メカニズムベースPKI——指紋からの秘密鍵動的生成

柴田陽一[†1] 三村昌弘[†2] 高橋健太[†2]
中村逸一[†3] 曽我正和[†4] 西垣正勝[†1]

公開鍵基盤（PKI）における秘密鍵は通常，ユーザが所有しているデバイスに保存されることになる．よって，デバイスの耐タンパ性の確保や盗難・紛失などに対して注意を払わなければならない．そこで本論文では，秘密鍵そのものではなく，秘密鍵を生成するメカニズムのみをデバイスに実装する「メカニズムベース PKI」を提案する．本方式では，ユーザが文章に署名を付す瞬間に，ユーザがデバイスに秘密鍵の種を入力することにより，デバイス内で秘密鍵を生成する．普段はデバイス内に秘密鍵は存在せず，デバイスの盗難・紛失の際にも問題はない．秘密鍵の種には様々な候補が考えられるが，ここでは一例として指紋を使用する方法について示す．しかし，指紋はアナログデータであり，指紋からつねに一意の秘密鍵をリアルタイムで生成することは困難であった．本論文では統計学的なアプローチによりこの問題を解決する「統計的 AD 変換」についてもあわせて提案する．基礎実験の結果，統計的 AD 変換によって指紋からつねに一意なユニークコードをリアルタイムで抽出可能であることが確かめられた．

Mechanism-based PKI—A Real-time Key Generation from Fingerprints

Yoichi Shibata,[†1] Masahiro Mimura,[†2] Kenta Takahashi,[†2]
Itsukazu Nakamura,[†3] Masakazu Soga[†4]
and Masakatsu Nishigaki[†1]

This paper proposes a “mechanism-based PKI”, in which only a mechanism for generating user’s private keys is installed on a smart card. The private key is generated inside the smart card at the event that the legitimate user gives a “seed of private key” to his/her smart card in order to sign a document. The key exists nowhere except while users are signing a document. Thus, users no longer need to pay considerable attention to their smart cards. In addition, this paper also proposes a “statistical A/D conversion”, which is an effective scheme to convert fingerprint to just one and the same ID in real-time. The statistical A/D conversion enables us to use fingerprint as a seed of private key. We construct an example system for real-time key generation form fingerprint. From some basic experiments that we carried out, the availability of the system is confirmed.

1. はじめに

IT 技術の進歩により電子商取引も本格化の兆しが見えており，実際に携帯端末からの電子バンキングなどのサービスも開始されている[1)]．特に携帯電話の普及が著しい現代においては，携帯電話を使っての様々な電子商取引サービスはビジネス界においても非常にホットな題材となっている[2)]．

対面での相互確認が不可能な電子商取引においては，公開鍵基盤（PKI）に基づくディジタル署名により契約文書などの正当性を証明することになり，すでに日本でも政府の「e-Japan 構想」[3)] に従い，法的整備も進んでいる．ここで，ディジタル署名の際に用いられる秘密鍵は，たとえば RSA 方式においては 1024 ビット以上が推奨されており，また，適当な時間間隔で更新されるという仕様になっている．よって，人間が秘密鍵を暗記することは不可能であり，秘密鍵はユーザのデバイスなどに何らかの形で蓄えられることになる．

しかしこれは，ユーザの認証が「ユーザが本人であるか否か」ではなく，「秘密鍵が格納されているデバイスを所持しているか否か」によって行われていること

†1 静岡大学情報学部
Faculty of Information, Shizuoka University
†2 株式会社日立製作所システム開発研究所
System Development Laboratories, Hitachi, Ltd.
†3 株式会社 NTT データビジネス開発事業本部
IT Business Development Sector, NTT Data Corporation
†4 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information, Iwate Prefectural University

を意味しており，すなわち，万一，秘密鍵が格納されているデバイスが盗まれた場合には，不正者による成りすましが可能となってしまう恐れがある．また，秘密鍵が格納されているデバイスを紛失してしまった際にも問題が大きい．実際に 1 割強のユーザが携帯電話やノート PC を紛失しているという報告も出ており[4]，秘密鍵が携帯デバイスに格納されている場合には，デバイスの盗難・紛失は大きな脅威となる．

そこで本論文では，秘密鍵そのものではなく，秘密鍵を生成するメカニズムのみをデバイスに実装する「メカニズムベース PKI」を提案する．本方式では，ユーザが文書に署名を付す瞬間に，ユーザがデバイスに「秘密鍵の種」を入力することにより，デバイス内でそのつど秘密鍵を生成し，文書に署名を施す．普段はデバイス内には秘密鍵は存在せず，デバイスを盗まれたり失くしたりしても問題は起こらない．

また本論文では，メカニズムベース PKI の一実現形態としてユーザの指紋を秘密鍵の種とする方法を示す．ここで，指紋などのアナログデータを秘密鍵の種とする場合に必須となる「アナログデータからつねに一意の ID をリアルタイムに生成する技術」として統計的 AD 変換を提案し，統計的 AD 変換によって指紋からユニーク ID を抽出する方法を具体的に説明する．

以下では，2 章で現在の PKI の問題点を改めて指摘し，メカニズムベース PKI の必要性を述べる．3 章で指紋を秘密鍵の種とする方法を例にとり，メカニズムベース PKI の具体的な実装法を示す．4 章ではメカニズムベース PKI の中核技術である秘密鍵の種に関して議論し，生体情報からつねに一意な ID を抽出する技術である統計的 AD 変換を提案する．5 章では統計的 AD 変換により指紋からユニーク ID を抽出するための具体的な方法を説明する．6 章ではメカニズム PKI，統計的 AD 変換に関する今後の課題について議論する．最後に 7 章で本論文をまとめる．

2. ディジタル署名と本人認証

2.1 既存のディジタル署名における問題点

対面での相互確認が不可能な電子商取引においては，契約文書などにディジタル署名を付けて，その正当性を証明することになる．このとき，ディジタル署名を行うには秘密鍵が必要である．一般的には，秘密鍵は前もって公的機関などで公開鍵と対の形で同時に生成され，ユーザの携帯デバイスなどに安全に格納される．

しかし，この方式では携帯デバイスを紛失してしまった場合には大きな問題が発生する．そして，万一，紛失した携帯デバイスが悪意のある人に拾得されたり，携帯デバイスを盗まれて不正に使用されてしまった場合には，その被害は甚大なものとなる．

この問題に対処するためには，秘密鍵を格納する携帯デバイスを耐タンパデバイスとし，署名を施す際にはそのつどパスワードやバイオメトリクスにより本人認証を行ったうえで携帯デバイスをアクティベートする[5] などの方策が必要不可欠となる．

しかし最近では，サイドチャネル攻撃により IC カード内の情報がかなりの精度で解読可能であるという報告[6] もあり，「秘密を守る」ことの難しさが再認識されている．耐タンパデバイスの安全性をさらに高めることができたとしても，攻撃技術もまた進歩する．そこに秘密鍵が格納されている限り，漏洩の危険はつきまとう．「秘密鍵を保持する必要のない」ディジタル署名の方式や運用の構築が望まれる．

また，特にパスワード認証により携帯デバイスをアクティベートする方法においては，不正者は携帯デバイスを盗んだうえでパスワードを解析することができれば，盗んだ携帯デバイスを使って偽の署名を生成することが可能である．よって，秘密鍵の鍵長をいくら長くしてもパスワードが脆弱であるとその安全性を維持することができないという問題もかかえている．

2.2 秘密鍵の保存の必要がないディジタル署名

既存のディジタル署名では，「秘密鍵が携帯デバイスとリンクしており，ユーザ本人と直接リンクしていない」ことが，2.1 節に示した問題の原因であると考えられる．

不正者による鍵のブレイクに対処するため，秘密鍵は十分な鍵長を持ち，かつ，適当な時間間隔で更新される必要がある．よって，「ユーザが秘密鍵を記憶し，署名のつどユーザが秘密鍵を入力する」という方法によって秘密鍵をユーザにリンクさせることは不可能である．

そこで本論文では，秘密鍵そのものではなく，秘密鍵を生成するメカニズムのみを携帯デバイスに実装する「メカニズムベース PKI」を提案する．本方式では，

(1) ユーザが文書に署名を行う瞬間に，ユーザが携帯デバイスに秘密鍵の種を入力する，
(2) 携帯デバイス内でそのつど秘密鍵が生成される，
(3) 生成された秘密鍵により文書に署名が施される，
(4) 秘密鍵は使用後，即座に携帯デバイスから削除される，

というスキームにより，ディジタル署名が実行される．

ここで，携帯デバイスに実装される秘密鍵生成用のメカニズムは共通で公開されている．これは，現代暗号において，「暗号アルゴリズムは共通で公開されて

おり，鍵によって暗号の強度が保たれ，かつ，鍵を変えることにより暗号結果も変わる」のと同じコンセプトによるものである．逆にいえば，秘密鍵生成メカニズムは公開されていても問題ない．秘密鍵の種がユーザごとに固有であり，その結果，生成される秘密鍵もユーザごとに独立となる．

普段は携帯デバイス内に秘密鍵は保存されていないので，不正者が携帯デバイスを盗んでも偽の署名を行うことはできない．よって，携帯デバイスを紛失してしまったとしても気に病む必要はない．また，盗んだ携帯デバイスを高度なクラッカが解析しても，デバイス内に秘密鍵自体が存在しないので秘密鍵漏洩の心配もない．すなわち，基本的には携帯デバイスを耐タンパ化する必要性はない．

2.3 秘密鍵の種

メカニズムベース PKI においては,「秘密鍵の種」をユーザがどのように所持するかが重要な論点となる．

デバイスなどに秘密鍵の種を保存することは,「秘密がどこにも存在しない」というメカニズムベース PKI のコンセプトに反するので，秘密鍵の種は基本的に人間の記憶情報または生体情報となると考えられる．本論文では，以降，秘密鍵の種としてユーザの指紋を使用する方法を例に採り，メカニズムベース PKI の具体的な実現方式を説明する．

なお，生体情報から秘密鍵を生成する方法はすでに「バイオメトリクス PKI」として提案され，いくつかの手法が研究されている[7),8)]が，本方式は「秘密鍵をそのつど動的に生成する」ことを特徴とするものであり，生体情報を秘密鍵に反映させるというバイオメトリクス PKI のコンセプトを超えるものであると認識している．特に，文献 7) は DNA の解析に時間がかかることから，DNA から作られた秘密鍵を IC カードに格納して使用せざるをえず，秘密鍵を携帯デバイスから解放するには至っていない．また，文献 8) ではユーザのペン入力情報を秘密鍵に変更する方法が示されているが，毎回変動するユーザのペン入力情報をつねに同一の秘密鍵に変換するだけの精度は得られていない．

また，生体情報のセキュリティシステムへの活用という意味では，本方式はバイオメトリクス認証技術との関連が高い．しかし，既存のバイオメトリクス認証システムは，事前に登録してあるユーザの生体情報と認証時に読み取った生体情報との類似度から，認証を申し出ているユーザが登録されているどのユーザであるかを識別するものがほとんどである[9)]．すなわち，システム内には生体情報が秘密裡に格納されている．これに対し，本方式は「秘密がどこにもない」システムの実現を目指すものである．

3. メカニズムベース PKI

本章では，秘密鍵の種として指紋を利用する方法を採用し，メカニズムベース PKI の具体的な実装方法について説明する．なお，本章で説明する署名アルゴリズムには ElGamal 署名[10)] を用いているが，本方式に対応可能なものであれば他の署名アルゴリズムを用いてもかまわない．

3.1 前提条件

本章の説明では以下の状況を前提としている．

- 携帯デバイスとして IC カードを例に採る．
- IC カードには「記憶領域」と「作業領域」が存在する．作業領域に現れるデータは使用後ただちに消去される．
- IC カードには秘密鍵生成アルゴリズムおよび署名アルゴリズムが実装されている（ElGamal 署名に必要な乱数発生器なども実装されている）．
- 既存の PKI に基づく CA（信頼できる第三者機関）が存在する．CA はユーザ情報と公開鍵の登録作業を行い，公開鍵証明書を発行する．

3.2 鍵の生成と公開鍵の登録

指紋から秘密鍵を生成し，これに対応する公開鍵を作り，CA に公開鍵とユーザ情報を登録して公開鍵証明書の発行を受けるまでの手順を説明する．**図 1** に処理の流れを図示する．なお，以下の説明の中で,「記憶領域に保存する」と明言されていないデータは作業領域に現れるデータである．

いったん，以下の処理によって公開鍵を登録すれば（公開鍵証明書の発行を受ければ），その後，ユーザは任意のメッセージに署名を行うことが可能となる．なお，以下の処理は秘密鍵を更新するたびに行われる．

(1) IC カードにユーザの指紋を入力する．
(2) 指紋情報を後述（4 章）の方法によりユニーク ID に変換する．
(3) ユーザはランダムなパスナンバを入力する．パスナンバは記憶領域に保存する．
(4) (2) の ID と (3) のパスナンバを連結する．
(5) (4) のデータをハッシュ化し，秘密鍵のビット長へと変換する．ハッシュ化後のデータが当該ユーザの秘密鍵 x である．秘密鍵が漏洩したり，秘密鍵の有効期限が過ぎた場合には，パスナンバを変えることにより，同じ指紋から次の秘密鍵を生成することが可能である．
(6) 公開鍵 $y = g^x \bmod p$ を生成する．y を生成後,

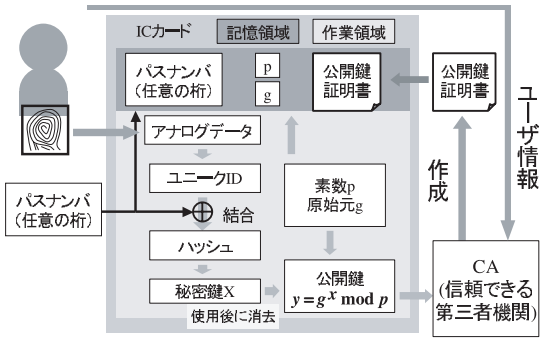

図 1 公開鍵の生成と登録
Fig. 1 Generation and registration of public key.

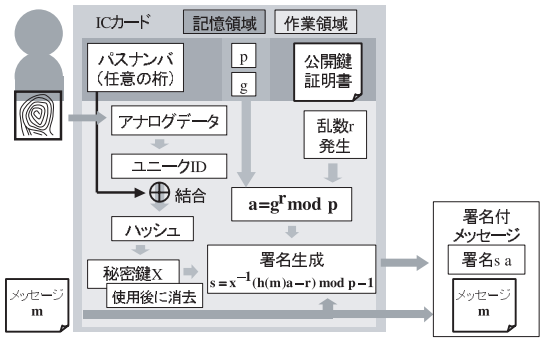

図 2 署名生成
Fig. 2 Signing a document.

x をはじめとする作業領域内のすべてのデータはすぐに消去される．なお，作業領域のデータの消去にあたっては，携帯デバイスの仕様に応じ，オール 0 値を上書きするなどの処置をとるなど，データが完全に消去されるようにする．

(7) 公開鍵 y および公開情報 p，g とユーザ情報を CA に送信し，公開鍵証明書の発行を受ける．p，g および CA から返送された公開鍵証明書は IC カードの記憶領域に保存する．

3.3 署名生成

指紋から秘密鍵を生成し，メッセージに署名を行う手順を説明する．**図 2** に処理の流れを図示する．なお，以下の説明の中で,「記憶領域に保存する」と明言されていないデータは作業領域に現れるデータである．

(1) IC カードにユーザの指紋を入力する．

(2) 指紋情報を後述（4 章）の方法によりユニーク ID に変換する．

(3) (2) の ID と記憶領域のパスナンバを連結する．

(4) (3) のデータをハッシュ化し，秘密鍵 x を得る．後述（4 章）の方法により指紋情報からつねに同一のユニーク ID を得ることができるため，必ず同じ秘密鍵 x が生成される．

(5) 乱数 r を生成し，$a = g^r \bmod p$，$s = x^{-1}(h(m)a - r) \bmod p - 1$ によりメッセージ m に対する署名 s，a を得る．ここで $h(m)$ は m のハッシュ値である．その後，x をはじめとする作業領域内のすべてのデータは消去される．なお，作業領域のデータの消去にあたっては，携帯デバイスの仕様に応じ，オール 0 値を上書きするなどの処置をとるなど，データが完全に消去されるようにする．

3.4 署名検証

署名付きメッセージ m，s，a と公開鍵証明書 y，g，p を受け取った相手は，$y^s a = g^{h(m)a} \bmod p$ により署名の検証を行い，メッセージの正当性を確認する．

3.5 メカニズムベース PKI の特徴

本署名方式は秘密鍵を生成するメカニズムのみが携帯デバイスに格納されており，秘密鍵は（携帯デバイスの作業領域に署名のつど，一瞬，現れるのみで）通常の記憶装置上には存在しない．このため，本署名方式は以下の利点を有する．

- 携帯デバイスだけを盗まれても，本人の指紋（秘密鍵の種）がなければ，他人には使用できない．
- 携帯デバイスの記憶領域には公開してもよい情報（公開鍵，公開情報）と破棄してもよい情報（パスナンバ）しか保存されていないので，内部を解析されても問題ない．
- このため，携帯デバイス自身は基本的には耐タンパデバイスである必要はない（ただし，携帯デバイスの耐タンパ化に関しては 6 章で詳しく述べる）．

また，本署名方式は，

- パスナンバを変更することにより，秘密鍵の再発行が可能である，
- 公開鍵証明書を使用する，

などの特徴を有し，既存の PKI に完全に適合するものとなっている．

4. 指紋からのユニーク ID の抽出

本論文では秘密鍵の種としてユーザの指紋を用いているが，指紋はアナログデータであり，取得のたびに読み取り誤差などにより変動してしまう．しきい値によりアナログデータを量子化するにしても，しきい値付近のデータが誤差により変動してしまうと，量子化の結果が異なってしまう．指紋から生成される秘密鍵 x が 1 ビットでも異なると，正しい署名ができな

い．よって，指紋を秘密鍵の種として用いるためには，指紋をつねに一意なユニーク ID に変換する必要がある．本章では，この問題を解決する手法として，統計的 AD 変換を提案し，その仕組みを説明する☆．

4.1 生体情報からのユニーク ID 抽出

生体情報を秘密鍵の種として用いるためには，生体情報を一意なユニーク ID に変換する必要があるが，DNA を除いた生体情報はアナログデータであり，取得のたびに読み取り誤差などにより変動してしまう．そのため，従来，ユーザの生体情報をつねに一意なユニーク ID にリアルタイムで変換することは非常に難しいとされていた．このような理由で，DNA を除き，生体情報を用いた既存の個人認証は，通常，登録されている生体情報と認証を申し出ているユーザの生体情報とのパターンマッチングにより行われている[9]．

4.2 統計的 AD 変換

著者らは，正規ユーザの指紋の特徴量の平均や標準偏差が，不特定多数の指紋の特徴量の平均や標準偏差と異なるという統計的な性質に着目し，ユーザ各々の指紋をリアルタイムでつねに一意なユニーク ID に変換することができる「統計的 AD 変換」という技術を構築した．以降はその方式の概要である．

- 指紋の登録

(1) 正規ユーザの指紋を複数回読み取る．同一の指紋であるが，読み取り誤差が混入するため，異なった指紋データが得られる．

(2) 複数個の指紋データのそれぞれについて，特徴量 V を算出する．

(3) 算出された特徴量の統計量を測り，正規ユーザの指紋の特徴量の平均 μ と標準偏差 σ を計算する．

(4) セキュリティパラメータ n を用意し，複数個の指紋データそれぞれの特徴量 V のほぼすべてが包含される範囲 $[\mu - n\sigma, \mu + n\sigma)$ を決定する．指紋読み取り時に混入する誤差が正規分布に従うと仮定するなら，$n = 3$ とすれば，統計学的に $[\mu - 3\sigma, \mu + 3\sigma)$ の中に約 99.7%の指紋が含まれることになる．

(5) $[\mu - n\sigma, \mu + n\sigma)$ の外を幅 $2n\sigma$ ごとに区切り，$[\mu + (2i - 1)n\sigma, \mu + (2i + 1)n\sigma)$ $(i = 0, \pm1, \pm2, \cdots)$ の各区間を生成する．各区間の境界となる値，すなわち，$\{\cdots, \mu - 5n\sigma, \mu - 3n\sigma, \mu - n\sigma, \mu + n\sigma, \mu + 3n\sigma, \mu + 5n\sigma, \cdots\}$ の値を IC カードに記憶する．この値を「スケール」と呼ぶことにする．

(6) $[\mu + (2i - 1)n\sigma, \mu + (2i + 1)n\sigma)$ $(i = 0, \pm1, \pm2, \cdots)$ の各区間に対して，それぞれ乱数 r_i を定め，IC カードに記憶する．この値を「候補 ID」と呼ぶことにする．また，スケールと候補 ID の組を「ID テーブル」と定義する．

- AD 変換（指紋からの ID 抽出）

(1) 指紋を読み取り，特徴量 V を算出する．

(2) 算出された特徴量が含まれる区間を ID テーブルから検索する．たとえば V が $[\mu + (2L - 1)n\sigma, \mu + (2L + 1)n\sigma)$ の中に含まれたならば，r_L が ID となる．同じ指紋から複数の指紋データを読み取る必要があるのは登録時のみであり，ID 抽出時には毎回，1 枚の指紋データを読み取るだけであることに注意されたい．

登録時に 1 つの指紋から何度も指紋データを読み取って統計量を算出することにより，その指紋に対する読み取り誤差の混入の期待値を測定している．たとえば指紋読み取り時に混入する誤差が正規分布に従うと仮定するなら，$n = 3$ とすれば，統計学的に $[\mu - 3\sigma, \mu + 3\sigma)$ の中に約 99.7%の指紋が含まれることになる．このように，セキュリティパラメータ n の値を適切に選んでやれば，$[\mu - n\sigma, \mu + n\sigma)$ の中にほぼすべての指紋の特徴量を含めることができる．よって，前もって（登録時に）十分な数の指紋データから特徴量の平均と標準偏差を求めておけば，その後（ID 抽出時に）読み取られる正規ユーザの指紋は（読み取り時にそのつど，誤差が混入するが）つねにほぼ確実に $[\mu - n\sigma, \mu + n\sigma)$ の中に入ることが期待される．すなわち，ID テーブルには $[\mu + (2i - 1)n\sigma, \mu + (2i + 1)n\sigma)$ $(i = 0, \pm1, \pm2, \cdots)$ の区間が登録されているが，正規ユーザの指紋であれば，その特徴量はほぼ確実に $i = 0$ の区間である $[\mu - n\sigma, \mu + n\sigma)$ の中に含まれることになり，正規ユーザの ID はつねに r_0 となる．ここで，指紋登録時にスケールとして登録されるのは各区間 $[\mu + (2i - 1)n\sigma, \mu + (2i + 1)n\sigma)$ の境界の値である $\{\cdots, \mu - 5n\sigma, \mu - 3n\sigma, \mu - n\sigma, \mu + n\sigma, \mu + 3n\sigma, \mu + 5n\sigma, \cdots\}$ の実際の数値だけであり，ID テーブルの情報を見てもどの区間が $i = 0$ の区間であるかは分からず，どの候補 ID が r_0 であるかを予測することは不可能である．すなわち，デバイスに記憶されるスケールの値 $\{\cdots, \mu - 5n\sigma, \mu - 3n\sigma, \mu - n\sigma, \mu + n\sigma, \mu + 3n\sigma, \mu + 5n\sigma, \cdots\}$ と候補 ID $\{r_i\}$ は秘密情報にあたらない．スケールの値は特徴量 V を量子化するためのしきい値にすぎず，指紋が入力されない限り，

☆ なお，メカニズムベース PKI のコンセプトは署名の際に秘密鍵の種からそのつど，秘密鍵を生成することにあり，秘密鍵の種はアナログデータに限られるものではない．

正しい ID がどの r_i であるかの確からしさはすべて等確率である．すなわち，ID テーブル自体が持つ情報量は情報理論的にはゼロであり，ID テーブルは公開してもかまわない．

実際には，指紋読み取り時に混入する誤差が正規分布に従うという保証はないので，本人拒否率と他人受入率を勘案してセキュリティパラメータ n を調節することになる．しかし，通常，本人拒否率と他人受入率はトレードオフの関係にあるので，両者を満足する n の決定は難しいであろう．そこで，本方式では，本人拒否率を改善するために n を用い，他人受入率は特徴量 V の次元 M を増加させることにより調整する方策を採る．すなわち，まず，本人拒否率が十分小さくなるまでセキュリティパラメータ n の値を大きくする．そして，他人受入率を減らすためには，特徴量 V をベクトルとし，十分な数の特徴量 $\{V_1, V_2, V_3,\cdots, V_M\}$ を用意する．具体的には，正規ユーザに対する V_1 の平均 μ_1 と標準偏差 σ_1 およびセキュリティパラメータ n_1，V_2 の平均 μ_2 と標準偏差 σ_2 およびセキュリティパラメータ n_2，V_3 の平均 μ_3 と標準偏差 σ_3 およびセキュリティパラメータ n_3，$\cdots$ を計算し，V_1 のスケール $\{\cdots, \mu_1-3n_1\sigma_1, \mu_1-n_1\sigma_1, \mu_1+n_1\sigma_1, \mu_1+3n_1\sigma_1,\cdots\}$ と各区間 $[\mu_1+(2i_1-1)n_1\sigma_1, \mu_1+(2i_1+1)n_1\sigma_1)$ の候補 ID $\{r_{1i_1}\}$，V_2 のスケール $\{\cdots, \mu_2-3n_2\sigma_2, \mu_2-n_2\sigma_2, \mu_2+n_2\sigma_2\ ,\ \mu_2+3n_2\sigma_2,\cdots\}$ と各区間 $[\mu_2+(2i_2-1)n_2\sigma_2, \mu_2+(2i_2+1)n_2\sigma_2)$ の候補 ID $\{r_{2i_2}\}$，V_3 のスケール $\{\cdots, \mu_3-3n_3\sigma_3, \mu_3-n_3\sigma_3, \mu_3+n_3\sigma_3, \mu_3+3n_3\sigma_3\ ,\cdots\}$ と各区間 $[\mu_3+(2i_3-1)n_3\sigma_3, \mu_3+(2i_3+1)n_3\sigma_3)$ の候補 ID $\{r_{3i_3}\}$，$\cdots$ の値を ID テーブルとして記憶する．特徴量 V_1 の値が $[\mu_1-n_1\sigma_1, \mu_1+n_1\sigma_1)$ の中に入る者は正規ユーザ以外にも多数存在する可能性があるが，「V_1 の値が $[\mu_1-n_1\sigma_1, \mu_1+n_1\sigma_1)$ 内に含まれ，かつ，V_2 の値が $[\mu_2-n_2\sigma_2, \mu_2+n_2\sigma_2)$ に含まれ，かつ，$\cdots$，かつ，V_M の値が $[\mu_M-n_M\sigma_M, \mu_M+n_M\sigma_M)$ に含まれる」を満たす者は高い確率で正規ユーザのみとなる．そして，(特徴量のベクトルの各基底の独立性が高ければ) M が大きくなるほどこの条件を満たす者が正規ユーザのみとなる確からしさは向上する．なお，その際，正規ユーザの ID は $r_{10}|\ r_{20}|\ r_{30}|\cdots|\ r_{M0}$ である．ここで，記号 "|" は連結を表す．

特徴量 V のベクトルの次元 M を増やすことは，指紋から抽出される ID のビット数を増やすためにも重要である．例として，指紋画像を小ブロックに分割して，各ブロックの隆線の傾き（0°〜180°：180° で 0° に戻る）を特徴量とした場合を考えよう．すなわち，ブロック j の隆線の傾きが特徴量 V_j である．今，同じ指の指紋データを何度も読み取って統計量を算出した結果，ブロック 1 の隆線の傾きが $\mu_1 = 67.5°$，$\sigma_1 = 7.5°$，$n_1 = 3$ であったとすると，スケールは $\{0°, 45°, 90°, 135°\}$ となる．仮に，$[0°, 45°)$ の区間の候補 ID を 00，$[45°, 90°)$ の区間の候補 ID を 01，$[90°, 135°)$ の区間の候補 ID を 10，$[135°, 180°)$ の区間の候補 ID を 11 としたなら，V_1 の値に応じて 00，01，10，11 のうちのいずれかの値が ID（の一部）として抽出されることになるので，特徴量 V_1 から抽出できる ID は 2 ビットということになる．V_j より d_j ビットの ID が抽出される場合，M 次元の特徴量ベクトル $\{V_1, V_2, V_3,\cdots, V_M\}$ 全体で $\sum_{j=1}^{M} d_j$ ビットの ID が抽出できる．

最後に，今回は指紋を例に採り説明をしたが，本論文で提案する統計的 AD 変換は任意のアナログ情報に対して適用可能なアイデアであることに留意されたい．

4.3 関 連 研 究

生体情報からつねに一意の ID を抽出することは難しく，著者が知る限り，これを実現する研究や技術開発が報告されているのは世界で 2 例のみである[11),12)]．

Bioscript[11)] は指紋からつねに一意の ID を抽出する技術である．登録時に同一の指紋から読み取った複数の指紋データを用い，指紋データとフィルタ関数 H の畳み込み積分値がつねに一意となるように H の値を調整することにより，指紋から一意のデータを抽出することを可能にしている．ただし，文献 11) によると，ID 抽出時にも複数の指紋データの入力が必要となっており，本論文が提案している統計的 AD 変換とは異なる．

虹彩コード[12)] は虹彩から ID を抽出する方法である．瞳孔の中心から虹彩の左右の端までの半径距離を考慮し，上瞼と下瞼付近の虹彩を除外すれば，つねに同一の虹彩情報（虹彩コード）が取得できることが報告されている．ただし，正確には同じ虹彩であっても読み取り誤差のため，毎回の虹彩コードの正規化ハミング距離の平均は 0.084 程度となるのが現状であり[12)]，2048 ビットのコードのうち，平均 172 ビット程度は異なっていることになる．虹彩はもともと読み取り誤差の混入が少ない生体情報であるといえ，虹彩コードの方法のように読み取り時に混入する誤差を抑えるという工夫により，つねに一意の ID を抽出することが可能である．一方，本論文が提案する統計的 AD 変換は，読み取り誤差が発生したとしても，その誤差を許容してしまうような仕組みを提唱するものであり，指紋をはじめ，読み取り誤差の混入が大きい種々なアナ

ログデータに対して適用が可能だと思われる．

なお，Bioscript も虹彩コードも，「秘密鍵を生成するメカニズムのみをデバイスに実装することによりいっさいの秘密が残存しない署名を実現する」というメカニズムベース PKI のコンセプトについては言及していない．

5. 指紋の特徴量

4.2 節で説明した統計的 AD 変換を用いて指紋から ID を抽出するためには，指紋の中のどの情報を特徴量として使用すればよいのであろうか．特徴量の選定については，本人—他人間の有意差の大きさ，読み取り誤差の混入しやすさ，抽出される ID のビット数，測定のしやすさなどの様々な要因を考慮して議論，検証する必要があるが，本論文ではその一例として，指紋の隆線の傾きに基づく特徴量について説明し，簡単な実験によりその実用性を評価した．

5.1 指紋の隆線に基づく特徴量

今回は Veridicom 社の 5th Sense☆という指紋読み取り装置を使用して，指紋画像を取得する．指紋画像は 300×300 画素のモノクロ画像として得られる．本論文では，この指紋画像を小さなブロックに分割し，各ブロックにおける隆線の角度を特徴量とする方式を説明する．なお，各ブロックの隆線の角度の抽出に関しては，基本的に文献 13) の 2.4 節で述べられている方法を採用した．

- 特徴量の抽出手順

(1) 指紋画像に対して，輝度の正規化を行う．

(2) 指紋画像を小さなブロックに分割する．本方式では 1 ブロックのサイズを 16×16 画素，ブロック数を 10×10 個とした．すなわち，300×300 画素の指紋画像の中の中央の 160×160 画素を使用する．

(3) すべての画素 (u, v) に，Sobel 演算子を適用し，各画素の x 勾配 $\partial_x(u, v)$ と y 勾配 $\partial_y(u, v)$ を得る．

(4) 各ブロックごとに (3) で得た $\partial_x(u, v)$ と $\partial_y(u, v)$ を使って，以下の計算を行い，$\theta(p, q)$ を得る．なお，$\sum_{u=p-8}^{p+8} \sum_{v=q-8}^{q+8}$ は第 (p, q) ブロックに含まれる 16×16 画素における和を意味する．$\theta(p, q)$ がブロック (p, q) における隆線の角度である．

$$\nu_x(p, q) = \sum_{u=p-8}^{p+8} \sum_{v=q-8}^{q+8} \{\partial_x^2(u, v) - \partial_y^2(u, v)\}$$

$$\nu_y(p, q) = \sum_{u=p-8}^{p+8} \sum_{v=q-8}^{q+8} 2\partial_x(u, v)\partial_y(u, v)$$

$$\theta(p, q) = \frac{1}{2} \tan^{-1}\left(\frac{\nu_y(p, q)}{\nu_x(p, q)}\right)$$

(5) (4) で求めた $\theta(p, q)$ にはノイズによって誤差が生じている可能性がある．そこで，low-pass フィルタをかけ，ノイズによる誤差を吸収する．まず，以下の計算により，$\Phi_x(p, q)$ と $\Phi_y(p, q)$ を求める．

$$\Phi_x(p, q) = \cos(2\theta(p, q))$$
$$\Phi_y(p, q) = \sin(2\theta(p, q))$$

求めた $\Phi_x(p, q)$ と $\Phi_y(p, q)$ に対して，low-pass フィルタをかけ，その結果である $\Phi'_x(p, q)$ と $\Phi'_y(p, q)$ を求める．そして，誤差吸収後の隆線の角度 $V(p, q)$ を $\Phi'_x(p, q)$ と $\Phi'_y(p, q)$ から以下の計算により求める．

$$V(p, q) = \frac{1}{2} \tan^{-1}\left(\frac{\Phi'_y(p, q)}{\Phi'_x(p, q)}\right)$$

この $V(p, q)$ がブロック (p, q) の特徴量となる．

(6) $j = 10p + q$ の変換により，10×10 ブロックの各特徴量 $V(p, q)$ から $\{V_j | 1 \leq j \leq 100\}$ の特徴量ベクトルが得られる．

ただし，実際には，この前処理として，指紋読み取り時の位置ズレ（平行移動，回転移動）を補正する処理が加わる．今回は，指紋データの端点や分岐点の位置を利用して位置合わせを行っている．位置ズレ補正のために，位置合わせの基準となる指紋データの端点や分岐点の位置情報（端点および分岐点の座標情報のみであり，端点や分岐点における隆線の方向や端点なのか分岐点なのかという情報は含まない）を ID テーブルとともに記録しておく必要があるが，端点や分岐点の単なる位置情報だけが分かっても，そこから指紋を再現したり，正しい ID を推測することは不可能であることに注意されたい．

5.2 実証実験

5.1 節で説明した指紋の特徴量ベクトル $\{V_j | 1 \leq j \leq 100\}$ を用い，実際に指紋から何ビットの ID がどれくらいの精度で抽出可能であるか実験を行った．

今回の実験では，以下について検証する．

(1) FRR（本人拒否率）：ユーザ A が登録されている場合に A の指紋から本来抽出されるべき ID が抽出されない確率．

☆ 5th Sense は Veridicom 社の登録商標です．

(2) FAR（他人受入率）：ユーザ A が登録されている場合に A の指紋ではない人物の指紋から A と同一の ID が抽出されてしまう確率．

(3) ビット長：抽出される ID のビット長．本来ならば，抽出される指紋 ID のエントロピを計算して，実効ビット長を求めるべきであるが，本研究の現時点では単純に生成される ID のビット長を測定する．

(4) 無効ブロック数：無効ブロックの数．今回の各特徴量 V_j の値の範囲は 0〜180°（180° で 0° に戻る）であるので，登録時に $2n_j\sigma_j$ の値（V_j のスケールの幅）が 90° を超えてしまった場合には，ID テーブルの情報から V_j に対する ID を推測することが非常に容易となる．そこで，このような V_j に対する指紋ブロックは無効ブロックとし，指紋 ID の抽出には使用しないことにする．

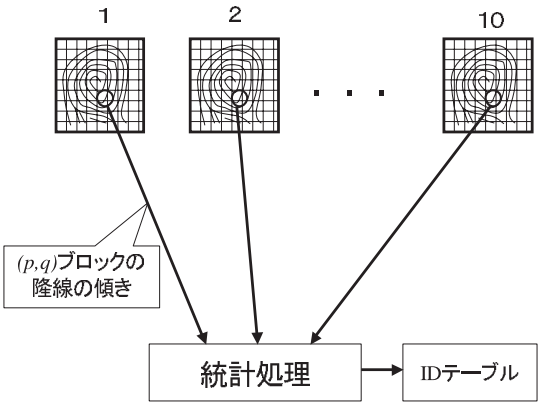

図 3 指紋の登録
Fig. 3 Registration of fingerprints.

実験に先立ち，本学の男子学生 10 人を被験者として，以下の指紋画像を採取した．(i) が正規の指紋，(ii) (iii) が不正者の指紋という位置付けである．

(i) 被験者 1 のある 1 本の指を正規の指として選び，その指から 20 枚の指紋画像を取得．

(ii) 被験者 2 のある 1 本の指を選び，その指から 20 枚の指紋画像を取得．被験者 3，4，5 からも同様にそれぞれ 20 枚，合計 80 枚の指紋画像を取得．

(iii) (i)，(ii) の指とは異なる指，すなわち，被験者 1 の他の指（9 本），同様に被験者 2〜5 それぞれの他の指（9 本 ×4 人），被験者 6〜10 のすべての指（10 本 ×5 人）の指紋画像を各々1 枚ずつ合計 95 枚取得し，その中から無作為に 90 枚を選出．

実験手順を以下に示す．今回は，登録時に正規ユーザの ID テーブルを作成するために使用する指紋画像は 10 枚とする．

(1) 被験者 1 の (i) の指紋画像 20 枚を，無作為に，登録用の指紋 10 枚と FRR 評価用の指紋 10 枚に分ける．

(2) 被験者 1 の登録用の 10 枚の指紋画像から，5.1 節の方法により 100 次元の特徴量 $\{V_j|1 \leq j \leq 100\}$ を計測し，4.2 節の方法により指紋を登録し，ID テーブルを作成する（この一連の流れを**図 3** に示す．**図 4** は，図 3 の中の「統計処理」を示すものである．作成される ID テーブルは**図 5** のようになる．これらの処理は各ブロックごとに行われる）．ただし，セキュリティパラメータ n_j の影響を測るため，すべての n_j を一律に 2.0 から 8.0 まで 1.0 刻みで変

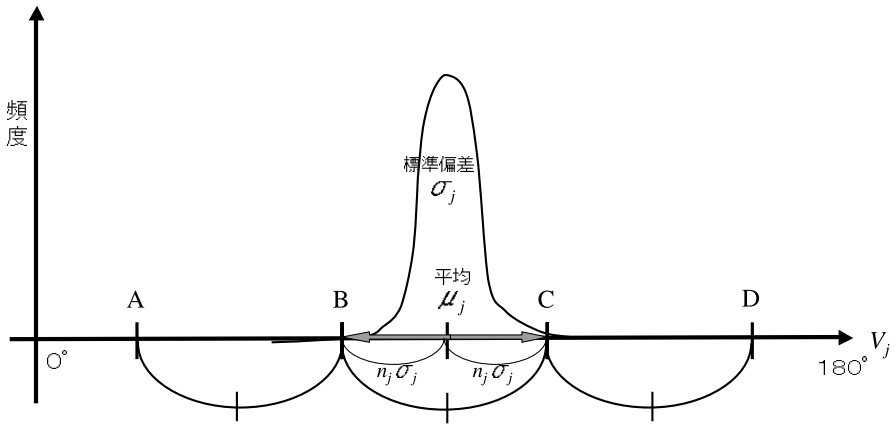

図 4 ID テーブル生成のための統計処理
Fig. 4 Statistical processing for ID table generation.

更し，各々の場合の ID テーブルを作成する．すなわち，7 種類の ID テーブルを作成する．なお，登録時に $2n_j\sigma_j$ の値（スケールの幅）が 45° 未満の場合にはスケールの幅を 45° に伸張し，$2n_j\sigma_j$ の値が 90° 以上の場合には無効ブロックとする．

(3) 作成した 7 種類の ID テーブルを用いて，被験者 1 の FRR 評価用の 10 枚の指紋画像から ID を生成し（この一連の流れを**図 6** に示す），FRR を求める．すなわち，FRR は「10 枚中，誤って異なる ID が生成されてしまう指紋画像数」のパーセンテージとなる．

(4) 作成した 7 種類の ID テーブルを用いて，その指以外のすべての指紋画像（(ii) と (iii) の指紋画像 170 枚）から ID を生成し（この流れも図 6 と同様になる），FAR を求める．すなわち，FAR は「170 枚中，誤って同じ ID が生成されてしまう指紋画像数」のパーセンテージとなる．

(5) 作成した 7 種類の ID テーブルを解析して，抽出される ID のビット長および無効ブロック数を調べる．

表 1 にこの結果を示す．また，被験者 1 の他の指や，他の被験者の指を正規の指として同様の実験を行ったが，その結果はすべて，表 1 とほぼ同じ傾向となった（実際，表 1 は同様の複数の実験結果の中から無作為に 1 つを選んだものである）．

スケール	候補 ID
$[0°, A)$	ID_0
$[A, B)$	ID_1
$[B, C)$	ID_2
$[C, D)$	ID_3
$[D, 180°)$	ID_0

図 5 V_j の ID テーブル
Fig. 5 ID table for V_j.

表 1 の結果から，セキュリティパラメータの値（今回はすべての特徴量 $\{V_j|1 \leq j \leq 100\}$ のセキュリティパラメータ n_j は一律としている）は $n = 6.0$ 程度にまで大きくしないと FRR をゼロにすることができないことが分かる．しかし，n の値を大きくすることはスケールの幅を大きくすることに相当し，その結果，FAR の増加，ビット長の減少，無効ブロック数の増加という弊害が現れることになる．

ただし，4.2 節で述べたように，本論文で提案している統計的 AD 変換においては，他の何らかの方法により特徴量の次元数 M をさらに増加させることにより FRR をゼロに保ったまま，FAR を減少させることが可能であると考える．また，表 1 から分かるように，5.1 節で説明した特徴量だけでは $n = 6.0$ のときのビット長は 90[bit] 程度であり，楕円暗号を採用するとしたとしても，まだ公開鍵暗号の鍵としては脆弱である．ID の実際のエントロピを考慮すると，さらに有効ビット長は短いであろう．ビット長を伸張するためにも，特徴量の次元数を増やすことは不可欠であると思われる．特徴量の次元数を増加させる方法として，「指紋のブロックの隆線の傾き」という特徴量に加えて，これとは異なる特徴量も採用することが有力な方法と考えられる．

一方，あえて大きな読み取り誤差が混入するようにして 10 枚の指紋画像を取得し，登録時にこの劣悪条件の指紋画像を用いて ID テーブルを作成するようにしてやれば，はじめから FRR が低いスケールが作成されることが期待される．これを確認するために，実験手順 (1) において，被験者 1 の (i) の指紋画像 20 枚を登録用の指紋 10 枚と FRR 評価用の指紋 10 枚に分ける際に，誤差の大きい指紋画像（表 1 の FRR の実験の際に，実際に異なる ID を生成してしまった指

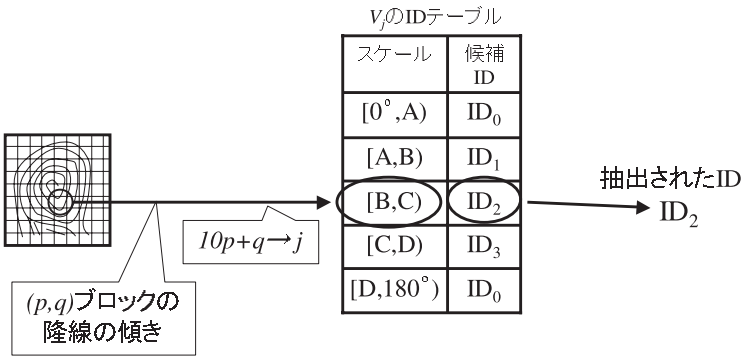

図 6 ID 抽出
Fig. 6 ID extraction.

表 1 実験結果
Table 1 Experimental result.

セキュリティパラメータ n	2.0	3.0	4.0	5.0	6.0	7.0	8.0
FRR[%]	0.500	0.300	0.300	0.200	0.000	0.000	0.000
FAR[%]	0.000	0.000	0.000	0.000	0.036	0.059	0.166
ビット長 [bit]	192.3	171.5	143.7	115.0	88.2	66.0	40.5
無効ブロック数 [個]	1	6	16	32	39	52	63

表 2 追実験の結果
Table 2 Additional experimental result.

セキュリティパラメータ n	2.0	3.0	4.0	5.0	6.0	7.0	8.0
FRR[%]	0.400	0.000	0.000	0.000	0.000	0.000	0.000
FAR[%]	0.000	0.000	0.000	0.000	0.018	0.041	0.065
ビット長 [bit]	189.3	172.5	160.4	140.5	119.8	95.9	66.8
無効ブロック数 [個]	1	11	15	20	24	30	42

紋画像）は意図的にこれらをすべて登録用の指紋 10 枚のほうに仕分けし，同様の実験を行ってみた．結果を**表 2** に示す．表 2 より，セキュリティパラメータ n が 3.0〜4.0 の辺りで，FRR と FAR がともにゼロになるという非常に有効な結果が得られている．他の指で同様の実験を行った結果も，すべてほぼ同じ傾向となった．この結果から，指紋の登録時に意図的に指紋の読み取り誤差を大きくすることにより，本方式の実用性が向上するであろうことが確かめられた．

6. 今後の課題

6.1 統計的 AD 変換

第 1 に，FAR を減少させるために，指紋の他の特徴量を考案することが緊急の課題であると考える．特徴量の次元数の増加は ID のビット長を伸張させるためにも不可欠である．特徴量の次元数を増加させる方法としては，5 章で示した「指紋のブロックの隆線の傾き」という特徴量に加えて，これとは異なる特徴量を合わせて採用する方法が考えられる．たとえば指紋には複数の特徴量（隆線の端点や分岐点）が存在するが，その中からいくつかの点を選んだ際に，「その配置が特定の図形（正三角形や正方形など）となる特徴点の組がいくつあるか」といったものが他の特徴量として考えられる．なお，その際，ID の有効ビット長を評価する必要がある．

第 2 に，誤差が多く含まれる指紋画像を意図的に採取する方法を確立しなければならないと思われる．誤差が多く含まれる指紋画像を採取できれば，これを用いて指紋の登録を行うことにより実用的な ID テーブルを作成することが可能となる．

第 3 に，統計的 AD 変換は指紋に限らず，他の生体情報（アナログデータ）から ID を抽出する方法ととらえることができるため，生体情報を用いての CHAP 型認証システムへの応用など，幅広い分野への適応を模索していきたい．

6.2 携帯デバイスの非耐タンパ化

メカニズムベース PKI では，携帯デバイス内に秘密鍵が存在しないため，デバイスの耐タンパ性は基本的には不要となる．しかし，3.2 節で示した公開鍵の登録時，および，3.3 節で示した毎回の署名生成時に，一瞬ではあるが，秘密鍵が携帯デバイスの作業領域に現れる．よって，不正者が作業領域に現れた秘密鍵をタッピングできるように携帯デバイスを改造した場合には，秘密鍵が漏洩する．

すなわち，本署名方式においては，携帯デバイスに不正な改造が施されていないことを証明するための仕組みだけは必要となる．今後，秘密鍵が使用のたびに変化する暗号アルゴリズム[14] を採用するなどの方策を検討し，携帯デバイスの完全な非耐タンパ化を実現していきたい．

6.3 生体情報以外の秘密鍵の種

本論文では，秘密鍵を生成するための種として生体情報（指紋）を用いたが，メカニズムベース PKI は「秘密鍵を生成するメカニズムのみをデバイスに格納すること」がコンセプトの要点であり，秘密鍵の種となる情報に対する制約は存在しない．

生体情報は（身体の一部であるため）ユーザがつねに所持しており，また，ユーザごとに個別の情報となっているため，確かに秘密鍵の種としては非常に適した情報であるといえるが，生体情報をセンシングする読み取り装置が必要となる，生体情報の多くは（DNA は髪の毛などから，指紋は残留指紋などから）容易に複製をとることができる[15]，などの様々な脆弱性も指摘されている．よって，生体情報以外に，秘密鍵の種

として適切な情報を検討していきたい．

6.4 生体情報の偽造

特に指紋においては文献 15) で人工指による成りすましが可能であるという深刻な問題が報告されている．本論文の方式も指紋が漏洩しないという条件の下に安全性が示されているだけであり，完全な指紋の陰影を有する人工指が作られた場合，クラッカがパスナンバさえ解析できれば，人工指を用いて秘密鍵を偽造することが可能になってしまう．本方式を実用化するにあたっては，人工指などによる成りすましに対する対策も必須となる．

7. ま と め

秘密鍵を生成するメカニズムのみをデバイスに実装する「メカニズムベース PKI」を提案した．本方式では，ユーザが文書に署名を付す瞬間に，ユーザがデバイスに秘密鍵の種を入力することにより，そのつど，秘密鍵が生成される．普段はデバイス内には秘密鍵は存在せず，デバイスの盗難・紛失の際にも被害を最小限に抑えることが可能である．

本論文では，指紋を秘密鍵の種として，メカニズムベース PKI の具体的な実装方式を説明し，メカニズムベース PKI が持つ特徴を述べた．

また，アナログデータである指紋を秘密鍵の種として用いるためには，指紋をつねに一意なユニーク ID にリアルタイムに変換する必要があることから，そのための技術として統計的 AD 変換を提案した．統計的 AD 変換はアナログデータが持つ特徴量から，その特徴量が持つ統計的な性質に基づき，一意なディジタルデータを抽出する方式である．さらに，指紋の隆線の角度を特徴量とした場合の，指紋から ID を抽出する基礎実験を行い，その実用性を確認した．

最後にメカニズムベース PKI の改良，統計的 AD 変換の応用を含めた今後の課題を検討した．

参 考 文 献

1) MYCOM PC Web：アイワイバンクネットバンキングを開始. http://pcweb.mycom.co.jp/news/2001/12/17/03.html
2) DoCoMo NET：FOMA サービスを提供開始. http://www.nttdocomo.co.jp/new/contents/01/whatnew0903.html
3) 首相官邸ホームページ：高度情報通信ネットワーク社会推進戦略本部 e-Japan 戦略. http://www.kantei.go.jp/jp/singi/it2/index.html
4) ZDNet News：ノート PC・携帯の紛失による情報漏洩に低い危機意識 ガートナー調査. http://www.zdnet.co.jp/news/0206/20/njbt_10.html
5) 日立エンジニアリング株式会社：カード内に指紋を封じ込めた高セキュリティIC カード内指紋照合認証システム「セキュアバイオロック」. http://www.hitachi-hec.co.jp/sonota/20020628.htm
6) 電子政府情報セキュリティ技術開発事業：暗号アルゴリズムの実装方式とリスク分析に関する調査. http://www.ipa.go.jp/security/fy14/crypto/implementation/risk_anal.pdf
7) 板倉征男，辻井重男：DNA-ID を用いた DNA 個人情報管理システムの提案，情報処理学会論文誌，Vol.42, No.8, pp.2134–2143 (2001).
8) 赤尾雅人，山中晋爾，花岡悟一郎，今井秀樹：ペン入力情報を用いた暗号鍵生成手法，暗号と情報セキュリティシンポジウム（SCIS 2003）予稿集，pp.299–304 (2003).
9) 日経 BP 社（編）：日経 NETWORK 2003 年 2 月号特集 1 認証のキホン，問 4 なぜ生体認証をネットワークでもっと使わないのですか?，p.67, 日経 BP 社 (2003).
10) ElGamal, T.: A public key cryptosystem and a signature system based on discrete logarithms, *IEEE Trans. IT*, Vol.IT-13, No.4, pp.469–472 (1985).
11) Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, B.: Biometric Encryption. http://www.bioscrypt.com/assets/Biometric_Encryption.pdf
12) Daugman, J.: How Iris Recognition Works. http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf
13) Lin Hong, Y.W. and Jain, A.: Fingerprint Image Enhancement: Algorithm and Performance Evaluation, *IEEE Trans. pattern analysis and machine intelligence*, Vol.20, No.8, pp.777–789 (1998).
14) Boneh, D. and Franklin, M.: Identity-based encryption from the weil pairi, *CRYPTO'01*, LNCS2139, Springer-Verlag (2001).
15) 松本 勉：セキュリティ技術の弱点を発見したらどうしますか?, 電子情報通信学会誌, pp.202–204 (2001).

(平成 15 年 12 月 4 日受付)
(平成 16 年 6 月 8 日採録)

柴田 陽一

平成 15 年静岡大学情報学部情報科学科卒業．現在，同大学大学院修士課程．情報セキュリティに関する研究に従事．

三村　昌弘（正会員）

昭和 43 年生．平成 9 年東京工業大学大学院工学専攻博士課程修了．同年（株）日立製作所に入社．システム開発研究所に所属．以来，指紋照合装置およびバイオメトリクス認証システムの研究開発に従事．現在に至る．研究員（工学博士）．電子情報通信学会会員．

高橋　健太（正会員）

平成 10 年東京大学理学部情報科学科卒業．平成 12 年同大学大学院修士課程修了．同年（株）日立製作所入社．以来，生体認証技術の研究開発に従事．

中村　逸一（正会員）

昭和 60 年茨城大学工学部卒業，昭和 62 年同大学大学院修了．同年日本電信電話株式会社入社．LAN システムの研究に従事．平成 8 年より（株）NTT データにてセキュリティ技術の研究・開発に従事．現在同社ビジネス開発事業本部企画部部長．

曽我　正和（正会員）

昭和 33 年京都大学工学部電子工学科卒業．昭和 35 年同大学大学院修士課程修了．昭和 35 年〜平成 8 年三菱電機，計算機製作所副所長，情報電子研究所所長を経て平成 8 年静岡大学情報学部教授，平成 11 年岩手県立大学ソフトウェア情報学部教授，現在に至る．博士（工学）（東京大学）．汎用計算機，制御用計算機，制御用システムの開発．フォールトトレラントシステム，セキュリティシステムに関する研究に従事．IEEE，電子情報通信学会各会員．

西垣　正勝（正会員）

平成 2 年静岡大学工学部光電機械工学科卒業．平成 4 年同大学大学院修士課程修了．平成 7 年同大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，平成 8 年静岡大学情報学部助手．平成 11 年同講師，平成 13 年同助教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シュミレーション等に関する研究に従事．