J. Cryptology (1991) 3: 137–146

Journal of Cryptology

CRYPTOPOST™ A Cryptographic Application to Mail Processing[1]

José Pastor
Technical Systems and Advanced Products Division, Pitney Bowes Corporation, Stamford, CT 06926, U.S.A.

Abstract. A public key cryptography protocol is designed for the authentication of documents. When applied to the authentication of postage on mail envelopes it permits the development of a universal automated and standardized mail processing and postage verification system. The mail processing automation problem is present, and the protocol solution and characteristics of the proposed cryptographic CRYPTOPOST™ system are described. Partial details of one implementation are disclosed.

Key words. Digital signatures, Authentication of documents, Public key, Cryptosystem.

1. Introduction

The task of the postal systems of the world was in the past, and still it is today, to process and deliver mail at a minimum cost and with high reliability and security. The task can be abstracted as follows: The postal systems collect "letters"[2] proceeding from a multitude of nonhomogeneous and almost random sources, and then classify and deliver them to another set of random addresses. The service is prepaid and the "letters" have to show a verifiable proof of payment. That means the postal system has to verify the authenticity of a random set of documents and map this set into another random set of addresses.

In the old days of manageable mail volumes, all mail was franked with the same conventional stamps, and was processed in a uniform way. The postal clerks were all equipped with the same built-in generic scanning and data processing mechanism for matching addresses to pigeon holes, verifying the postage, and classifying the mail for delivery.

Today the explosion of information and direct marketing via mail activity threatens to overwhelm postal systems worldwide. In spite of the increasing postal

[1] Date received: March 28, 1990. Date revised: December 12, 1990.

[2] A "letter" is defined as a message directed to a specific person or address and recorded in or on a tangible object... including but not limited to, paper in sheet or card form, recording disks, and magnetic tapes. 112, 31 *USPS Domestic Mail Manual*, issue 33, December 17, 1989.

rates and levels of mechanization the postal systems are often overloaded. To attack the problems and satisfy the needs and demands of mailers many different classes and subclasses of mail have been created with a wide variety of proof of payment markings. That complicates verification of postage. Every class has a different rate structure that requires a different physical and administrative acceptance and verification procedure. Most of these procedures are manual and very inefficient.

To visualize the magnitude of the problem and to appreciate the challenge of the postal systems better consider that all the postal items delivered in 1986 by the USPS would cover a 100 m wide belt around the earth, and the volume keeps increasing. All parties involved agree that to regain control and improve the services offered by such a gigantic operation automation is a must.

Automation is being attempted[3] with the installation of advanced mail processing systems. These expensive, complex, and efficient (but still in evolution) systems consist of OCR reader–sorter machines. The objective, besides sorting the machine-processable mail at the entry point, is to print the destination information in machine-readable form (the POSTNET™ bar code in the U.S.A.) to ease the task of mail sorting at the regional and local distribution postal centers and offices.

To increase the volume of mail which can be processed by automatic means, some postal offices offer special discounted rates to mailers who print the destination code in machine-readable form. This creates new categories of mail and necessarily new and special acceptance and payment verification procedures. This privilege, as conceived, is limited to mailers with a sufficiently large volume and therefore the total volume of specially prepared mail is bounded.

The optimization of the service requires, besides the destination postal code in machine-readable form, enough information on the envelopes to generate at the entry point traffic data bases indicating geographic and calendar mail flow patterns that could enable optimum budgeting, procurement, and deployment of resources.

Finally, the optimization of this process also requires (in our opinion and in that of some postal authorities) some kind of universal standardization similar to the CCITT standardization for telecommunications which will allow single-stream processing of mail.

The development and application of cryptography described in this paper represents a possible approach to a high level of automation and universal standardization of mail processing and verification from generation to final delivery.

2. CRYPTOPOST™. General Description

Our method is designed to meet two major objectives: automation of the mail process and protection of postal services revenue. The rationale for the method is as follows:

First: All the information necessary for the creation of mail traffic data bases can be printed on the envelope, in a machine-readable form, using modern printing

[3] See *International Journal of Research & Engineering, Postal Applications.* Inaugural issue 1989. Semiannual publication of the Universal Postal Union.

technology. Therefore, if this printing is done, the mail classification and sorting process can be simplified by replacing the requirements of the OCR readers to more simple and reliable bar code or bit-map readers.

Second: Since the mailing envelopes have to be read automatically to generate the traffic data bases, it seems logical to read and verify, at the same time and with the same readers, a proof of postage payment. That indeed is possible if the proof of payment exists as some sort of marking in machine-readable form. This can also be accomplished by printing a proof of payment on demand, simultaneously and with the same printer used for the traffic information. If proof of payment is printed in this fashion, the envelope is transformed into a special credit or debit instrument generated directly by the creditor or debtor. Therefore, since it is desirable to use commercial nonsecure electronic printers that are easily programmed, there is a need for some high level of security against counterfeiting. These requirements can be satisfied with the use of cryptography.

Third: Symmetric cryptographic methods could be used, but they would produce another category of mail equivalent to Permit and Meter Mail where the permit or meter number could be an entry into a data base of encrypting keys for the mailers. The mail in those categories has geographic and temporal restrictions and require special preparation on the part of the mailer and special acceptance, verification, and control by the carrier, and once the mail has entered the system the ability to verify proof of payment effectively is lost. In contrast, the use of public key cryptography allows the design of a protocol for the generation of "digital stamps" that, when used as proof of postage payment, produce mail as unrestricted as the mail with conventional stamps, but machine readable and verifiable by a universal device and incorporating important data for the optimization of the postal systems operations.

It is the belief of the author that the implementation of a system such as CRYPTOPOST™ could offer a universal standardized solution to the mechanization and optimization of mail processing.

3. The Protocol

Usually two parties are involved in mail preparation and delivery: the mailer and the carrier. The carrier can delegate some of his activities related to the dispensing of postage to a third party, a trustee, who we call the provider. Therefore we consider three parties: the provider, the mailer, and the carrier (verifier).

The provider, acting as one authenticating agent, provides to the mailer the authorization to print postage. The carrier, acting as a service that has to deliver the mail, is the verifier of the authenticity and validity of the printed postage on the document. The provider collects the moneys from the mailer for the verifier.

The basic protocol [3] is a double public key encryption to communicate between provider and mailer, mailer and verifier, and provider and verifier[4] (see Fig. 1). The

[4] In this paper an RSA–RSA protocol is described, but hybrid public–secret key systems are also possible.

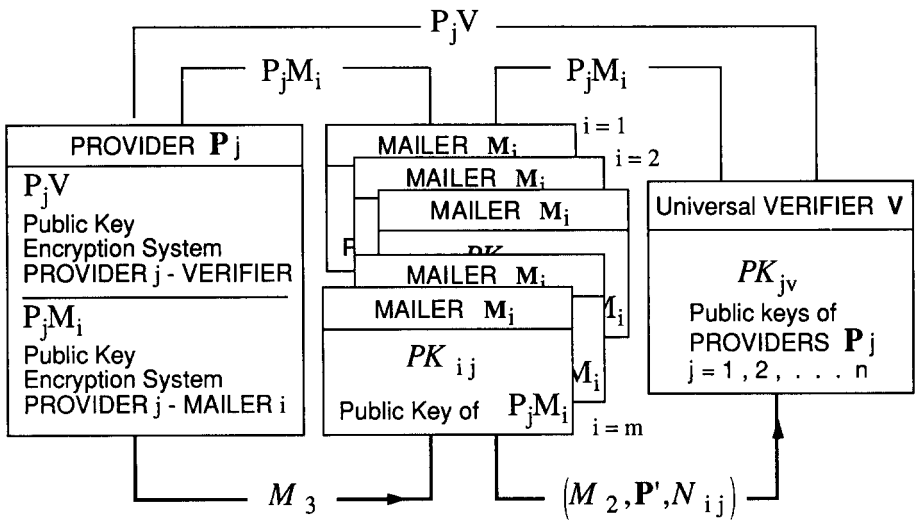

Fig. 1. CRYPTOPOST™. Document authentication protocol applied to mail processing. There are n providers, $j = 1, \ldots, n$, m mailers, $i = 1, \ldots, m$, and many verifiers, all of them with a universal verifier device. Inside the boxes are described the cryptographic parameters each party has. Only the providers have full information about their own public key encryption systems. The mailers have only their public key, and the verifiers have only the public keys of the providers. The cryptographic systems used to communicate among the parties are depicted at the top of the figure with thin lines. The data they use to communicate is depicted at the bottom of the figure with bold arrowed lines. Please follow the text to find the meaning of all the parameters.

provider $\mathbf{P}_j$ has a public key system P_jV to communicate with the verifier,

$$P_jV = (N_{jv}, PK_{jv}, SK_{jv}),$$

where N_{jv}, PK_{jv}, and SK_{jv} are respectively modulus, public, and secret key of an RSA encryption system. The provider $\mathbf{P}_j$ also has a public key system P_jM_i for every mailer $\mathbf{M}_i$,

$$P_jM_i = (N_{ij}, PK_{ij}, SK_{ij}),$$

where N_{ij}, PK_{ij}, and SK_{ij} are respectively modulus, public, and secret key of an RSA encryption system.

There can be a multitude of verifiers in the system, namely all the post offices and carrier delivery agents. Every verifier entity has the same basic verification device, consisting of a reader and a processor. Just for the purpose of the protocol, the verification devices have only the public key PK_{jv} of the P_jV system.

The P_jM_i system is used to communicate between the mailer and the provider, and to encipher the proof of payment by the mailer.

Each mailer has a secure electronic controller box that does the accounting and encrypting of the proof of payment, and controls his unsecured electronic printer for the printing of the "digital stamp." This controller box, for communication with the provider and proof of payment encrypting purpose, has only the public key PK_{ij} of the P_jM_i system, and the identification number ID_i of the mailer.

Step 1. *Provider Sends Authorization to Mailer*

The mailer $\mathbf{M}_i$ requesting authorization to print postage communicates with the provider $\mathbf{P}_j$, and the provider sends to the mailer a signature code M_3, which is the double encryption of the authorization code M_1 with the secret keys SK_{jv} and SK_{ij} of the P_jV and P_jM_i systems, respectively. In this case

$$M_3 = [M_2]^{SK_{ij}} \mod N_{ij},$$

where

$$M_2 = [M_1]^{SK_{jv}} \mod N_{jv}.$$

The authorization M_1 has three components: the authorization *per se*, M_0, some information ID_i related to the identity of the authorized mailer $\mathbf{M}_i$ (i.e., ZIP code), and the secret key SK_{ij} of the mailer's encrypting system P_jM_i:

$$M_1 = (M_0, ID_i, SK_{ij}).$$

The authorization *per se*, M_0, includes the identity of the provider who issues the authorization, and the identity of the mailer to whom that specific authorization is issued. The identity of the provider includes a brief sentence in the vernacular language of the country where the postal operation is taking place (for instance "Cryptopost mail by provider *A*"), and a number with some structure, for instance a palindromic number. The sentence is included for easy human recognition, and the number for automatic machine recognition. This signature can be communicated via any open channel to the electronically secure control box[5] of the nonsecure commercial electronic printer, or written on a smart card if the digital stamp printing device is activated by a value smart card.

Step 2. *Handshake of Authorization and Mailer*

The mailer device decrypts M_3 with his public key PK_{ij} and recovers M_2.

The purpose of the second encrypting with the P_jM_i system is to accomplish a unidirectional handshake between provider and mailer to avoid the mailers impersonation, as is described in Section 7. In some implementations, for example with smart cards, this second encryption acts as a true handshake, and the printing of postage is not possible if there is no handshake agreement.

Step 3. *Mailer Prints the Digital Stamp*

The mailer encrypts the postal information $\mathbf{P}$ corresponding to the particular "letter," with his public key, obtaining $\mathbf{P}'$:

$$\mathbf{P}' = [\mathbf{P}]^{PK_{ij}} \mod N_{ij}.$$

The mailer prints on the envelope in a prearranged format, and in machine-readable form (e.g., bit map), the concatenation $\mathbf{M}$,

$$\mathbf{M} = (M_2, \mathbf{P}', N_{ij}),$$

[5] This operation is standard practice for the Pitney Bowes POSTAGE BY PHONE™ electronic postage meters

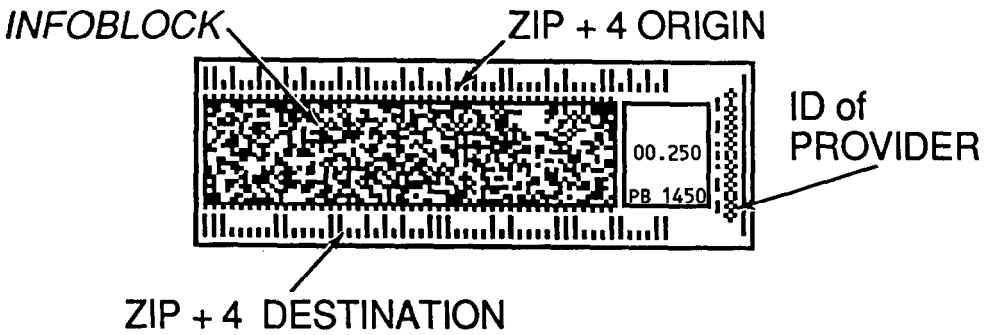

Fig. 2. A sample of the CRYPTOPOST™ cryptographic mail system imprint. The bar codes above and below the *INFOBLOCK* are respectively the origin and destination ZIPs in USPS POSTNET™ code. The vertical graphic code on the right-hand side of the imprint is the provider's *ID*. All the other details are for practical reasons unrelated to the cryptographic characteristics.

and selected components $\mathbf{P}_0$ of the plain text $\mathbf{P}$. The whole set is the digital stamp (Fig. 2).

Step 4. *Verification*

1. *The Verifier Recovers the Authorization.* The verifier—the USPS in the case of the United States—reads the bit map, deformats $\mathbf{M}$, and recovers the three components. With the public key, PK_{jv}, of the P_jV encrypting system residing in his verification device he decrypts M_2 and recovers M_1,

$$M_1 = [M_2]^{PK_{jv}} \mod N_{jv}.$$

From M_1 he extracts the three components. Then he verifies if the authorization *per se*, M_0, has the predefined structure of the system. This structure can be created only by the provider who is in possession of the secret key SK_{jv}, pair of the public key PK_{jv}, and can only be transferred from provider $\mathbf{P}_j$ to the verifier if the mailer is in possession of the public key PK_{ij}, pair to the secret key SK_{ij}.

2. *The Proof of Payment Validation.* Once the verifier has confirmed the structure and validity of M_0, he recovers $SK_{i,j}$ from M_1, and $N_{i,j}$ from $\mathbf{M}$, and decrypts $\mathbf{P}'$, obtaining $\mathbf{P}^*$,

$$\mathbf{P}^* = [\mathbf{P}']^{SK_{ij}} \mod N_{ij}.$$

If $\mathbf{P}^* = \mathbf{P}_0$, then the mailer is an authorized one and the postage *could be* authentic, and accounted for by an electronically secure controller of an unsecured printer. (See details about counterfeiting detection in Section 7.)

A similar protocol called "On-Line, Off-Line Digital Signature" was recently proposed by Even *et al.* [1].

4. Implementation

The encrypting system for the provider–verifier pair in our implementation is a 500-bit RSA, and the provider–mailer system is a 300-bit RSA. That means the

overall concatenated information block **M** has 1100 bits. Naturally, M_2 being larger than N_{ij} is encrypted in two blocks with the proper padding, and M_3 is a concatenation of two blocks of size $|N_{ij}|$ that, when decrypted, reconstruct the $|N_{jv}|$ size of M_2.

Since the communication established between the provider and verifier by the encrypting system P_jV and the printed envelope is a one-way channel, redundancy for error-correcting capability is added to the information block. To take care simultaneously of any possible random and burst errors present in the mail environment (e.g., errors in printing, ink smudges, degraded print quality, errors in reading, etc.) the error-correcting code selected and implemented is a concatenation of BCH and Hamming.

The 1100 bits of encrypted information—the envelope signature—are divided in blocks of 11 bits. Operating in a 2^{11} finite field Galois extension, the information block is BCH coded [5] for the correction of 16 errors; therefore we have 132 blocks of 11 bits. Every block is Hamming coded [2] for the correction of one error. As a result the final *INFOBLOK* to be printed on the envelope or document has 1980 bits. This block of logic bits is printed with additional formatting with a dot matrix printer in the form of *INFOBITS*. (One *INFOBIT* is a logic bit printed with a resolution of n printer dots per logic bit.)

The signature M_3 can be changed any time the mailer requests a new authorization, without the need to notify the verifier, as long as the changes are within the agreed general constraints of structure for M_0. All the postage generated by the mailer between changes will produce an information block **M** with two constant components, M_2 and N_{ij}. The postage encrypted information **P′** is always different, even for identical "letters" with identical origin, destination, and postage because a continually changing parameter is included in **P**. In our implementation we selected the date and time of generation in tenths of a second. The changes in **P′** are reflected in changes in the 32 redundancy BCH code characters computed for the possible correction of 16 errors. The final formatting after the coding and before the printing of the *INFOBLOCK* serves to disguise the fixed components of **M**.

Verification follows the reverse process. The reader is a CCD array and associated logic that oversamples every *INFOBIT*, transforms them into logic bits; deformats the *INFOBLOCK*; 15-bit words are then identified and Hamming corrected for random isolated errors, the Hamming bits are disregarded and the 11-bit words are BCH corrected for up to 16 errors. The result is **M** that is decrypted according to the protocol. The whole operation is done at the present time in 1 second with a hybrid of hardware and software. Engineering analysis and predesigns indicate that with a special ASIC hardware the whole reading and verification will be feasible at 10 items per second.

Figure 2 is an example of an RSA–RSA version of the system. The *INFOBLOCK* is in the center area. All the other information is printed for practical and ergonomic reasons.

5. Universality

The CRYPTOPOST™ system described has universal application. This means that postal systems and carriers operating with different providers in different countries and with different currencies can verify all the mail produced within the system with

a universal device. All that is needed is a provider identifier code in a machine-readable form added to the format of the CRYPTOPOST™ printed block of information. This will be the entry into a table of public keys stored in the verifier memory. With the implementation described in Section 3, only 1000 bits of memory are required for each provider. In the United States there are presently only four approved independent providers plus the postal service itself, therefore the system could be made of universal domestic use with only 5000 bits of memory on the verifiers table of public keys. A memory chip of 64 KBytes will be more than enough to have a worldwide operational system. The possible position of provider *ID* is shown in Fig. 2. Different technical implementations of the printing end extend this CRYPTOPOST™ capability not only to the highly mechanized production mailer but to the individual [4].

6. Security

The security of the CRYPTOPOST™ system is the security of the encrypting methods used. Two different levels of security are implemented according to the value of the damage produced by a potential violation of the two cryptographic systems. Violation of the provider–verifier system would be catastrophic, therefore a 500-bit RSA is used. The potential violation of the provider–mailer would produce minor damage, therefore only a 300-bit RSA is used. In theory such levels of security seem low, in particular for the individual mailer operation. However, the practical implementation speed requirements demand that the computations be made in hardware, therefore the public keys can be embedded in the microchips, adding another physical protection fence to the system beside the inherent mathematical security. That means the system will work with two public key encrypting systems, but will all the public keys kept secret.

The public keys are kept secret for convenience. The provider–mailer encrypting system could be also a symmetric secret key system with key K_i instead of the public system P_jM_i, but the provider–verifier system has to be a public key system in order to provide the CRYPTOPOST™ universality characteristic.

Obviously, the mailer could easily compute his pair of keys, or obtain his secret key K_i, without tampering with his control box to find PK_{ij}, because N_{ij} is always printed, and SK_{ij} or K_i is eventually disclosed internally in the verification device. That means the creditor could cheat to the verifier—that is the credit issuer through his trustee, the provider—but only with his cooperation.

For practical reasons a tradeoff between security level, number of bits on the "digital stamp," and graphic representation of the data (bit map versus bar code) is necessary. The bit content of the *INFOBLOCK* for this double RSA system matches the needs of information for automation, universality, and fraud detection for different counterfeiting scenarios. That means the high level of security offered to the postal operations is a direct benefit of the CRYPTOPOST™ solution. To reduce the bit content and the size of the *INFOBLOCK* preserving the basic characteristics of the system, without sacrificing security, or to preserve the bit content and increase the security if needed, a hybrid protocol that uses elliptic curve logarithm cryptography could be used. (This work will be reported in other publications).

7. Counterfeiting and Fraud Attempts Detection

Mailer Impersonation with Different Control box

Assume mailer $\mathbf{M}_{i'}$ is a bona fide CRYPTOPOST™ system subscriber that intercepts message M_3 directed to mailer $\mathbf{M}_i$ and tries to impersonate him. When $\mathbf{M}_{i'}$ deciphers M_3 with his public key $PK_{i'j} \neq PK_{ij}$ he will obtain $M_2' \neq M_2$. The ID_i' component of M_2' will not coincide with the $ID_{i'}$ that resides on the $\mathbf{M}_{i'}$ mailer's controller box memory. This discrepancy will block the proof of payment printing operation. Even if mailer $\mathbf{M}_{i'}$ pretends to impersonate mailer $\mathbf{M}_i$ by some clever manipulation of his controller box and uses M_2' in his digital stamp the verifier will detect the attempted fraud because the decryption of M_2' will produce an M_0 without the proper predefined structure. The verifier very likely will deny the service.

Counterfeiting Attempts

To detect counterfeiting attempts, information included in M_1 and $\mathbf{P}_0$ is compared.

In M_1 the mailer's ZIP + 4 (or postal zone) is included along with the authorization date T_a. Postal data **P** includes, besides the postage value and the mail class, the ZIP + 4 code of both mailer location and addressee, the date and time of printing, in tenths of seconds, and selected characters of the address. All of this information is encrypted. Besides the *INFOBLOCK* the imprint also includes the ZIP + 4 codes of origin and destination printed in standard POSTNET™ bar code form. (See Fig. 2.)

The following counterfeiting scenarios are conceivable:

Case 1. The counterfeiter tries to print his own *INFOBLOCK*
The attempt will be detected during the decryption since M_0 will not have the correct structure.

Case 2. The counterfeiter copies a real valid imprint from other envelopes.
There are two possible attempts of fraud:

1. Mailpieces have identical addresses.

The attempt will be detected because there cannot be two letters with the same date and time created and sent at the same time, or outside the time or geographic window. (This fraud attempt is detected using traffic analysis data bases and suspicious mail data bases generated at different points of the mail flow, including the destination post office. The operational details are outside the scope of this publication.)

2. Mailpieces have different address.

The attempt will be detected automatically by comparing the bar coded and decrypted ZIP codes.

Case 3. The counterfeiter copies a valid *INFOBLOCK* from a letter and prints valid POSTNET™ bar codes for his letter.
The attempt will be detected as in 2 of case 2.

8. Conclusions

A cryptographic protocol for document authentication, when applied to the problems of mail preparation and processing, can create a universal standard for automation and optimization of postal services operations.

The models, demonstrations, implementations, and engineering analysis performed up to date indicate that the system is feasible in a diversity of implementations and architectures at all mail production levels (ranging from the individual mailer to mass-production mail), at all levels of verification (ranging from fully automated verification with adapted OCR-sorting machines to handheld wand operation by the delivery carrier), and by all postal authorities in the world with a universal verification device [4].

This set of solutions is also applicable to shipping and other secure-materials transport environments, including the electronic notarization of documents.

Acknowledgments

Comments and suggestions from the anonymous reviewers and the editors are greatly appreciated and incorporated in the final version of the paper.

References

[1] S. Even, O. Goldreich, and S. Micali. On-line, Off-line Digital Signatures. In *Advances in Cryptology—CRYPTO* '89, G. Brassard (ed.). Lecture Notes in Computer Science, Vol. 435. Springer-Verlag, Berlin, 1990, pp. 263–275.

[2] R. W. Hamming. *Coding and Information Theory.* Prentice-Hall, Englewood Cliffs, NJ, 1980.

[3] J. Pastor. *Reliable Document Authentication System.* US Patent 4, 853, 961, August 1, 1989.

[4] J. Pastor. CRYPTOPOST™. A Universal Information-Based Franking System for Automated Mail Processing. In *Proceedings of Fourth Advanced Technology Conference of the U.S. Postal Service,* Washington, DC, November 5–7, 1990, Vol. I, pp. 429–442.

[5] W. W. Peterson and E. J. Weldon. *Error-Correcting Codes,* 2nd ed. MIT Press, Cambridge, MA, 1972.