ESIGN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　酒井 康行

ESIGN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)

- **種別**:署名
- **安全性の根拠**:
  $n=p^2q$ 型素因数分解問題が難しい
  e乗根近似問題が難しい
- **証明可能安全性**:
  電子署名法に係る指針にある ESIGNは、e乗根近似問題が難しいという仮定の下で、ハッシュ関数をランダムオラクルとしても、適応的選択文書攻撃に対して存在的偽造不可であるという証明は現時点では無い。
- **実装性の特長**:
  RSA署名と比べて署名生成速度が高速
- **SW実装情報**:
  鍵生成 610ms、署名生成 1.04ms、署名検証 0.70ms
  (|n|=1152, e=1024, SHA-1使用, Celeron 800MHz, 自己評価書に記載)

ESIGN署名のバージョンについて

ESIGNは7つの応募または発表を行っている（以下は主なもの）

<table>
<tr><th></th><th>推奨パラメータ</th><th>エンコード</th><th>証明可能安全性</th></tr>
<tr><td>電子署名法に
係る指針</td><td>|n|≧1024, e≧8</td><td rowspan="2">EMSA</td><td rowspan="2">無 （効率的攻撃法が
あるかどうかは現在評価中）</td></tr>
<tr><td>CRYPTREC2001</td><td>|n|≧1152, e≧1024</td></tr>
<tr><td>CRYPTREC2000</td><td>|n|≧960,　e≧8</td><td colspan="2">規定無し(プリミティブのみの提案)</td></tr>
<tr><td>IEEE P1363a</td><td>規定無し(P1363の方針)</td><td rowspan="2">EMSA5</td><td rowspan="2">有 （$n=p^2q$型素因数分解
仮定, e乗根近似仮定,
ランダムオラクルモデル,
適応的選択文書攻撃に
対して存在的偽造不可）</td></tr>
<tr><td>NESSIE
(右記に変更予定)</td><td>|n|≧1152, e≧1024</td></tr>
</table>

詳細評価方針

- 次の観点から評価を実施中
  - プリミィティブ評価:
    e乗根近似問題の困難性
  - スキーム評価:
    電子署名法に係る指針における推奨パラメータ:
    $|n| \geqq 1024$, $e \geqq 8$ の安全性
    その他の標準化機関における推奨パラメータの安全性
  - その他

評価コメント：e乗根近似問題

- e=2の場合：
  Brickellらの方法[Crypto95]や、Valleeらの方法[Eurocrypt88](LLLアルゴリズムを用いて低い次数のmodular polynomialを解く)およびこれを改良したCoppersmithの方法[Eurocrypt96]により、e乗根近似問題は解ける。
- e=3の場合：
  上記の方法はe=3の場合にも拡張できる。
- e ≧4の場合：
  e乗根近似問題の効率的解法は知られていないという主張は妥当である。

評価コメント：エンコーディング(1/2)

EMSAエンコーディングを用いたESIGN（証明可能安全性無し）
（このESIGNは電子署名法に係る指針にある）

- 新しい攻撃方法(署名偽造)を発見したと主張する外部評価者がいる（正当性未検証）。評価者の主張が正しいならば、その攻撃を用いると、ハッシュ関数の出力が160ビット(SHA-1)の時、次のような場合に署名の偽造が無視できない確率で成功する。
  （１）|n|=1024かつe=4
  （２）|n|=2048かつe=7
  （３）|n|=2048かつe=8
- 上記評価者による新攻撃は、e=1024の場合の安全性は脅かさない（と評価者は述べている）。

評価コメント：エンコーディング(2/2)

EMSA5エンコーディングを用いたESIGN（証明可能安全性有り)
（IEEE P1363a, NESSIE)

e乗根近似問題が難しいという仮定の下で、
ハッシュ関数をランダムオラクルとした場合、
適応的選択文書攻撃に対して存在的偽造不可
（署名における最強の意味での安全性）である
という証明は妥当である。