安全性詳細評価報告書 (HIME-1)

概 要

本稿では応募暗号 HIME-1 に対する詳細評価としてその安全性を提出された暗号技術仕様書 (以下, 技術仕様書) および自己評価書の記述に基づいて議論する．本稿の構成は以下の通りである．

まず第 1 節では, HIME-1 の技術仕様書の記述には暗号アルゴリズムが一意的に特定できない問題点があることを指摘する．

第 2 節では HIME-1 の暗号スキームと暗号プリミティブの両面から安全性評価を行う．暗号スキームに関しては「HIME-1 は IND-CCA2 を達成している」と評価書で主張されているが, 2 つの理由により, その安全性は証明されていないものと考えられる．また暗号プリミティブでは, 現在での安全性には問題ないものの, 将来的な安全性や他の暗号との比較の上での弱点を指摘し，近い将来には解読可能になり得ることを示す．さらに補助的に使用される関数の安全性も高くはないことを指摘する．

1 アルゴリズム仕様詳細の曖昧性

詳細評価にあたり留意すべき点から述べたい．『HIME-1 暗号は鍵共有用として提案しているが, 鍵共有の運用法などが一切記述されていない』点である．これでは, 単なる秘匿のアルゴリズムを提示しているだけであり, 今回の詳細評価も「秘匿」アルゴリズムとしての評価にならざるを得ない点を断っておく．

以下では, HIME-1 の「秘匿」としての安全性を評価するが, まず考えなければならない問題は,『暗号技術仕様書の記載のみでは, 暗号アルゴリズムが一意的に特定できない』ことである．なぜならば定数などの仕様詳細が記述されていないからである．更には，記述されたアルゴリズム等に (数学的に) 誤った記述があることも問題であると考える．

HIME-1 暗号のアルゴリズム記述はパラメータに一般性を持たせた形で書かれているが，各パラメータの条件や推奨値を明確にしていない．**結果的として，安全性が評価できるものは，技術仕様書 3 節の実装 (具体例) におけるパラメータ $|n| = 1024, k = 512, d = 3, k_0 = 128, k_1 = 128$ のものしかない．**具体的に言えば，

- 公開鍵 パラメータ $(n, k, d, k_0, k_1, G, H)$ について
  k_0, k_1 の値に関する条件も推奨値がまったくない．(明らかな条件 $k > k_0, k_1$ は除く) $|n| = (d+1) \times \frac{k}{2}$ ではあるが、実際高いビットでどのような値が良いかの規準も与えていない．

- 『ハッシュ関数』について
  技術仕様書に書かれている (ハッシュ関数と提案者は呼ぶ) 2 つの関数 G, H について， 3.2.6 節に記述があるが，定数 C, C_1, C_2, C_3 に具体的数値がはいっていない．推奨値すら存在していないことになる．(例えば, $C = C_1 = C_2 = C_3 = 0$ にした場合などにハッシュ関数に対する攻撃がより効率的になる可能性もある．) また, 3.2.5 節での H_1 の定義で $x = x_1||x_2||x_3$ としているが，説明がない．(明らかに $|x_1| = |x_2| = 128, |x_3| = 126$ を仮定していると読めるが，不適切な表現と言わざるを得ない．)

  更に，以下の記述の誤りがある．

  * hash 関数の定義域 $\{0,1\}^\infty$ は誤りで $\{0,1\}^*$ にすべきである．

  * 3.2.6 節の H_1 の定義域が $\{0,1\}^{896}$ としているが $\{0,1\}^{382}$ の誤りであろう．

- 鍵生成 (3.2.1 節) および素数生成 (3.3.3 節) の不備
  仕様書 3.2.1 節の鍵生成アルゴリズム詳細で n の鍵長を入力値としてあるがアルゴリズム内で入力値は使用されずに, $|p| = 256$ としている点は不適切である．また，3.3.3 節の素数生成は正確には素数判定を記述しているにすぎず，出力値はあくまで，擬素数かどうかの判定でしかない．これを利用したのであれば，これを用いた生成アルゴリズムを正確に記述すべきであろう．しかし，これはあくまで，確定的素数生成ではない．現代暗号には，確定的素数生成法がいくつか提案されており，この検討がアルゴリズムの正当性には必要である．

- Jacobi 記号計算の誤り
  仕様書 3.3.5 節における Jacobi 記号の計算アルゴリズムの記述に誤りが見受けられる．Step 3 で a が偶数の場合に j に代入する値は, $\mathrm{JACOBI}(a/2, n) \cdot (-1)^{n^2-1/8}$ ではなく, $\mathrm{JACOBI}(a/2, n) \cdot (-1)^{(n^2-1)/8}$ である．

- 誤植等
  spell の誤り (significat など)，関数の宣言の内容ととの不整合 (BINARY-EUCLID) を指摘しておく．

2 攻撃評価

本節では, 暗号スキームと暗号プリミティブの両面から安全性評価を行い，結論として，以下を指摘する．

- 暗号スキームにおける証明可能安全性に関しては自己評価書の主張「HIME-1 は IND-CCA2 を達成している」の証明に不備があるため，この主張は証明されていないと考える．

- 暗号プリミティブ，すなわち HIME-1 基本方式 (技術仕様書付録 A) の安全性では，現時点では安全性には問題がないと考えられるが, 検討の対象とした具体例においては鍵長などに可変性がないため, そのままでは近い将来に解読可能になり得ると考える．

- 補助関数 H_1 は通常のハッシュ関数よりもビット長が短いため, コリジョンを見つけやすくなっている．

以下，2.1 節では暗号スキームに対する安全性, すなわち『証明可能安全性』について論じ，2.2 節では暗号プリミティブの安全性, すなわち『素因数分解アルゴリズムへの耐性など』について検証する．さらに，2.3 節では補助関数 H_1 の安全性について議論する．

2.1 暗号スキームに対する安全性評価

HIME-1 は技術仕様書付録 A に記載されている HIME-1 基本方式に OAEP の手法を適用することで，IND-CCA2 を達成するように設計しているが，それを検証するには以下の二つの点を見なくてはならない．

1. HIME-1 基本方式に OAEP が正しく適用されているか．
2. OAEP 手法の不備を回避しているか．すなわち，元とした OAEP 手法 [BR] では IND-CCA2 を必ずしも証明できないことが指摘されている [Shoup] ため，改良型手法を用いるか，この技法のままであれば，あらたな条件 [FOPS] を満たしているか検証する必要がある．

まず，第 1 点から検討を行う．OAEP の安全性に関しては以下の定理の条件を検証する必要がある．

定理 (Bellare-Rogaway[BR]) ランダムオラクルモデルの下で一方向性置換 f が OW-CPA であるとき, OAEP は IND-CCA である．

以下，HIME-1 基本関数を f_{HIME} と書くことにする．

2.1.1 一方向性と置換性

f_{HIME} が一方向性であるにはその逆計算，すなわち $m^{2n} \bmod n$ から $m \bmod pq$ の計算が困難性であることを証明する必要がある．この点に関しては, 自己評価書において逆計算が n の素因数分解と同等の困難さであることを示し、結果として素因数分解の一方向性に帰着したことで OW-CPA を主張している。しかし、一般の素因数分解とは異なり、n の形が特殊である点でより深い議論・論証が求められると考えるが、技術仕様書 2.2.4 節の備考にしか考察がない。現時点で、この型のものの安全性に問題があるとは言えないが、d が大きい場合には、効率的な方法が見付かっている分 [BDH]、慎重な議論が求められる。したがって、自己評価書の記述だけでは不十分であると考える。

一方，置換性については，自己評価書では f_{HIME} が置換であるとしているが，f_{HIME} は置換でない. なぜならば関数 f_{HIME} は与えられた値の $2n$ 乗を計算する関数であり，その値域は $\mathbf{Z}_n^*$ の平方剰余元全体に含まれているからである.

結果として，HIME-1 の基本関数 f_{HIME} は OAEP の仮定を満たしていないため, 自己評価書定理 1.2 の主張はそのままでは誤りである．よって HIME-1 は提出された文書だけからでは『証明可能安全性を有する』ことが証明されていないものと結論する．

2.1.2 OAEP による証明可能安全性

次に第 2 点について検証を行う.

証明可能安全性に関しては, Bellare-Rogaway の定理では IND-CCA2 が必ずしも成り立つわけではない点が最近になって指摘された ([Shoup]). したがって，IND-CCA2 を主張するには，自己評価書における [BR] だけの引用では不十分であり, なんらかの付加証明が必要となる．(例えば Fujisaki ら [FOPS] による修正を使うならば基本関数 f_{HIME} が Partial OW であることを示す必要がある.) しかし自己評価書では一切，これらの考察および証明が欠けているので,「HIME-1 が IND-CCA2 である」ことは証明できていないものと考える．

以上まとめると, HIME-1 は基本暗号化関数が置換性を有していないため, 証明可能安全性の仮定を満たしておらず, その結果として証明可能安全性を有していない. さらに, 置換性を有するように修正できたとしても, その関数が Partial OW を持つなどの付加情報が示されない限り, HIME-1 は IND-CCA2 を達成しえないことが結論づけられる.

2.2 暗号プリミティブに対する安全性評価

本節では, HIME-1 の暗号プリミティブ (暗号基本方式) の安全性評価として, 対象となる素因数分解問題の困難性に関する評価を行う. すなわち，ここでは具体例である 1024bit のもののみを考えることとする.

結論として, HIME-1 の鍵長は現時点では安全と思われるが，将来的には同 bit の RSA 暗号より早くに解読可能になり得ることを指摘する.

2.2.1 素因数分解アルゴリズムに対する耐性

256 bit の素数の積である 1024 bit の合成数の素因数分解は (現在の) 素因数分解アルゴリズムに対して十分な耐性を持つと考えられている．したがって，実際面での安全性には現在において問題はないものと結論づけられる.

一方，自己評価書に記載してあるように，素因数分解の準指数時間算法として，計算時間が n のサイズに応じるものでは数体ふるい法があり，計算時間が n の素因子のサイズに応じるものでは楕円曲線法がある．今回の具体例のように，n を 1024 bit とし，各素因子のビット数が全体のビット数の 1/4 となる 256 bit の場合には，数

体ふるい法よりも楕円曲線法の方が予想計算時間がより少なくなることが計算により確認される．これは，言い替えれば，RSA 暗号ベースで同じ bit 長をもつ公開鍵暗号では，まだ数体ふるい法の方が計算時間が少ないので，それらよりも 安全性が落ちている と言うことも言える．

この事実は，符号化・復号化のために d を奇数としなくてはならないために，最小のものが $d = 3$ となることに由来するものであり，本暗号の本質的な問題のひとつと考えられる．($d = 1$ では本暗号の特徴である復号の高速化がでないので，この場合を除外している．)

2.2.2 実計算における耐性

次に HIME-1 のパラメータの将来的な安全性について考える．本節では計算機能力の進歩だけを仮定した場合に, 素因数分解アルゴリズムの分解能力がどの程度進展するかにより HIME-1 基本方式の安全性を計る．

最も計算量が少ないアルゴリズムである数体ふるい法は前節で述べたように n のサイズに計算時間が依存する．2000 年 12 月時点での世界記録は 512-bit であり ([RSA-155], 1024-bit の素因数分解に必要な計算量は 512-bit の場合の約 7500000 倍となることから，[RSA-155] と同じ計算機資源を用いた場合, 分解に必要な時間は約 4400000 年となり, 事実上分解不可能である．

一方，計算能力を考慮に入れた試算として, 数体ふるい法による記録 (桁数 D 桁) と達成年 (西暦 Y) の間の近似式

$$Y = 13.24D^{1/3} + 1928.6$$

[RSA-155] がある．これは 1024-bit (309 桁) の素因数分解は 2018 年に可能を意味する．近似式は経験的な結果であり, 信憑性には議論の余地があるが, 近い将来，1024bit では危ういということは確かであろう．

前節で指摘したように HIME-1 では楕円曲線法に対する耐性，すなわち素因数の大きさについての試算も重要である．残念ながら定量的な見積もり報告はなされていないが, 楕円曲線法による記録 (桁数 D 桁) と達成年 (西暦 Y) の間の近似式

$$Y = 9.3\sqrt{D} + 1932.3$$

がある ([Bre]). この近似式から見れば 256-bit(76.8 桁) の素因数分解は 2013 年に可能という結果を得られる．

以上により HIME-1 の素因数分解アルゴリズムに対する耐性は, 現時点では問題がないものの 2015〜2020 年頃には分解可能という試算もあり長期的な安全性は保証できないと考えられる．

2.3 補助関数 H_1 の安全性

HIME-1 では補助関数として『ハッシュ関数』と呼ぶ関数 H_1 を使用しているが, H_1 のハッシュ性に関する議論は何もなされていない点は非常に問題であると考える．

さらに，H_1 が正当な「ハッシュ性」を持ったとしても, 以下のような安全性の問題点が指摘できる．

仕様によると H_1 の入力長は 382(技術仕様書では 896), 出力長は 128-bit となっている．したがって H_1 のコリジョンは 2^{64} 程度の計算量で求めることが可能となり，HIME-1 では関数 H_1 のコリジョンを計算可能であると結論づけられる．

3 まとめ

本稿では, 評価するアルゴリズムとしては，一般的記述ではパラメータ等が不明瞭なため，唯一の具体例である 1024 bit のものを取り上げ，これに対する安全性評価を行った．

暗号スキームレベルでは, 自己評価書には HIME-1 は証明可能安全性を持つとの主張があるものの, 2 つの理由により, その主張の正当性は低いと考える. また暗号プリミティブのレベルでは, 現在での安全性には問題ないものの, 鍵長などに可変性がないため, 近い将来には解読可能になり得ることを指摘した.

本稿の参考文献は以下の通りである.

参考文献

[BR] M. Bellare and P. Rogaway, *Optimal asymmetric encryption - How to encrypt with RSA*, proceedings of EURAOCRYPT1994, LNCS 950, 1994.

[BDH] D. Boneh, G.Durfee and N.Howgrave-Graham, *Factoring $N = p^r q$ for large r*, proceedings of CRYPTO1999, LNCS 1666, 1999.

[Bre] R. P. Brent, *Recent progress and prospects for integer factorisation algorithms*, To be appear in proceedings of COCOON 2000 (Sydney, July, 2000). Available from Brent's website `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub196.html`.

[FOPS] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern, *RSA-OAEP is Still Alive!*, preprint. Available from `http://eprint.iacr.org/2000/061.pdf`

[RSA-155] S. Cavallar et al., *Factorization of a 512-Bit RSA Modulus*, proceedings of EUROCRYPT2000 (Bruges, May, 2000), LNCS 1807, 2000.

[Shoup] V. Shoup, *OAEP Reconsidered*, preprint. Available from `http://eprint.iacr.org/2000/060.pdf`