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

鍵付き準同型暗号における演算の拡張と安全性
How extension of evaluation algorithms affects security of keyed-homomorphic encryption

篠木 寛鵬 * 縫田 光司 †
Hirotomo Shinoki Koji Nuida

キーワード 準同型暗号，鍵付き準同型暗号

あらまし

準同型暗号は暗号文の状態のまま演算を行うことができる公開鍵暗号方式である．しかし，準同型暗号は公開鍵暗号において達成することが望ましいとされる IND-CCA2 安全性をみたすことができない．そこで，演算に必要な鍵を導入することで安全性を高めた鍵付き準同型暗号が Emura ら [1] によって提案された．鍵付き準同型暗号については，KH-CCA 安全性とよばれる安全性が定義されている．この安全性をみたせば，演算鍵をもたない攻撃者に対して IND-CCA2 安全性を，演算鍵をもつ攻撃者に対して IND-CCA1 安全性を達成できる．

鍵付き準同型暗号の演算アルゴリズムは 2 つの暗号文に対して実行するものとして定式化されている．しかし，演算アルゴリズムを複数回使用して 3 つ以上の暗号文に対する計算を行う際，より小さい計算量で同じ結果を得る方法が存在する場合がある．このような 3 つ以上の暗号文を入力とするアルゴリズムを追加し，同様に KH-CCA 安全性を定義することができる．ただし，KH-CCA 攻撃者は演算オラクルを使用できる設定であるため，元の鍵付き準同型暗号が KH-CCA 安全であっても追加後の方式が KH-CCA 安全かは明らかでない．

そこで本研究では，KH-CCA 安全性が引き継がれる条件について考察を行った．鍵付き準同型暗号 $\mathcal{E}$ について，演算アルゴリズムに演算の合成を計算する機能をすべて追加することを考え，その方式を $\mathrm{Comp}(\mathcal{E})$ とかく．このとき以下の 2 つの定理が成立することを示した．

定理 1. KH-CCA 安全な鍵付き準同型暗号および SUF-CMA 安全なメッセージ認証コードが存在すると仮定する．このとき，KH-CCA 安全な鍵付き準同型暗号 $\mathcal{E}$ であって $\mathrm{Comp}(\mathcal{E})$ が KH-CCA 安全でないものが存在する．

定理 2. 鍵付き準同型暗号 $\mathcal{E}$ が KH-CCA 安全かつ circuit private ならば，$\mathrm{Comp}(\mathcal{E})$ も KH-CCA 安全である．

また，本研究では線型演算が可能な鍵付き準同型暗号に対して 1 回の乗算を行うアルゴリズムを追加し，鍵付きレベル 2 準同型暗号に変換する方法を提案した．Catalano と Fiore [2] は線型準同型暗号に 1 回の乗算アルゴリズムを追加する方法を提案し，IND-CPA 安全性や circuit privacy が引き継がれることを示した．この Catalano-Fiore 変換を鍵付き準同型暗号へそのまま適用しても KH-CCA 安全性は引き継がれない．実際，レベル 2 暗号文はレベル 1 暗号文いくつかの組として表されているため，改ざんが可能である．そこで，レベル 2 暗号文を共通鍵暗号でさらに暗号化する処理を追加する．この処理を行うことにより，元方式が KH-CCA 安全かつ circuit private であるときにこれらの性質が変換後の方式に引き継がれることを示した．

参考文献

[1] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda, and S. Yamada, “Chosen ciphertext secure keyed-homomorphic public-key encryption,” PKC 2013, pp.32–50, 2013.

[2] D. Catalano and D. Fiore, “Using linearly-homomorphic encryption to evaluate degree-2 functions on encrypted data,” ACM CCS 2015, pp.1518-1529, 2015.

* 東京大学, 〒 113-8654 東京都文京区本郷 7-3-1, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8654 Japan.
† 九州大学, Kyushu University / 産業技術総合研究所, AIST