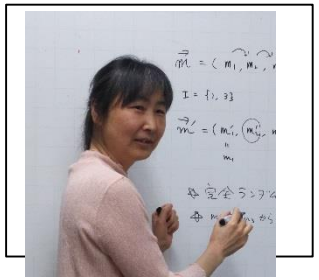
情報通信工学	通信ネットワーク・セキュリティ	暗号理論，ディジタル署名，マルチパーティプロトコル，
情報通信系	教授	尾形 わかは



過去の研究実績

1. 効率の良い検証可能な検索可能暗号方式の提案
2. 情報量的安全性を持つパスワード付秘密分散法の提案と実装
3. 複数の秘密情報を効率よく分散するのに適した計算量的安全性を持つ秘密分散方の提案
4. 否認不可署名の安全性評価

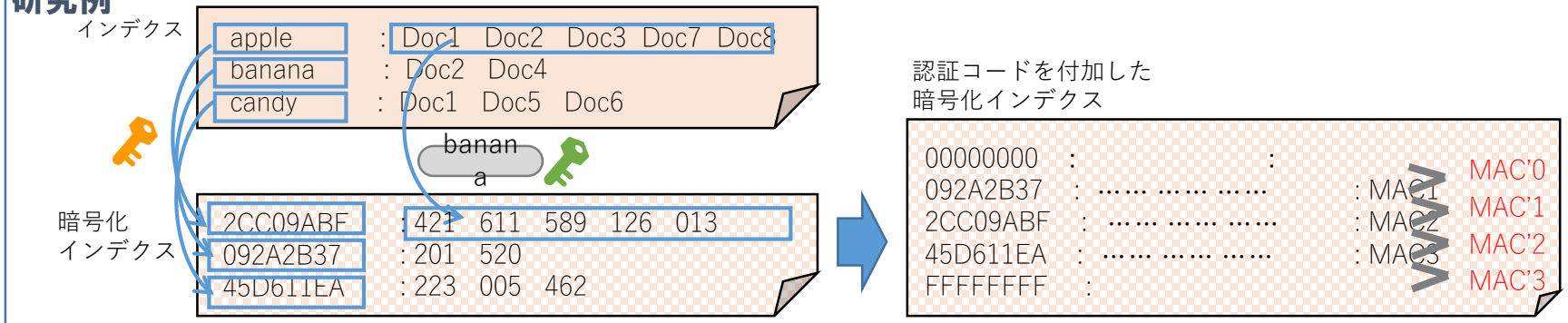
現在、注力している研究

1. 効率・使い勝手・プライバシー保護をバランスさせた，検索可能暗号方式の設計
2. プライバシーを保護したビッグデータ解析手法の設計
3. 公開鍵証明書が不要で多数のディジタル署名を圧縮保存・検証可能な署名方式を安全性解析と設計

今後取り組んでいきたい研究

1. 検証可能で効率の良い分散データストレージの開発
2. 量子コンピュータ普及後に利用可能な暗号技術の開発

研究例



検索用インデクスを適切に暗号化し，さらに認証コードをつけることで，プライバシーと保護したまま検索が実現できる

利便性と安全性は相反しますが，できるだけ利便性を損なわずに安全性を確保する方法を探索しています．また，利用場面やユーザの希望に応じて，利便性と安全性のバランスを取ることが出来るシステムも目指しています．
単純な暗号技術の組合せでは必要な安全性が確保できない場合もあるため，常に厳密な安全性証明を行っています．

③ http://www.crypt.ict.e.titech.ac.jp/，ogata.w.aa@m.titech.ac.jp