社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38 (23)
2007／7／19

公開鍵暗号基盤における匿名バイオメトリクスを用いた秘密鍵管理の提案

泉 昭年† 上繁 義史†† 櫻井 幸一†

† 九州大学大学院 システム情報科学研究院 〒 819-0395 福岡市西区元岡 744 番地
†† 長崎大学 情報メディア基盤センター 〒 852-8521 長崎県長崎市文教町 1-14
E-mail: †izumi@itslab.csce.kyushu-u.ac.jp, ††yueshige@nagasaki-u.ac.jp, †††sakurai@csce.kyushu-u.ac.jp

あらまし 公開鍵暗号基盤においてトークンに秘密鍵とバイオメトリクスを組み合わせた，保護秘密鍵を保管する方式を提案する．提案方式では，秘密鍵所有者の指紋から抽出したバイオメトリクス情報によって秘密鍵を暗号化し，それを保護秘密鍵として指紋読み取り機能を持つトークンに格納する．ユーザは秘密鍵使用時には保護秘密鍵と補助データが格納されたトークンに指紋を提示することで保護秘密鍵から秘密鍵を復元することが可能である．本提案方式を用いることで，テンプレート（登録情報）を用いず本人認証を行うことが出来るため，従来のバイオメトリクス認証で生じるようなテンプレート漏洩の危険性は無い．
キーワード 公開鍵暗号基盤，匿名バイオメトリクス，テンプレート，Fuzzy Vault

A Proposal of Secret Key Management Using Anonymous Biometrics in Public Key Infrastructure

Akitoshi IZUMI†, Yoshifumi UESHIGE††, and Kouichi SAKURAI†

† Aculty of Information Science and Electrical Engineering, Kyushu University, Motooka, Nishi-ku, Fukuoka 819-0395, Japan
†† Information Media Center, Nagasaki University 1-14 Bunkyo-machi Nagasaki-shi, 852-8521, Japan
E-mail: †izumi@itslab.csce.kyushu-u.ac.jp, ††yueshige@nagasaki-u.ac.jp, †††sakurai@csce.kyushu-u.ac.jp

Abstract We propose the scheme that stores protected secret key which is made by combination of biometrics and secret key in the smartcard in PKI. In our proposal, the user encrypts the secret key using biometrics information extracted from owner of that secret key and stores it as protected secret key in smartcard which has fingerprint reading function. The user can restore the secret key form protected secret key by presenting his fingerprint to smartcard that has protected secret key and helper data. In our scheme, the template is not need for authentication. So, the problem of the leaks of the template which arise in traditional biometric authentication won't arise in our scheme.
Key words PKI, Anonymous Biometrics, template, Fuzzy Vault

1. まえがき

近年の急速なインターネットの発達により，我々はネットワークを介しての情報交換を容易に高速に行えるようになった．今後もますます普及していくことが予想される．しかしながら，ネットワークを介しての情報交換には攻撃者による電子的なデータの盗聴，改ざん，および成りすましなどの攻撃が考えられ，それらに対するセキュリティリスクが常に存在する．公開鍵暗号基盤において秘密鍵の管理は非常に深刻な問題である．例えば，デジタル文書の正当性を保証するために，現在 PKI が提供する機能の一つであるデジタル署名が用いられている．デジタル署名の正当性は署名に用いられた秘密鍵はそのデジタル文書の正当な所有者のみが所有しているという点に依存しているため，秘密鍵の盗難・紛失はこれまでにその秘密鍵で作成されたデジタル署名の正当性の崩壊を意味する．現在，秘密鍵やパスワードなどの秘密情報管理のため，USB トークンにてバイオメトリック認証を用いる装置が市販されているが [1]，バイオメトリックテンプレートと秘密情報をそのままトークン内に格納するため，トークンの盗難時には秘密情報の流出やテンプレートから認証可能な人工バイオメトリクスを復元される危険

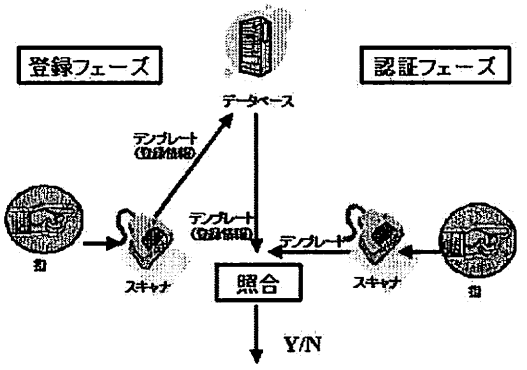

図 1 バイオメトリクス認証

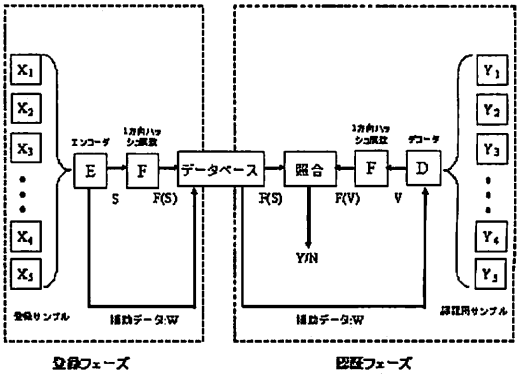

図 2 匿名 バイオメトリクスの基本的構成

がある．従って，トークン内にテンプレートを格納することなくバイオメトリック認証を行う必要がある．

そこでトークンにて匿名バイオメトリクスを用いて秘密鍵を活性化させる手法を提案する．本来匿名バイオメトリクスはテンプレート漏洩問題を解決するための手法であり，そのためにユーザのバイオメトリック情報から一意で逆変換不可能なデータ S を抽出し，それに基づいて本人認証を行う方式である．この一意で逆変換不可能なデータ S を暗号鍵として用いて秘密鍵を暗号化することで保護秘密鍵を生成し，トークン内に保管する．

秘密鍵を使用する際にはバイオメトリック情報から抽出した $V = S$ を用いて保護秘密鍵を復号化することで秘密鍵を復元できる．

本提案方式ではトークン内に登録情報としてテンプレートを格納することなく本人認証を行うことができるため，バイオメトリクス認証に特有のテンプレート漏洩問題を解決することができる．以上の方法でテンプレート漏洩問題を解決した秘密鍵管理を提案する．

2. 関連研究

2.1 バイオメトリクス認証

バイオメトリクス本人認証では，身体的特徴（指紋や虹彩），行動的特徴（声紋や署名）などの生体的特徴を抽出し，あらかじめ登録された特徴のデータベース（テンプレート）との間で類似性を評価し，十分に類似性が高ければ本人と認証する（図1）

本研究では，指紋認証トークンシステム [1] に匿名バイオメトリクス [3] を適用させた秘密鍵管理システムを提案する．

2.2 指紋認証トークンシステム

指紋認証トークンは，指紋センシング，指紋データ登録および照合までの一連の処理を装置内で完結できる指紋認証機能を持った個人専用のパスワード保管ツールとして研究開発されている．[1]，[2]．静電容量型指紋センサ，登録指紋データ保管用不揮発性メモリ，および指紋照合用 CPU から構成される．

指紋認証と一君は PC の USB コネクタに接続すると標準キーボードとして認識され，指紋センシングで得た指紋データとトークン内に保管する登録指紋データを照合し，指紋認証の結果，本人であると確認されると，トークン内に保管するパスワードを PC に送信するシステムである．トークン内に保管されている指紋データやパスワードなど保護すべき個人情報の脅威に対処するため，耐タンパ性に優れた装置構成をとる必要がある．

2.3 Fuzzy Vault を用いた秘密保護

現在、Fuzzy Vault[6] にバイオメトリクスを適用させた秘密保護方式の研究が盛んに行われている．実装例として、指紋認証を Fuzzy Vault に適用させた方式 [7]、指紋認証と Fuzzy Vault を用いてデジタル署名を生成する方式 [8]、さらに、オンライン署名を Fuzzy Vault に適用された方式 [9] などが挙げられる．Fuzzy Vault は多項式復元の困難性に基づいており、認証するユーザが提示する M 個の点に正当な点を N 個含まれていれば、ラグランジュ補完法により $N-1$ 次多項式を復元することが可能となる．従って、最悪 ${}_M C_N$ 回、多項式復元を行うことになり、非常に高い計算量を必要とする．[9] によると、Intel Celeron (M) 1.5GHz、512MB RAM を実験環境として、認証に平均 30 秒を要している．以上より、Fuzzy Vault を用いる方式をトークンにて実装することは不可能である．

2.4 匿名バイオメトリクス

従来，テンプレートは生のバイオメトリクス情報から特徴抽出処理を通して生成され，かつ，特徴抽出処理は画像情報から一部の有用な情報のみを抽出する変換であり，その逆変換は一意に決定できないことから，テンプレートから元のバイオメトリクス情報を復元することは不可能であるとされてきた [4]．しかし，元の画像を含まない特徴点だけの指紋テンプレートから認証可能な人工指パターンが生成可能なことが示されている [5]．このような背景からテンプレート保護に関する研究として，匿名バイオメトリクスがある．Tuyles らによって，補助データを用いる匿名バイオメトリクスの一般形が示されている (図2)．図 2 において，登録時の登録サンプル $X_i (i = 1...N)$ はエンコーダ E によって特徴ベクトル S と補助データ W とを生成する．特徴ベクトル S はハッシュ関数などの不可逆な一方向関

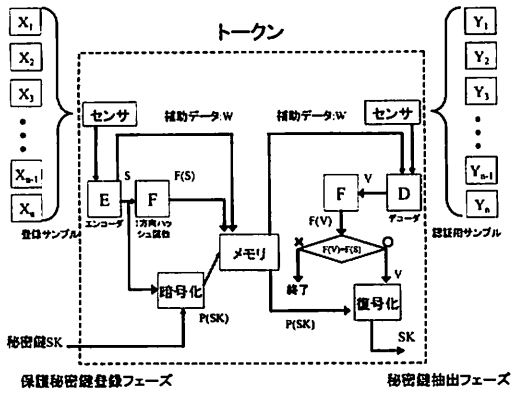

図 3 匿名バイオメトリクスを用いた秘密鍵保管

数 F によって $F(S)$ に変形される．ハッシュ関数を用いることで $F(S)$ から S を推定することを不可能にしている．測定時の雑音による揺らぎによって，単純なハッシュ関数を用いるだけでは登録サンプル X_i と認証用サンプル Y_i とは照合することが出来ない．そのため，揺らぎを含んだ入力から，常に一定の S を生成することが必要となる．そこで，補助データ W を別途生成し，W を用いて認証用サンプル Y のエラー訂正を行うことでデコード結果 V が登録時の特徴ベクトル S と同一のデータとすることが出来る．本提案方式では保護秘密鍵登録時と，秘密鍵抽出時に同一の指紋データを必要とするため，匿名バイオメトリクスの補助データを使った認証用サンプルのエラー訂正の概念を用いる．匿名バイオメトリクスは Fuzzy Vault のように認証時に繰り返し処理を行うことが無いため、トークンにても実用的な処理時間を実現可能であると考えられる．

3. 匿名バイオメトリクスを用いた秘密鍵の暗号化・復元

本章では秘密鍵管理に匿名バイオメトリクスを適用することによって秘密鍵を暗号化して保護秘密鍵を作成，それから秘密鍵を復元する方法を示す．また，トークン型指紋認証システムとの比較を行うことで，今回提案する手法がテンプレート漏洩問題を解決していることを示す．本提案方式は保護秘密鍵登録フェーズと秘密鍵抽出フェーズに分かれており，保護秘密鍵登録フェーズではユーザのバイオメトリクス情報を元に作成した秘密情報を暗号鍵としたユーザの秘密鍵の暗号化をトークン内で行う．秘密鍵抽出フェーズでは保護秘密鍵登録フェーズと同様にユーザのバイオメトリクス情報を元に作成した秘密情報を用いて保護秘密鍵の復号化を行い，秘密鍵の活性化を行う．

3.1 前提条件

今回も出るとして用いるトークンは，バイオメトリクス情報を読み取るための静電容量型指紋センサなどのバイオメトリクス読取装置，登録データである補助データ W と保護秘密鍵 $P(SK)$ を格納するための保管用不揮発性メモリ，およびバイオメトリクス情報のエンコード，ハッシュ関数，暗号化などの演算に必要なメモリと演算機能を有すると仮定する．また，図3において，演算，バイオメトリクス読み込みは全てトークン内で行われるものとする．

3.2 Secret Extraction Codes(SECs)

一般的にバイオメトリクス情報はノイズを含んでいるため，バイオメトリクス情報から常に同一のデータを抽出することは困難である．匿名バイオメトリクスではその問題を解決するために Secret Extraction Code を用いる．$\mathcal{X}$，$\mathcal{Y}$ はそれぞれ雑音路への入力アルファベット，出力アルファベットを，$\mathcal{S}$ は秘密情報集合を表す．このとき，Secret Extraction Code は以下のように表される．

定義 1 (Secret Extraction Code) $n, \epsilon > 0$ として，$\mathcal{X}^n \times \mathcal{Y}^n$ 上に定義される $(n, |\mathcal{S}|, \epsilon)$ はエンコーディング領域 $\mathcal{E}_i \subseteqq \mathcal{X}^n$ とデコーディング領域 $\mathcal{D}_i \subseteqq \mathcal{Y}^n$ の組集合として以下のように表される．

$$\mathcal{C} = \{(\mathcal{E}_i, \mathcal{D}_i) | i = 1, 2, ..., |\mathcal{S}|\}, \tag{1}$$

$i, j = 1, 2, ..., |\mathcal{S}|, i \neq j$ に対して

$$\mathcal{E}_i \cup \mathcal{E}_j = \phi, \mathcal{D}_i \cup \mathcal{D}_j = \phi, \cup \mathcal{D}_i = \mathcal{Y}^n, \tag{2}$$

そして全ての $x_i^n \in \mathcal{E}_i$ と $i = 1, 2, ..., |\mathcal{S}|$ について

$$P_{Y^n|X^n}(\mathcal{D}_i | x_i^n) \leqq 1 - \epsilon, \tag{3}$$

ここで $P_{Y^n|X^n}$ は入力を X^n, 出力を Y^n とするような無記憶雑音路を表す．通常の匿名バイオメトリクスは複数人がバイオメトリクス認証を行う環境を想定しているため，データベース内に $\mathcal{C}$ を格納しており，それぞれの人物がどのエンコード領域，デコード領域を用いてエンコード，デコードを行うかを表すために $\mathcal{C}$ のインデックスを補助データ W とする．しかし，本提案方式ではトークンの所有者のみがトークンに対して認証を行うような環境を想定しているため $\mathcal{C}$ 全体を保存する必要は無い．そこで $\mathcal{C}$ の要素の一つ C を補助データ W として定義する．

3.3 保護秘密鍵登録フェーズ

（1） ユーザのバイオメトリクス登録サンプル $X_i (i = 1, ..., N)$ を測定し，秘密鍵 SK と共にトークンへ入力する．

（2） トークン内で，エンコーダ E は登録サンプル X_i から秘密情報 S と補助データ W を生成する．

（3） 作成された秘密情報 S を暗号鍵として秘密鍵 SK を対称鍵暗号にて暗号化し，これを保護秘密鍵 $P(SK)$ とする．

（4） 照合用の秘密情報のハッシュ値 $F(S)$ を求め，補助データ W と保護秘密鍵 $P(SK)$ と共にメモリ内へ保管する．

（5） 秘密情報 S およびバイオメトリクス登録サンプル X_i を適切な方法を用いてトークン内から廃棄する．

3.4 秘密鍵抽出フェーズ

（1） ユーザのバイオメトリクス認証サンプル $Y_i (i = 1, ..., N)$ を測定し，トークン内へ入力する．

（2） トークン内で，デコーダ D は認証用サンプル Y_i とメモリに保管されている補助データ W から秘密情報 V を生成する．

(3) 秘密情報 V のハッシュ値 $F(V)$ が $F(S)$ と等しければ，V を復号鍵として用いて保護秘密鍵から秘密鍵を復元する．

(4) 秘密情報 V およびバイオメトリクス認証サンプル Y_i を適切な方法を用いてトークン内から廃棄する．

3.5 安全性に関する議論

提案方式は，登録時にはバイオメトリクス情報 $X_i(i = 1,...,N)$ から抽出された秘密情報 S を暗号鍵として，ユーザの秘密鍵 SK を暗号化したものを保護秘密鍵 $P(SK)$ として登録，そして認証時のバイオメトリクス情報の雑音除去のための補助データ W を作成し，秘密情報のハッシュ値 $F(S)$ と共にトークン内に格納する方式である．秘密鍵を使用する際，すなわち認証時にはトークンにバイオメトリクス情報 $Y_i(i = 1,...,N)$ を提示し，登録時のバイオメトリクス情報と十分に類似度が高ければ補助データの作用によって登録時のバイオリクスから抽出できる秘密情報と同一の秘密情報 V を Y_i から抽出する．$F(V) = F(S)$ であれば，保護秘密鍵より秘密鍵の復元が可能となる．

ここで，トークンが盗難された際について安全性の議論を行う．攻撃者は手に入れたトークン内の情報に対して自由にアクセス可能であると仮定する．従って，攻撃者はトークン内のメモリに保管されている補助データと保護秘密鍵を常に利用することができる．

補助データから認証時に利用可能なバイオメトリクス情報の復元，および攻撃に有益な情報を得る攻撃について考える．匿名 バイオメトリクスの条件より [3]，補助データと登録時のバイオメトリクスの相互情報量は限りなく 0 に近い値になる．そのため，攻撃者が補助データから認証に利用可能なバイオメトリクス情報を復元，さらには攻撃の際に有益な情報を入手することは不可能である．

次に，保護秘密鍵から秘密鍵の復元，および推測を行う攻撃について考える．本提案方式は，バイオメトリクス情報から登録時には秘密情報 S を抽出して秘密鍵を暗号化，秘密鍵復元にはバイオメトリクス情報から秘密情報 V を抽出して複号化する方式である．この暗号化，復号化は共通鍵暗号方式を用いて行われる．従って，保護秘密鍵から秘密鍵を復元するには秘密情報 S の復元が必要となる．この対策としては，S の情報量を十分に確保することが挙げられる．しかしながら，指紋から抽出可能な情報量は高々数百ビットとなっているため，総当り攻撃によって $F(S) = F(V)$ となるような S を探し当てられる可能性は十分に考えられる．そこで，ハッシュ関数 $F()$ については耐タンパー性を考慮する必要がある．

また，補助データと攻撃用の任意のバイオメトリクス情報から認証可能な，すなわち正規のユーザが保護秘密鍵登録フェーズで登録したバイオメトリクス情報と同一のバイオメトリクス情報を復元するには，攻撃用のバイオメトリクス情報と保護秘密鍵登録時のバイオメトリクス情報に十分な類似度が無ければならない．これは，類似度を閾値として適切な値を設定することでこのような攻撃に対応することができると考えられる．さらに，一定回数連続で認証に失敗した際にはバイオメトリクス認証を停止させる措置をあわせることで，高い確率で攻撃を防ぐことができる．攻撃者は入手したトークンに任意のバイオメトリクス情報を提示することによって認証を成功させることはほぼ不可能である．

	テンプレート漏洩	格納する情報
提案方式	無し	保護秘密鍵 補助データ 秘密情報 S のハッシュ値 $F(S)$
既存方式	問題あり	テンプレート 秘密鍵などの秘密情報

表 1 テンプレート漏洩問題，格納される情報の比較

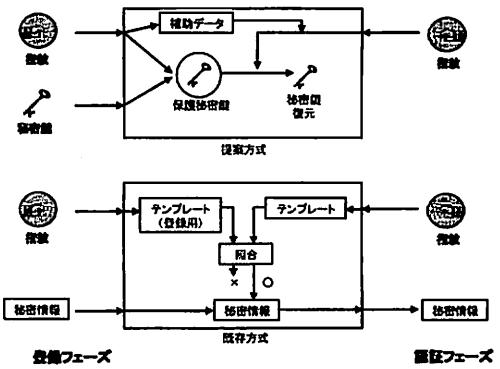

図 4 既存方式と提案方式の動作内容の比較

3.6 指紋認証トークンシステムと提案方式の比較

既存方式である指紋認証トークンシステムは，トークン内に認証用のテンプレートと，パスワードなどの秘密情報を格納する．秘密情報を使用する際には認証用のテンプレートとトークン内に格納してあるテンプレートの照合を行い，類似度が十分に高ければ秘密情報をトークン外に出力する方式であった．

提案方式においてトークン内のメモリに保管される情報は補助データと保護秘密鍵のみである．補助データから認証に利用可能なバイオメトリクス情報を復元することは不可能である．保護秘密鍵の作成には，秘密鍵を平分とみなし，秘密情報 S を用いて暗号化を行う．S は保護秘密鍵作成後にはトークンから廃棄されている．従って，S が十分な情報量を持つ限り，保護秘密鍵から秘密鍵の復元は不可能であると考えられる．

指紋認証トークンシステムにおいてトークン内に保管される情報は認証用のテンプレートと秘密鍵やパスワードなどの秘密情報である．トークン内の情報にアクセス可能な攻撃者からは直接使用可能な秘密情報，人工バイオメトリクス作成のためのテンプレート情報が漏れてしまうだろう．提案方式では内部情報単体から認証可能なデータや秘密鍵の復元が不可能であるため，テンプレート照合型のバイオメトリクス認証において生じる，テンプレートの漏洩問題が発生する可能性はない．トークン内部の情報から認証可能であるような人工バイオメトリクスが作成されることは無いと言える．表 1 にテンプレート漏洩問題，格納される情報についての比較，および図 4 に提案方式と

既存方式の動作内容の比較を記す.

4. 具体的な運用方法

これまでに匿名バイオメトリクスを用いる事によって，トークンを用いた秘密鍵管理を提案した．トークン内には秘密鍵から作成した保護秘密鍵と，バイオメトリクス情報を修正するための補助データを格納し，秘密鍵を使用する際には保護秘密鍵とバイオメトリクス情報から秘密鍵を復元することができる．さらに，指紋認証トークンシステムと提案方式を比較することによって，従来手法のようにテンプレートの照合を行うことが無いため耐タンパー性に依存することなくテンプレートの漏洩による秘密鍵の危惧化が無いことを示した．

本章では提案方式が現在 PKI の提供する暗号化・署名・認証に適用可能であることを示す．

4.1 提案方式を用いた PKI における暗号化

公開鍵暗号方式では，全体に公開する公開鍵と公開せず自分だけが所有する秘密鍵が存在し，それぞれを暗号鍵，複号鍵のどちらにも用いることが出来る．例えば，公開鍵でデータの暗号化を行うことで，その公開鍵と対なる秘密鍵を所有する人物にしか復号することの出来ない暗号文を作成することが出来る．逆に，秘密鍵でデータの暗号化を行い，その暗号文を対になる公開鍵で復号することが出来れば，暗号文の作成者は，公開鍵とついになる秘密鍵の所有者であるということを証明することが出来，この技術はディジタル署名に用いられている．また，秘密鍵がトークン内に格納されている状態であるため，暗号化をトークン内部で行うのか，トークン外へ秘密鍵を配送し，外部で暗号化や複号化の処理を行うかの選択が必要である．本節では，どちらの鍵を暗号化・復号化に用いるのか，さらにトークンの内外どちらで処理を行うのかの場合に分けて，用途に合った使用法を検討する．

- 秘密鍵を復号鍵，公開鍵を暗号鍵としてトークン内で処理

始めにトークンへ公開鍵を用いて暗号化した暗号文を入力し，トークンに指紋を提示し保護秘密鍵から秘密鍵を抽出後，複号化する．復号後，秘密鍵を安全な方法でトークン内から消去する．一般的にトークンの処理することの出来る暗号文のサイズや処理速度は限られているため，暗号文のサイズが大きい場合には不向きであると考えられるが，秘密鍵がトークン内から出ないので秘密鍵保護の観点からすると優れているといえる．

- 秘密鍵を暗号鍵，公開鍵を復号鍵としてトークン内で処理

まず，暗号化したいデータをトークン内で生成するか，外部からトークン内へ入力する．その後，トークンに指紋を提示し，保護秘密鍵から秘密鍵を抽出後，データの暗号化を行い，秘密鍵を安全な方法でトークン内から消去する．暗号文は公開鍵を持つユーザへ送信される．トークン内での処理のため，データのサイズは制限されるが，秘密鍵がトークン外へ出ないため，秘密鍵が外部に漏れる危険性は少ない．

- 秘密鍵を復号鍵，公開鍵を暗号鍵および秘密鍵を暗号鍵，公開鍵を復号鍵としてトークン外で処理

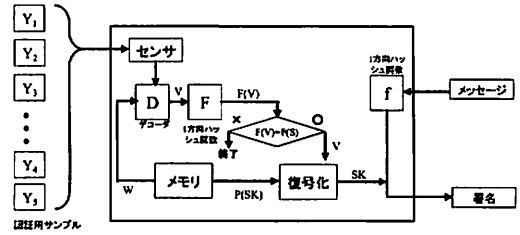

図 5 提案方式を用いた署名作成

扱うデータが膨大で，トークンの処理能力では秘密鍵を用いての暗号化や復号化が困難である場合，トークン外部にて秘密鍵を用いたデータの暗号化や複号化を考えるかもしれない．その際トークン外でデータの処理を行うため，トークンへ指紋を提示し保護秘密鍵から秘密鍵を抽出した後，復号鍵である秘密鍵をトークン外へ出力しなければならない．このように秘密鍵がトークン外部へ出てしまう場合，秘密鍵が漏洩する危険性が非常に高まってしまう．秘密鍵をトークン外へ出すことは好ましくないといえるだろう．

以上，それぞれの場合について例を挙げて考察を行ったが，秘密鍵を復号鍵，公開鍵を暗号鍵および秘密鍵を暗号鍵，公開鍵を復号鍵としてトークン外で処理する場合は秘密鍵が漏洩する危険性が高いが，トークン内で処理を行う限り秘密鍵の漏洩の危険性は少ないということがわかった．

4.2 提案方式を用いたデジタル署名

提案方式に公開鍵暗号アルゴリズムを備えることで，トークン内にて一般的な方法と同様に署名生成を行うことが出来る．署名したいメッセージにハッシュ関数を適用し，メッセージのダイジェストを生成する．ユーザはトークンへ指紋情報を提示することで保護秘密鍵から秘密鍵を抽出し，ダイジェストを秘密鍵を用いて暗号化し，署名を生成することが出来る．この際，暗号化を行った後は速やかに秘密鍵を安全な方法で廃棄しなければならない．その後，トークンから署名と，対応するメッセージが出力される．図 5 は匿名 バイオメトリクスを用いて保護秘密鍵を登録したトークン内での署名生成の過程を図式化したものである．ここで，メッセージのダイジェストを生成するためのハッシュ関数を f とする．トークン内での署名生成の過程を図 5 に示す．

4.3 提案方式を用いた認証

まず，ユーザは認証を行わなければならないシステムに始めにアカウントを作成する際に，パスワードを自分の秘密鍵で暗号化した暗号文を渡すものとする．システム n への認証に用いるパスワードを PW_n とし，それを公開鍵を用いて暗号化した暗号文を $PK(PW_n)$ とする．システム n はユーザの暗号文 $PK(PW_n)$ を保管する．ユーザがシステムに認証を行う際には，ユーザはシステムに保護秘密鍵を登録したトークンを接続し，システムに保管されてある暗号文 $PK(PW_n)$ へアクセス後，$PK(PW_n)$ をトークンへ入力する．その後，ユーザはトークンに対し認証用指紋サンプルを提示し，保護秘密鍵から秘密

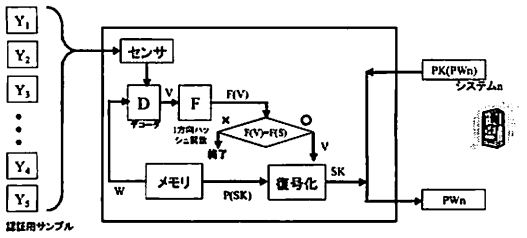

図 6　提案方式を用いた認証

鍵 SK を復元する．トークン内で秘密鍵 SK を用いて暗号文 $PK(PW_n)$ を復号化する事でユーザは PW_n を得ることが出来，そのまま PW_n をトークンからシステムへ出力するだけでユーザの認証は終了する．$PK(PWn)$ の復号後，秘密鍵 SK は安全な方法で廃棄されるものとする．ここで，認証用指紋サンプル Y_i が保護秘密鍵登録時に提示したサンプル X_i と十分に一致していなければ秘密鍵 SK を復元することは出来ないため，他人によるなりすましの認証が起きる事はない．図 6 に認証までの過程を示す．

5. まとめと今後の課題

本論文では秘密鍵管理のため，匿名バイオメトリクスを用いたトークン型秘密鍵管理方式を提案し，その安全性について議論し，従来方式に見られるようなテンプレート漏洩問題を解決した．さらに，PKI の提供する暗号化・署名・認証機能に適用可能であるかの検討を行った．今後の課題として，安全性の評価および計算量の評価が挙げられる．

文　献

[1] 首藤・重松・羽田野・山口・岡崎・町田，" 指紋認証トークンシステム，" NTT 技術ジャーナル 2003.12，pp43-46

[2] ソニー指紋認証システム，http://www.sony.co.jp/Products/puppy/

[3] Tuyls P.,Goseling J.，" Capacity and examples of template-protecting biometric authentication systems，"ECCV Workshop BioAW,no.77，2004

[4] International Biometric Group，" Generating Images from Templates，" I.B.G. White Paper，2002

[5] Hill C.J.,，" Risk of masquerade arising from the storage of biometrics，" Bachelor thesis，Dept. of CS，Australian National University，2002

[6] Juels, A., Sudan, M., "A fuzzy vault scheme," IEEE International Symposium on Information Theory (2002) 408

[7] Uludag, U.,Pankanti, S., Jain., A. "Fuzzy vault for fingerprints" Proceeding of International Conference on Audio- and Video-Based Biometric Person Authentication (2005) 310-319

[8] Hyung-Woo Lee, Geun-Shik Han, Suung-Hyun Yuun, Haeryong Park, "Biometric Digital Signature Key Generation and Management Framework for Fingerprint", JWIS 2006

[9] Alisher Kholmatov, Berin Yanikoglu, "Biometric Cryptosystem Using Online Signatures", The 21st International Symposium on Computer and Information Sciences Novenverr 1-3, 2006