公開鍵暗号技術評価報告

2001年4月18日

公開鍵暗号評価小委員会委員長
横浜国立大学 大学院 環境情報研究院 教授
松 本　勉

公開鍵暗号技術の評価作業の概要（平成12年度）

- 公開鍵暗号評価小委員会を構成
- 詳細評価対象暗号の決定
  - 公募により提案された暗号のスクリーニング
  - 公募への提案の有無に関わらず評価を要する暗号を選択
- 詳細評価＜安全性評価＋ソフトウェア実装評価＞
  - 各暗号につき国内外の優秀な複数の暗号研究者（匿名）に委託して行った安全性評価
  - 応募者実装コードの同一プラットフォーム上での計測
  - 公表文献・学会発表等の調査
  - 暗号技術評価委員会における安全性および実装性の評価とりまとめ

評価対象

- 公開鍵暗号
  - 守秘、認証、署名、鍵共有
  - 暗号プリミティブに基づく暗号スキーム
    - 暗号プリミティブ：素因数分解問題や離散対数問題等に基づく基本暗号
    - 暗号スキーム：暗号プリミティブやハッシュ関数等に基づく暗号アルゴリズム

評価基準

- 安全性評価
  - 暗号スキームに関する安全性評価項目
    - 攻撃の方法：受動的攻撃、能動的攻撃
    - 攻撃の目標：実現すべき機能（守秘、認証、署名、鍵共有）の欠損状況
    - ある仮定の下での証明可能安全性を有するか
  - 暗号プリミティブに関する安全性評価項目
    - 既知の攻撃法に対する計算量的耐性
  - 鍵やパラメータの選択方法が明確か
- 実装性評価
  - 第三者が実装可能か
    - 仕様に曖昧さがなく、実装に必要な情報はすべて公開されているか
  - 許容できるソフトウェアによる処理性能を有するか

詳細評価対象公開鍵暗号一覧（平成12年度）

機能 安全性の根拠	署名	守秘	鍵共有
素因数分解問題 **IF**	ACE Sign ESIGN-signature 註1） RSA-PSS	EPOC-1 註3） EPOC-2 註3） EPOC-3 註3） HIME-1 註4） HIME-2 RSA-OAEP	
離散対数問題 **DL**	DSA	ACE Encrypt	DH
楕円曲線 **離散対数問題** **ECDL**	ECDSA in SEC1 MY-ELLTY 註2） ECMR-160/192/OEF-h	ECAES in SEC1 PSEC-1 註3） PSEC-2 註3） PSEC-3 註3）	ECDHS in SEC1 ECMQVS in SEC1 HDEF-ECDH

詳細評価対象公開鍵暗号一覧についての註

1）ESIGN-identificationというスキームが「認証」機能の項目で応募されたが、
認証プロトコルとしての記述がなく、「署名」機能の項目で応募された
ESIGN-signatureと名称以外は同一であるので、ESIGN-signatureに合併した。
2）MYELLTY ECMR-160/192/OEF-h は、MY-ELLTY ECMR-160-h,
MY-ELLTY ECMR-192-h, MY-ELLTY ECMR-OEF-hという異なる3件の
応募であったが、使用する体が異なるだけで、署名スキームとしては同一の
ものと見なせるため、3件をまとめて評価することとした。
3）EPOC-1, EPOC-2, EPOC-3はEPOCという名称の暗号の組として、また
PSEC-1, PSEC-2, PSEC-3はPSECという名称の暗号の組として、それぞれ
応募されたが、個々に異なる方式であるので、このように分類した。
4）HIME-1は「鍵共有」機能の項目で応募されたが、暗号の形式としては共有すべき
鍵を一方のエンティティが公開鍵方式で暗号化して他方のエンティティに送る
というものであり、このような使い方は「守秘」機能の項目に分類される全ての暗号に
適用できるものであるから、HIME-1は「守秘」機能の項目に配置した。すなわち,
「鍵共有」機能の項目には共有される鍵の生成に両エンティティが関与するもの
だけを配置することにした。

公開鍵暗号技術の総評

- 本プロジェクトで詳細評価を行った公開鍵暗号技術は、
  - 実装性についてはいずれの暗号も概ね許容できる処理性能を有していることが、ソフトウェア実装評価の結果から確認できる。

  そこで以下では、
  - 安全性に重点をおいて、署名、守秘、鍵共有の機能別に、各々の暗号技術に対する本プロジェクトにおける評価をまとめる。
  - 安全性に関して暗号技術の提案者の主張とは異なる指摘がなされ、その妥当性について本プロジェクトで結論を出すに至らなかった事項については、その旨を明記している。
  - これらの事項については、本プロジェクトの後継プロジェクト等で評価を続けることが望ましい。

公開鍵暗号技術の安全性評価の考え方

- 電子政府で用いる暗号技術に求められる基本的な性質
  - パラメータ指定の仕方を含み具体的に規定された暗号が、
  - 現時点において安全であり、
  - 直ちに安全でなくなる危険性も小さいであろうと、
  - 広くコンセンサスを得られるものであること
- 豊富な使用実績があり現時点までに安全性の上で特段の問題点が指摘されていないという経験的な知識もそのようなコンセンサスの形成に役立つであろうが、
- 安全性を評価する上で曖昧な部分をなるべく絞りこむ方法として、証明可能安全性という概念を用いることが有効であろう。

公開鍵暗号の「証明可能安全性」とは(1)

- 証明可能安全性という概念は、暗号が安全であることが証明されているということを示すものではない。
- 本報告では、
  - 「ある仮定の下での証明可能安全性を有する」

  という表現を用いて次の状況を示す：
- ある公開鍵暗号が証明可能安全性を有するとは、
  - その暗号またはその暗号の理想化暗号に対して、
  - その暗号で守りたい安全性を脅かす攻撃方法があれば、それを使って、別の数学的問題を低い計算量で解く方法が導けることを、
  - 何らかの前提のもとで、厳密に証明できること。

公開鍵暗号の「証明可能安全性」とは(2)

- ただし、ある暗号の理想化暗号とは、
  その暗号スキームが用いる補助関数（ハッシュ関数など）を仮想的なもの（ランダム関数など）に置き換えた以外はもとの暗号と全く同じである仮想的な暗号のことを指す。

- 表現「ある仮定の下での」は、その暗号自身についてであるか仮想暗号についてであるかの違い、数学的問題の種類や計算量的困難性の違い、問題とする安全性の種類の違い、攻撃方法の種類の違い、前提の違い、などがあり、これら次第でその暗号の安全性に対して与えられる信頼感には多様性があることを伝えるために用いている。

公開鍵暗号の「証明可能安全性」とは(3)

- 証明可能安全性の証明自体が誤りでない限り、
  ある暗号が証明可能安全性を有すること自体が
  時間経過によって覆ることはない。

- しかし、数学的問題の計算量的困難性の見積りは、
  理論の進歩や技術環境の変化によって変動するものであるから、
  ある仮定の下での証明可能安全性を有していて、
  その仮定が現時点においては満たされていると判断される暗号で
  あっても、安全とはいえない暗号に将来変わることがありえる。

- さらに、安全性において理想化暗号とのギャップが著しいことが将来
  判明することもありえる。

公開鍵暗号の「証明可能安全性」とは(4)

- また、ある暗号が証明可能安全性を有することが現時点で示されていないことが、その暗号が安全でないことを意味するわけではない。

- 利用実績があり現時点で特段の安全性上の問題点が発見されていないが、安全性を証明可能安全性という形で示すことが現時点の証明技術ではできていないという場合もある。

- なお、証明可能安全性を達成する暗号を構成する方法は、署名や守秘のための暗号に対しては確立されつつあるが、鍵共有のための暗号に対しては必ずしもそのような状況には至っていないと考えられる。

(1) ACE Sign　　署名

- ACE Signは、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。若干強い数学的仮定が必要なものの，証明可能安全性を有することの証明が、他の署名機能をもつ暗号と異なり、補助関数を仮想的なものに置き換えることなく行えることが特徴である。
- また法（モジュラス）である合成数nと素因数pのサイズには以下の条件がある：1024≦｜n｜≦16384、｜p｜≧512。さらに素因数の形も限定されている。なお、補助関数として用いられている共通鍵暗号はMARSに限定された仕様となっている。
- 参考情報：本応募暗号の提案者は，同名であるが仕様が本応募とは異なる暗号を暗号技術公募への応募後に発表している。

(2) ESIGN-signature　署名

- ESIGN-signatureは、現時点においては安全性に大きな脅威を与える問題点は解消されている。
- ある仮定の下での証明可能安全性を有する。この仮定を満たすためには適切なパラメータを選択することに注意を払う必要がある。
- 法である合成数の素因数分解の形がRSA署名方式（教科書的RSA署名方式およびRSA-PSS）と異なるため、法がRSA署名方式と同じサイズでも安全性は同等とは限らないことに注意を払う必要がある。
- さらに、安全性は法nにおけるe乗根近似問題の困難性に依存しており、これはnの値とeの値に依存するという特徴がある。
- この点で、提案者の仕様書中の条件(e≧5)、提案者の推奨パラメータ(e≧8, ｜p｜=｜q｜≧320, ｜n｜≧960)、ソフトウェア実装評価時の提案者による採用パラメータ(e = 2^10, ｜p｜=｜q｜= 384, ｜n｜= 1152)、電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針案の条件(e≧8, ｜n｜≧1024)のように各所であげられた条件やパラメータ設定例が異なるので使用においては、十分な吟味が必要である。

(3) RSA-PSS　　署名

- RSA-PSSは、現時点において安全性の上で特段の問題点は指摘されていない。
- 現在多く使われている教科書的RSA署名方式は証明可能安全性を有することは確認されていないのに対し，RSA-PSSはある仮定の下での証明可能安全性を有していることが利点であるが、その仮定を満たすために適切なパラメータを選択することに注意を払う必要がある。

(4) DSA　　署名

- FIPS 186-2のDSAは、現時点において安全性の上で特段の問題点は指摘されていない。ただし、パラメータの選択にあたっては離散対数問題が困難になるように注意を払う必要がある。
- 法のサイズは512ビット以上1024ビット以下と規定されていて1025ビット以上にはできないため、達成しうる安全性には上限があることにも注意を払う必要がある。
- 証明可能安全性を有することは確認されていない。
- なお、乱数生成方法の例としてFIPS 186-2 Appendix 3に記述されている方法は、最近その有効性については疑問が提示されており、更なる検討が必要である。

(5) ECDSA in SEC1　　署名

- ECDSA in SEC1は、現時点において安全性の上で特段の問題点は指摘されていない。
- 推奨パラメータを記したSEC2で具体的に示されている楕円曲線については，どの曲線も既知の効率的攻撃法は適用できないことが保証されている。なお、高速処理可能で使用実績があるためSEC2に含まれているKoblitz曲線とよばれる楕円曲線は、限定されたクラスの楕円曲線であるため、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。
- 証明可能安全性を有することは確認されていなかったが、最近、スキームとしてのECDSAがある仮定の下での証明可能安全性を有するという主張がある論文によりなされている。ただし、この主張の妥当性と、証明の方法の現実的効果とについて、本評価では結論を得るに至っていないため、更なる検討が必要である。

(6) MY ELLTY ECMR-160/192/OEF-h 署名

- MY-ELLTY ECMR-160/192/OEF-hは、
  ハッシュ値のサイズが短すぎるため、2^40(または2^48)の計算量により、Birthday Attackによる署名の存在的偽造が可能である
  という点において安全性に問題なしとはいえず、
  長期間有効性を保つことが求められる署名方式としては
  推奨できない。
- なお、提案者の証明可能安全性の論述には誤りがあるため、証明可能安全性を有すると現時点においては認められていない。

(7) EPOC-1

守秘

- EPOC-1は、以下に示す点を除けば、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。この仮定を満たすため適切なパラメータを選択することに注意を払う必要がある。
- 法である合成数の素因数分解の形がRSA方式と異なることなどにより、RSA方式と同じサイズでも安全性は同等とは限らないことに注意を払う必要がある。
- また、証明で十分な安全性を導くためには、パラメータの条件として提案者が示していない条件を追加する必要があるとの指摘がある。
- ただし、この指摘の妥当性について本評価では結論を得るに至っていないため、パラメータ選択条件の明確化について更なる検討が必要である。

(8) EPOC-2

守秘

- EPOC-2は、以下に示す点を除けば、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。この仮定を満たすため適切なパラメータを選択することに注意を払う必要がある。
- 法である合成数の素因数分解の形がRSA方式と異なることなどにより、RSA方式と同じサイズでも安全性は同等とは限らないことに注意を払う必要がある。
- また、証明で十分な安全性を導くためには、パラメータの条件として提案者が示した条件とは異なる条件が必要であり、特に提案者の推奨パラメータでは十分でないとの指摘がある。
- ただし、この指摘の妥当性について本評価では結論を得るに至っていないため、パラメータ選択条件の明確化について更なる検討が必要である。

(9)EPOC-3

守秘

- EPOC-3は、以下に示す点を除けば、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。この仮定を満たすため適切なパラメータを選択することに注意を払う必要がある。
- 法である合成数の素因数分解の形がRSA方式と異なることなどにより、RSA方式と同じサイズでも安全性は同等とは限らないことに注意を払う必要がある。
- また、証明で十分な安全性を導くためには、パラメータの条件として提案者が示した条件とは異なる条件が必要であり、特に提案者の推奨パラメータでは十分でないとの指摘がある。
- さらに、拠り所とするGAP問題という比較的新しい問題の採用が適当であるかまだ見極められていないという指摘もある。
- ただし、これらの指摘の妥当性について本評価では結論を得るに至っていないため、更なる検討が必要である。

(10) HIME-1

守秘

- HIME-1は仕様に曖昧さが存在し、そのままでは第三者が適切に実装することができない。
- 提案者の証明可能安全性の論述には誤りがあるため、証明可能安全性を有すると現時点においては認められていない。
- HIME-1の法である合成数の素因数分解の形がRSA方式と異なるため、RSA方式と同じサイズでも安全性は同等とは限らないことに注意を払う必要がある。特に、パラメータの選択にあたっては、楕円曲線を使用した素因数分解法（ECM）が数体ふるい法（NFS）よりも効率的になる可能性があることに十分注意を払う必要がある。

(11) HIME-2

守秘

- HIME-2は仕様に曖昧さが存在し、そのままでは第三者が適切に実装することができない。
- 提案者の証明可能安全性の論述には誤りがあるため、証明可能安全性を有すると現時点においては認められていない。
- HIME-2の法である合成数の素因数分解の形がRSA方式と異なるため、RSA方式と同じサイズでも安全性は同等とは限らないことに注意を払う必要がある。特に、パラメータの選択にあたっては、楕円曲線を使用した素因数分解法（ECM）が数体ふるい法（NFS）よりも効率的になる可能性があることに十分注意を払う必要がある。

(12) RSA-OAEP　　守秘

- RSA-OAEPは、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。この仮定を満たすため適切なパラメータを選択することが必要である。
- 一般的なOAEP変換は、適応的選択暗号文攻撃に対して強秘匿であるという性質を示すために十分でなかったが、RSA-OAEPについては、適応的選択暗号文攻撃に対して強秘匿であることをある仮定の下で証明できることが確認されている。

(13) ACE Encrypt　　守秘

- ACE Encryptは、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。証明可能安全性を有することの証明が、他の守秘機能をもつ暗号と異なり、補助関数を仮想的なものに置き換えることなく行えることが特徴である。
- パラメータの条件としては、法pのサイズに制限があること:

  $1024 \leqq |p| \leqq 16384$、および、パラメータqのサイズが $|q| = 256$ と固定されていることがあげられる。なお、補助関数として用いられている共通鍵暗号はMARSに限定された仕様となっている。
- 参考情報:本応募暗号の提案者は，同名であるが仕様が本応募とは異なる暗号を暗号技術公募への応募後に発表している。

(14) ECAES in SEC1

守秘

- ECAES in SEC1は、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有する。
- SEC2で具体的に示されている楕円曲線については，どの曲線も既知の効率的攻撃法は適用できないことが保証されている。なお、高速処理可能で使用実績があるためSEC2に含まれているKoblitz曲線とよばれる楕円曲線は、限定されたクラスの楕円曲線であるため、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。

(15) PSEC-1

守秘

- PSEC-1は、プリミティブ暗号化関数の問題で、証明可能安全性は確認されていないないという指摘がある。
- また、証明可能安全性が成り立つためには提案者の示していない条件がパラメータに課せられるという指摘があり、これが正しい場合、1回の暗号処理で安全に扱える平文の長さが著しく制限されることになる。
- ただし、これらの指摘の妥当性について本評価では結論を得るに至っていないため、更なる検討が必要である。

(16) PSEC-2

守秘

- PSEC-2は、以下に示す点を除けば、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有している。しかし、その証明で十分な安全性を導くためには、パラメータの条件として提案者が示した条件とは異なる条件が必要であり、特に提案者の推奨パラメータでは十分でないとの指摘がある。
- ただし、この指摘の妥当性について本評価では結論を得るに至っていないため、パラメータ選択条件の明確化について更なる検討が必要である。

(17) PSEC-3

守秘

- PSEC-3は、以下に示す点を除けば、現時点において安全性の上で特段の問題点は指摘されていない。
- ある仮定の下での証明可能安全性を有している。しかし、その証明で十分な安全性を導くためには、パラメータのサイズを明確に指定しなければならないとの指摘がある。
- また、復号アルゴリズムにある処理を追加しなければならないという指摘がある。
- さらに、拠り所とするGAP問題という比較的新しい問題の採用が適当であるかまだ見極められていないという指摘もある。
- ただし、これらの指摘の妥当性について本評価では結論を得るに至っていないため、更なる検討が必要である。

(18) DH　鍵共有

- Diffie-Hellman方式には、プロトコルに多くのバリエーションが存在するので、個々のプロコトル毎の評価が必要である（参考：実使用されているプロトコルの例：RFC2631, ISO/IS11770-3, Oakley, PGP）。今年度の評価対象は、基本的なスキームのみである。
- 基本的スキームの使用に際しては、現時点において、受動的攻撃（鍵共有のために通信されるデータに攻撃者が影響を与えることがない場合）に対して問題点は指摘されていないが、能動的攻撃（鍵共有のために通信されるデータに攻撃者が影響を与える可能性がある場合）に対して、最低限以下の３点に注意を払う必要がある。
  - A.　公開鍵とエンティティとの結びつきを保証する手段を確保する。
  - B.　（更新を前提とする）セッション鍵の共有方式として使用する場合は、交換する公開鍵は一時的なものとする。
  - C.　共有される鍵が乱数と見分けがつかなくするためには鍵導出関数を使用する。

(19) ECDHS in SEC1　　鍵共有

- ECDHS in SEC1は、現時点において、受動的攻撃に対して問題点は指摘されていないが、能動的攻撃に対して、最低限以下の２点に注意を払う必要がある。
  - A. 公開鍵とエンティティとの結びつきを保証する手段を確保する。
  - B. （更新を前提とする）セッション鍵の共有方式として使用する場合は交換する公開鍵は一時的なものとする。
- SEC2で具体的に示されている楕円曲線については，どの曲線も既知の効率的攻撃法は適用できないことが保証されている。なお、高速処理可能で使用実績があるためSEC2に含まれているKoblitz曲線とよばれる楕円曲線は、限定されたクラスの楕円曲線であるため、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。

(20) ECMQVS in SEC1　　鍵共有

- ECMQVS in SEC1は、現時点において、受動的攻撃に対して問題点は指摘されていないが、能動的攻撃に対して、最低限以下の２点に注意を払う必要がある。
  - A. 公開鍵とエンティティとの結びつきを保証する手段を確保する。
  - B. （更新を前提とする）セッション鍵の共有方式として使用する場合は、交換する公開鍵は一時的なものとする。
- SEC2で具体的に示されている楕円曲線については，どの曲線も既知の効率的攻撃法は適用できないことが保証されている。なお、高速処理可能で使用実績があるためSEC2に含まれているKoblitz曲線とよばれる楕円曲線は、限定されたクラスの楕円曲線であるため、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。

(21)HDEF-ECDH　　鍵共有

- 本提案は、スキームとしては、楕円曲線版DH方式（ECDH）の基本形(各エンティティが同じ楕円曲線を使うスキーム)とその変形版(エンティティ毎に異なる楕円曲線を使うスキーム)とから成り立っているが、

  提案の中心は、ある限定されたクラスの楕円曲線パラメータの生成法を示すことに重点が置かれている。
- ECDHの基本形の評価は、(18)DHの評価に準じる。
- 基本系における基本的なスキームの使用に際しては、現時点において、受動的攻撃に対して問題点は指摘されていないが、能動的攻撃に対して、最低限以下の3点に注意を払う必要がある。
  - A.　公開鍵とエンティティとの結びつきを保証する手段を確保する。
  - B.　（更新を前提とする）セッション鍵の共有方式として使用する場合は、交換する公開鍵は一時的なものとする。
  - C.　共有される鍵が乱数と見分けがつかなくするためには鍵導出関数を使用する。

(21)HDEF-ECDH （つづき） 鍵共有

- また、ECDHの変形版は基本系より安全性が向上するという提案者の主張が妥当であるかどうか、本評価においては結論が得られなかったため、更なる検討が必要である。
- 提案方法で生成された楕円曲線は、既知の効率的攻撃法は適用できないことが保証されているが、限定されたクラスの楕円曲線であるため、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。

おわりに

- 継続的な評価が必要
- 評価に関するコメント
- 皆様の多大なる貢献に感謝
  - 公募に対して提案していただいた応募者の皆様
  - 公開鍵暗号評価小委員会委員・オブザーバーの皆様
  - 匿名の評価委託先である暗号研究者の皆様
  - 暗号技術評価委員会事務局の皆様