ECDSA評価の現状報告
(詳細評価)

平成14年1月28日

公開鍵暗号評価小委員会
委員　新保　淳

ECDSA

- 応募暗号種別：署名
- 安全性の根拠：楕円曲線上の離散対数問題
- 証明可能安全性：確立された安全性証明は無い
  （Random oracle modelでの証明例は無い）
  Generic group modelを利用したBrownの結果あり
- 特長：（RSA署名に比べて）
  - 鍵長が短い
  - 署名文が小さい
  - 署名生成時間が短い
- SW実装情報(ECDSA in SEC1応募者）：
  鍵生成1.9ms, 署名生成3.7ms, 署名検証9.7ms
  (PentiumⅢ650MHz)

ECDSA規格

- CRYPTREC2001での評価対象は以下の2つ
  - ECDSA in SEC1：CRYPTREC2000から応募
  - ANSI X9.62：電子署名法に係る指針に記載された署名方式の1つ
- 署名スキームは同一
- 推奨する楕円曲線に差異あり
  - SEC1：ランダム曲線の他にKoblitz曲線を推奨
    ほとんどの曲線でパラメータaを固定
  - ANSI：サンプルとしてランダム曲線とWeil法によって生成された曲線を掲載
    曲線パラメータaもランダム

詳細評価

- 次の観点から4名の評価者に評価を依頼:
  - 暗号スキームに関して
    - Generic group modelにおける証明可能安全性の検証
  - 暗号プリミィティブに関して
    - Koblitz曲線の安全性の検証(ECDSA in SEC1)
  - その他、気が付いたこと
    - 自由な観点から安全性に関する評価

Brownの論文

- Generic DSAに対するgeneric group modelでの安全性証明

  [Generic DSA] ECDSAを任意の素数位数の(加法)群を利用した署名スキームに一般化

  [Generic group model] 群要素の表現がランダムに与えられると仮定した仮想的なモデル

  – 素数位数nの加法群Z_nからビット列集合Sへの全単射σをランダムに与える
  – σを定めるgeneric group oracleへの問い合わせを用いて群演算を行う
- [主定理]適応的選択文書攻撃により存在的偽造を行う偽造者が存在するならば、ハッシュ関数の衝突を求めるアルゴリズムを構成可能

評価コメント －証明可能安全性－

- Brownの定理は概ね正しい
  - アルゴリズムの成功確率や実行時間を修正のうえ、別証明を与えた評価者あり
  - Brownの証明は記述不足（不完全）との指摘あり
- Generic group modelでの証明の意味合い
  - Random oracle modelに比べてモデルの歴史が浅く、現実的意味合いは、より制限される
  - ある程度評価する意見から評価しない意見まで割れている
    - 現在のECDLP解法が群演算をブラックボックス化したgeneric model型のため、これら攻撃に対する安全性の一指標
    - ECDSAでは群要素の表現はgenericとは言えず、ECDSAに対する具体的な攻撃が説明できない

評価コメント －Koblitz曲線の安全性－

- ECDLPの解法であるrho法に対して、Koblitz曲線では若干の高速化手法あり

  [Wiener etc.][Gallant etc.]
  - F_{2^m}上の曲線で $\sqrt{2m}$ 倍高速に解ける

    （m=160で約16倍高速）
  - パラメータサイズを若干大きくすることで対応可能
- 専用の攻撃が発見される可能性を危惧する意見あり

評価コメント －擬似乱数生成器－

- ANSI X9.62に記載の擬似乱数生成器には注意が必要
  - DSA[FIPS 186]に対するBleichenbacherの攻撃:

    k=rand mod nが[1,n-1]で一様に分布しない
    - FIPS186-2 (+change notice 1)と類似の修正を推奨する意見あり
- 線形合同法による弱い乱数生成器を用いたDSA実装に対する攻撃例[Bellare etc.]

評価コメント
－楕円曲線パラメータの検証－

- 楕円曲線パラメータはトラップドアが無いことを検証可能にすべきという意見あり
  - “verifiable curve generation”を利用しても曲線やベース点Gは限定されない
  - （定義体q,seed,a,b,ベース点G,位数n,公開鍵Y ）の全体を公開鍵証明書に含めることを推奨
  - さらには、楕円曲線パラメータ検証を行う信頼できる第三者機関の設立を推奨