OK-ECDSA,OK-ECDH
評価の現状報告
(スクリーニング評価)

平成14年1月28日

公開鍵暗号評価小委員会
委員　新保　淳

OK-ECDSA
(応募者の主張)

- 応募暗号種別：署名
- 安全性の根拠：モンゴメリ型楕円曲線上の離散対数問題
- 証明可能安全性：スキームはECDSAそのもの
  確立した安全性証明は無い
  (Generic group modelを用いたBrownの結果を引用)
- 特長：
  - サイドチャネル攻撃に対して耐性が高い
  - ICカード実装に適し、実行時のメモリ使用量が小さい
- SW実装情報：署名生成11.0ms, 署名検証21.6msec
  (Pentium III 866MHz)

OK-ECDH
(応募者の主張)

- 応募暗号種別：鍵共有
- 安全性の根拠：モンゴメリ型楕円曲線上の離散対数問題
- 証明可能安全性：スキームはECDHそのもの
  安全性の証明例は無いが、受動的攻撃に対し
  経験的に安全であると信じられている
- 特長：
  - サイドチャネル攻撃に対して耐性が高い
  - ICカード実装に適し、実行時のメモリ使用量が小さい
- SW実装情報： 鍵共有11.0ms (Pentium III 866MHz)

OK-ECDSA,OK-ECDH の技術的特徴

- モンゴメリ型楕円曲線でのランダム化射影座標の利用
  - 秘密情報に関わらず計算手順が同一
  - 計算対象の値がランダム化される
- モンゴメリ型楕円曲線の加算（Y座標を用いない）においてY座標を復元する手法を導入
- スキームはECDSA,ECDHそのもの
  - プリミティブの実装レベルでの差異のみ
- モンゴメリ型楕円曲線は限定されたクラスの曲線だが、一般の楕円曲線の約40%が変換可能

スクリーニング評価

- OK-ECDSAとOK-ECDHは技術的特徴が共通なので同一の評価者(3名)に評価を依頼した
- 暗号技術仕様書に関して:
  - 不明点や疑問点はない
  - 楕円曲線パラメータの推奨値が(一部)欠けているとの意見あり
- 自己評価書に関して:
  - コメントはサイドチャネル攻撃耐性に集中

評価コメント

- サイドチャネル攻撃耐性の評価が十分とはいえない
  - 耐性が高いという主張は正当と考えられるが、実装による定量的評価に乏しい
  - 提案者の評価は理論的な考察のみであり、実装レベルでの留意点が記述されていないため、耐性の低い実装が行われる可能性がある
  - 他の手法との実装比較、プラットフォームの特徴や演算サイクルを考慮した評価が必要
  - 必要メモリ量に関しても同様
  - スマートカード上での実装評価結果がない
  - ハードウェア実装結果の根拠が示されていない