安全性を証明可能な機能付き電子署名方式

Provably Secure Digital Signature Scheme with Additional Functionality

駒野　雄一　■ KOMANO Yuichi
新保　淳　■ SHIMBO Atsushi
岡田　光司　■ OKADA Koji
太田　和夫　■ OHTA Kazuo

証明可能安全性は，情報セキュリティの基盤技術である暗号方式やデジタル署名方式の安全性を保証する指標である。証明可能安全性により，誰もが方式の安全性を納得することができるようになり，標準方式の選定基準の一つともされている。ある方式が証明可能安全であることを示すには，安全性モデル（攻撃環境と安全性要求）を定式化し，方式がそのモデルを満たすことを証明する。安全性モデルは，方式（機能）ごとに適切に定式化されなければならない。

東芝と国立大学法人 電気通信大学（以下，電気通信大学と略記）は共同研究により，機能付き電子署名方式の一つである多重署名方式の安全性モデルを定式化し，落とし戸付き一方向性置換を用いる証明可能安全な多重署名方式を開発した。この方式は，署名対象文書を多重署名の初期値に埋め込むことで，署名対象文書が一定サイズよりも大きいときに，落とし戸付き一方向性置換に緊密な安全性を持つ公知技術の中でもっとも総通信量を小さくすることができる。

Provable security is an index that ensures the security of fundamental cryptographic primitives such as public key encryption and digital signature schemes. It not only allows everyone concerned to confirm the security of the primitives, but also provides a criterion for establishing the relevant standard. In order to prove the security of a scheme, the scheme is first provided with a security model (attack scenario and security goal) and then it is shown that the scheme satisfies the model. However, the model needs to be formalized for each primitive (functionality).

Toshiba and the University of Electro-Communications have proposed a digital signature scheme with additional functionality that can achieve the shortest bandwidth among multisignature schemes having a trapdoor one-way permutation and security equivalent to that of the proposed scheme, by embedding the message (with practical length) to be signed into an initial multisignature.

1　まえがき

公開鍵暗号方式やデジタル署名方式は，情報セキュリティ分野における基盤技術として，様々な場面で利用されている。従来は，これら基盤技術の設計は経験的に行われており，提案と解読が繰り返されていた。

基盤技術の安全性を保証する理論として，証明可能安全性の概念が確立されつつある。ある方式が証明可能安全であるとは，その方式が適切に定式化された安全性を満たすことを数学的に証明できることを言う。証明可能安全性の概念により，定式化されたモデルに限定されるが，誰もが方式の安全性を納得することができ，標準暗号選定の評価項目の一つとしても利用されている。

証明可能安全性の議論は，安全な方式の設計にも活用できる。例えば，安全性証明が破綻（はたん）する要因を特定して設計にフィードバックすることで，証明可能安全な方式を構成したり，安全性証明で得られる定量的な評価値からパラメータの推奨値を設計したりすることが可能である。

ここでは，デジタル署名方式を用いて証明可能安全性について述べる。次に，付加機能を持つデジタル署名方式として，署名サイズを抑えたまま複数の署名者の承認を保証する多重署名方式について，安全性モデルを構築する。更に，東芝と電気通信大学が共同開発した落とし戸付き一方向性置換(注1)を用いる多重署名方式について述べる。

2　証明可能安全性

この章では，デジタル署名方式を例に，証明可能安全性について述べる。

2.1　デジタル署名方式の安全性

デジタル署名方式とは，紙社会における印鑑やサインを電子的に実現したものであり，“誰”が“何”を承認したかを，すなわち署名者と文書の真正性を保証する技術である。デジタル署名方式の証明可能安全性は，①安全性モデル（攻撃環境と安全性要求），②帰着元の問題，③証明モデル，④帰着効率により規定される。

①の安全性モデルは，デジタル署名方式に対する攻撃者の目標と攻撃環境で定まる項目である。例えば，攻撃者がシス

（注1）　落とし戸付き一方向性置換は，公開情報を用いる関数演算は容易であるが，秘密情報なしで逆関数演算を行うことが困難となる1対1関数のこと。RSA関数[1]は，落とし戸付き一方向性置換であると信じられている。

テム上の欠陥を利用して任意の文書に対応する署名を入手することができたとしても（攻撃環境），新たな文書と署名の組を偽造すること（攻撃者の目標）が難しい，などのモデルが定式化される。

②の帰着元の問題は，デジタル署名方式の安全性証明における帰着元の問題のことであり，素因数分解問題やハッシュ関数の衝突探索問題など，数学的に困難と広く信じられている問題が用いられる。

③の証明モデルは，帰着を構成するときの仮定を示す項目である。理想的なランダム オラクル（関数）を仮定するランダム オラクルモデルや，特殊なオラクルは仮定しない標準モデルなどがある。

④の帰着効率は，帰着元と帰着先の問題の困難さの乖離（かいり）の大きさを表し，乖離が小さい（帰着効率が良い）ときに，デジタル署名は帰着元の問題に対して緊密な安全性を持つという。

デジタル署名方式の設計者の目的は，“③の現実的なモデルで，②のできるだけ困難な問題に対して，④の緊密な安全性を持つ，①の十分な安全性を実現”し，“効率的に実装可能”な方式を構成することである。ただし，すべての要件を満たすデジタル署名方式を構成することは容易ではなく，安全性証明も複雑になる。

2.2　証明可能安全性と方式設計

方式の安全性は，一般的に②の帰着元の問題が方式を解読する問題に帰着することを示すことで証明される（**図1**）。ここで，問題Aが問題Bに帰着するとは，問題Bの解法を使えば問題Aを解くことができることを言う。

証明可能安全性の議論により，定式化された範囲に限られるが，誰もが方式の安全性を納得することができる。近年では，暗号やデジタル署名の標準方式の選定において，方式の安全性の帰着元の問題の困難さや帰着効率の良しあしが選定基準として考慮されるなど，証明可能安全性の議論は必要不可欠なものとなりつつある。

一方，証明可能安全性の議論を方式設計にフィードバックすることも可能である。具体的には，帰着の構成に失敗する原因を特定して証明可能安全な方式へと改良を図ったり，帰着に冗長な部分を排除することで，方式の効率改善を行ったりすることが可能となる。

また，②の帰着元の問題の困難性と④の帰着効率は，方式のパラメータ設計に影響を与える。例えば，方式の解読の困難さが問題A_1と等価な方式S_1及び，方式の解読の困難さが問題A_2と等価な方式S_2が存在すると仮定する。このとき，問題A_1が問題A_2よりも困難である場合には，問題A_1のサイズは問題A_2のサイズよりも小さくてよいため，方式S_1のパラメータを小さくとる（署名サイズを抑える）ことができる。同様に，同一の問題Bに対して，帰着効率が良い方式S_3と帰着効率がよくない方式S_4が存在する場合には，方式S_3は方式S_4よりもパラメータを小さくとることができる。

2.3　付加機能を持つデジタル署名方式

近年，応用に対応した付加機能を持つデジタル署名方式が提案されている。例えば，署名者の匿名性を保証したままグループの属性だけを証明するグループ署名方式や，署名サイズを抑えたまま複数の署名者の承認を保証する多重署名方式が提案され，購買者のプライバシー保護を実現する電子決済システム[(2)]や文書回覧システムなどに利用されている。

付加機能を持つデジタル署名方式の安全性も，2.1節の①～④により規定される。しかし，付加される機能により攻撃者が入手しうる情報や攻撃者の目標が異なるため，①の安全性モデルは機能ごとに定式化する必要がある。

例えば，グループ署名方式では偽造が困難であるという性質に加えて，署名者の匿名性などが必要とされる。そのため，署名の偽造や署名者の特定（暴露）など，攻撃者の複数の目標それぞれについて安全性を保証しなければならない。更に，実社会の攻撃者は，目標を達成するためにグループメンバーの一部と結託する（メンバーの秘密鍵を入手する）ことも可能であり，攻撃環境も適切にモデル化しなければならない[(3)]。

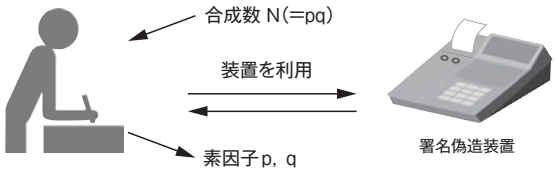

図1. 帰着を用いた安全性証明 — 安全性を証明するには，デジタル署名を偽造する装置を用いて素因数分解問題を解くアルゴリズムを構成する。対偶をとると，素因数分解問題が計算困難なら，デジタル署名の偽造が困難であることを保証できる。

Security proof with reduction

3　証明可能安全な多重署名方式

ここでは多重署名方式の概念を紹介し，多重署名方式の安全性モデルの構成と具体的な方式について述べる。

3.1　多重署名方式

多重署名方式とは，署名サイズを抑えたまま複数の署名者の承認を保証する技術であり，連判状を電子的に実現したものである（**図2**）。多重署名方式は，次の三つのアルゴリズムを利用して，稟議（りんぎ）的に署名生成が行われる。

(1)　鍵生成　　安全性のパラメータを入力として，各署名者の公開鍵（pk_i）と秘密鍵（sk_i）を生成する。iは署名者を表すインデックスで，簡略化のため，署名生成の参加順番と同一視する。pk_iは公開鍵登録簿に登録され，sk_iは

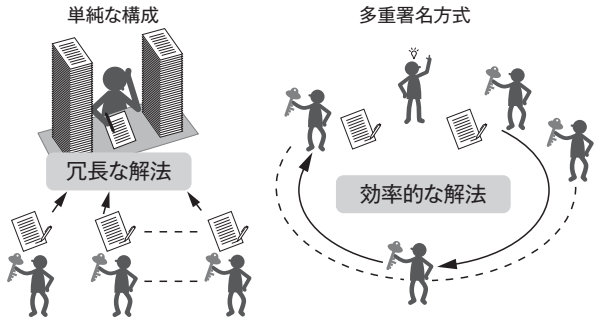

図2. 多重署名の概念 — 多重署名により，通常のデジタル署名を連結する単純な構成よりも署名サイズを削減し，署名の管理も容易になる。

Concept of multisignatures

署名者が秘密裏に保持する。

(2) 署名生成　　インデックスi（$i \in \{1, 2, ..., L\}$）を持つ署名者（以下，第iユーザーと呼ぶ）は，署名対象文書（M），第i-1ユーザーが出力する署名（σ_{i-1}，ただしσ_0は公開情報），及び第iユーザーのsk_iを入力として，署名（σ_i）を出力する。

(3) 署名検証　　M，署名（σ_L），署名生成を行ったL人の署名者の公開鍵$\{pk_j\}_{j=1}^{L}$を入力として，σ_LがMと$\{pk_j\}_{j=1}^{L}$に対応する多重署名であるか否かを判定する。

3.2 多重署名方式の安全性モデル

一般的に，攻撃者にもっとも有利な環境で動作したとしても，もっとも小さな被害を与えることすらできないことが，もっとも高いレベルの安全性としてモデル化される。

以降では，多重署名方式の安全性モデル[4]について述べる。まず，攻撃環境を考える。実際のシステムでは，攻撃者はシステムの欠陥を利用して攻撃のヒントとなる情報を収集する。証明可能安全性の理論では，システムの欠陥は入力（要求）に対して絶対的な回答を行うオラクルによりモデル化される。攻撃者にもっとも有利な環境は，システムに介在すると思われる欠陥のそれぞれに対応するオラクルを自由に利用できることである（ただし，各オラクルの利用回数は安全性のパラメータに対して多項式回とする）。多重署名方式に対して，攻撃者にもっとも有利な攻撃環境を**図3**に示す。

次に，多重署名方式の攻撃者の目標を考える。多重署名方式の目的は，署名サイズを抑えたまま複数の署名者の承認を保証することである。したがって，多重署名方式に求められる安全性要件は，署名生成処理に参加していない署名者の承認情報を含む多重署名は偽造できないことである。このとき，攻撃者の目標（多重署名方式の最小の被害）は，攻撃者が選んだ文書について，署名生成処理に参加していない署名者の承認情報を含む多重署名が偽造されることである。ここで，文書は，運用上は被害をもたらさない無意味な文字列でもよいことに注意する。このような攻撃を存在的偽造と呼ぶ。

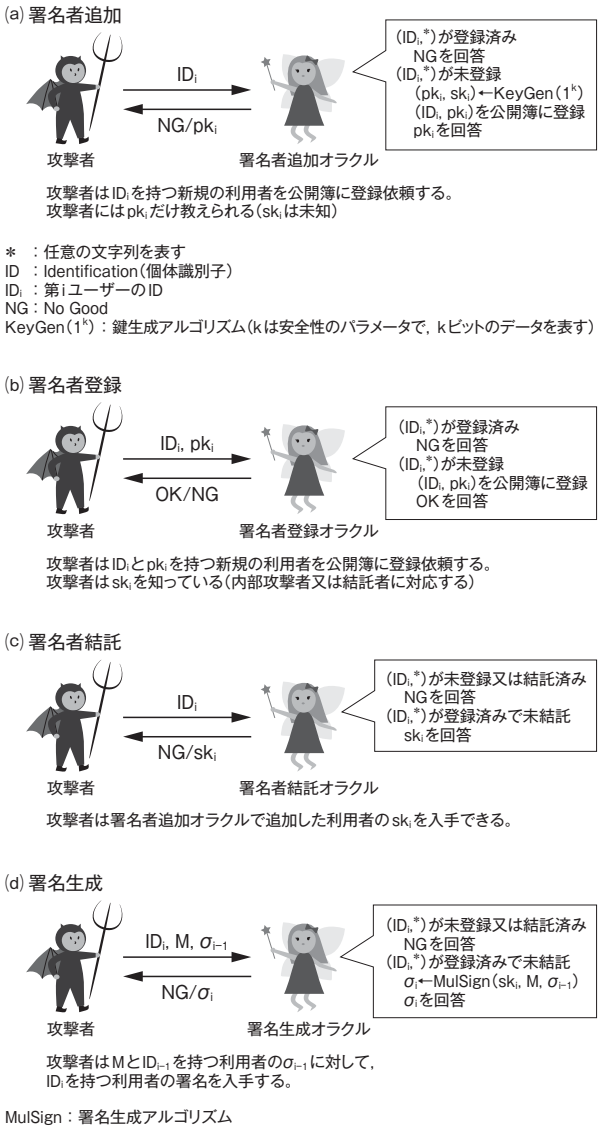

図3. 多重署名方式への攻撃環境 — 攻撃者はこれら四つのオラクルを利用して，攻撃に必要な情報を収集する。このような攻撃を，適応的選択文書攻撃及び適応的内部攻撃と呼ぶ。

Attack scenario against multisignatures

すなわち，多重署名方式の設計者の目標は，図3に示す適応的選択文書攻撃及び適応的内部攻撃に対して存在的偽造が困難[4]で，効率的な方式を構成することである。

3.3 証明可能安全な多重署名方式

当社は電気通信大学との共同研究により，文書復元型の署名方式 PSS-R[5]（Probabilistic Signature Scheme with message Recovery）の概念を利用し，**表1**の安全性を満たす確率的多重署名方式 S-PSS-MSS（Short PSS-based MultiSignature Scheme）を提案した[6]。提案方式の処理フローチャートを**図4**に示す。

ここで，方式が確率的であるとは，安全性を向上させるために，署名生成処理内部で発生させた乱数列を利用して署名を

表1. S-PSS-MSS[6]が満たす安全性

Security level of proposed scheme (S-PSS-MSS[6])

項　目	証明可能安全性
① 安全性モデル	適応的選択文書攻撃及び適応的内部攻撃に対して存在的偽造が困難[4]
② 帰着元の問題	落とし戸付き一方向性置換の一方向性
③ 証明モデル	ランダム オラクルモデル
④ 帰着効率	帰着元の問題に緊密な安全性

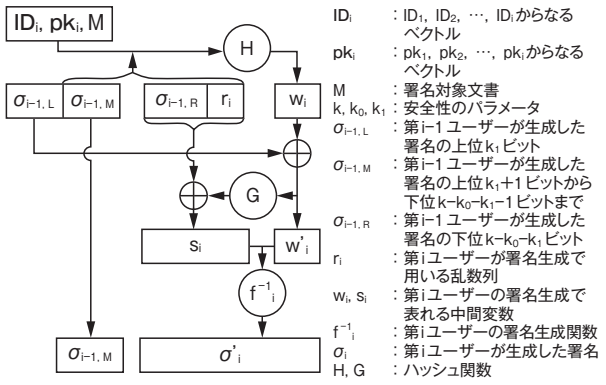

図4. S-PSS-MSS[6]の処理手順 — $\mathbf{ID}_{i-1}$, $\mathbf{pk}_{i-1}$, M, σ_{i-1}を入力として受け付けたら，$\mathbf{ID}_i=\mathbf{ID}_{i-1}||\mathrm{ID}_i$, $\mathbf{pk}_i=\mathbf{pk}_{i-1}||\mathrm{pk}_i$と情報を付加し，$\sigma_{i-1}=\sigma_{i-1,L}||\sigma_{i-1,M}||\sigma_{i-1,R}$と第i−1ユーザーの署名を分割して，乱数列$r_i$とともに上図の手順で多重署名$\sigma_i=\sigma_{i-1,M}||\sigma'_i$を計算する。S-PSS-MSSは，$\sigma_{0,R}$に署名対象文書を埋め込むことで，総通信量を削減することが可能である。太字はベクトルを表す。

Proposed scheme (S-PSS-MSS[6])

生成することをいう。多重署名の検証時には，署名生成で用いた乱数を入手あるいは復元しなければならない。乱数列のビット長をk_0とするとき，通信量（署名対象文書，署名，その他の付加情報の総ビット長）は署名者一人当たり最低でもk_0ビット大きくなることに注意する必要がある。

S-PSS-MSSは，署名者一人当たりの通信量がk_0ビットだけ大きくなる方式である。すなわち，表1の安全性を持つ方式としては，通信量の増加を最小限に抑えた方式である。更に，Mをσ_0の一部に埋め込むことで，Mが一定サイズよりも大きいときに，落とし戸付き一方向性置換に緊密な安全性を持つ公知技術の中でもっとも総通信量を小さくすることが可能である。

また，S-PSS-MSSは，署名者ごとに異なるMを選択できる文書可変性，署名者の署名順序を自由に設定できる署名順序可変性，及び署名者の署名順序を後に検証できる署名順序検証可能性を満たしている。

4　あとがき

ここでは，情報セキュリティ基盤技術の安全性を保証する概念として確立されつつある証明可能安全性について，デジタル署名方式を例に述べた。

証明可能安全性の基となる安全性モデルは，対象（機能）ごとに適切に定式化される必要がある。ここでは，多重署名方式の安全性モデルの定式化を説明し，落とし戸付き一方向性置換を用いる方式を述べた。

多重署名方式は，文書回覧システムや電子メールソフトウェアなど，複数の機関や個人による承認と権利主張が必要な場面で用いられる。

文　献

(1) Rivest, R. L., et al. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. **21**, 2, 1978, p.120－126.
(2) 加藤岳久，ほか. 匿名認証技術とその応用. 東芝レビュー. **60**, 6, 2005, p.23－27.
(3) Bellare, M., et al. "Foundations of Group Signatures: The Case of Dynamic Groups". CT-RSA 2005, LNCS 3376. Alfred Menezes. Springer, 2005, p.136－153.
(4) Komano, Y., et al. "Formal Security Model of Multisignatures". ISC 2006, LNCS4176. Sokratis K. Katsikas, et al. Springer, 2006, p.146－160.
(5) Bellare, M., et al. "The Exact Security of Digital Signatures - How to Sign with RSA and Rabin". EUROCRYPT 1996, LNCS 1070. Ueli M. Maurer. Springer, 1996, p.399－416.
(6) Komano, Y., et al. "On the Security of Probabilistic Multisignature Schemes and Their Optimality". Mycrypt 2005, LNCS 3715. Ed Dawson, Serge Vaudenay. Springer, 2005, p.132－150.

駒野　雄一　KOMANO Yuichi
研究開発センター　コンピュータ・ネットワークラボラトリー。暗号技術及び暗号応用システムの研究・開発に従事。国際暗号学会（IACR），電子情報通信学会会員。
Computer & Network Systems Lab.

新保　　淳　SHIMBO Atsushi
研究開発センター　コンピュータ・ネットワークラボラトリー主任研究員。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.

岡田　光司　OKADA Koji, D.Eng.
東芝ソリューション（株）IT技術研究所 研究開発担当主務，工博。情報セキュリティ技術の基礎研究及び応用開発に従事。国際暗号学会（IACR），電子情報通信学会会員。
Toshiba Solutions Corp.

太田　和夫　OHTA Kazuo, D.Sc.
国立大学法人 電気通信大学 情報通信工学科教授，理博。情報セキュリティ及び暗号理論の研究に従事。国際暗号学会（IACR），電子情報通信学会会員。
The University of Electro-Communications