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

公開鍵暗号の平文空間の効率的な拡張方法について
On Expanding the Plaintext Space of Public Key Encryption

松田 隆宏 *
Takahiro Matsuda

キーワード 公開鍵暗号、平文空間、選択暗号文攻撃に対する安全性

あらまし

「平文空間が 1 ビットの選択暗号文攻撃 (CCA) に対して安全な公開鍵暗号 (PKE) から、任意の長さの平文を暗号化できる CCA 安全な PKE を構成できるか」という問題は、Myers と Shelat (FOCS'09) が、CCA 安全な 1 ビット PKE から CCA 安全な鍵カプセル化メカニズム (KEM) を構成できることを示したことによって肯定的に解決され、後にいくつかの論文において効率化が図られた。Matsuda と Hanaoka (ASIACRYPT'15) は、CCA 安全な 1 ビット PKE から CCA 安全な KEM を構成する際に KEM の暗号文サイズが $O(k)\cdot|c_1|$、暗号化のコストが $O(k)\cdot e_1$ とできる方法を示した。(ただし、k はセキュリティパラメータ、$|c_1|$ は構成要素の 1 ビット PKE の暗号文サイズ、e_1 は構成要素の 1 ビット PKE の暗号化 1 回にかかるコストを表す。) Matsuda-Hanaoka 方式では、構成された CCA 安全な KEM は構成要素の CCA 安全な 1 ビット PKE の鍵対を 2 つ用いる。一方、松田 (SCIS'17) は、構成要素の CCA 安全な 1 ビット PKE の鍵対を 1 つのみしか用いずに CCA 安全な KEM を構成する方法を示した。この KEM の暗号文サイズは $O(k)\cdot|c_1|$ であるものの、暗号化のコストは $\omega(k\log k)\cdot e_1$ である。本稿では後者の方法を改善し、構成要素の CCA 安全な 1 ビット PKE の鍵対は一つのみしか用いずに、暗号文サイズが $O(k)\cdot|c_1|$、暗号化のコストが $O(k)\cdot e_1$ であるような CCA 安全な KEM の構成方法を示す。

* 国立研究開発法人 産業技術総合研究所 サイバーフィジカルセキュリティ研究センター〒 135-0064 東京都江東区青海 2-3-26 臨海副都心センター Cyber Physical Security Research Center (CPSEC), National Institute of Advanced Industrial Science and Technology (AIST), AIST Tokyo Waterfront 2-3-26 Aomi, Koto-ku, Tokyo, 135-0064, JAPAN. Email: t-matsuda@aist.go.jp.