証明可能安全性理論に向けて

Introduction to the Theory of Provable Security of Public Key Cryptosystems

太田和夫

Abstract

実用的な暗号技術として，安全が理論的に証明できる（証明可能安全な）方式が期待されている．公開鍵暗号の発明後しばらくの間，『ある攻撃に対して安全な方式は，別の攻撃に対しては安全性証明がつかない』と信じられていた（folklore）．

本稿では，「folklore」のじゅ縛から逃れ，「安全性証明」への道筋を示したGoldwasser，Micali，Rivestによる記念碑的な論文を紹介することで，本小特集の導入とする．安全性定理に込められた「ココロ」，じゅ縛からの解放の「アイデア」などを解説した．

キーワード：公開鍵暗号，証明可能安全性，帰着，Rabin署名方式，Fiat-Shamir変換，ゼロ知識証明

1. はじめに

実用的な暗号技術として，安全性を理論的に証明できる（証明可能安全な）方式が期待されている．1976年に公開鍵暗号[1]が発明された後しばらくの間，音号研究は「作っては破る」という試行錯誤を繰り返した．暗号の設計は，いわば一種の職人芸だった．この経験を踏まえて，1980年代半ばに，暗号研究は「職人芸」から安全性を証明できる「科学」へと整備された．

暗号の安全性は数学の記述を用いて次の定理で表現される．

定理

方式Πを破る攻撃者Aが存在したならば，問題Pを解く効率の良いアルゴリズムを構成できる．すなわち，問題Pが難しいなら，方式Πを破る攻撃者Aは存在しない．

1980年当時，『ある攻撃に対して安全な方式は，別の攻撃に対しては安全性証明がつかない（もしくは，完全解読すら可能）』と信じられていた（folklore）．

本稿では，「folklore（以下，両立不可能性と呼ぶ）」のじゅ縛から逃れ，「安全性証明」への道筋を示したGoldwasser，Micali，Rivestによる論文[2]を紹介することで，本小特集の導入とする．定理に込められた「ココロ」，じゅ縛からの解放の「アイデア」などを解説したい．

太田和夫　正員　電気通信大学電気通信学部情報通信工学科
E-mail　ota@ice.uec.ac.jp
Kazuo OHTA，Member（Faculty of Electro-Communications，University of Electro-Communications，Chofu-shi，182-8585 Japan）．
電子情報通信学会誌　Vol.90 No.6 pp.426-430 2007年6月

2. 安全性の定義

問題Pとして何を採用するかによって，方式Πに対する信頼感が変ってくる．また，方式Πの利用状況はあらかじめ予想できないので，自らにとって有利な「攻撃条件」を許したとして動作する攻撃者Aの存在を否定できるほど，方式Πは信頼できるものとなる．よって「攻撃条件」を定式化することが，「証明可能安全性理論」のスタートとなる．

以下，方式Πとして「ディジタル署名方式」を想定する．「公開鍵暗号方式」については，文献(3)を参照．

署名法の安全性（「攻撃条件」）を議論するために，次の三つの概念を定義する．

① ディジタル署名とは何か？
② 攻撃者が実行可能なシナリオは？
③ 方式を破るときの攻撃のゴールは？

2.1 方式Πのモデル化

ディジタル署名法を以下のようにモデル化する[2]．

定義1（ディジタル署名法のモデル化）

（1） 鍵生成アルゴリズム$\mathcal{K}$，入力kに対して公開鍵と秘密鍵の組(pk,sk)を生成する．ここで，k

は安全性のパラメータ．$\mathcal{K}$は確率的アルゴリズムである．

（2） 署名生成アルゴリズム$\mathcal{S}$は，文書mと(pk,sk)に対して$\sigma=S(\mathrm{pk},\mathrm{sk},m)$で署名$\sigma$を生成する．ここで$\mathcal{S}$は確率的アルゴリズムである．

（3） 署名検証アルゴリズム$\mathcal{V}$は，文書m，署名σと公開鍵pkを入力として，$\mathcal{V}(\mathrm{pk},m,\sigma)$＝合格(accept)か不合格(reject)を出力する．

2.2 攻撃のシナリオ

攻撃をシナリオによって次のように分類する．

（1） 唯鍵攻撃（KOA：Key Only Attack）

公開鍵だけを用いてある文書に対する署名を偽造する攻撃．ある文書の選び方は，攻撃のゴールによって異なる．

（2） 既知文書攻撃（KMA：Known Message Attack）

文書と対応する署名文を用いて，新たに別の文書に対する署名を偽造する攻撃．偽造者は文書と署名の組を複数個入手してよいが，文書は選択できない．

（3） 選択文書攻撃（CMA：Chosen Message Attack）

偽造者が文書(複数個も許す)を選択し，それぞれの文書に対する署名を知り得る状況下で，新たに別の文書に対する署名を偽造する攻撃(注1)．

以降，シナリオを記号ATKを用いて，攻撃法の英語表記の頭文字で表す(ATK ∈ {KOA, KMA, CMA})．

2.3 攻撃のゴール

攻撃のゴール(偽造のレベル)を次のように分類する．

（1） 全面的解読（TB：Total Break）

秘密の署名生成関数($\mathcal{S}$)を計算できる．

（2） 普遍的偽造（UF：Universal Forgery）

秘密の署名生成関数と等価なアルゴリズムを効率的に発見できる．

（3） 選択的偽造（SF ： Selective Forgery）

あらかじめ選んだ文書に対する署名を偽造できる(注2)．

（4） 存在的偽造（EF ： Existentional Forgery）

少なくとも一つの文書の署名を偽造できる．その文書は，偽造者があらかじめ意図して選んだものでなくてもよい(注3)．

以降，ゴールを記号GOALを用いて，偽造レベルの英語表記の頭文字で表す(GOAL ∈ {TB,UF,SF,EF})．

(注1) この攻撃は文書選択の契機によって，一般的(generic)，指向的(directed)，適応的(adaptive)と細分化される．

(注2) 普遍的偽造が任意の文書に対して偽造可能なのに対して，選択的偽造ではあらかじめ選んだ一つの文書あるいは文書の集合に対してのみ偽造可能であればよい．

(注3) この攻撃で署名が偽造される文書は，ランダムで意味のない場合も許される．実用上は大した問題とはならない場合が多い．このような偽造すら存在しないなら，署名法は非常に安全と考えられる．

2.4 安全性の定義

署名法Πの安全性を次のように定義する．

定義2

多項式時間確率的チューリング機械AがGOAL-ATKで署名法Πを破るには，AをシナリオATKで動かしたとき，無視できない確率でゴールGOALに成功すること．このようなAが存在しないとき，署名法はGOAL-ATK-安全を満たすという．

方式Πが最も安全なのは，攻撃者にとって最も有利な攻撃シナリオ（署名法では選択文書攻撃）を許したとしても，最小のゴール（署名法では存在的偽造）すら失敗するときと考えてよかろう．署名法の場合に，ΠがEF-CMA-安全のとき，「署名法Πは安全」という．

暗号研究が「職人芸」だった時代には，設計者があらかじめ気付いた攻撃に対して，個別に安全性を論じるのみであった．これに対して，Goldwasserらは，上記の定義のように，攻撃法をシナリオとゴールの組合せとしてとらえて，それぞれ理想条件を採用することで「安全性概念」を定式化した(これぞ，証明可能理論の「ココロ」！)．

2.5 諸概念の関係

定理の記述を思い出そう．「方式Πの安全性を計算問題Pの難しさに帰着できた」ので，この証明法は「帰着技法」と呼ばれる．

帰着Rにより，GOAL2-ATK2 (＝B)な攻撃者を用いてGOAL1-ATK1 (＝A)な攻撃者を多項式時間で構成できるとき，問題Aは問題Bに多項式時間帰着可能といい，記号「GOAL1-ATK1$\Leftarrow_R$GOAL2-ATK2」で表す．

シナリオの難易，ゴールで達成される攻撃能力に注目すると，図1の「安全性概念の関係」を得る．

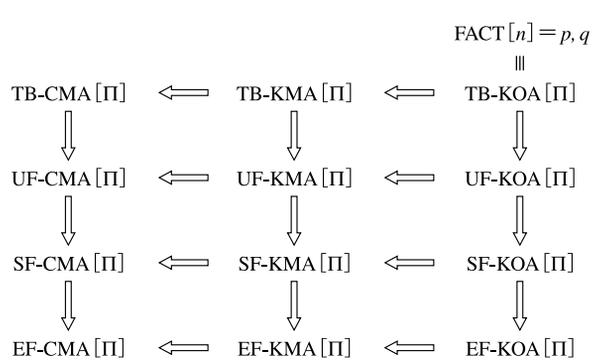

図1 署名の安全性概念の関係 (Rabin署名の場合)　記号$A[\Pi]\Leftarrow_R B[\Pi]$は，方式Πで帰着$R$により$B$な攻撃者を用いて$A$な攻撃者を多項式時間で構成可能を表している．

3. Rabin 署名の両立不可能性

Rabin 署名について，「両立不可能性(folklore)」を証明できる[4),(5)]．この例によって両立不可能性が信じられるようになった[注4]．

主張[両立不可能性]
次の二つの条件を同時に満たす FACT に安全性の根拠をおく署名法は存在しない．

① 署名法に対して偽造のゴール(UF，SF，EF のいずれでもよい)を実現する偽造アルゴリズム A を用いて，素因数分解アルゴリズムを構成できる．
② 署名法は CMA に対して安全である．

3.1 Rabin 署名の両立不可能性

Rabin 法は，RSA 法と同様，素因数分解問題(FACT)の計算困難性を利用した公開鍵方式である．合成数 n に対する $x^2 \bmod n$ が与えられたとき，平方根の計算が n の素因数分解に等価なことを利用すると，FACT $[n] \Leftarrow_R$SF-KMA を証明できる（FACT $[n] \Rightarrow$SF-KMA は明らか)．

ところが，この R は定理 3 で示すように，CMA シナリオでのゴール TB 攻撃を与える．Rabin 署名では，SF-KMA- 安全の証明が TB-CMA 攻撃を与えてしまうのだ．

3.2 両立不可能性の証明

Rabin 署名について「両立不可能性」の議論を精密にしよう．下記の議論は，実は一般に「単一鍵素因数分解に基づく署名法」などに拡張できる．しかし，一方で，ほかの「すべての署名法」に適用できるとは限らないことに注意しなければならない．

定理 3
FACT $[n] \Leftarrow_R$ GOAL-KOA $[\Pi]$ なら多項式時間 TB-CMA 攻撃者を構成できる．ただし GOAL は TB を除く．

証明：
多項式時間帰着 R が FACT $[n] \Leftarrow$GOAL-KOA $[\Pi]$ を証明するので，R に対して GOAL-KOA 攻撃者をシミュレートできれば，R は FACT $[n]$ (= n の素因数)を出力する．

CMA シナリオで動作する攻撃者 M を次のように構成する[注5]．CMA シナリオで利用が許されている真の署名者 $\mathcal{S}$ を用いて R が A に期待する動作をシミュレートして，R を走らせる．その結果，R が公開鍵 n の素因数を出力するので，M はその値を M の出力とする．

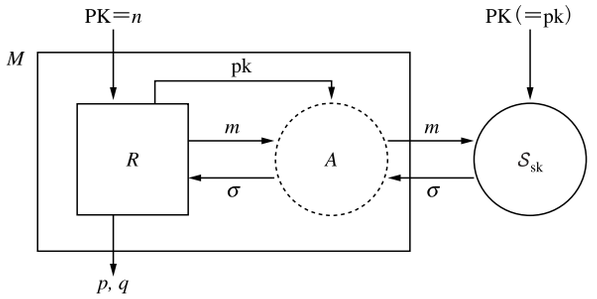

図 2 メタ帰着 M の構成（US の場合）

M は $\mathcal{S}$ を用いて多項式時間で A をシミュレートでき，かつ R は多項式時間で n の素因数を出力するので，M は多項式時間 TB-CMA 攻撃者となる． ■

帰着アルゴリズム族に若干の性質(KPBB 性[注6])を仮定すると，次の定理を証明できる．

定理 4
FACT $[n] \Leftarrow_{R^*}$ GOAL-CMA $[\Pi]$ なら，FACT 問題は多項式時間で解ける．

証明：
FACT $[n] \Leftarrow_{R^*}$ GOAL-CMA $[\Pi] \Leftarrow$ GOAL-KOA $[\Pi]$ が多項式時間帰着 R となる[注7]．2 番目の矢印は図 1 による．定理 3 より，多項式時間 TB-CMA な A を構成できる．

再び図 1 により，A から GOAL-CMA 攻撃者 A' も構成できるので，$R^{*A'}$ は多項式時間でFACT問題を解く．

系 5
FACT 問題が難しいなら，KPBB 性を満たす帰着のみで署名法 Π の GOAL-CMA-安全は証明できない[注8]．

定理 3 で GOAL が EF のときには，M は TB-KMA 攻撃者とできるので，同様の議論で次の系を証明できる．

系 6
FACT 問題が難しいなら，KPBB 性を満たす帰着のみで署名法 Π の EF-KMA-安全は証明できない．

3.3 Rabin 署名の安全性のまとめ

以上の議論によって，Rabin 署名の安全性は，SF-KMA-安全が示せて(3.1 の結果)，TB-CMA-安全と EF-KMA-安全は証明不可能なことが証明できた(系

(注 4) Rivest はそのように誤解したと文献(2)で明記している．
(注 5) 帰着 R を利用した新たな帰着なので，M をメタ帰着と呼ぶ．
(注 6) Paillier らは，Key-Preserving Black Box Reduction という性質を仮定している[6]．帰着の KPBB 性は推移的である．
(注 7) ここで KPBB 帰着の推移性を用いた．
(注 8) 否定的な結論を得るには，帰着 R の存在は不要であることに注意．

5,6)．更に定理3によりTB-CMA攻撃者を構成できる．

4. 証明可能安全に向けて

いよいよ本題に入ろう．Micali らは文献(2)で，どのようにして両立不可能性を破ったか？

4.1 両立不可能性回避のアイデア

答えは，定理3の証明に隠されている．メタ帰着 M の構成に成功したのは，入力 n を方式 Π の公開鍵として設定できたため，CMA シナリオでの署名者 $\mathcal{S}$ からの出力を R に中継するだけで，攻撃者 A をシミュレートできたことによる（図2）．S への入力公開鍵を PK で表すと，pk＝PK が常に成立することに注意しよう．

ここで，方式 Π の公開鍵の一部に，第二の成分を追加するとどうだろう？

定理3と同様の証明を試みる．メタ帰着 M と S に公開鍵 PK $=(N,T)$ が渡される．このとき R への入力は合成数だけなので，M は PK から N を取り出して R に入力する．R は pk$=(n,t)$（t は R が設定する）を A に渡す．このとき，$N=n$ となっている．

定理3の証明で，R は入力 N に対してその素因数を出力するのであった．証明が有効であるには，$T=t$ が成り立つ必要があるが，帰着 R には T が入力されないので，この条件は成り立たない．

このように公開鍵に新たな成分を含めることによって，TB-CMA 攻撃者は構成できず，その結果，定理4，系5が成り立たなくなり，GOAL-CMA-安全の証明がつく可能性が残っている．

4.2 もう一つの課題——$\mathcal{S}$のシミュレーション——

UF-CMA-安全性を証明するには，A が CMA シナリオで動くので，R は A からの署名依頼 m' に対して署名 σ' を答えなければならない(注9)．そのため，R は A への入力 pk を選べる優位性を有効に使うこととする．

pk の設定法は，例えば次のアプローチで成功している．

方法1

ランダムオラクルの利用[7),8)]

方法2

2平面の利用（平面1で乱数を介して文書と署名の対応を保証，平面2で乱数列の妥当性を保証）[9)]

方法3

普遍的一方向性ハッシュ関数の利用[10)]

方法4

制約の強い数論的仮定の利用[11)]

(注9) 有利な攻撃条件を A に許すほど，帰着 R の構成は難しくなることに注意．

などが挙げられる．

ここでは，方法1について紹介する．

5. ランダムオラクル（ZKIP の利用）

任意長の文書に署名を生成するには，文書にハッシュ関数 H を適用することで，あらかじめ定められたビット長に変換した後に RSA 関数などの落し戸付き関数を適用するものが実用的である（「Hash then Sign 法」[7)]）．

5.1 ランダムオラクルモデル（ROM）

$H(m)=H(m')$ を満たす m と m' が簡単に求まると，m に対して生成された署名 σ が m' の署名にもなり，文書のすり替えが可能となる．そこで，ハッシュ関数を理想的なものとしてモデル化したのが，ランダムオラクルモデル（ROM）である[7)]．攻撃者も含めてすべての要素がオラクルとして H を利用でき，H は初出の入力 x には $H(x)$ として乱数値を出力するものとする(注10)．

5.2 ZKIP と Fiat-Shamir 変換

ゼロ知識証明（ZKIP）性が保証されたプロトコル（証明者が X をコミット後に，検証者がチャレンジ c を質問し，証明者が Y を答えることで，公開鍵 I に対する秘密 s を保持することを示す手順[12),13)]）が与えられたとき，署名者が $c=H(X,m)$ でチャレンジを生成して，文書 m に対する署名を $\sigma=(X,c,Y)$ とすると「安全な署名」を構成できる（Fiat-Shamir 変換[8)]）．

帰着 R の構成法：証明の概要は以下のとおり．

人力 I のとき，R は pk$=(I,\boxed{H'})$ とおいて，攻撃者 A を呼び出す．$\boxed{H'}$ については後述する．文書 m に対する偽造署名 σ を A から入手できれば，ZKIP の健全性によって，R は I に対応した秘密 s を出力できる．

CMA シナリオで A に偽造署名を出力させるために，R は ZKIP のゼロ知識性のシミュレータを用いて，A からの署名依頼 m' に対して，まず $c'=:\boxed{H'}(X',m')$ で $\boxed{H'}$ を定め，次に署名 σ' を回答する（pk$=(I,\boxed{H'})$）．このとき，$\boxed{H'}$ は，R が c' を与えたので R の配下にあり，$\mathcal{S}$ は，$\boxed{H'}$ にアクセスできないことに注意しよう．

c' は乱数値なので，初出の (X',m') に対する関数値として c' を採用しても，A は $\boxed{H}$ から $\boxed{H'}$ への置き換えを検出できず，m に対する偽造 σ を出力する．

(注10) この性質を満たすランダムオラクル H はプログラムでは表現できない．標準モデルでは関数 H をプログラムとして指定する必要があるが，ここで扱いたいランダムオラクル H はプログラムでは表現できないので，記号 $\boxed{H}$ で記すことにした．

5.3 両立不可能性回避の確認

最後に，定理3が動作しないことを確認しておこう．

署名オラクル$\mathcal{S}$にはPK＝$(I, \boxed{H})$が入力され，PKに対応するSKを用いて動作する．一方，Rは公開鍵pk＝$(I, \boxed{H'})$をAに入力して動作する．一般にPK≠pkなので，メタ帰着Mは，PKで動作する$\mathcal{S}$からの回答をRに渡すことはできない．よって，RはAを利用でき，メタ帰着Mは$\mathcal{S}$を利用できない(注11)．

5.4 ROMと標準モデル

Fiat-Shamir署名は，平方剰余問題を証明するZKIP[12]に，Fiat-Shamir変換のアイデアを適用した署名法であり，単一鍵素因数分解に基づく署名法の一つになっている．

ところで，標準モデル（ハッシュ関数をプログラムとして有限ビット長で具体的に与える）では，「単一鍵素因数分解に基づく署名法」については，帰着に一定の制限が付いているものの，系5でEF-CMA-安全は証明できないことが証明されている．よって，Fiat-Shamir署名は，この帰着の制限のもとで，ROMでは安全性が保証できるが，標準モデルでは保証することが不可能な方式の具体例となっている．

なお，帰着に制限を仮定せずとも，「ROMで安全なことを証明できるが，標準モデルで攻撃可能な方式が存在する」ことが示されている[14],[15]．

6. おわりに

公開鍵暗号の証明可能安全性研究の記念碑的な論文[2]を，安全性証明の両立不可能性の回避方法に注目して解説した．

ROMの別のアプローチ（例えばRSA-FDH署名[7]など）は，本小特集4.の駒野氏の記事に譲りたい．また，4.2で挙げたほかの方法についても触れたかったが，誌面が尽きてしまった．別の機会に解説したい．

(注11) Rが$\mathcal{S}$を利用可能と仮定すると，定理4と同様の結果が成り立つことを証明できる．

文　献

(1) W. Diffe and M.E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol.22, no.6, pp.644-654, 1976.

(2) S. Goldwasser, S. Micali, and R. Rivest, “A “paradoxical” solution to the signature problem,” 25th Annual Symposium on the Foundations of Computer Science, pp.441-448, 1984.

(3) M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, “Relations among notions of security for Public-key encryption schemes,” Lect. Notes Comput. Sci., vol.1462, pp.26-45, 1998.

(4) M.O. Rabin, Digital signatures and public-key functions as intractable as factorization, Technical Report LCS/TR-212, MIT Laboratory for Computer Science Technical Report, 1979.

(5) H. Williams, “A modification of the RSA public-key encryption procedure (corresp.),” IEEE Trans. Inf. Theory, vol.26, Issue 6, pp.726-729, 1980.

(6) P. Pailler and J.L. Villar, “Trading one-way against chosen-ciphertext security in factoring-based en-cryption,” Lect. Notes Comput. Sci., vol.4284, pp.252-266, 2006.

(7) 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, 1993.

(8) A. Fiat and A. Shamir, “How to prove yourself,” Lect. Notes Comput. Sci., vol.263, pp.186-208, 1986.

(9) S. Goldwasser, S. Micali, and R. Rivest, “A digital signature scheme against adaptive chosen message attack,” SIAM J. Comput., vol.17, no.2, pp.281-308, 1988.

(10) M. Naor and M. Yung, “Universal one-way hash functions and their cryptographic applications,” 21th Annual ACM Symposium on Theory of Computing (STOC), pp.33-43. 1989.

(11) R. Gennaro, S. Halevi, and T. Rabin. “Secure hash-and-sign signatures without the random oracle,” Lect. Notes Comput. Sci., vol.1592, pp.123-139, 1999.

(12) S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems (extended abstract),” Seventeenth Annual ACM Symposium on Theory of Computing (STOC), pp.291-304, 1985.

(13) 暗号・ゼロ知識証明・数論，岡本龍明，太田和夫(編)，共立出版，1995.

(14) R. Canetti, O. Goldreich, and S. Halevi, “The random oracle methodology, revisited,” 30th Annual ACM Symposium on Theory of Computing (STOC), pp.209-218, 1998.

(15) U. Maurer, R. Renner, and C. Holenstein, “Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology,” Lect. Notes Comput. Sci., vol.2951, pp.21-39, 2004.

（平成19年1月16日受付　平成19年3月6日最終受付）

太田　和夫（正員）

昭52早大・理工・数学卒．昭54同大学院修士課程了．同年日本電信電話公社(現NTT)入社．平13より電通大・教授．暗号・認証の理論研究に従事．理博．平4年度本会業績賞，小林記念特別賞，平10電気通信普及財団(テレコムシステム技術賞)各受賞．