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

2003－CSEC－23 (14)
2003／12／19

二次元バーコードを用いた公開鍵署名による郵便物認証

鈴木敬嘉，宇田隆哉，伊藤雅仁，市村哲，田胡和哉，星徹，松下温

現状では、郵便において送り主を認証することは困難である。送り主を特定するために、郵便物にホログラム印刷が用いられることがあるが、印刷費が高くプリンタも特殊なもので、個人が容易に利用できるものではない。近年普及してきている非接触型ＩＣカードの内部データ確認のためにはデジタル署名が利用されており、送り主の認証にもデジタル署名を利用できると考えられる。しかしＩＣカードとは異なり紙媒体ではバイナリデータをそのまま利用することはできない。そこで本論文では、紙媒体においてバイナリデータを表示可能な手段のうち単位面積当たりの表現可能なデータ量の多い二次元バーコードを利用し、安全な郵便の利用法を提案する。

Authentication of postal matters with public key signatures using 2-D barcode

Takayoshi Suzuki, Ryuya Uda, Masahito Ito, Satoshi Ichimura, Kazuya Tago, Tohru Hoshi, Yutaka Matsushita

Now it is difficult to authenticate a sender of a postal matter. In some cases holography printing is used, but it is costs a lot of money. Something like holography printing can be available by using only some special printers. We took notice of digital signature that used to authenticate IC card. It can also be used to authenticate a sender of a postal matter. We propose the safe use of the post using QR code that includes so much data expressed on paper.

１．はじめに

１．１　背景

現状では、郵便において送り主を認証することは困難であり、通常、その内容（文面、品物）から判断している。内容に依存せずに送り主を特定するためは、郵便においてホログラム印刷が用いられることがある。しかしホログラム印刷は加工費が高い。プリンタを用いてホログラム印刷に近いものを作成することも可能であるが、プリンタ自体が特殊なもので個人が容易に利用できるものではない。近年普及してきている非接触型ＩＣカードの内部データ確認のためにはデジタル署名が利用されており、送り主の認証にもデジタル署名が利用できると考えられる。しかしＩＣカードとは異なり紙媒体ではバイナリデータをそのまま利用することはできない。そこで、本論文では、紙媒体においてバイナリデータを表示可能な手段のうち単位面積当たりの表現可能なデータ量の多い二次元バーコードを利用し、安全な郵便の利用法を提案する。

東京工科大学コンピュータサイエンス学部松下研究室
Tokyo University of Technology Matsushita Lab.

１．２　郵便配送におけるコードの利用

葉書や封書は郵便情報を基に配達局で区分機によって住所表示番号を抜き出され、郵便番号と住所表示番号の情報が局内バーコードという形で無色のインクにて印字される。区分機が読み取れない場合は人が目視することにより読み取れなかった部分を入力し、ＩＤバーコードを無色のインクで印字する。配達順はバーコードの情報を元に決定される。局

内バーコードやＩＤバーコードの生成を省略するため、送り主が（郵便）カスタマーバーコードと呼ばれるものを印字することが推奨されている。

住所表示番号を得るアルゴリズム及びバーコードの規格は日本郵政公社によって公開されている。規格どおりにバーコードを印字して配送に出すと、郵便料金が割引される。これは葉書および封書の一部において利用可能であるが、枚数に制限があるため個人が利用することはあまりない。

しかし、カスタマーコードは郵便において規格化された仕様であり、区分機は画像認識、カスタマーコードどちらかの利用を必須としているため、本研究においてもカスタマーコードの利用を想定して認証を行っている。

１．３　郵便における問題点、解決策

葉書、封書は個人が住所や氏名を印刷して投書しているが、小包等では専用のプリンタを利用せねばこれを印刷することは困難である。

また郵便は安全を確認することができない。例えば、知人からのみ郵便物を受け取るとは限らず、知人から郵便物が届いたとしてもそれは本当に本人によって出されたものであるのか確認するすべがない。もし、届いた郵便物が信頼できる相手から送られて来た物であると確認できるならば、それは安全であるといえるだろう。そこで本論文では、差出人を特定するために、公的機関での利用も進んでいるデジタル署名を使用し、差出人確認をする手法を提案する。

デジタル署名を利用するにあたり、一般に普及している一次元のバーコードでは、限られた紙面積中に署名を表すために必要な情報量を得ることは困難である。そこで、本研究では単位面積当たりの情報量が比較的多い二次元バーコードを利用して、署名、郵便情報を表示している。現状の郵便と互換性を持たせるためにカスタマーコードを利用し、これにデジタル署名を付加することで、郵便をより安全かつ便利にすることが本研究の目的である。また小包等では、フロッピーディスクに郵便情報を入れて郵便局に持参すると、その情報を基に郵便を利用できるというサービスもあることから、バーコードを読み取る端末は必要になるが、個人利用においても本手法は抵抗なく受け入れられると考えられる。

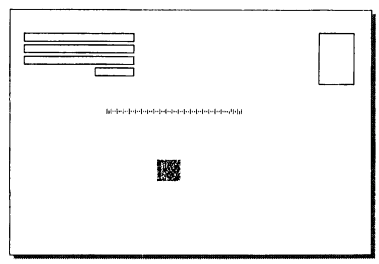

図１　二次元バーコードつき郵便イメージ

２．提案

1.3 節で述べた認証手法を実現するには、印字されたバーコードの内容を人間が容易に確認できる仕組みと、デジタル署名を個人が簡単に認証できる仕組みが必要である。文字の場合と異なり、バーコード印字された情報を人間が目で見て内容を読みとるのは困難であり、デジタル署名の確認には何らかの認証デバイスが必要である。そこで本研究ではバーコードを読み取る端末に携帯電話を用い、署名を検証し署名の真偽を返す Web サーバと連携し認証を行うシステムを構築した。携帯電話は一般の PC に比べて演算性能も低く、データを格納するメモリ領域も小さく、機種による機能の差異も大きいことから、携帯電話端末だけに署名検証に必要なアルゴリズム、データ量を格納することは現実的ではないと考え、携帯電話においてもはや標準実装となっているウェブ通信機能を生かし、本研究で

はウェブサーバ側で署名検証を行っている。

2．1　情報入力部

二次元バーコードを利用する上で重要なのは利用するコードの規格である。海外（主に米国）ではPDF417[1]が普及しているが、日本ではＱＲコード[1]が普及している。専用バーコードリーダではレーザ光の反射をセンサーで読み取ることにより、バーコードの位置を特定しバーコードの規格に基づき情報を読み取っているが、本研究の実装では専用のリーダを用いず、携帯電話付属のカメラからバーコードを画像として取り込んで認識し、情報を取り出している。市販の携帯電話の中にはＱＲコードを認識できる物もあり、今後の普及も見込まれているため、採用した。このシステムは Java を用いて実装しており、バーコードから読みとったデータのうち、送り主の情報を分離してサーバに送信している。

図2　二次元バーコードの種類

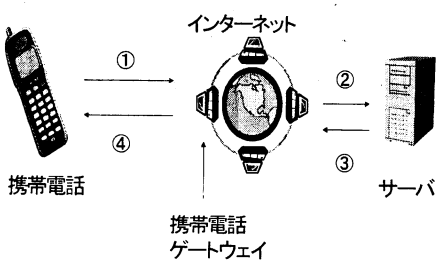

図3　ネットワーク概要

2．2　入力及び表示部・サーバ間

デジタル署名の検証はメモリ容量、処理速度から考えると携帯電話で行うことは難しい。また携帯電話では外部ネットワークとの通信手段が PC と比較して制限されている。ネットワークを用いた外部機器との接続は赤外線インターフェースとインターネット（HTTP,HTTPS）が標準的に利用可能である。本研究ではインターネットを通じてサーバ側に送り主のコード情報と署名を送る際、機種の互換性を考慮してHTTPプロトコルを利用して実装しているが、セキュリティ面を考えるとHTTPSでの実装が望ましいといえる。

2．3　サーバ側処理

サーバは、署名と送り主の情報を受け取り、サーバに保存されている公開鍵で署名部を検証し、その結果を端末に送信する。

署名アルゴリズムは ECDSA（楕円曲線暗号）[2]を用いた。これは、160 ビットの署名長で RSA[2]の 1024 ビット署名と同等の強度があるとされており、比較的リソースが限られている場面に適していると判断したためである。

署名は Base64 変換[2]されバーコードに付加される。サーバは変換された署名を受け取り、Base64 逆変換[2]で署名を復元し検証し、認証情報の真偽を携帯電話端末に返す。

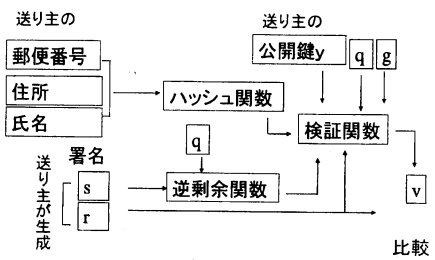

図4　署名アルゴリズムの概観

2．4　表示部

表示部では読み取ったバーコードの情報とサーバから送られてきた署名の検証結果を表示する。

3．評価

3．1　バーコード情報

HTTPを用いてCGIで実装するには、バイナリデータの扱いに注意する必要がある。

署名がバイナリデータのままでは、「+」や「&」記号が含まれることがあり、CGIで受信ミスとなる可能性があるためBase64変換を利用している。なお、Base64においても「+」記号を使用するため、さらにこれを他の文字に置き換えている。160ビットの署名をBase64変換すると、平均で460ビット程度となり、これは英数字で60文字程度となる。ＱＲコードでは独自の圧縮方式により英数字2文字を11ビット、漢字1文字を13ビットで表すことが可能であり、今回実装に使用した携帯電話においては認識可能なＱＲコードの最大容量は2168ビット（バイナリモード8ビット×271文字，ＱＲコード，モデル2，バージョン10，訂正レベルL）であったため、署名自体に約330ビット使用し、残りを郵便情報に割り当てている。残りが1800ビットであれば漢字で約130文字であり、これは郵便の利用において十分であると考えられる。実装においては、送り主、受け取り主の氏名、7桁郵便番号、郵便番号以下の住所、バーコードの作成日、送り主の郵便情報に対して署名を生成している。

3．2　署名検証

署名検証では、サーバはメッセージ、署名、公開鍵を受け取りその真偽を返す。

署名アルゴリズムはECDSA（フリーライブラリより）を使用している。署名を行うデータは署名時にSHA-1を用いて160ビットハッシュ値にし、署名を生成している。署名はハッシュ値より生成されるため、入力するデータ量の制限は、バーコードの表示スペースおよび読み取り可能範囲に依存する。

3．3入力及び表示部

バーコードの読み取り部、バーコード情報・検証結果の表示部は携帯電話対応のJavaで実装した。Javaは今後も携帯電話に標準的に実装されてゆくと考えられる。

4．結論

現状では、郵便物の送り主の認証は難しく、費用もかかる。本研究で開発したシステムを用いれば、普及している携帯電話を用いて一般の利用者が簡単に郵便の送り主を認証することが可能である。また、現在の郵便の区分機に使用されているカスタマーコードを用いることで、既存の郵便との互換性を維持している。本研究は既存システムとの融合を図り、強固な公開鍵署名を用いて簡易に郵便物の認証が行えるという点で、郵便の安全性向上に寄与できると考えられる。

参考文献

[1]二次元コードHandBook
http://www.keyence.co.jp/barcode/download/download_tech.html
[2] ディジタル署名と暗号技術：安全な電子商取引のためのPKI（公開鍵基盤）、セキュリティシステム、法律基盤　ウォーウィック・フォード，マイケル・バウム著；山田慎一郎訳　ピアソン・エデュケーション 2001年