高圧縮・高セキュリティ・高速処理を実現する幾何学的データ暗号方式

六井　淳（総合理工学部）

本研究に関連する特許
1）特許第6296589号

【概要】

代表的な暗号方式として，暗号化と復号化に同一の鍵を用いる共通鍵方式と，暗号化と復号化に別々の鍵を用いる公開鍵方式がある。

共通鍵方式はブロック暗号と呼ばれる方式が幅広い分野で利用されており，米国政府標準暗号として知られるData Encryption Standard（DES）が長く標準暗号として利用されてきた。

本研究では，幾何学的アプローチに基づいた全く新しい共通鍵暗号方式を提案する。木構造の構造情報とデータの配置情報の幾何学的組み合わせを利用した暗号方式であり，高圧縮，高セキュリティ，高速処理の特徴を持つ。

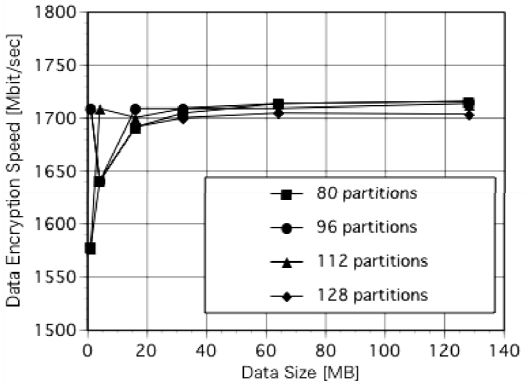


図１　暗号化処理速度

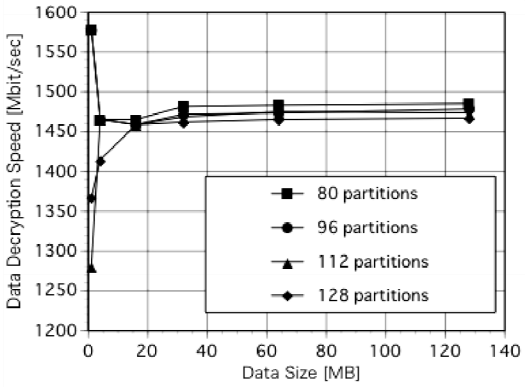
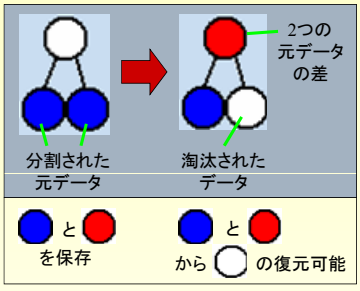


図２　復号化処理速度

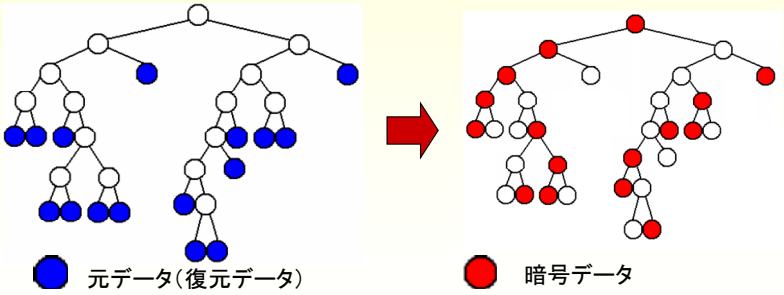
同一計算機環境　AES（DESの改良版）比で約4～5倍の処理速度を実現

木構造を用いた幾何学的データ暗号方式



符号化を行うことで，差分データは高い圧縮効果を得られる（左図）。

木構造を鍵とする暗号化であり，分割数12で木構造は58786，リーフノードは479001600，組み合わせは21858588057600となり，膨大な組み合わせ数，強度を実現。



復元のためには，木構造情報とデータ配置情報の2つが必要。鍵情報を分離管理することで高いセキュリティ強度が得られる。

【応用例】

- 安全かつ高速，高圧縮機能を両立させた暗号通信
- 二重鍵特性を利用したライセンス管理
- 通信経路と保存の双方を暗号化した情報共有化システム

【研究シーズ，特許に関するお問い合わせ先】
島根大学 地域未来協創本部 産学連携部門
〒690-0816　島根県松江市北陵町2番地
電話：0852-60-2290　FAX：0852-60-2395　電子メール：crcenter@ipc.shimane-u.ac.jp