暗号アルゴリズム「EPOC」

詳細評価(攻撃評価)レポートサマリー

今日、公開鍵暗号を提案するにあたっては、今までの歴史的経緯もあって、妥当な仮定のもとでその安全性が証明されていることが標準的となっている。

EPOC 暗号は、この要件をみたす公開鍵暗号の 1 つである。

EPOC 暗号は EPOC-1, EPOC-2, EPOC-3 の 3 つのバージョンをもち、それぞれ、EPOC 暗号仕様書、及び EPOC 暗号自己評価書に記載されている通り、ある仮定のもとで、最強とされる安全性（適応的暗号文選択攻撃に対する安全性：semantically secure against adaptive chosen ciphertext attack）が証明された公開鍵暗号方式である。ただし、その安全性が証明されるために要求される仮定は、EPOC-1 に関しては p-部分群仮定と真のランダム関数の仮定、EPOC-2 に関しては $n=p^2q$ 型の素因数分解仮定と真のランダム関数の仮定、EPOC-3 に関しては $n=p^2q$ 型の Gap-素因数分解仮定と真のランダム関数の仮定である。

本評価書では、EPOC 暗号に対して、EPOC 暗号仕様書、及び EPOC 暗号自己評価書に記載されている内容を検証すると共に、特長・適応性、安全性、効率性の観点から詳細評価を行うことを目的とする。