DSA署名評価の現状報告
(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　洲崎 誠一

DSA署名
（電子署名法に係る指針に記載された署名方式の1つ）

- 暗号種別：署名
- 安全性の根拠：有限体上の離散対数問題.
- 証明可能安全性：証明可能安全性は示されていない.
- 特長：元メッセージに対して署名が2倍の長さになるというElGamal署名の短所を，Schnorrの手法により改善.

詳細評価

- 次の観点から複数（４名）の評価者に評価を依頼:
  - 暗号プリミィティブに関して.
  - 暗号スキームに関して.
  - FIPS 186-2 Appendix 3で与えられている乱数生成法に関して.

評価コメント　－ パラメータの選択 －

- いくつかの特殊なパラメータにおける攻撃法が報告されており，適正なパラメータを選択することが必要.
- 同じ乱数kを複数のメッセージ（署名対象）に適用してはならない.
- パラメータのサイズを，より大きな値にすべきという指摘あり.

評価コメント　－ 証明可能安全性 －

- 現在までに，何らかの妥当なモデルや仮定のもとでの証明可能安全性は報告されていない（DSA署名に若干の変更を加えれば，離散対数問題の困難性と同等の証明可能安全性を示すことができる）．

評価コメント　－ 乱数生成 －

- Appendix 3の乱数生成法では，出力される乱数に偏りがでるので，Change Notice 1として付記された手順で乱数を生成することを推奨（詳細な攻撃法は明らかにされていない）.
- 乱数kのいくつかのビットがわかる場合には秘密鍵がわかってしまうという報告あり.
- 乱数生成方法として，SHA-1とDESを利用した方式が規定されているが，DESを利用した方式には特殊な性質があるのでSHA-1を利用したほうがよいという指摘あり.

評価コメント　－ その他 －

- SHA-1に関しては，有効な攻撃法は報告されておらず，現在までのところ安全な一方向性ハッシュ関数だと見なすことができる.
- 実装方法によっては，リプレイアタックをされるという指摘あり.