UC San Diego Computer Science technical report UCSD-TR-CS96-485

DESIGNING CRYPTOGRAPHIC POSTAGE INDICIA

J. D. TYGAR
Carnegie Mellon University
Computer Science Dept, 5000 Forbes Ave, Pittsburgh PA 15213, USA

Bennet YEE
University of California, San Diego
Dept of Comp Sci and Eng, 0114, La Jolla, CA 92093, USA

Nevin HEINTZE
Bell Laboratories
600 Mountain Ave, Murray Hill NJ 07974, USA

Abstract

We apply cryptographic techniques to the problem of fraud in metered mail. We describe a mail system that combines off-the-shelf barcode technology, tamper-proof devices, and cryptography in a fully-integrated secure franking system. This system provides protection against:

1. Tampering with postage meters to fraudulently obtain extra postage;
2. Forging and copying of indicia;
3. Unauthorized use of postage meters; and
4. Stolen postage meters.

We provide detailed justification for our design, and discuss important tradeoffs involving scanning strategies, encryption technology and 2-D barcode technology. The US Postal Service' recent Information Based Indicia Program (IBIP) announcement adopted the principal design features of our model.

An earlier version of this paper appeared in Securicom '96.

1 Motivation

The US Postal Service[1] handles over 165 billion pieces of mail each year through almost 40,000 autonomous post office facilities. Much of this mail is metered, which means that the mail does not have an ordinary stamp attached to it. Instead, a postage meter prints a special mark (called a postal indicia) on the mail. Fraud is a serious problem for the US Postal Service:

- The US Postal Service recently calculated that meter fraud cheats the agency out of substantially more than $100 million each year [4].
- There are over 82,000 postage meters in the US that are currently reported as lost or stolen [14].
- The US Postal Service is prosecuting two cases in New York and Boston; each involves more than $4 million dollars in postage meter fraud [11].

To address these problems, we propose a new system for printing postage indicia with cryptographic information. This system allows a PC or workstation with a laser printer and a tamper-proof device to produce unforgeable postage indicia. This paper describes that design.

The design of cryptographic postage indicia is an interesting exercise in security engineering. The US Postal Service's recent Information Based Indicia Program (IBIP) [13] adopts the principal design features of our model.

2 Postal Fraud

Today's postage meters and indicia are not very secure. They are vulnerable to at least four kinds of fraud:

- The postage meter may be tampered with so that it generates free postage;
- The indicia imprint produced by a postage meter may be forged or copied, using a rubber stamp, a color photocopier, or a color laser printer.
- A valid postage meter may be used by an unauthorized person; and
- A postage meter may be stolen.

A number of these issues can be addressed by cryptography. Thanks to recent developments in digital barcoding, we can now use off-the-shelf technology to replace old-fashioned stamps by machine readable indicia. These indicia can be printed by laser printers or similar devices, under the control of a workstation, a PC, or a dedicated postage device. Moreover, we can include cryptographically signed information in the indicia to prove the authenticity of the indicia. By including information such as the mailing date and the zip code of the sender and receiver, we can also guard against forged or copied indicia. Pastor [8] gave a rough outline of how such a system could work.

Unfortunately, Pastor's system and similar proprietary proposals are vulnerable to additional types of attack:

[1] This paper addresses mail in the United States, but the basic design can be generalized to mail in other countries.

- Cryptographic techniques are vulnerable to misuse, leading to systems that can be successfully attacked by an adversary.
- Postage meter credit may still be tampered with, even if cryptographic techniques are used.
- A postage meter may be opened and examined by adversaries looking for cryptographic keys, thus allowing the adversary to build new bogus postage meters.

Even more problematic, Pastor's proposal relies on an implicit assumption that a master list containing all examined indicia is maintained. This would require a large, distributed database on a highly available network connecting post office facilities. With nearly 40,000 postal facilities and a yearly volume of 165 billion pieces of mail, such an integrated, real-time, distributed, highly-available database would be unrealistic at present without dramatically increasing the cost of postage.

This paper describes a complete postal franking system addressing these concerns. This system is most suitable for a PC or workstation printing out cryptographic indicia on a standard laser printer. A slightly less secure design also allows postal meters to print out cryptographic indicia. Central to our design is the use of tamper-proof computing devices, such as those in the specified in the US FIPS 140-1 standard [6]. Using this technology, we can produce secure, unforgeable postal indicia.

3 Traditional Indicia

Here we review the structure of traditional indicia and define necessary properties for cryptographic indicia.

Today's postage meters are portable devices containing a print mechanism and a postage accounting mechanism, enclosed in a sealed case. Each postage meter is initialized with a postage credit by a post office; as each letter is stamped, the postage value is deducted from the machine's credit. Meters are periodically returned to the post office so that additional postage credit may be transferred to them. Although postage meter cases are not tamper-resistant or tamper-proof, they are supposed to be tamper-evident. Meters are subject to periodic inspection by postal authorities. Unfortunately, the tamper-evident mechanisms frequently fail. Further problems are created by stolen or missing meters, which cannot be inspected but may be in use. Finally, postal employees often fail to recognize signs of tampering.

Traditional postage meters maintain three important *registers*:

ascending register The monetary total value of all indicia ever produced by this meter.

descending register The remaining credit available in the meter.

piece-count register The number of indicia with non-zero postage produced by the meter[2].

When a new indicia is printed by a meter, the postage value of the new indicia is added to the ascending register and subtracted from the descending register, and the piece-count is incremented by one. During normal operation, the ascending and descending registers sum to a constant value. When the meter is refilled and additional postage credit is transferred to a meter, the sum of the ascending and descending registers increases.

[2] Zero postage indicia are sometimes used for testing.

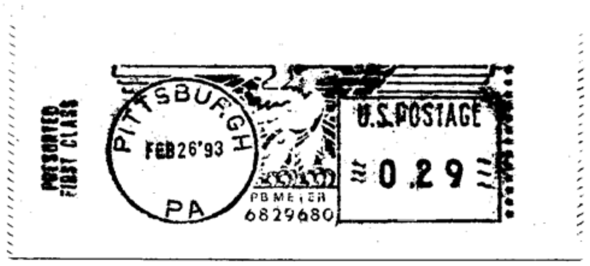

Figure 1: Traditional indicia can be easily forged or reproduced by a laser printer.

Figure 1 shows an example of a traditional indicia. It contains information about postage value, date, etc. On the left side of the indicia are the words "Presorted First Class" printed vertically, identifying the class of the mail. Immediately to the right is the city-state circle, which notes the city (Pittsburgh), state (Pennsylvania) and the date (26^{th} February, 1993) of the indicia. Further to the right, and directly underneath the eagle, is a meter identification mark (PB METER 6829680). This indicates that the imprint was made by a Pitney-Bowes meter, serial number 6829680. Finally, in the box on the right-hand end of the indicia is the postage value (29 cents).

The basic function of an indicia is to demonstrates to the postal carrier that postage has been paid. To make copying more difficult, the indicia is printed using special fluorescent ink. However ink fluorescence is rarely checked, and in any case fluorescent ink is openly sold without restriction. Moreover, rubber stamps that produce bogus indicia can be easily special ordered. So, little sophistication and little investment is required to defeat the traditional postal indicia security measures.

4 Cryptographic Indicia

Using cryptography, we can design postage indicia that substantially improve upon the security of traditional postage meter indicia. In particular, we can guarantee the following two properties: (a) copied indicia are detectable and (b) malicious users cannot generate valid new indicia (even by modifying existing indicia).

We achieve the first property by including additional information in indicia: the destination, sender, and return address of the mail, and the date/time of creation of the indicia. Such indicia can be copied, but since the destination address is included in the indicia, the copied indicia is only valid for mail to the same address. As we shall discuss later, this check can be automated. The inclusion of time stamps allows us to set a maximum "lifetime" for an indicia. Serial numbers trace the source of the attack to a unique postage meter licensee.

The second property is achieved using cryptography. Indicia information is digitally represented, cryptographically signed [12], and printed on an envelope as a 2-D barcode[3]. Such barcodes can be printed using commodity laser printers, and they can be scanned

[3] In addition to the 2-D barcode, the envelope will contain human-readable versions of some information, such as the postage value, and addresses.

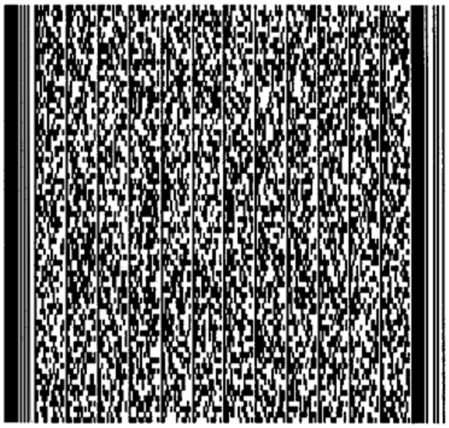

Figure 2: PDF417 barcode representation of The Gettysburg Address

and re-digitized at a post office. Several 2-D barcode technologies exist; figure 2 shows Lincoln's Gettysburg Address encoded in Symbol Technologies PDF417 barcode [3, 9, 10]. PDF417 can store 400 bytes per square inch.

Central to the security of cryptographic indicia is checking indicia validity. Section 5 addresses this important issue.

5 Indicia Design

What type of cryptographic signature algorithm should we use? Most cryptographic signature algorithms require different amounts of time for generating the signature and verifying the signature. For a cryptographic postal indicia system, the bottleneck is signature verification: a typical postoffice will verify many more mail items than a typical mailer will generate. This argues that we should use a signature mechanism with fast verification time. The two most widely used signature mechanisms are RSA [12] and DSA [7]; of these RSA is best suited for our purposes because it gives the fastest signature verification times.

RSA is a block cipher; it signs plaintext in fixed length blocks. Given the state of cryptography today, we recommend that use of RSA with 128 byte blocks. Smaller block sizes will not be safe for the expected lifetime of our system. If indicia include a certificate containing the verification public key (see Section 6), then barcodes will contain 256 bytes of data, of which 128 bytes will be for mail-specific information. Depending on the amount of error-correction required, such 2-D barcodes will occupy 0.6 to 1.0 square inches.

For the best security, cryptographic postage indicia should contain the following items:

- **meter number** (4 bytes) **and type** (2 bytes)**:** This field identifies the manufacturer, model number, individual meter number, and revision number for the meter's software.

- **postage** (2 bytes)**:** In addition to the 2-D barcode, this field should appear in human readable form.
- **date/time** (7 bytes)**:** In addition to the 2-D barcode, this field should appear in human readable form.
- **item count** (4 bytes)**:** This field contains a piece count for this particular meter. For privacy reasons[4], this should not be readable to non-USPS parties.
- **ascending and descending registers** (4 bytes each)**:** Again, for privacy reasons, this should not be readable to non-USPS parties.
- **entry address** (5 bytes)[5] **:** This is the address from which the mail is stamped and enters the mail system.
- **return address** (5 bytes)**:** This is the address to which undeliverable mail should be returned. It may or may not be the same as the entry address. The return address must also be fully written out in human readable form.
- **destination address** (5 bytes)**:** The destination address must also be fully written out in human readable form.

These items use a total of 38 bytes of our 128 byte data field, leaving 90 bytes available for future advanced services.

Up to now, we have discussed systems which incorporate the destination address in the indicia. Unfortunately, this requirement precludes the traditional stand-alone model of a postage meter which afixes an indicia without knowing the destination address. To use a stand-alone system with the above indicia, the operator would need to scan or manually enter the address information into the unit.

A more convenient, but less secure system, is also possible: a stand-alone meter could omit destination address information from the indicia. (Note that entry address and return address information are likely to be fixed, so that these can be reasonably included in an indicia produced by a stand-alone device.) Without the destination address information, our indicia validity checking becomes more difficult; we discuss this in Section 6.

6 Sampling Strategies and Fraud Detection

Cryptographic indicia provide no security unless mail is inspected. Maximum security is obtained if every indicia is scanned and verified. However the support for this (in terms of scanning and verification equipment) is unlikely to be in place in near future. The alternative is to check only a fraction of the mail stream.

We discuss three inspection strategies: random sample scanning, selective scanning using hand-held scanners and universal scanning. As the system evolves, we expect that each strategy (and perhaps combination of strategies) will have its place. It is therefore important to adopt a system that supports all three.

[4] If items counts or ascending/descending register values can be read from the envelope, then it is possible for an outsider (e.g. business competitor) to find out the size of a mailing list by comparing the item counts from successive mailings.

[5] The USPS 11 digit "zip+4+2" address representation uniquely identifies all addresses in the US and fits in 5 bytes.

6.1 Random Sampling

In random sampling, some small sample of the mail entering the system is selected and scanned. As we increased the proportion of scanned mail, we increase the chances of detecting fraud, but we also increase the cost of scanning. An important design issue is how to check only a fraction of the mail stream, and still provide effective fraud control. It is important that sampling be sufficiently random so that the chance that any particular item is sampled is bounded above and below by a minimum and maximum value.

Each scanned item will be subjected to a number of static checks. Some of these checks indicate definite fraud, while others only indicate possible fraud. Envelopes that are definitely fraudulent can be withdrawn from the mail stream. Those that are just suspicious must remain in the system, but will be recorded for follow-up fraud investigation (for instance, the envelope could be photocopied or digitally scanned). We now outline each check in detail:

Validity: Is the indicia valid (does it have a correct format and signature)?
(If this check fails, then the indicia almost certainly is fraudulent.)

Meter Number: Is the meter on a list of stolen or suspicious meters?
(The trustworthiness of this test depends on the integrity of the list of stolen/suspicious meters.)

Item Counts: Are the sequence count, ascending register and descending register consistent?
(If this check fails, then the indicia is likely to be fraudulent.)

Item Count Limits: Do the item counts fall within the bounds specified in the meter's current account information[6] ?
(The trustworthiness of this test depends on the integrity and timeliness of the meter accounting information.)

Date: Is the date recent?
(This test may occasionally fail for legitimate mail because the mail may be stamped but not posted immediately, or because of post office delays.)

Entry Address: Do the entry address on the indicia and the meter's registered address correspond, and are they consistent with the actual point of entry of the mail item into the mail stream?
(US postal regulations require that metered mail be posted at the post office where the meter is registered. Currently, this rule is not strictly enforced. Hence, a failure of the entry address check indicates a suspicious mail item, but it does not indicate definite fraud. If compliance with the regulation becomes mandatory, then the reliability of this check would correspondingly increase.)

Return Address Does the return address on the envelope correspond with that on the indicia?

Destination Address Does the destination address on the envelope correspond with that on the indicia? (If the destination address is omitted from the indicia, this check cannot be performed.)

[6] A meter's account specifies the current meter credit and count numbers, and this sets upper and lower bounds on the sequence count, and ascending and descending registers counts for a particular period.

In addition to these checks, information from sampled mail items that are stamped by the same meter should be collected and subjected to some statistical checks. To describe these checks, suppose that one in every α items is scanned.

Item Counts: Dates should increase with item counts. The average increment between items should be about α. The same item count should not occur twice.

Account Check: If, over some interval of time, n items with a specific meter (or PC postage system) number are scanned, then the account for that meter should indicate about $\alpha \times n$ items.

Depending on the equipment used, some of these checks may be performed on-line (that is, the check is done as the piece of mail is being scanned). However, it is likely that most checks will have to be done off-line (particularly those that involve looking up a database of previously scanned material). From the point of view of catching fraudulent letters, it is better to perform checks on-line: if we find a suspicious letter, we can capture the particular item, rather than let it pass on through the system. Note that we only suggest delaying delivery of mail in those cases where there is clear fraud.

Random sample scanning is particularly effective against high volume violators, such as most postage meter users.

6.2 Selective Scanning with Hand-Held Scanners

This strategy involves selecting some portion of the mail stream for validation based on criteria such as suspicious visual indicators (for example, the indicia may look unusual or tampered, the return address may be unusual, etc.). All of the static checks described above for random sampling are applicable. (We presume that hand-held scanners will be periodically downloaded with lists of suspicious meters and revoked certificates; see Section 7.) Those checks that cannot be carried out on the spot could be performed later by storing the scanned indicia in the hand-held unit and transmitting them to a central server at the end of the day.

6.3 Universal Scanning

Universal scanning means that each mail item is scanned. Here we can check for uniqueness of meter numbers and item count numbers. We can also check for the consistency of postage used with descending register values. The implementation of such a system faces two challenges. First, all envelopes must be scanned or recorded in some form.

Second, universal scanning involves considerable database requirements. Fortunately we can take advantage of the locality characteristics of mail. Since metered mail typically enters the mail stream at a single sorting center[7], we can set up a localized database at all initial sorting centers. Most checks can be performed by looking up the local database. Some checks will require communication between databases (when mail enters the mail stream at a different sorting center). These are likely to be rare.

Universal scanning will not be cost-effective in the next few years. However, it may become cost-effective in the future. The system we have described is compatible with such a move. All of the checks described for random sampling are applicable, and are

[7] As noted earlier, US postal regulations require that metered mail be posted at the post office where the meter is registered.

in fact more effective in this setting. In particular, universal scanning would greatly increase the chances of detecting violators who post a low volume of mail.

6.4 Fraud Detection

There are two basic kinds of attacks: copying of indicia and forging of indicia. For each of these, there are two subcases: those involving indicia that include destination address information, and those involving indicia that omit it.

The table below summarizes our fraud detection methods.

	Copied Indicia	*Forged Indicia*
Destination Address Included	Immediate detection of changed address information; otherwise use statistical methods.	Immediate detection.
Destination Address Omitted	Immediate detection of changed entry or return address; otherwise use statistical methods.	Immediate detection.

7 Key Management and Protection

Fundamental protection for our keys will be provided by a tamper-proof device that will be able to:

- store and maintain ascending, descending, and item count registers;
- keep the device's private/public key pair, and a certificate signed by an authority (typically a manufacturer or the postal service) attesting to the device's public key (the private key should never be disclosed outside the device);
- prepare bytes (including the appropriate message digitally signed by the device's public key) for transformation in 2-D bar code format; and
- be tamper-proof in the sense that any attempt to penetrate it will result in the private key of the device being erased.

Several appropriate tamper-proof platforms exist, and more are forthcoming. Some of these are very secure, satisfying the highest security level specified by US Federal Information Processing Standard 140-1 [6]. (This publication gives four security levels for cryptographic modules. The highest levels of security are considered nearly unbreakable systems. The US National Institute of Standards and Technology has also recently announced a system for validating and ranking proposed physical devices according to the FIPS 140-1 criteria.) Some examples of possible technologies include the μABYSS [16] and Citadel [17] systems from IBM; the iPower [5] encryption card by National Semiconductor; the Crypta Plus [15] encryption card by Telequip; the CY512i chip from Cylink [1]; and some tamper-proof smart card systems [2]. There will be additional announcements of tamper-proof devices with increased processing power from major vendors in the next few months. For a fuller descriptions of potential platforms, see

[18]. Many of these devices are highly portable and exist in PCMCIA or smart card format. We propose that users lease a secure device (private ownership of postal meters or postal equipment is illegal in the US) from an authorized vendor. The same types of secure devices could be used for both postage meters and computer-generated postage.[8]

Key generation and maintenance must address two issues. First, we want each device to have its own key to reduce the risk exposure should a key be compromised. Second, it is not practical to maintain more than a small number of keys in each hand-held scanner.

These two problems can be elegantly solved by the use of public key certificates. We use vendor-specific and device-specific public/private key pairs. Specifically, each vendor has a public/private key pair: the public key is revealed to the post office, and the private key is used only by the vendor. Each device has a different public/private key: the public key is revealed to the vendor and the private key is used to encrypt indicia.

The two groups of keys are used as follows. A device generates its key pair on initialization (typically performed in a secure facility by the vendor). The device transfers its public key to the vendor and the vendor generates a simple public key certificate for the device's key, signed using the vendor's private key. These certificates are far simpler than X.509 or other proposed public key certificates; they contain only a license number, an expiration date, and the public key corresponding to the license. This certificate is then transferred back to the device. The device includes the certificate (along with a vendor identifier) in any indicia it generates. When an indicia is scanned, the post office uses the vendor's public key to check the certificate and obtain the device specific key, which in turn is used to verify the signed data in the main part of the indicia.

Note that the security of the system (from a fraud point of view) does not depend on keeping the public keys secret — these keys could be published, and in fact the communications between tamper-proof devices and vendor's certificate generators can be public. However, if both the device specific and vendor specific public keys are kept secret, then we obtain an additional benefit: cryptographic indicia can only be read by the post office and vendors. This could be used to satisfy privacy requirements for sensitive information contained in the indicia.

We anticipate a relatively small number of vendors, and we believe that all scanning devices will be able to easily store all vendor public keys. Updated lists of vendor public keys can be periodically downloaded into each scanning device.

Key certificates should be renewed in conjunction with the legally required physical inspection of equipment. New key certificates could be downloaded through a network or modem; or the physical device could be sent back to the factory for certificate renewal. Since most existing and proposed tamper-proof devices are highly portable, this is a very practical measure.

Although tamper-proof devices should be free from attack, one must not exclude the possibility that some private key may become compromised by an adversary. For this reason, a revocation list should be maintained of revoked private keys. This list can periodically be downloaded to scanning devices (along with a list of license numbers of

[8] Permitting the same types of secure devices to be used in stand-alone meters and in PC configurations does not mean that the secure devices may be swapped between a stand-alone meter and a PC. A stand-alone meter might be permitted to omit the destination address from the indicia; a PC-based system, however, should not. Because a PC may emulate the stand-alone meter to the secure device, we recommend special care in statistical monitoring of indicia generated by secure devices registered for use in stand-alone meters.

stolen or lost equipment.)

8 Conclusion

In the coming months, the US Postal Service plans to begin to experiment with cryptographic indicia through its IBIP program [13]. This will provide an exciting opportunity to see public key cryptography techniques deployed on a wide scale (if successful, most people in the US will be receiving mail with cryptographic indicia in the near future).

References

[1] Cylink Corp. CY512i press release, February 1995.

[2] Louis Claude Guillou, Michel Ugon, and Jean-Jacques Quisquater. The smart card: A standardized security device dedicated to public cryptology. In Gustavus J Simmons, editor, *Contemporary cryptology: The science of information integrity*. IEEE Press, Piscataway, NJ, 1992.

[3] Stuart Itkin and Josephine Martell. A PDF417 primer: A guide to understanding second generation bar codes and portable data files. Technical Report Monograph 8, Symbol Technologies, April 1992.

[4] Bill McAllister. Postage meter fraud estimated at $100 million this year. *Washington Post*, September 1993.

[5] National Semiconductor, Inc. iPower chip technology press release, February 1994.

[6] U. S. National Institute of Standards and Technology. Federal information processing standards publication 140-1: Security requirements for cryptographic modules, January 1994.

[7] U. S. National Institute of Standards and Technology. Federal information processing standards publication 186: Digital signature standard, May 1994.

[8] José Pastor. CRYPTOPOST$^{\mathrm{TM}}$: A universal information based franking system for automated mail processing. *U.S.P.S. Advanced Technology Conference Proceedings*, 1990.

[9] Theo Pavlidis, Jerome Swartz, and Ynjiun P. Wang. Fundamentals of bar code information theory. *Computer*, 23(4):74–86, April 1990.

[10] Theo Pavlidis, Jerome Swartz, and Ynjiun P. Wang. Information encoding with two-dimensional bar codes. *Computer*, 24(6):18–28, June 1992.

[11] Judy Rakowsky. 4 men accused of pocketing $4 million in postage fraud scheme. *Boston Globe*, February 1995.

[12] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[13] U. S. Postal Service. Information Based Indicia Program (IBIP) New Technology Metering Devices, May 1995.

[14] U. S. Postal Service and U. K. Royal Mail. Personal communications.

[15] Telequip, Inc. Crypta Plus press release, January 1995.

[16] Steve H. Weingart. Physical security for the μABYSS system. In *Proceedings of the IEEE Computer Society Conference on Security and Privacy*, pages 52–58, 1987.

[17] Steve R. White, Steve H. Weingart, William C. Arnold, and Elaine R. Palmer. Introduction to the Citadel architecture: Security in physically exposed environments. Technical Report RC16672, Distributed security systems group, IBM Thomas J. Watson Research Center, March 1991. Version 1.3.

[18] Bennet S. Yee. *Using Secure Coprocessors*. PhD thesis, Carnegie Mellon University, 1994.