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

鍵失効可能な検索可能暗号

A Study on Searchable Encryption with Key Revocation

平野 貴人 * 川合 豊 * 小関 義博 * 渡邉 洋平 †
HIRANO, Takato KAWAI, Yutaka KOSEKI, Yoshihiro WATANABE, Yohei
岩本 貢 † 太田 和夫 †
IWAMOTO, Mitsugu OHTA, Kazuo

キーワード 検索可能暗号，鍵失効，安全性.

あらまし

検索可能暗号とは，秘密鍵を持つユーザが，暗号化されたキーワードを用いて，暗号化されたデータを復号することなく検索できる暗号技術である．

著者らは，SCIS2021 にて鍵更新可能な検索可能暗号を提案した [1]．本稿では，更に鍵失効ができる検索可能暗号を提案する．また，鍵失効に関わる安全性を定式化し，提案方式はその安全性を満たすことを証明する．

参考文献

[1] 平野，川合，小関，渡邉，岩本，太田．“検索可能暗号の鍵更新について．SCIS2021，3B2-1.

* 三菱電機株式会社，神奈川県鎌倉市大船 5-1-1.
† 電気通信大学，東京都調布市調布ヶ丘 1-5-1.