SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Intel SGX を用いたアルゴリズム変換型プロキシ再暗号化システムの実装・評価
Implementation and Evaluation on a Proxy Re-Encryption System for Conversion of the Cryptgraphical Algorithms using Intel SGX

西平　侑磨 * 鈴木　達也 † 渡邉　英伸 ‡ 大東　俊博 * §
Yuma Nishihira Tatsuya Suzuki Hidenobu Watanabe Toshihiro Ohigashi

キーワード 暗号アルゴリズムの更新，プロキシ再暗号化，オンラインストレージ，Intel SGX，TEE

あらまし

暗号の 2010 年問題のように安全性を保つため政府機関が鍵長の長い暗号アルゴリズムへの移行を推進した場合や複数のサービスを統合する際に暗号アルゴリズムの統一をしたい場合などに暗号アルゴリズムの変更が求められる．岡部らは IOTS 2018 において暗号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提案した [1]．この方式ではユーザが更新前の暗号アルゴリズムと更新後の暗号アルゴリズムの疑似乱数列を排他的論理和 (XOR) することで再暗号化鍵を生成してサーバへ送信し，サーバで暗号文と XOR することで暗号アルゴリズムを更新する．これにより通信回数は削減されるが，再暗号化鍵が暗号文のサイズに依存するため巨大なサイズの暗号文を再暗号化する際，通信にかかる負担が大きくなる．

そこで本稿では Intel SGX を用いたアルゴリズム変換型プロキシ再暗号化システム (図 1) を提案する．このシステムでは，ユーザは Remote Attestation によって共有される共通鍵でアルゴリズム更新対象の秘密鍵 K を暗号化しサーバへ送る．サーバは Enclave 内で復号を行い秘密鍵 K を得る．この秘密鍵 K を更新前の暗号アルゴリズム $f()$ と 更新後の暗号アルゴリズム $f'()$ に入力し得られた疑似乱数列 Z , Z' から再暗号化鍵 $Z \oplus Z'$ を生成し，暗号文の暗号アルゴリズムを更新する．提案方式ではサーバ側で再暗号化鍵を生成するため，ユーザは秘密鍵と同サイズの暗号文を送信するだけで良い．

* 東海大学情報通信学部, 〒 108-8619 東京都港区高輪 2-3-23
† 筑波大学理工情報生命学術院, 〒 305-8571 茨城県つくば市天王台 1-1-1
‡ 広島大学情報メディア教育研究センター, 〒 739-8511 広島県東広島市鏡山 1-4-2
§ 情報通信研究機構, 〒 184-8795 東京都小金井市貫井北町 4-2-1

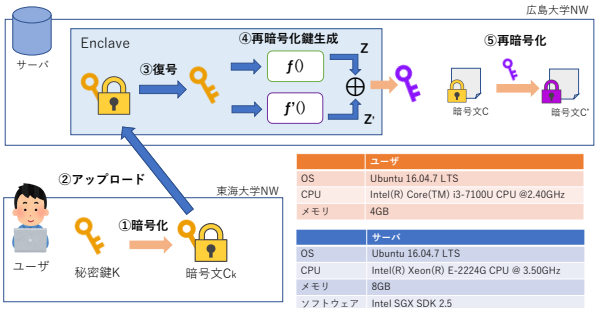

図 1: 提案手法の概要および実験環境

表 1: 暗号文サイズごとのユーザが要する時間 [sec]

	提案手法		岡部らの手法	
	処理	通信	処理	通信
1MB	0.00001	1.69595	0.02197	0.45108
10MB	0.00002	1.65604	0.16897	1.98394
100MB	0.00001	1.72994	1.66202	17.3692
200MB	0.00002	1.72778	3.31859	34.3965
300MB	0.00001	1.68699	4.96972	54.8759

暗号アルゴリズムの更新する際に岡部らの方式と比べて提案方式はユーザが要する時間をどの程度短縮できるかの実験を行った．実験では 10 回の試行の平均値を取得した．表 1 より提案手法でユーザが要する時間は一定となり，岡部らの手法と比較すると 10MB 程度から提案手法が有効となることがわかった．また表 1 には記載していないが，提案手法のサーバが要する時間は岡部らのユーザの処理時間と同程度であり，暗号アルゴリズム更新時間全体でも提案手法が有効となる．

参考文献

[1] 岡部大地，石橋拓哉，木村隼人，渡邉英伸，大東俊博,“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,” インターネットと運用技術シンポジウム論文集，第 2018 巻，p.41，Nov. 2018.