バイオメトリクスを利用した鍵更新
～効果的な鍵漏洩問題対策～

山中 晋爾
情報理工学系研究科 電子情報学専攻

1　はじめに

様々な場面においてIT化が進む今日において，情報セキュリティの重要性が高まってきている．いまや，大学や企業の大型コンピュータはもとより，パーソナルコンピュータや携帯電話のみならず，家電製品までもがインターネットに接続されるようになっている．このような背景において，通信内容の完全性 (改ざんされていないことを保障する)・秘匿性 (盗聴に対してロバストである)・本人性 (通信相手が認証されている相手である) などが必要とされている．こうした中，指紋や虹彩といった生体情報をセキュリティ，とくに本人認証，に対して応用する，いわゆるバイオメトリクス (biometrics) 技術が注目を浴びている．

バイオメトリクスは，大きく分けて身体的特徴 (physiological characteristics) もしくは身体的特性 (behavioral characteristics) の２つに分類できる。身体的特徴の代表例としては指紋、網膜あるいは顔等が挙げられ、身体的特性の代表例としては、筆跡、音声等が挙げられる。前者の身体的特徴は，不変的なものであり，かつ他者と同一である可能性が稀であることを利用している．一方，後者の身体的特性も，声紋や個人の癖といったものを特徴点として用いる．そして長年の研究成果により，バイオメトリクスは本人確認の手段として，その有効性が確認されている．

さらに，このバイオメトリクスを公開鍵暗号系の秘密鍵の代わりに利用する方法も提案されてきている．すなわち，受信者の公開鍵で暗号化されたメッセージは，受信者がバイオメトリクスを用いて生成した秘密鍵を利用しないと復号できない，という方式である．もともと，バイオメトリクスは本人以外の第三者がまねすることができないものであるから，このアイディアは理にかなったものである．そして同時に，前述した完全性・秘匿性をも維持することが可能となる．しかしながら，この方式には秘密情報の漏洩に脆弱である，という公開鍵暗号系がもともと内包している弱点も受け継いでしまっている．

そこで本報告では，バイオメトリクスを利用して秘密鍵を更新するという方式を提案し，またその実現方法について述べる．

2　提案方式の概要

前節で述べたとおり，バイオメトリクス情報を基にした秘密情報を秘密鍵として利用する方法は既に提案されている．しかしながらそれらの方式では，秘密鍵 (もしくは秘密情報) は漏洩しないことが前提となっており，それが攻撃者に漏れてしまえば，暗号システムそのものが破綻してしまう．その場合，公開鍵失効リストに漏洩した秘密鍵に対応する公開鍵を登録し，新たに公開鍵/秘密鍵ペアを生成した上で，鍵の更新を送信者に通知する必要がある．そしてこれは，正当な秘密鍵の所有者や，公開鍵利用者，つまり送信者の負担が大きい．

これに対して，提案方式は次のような仕組みで動作する．ユーザは普段暗号文を復号するのに利用するモバイル端末に，ある期間だけ有効な秘密鍵 K_{s_i} を入れておく．この端末は，常に外部からの攻撃にさらされており，秘密鍵が第三者に漏洩する可能性がある．また，ユーザの秘密鍵は自身のバイオメトリクスを用いた場合のみ，更新することが可能となる．この更新はある期間ごとに，必ず行われるものとする．以下では，提案方式を構成するアルゴリズムについて概説する．

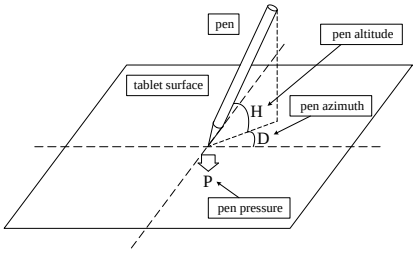

図 1: オンラインペン入力情報

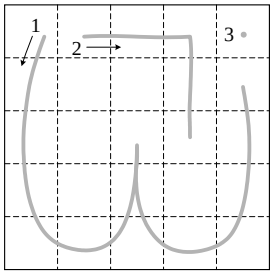

図 2: グラフィカル・パスワード

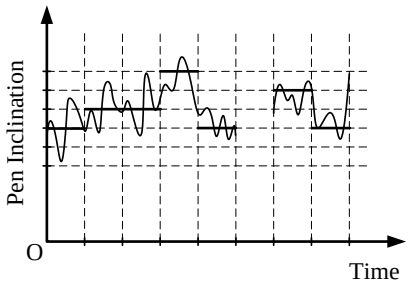

図 3: 方位データの例

バイオメトリクス鍵生成: ユーザは本人のバイオメトリクス情報およびグラフィカル・パスワードを利用して，本人固有の秘密情報を生成する．この秘密情報は,「初期鍵ペア生成」および「鍵更新情報作成」を行う場合に用いられる．

初期鍵ペア生成: ユーザのバイオメトリクスを元にある秘密情報を生成する．そしてこの情報を元にしてユーザの公開鍵 K_p と期間 0 の秘密鍵 K_{s_0} を生成する．

鍵更新情報作成: 安全な場所において，ユーザのバイオメトリクスを元に秘密情報を生成する．この情報を元にして鍵更新情報 D_{ku_i} を生成する．作成された D_{ku_i} は，安全な通信路を用いてユーザの端末に送信される．

秘密鍵更新: ユーザの端末は，送られてきた更新情報 D_{ku_i}，および古い秘密鍵 $K_{s_{i-1}}$ を元に，新しい秘密鍵 K_{s_i} を生成する．その後，新しい鍵の生成に用いられた D_{ku_i} および $K_{s_{i-1}}$ は削除される．

暗号化: メッセージの暗号化には，公開鍵 K_p を利用する．このとき送信者は，今，秘密鍵がどの期間 (K_{s_i} の i) のものであるかをあらかじめ知っているものとする．

復号: メッセージの復号には，秘密鍵 K_{s_i} を利用する．ただし，K_{s_i} と K_p が対となる鍵であり，メッセージを暗号化する際に入力された期間番号 j と i が一致している場合にのみ復号が成功する．

提案手法ではバイオメトリクスデータとして，身体的特性であるオンライン筆記データを利用する．身体的特徴のタイプのバイオメトリクスを用いない理由は，指紋や虹彩のデータが漏洩したときに秘密情報を変更できないためである．このデータは，図 1 に示すようなタブレットから入手する．タブレットからは 3 グループ・5 種類のデータが得られる．すなわち，タブレット平面上の x 座標および y 座標，筆圧 P，ペンの傾き情報である方位 D および高度 H である．

ここで，x, y 座標をグラフィカル・パスワードとして用いることを考える．グラフィカル・パスワードとは，図 2 に示すように，筆記平面をある大きさの区画で区切り，どのマスをペン先が通過したかにより，その経路をパスワードとして用いる手法である．ただし，どのような筆記を行うか，筆記の経路は攻撃者に知られないことを仮定しておく．

残りの筆圧，方位，高度のデータには，本人の筆記時の癖により個人的な特徴が現れやすい．そこで，それぞれのデータから個別に秘密情報を生成する．そして，最終的にはグラフィカル・パスワード，筆圧，方位，高度のデータから秘密情報を生成し，これをバイオメトリクス鍵として用いる．

3 おわりに

本報告では，バイオメトリクスを利用して秘密鍵の更新を行う，新しい公開鍵暗号方式を提案し，その実現方法を示した．今後の課題としては，手書き署名など本人が書き慣れたものを用いたときに秘密情報の生成が可能かどうかの検討，また生成された秘密情報のばらつき具合 (ランダムネス) の評価手法の考察などがあげられる．