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

高効率な失効機能付き ID ベース認証鍵交換の構成
Construction of Efficient Revocable Identity-Based Authenticated Key Exchange

中川 皓平 * 割木 寿将 † 岡野 裕樹 * 藤岡 淳 † 永井 彰 *
Kohei Nakagawa Kazuma Wariki Yuki Okano Atsushi Fujioka Akira Nagai

キーワード RIB-AKE プロトコル, rid-eck モデル, 失効機能付き ID ベース認証鍵交換

あらまし

ID ベース AKE には長期運用の観点から, PKI と同様, 鍵失効機能が必要とされる. 失効機能を有する既存の ID ベース AKE としては, PKG を階層化した RHIB-AKE が存在する [1]. この RHIB-AKE は, 階層化により PKG の鍵生成にかかる負担を抑えることができる反面, 各参加者の鍵交換に要する計算コストが大きい. ID ベース鍵交換は IoT 機器などの計算リソースの小さい機器上での応用が期待されているため, より小さい計算コストで鍵交換プロトコルを実行できることが望ましい. そこで本稿では, PKG を階層化しないような失効機能付き ID ベース AKE(RIB-AKE) を新たに考え, その安全性の定義と実現例を与える. なお, 実現例については KEM に基づく generic な構成と, より計算コストの小さい dedicate な構成を示す.

参考文献

[1] 岡野 裕樹, 米山 一樹, 藤岡 淳, 永井 彰, “失効可能な階層型 ID ベース認証鍵交換の安全性モデルと構成について,” SCIS2021.

* NTT 社会情報研究所 〒 180-8585, 東京都武蔵野市緑町 3-9-11. NTT Social Informatic Laboratories, 3-9-11, Midoricho, Musashino-shi, Tokyo 180-8585, Japan. kouhei.nakagawa.yz@hco.ntt.co.jp
† 神奈川大学 〒 221-8686 神奈川県横浜市神奈川区六角橋 3-27-1, Kanagawa University, 3-27-1, Rokkakubashi, Kanagawa-ku, Yokohama-shi, Kanagawa 221-8686, Japan.