暗号アルゴリズム
「ECDHS (Elliptic Curve Diffie-Hellman Scheme) in SEC 1」
詳細評価 (攻撃評価) レポートサマリー

本詳細評価書では、ECDHS の概要が述べられた後、ECDHS の安全性評価を以下の項目に対して行った。

- ECDLP に対する攻撃法
  - Generic 攻撃法
    - ・Pollard-ρ法, Pollard-λ法に対する安全性
    - ・Pohlig-Hellman 法に対する安全性
  - Non-generic 攻撃法
    - ・MOV 法, FR 法に対する安全性
    - ・SSSA 法に対する安全性
    - ・Weil descent（Gaudry-Hess-Smart attack）に対する安全性
- ECDLP 以外の ECDHS に対する攻撃法
  - ECDHP の安全性と ECDDH 仮定
  - 小部分群攻撃法に対する安全性
  - Man-in-the-middle 攻撃法に対する安全性
  - 鍵導出関数（key derivation function）への攻撃法に対する安全性

その結果、SEC 1（暗号技術仕様書, 自己評価書）の記述は、現時点で十分妥当なものであると判断した。また、記述自身も大変わかりやすく、実装するのに不足はない。あとは、Weil descent 攻撃法など ECDHS の安全性に影響する現在進行中の研究動向が、仕様記述に反映されるのを注意深く追うだけである。