暗号アルゴリズム評価報告書
EPOC-2 および EPOC-2 の改訂版

2001 年 12 月 14 日

産業技術総合研究所

渡辺 創

暗号アルゴリズム評価報告書
EPOC-2 および EPOC-2 の改訂版 (EPOC-2' と以下略記)

2001 年 12 月 14 日

1 まえがき

本報告書は, CRYPTREC2000 応募暗号である EPOC-2 と, その改訂版として CRYPTREC2001 に応募された暗号である EPOC-2' について, その安全性評価を行なったものである. 以下 2 章では, まず CRYPTREC2000 において EPOC-2 を評価した報告書 (CRYPTREC2000 詳細評価報告書#2[3], 以下 #2) で問題があると指摘されていた点を示す. 次に指摘された点それぞれについて, その主張の有効性について論じる. 3 章では, CRYPTREC2001 に応募された暗号である EPOC-2' の仕様と自己評価について, 2 章で指摘された問題点のうち, 有効であると判断されたものが改訂の後でも有効であるかどうかを論じる. 最後に 4 章で本評価の結論を述べる.

2 EPOC-2 CRYPTREC2000 詳細評価報告書 #2

2.1 指摘された問題点

まず EPOC-2 に関して, #2[3] で指摘されていた点を以下に挙げる.

2.1.1 EPOC-2 で用いられているプリミティブに関する指摘

1. 仕様が曖昧であり, 最低限の相互接続性が保証される程度のものである. 鍵生成法の記述は, 実装するには不完全なものである, と指摘されている. 例として次の 2 つが挙げられている.
   - EPOC-2 で使用する素数 p について, $p-1$ なる値への条件は挙げられていない (実際は, これが小さな素数の積でないことが望まれるであろう).
   - EPOC-2 で使用するパラメータ g の生成法が明確に示されていない.
2. EPOC-2 の仕様記述において, 元になった論文 [7] と矛盾している部分がある. このため, EPOC-2 の仕様記述では安全性が保証されない可能性がある, と指摘されている. 具体的には以下のような指摘である.
   - EPOC-2 の仕様記述において,

パラメータ h はランダムに選ばれた $h_0 \in \boldsymbol{Z}_n^*$ より $h = h_0^n \bmod n$ のように構成される. $h = g^n \bmod n$ としても良い (英語では "can be").

と書かれてあるのに対し, 元となった論文 [7] では, $h = g^n \bmod n$ が必須となっている.

3. EPOC-2 で用いるパラメータ $n = p^2q$ の最小推奨サイズ (960 bits) について, 安全性を保証できる期間, すなわち寿命が短い可能性がある, と指摘されている. その理由は以下の通りである.

   - p^2q の形をした合成数に対する現時点で最強の素因数分解法は数体ふるい法 (NFS) である. 合成数のサイズ D(digits) と, そのサイズの合成数が NFS で解ける年を予想した数式 [6]

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

     に合成数 n の最小推奨サイズ 960(bits)=289(digits) を代入した場合, その寿命が来るのは $Y = 2016$(年) となる.

4. EPOC-2 で用いるパラメータ k,r の条件と, 推奨パラメータサイズに矛盾がある, と指摘されている. 具体的には以下の通りである.

   - 仕様では $r > 2k$ なる条件が挙げられている. それに対して推奨パラメータとして $k \geq 320$ が挙げられている. さらに代表的なパラメータとして $r = 832$ が挙げられている. k を最小推奨サイズとした場合, $r > 2k$ が満たされない可能性がある. 結果として, 安全性に関する主張が満たされなくなる可能性がある.

5. EPOC-2 の安全性を証明するための仮定, p-subgroup 仮定, の定義に問題がある, そのため EPOC-2 では, 素因数分解問題の困難性 (素因数分解問題仮定) に基づく安全性の証明がなされているとは言えない, と指摘されている.

2.1.2 EPOC-2 のスキームに関する指摘

1. EPOC-2 が最強の安全性を満たすためには $l_R \simeq k - 1$ である必要がある, しかし仕様では $l_R \leq k - 1$ であることのみが条件として挙げられている, これでは $l_R << k - 1$ であっても構わないことになるため, 結果として安全性が証明できてない, と指摘されている.
   ただし, 自己評価書 [2] では $l_R = k - 1$ と設定され, 安全性の議論がなされている, とも指摘されている.
2. EPOC-2 が最強の安全性を満たすためには $l > 2k$ とするべきである, しかし仕様ではその記述がないため, $l << 2k$ であっても構わないことになり, 結果として安全性が証明できてない, と指摘されている.
   ただし, 自己評価書 [2] では $l = (2 + c_0)k$ と設定され, 安全性の議論がなされている, とも指摘されている.
3. EPOC-2 で用いるパラメータ h のオーダ d は大きい値となるように選ばれるべきであるが, 仕様書や自己評価書 [2] ではそれについての明確な記述がない, と指摘されている.

2.2 指摘された問題点に対する考察

2.2.1 EPOC-2 で用いられているプリミティブに関する指摘

1. #2 で指摘された通り, そこで例示された, 素数 $p-1$ についての条件, g の生成法の記述等が欠落している.
   $p-1$ が小さな素数をその因数として持つような p を使用すると, 簡単に素因数分解ができてしまう. また g の生成法が示されていないことにより, 適当でない値が使用されてしまう可能性がある. これらの結果, EPOC-2 が簡単に破られてしまう危険がある. 暗号学的には当然満たすべき条件ではあるが, 実装者がそのような知識を持っている保証はない. したがって #2 の指摘は妥当であり, 記述を加える必要があると思われる.
2. #2 で指摘された通り, 英語版の仕様書では, プリミティブの説明と EPOC-2 暗号仕様 (スキーム) の記述両方で,

   > パラメータ h はランダムに選ばれた $h_0 \in \boldsymbol{Z}_n^*$ より $h = h_0^n \bmod n$ のように構成される. $h = g^n \bmod n$ としても良い (英語では "can be").

   と書かれている. 元となった論文 [7] では, $h = g^n \bmod n$ が必須となっている. またそこでは h_0 を用いた定義とはなっていない. 日本語版の仕様書において, プリミティブの説明では #2 の指摘のような記述となっているが, EPOC-2 暗号仕様 (スキーム) の記述では,

   > $hLen = (2 + c_0)k(c_0$: 正定数) のとき, h は $g^n \bmod n$ としても良い.

   と書かれている. このように英語版では, 日本語版で書かれていた条件が欠落している. この矛盾が解決され, さらに以降で議論するパラメータサイズにおける欠陥の可能性等が解決すれば, ここでの指摘も解決するかもしれない. しかし現在提示されている内容だけでは, #2 の評価結果に影響を与えるかどうか明らかではない.
3. #2 で指摘された通り, NFS を用いて素因数分解できる数の大きさと, それが達成されると予想される年の関係を表した数式 [6] を信頼するならば, $n = p^2q$ の最小推奨サイズ (960 bits) では, 2016 年に解読されてしまうことになる. 確かにこれは寿命として短いと考えられ, したがって使用に際しては, より長いサイズの合成数を用いるべきであると考えられる.
4. #2 で指摘された通り, パラメータ k,r の条件 ($r > 2k$) と, 推奨パラメータサイズに関する記述は書かれている. ただし仕様書の記述を見ると, 矛盾と言うのはおかしい. #2 での指摘では, 矛盾を引き起こすサイズとして, k は最小推奨サイズ (320 bits), r は代表的な (英語版では typical) パラメータのサイズ (832 bits) を用いている. このとき条件, $r(= 832) > 2k(= 640)$ は成立しており何ら問題はない. 仕様書においても, 代表的なパラメータ k のサイズとしては $k = 384$ と記述されており, この場合も $r(= 832) > 2k(= 768)$ となり, 条件は成立している. 以上述べたように, この部分について #2 の指摘は誤っているように思われる.
5. #2 ではまず, p-subgroup 仮定を定義し, 元になった論文 [7] での仮定 (#2 では OU 仮定と呼んでいる) との等価性を証明している. さらに computational p-subgroup 仮定を定義し, それが [7] で用いられている関数の逆計算の困難性 (OU 関数仮定), さら

に素因数分解問題仮定と等価であることを証明している. 結果として,

$$OU \text{ 仮定 } = p\text{-subgroup 仮定}$$

$$\leq \text{computational } p\text{-subgroup 仮定 } = \text{OU 関数仮定 } = \text{素因数分解問題仮定}$$

が示されている (大きい方がより一般的な仮定であることを表す). この証明の中で, 2 の $h = g^n \bmod n$ が用いられている. #2 の指摘は正しいように思われるが, 2 の矛盾点等もあり, 結論には至らなかった.

2.2.2 EPOC-2 のスキームに関する指摘

1. #2 で指摘された通り, EPOC-2 が最強の安全性を満たすためには $l_R \simeq k-1$ である必要があると思われる. $l_R << k-1$ では, 明らかに安全性が証明できない. 仕様の記述は指摘されたように, あるいは自己評価書 [2] の記述 ($l_R = k-1$) のように修正されるべきである.
   ちなみに #2 では, l_R を 1bit 短くすると, 解読成功確率
   $$\frac{\varepsilon'}{q_H + q_G}, \text{ ここで } \varepsilon' \text{ は } \varepsilon/2 \leq \varepsilon' + \frac{q_D}{d} + \frac{q_G + q_H}{2^{l_R}},$$
   の $(1/2)^{l_R}$ の「1/2」の乗算回数が 1 回減るとの解析がなされている.
2. #2 で指摘された通り, EPOC-2 が最強の安全性を満たすためには $l > 2k$ とするべきである. $l << 2k$ では, 明らかに安全性が証明できない. 仕様の記述は指摘されたように, あるいは自己評価書 [2] の記述 ($l = (2 + c_0)k$) のように修正されるべきである.
3. #2 で指摘された通り, EPOC-2 で用いるパラメータ h のオーダ d に関する明確な条件の記述は見られないが, 暗黙のうちにその性質を利用して, 仕様書 [1] や自己評価書 [2] が記述されているように思われる. 仕様書や自己評価書で, それについての明確な記述を付加すべきである.

3 EPOC-2' CRYPTREC2001 応募仕様書および自己評価書

本章では, CRYPTREC2001 に応募された EPOC-2 の改訂版 (EPOC-2') の応募資料, 仕様書および自己評価書に基づき, #2 で指摘された点についてその有効性を議論する.

3.1 EPOC-2 で用いられているプリミティブに関する指摘

1. #2 で指摘された, 素数 $p-1$ についての条件, g の生成法の記述等が依然欠落している. 同様に記述を加える必要があると思われる.
2. EPOC-2' の仕様書でこの部分に関する記述は, プリミティブ関数, KGP-OU の規定中に現れる. そこでは h, g がランダムに, かつ独立に選ばれているという以上の記述はない. したがって考察と同様, 現在提示されている内容だけでは, #2 の評価結果に影響を与えるかどうか, 依然不明である.

3. EPOC-2' の仕様書では, $n = p^2q$ のビットサイズ設定基準は,

$$\text{bit size of } n \geq 1024, pLen \geq 342,$$

パラメータ推奨値は,

$$\text{bit size of } n = 1152, pLen = 384,$$

と規定されている. n 1024 bits の場合, $D = 309$ となり, $Y = 2018$ となる (これは [6] にも記述されている). これを信用するならば, やはり暗号の寿命として短いと考えられ, より長いサイズの合成数, 素数を用いるべきであると考えられる. しかし見直す際には, RSA 暗号等, 他の暗号も同様に見直されるべきである.

4. 指摘が誤りであるため, 考察の必要はなし.
5. 特に新たな記述はなく, 2 と関係することもあり, 同様に結論には至らなかった.

3.2 EPOC-2 のスキームに関する指摘

1. EPOC-2' の仕様書では, $l_R \simeq k - 1$ であるよう記述されている. 記号が異なるが具体的には,

$$rLen = \lfloor (pLen - 1)/8 \rfloor$$

と定義されている. したがって問題は解決されている.

2. EPOC-2' の仕様書では, 指摘されたような $l > 2k$ なる条件は記述されていない. パラメータサイズとして具体的には,

$$\text{乱数}, 0 \leq r < n \text{ なる整数}$$

のみ記述されている. n は $3k$ bits であるから, そのように見なせば問題は解決していると言える.

3. EPOC-2' の仕様書でも h のオーダ d に関する明確な条件の記述は見られない. やはり仕様書や自己評価書で, それについての明確な記述を付加すべきである.

4 結論

以上述べたように指摘の誤りや, 仕様記述の不備に起因する問題点がほとんどであった. またその他の有効な攻撃については, 新たに見つからなかった. したがって, 注意深く実装すれば, あるいはさらなる改訂版を出しそれに基づいた実装をすることにより, 安全な暗号を用いることが可能であると考えられる. また評価者は, プリミティブに関する指摘 2 について, および p-subgroup 仮定に関する指摘 (両者には関係がある) について結論を出すことができなかった. この点についてはさらなる評価をしていただきたい.

参考文献

[1] Specification of EPOC, CRYPTREC2000 応募書類.

[2] Self Evaluation of EPOC, CRYPTREC2000 応募書類.

[3] Evaluation Report on the EPOC Cryptsystem,
CRYPTREC2000 詳細評価報告書 #2

[4] Specification of EPOC-2, CRYPTREC2001 応募書類.

[5] Self Evaluation of EPOC-2, CRYPTREC2001 応募書類.

[6] S.Cavallar, B.Dodson, A.K.Lenstra el.al,
Factorization of a 512-Bit RSA Modulus, Eurocrypt 2000, LNCS1807, pp.1-18, Springer-Verlag, 2000.

[7] T.Okamoto and S.Uchiyama,
A New Public-Key Cryptsystem as Secure as Factoring, Eurocrypt'98, LNCS1403, pp.308-318, Springer-Verlag, 1998.