciphertext. When saving data to an external server with low reliability, there is a possibility of encrypting and saving the file for security. In such a scenario, SE that enables retrieval while keeping the keyword concealed to the server is effective. In this poster, we report extensions of SE with public key.

公開鍵検索可能暗号

公開鍵検索可能暗号(Public key Encryption with Keyword Search, 以下PEKS)は2004年にBonehらが提案した．登場人物として暗号化されたファイルに対して検索を行いたい受信者，ファイルを送信する送信者，そしてデータを保存するサーバの三者を用意する．BonehらのPEKSは以下の4アルゴリズムからなる．



- **KeyGen**

受信者が実行する鍵生成を行う確率的アルゴリズムである．セキュリティパラメータλを入力とし，公開鍵pk及び秘密鍵skを出力する．

- **PEKS**

送信者が実行する検索用キーワードを暗号化する確率的アルゴリズムである．暗号文に紐づけたいキーワードwを入力とし，キーワードに対応した検索可能暗号文c_wを出力する．

- **Trapdoor**

受信者が実行する検索用トラップドアを生成する確率的アルゴリズムである．検索したいキーワードをw'を入力とし，キーワードに対応した検索用トラップドア$\mathrm{Td}_{w'}$を出力する．

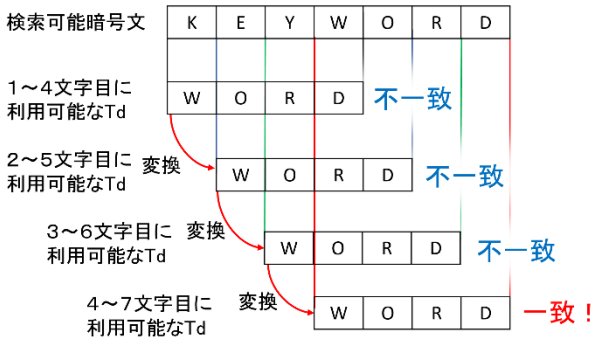
- **Test**

サーバが実行するキーワード判定を行う確定的アルゴリズムである．cとTdの1つずつを入力とし，キーワードが一致したときには1を，そうでないときには⊥を出力する．

サーバはどの暗号文が検索に一致したかは知ることができるが，送信者がサーバに送信した検索可能暗号文からはキーワードに関する情報は漏れない．

PEKSの拡張方式

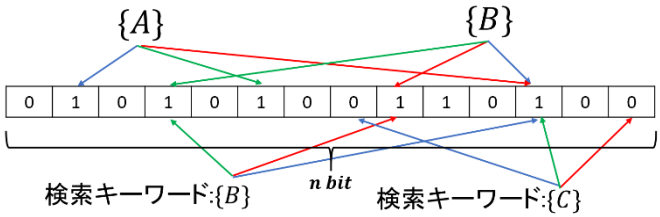
PEKSの拡張のひとつとして，文字列の部分一致検索が可能な方式が知られている．受信者が検索の際トラップドアに入力したキーワードを含むものを判定できる方式である．この方式では検索可能暗号文を生成する際にキーワードを一文字ずつ暗号化する．サーバが実行するTestアルゴリズムでは，トラップドアを変換しながら検索可能暗号文の要素を前から探索していき，部分一致判定を行う．



ブルームフィルタ

ブルームフィルタとは1970年にBloomが提案した確率的データ構造である．偽陽性による誤検出の可能性があるが，キーワードを空間効率よく登録し検索可能である．

登録キーワード：$\{A, B\}$をハッシュH_1, H_2, H_3で登録



今後の研究方針

ブルームフィルタとPEKSの組み合わせ，送信者のアクセス制御など，他の技術との組み合わせを模索しつつPEKSの拡張を目指していきたい．