暗号アルゴリズム「EPOC」
詳細評価(攻撃評価)レポート

２００１年1月１２日

1. まえがき

今日、公開鍵暗号を提案するにあたっては、今までの歴史的経緯もあって、妥当な仮定のもとでその安全性が証明されていることが標準的となっている。EPOC 暗号は、この要件をみたす公開鍵暗号の 1 つである。

EPOC 暗号は EPOC-1, EPOC-2, EPOC-3 の 3 つのバージョンをもち、それぞれ、EPOC 暗号仕様書[EPOCa]、及び EPOC 暗号自己評価書[EPOCb]に記載されている通り、ある仮定のもとで、最強とされる安全性（適応的暗号文選択攻撃に対する安全性[BDPD98]：semantically secure against adaptive chosen ciphertext attack）が証明された公開鍵暗号方式である。ただし、その安全性が証明されるために要求される仮定は、EPOC-1 に関しては p-部分群仮定と真のランダム関数の仮定、EPOC-2 に関しては $n=p^2q$ 型の素因数分解仮定と真のランダム関数の仮定、EPOC-3 に関しては $n=p^2q$ 型の Gap-素因数分解仮定と真のランダム関数の仮定である。

本評価書では、EPOC 暗号に対して、[EPOCa][EPOCb]に記載されている内容を検証すると共に、特長・適応性、安全性、効率性の観点から詳細評価を行うことを目的とする。

2. 暗号プリミティブについて

EPOC の中で利用されている暗号化関数は、OU (Okamoto-Uchiyama) 関数である [OU98]。ここで、OU 関数の一方向性を破ることは、$n=p^2q$ の素因数分解問題を解くことと同じくらい難しいことが証明されている [OU98]。EPOC 暗号はこの OU 関数をもとにし、[FO99a][FO99b][OP00]による手法を施すことで構成されている。正確には、[FO99a]による手法で EPOC-1 が、[FO99b]による手法で EPOC-2 が、そして[OP00]による手法で EPOC-3 が構成されている。一方、OAEP-RSA で用いられている暗号化関数は RSA 関数[RSA78]であり、RSA 関数の一方向性を破ることは RSA 問題を解くことと同じくらい難しい。OAEP-RSA は RSA 関数に[BR94]による手法を施すことで構成されている。

3. 特長・適応性

今回提出されている秘匿通信を目的とする EPOC 暗号は、EPOC-1, EPOC-2, EPOC-3 という 3 つのバージョンをもつ。本節では、[EPOCa] [EPOCb] にそって、それぞれのバージョンの特長・適応性を述べる。

3. 1　EPOC-1

共通鍵暗号の鍵（高々256 bit）の配送に適している。

3. 2.　EPOC-2

EPOC-2 は、公開鍵暗号と共通鍵暗号を組み合わせたハイブリッド暗号化方式である。EPOC-2 は、任意長の共通鍵暗号鍵の配送、及び長い平文の秘匿通信、特にカプセル的な利用方法（つまり、鍵配送とデータ配送が同期している）に適している。

3. 3.　EPOC-3

EPOC-3 は、任意長の共通鍵暗号鍵の配送、及び長い平文の秘匿通信、特にカプセル的な利用方法（つまり、鍵配送とデータ配送が同期している）に適しており、更にセッション的利用方法（つまり、セッション開設時における鍵配送とそれ以降の該セッション開設中の共通鍵暗号によるデータ暗号化）に適している。ただし、EPOC-3 は安全性のための仮定では EPOC-2 に比べ、より強い仮定（4 節で後述）が必要とされるが（したがって、この意味では EPOC-2 の方が優位であるが)、復号の処理速度（5 節で後述）やセッション的利用方法等の性能・機能面では、EPOC-2 よりも優れている。

4. 安全性

4. 1. EPOC 暗号の安全性

EPOC 暗号は[EPOCa][EPOCb]に記載されている通り、ある仮定のもとで最強の安全性（適応的選択暗号文攻撃に対して強秘匿性[BDPD98]）が証明されている公開鍵暗号化方式である。より正確に言えば、[EPOCb]に記載の通り、次の結果が既に示されている。

定理 4.1 [EPOCb] p-部分群仮定が正しければ、ランダムオラクルの下で、EPOC-1 は適応的選択暗号文攻撃に対して強秘匿である。

定理 4.2 [EPOCb] EPOC-2 で用いる共通鍵暗号をバーナム暗号とする。このとき、$n=p^2q$ に対する素因数分解仮定が正しければ、ランダムオラクルの下で、

EPOC-2 は適応的選択暗号文攻撃に対して強秘匿である。

定理 4.3 [EPOCb] EPOC-2 で用いる共通鍵暗号が受動的攻撃の下で安全であるとする。このとき、$n=p^2q$ に対する素因数分解仮定が正しければ、ランダムオラクルの下で、EPOC-2 は適応的選択暗号文攻撃に対して強秘匿である。

定理 4.4 [EPOCb] EPOC-3 で用いる共通鍵暗号をバーナム暗号とする。このとき、$n=p^2q$ に対する Gap-素因数分解仮定が正しければ、ランダムオラクルの下で、EPOC-3 は適応的選択暗号文攻撃に対して強秘匿である。

定理 4.5 [EPOCb] EPOC-3 で用いる共通鍵暗号が受動的攻撃の下で安全であるとする。このとき、$n=p^2q$ に対する Gap-素因数分解仮定が正しければ、ランダムオラクルの下で、EPOC-3 は適応的選択暗号文攻撃に対して強秘匿である。

以上の結果において、安全性が証明されるために要求される仮定をまとめると表 1 のようになる。

表 1: EPOC が安全であるために要求される仮定

	数学的仮定	ランダム関数仮定
EPOC-1	p-部分群仮定	真にランダム
EPOC-2	$n = p^2q$ の素因数分解仮定	真にランダム
EPOC-3	$n = p^2q$ の Gap-素因数分解仮定	真にランダム

4. 2. 他方式との比較

ここでは、EPOC 及び他方式との安全性の比較を行う。EPOC[EPOCa][EPOCb], OAEP-RSA[BR94], Cramer-Shoup 暗号[CS98] はいずれもある仮定のもとで、最強の安全性（適応的選択暗号文攻撃に対して強秘匿性[BDPR98]）が証明された公開鍵暗号方式である。表 2 では各方式の安全性が証明されるための仮定がまとめられている。これらの方式が安全であるための基になる数学的仮定は、素因数分解問題あるいは離散対数問題に深く関連している。

まず、Cramer-Shoup 暗号では DDH 仮定が要求され、これは（基本的な離散対数仮定よりも強い仮定である）DH（Diffie-Hellman）仮定よりも更に強い仮定である。しかしながら、ランダム関数仮定においては、OAEP-RSA と EPOC

が真のランダム関数のもと（ランダムオラクルモデル）で安全性が示されているのに対し、Cramer-Shoup 暗号では現実的な汎用一方向性ハッシュ関数(Universal One Way Hash Function)で安全性が示されているので、この点ではCramer-Shoup 暗号が優れていると言える。

一方、EPOC 及び OAEP-RSA のベースとなる数学的仮定は素因数分解問題に深く関連している．EPOC-1,EPOC-3 で要求される p-部分群仮定、$n = p^2q$ 型の Gap-素因数分解仮定はいずれも $n = p^2q$ 型の素因数分解仮定よりも強い仮定であるので、仮定の強弱の意味においては、この中で一番仮定の弱い $n = p^2q$ 型の素因数分解仮定のもとで安全性が保証される EPOC-2 が優れていると言える。また、$n = p^2q$ 型の素因数分解と $n = pq$ 型の素因数分解が同じくらい難しいとすれば（このことについては 4.3.1 節で後述）、RSA 仮定の方が $n = p^2q$ 型の素因数分解仮定よりも強いため、結局、数学的仮定の中では EPOC-2 が一番優れていると言える。

表 2: 各種方式が安全であるために必要とされる仮定

	数学的仮定	ランダム関数仮定
EPOC-1	p-部分群仮定	真にランダム
EPOC-2	$n = p^2q$ の素因数分解仮定	真にランダム
EPOC-3	$n = p^2q$ の Gap-素因数分解仮定	真にランダム
OAEP-RSA	RSA 仮定	真にランダム
Cramer-Shoup	DDH 仮定	UOWHF

（ただし、DDH 仮定は決定 Diffie-Hellman (Decision Diffie-Hellman) 仮定を、UOWHF は汎用一方向性ハッシュ関数 (Universal One Way Hash Function) を意味する。）

4. 3. 不明点

4. 3. 1. $n = p^2q$ 型 の素因数分解について

現在、$n = p^rq$ （r は大）の場合の素因数分解は Lattice Reduction Algorithm を応用した素因数分解法（Lattice Factoring Method）[BDH99]により、入力サイズの多項式時間で解かれることが知られている。しかしながら、$n = p^rq$ （r は小）の場合、特に $n = pq$ 及び $n = p^2q$ の場合にはこの方法は効率的ではない。現在、素因数依存型（つまり、計算量が素因数の性質によって決まるタイプ）の強力な素因数分解アルゴリズムとしては楕円曲線法 [Len87][Cop93]が知られており、$n = p^2q$ 型の素因数分解に対しての楕円曲線法の工夫も報告されてい

る[PO96]。また、合成数依存型（つまり、計算量が合成数のサイズのみによって決まるタイプ）の強力な素因数分解アルゴリズムとして、数体ふるい法[LLMP90]が知られている。結局のところ、現在、$n = pq$ 型、及び $n = p^2q$ 型の大きな合成数 n を素因数分解する上で最高速とされているアルゴリズムは合成数依存型の素因数分解アルゴリズムである数体ふるい法である。したがって、[EPOCb]に記載されている通り、現時点では $n = p^2q$ のサイズを $n = pq$ のサイズと同じくらいにすれば困難性は同等であると考えられるが、$n = pq$ 型の素因数分解の困難性に比べて $n = p^2q$ 型の素因数分解の困難性が本質的に同等かどうかは現在報告されていない。

4. 3. 2. ランダムオラクルモデルとその実現方式の安全性について

EPOC の安全性は、OAEP-RSA の場合と同様、理論的には真にランダムな関数を仮定して（つまり、ランダムオラクルモデルのもとで）証明されている。しかし、方式の実現に際しては、実際にはそのランダム関数の部分を実用的なハッシュ関数（例えば、SHA-1）で置き換えて構成されている。したがって、このように実現された方式に対しては、厳密には理論どおりの安全性がそのまま保証される訳ではないが、このアプローチは OAEP-RSA の提案以来、標準的であり、現在までこのアプローチに対する問題は特に報告されていない。ただし、これに関連した結果として、ランダムオラクルモデルのもとでは安全であるが、それを実際的な関数で実現した場合、安全でなくなるような特別な例が示されている[CGH98]。しかし、彼らの結果は、ランダムオラクルモデルとその実現方式において安全性のギャップが生じる例が現実にあるという意味では興味深いが、その例の構成法はかなり特殊であるため、今まで実際に注意深く構成された各暗号方式に対して、どの程度の意味をもつのかは不明である。

5. 効率性

[EPOCb]では EPOC の効率性についての議論が行われている。ここで、議論の対象となっているのは、EPOC（EPOC-1, EPOC-2, EPOC-3）に対しての暗号化処理量、復号処理量、暗号文長である。パラメータ設定としては 2 種類が与えられており（表 3, 表 4）、その設定のもと、EPOC-1, EPOC-2, EPOC-3 におけるそれぞれのデータが与えられている。また、OAEP-RSA のデータとの比較も行われている（EPOC, RSA-OAEP はいずれも素因数分解問題をベースにした公開鍵暗号であるため、比較の対象として妥当であると思われる）。ただし、効率性の評価には全体のプロセスの中で最も支配的だと考えられる剰余乗算の

回数により評価されている。実際、[EPOCb]に記載されている通り、その他の処理（加算、ハッシュの処理）はこれに比べるとほぼ無視できる程度のものと思われる。

データからもわかるように、効率を重視したパラメータ設定（パラメータ設定 1）において、EPOC 暗号は OAEP-RSA に比べ、暗号化処理速度においては劣るものの、復号処理速度では優れている。

表 3　：パラメータ設定 1（[EPOCb, 4.1 節]）

	EPOC-1	EPOC-2	EPOC-3
平文の長さ（mLen）	128	128	128
ハッシュ値の長さ（hLen）	208	128	128
乱数の長さ（rLen）	80	128	128
乱数の長さ（Rlen）			128
共通鍵暗号の鍵長（gLen）		128	128

（ただし、単位は bit である。）

表 4：パラメータ設定 2（[EPOCb, 4.2 節]）

	EPOC-1	EPOC-2	EPOC-3
平文の長さ（mLen）	128	128	128
ハッシュ値の長さ（hLen）	832	832	128
乱数の長さ（rLen）	80	128	832
乱数の長さ（Rlen）			128
共通鍵暗号の鍵長（gLen）		128	128

表 5：　処理量等の比較（パラメータ設定 1 のもと）

方式	鍵長 (bits)	暗号文長 (bits)	暗号化 (#M(1152))	復号化 (#M(1152))
EPOC-1	1152	1152	364	266
EPOC-2	1152	1280	224	188
EPOC-3	1152	1408	224	64
OAEP-RSA	1152	1152	33	432

（ただし、EPOC-2, EPOC-3 で用いる共通鍵暗号としては、バーナム暗号を用いている。また、#M(1152)は 1152bits の法のもとでの剰余乗算の回数を意味する。）

表 6： 処理量等の比較（パラメータ設定 2 のもと）

方式	鍵長 (bits)	暗号文長 (bits)	暗号化 (#M(1152))	復号化 (#M(1152))
EPOC-1	1152	1152	1300	786
EPOC-2	1152	1280	1280	775
EPOC-3	1152	1408	1280	64
OAEP-RSA	1152	1152	33	432

（ただし、EPOC-2, EPOC-3 で用いる共通鍵暗号としては、バーナム暗号を用いている。）

6. まとめ

本評価では、EPOC 暗号に関して現在提出されている EPOC 暗号仕様書[EPOCa]、及び EPOC 暗号自己評価書[EPOCb]の記載内容を検証すると共に、EPOC 暗号に対して詳細評価を行った。

参考文献

[BR94] M. Bellare and P. Rogaway, ``Random Oracles are Practical: A Paradigm for Designing Efficient Protocols", Proc. of the First ACM Conference on Computer and Communications Security, pp.62-73.

[BR94] M. Bellare and P. Rogaway, ``Optimal Asymmetric Encryption", Proc. of Eurocrypt'94, LNCS 950, Springer-Verlag, pp.92-111, 1994.

[BDPR98] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, ``Relations Among Notions of Security for Public-Key Encryption Scheme", Proc. of Crypto'98, LNCS 1462, Springer-Verlag, pp.26-45, 1998.

[BDH99] D. Boneh, G. Durfee and N. Howgrave-Graham, ``Factoring $N=p^r q$ for Large r", Proc. of Crypto '99, LNCS 1666, Springer-Verlag, pp.326-337, 1999.

[CGH98] R. Canetti, O. Goldreigh and S. Halevi, ``The Random Oracle Methodology, Revisited'' (preliminary version), Proc. of STOC, ACM Press, pp.209-218, 1998.

[Cop93] D. Coppersmith, ``Modifications to the number field sieve'', Journal of Cryptology, vol. 6, pp.169-180, 1993.

[CS98] R. Cramer and V. Shoup, ``A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack'', Proc. of Crypto '98, LNCS 1462, Springer-Verlag, pp.13-25, 1998.

[FO99a] E. Fujisaki and T. Okamoto, ``How to Enhance the Security of Public-Key Encryption at Minimum Cost", Proc. of PKC'99, LNCS 1560, Springer-Verlag, pp.53-68, 1999.

[FO99b] E. Fujisaki and T. Okamoto, ``Secure Integration of Asymmetric and Symmetric Encryption Schemes", Proc. of Crypto'99, LNCS 1666, Springer-Verlag, pp.535-554, 1999.

[FOPS00] E. Fujisaki, T. Okamoto, D. Pointcheval and J. Stern, ``RSA-OAEP is Still Alive'', manuscript, December, 2000, available from http://cgi.dmi.ens.fr/cgi-bin/pointche/papers.html?FuOkPoSt00.

[LLMP90] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse and J. M. Pollard, ``The Number Field Sieve'', Proc. of STOC, pp.564-572, 1990.

[Len87] H. W. Lenstra Jr., ``Factoring integers with elliptic curves'', Annuals of Mathematics, 126, pp.649-673, 1987.

[OP00] T. Okamoto and D. Pointcheval, ``OCAC: an Optimal Conversion for Asymmetric Cryptosystems", manuscript, 2000.

[OU98] T. Okamoto and S. Uchiyama, ``A New Public-Key Cryptosystem as Secure as Factoring", Proc. of Eurocrypt'98, LNCS 1403, Springer-Verlag, pp.308-318, 1998.

[PO96] R. Peralta and E. Okamoto, ``Faster Factoring of Integers of a Special Form", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E79-A, 4, pp.489-493, 1996.

[RSA78] R. Rivest, A. Shamir and L. Adleman, ``A Method for Obtaining Digital Signature and Public-Key Cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

[Sho00] V. Shoup, ``OAEP Reconsidered", manuscript, November 2000 (revised December 2000) available from http://www.shoup.net/papers/

[EPOCa] EPOC暗号仕様書

[EPOCb] EPOC暗号自己評価書