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

ユーザの持つメモリが定数な検証可能な動的検索可能暗号
Verifiable Dynamic Symmetric Searchable Encryption with Constant User Memory

小澤 響平 * 山本 博章 † 藤原　洋志 ‡
Kyohei Ozawa Hiroaki Yamamoto Hiroshi Fujiwara

キーワード 検索可能暗号, 動的データ, 検証可能, Forward 安全, Backward 安全

あらまし

近年、クラウドサービスの普及によって、クライアントが自分のデータをサーバに保存する機会が増えている。このとき、データを暗号化したまま検索ができることが望まれるが、そのようなシステムのことを検索可能暗号と呼ぶ。我々はデータの検索、更新、検証結果の検証が行える検索可能暗号を開発した。この手法はデータを二分木構造で管理することにより並列化が可能であり、データの更新に関する安全性である Forward 安全と Backward 安全を満たしている。しかしユーザは多くのデータを持つ必要があったため、本論文では同様の安全性を満たし、ユーザの持つデータ量を削減した手法を提案する。

* 信州大学大学院, 長野県長野市若里 4 丁目 17- 1, Graduate school, Shinshu University, 4-17-1, Wakasato, nagano city, nagano
† 信州大学, 長野県長野市若里 4 丁目 17- 1, Shinshu University, 4-17-1, Wakasato, nagano city, nagano
‡ †