暗号アルゴリズム評価報告書
RSA-PSS

２００１年度

日本電信電話株式会社

藤岡 淳

暗号アルゴリズム評価報告書 RSA-PSS

1　はじめに

本報告書で評価の対象となる RSA 署名は RSA 関数と PSS エンコード法とからなり，本報告では，以下の観点からその詳細評価を行なう．

- RSA-PSS の安全性の証明を検証する
- RSA 署名でのパラメータ選択が適切かどうかを検証する

2　安全性の証明

2.1　RSA 署名とその安全性

安全性の観点から，ディジタル署名方式は選択的メッセージ攻撃に対して存在的偽造不可となることが求められる．しかしながら，これを前提なしに保証することは困難であり，多くの場合，ある数学的な問題を仮定し，その署名法に対する偽造法が存在した場合に，その数学的な問題が解けることを示すことでその安全性を保証している．

一般に RSA 署名は， RSA 関数とメッセージのエンコード法を組み合わせて用いられるが，そのエンコード法によっていくつかの方式が存在する． RSA 社から発行されている標準文書 PKCS#1 [PKC98] では，メッセージの単純なハッシュ値を RSA 署名プリミティブで変換する手法が記述されているが，この手法では，上記の意味での署名スキームに対する安全性が保証されていない．

数多くの研究により通常のモデルで RSA 署名の安全性を RSA 関数の逆問題で保証する試みがなされているが，その多くは失敗しているか効率面で問題がある．そこで，エンコード法を工夫し，そのエンコードに用いられるハッシュ関数をランダムなものと仮定 (ランダムオラクルモデルという) することで署名の安全性を証明しようとする技法が考案されている．

RSA 署名においても， PSS というエンコード法 [BR96] を用いると，ランダムオラクルモデルにおいて RSA-PSS (以下， RSA-PSS96 と呼ぶ) の安全性は RSA 関数の逆問題に帰着されることが証明されている．

しかし，この RSA-PSS96 を IEEE P1363a で採用する際に，他の手法との互換性などの点からいくつかの変更が行なわれ，この変更された手法 (以下， RSA-PSS00 と呼ぶ) は，文献 [PKC01] で公開されている．主な変更は

- メッセージのハッシュ値と salt (乱数の種) のハッシュ値を RSA 関数に入力する．
- ハッシュ ID の有無に関するパラメータの導入．

この変更が行なわれたスキームが今回詳細評価の対象方式である (ちなみに，NESSIE プロジェクトにも同じスキームが提案されている).

2.2 詳細評価対象方式の安全性

RSA-PSS96 の安全性は文献 [BR96] で証明されているが，同様に，変更された RSA-PSS00 の安全性は文献 [Jo01] で証明されている.

以下のこの文献に示されている証明の概略について述べる.

RSA-PSS00 を含むより広い方式 RSA-GenPSS を定義し，RSA-GenPSS の入力をハッシュ値に限定した RSA-GenPSS-Reduced を定義する．その後，RSA-GenPSS-Reduced が安全ならば RSA-GenPSS が安全であることを証明 (文献 [Jo01] の **Lemma 7.1**) し，最終的に RSA 関数が安全ならば RSA-GenPSS-Reduced が安全である (すなわち，RSA-GenPSS が安全) であることを証明 (文献 [Jo01] の **Theorem 9.1**) している.

ここで，RSA-PSS00 ではなく RSA-GenPSS を証明の対象としているのは，RSA-PSS00 で導入されたパラメータを悪用する攻撃者を想定しているためであり，RSA-GenPSS が安全であるならば，(そのような偽造者を含む場合でも) RSA-PSS00 が安全であることになる.

ただし，以上の証明において，RSA-PSS00 で導入されたハッシュ ID に関するパラメータを用いない場合には，ハッシュ関数をすりかえる攻撃に対しては，なんら安全性を保証していない点を認識すべきである.

また，このパラメータの導入により安全性の帰着に関して，やや効率が落ちている (2^8 ないし 2^{16} 程度) 点にも注意が必要である.

2.3 その他の安全性

自己評価書において，評価すべき攻撃法は，暗号学的なものから非暗号学的なものまで十分に網羅されており，その選択の理由について問題は見い出せない.

自己評価書では，以下の安全性について検討されている.

- n の因数が不明なとき，c モジュロ n の e 乗根を得る.

  数学的に未解決問題であるが，困難であると予想されている.

- n の因数を計算し，その後 c モジュロ n の e 乗根を得る.

  当然可能であるが，素因数分解の可能性については，パラメータの妥当性に関する章を参照のこと.

- 二人のユーザによるモジュロ値の共有.

  危険であることが指摘されている.

- 小さな秘密指数 d の値.

  攻撃の可能性が記述されている.

- 公開指数 e の低い値.

  $e = 3$ の場合でも，特に問題は発見されていないが，それ以外の推奨パラメータを用いることに問題はないと思われる.

- RSASP/RSAVP の乗法性.

  PSS エンコード法の採用により防止できると思われる.

  注) RSASP は RSA 署名生成プリミティブ，RSAVP は RSA 署名検証プリミティブのこと.

- 秘密指数に関する部分情報の漏洩.

  秘密指数 d を正しく保護すべきことが指摘されている.

- 因数 p, q に関する部分情報の漏洩.

  秘密因数 p, q を正しく保護すべきことが指摘されている.

RSA 関数の逆問題は素因数分解問題よりもやや強い仮定ではあるものの，一般にはほぼ等価に近い問題と認識されている.

また，実装攻撃に関しても，故障依存攻撃，電力解析攻撃，タイミング解析攻撃が適用不可能なように実装すべきであることを指摘している.

3 パラメータ選択

RSA 署名のパラメータ選択については自己評価書に記述されている.

因数 n に関しては，RSA-512 を基準値として，1024 bit のモジュロ値では RSA-512 の 7×10^6 倍，2048 bit のモジュロ値では 9×10^{15} 倍の計算量が必要とされるとあるが，これは，現在の予想と反していない.

また，e や d の選択については，先の章を参照されたい.

4 まとめ

RSA 関数の逆問題が困難であると仮定した場合に，RSA 署名 (RSA-PSS00) の安全性をランダムオラクルモデルにおいて保証する証明に問題はないと思われる.

以上のことから，対象スキームの安全性の証明は十分に信頼に足るものであると結論付けることができる.

また，パラメータの選択にも，特段大きな問題はないものと考える.

参考文献

[BR96] Bellare, M. and Rogaway, P.: "The Exact Security of Digital Signatures - How to Sign with RSA and Rabin", Proc. of EUROCYRPT '96. Springer–Verlag, 1996.

[Jo01] Jonsson, J.: "Security Proofs for the RSA-PSS Signature Scheme and Its Variants", http://eprint.iacr.org/2001/053/

[PKC98] PKCS#1 vol.2.0: RSA Cryptography Standard, October 1, 1998, http://www.rsasecurity.com/rsalabs/pkcs/

[PKC01] PKCS#1 vol.2.1 draft 2: RSA Cryptography Standard, January 5, 2001, http://www.rsasecurity.com/rsalabs/pkcs/