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

効率的な漏洩耐性鍵隔離暗号
An Efficient Construction of Leakage-Resilient Key-Insulated Encryption

淺野 京一 * 岩本 貢 * 渡邉 洋平 * †
Kyoichi Asano Mitsugu Iwamoto Yohei Watanabe

キーワード 鍵隔離暗号, 漏洩耐性暗号, 漏洩耐性鍵隔離暗号, 漏洩耐性秘密分散法

表 1: 漏洩耐性秘密分散法の比較

$(2,2)$-LR-SS	計算量 (Share)	計算量 (Rec)	シェアのサイズ	適応的安全性
[2]	$2(O_{\mathsf{Share}'} + O_{\mathsf{Ext}})$	$2(O_{\mathsf{Rec}'} + O_{\mathsf{Ext}})$	$2(\eta + d + m)$	✓
提案方式	$O_{\mathsf{Share}'} + O_{\mathsf{Ext}}$	$O_{\mathsf{Rec}'} + O_{\mathsf{Ext}}$	$\eta + d + 2m$	–

あらまし

公開鍵暗号における秘密鍵の漏洩への対策の 1 つとして鍵隔離暗号 (KIE) がある．KIE では, 利用者が復号鍵と補助鍵の 2 種類の秘密鍵を持ち, 補助鍵を用いて復号鍵を定期的に更新することで, 復号鍵が漏洩していない期間の安全性を保証できる．このように, KIE では秘密鍵が一切漏洩していない期間の安全性は保証されるが, 部分的にでも秘密鍵が漏洩した時点でその期間の安全性は保証できない．一方, 秘密鍵が部分的に漏洩した場合でも安全性を保証する公開鍵暗号として漏洩耐性暗号 (LR-PKE) が知られているが, KIE のように復号鍵を更新する機構を持っておらず, 秘密鍵全体が漏洩した場合の安全性を保証できない．そこで淺野ら [1] は, CSS 2021 において, KIE が満たす安全性と LR-PKE が満たす安全性を両立する公開鍵暗号として, 漏洩耐性鍵隔離暗号 (LR-KIE) とその構成を提案した．本稿では, 淺野らの提案した構成を見直し, より効率的な構成を提案する．具体的には, 淺野らの構成に用いられている漏洩耐性秘密分散法 (LR-SS) に要求する安全性を弱められることを示し, そのような弱い安全性を満たす効率的な LR-SS の構成を提案する．

表 1 で, 本稿で提案する安全性を弱めた漏洩耐性秘密分散法と, 淺野らの構成に用いられている LR-SS [2] を具体的に作った場合を比較した．ただし, Share はシェアを生成するアルゴリズムで, Rec はシェアから元の秘密を復元するアルゴリズムとする．また, それぞれ内部で秘密分散法と抽出器を使用しているが, それぞれの計算量を $O_{\mathsf{Share}'}$, $O_{\mathsf{Rec}'}$, O_{Ext} とし, $(\eta, \mu + l, d, m, \epsilon_{\mathsf{Ext}})$-抽出器で用いるソースのサイズを η, シードのサイズを $d = \mathcal{O}(\log(\eta/\epsilon_{\mathsf{Ext}}))$, 秘密のサイズを m, 漏洩量を l とする．

参考文献

[1] 淺野京一, 岩本貢, 渡邉洋平, “秘密鍵の漏洩耐性を有する鍵隔離暗号”, CSS 2021, pp. 997–1004.

[2] N. Chandran, B. Kanukurthi, S. L. B. Obbattu, and S. Sekar, “Adaptive Extractors and Their Application to Leakage Resilient Secret Sharing”. CRYPTO 2021, pp. 595–624.

* 電気通信大学, 182-8585 東京都調布市調布ケ丘 1-5-1, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan
† 産業技術総合研究所, 135-0064 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo, 135-0064, Japan