暗号アルゴリズム評価報告書
RSA-OAEP

２００１年度

日本電信電話株式会社

藤崎 英一郎

暗号アルゴリズム評価報告書 RSA-OAEP

1 はじめに

本報告書で評価の対象となる RSA-OAEP（暗号）は「CRYPTOREC の暗号アルゴリズムの評価（継続評価）」に 2001 年度提出された暗号技術仕様書に記載のものである。

RSA-OAEP は，Ronald Rivest，Adi Shamir，Leonard Adleman による RSA（落とし戸付き）関数 [9] に Mihir Bellare と Phillip Rogaway によって発明された OAEP エンコード法 [3] を適用したものであるが，より細部の実装上の改良が対象の RSA-OAEP にはなされている（これは，RSA 社から発行されている標準文書 PKCS #1 v2.1 [2] とも一箇所異なっている）。

上記暗号技術仕様書の RSA-OAEP は，RSA 暗号基本演算 RSAEP，RSA 復号基本演算 RSADP，EME-OAEP エンコードアルゴリズム，EME-OAEP デコードアルゴリズムから構成される。さらに上記各演算アルゴリズムは，ハッシュ関数 $Hash$，MGF と擬似乱数 $seed$ を呼び出すが，これらの補助アルゴリズムは本報告書の評価の対象にならない。

本報告では，以下の観点からその詳細評価を行なう。

- RSA-OAEP の安全性（の証明）を検証する。
- RSA-OAEP のパラメータ選択が適切かどうかを検証する。
- 仕様書で採用されている実装法の妥当性を検証する。

1.1 PKCS #1 v2.1 からの変更点

対象となる暗号技術仕様書記載 RSA-OAEP では，EME-OAEP の出力であるオクテット列の先頭に 1 オクテットキャラクタ 00 を常に加えることとする。これによりモジュロ n のオクテット列表現と EME-OAEP の出力オクテット列が常に同じ長さになり，実装上の曖昧さを排除する。

2 安全性について

公開鍵暗号に求められる安全性とは，選択暗号文攻撃 (chosen ciphertext attack) に対して強秘匿 (semantically secure or indistinguishable) であると考えるのが自然である。

RSA-OAEP が**選択暗号文攻撃に対して強秘匿** [8] であるかを次の 4 つの観点から考察する（以下，公開鍵暗号が選択暗号文攻撃に対して強秘匿であることを単に，公開鍵暗号が安全であると呼ぶ)。

1. 理想の環境（ランダムオラクルモデル）下での安全性。

   上記ハッシュ関数 $Hash$，MGF が理想的なものであると仮定する時，**RSA-OAEP の安全性と RSA 関数の（部分）一方向性の等価性**を示す文献 [5] が存在する（参考文献：[3, 10])。故に理想の環境下では，RSA 関数が**（部分）一方向性関数**であるか（**RSA 問題の解読困難性**）に考察を絞ることが出来る。文献 [5] については 2.1 章で解説する。

   実際には，理想の環境下での安全性の結果を現実世界で保持するには，耐タンパデバイス（もしくは信頼できるオンラインで利用できるセンタ）と擬似ランダム関数が必要となる。よって現仕様書の枠組みでは，理想環境は実現不可能であり，上記の結果は保存されない。しかし，過去の経験則から理想環境下ですら安全でないならば現実世界での安全性も疑わしいと考えて良いだろう [1, 4]。

2. RSA 問題の解読困難性。

   現在，理想環境下以外では RSA-OAEP の安全性を RSA 関数の一方向性で保証するような結果は知られていないが，現実の問題として RSA-OAEP の安全性を RSA 関数の一方向性（**RSA 問題の解読困難性**）と**ほぼ**等価と考えて良いと思われる。

   RSA 問題に対する既知の攻撃法について，2.2 章で暗号自己評価書をもとに考察する。

3. 実装上の潜在的な弱点について。

   仕様に曖昧さがある場合，実装された RSA-OAEP に**弱点が混入する可能性**がある。2.3 章で，Manger の攻撃法 [7] をもとに RSA-OAEP の潜在的な弱点について考察する。

4. 非暗号学的な攻撃法に対する安全性。

   異常処理解析攻撃，電力解析攻撃，タイミング攻撃など。

2.1 理想環境（ランダムオラクルモデル）下での RSA-OAEP の安全性

理想環境下での RSA-OAEP の安全性の結果は，文献 [10, 5] を参考にすると以下のようにまとめられる。

RSA 関数を一般の（落とし戸付き）一方向性置換関数 f に置き換えたとき，f-OAEP の安全性は f の一方向性に等価なのではなく [10]，代わりに f の（部分）一方向性（一方向性より強い性質）に等価である [5]（再記載版 [6]）。

ただし，RSA 関数の場合，上記（部分）一方向性は，一方向性と等価であることも同時に [5] に示されたので，結局，理想環境下での RSA-OAEP の安全性は RSA 関数の一方向性によって保証されることになる。

上記 [10, 5] は互いに矛盾しておらず証明にも特に問題は見いだせない。

2.2 RSA 問題の解読困難性についての考察

自己評価書には，評価すべき攻撃法が十分に網羅されており，その解説にも特に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 の素因数が不明なとき，c モジュロ n の e 乗根を得る（RSA 問題の解読困難性）。

  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 の素因数を計算し，その後 c モジュロ n の e 乗根を得る（素因数分解の解読困難性）。

  n の素因数分解が出来れば，RSA 問題の解読は当然可能である。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。

RSA 問題の解読困難性は素因数分解問題の解読困難性よりも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．以下は RSA 問題が何らかの制限を受けてしまった時の解読困難性についての検討である。

- 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。

  $d < n^{0.5}$ のとき攻撃の可能性が示唆されている。

- 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。

以下は，パディング処理無しの生の RSA 関数を暗号として使った場合，危険性が指摘されている。ただしこれは RSA 問題を解読するより易しい問題なので，RSA-OAEP とした時は特に問題は知られていない。

- 小さい公開指数 e の値。
- 複数ユーザに対する同一暗号文。
- 同一ユーザに対する関連のある複数暗号文。

2.3 実装上の注意点

仕様に曖昧さがある場合，又は誤って実装された場合 RSA-OAEP に弱点が混入する可能性がある。Manger の攻撃法 [7] はその興味深い 1 例である。

Manger によれば，選択暗号文攻撃で，ある誤った暗号文を RSA-OAEP の復号アルゴリズムに復号させて，復号アルゴリズムが**ある 2 箇所のチェックポイントのどちらでエラーに気づいたか攻撃者が区別**できるのであれば，攻撃者は RSA-OAEP を破る（選択暗号文攻撃で強秘匿性を破る）ことが出来る。

一見このような状況は，あり得ないようだが実際には容易に起こりうると想像される。何故ならば，復号アルゴリズムが暗号文の送信者に暗号文が**正しく復号できなかったと伝えるのはごく自然であるし**，プログラミングの立場から言えば，**プログラムのどこで問題が発生したか外部に伝えるのはよくあること**だからである。さらに言えば，プログラマーによる**エラーメッセージ文のスペルミス**なども十分このアタックに引っかかる可能性がある。

理想環境（ランダムオラクルモデル）下の証明でも，復号アルゴリズムのエラー出力の表現は唯一である。そこで Manger の攻撃法の対策として，**EME-OAEP デコードアルゴリズムのエラーメッセージが唯一**となることを徹底する必要がある。このことは特に暗号技術仕様書に強調されている。

これ以外にも，一般論として仕様の曖昧さが選択暗号文攻撃を可能にすることがたびたびある。暗号技術仕様書では，EME-OAEP の出力であるオクテット列の先頭に 1 オクテットキャラクタ 00 を常に加えるよう，PKCS #1 v2.1 から一箇所変更がなされている。これによりモジュロ n のオクテット列表現と EME-OAEP の出力オクテット列が常に同じ長さに

なり，実装上の曖昧さをより排除している。評価者が検討したところ，これ以外に仕様が曖昧である箇所は特に見つけられない。

2.4 非暗号学的攻撃に対する安全性

自己評価書では，異常処理解析攻撃，電力解析攻撃，タイミング攻撃などの非暗号学的攻撃に対して抵抗力をつけるための対策が指摘されている。これらの記述について特に問題は見つけられない。

3 パラメータ選択

RSA-OAEP 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

理想環境下（ランダムオラクルモデル）において，RSA-OAEP の安全性を RSA 問題の解読困難性で保証する証明 [5, 6] に問題はないと思われる。英語から日本語への翻訳に多少難があるが，暗号技術仕様書のスキームの記載，実装上の注意，暗号自己評価書の RSA 問題の解読困難性に関する現状の分析，非暗号学的な攻撃法に対する一応の対策ともに特に問題は見つけられない。

参考文献

[1] PKCS #1 v1.5: RSA Cryptography Standard, November 1993. available via: `http://www.rsasecurity.com/rsalabs/pkcs/`.

[2] PKCS #1 v2.1 draft 2: RSA Cryptography Standard, January 2001. available via: `http://www.rsasecurity.com/rsalabs/pkcs/`.

[3] M. Bellare and P. Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer-Verlag, 1995.

[4] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the rsa encryption standard pkcs#1. In H. Krawczyk, editor, *Advances in Cryptology — CRYPTO'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 1998.

[5] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. In J. Kilian, editor, *Advances in Cryptology — CRYPTO2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 260–274. Springer-Verlag, 2001.

[6] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption (revised version), December 2001. available via: `http://cgi.di.ens.fr/cgi-bin/pointche /papers.html`.

[7] J. Manger. A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0. In J. Kilian, editor, *Advances in Cryptology — CRYPTO2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 230–238. Springer-Verlag, 2001.

[8] C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In J. Feigenbaum, editor, *Advances in Cryptology — CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. Springer-Verlag, 1992.

[9] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[10] V. Shoup. OAEP Reconsidered. In J. Kilian, editor, *Advances in Cryptology — CRYPTO2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 239–259. Springer-Verlag, 2001.