暗号アルゴリズム

「ECMQVS (Elliptic Curve MQV Scheme) in SEC1」

詳細評価(攻撃評価)レポートサマリー

楕円曲線 MQV スキーム(ECMQVS)は、鍵共有(Key Agreement)の一方式である。そのプリミティブは、エンティティ *U* が所有する 2 組の鍵ペアとエンティティ *V* が所有する 2 つの公開鍵から、有限体の要素を 1 つ生成し、それを共有された鍵とする。

ECMQV プリミティブは、楕円離散対数問題または楕円 Diffie Hellman 問題が解かれれば破られるが、ECMQVS の安全性は、楕円 Diffie-Hellman 問題の安全性と等価である、と応募者は予測している。ただしその根拠は応募書類中では詳細に評価されておらず、Law、Menezez、Qu、Solinas、Vanstone の文献を参照しなければならない。楕円曲線離散対数問題と楕円曲線 Diffie-Hellman 問題に対する攻撃に対して安全な楕円曲線パラメータを用いれば、ECMQV プリミティブは安全であると思われる。

過去のいくつかの鍵共有法の提案は、安全性に欠陥が見つかっているが、その一因は、安全性と脅威に関する定義が、適切かつフォーマルになされていなかったことである。ECMQVS は、安全性と脅威に関して適切かつフォーマルに定義されている。その定義は、Law、Menezez、Qu、Solinas、Vanstone の文献に述べられている。この定義の上で、ECMQVS は安全であると思われる。

ECMQVS は、ANSI X9.42、ANSI X9.63 および IEEE P1363 において標準化されている。また、応募者自身が中心メンバーである SECG (Standards for Efficient Cryptography Group)でも採用されている。SECG においても外部評価者による安全性評価を実施しているが、欠陥は見つかっておらず、評価は高い。

応募書類は、数学的解説から実装に必要な様々な関数まで網羅し、自己完結したわかりやすい記述になっている。