Certicom's Bulletin of Security and Cryptography

C0DE&CiPHER

This issue of Code and Cipher focuses on Elliptic Curve Cryptography applied to address specific industry needs.

ECC and Digital Postage Marks

Digital technology has radically changed how companies do business–the postal system is no exception. The advent of the digital postage meter has transformed the processes for payment and revenue collection.

Digital Postage Marks (DPMs) provide the proof of payment as a piece of mail progresses through the postal system. They offer the potential for significant cost savings when compared with the use of legacy postage marks, due to their ease of reproduction and their machine-readability.

While it has become much easier to reproduce a Digital Postage Mark (DPM), it is much harder to confirm evidence of payment for use of that mark. This means that postal organizations risk losing revenue for pieces of mail that go out with fraudulent–or copied–digital postal marks. The revenue loss from any fraudulent use offsets any potential cost savings. This explains the interest by postal organizations in secure, yet cost-effective postage marks that would thwart fraud.

To prevent this fraud, digital signatures are used to encode digital postal marks and to prove the mark is valid. Signature size, however, is an important consideration, as it directly affects the size of the DPM that must go on a piece of mail. Equally important is the strength of the signature, which cannot be compromised.

This article examines the Elliptic Curve Pintsov Vanstone Signature scheme (ECPVS). Based on ECC, this method offers a signature size six times smaller than an RSA-based signature, yet still remains highly secure.

An overview of the process

To understand the importance of securing the DPM, we should take a step back and look at the postal process.

Company A generates digital postage marks for mail they send out to a number of different customer targets. The postal system verifies that the postage marks are valid and sends each piece of mail to its intended destination. However, fraud can occur when:

1) **An adversary, Eve, intercepts a piece of this mail, copies the DPM originally generated by company A, and uses it for her own purposes.**

2) **Company A takes the DPM it generates legitimately for one piece of mail, and uses it fraudulently on other pieces of mail it sends out, thereby reducing its overall mailing costs.**

In either case, each example illustrates the need for better authentication of the information contained within the DPM.

Using digital signatures to authenticate a DPM enables the verification of a postage mark. Each digital mark is tied to one specific piece of mail and cannot be re-used for fraudulent purposes. Terminals will never re-use a DPM. Digital postage verifiers will reject old, copied DPMs and can ultimately trace the origin of attempts to re-use copied DPMs.

Elliptic Curve Pintsov Vanstone Signatures

The use of ECC-based signature schemes in the postal industry is not new. Because the size of the digital signature affects the overall size of the DPM, ECC-based signatures provide an extremely small, yet highly secure option. In the "Performance Criteria for Information-based Indicia and Security Architecture for Open IBI Postage Evidencing Systems" (2001), the USPS

continues on page 4

ECC will be pushed into wider commercial usage by companies targeting the government market.

Crypto Column by Dr. Scott Vanstone

Public-Key Cryptography: Where is it Going?

In 1986, Whit Diffie published his article, "The First Ten Years of Public Key Cryptology"*, and in the section titled "Where is Public-Key Cryptography Going?" Diffie predicted that "[u]nless the available systems suffer a cryptanalytic disaster, …the very success of public key cryptography will delay the introduction of new ones until the equipment now going into the field becomes outmoded for other reasons." Since 1986, the "other reasons" have been clearly brought in play by the advent of the wireless world, with its constrained computing, storage and battery life.

In this column, I want to try to answer from a 2004 perspective the same question: "Where is public-key cryptography going?"

At the time of Diffie's article, Elliptic Curve Cryptography had just been discovered by Victor Miller and Neil Koblitz. Over the last 20 years, it has been researched extensively and adopted into a number of industry standards.

On October 24, 2003, a significant event in the history of ECC occurred. In an unprecedented move, the US Government's National Security Agency (NSA) licensed ECC, MQV (a public-key agreement scheme created by Menezes, Qu, and Vanstone) and related intellectual property for the U.S. Government's mission critical national security applications, declaring it a "crucial technology". The US Government is moving its key management to ECC and in particular, MQV.

Why is this significant? A major hurdle to wide-scale adoption of any security technology is standardization. When the NSA endorsed the Data Encryption Standard (DES) in 1979, it became a standard around the world. DES became FIPS-approved (NIST Federal Information Processing Standards) and then over time, moved into wider commercial usage, becoming one of the most widely used cryptographic algorithms of all time. Today, 25 years later, although DES is now being replaced by AES, it has not completely disappeared. As technology requires stronger and stronger security, I believe that ECC and AES are well positioned to experience a similar adoption rate and lifespan.

Following in the footsteps of DES, ECC, in conjunction with AES, has already been incorporated into a number of key international standards, including ANSI X9.63, IEEE Std 1363-2000, IETF RFC 3278, ISO 15946-3 and NIST SP 800-56. Adoption into global standards will assist in pushing ECC into wider commercial usage.

The adoption by the US Government will also help to push ECC into wider commercial usage. Today, government agencies and departments look for COTS (commercial off-the-shelf) products that have proven security built into them—it makes it easier to receive technical support and allows them to take advantage of the latest technology. Additionally, because security is a concern in many industries, these same products are also used outside the government. The advantages ECC provides apply equally as well to industries such as finance and the postal system, as shown in this issue of Code and Cipher.

Aside from the United States, other governments are also looking at ECC. For example the Chinese government is considering ECC as a way to fix security issues with 802.11 use in its country. The level of security and standardization of ECC makes it ideal in solving problems such as this one.

To answer the proposed question: *Where is public-key cryptography going?* For now, keep your eyes on the bright future of ECC.

For those interested in more detail information on practical implementations of ECC, see the recently published book by Hankerson, Menezes and Vanstone titled Guide to Elliptic Curve Cryptography, Springer Verlag, 2003.

*Whit Diffie's article appeared in Gus Simmons' book Contemporary Cryptology, The Science of Information Integrity, IEEE Press, 1992.

ECC and Electronic Check Presentment

The adoption of electronic payment and presentment mechanisms is becoming more widespread as the financial industry sees benefits in leveraging automation–not only to reduce back office costs but also to improve their customer service.

Most recently in the United States, President Bush signed the Check Clearing for the 21st Century Act ("Check 21"), which encourages financial institutions to exchange digital images rather than paper to process checks with each other. There are other examples globally.

This has huge ramifications on the check-cashing process as we know it today. Benefits include a reduction in the time it takes to clear a check through the system and earlier detection of issues relating to insufficient funds and fraudulent checks. The industry will also save on the costs associated with transportation and storage of paper checks.

ELECTRONIC PRESENTMENT, CHECK TRUNCATION AND CHECK IMAGING ADOPTION GLOBALLY[1]

- **Interbank Data Exchange (UK)**
- **Electronic message exchange of Euro cheques (France)**
- **Exchange of image based electronic cash letters (Hong Kong)**
- **Electronic posting with paper to follow (South Africa)**
- **Centralized Cheque Truncation System/National Image Archive (Singapore)**
- **Check 21 (USA)]**

[1] Sourced from "The Changing Landscape of Payments" a Unisys Whitepaper, May 2002. http://www.unisys.com/financial/insights/insights__compendium/chg_landscape_of_pmts.pdf

Achieving Maximum Security and Efficiency

Obviously, the security around digital images of checks is very important. Without some form of authentication of the digital image, someone could intercept the transmission of a digital image and alter it, causing additional losses for the banks. Authentication also ensures that the information on the check (ie values, payor, etc.) has not been tampered with.

However, the process of efficiently securing electronic check presentment, or check image capture, presents a major challenge: machines scan thousands of checks per minute, and each image must be signed to ensure that the information on the check can not be denied later.

This level of automation in the financial industry can only be achieved though the use of very strong, very fast, digital signatures. Elliptic Curve Cryptography (ECC), recommended by ANSI (American National Standards Institute), offers financial institutions high security using much smaller key sizes that any other public key cryptographic scheme available today.

A look at the process

In order for the process to work seamlessly, an agreement between banks exchanging electronic check data needs to be in place. The banks involved must also exchange root certificates in order to trust the signatures of the check images.

The check image is scanned at the receiving bank to ensure that check is compliant. The image is signed using ECDSA.

The paper check arrives later to serve as backup–or not at all. With Check 21, the paper check is not required past the point of capture of information for clearing and settlement.

Solution: Why ECDSA for ECP

Much like the digital postage mark process described in this newsletter, the crux of the electronic check presentment process is the verification of each digital signature on the thousands of checks that are processed.

continues on page 6

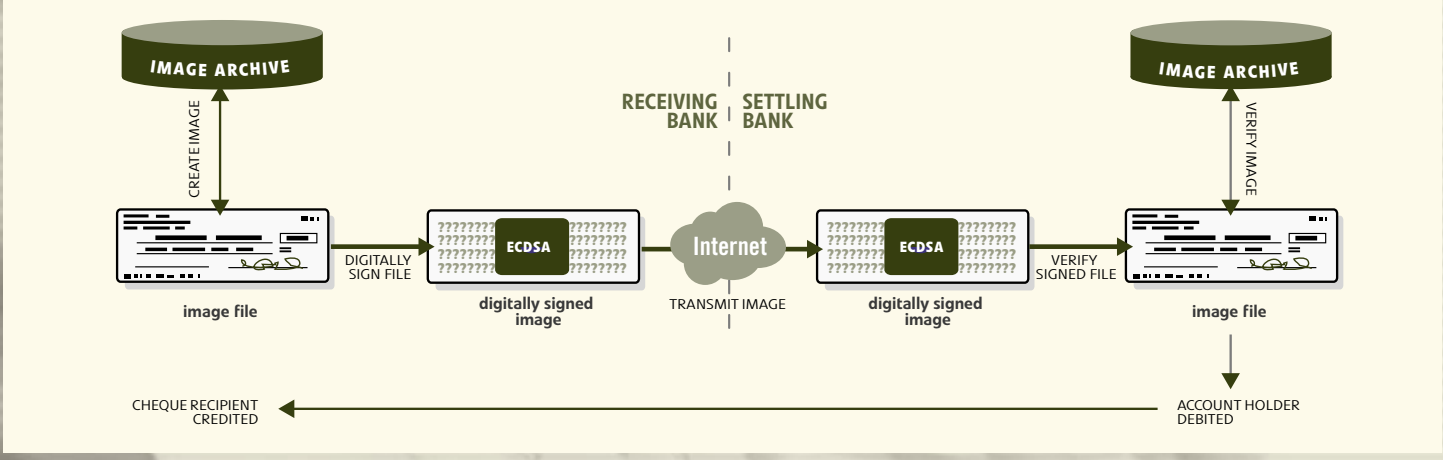

Figure A: the electronic check presentment process

ECC and Digital Postage Marks

continued from page 1

defines support for the use of ECDSA to generate the digital signatures for DPM.

A typical ECDSA signature is a 40 byte appendix added to a signed message. By comparison, the cryptographic overhead of an equivalent DPM using RSA would add 128 bytes. As shown in figure 1, this would take up most of the space on the envelope on a small piece of mail, so a small signature becomes very important.

ECC-based signature

RSA-based signature

Figure 1: A comparison of physical DPM size on a piece of mail.

An even smaller alternative is the Elliptic Curve Pintsov Vanstone Signature (ECPVS) scheme. ECPVS is a signature scheme that provides partial message recovery. At the same security level and elliptic curve, an ECPVS signature can add as little as 20 bytes to the original message length, which is a six times smaller than RSA--making ECPVS more efficient.

ECPVS is unique because all or part of the message can be embedded in and recovered from the signature. This partial message recovery makes ECPVS ideal for use with digital postage marks. Certain data elements, such as the date and the postage amount, are able to be read by humans, while other data elements, such as the address of the sender or a confirmation of the recipient's address, are restricted to being read only by machines. Furthermore, if the terminal's signature verification key is secret, rather than public, then the hidden part of the message is difficult to obtain, even by machine.

Another feature specific to ECPVS is the ability to adjust the level of security, depending on the requirements. In ECPVS, the length of the recovered part of the message is not tied to any other parameters of the scheme. Redundancy, the duplication added to an encrypted message, is one of these parameters. The amount of redundancy in a message determines the level of security. Only ECPVS enables tradeoffs between security level and bandwidth availability: if very short signatures are required due to bandwidth constraints, the amount of redundancy added by padding can be lowered, thereby decreasing the size of the signature component e, with a controlled impact on the security offered by the scheme.

ECPVS in the Real World

Pitney Bowes, a global provider of informed mail and messaging management, introduced digital mailing systems in 2002 that use ECPVS to provide security for the digital postal marks.

ECPVS is also being adopted into a number of standards, including IEEE P1363a, ANSI X9.92, and ISO 9796-3.

The relative benefits of ECPVS (size, flexibility and efficiency) also make it ideal for use in applications beyond the postal service such as cheque imaging and verification, or to sign short 1-byte messages (i.e. yes/no, buy/hold/sell, etc.) ■

How ECPVS Works

Using ECPVS, a plain text message (PD) is essentially split into two parts: parts C and V. Part C represents data elements that require confidentiality protection, such as the sender information, value of a serial piece count, or the value of the ascending register. These can be recovered during the verification process from the signature and allow for proof of deposit and mail tracing. Part V contains data elements presented in the plaintext within the DPM, such as the date, the sender's and recipient's postal codes, or the amount of the postage. Both C and V are signed.

The ECPVS uses a fixed elliptic curvew with a generator G of order n. Terminal A has Q_A and A.

To generate a signature, the mailer terminal A begins by generating a random positive integer k < n.

The terminal then takes the mailing information and performs a number of computations in order to encrypt the message. First, it calculates a point R on the curve (R = kG), to be used as a key for the transformation of C. This elliptic curve point R is then used in a bijective transformation (T_R)– typically a symmetric encryption algorithm–to destroy any algebraic structure C might have, with the result being e. The secrecy of e is based on the difficulty of the discrete log problem and on the randomness of k.

DPM INPUT

$PD = C \| V$

DPM CREATION

$R = kG$

$e = T_R C$

$d = H(e \| I_A \| V)$

$s = ad + k \pmod n$

DPM VERIFICATION

Retrieve Q_A

$d = H(e \| I_A \| V)$

$U = sG - dQ_A$

$C = T_U^{-1}(e)$

Check C for redundancy

The variable d is calculated using a hash function H, the encrypted message part e, and the identity of the mailer's terminal I_A, as follows: $d = H (e || I_A || V)$.

Finally, s (the other part of the signature pair), is calculated using d, k, and a, which is the private key of the terminal A as follows: $s = a d + k \pmod n$.

The signature pair (s, e) is then put into the DPM together with the portion V of the plain text PD.

To verify the DPM of an incoming mail piece, a postage verifier on the other end of the postal process parses the DPM into I_A, the signature (s,e), and the verification data V. Using these and the public key of terminal A, the postage verifier recovers C and subjects it to a redundancy test. If the redundancy check fails, the DPM is rejected; if the redundancy check passes, the plaintext message is recovered. ■

For more information about ECPVS, Certicom has posted two white papers. *"Postal Revenue Collection in the Digital Age"*, and *"Formal Security Proofs for a Signature Scheme with Partial Message Recovery"*.

Visit http://www.certicom.com/codeandcipher

Review of *"Guide to Elliptic Curve Cryptography"*

By Richard K. Hite
Senior Vice President, Emerging Technology, VISA International

As part of my role at VISA, I have closely followed many new and emerging security technologies over the years. In the mid 1990's, I became aware of efforts in the ANSI X9F1 working group to standardize public-key cryptographic protocols based on elliptic curves. My interest sparked, I set out to learn more about these fascinating objects. I learned that elliptic curves had been studied by pure mathematicians for over one hundred years, and first introduced to cryptographers by Hendrik Lenstra when he proposed using them to factor integers. Shortly thereafter, in 1985, Neal Koblitz and Victor Miller independently showed how elliptic curves could be used to implement public-key protocols traditionally implemented using the multiplicative group of a finite field.

Since 1985, the security and efficient implementation of elliptic curve cryptographic systems have been extensively studied. The elliptic curve discrete logarithm problem, whose intractability is fundamental to the security of elliptic curve systems, has weathered umpteen mathematical attacks. Elliptic curve systems have thereby come to be accepted today as the most viable public-key technology for high-security applications. They are also most suitable for constrained environments such as those in which smart cards and personal wireless devices are typically deployed.

Guide to Elliptic Curve Cryptography is an introduction to this fascinating area of cryptography. Two of its authors, Alfred Menezes and Scott Vanstone, are well known for their pioneering research on elliptic curve systems, and for their encyclopedic *Handbook of Applied Cryptography*, which they co-authored with Paul van Oorschot. *Guide to Elliptic Curve Cryptography* covers much ground, including the underlying finite field and elliptic curve mathematics, algorithms for implementing the arithmetic, standardized elliptic curve cryptography protocols (including ECDSA and MQV key agreement), and side-channel attacks. Also included are appendices that list sample parameters, standards, and publicly available software tools.

The writing is clear and concise. The authors' objective was to make the book accessible to security practitioners and engineers, and they have succeeded in this regard. Detailed descriptions of the various algorithms are provided, while at the same time the essential concepts and benefits of each algorithm are highlighted. An especially noteworthy feature of the book that will be appreciated by software developers is the extensive set of notes on implementing the algorithms in different software environments.

Guide to Elliptic Curve Cryptography is an indispensable reference for security practitioners interested in deploying public-key cryptography. It is a timely, well-written addition to the cryptographic literature, and will occupy a prominent space in my bookshelf. ■

For more information about *Guide to Ellliptic Curve Cryptography* please see page 6 of this issue.

ECC and Electronic Check Presentment

continued from page 4

Earlier issues of Code and Cipher have focused on the small key size of ECC and the direct relationship between key sizes and required computing resources. The underlying hard math problem behind ECC enables it to provide a higher security per bit over other public-key schemes. Given the volume of checks that must be signed, the smaller ECC key sizes provide for a greater efficiency and performance, while keeping the hardware requirements for check scanning to a reasonable level.

Since data must be maintained in archives for seven years, strong, efficient signatures are required. By signing the data using a strong ECC-based signature like ECDSA or ECPVS upfront, the information will remain secure for a longer period of time, until advances in computing power demand an even higher level of security.

ECC: Now and in the Future

The ANSI X9 standards (the definitive standards for financial institutions), specify ECDSA (Elliptic Curve Digital Signature Algorithm) for digital signatures in financial transactions. ECPVS (Elliptic Curve Pintsov Vanstone Signature) has been recently submitted and is pending approval.

Companies such as NCR have integrated ECC-based digital signatures in the scanning and signing technology they have developed for this new process.

Beyond check imaging and electronic check presentment, ECC also has other applications, not only in the financial industry, but also insurance, or national security. Many of the requirements for Electronic Check Presentment apply equally to document imaging and management in general. For the same reasons that ECC works well for the financial industry, it can also be used here. ■

For more information about Check 21, ECC and Electronic Check Presentment, take a look at these links:

http://www.bai.org/check21/

http://www.certicom.com/download/aid-237/success_ncr.pdf

http://www.unisys.com/financial/insights/insights__compendium/chg_landscape_of_pmts.pdf

Guide to Elliptic Curve Cryptography

Darrel Hankerson, Alfred Menezes and Scott Vanstone
Springer, December 2003, ISBN: 0-387-95273-X; 332 pages
Web: http://www.cacr.math.uwaterloo.ca/ecc/

Guide to Elliptic Curve Cryptography is a comprehensive treatise on the practical aspects of elliptic curve cryptography. Written by Scott Vanstone, Executive Vice President, Strategic Technology, together with Auburn University professor Darrel Hankerson and University of Waterloo professor Alfred Menezes, it explains the basic mathematics, describes state-of-the art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures.

The intended audience for the book comprises security professionals, developers, and those interested in learning how elliptic curve cryptography can be deployed to secure applications. Most of the material should be accessible to anyone with an undergraduate degree in computer science, engineering, or mathematics. In addition, the breadth of coverage and the extensive surveys of the literature included at the end of each chapter should make it a useful resource for the researcher.

Chapter contents:

Guide to Elliptic Curve Cryptography was published in December 2003 by Springer as part of their "Springer-Verlag Professional Computing Series". It can be ordered online through Springer's web site or from retailers such as Amazon.com and Chapters. ■

Code and Cipher

Code and Cipher, published quarterly by Certicom Corp., is an educational newsletter that covers the security and cryptography industry. In each issue we will examine security issues and cryptography trends in an objective manner. We welcome your thoughts, opinions and comments on anything that affects the industry. Please send us your feedback on this issue and what you'd like to see in upcoming ones:

5520 Explorer Drive, 4th Floor
Mississauga, Ontario, L4W 5L1
Canada

T (905) 507-4220
F (905) 507-4230
E codeandcipher@certicom.com

DON'T MISS
THE NEXT ISSUE OF
C0DE&CIPHER
SUBSCRIBE TODAY AT
WWW.CERTICOM.COM/CODEANDCIPHER

certicom™

© 2004 Certicom Corp. All rights reserved. Certicom, the Certicom logo, and Code and Cipher are trademarks or registered trademarks of Certicom Corp. All other companies and products herein are trademarks of their respective owners.