[Work in Progress] 研究報告

暗号の危殆化に対応可能なオンラインストレージシステムに関する検討

岡部 大地[1,a)]　石橋 拓哉[1]　木村 隼人[1]　渡邉 英伸[2]　大東 俊博[1]

A Study on Online Storage System using Proxy Re-Encryption Scheme for the Compromise of Cryptographic Algorithms

データを安全にオンラインストレージに預ける際，ユーザは自身のデータを暗号化して機密性や完全性を保護する．しかし，暗号アルゴリズムは常に安全というわけではなく，計算機能力の向上や暗号解読法の高度化によって安全性の低下（危殆化）が生じてしまうことがある．例えば，無線 LAN の暗号プロトコルである WEP に対するストリーム暗号 RC4 の脆弱性に起因した鍵復元攻撃 [1]，メール受信用プロトコル APOP への MD5 の脆弱性に起因したパスワード解析攻撃 [2] などの事例がある．危殆化が生じた場合，預けている暗号化ファイルを安全なアルゴリズムに置き換える必要が出てくる．オンラインストレージシステムにおいて危殆化が発生した場合，通常の危殆化対策ではストレージ内にある暗号化ファイルを一度ダウンロードし安全なアルゴリズムで再暗号化してからファイルをアップロードする必要があり，通信量や計算量に関するユーザの負担は比較的大きい．

ユーザを介さずに暗号文を別の暗号文へ再暗号化する技術としてプロキシ再暗号化が知られている．プロキシ再暗号化は再暗号化鍵を用いることで復号することなく別のユーザの暗号文に変換できる方式である．一般的にプロキシ再暗号化は公開鍵暗号の一種として提案されている．本研究では共通鍵暗号型のプロキシ再暗号化 [3] に注目し，その方式が鍵の変更だけでなく，アルゴリズムの変更にも応用可能であることを示す．さらに，提案方式に基づくオンラインストレージシステムに関して検討する．

共通鍵暗号型のプロキシ再暗号化は共通鍵暗号のストリーム暗号から実現される．ストリーム暗号の本質は擬似乱数生成器であり擬似乱数生成器を $f()$ としたとき，ストリーム暗号では秘密鍵 K を用いて擬似乱数列（キーストリーム）を $Z = f(K)$ のように得る．暗号化の際には平文 M と同じサイズのキーストリーム Z を排他的論理和（XOR）することで暗号文を作成し，復号の際は同じキーストリーム Z を XOR して平文 M を得る．共通鍵暗号型のプロキシ再暗号化ではユーザ A とユーザ B の持つ鍵 K_A，K_B から生成したキーストリーム $Z_A = f(K_A)$ と $Z_B = f(K_B)$ を生成し，再暗号化鍵 $Z_A \oplus Z_B$ を作成する．再暗号化鍵を用いることでユーザ A 用の暗号文 $C_A = M \oplus f(K_A) = M \oplus Z_A$ をユーザ B が復号することができる暗号文 $C_B = C_A \oplus (Z_A \oplus Z_B) = M \oplus Z_A \oplus (Z_A \oplus Z_B) = M \oplus f(Z_B)$ に変換できる．このプロキシ再暗号化方式では Z_A=$f(K_A)$ で作った暗号文を $Z_B = f(K_B)$ で作った暗号文に置き換えているが，例えば別のストリーム暗号の擬似乱数生成アルゴリズム $f'()$ を用いた $Z'_A = f'(K'_A)$ に置き換えるような変換も可能である．このように変換する対象を鍵の種類ではなく，アルゴリズムの種類に置き換えることで，暗号の危殆化が生じた際にアルゴリズムを変更する再暗号化処理が可能となる．

1 東海大学 情報通信学部，School of Information and Telecommunication Engineering, Tokai University
2 広島大学 情報メディア教育研究センター，Information Media-Center，Hiroshima University
a) 6bjt2208@mail.u-tokai.ac.jp

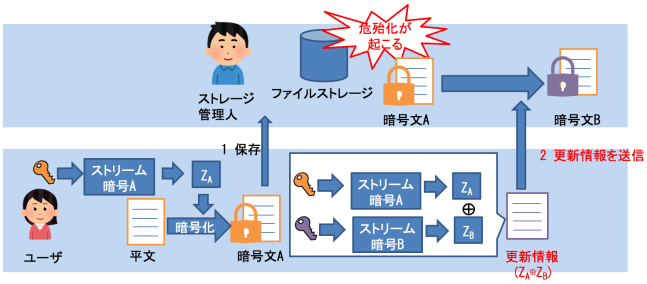

図 1　危殆化に対応可能なオンラインストレージシステム

表 1　実験結果の処理時間 [ms]

	1KB	10KB	100KB	1MB	10MB
暗号化/復号	0.06	0.36	3.36	33.86	335.74
更新情報作成	0.09	0.66	6.46	63.94	636.31
再暗号化	0.03	0.07	0.36	3.41	33.49

上記で述べたアルゴリズムの変更が可能な共通鍵暗号型プロキシ再暗号化方式を利用したオンラインストレージシステムを図 1 に示す．提案システムでは，暗号の危殆化が発生した場合に平文と同じサイズの再暗号化鍵を作成し，サーバにアップロードする．サーバでは，再暗号化鍵を利用して再暗号化を行うことで暗号文は安全な暗号で暗号化された状態になる．この場合，再暗号化をユーザ側で行う従来方式と比べて通信がアップロードだけになるため通信量を 1/2 に削減できる．通信以外の処理時間に関しては実験によって評価をした．2.7GHz CPU，8GB Memory の環境において，複数のファイルサイズで暗号化/復号，更新情報生成，再暗号化の処理時間を計測した結果を表 1 に示す．処理時間は 100 回実行した平均値である．クライアント側で必要な処理時間は従来方式では暗号化/復号の 2 倍の時間，提案方式では更新情報生成の時間が必要であるが，実験結果よりそれぞれが同程度であることがわかった．サーバ側で再暗号化処理が必要となるが，その処理時間も十分に小さいことが確認できた．提案システムの安全性および認証付き暗号としてデータを暗号化するとこの対処についても考察しているが，紙面の都合により割愛する．

参考文献

[1] E. Tews, R. Weinmann, and A. Pyshkin,"Breaking 104 Bit WEP in Less Than 60 Seconds,"Proc. WISA 2007, LNCS, vol.4867, pp.188–202, Springer, 2007.
[2] Y. Sasaki, L. Wang, K. Ohta, and N. Kunihiro, "Security of MD5 Challenge and Response: Extension of APOP Password Recovery Attack," Proc. CT-RSA 2008, LNCS, vol.4964, pp. 1–18, Springer, 2008.
[3] D. Watanabe, H. Sakazaki and K. Miyazaki, "Representative System and Security Message Transmission using Re-encryption Scheme Based on Symmetric-key Cryptography" JIP, vol. 25, pp.67–74, 2017.