Scott Vanstone on the ECC Conference
page 2

The Use of Public-Key Cryptography in BlackBerry
page 3

The origins of public-key cryptography and ECC
page 5

Certicom's Bulletin of Security and Cryptography

CØDE&CIPHER

This issue of Code and Cipher reviews the first annual Certicom ECC Conference and summarizes some of the key discussions at the event.

Grand Beginnings

The cryptography community comes together for the first annual Certicom ECC Conference

For two days in November, cryptography experts, industry leaders and members of the developer community gathered in the elegance of Toronto's Four Seasons hotel to discuss the science and the business of elliptic curve cryptography (ECC).

Taking a look back over the 20-year history of the discipline and casting a speculative eye forward to the future, the event's distinguished panel of speakers—comprising the very pioneers of public-key cryptography and ECC—captivated guests with a combination of technical insight and personal reflection on how their discoveries came about. Inspiring listeners with their evident passion for cryptography and the mathematics at its heart, they made a clear case for the advantages of ECC, both for today and over the long term.

The audience of industry professionals, academics and analysts from the United States, Canada and several European and Asian countries, represented a wide range of specializations and industry sectors—proof positive that interest in ECC is widespread and growing.

A meeting of minds

One of the primary goals of the conference was simply to bring these people together—to provide a meeting place for the cryptography community where new relationships could form and ideas could be exchanged. Many attendees expressed their excitement at the chance to network in such a concentrated way.

Another aim of the conference was to assemble a truly remarkable roster of speakers—individuals with extensive knowledge of ECC and cryptography—giving attendees an opportunity to speak one-on-one with leaders of the industry. Audience members were highly impressed by the caliber of the presentations and the facility with which they could mingle with these luminaries. In this regard, the event was an overwhelming success.

Recognizing cryptography leadership

Highlights of the ECC Conference included the recognition of the contributions of several leaders to the field of cryptography. Drs. Neal Koblitz and Victor Miller received the 20 Years of ECC award for their pioneering work in developing elliptic curve cryptography, and Dr. Walt Davis received the ECC Visionary Award.

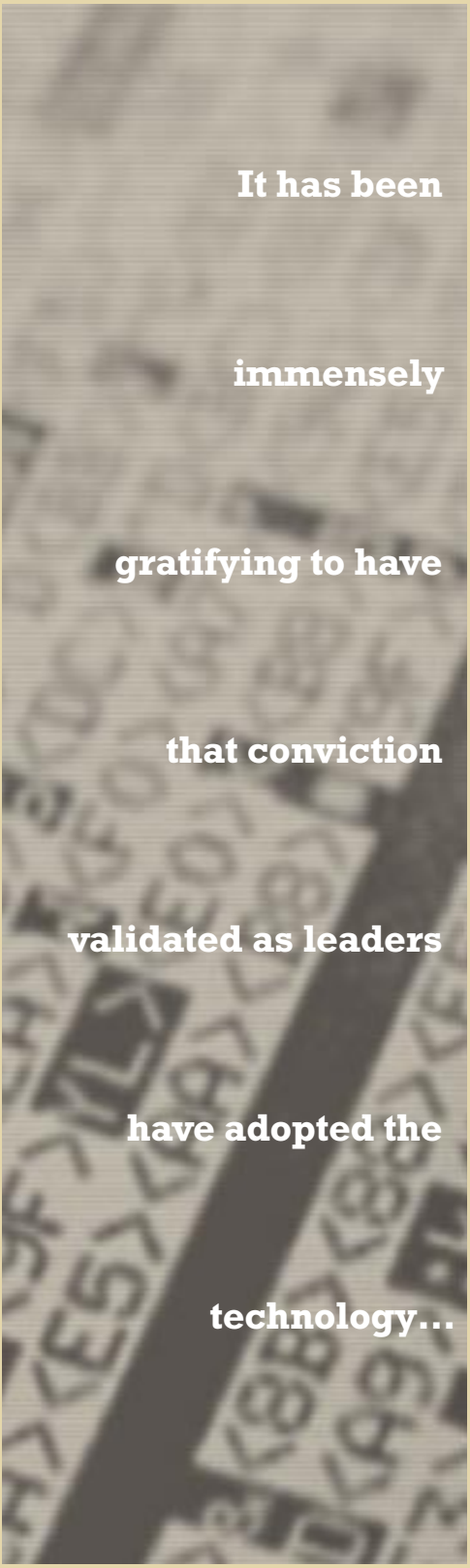
continues on page 4

Crypto News

ECDSA Now Has FIPS Validation

In September 2004, NIST instituted a validation system for the Elliptic Curve Digital Signature Algorithm (ECDSA) as approved in FIPS 186-2. This is significant because it is the first validation system for an ECC-based algorithm. This now means that accredited third parties can test vendor implementations of ECDSA, thereby ensuring the proper security and interoperability. Ultimately, this should help encourage further adoption of ECDSA.

The first three companies to receive a certificate number for ECDSA Validation were: Certicom Corp. (#1), nCipher Corporation Ltd. (#2) and SafeNet Canada, Inc. (#3). ■



Crypto Column by Dr. Scott Vanstone

Reflections: The year that was

I have always been convinced of the practical merits of elliptic curve cryptography (ECC). It has been immensely gratifying to have that conviction validated in the past few years as leaders such as the U.S. National Security Agency, Research in Motion and General Dynamics have adopted the technology for their own purposes.

Of course, I haven't been alone in my fervor for ECC. That point came home clearly during Certicom's first annual ECC Conference—a personal highlight of 2004.

Held at Toronto's Four Seasons Hotel in November, the ECC Conference was well-attended by cryptography experts, industry leaders and members of the developer community. Its program was designed to interest both a technical audience and business managers, and in my opinion was immensely successful on both fronts.

Even attendees relatively new to cryptography were pleased to discover that the conference also held significant historical value. On hand were luminaries such as Dr. Ralph Merkle, Dr. Neal Koblitz, Dr. Victor Miller and Dr. Walt Davis.

The pioneers

In the minds of many people in the cryptographic community, Dr. Ralph Merkle is the unsung hero of public-key cryptography. In his talk, he offered insight into how he discovered the concept while working on a project for a course he was taking in his senior undergraduate year. The audience was rapt, and I'm certain would have listened to him for hours.

In 1985, Dr. Victor Miller—then at IBM Watson Research Lab—and Dr. Neil Koblitz at the University of Washington independently invented elliptic curve cryptography. Both Dr. Miller and Dr. Koblitz were recognized and honoured at the 2004 ECC Conference for their achievements, and both gave insightful talks about the thought processes leading up to this great discovery. It was indeed a pleasure and a privilege to present each of them with mementos commemorating the occasion.

The conference was also the venue for introducing the first annual ECC Visionary Award. The recipient of this award was Dr. Walt Davis, who recently retired from his position as a senior vice-president at Motorola.

I first met Walt in 1994 and had the opportunity to discuss ECC in some depth with him then. He realized that security was a must for Motorola and that ECC was the only technology that would work in their constrained environments. Shortly thereafter, Certicom and Motorola embarked on a project to design and fabricate a VLSI (Very Large Scale Integration) device to implement ECC. At our conference, Walt talked about his vision for the future, the role that security will play in it, and the need for ECC.

I would like to thank these gentlemen, the other speakers, and all participants for making the conference a great success. I was humbled to be surrounded by so many fine and distinguished people. I look forward to seeing you at the next Certicom ECC Conference, which will be held October 3-5, 2005.

The Use of Public-Key Cryptography in BlackBerry

As Director of BlackBerry Security at Research In Motion Limited, Herb Little's role is to ensure that BlackBerry is as secure as possible. In his presentation "The Use of Public-Key Cryptography within BlackBerry", Little discussed why only public-key cryptography, and more specifically ECC, was used to solve the issues that RIM faced to secure BlackBerry.

For those unfamiliar with the BlackBerry, this handheld device acts as an extension of a user's desktop. Users have access to a number of applications, including calendar and real-time email in a small, portable device that can also be used as a mobile phone. The handheld is extensible by third party application developers. The development environment is freely available on RIM's website and includes a full featured crypto API that can be used to develop secure applications for a variety of verticals, including healthcare and financial. Currently, there are over two million BlackBerry users worldwide.

In earlier versions of the BlackBerry, the master key, which encrypts all the wireless transmissions, was created at the user's desktop computer and injected into the BlackBerry Enterprise Server (BES)–which pushes the user's email out–and the handheld via USB or the serial port. With the latest version of BlackBerry 4.0, however, the desktop application was made optional to simplify the product. This left BlackBerry developers with the challenge of how to get the handheld and server to agree on a master key without the help of a desktop.

RIM decided on a mechanism that could bootstrap from a small shared secret, i.e. a password, to a cryptographically strong key, all the while immune to offline dictionary attacks. For RIM, the use of public-key cryptography was the only viable solution in order to be able to manage the number of required keys. RIM chose the Simple Password Exponential Key Exchange (SPEKE).[1] (For the mathematically inclined, SPEKE is the same as the regular Diffie-Hellman key agreement protocol, except that the hash of the password is used as the generator of the group.)

Market demands and the need for stronger security in BlackBerry 4.0 also drove the switch to 256-bit AES from 3DES. AES is the symmetric-key encryption algorithm recommended by NIST, and 256-bit is the current recommendation for classified government communications. This necessitated a change in the matching public key algorithm, and it was here that the choice of ECC really shined.

The National Institute of Standards in Technology (NIST) recommends that the security level of key management should match the level of the bulk cipher. For Little and his team, who recognized this as well, the options were 512 bit ECDH (Elliptic Curve Diffie-Hellman), 15360-bit RSA, or 15360-bit Diffie-Hellman.

Each of these algorithms have their own advantages and trade-offs. Large keys have an impact on the performance of constrained devices. RIM ran a series of tests to determine the performance levels of the above three algorithms for key generation, encryption/verify (with public key) and decryption/sign (with private key). (See Figure 1)

Generally, ECC had the best timings for a general purpose cryptosystem. RSA is good for situations where only public key verification is needed.

In choosing a cryptosystem, there are several things to consider. If compatibility with an existing system is required, the device must support whatever the existing system dictates. ECC is RIM's preferred choice of cryptosystem for systems requiring a high level of security, key generation, or private key operations.

For operations involving only public keys (e.g. verifying a signature), RSA is RIM's preferred choice since an RSA public key operation is so fast.[2]

RIM uses the following ECC algorithms as part of BlackBerry 4.0:

- **Over the Air (OTA) Provisioning: ECSPEKE**
- **IT Policy Authentication: ECDSA**
- **Content Protection: ECDH**
- **OTA Re-key: ECMQV**

RSA is used on the BlackBerry for signature verification.

According to Little, "…once you get into the higher security levels, ECC, at least on the constrained device, is much more practical than RSA." For them, ECC-based algorithms provided a much better match for AES and SHA-2 than RSA and other alternatives. ■

Figure 1: Comparison of ECC vs. RSA vs. DH*

	ECC (256 R1)	RSA(3072)	DH (3072)
Key Generation	166 ms	N/A**	38 s
Encrypt Verify	150 ms	52 ms	74 s
Decrypt Sign	168 ms	8 s	74 s

** Timings were taken on a BlackBerry 7230 at a 128-bit security level. Timings at a 256-bit security level would show even greater differences between ECC, RSA and DH.*
*** Time was too long to measure*

[1] *as defined in IEEE P1363.2 Password Based Public Key Cryptography*
[2] *(especially when e=3)*

Grand Beginnings

continued from page 1

The full spectrum

Variety was a key consideration in designing the conference, in order to lay the foundation for a full understanding of ECC and its capabilities. To that end, speakers' subjects covered a vast range of topics, from the origins and early days of ECC through to practical implementations of elliptic curve cryptography today and its potential for the future.

RIM speakers David Yach and Herb Little talked about the inclusion of ECC in their company's highly successful products; Dr. Matt Campagna, standing in for Dr. Leon Pintsov, described how Pitney Bowes is using ECC-based digital signatures to secure the postage applied by postage meters; and Norm Kern explained how Unisys is employing ECC to facilitate check-clearing in the financial services sector.

Dr. Darrel Hankerson examined some of the challenges associated with–and approaches to–implementing cryptography on high-performance hardware; Dr. Robert Lambert looked specifically at embedding the elliptic curve digital signature algorithm (ECDSA) on an ARM processor.

John Stasak of the U.S. National Security Agency offered insight into the rationale behind his organization's choice of ECC for data protection and walked through the terms of the license by which the NSA acquired use of ECC.

Recognition and reflection

Dr. Alfred Menezes, Certicom founder Dr. Scott Vanstone, Dr. Ralph Merkle, and Drs. Koblitz and Miller all offered their individual perspectives on the evolution of public-key cryptography and ECC over the years–exploring the mathematical underpinnings as well as the personal histories involved.

The session concluded–prior to the award presentation for Dr. Davis–with Dr. Jerry Krasner's big-picture perspective on the importance of embedded security from a market competition perspective and why ECC is ideal.

Energized and engaged

"We were very pleased by attendee response to the event," said Melonia Montreuil da Gama, Certicom Marketing Programs Manager and ECC Conference organizer. "The feedback we received indicated overwhelmingly that attendees felt we'd put together a strong panel of speakers and a good slate of topics. They really appreciated the opportunities to network and make new contacts and to talk informally about the work they're doing. Almost everyone asked if we were planning to do it again."

In fact, Certicom is in the early stages of preparing for next year's ECC Conference, which will build on the success of this inaugural event to deliver even more of what audiences are looking for.

"What impressed me perhaps most of all," said Scott Vanstone, Certicom's Founder and Executive Vice-president of Technology, "was the sense of genuine community among those who attended the conference. More than just a roomful of people with some business interests in common, there was a true feeling of participation, of engagement and enthusiasm. I found it tremendously gratifying, and on a personal level as well as professionally I can't wait for next year when we get to do it all again." ■

The Speakers and Their Subjects

Dr. Alfred Menezes (University of Waterloo),
The First 29 Years of Public-key Cryptography

Dr. Darrel Hankerson (Auburn University),
Implementing Issues on Modern (Higher-performance) Hardware

Dr. Robert Lambert (Certicom), ***Embedding ECDSA***

David Yach (Research In Motion Limited),
Keynote Address

Dr. Scott Vanstone (Certicom), ***ECC Past, Present and Future***

Dr. Neal Koblitz (University of Washington),
The History and Prehistory of ECC

Dr. Victor Miller (Institute for Defense Analyses – Center for Communication Research),
The Invention of Elliptic Curve Cryptography

Dr. Ralph Merkle (Georgia Tech Information Security Center), ***Public-key Cryptography – The Early Years***

Dr. Leon Pintsov (Pitney Bowes Fellow and VP International Standards and Advanced Technology),
Elliptic Curve Cryptography in Postal Applications

Herb Little (Research In Motion Limited),
The Use of Public-key Cryptography in BlackBerry

John Stasak (National Security Agency),
NSA's Elliptic Curve Licensing Agreement

Norm Kern (Unisys),
Securing Check 21 Image Exchange

Dr. Jerry Krasner (Embedded Market Forecasters),
The Key Differentiator for Embedded Developers and Vendors

Dr. Walt Davis (Consultant),
Musings on the Past and Future of Wireless Security

The Certicom ECC Conference 2004 was held between November 15 and 17, 2004, in Toronto, Ontario, Canada. The second annual ECC Conference will take place from October 3-5, 2005.

A Brief History
The origins of public-key cryptography and ECC

At Certicom's ECC Conference in November 2004, several speakers offered their personal insights into the beginnings of public-key cryptography and the rise of ECC. The following article represents an amalgamation and condensation of the stories they told.

According to Dr. Alfred Menezes, Professor of Mathematics at the University of Waterloo and co-author—with Dr. Darrel Hankerson and Dr. Scott Vanstone—of the Guide to Elliptic Curve Cryptography, the history of public-key cryptography has had four phases thus far:

1975-1979: the early years
1980-1989: protocols
1990-1999: deployments
2000-present: new developments

Phase I: the early years

The first major event in this history was the definition of the concept of public-key cryptography itself. Prior to the 1970s, symmetric-key cryptography had been the only cryptographic mode: parties involved in covert communications would agree on a shared secret key and then use that key to encrypt and authenticate their exchanges.

In the early 1970's, a new idea began to take shape. One of its originators was Ralph Merkle. Today, Dr. Merkle is a Distinguished Professor of Computing at Georgia Tech's Information Security Center; back in the fall of 1974 he was an undergraduate student looking for a topic for his 'quarter project', and eventually settled on a problem of cryptography.

As he says, "I came to cryptography as an outsider, which had its advantages and disadvantages. The advantage was that I was uncommitted to prior schemes. The disadvantage is that I had a hard time describing to people what I actually meant."

Merkle's work—which originated around questions of how to recover security in a compromised system—led him to develop the Puzzles Method, a technique that showed it was possible to create problems of controllable difficulty using puzzles.

In his example, A begins creating random puzzles and sends them to B. B also creates puzzles and compares them to those of A, looking for a collision. When that collision occurs, B sends the common puzzle back to A. Since A and B both generated that puzzle, they can easily find its solution (in Merkle's scenario, a 40-bit number). This solution is their shared key.

While it might take A and B 2^{20}=1,000,000 puzzles to hit a match, an eavesdropper would have to try all 2^{40} possibilities to solve the common puzzle and deduce the shared key. In other words, the eavesdropper would have to do a lot more work to reach the same conclusion.

Contained within this realization were the seeds of public-key cryptography: the idea that puzzles—or keys—could be publicly known while the contents of the information exchanges they relate to would remain essentially secure.

Merkle admits that ideas seldom appear complete and polished all at once. Nor are they always immediately appreciated by others. In the beginning, Merkle found little support for his ideas and their application to cryptography. Fortunately, he wasn't the only one thinking along these lines. One day, someone said to him, "You know, there are these guys down in Berkeley who sound just like you." Those guys, it turns out, were Whit Diffie and Martin Hellman, with whom Merkle soon became an associate and collaborator. And it was Diffie and Hellman's 1976 paper, New Directions in Cryptography, that finally caused the concept of public-key cryptography to 'click' with readers.

Phase II: the Protocols

Two basic types of public-key schemes emerged in the 1970s: Diffie-Hellman for key agreement in 1975, and key transport and digital signing schemes proposed by Rivest, Shamir and Adleman (RSA) in 1977.

The Diffie-Hellman key agreement scheme derives its security from the hardness of the discrete logarithm problem: given p, g, and g^a, find a. RSA takes its security from the hardness of the integer factorization problem: given a number n that is the product of two primes, p and q, find p and q.

Yet by the 1980s, researchers realized that despite the hardness of these problems, the basic cryptographic functions themselves did not provide sufficient security. Careful protocol design was needed together with a methodology for defining precisely the security objective and proving that a protocol met that objective.

The first step was to imagine the most powerful adversary possible; the next, to assign that adversary a goal or set of goals as weak as possible. A protocol could be deemed secure if an ultra-potent adversary could not achieve his or her ultra-weak goals. This model evolved eventually into the notion of 'provable security', which invokes specific computational assumptions that can be used to prove that a proposed protocol meets the requirements of its security definition. It wasn't until the mid-1990s that provably secure protocols actually began to be efficient enough to warrant real-world application. However, other developments occurred before then. Most prominently, the ElGamal public-key encryption and signature schemes emerged in 1984 to rival those of RSA. Rather than integer factorization, the ElGamal techniques were based on the discrete logarithm problem. So too was elliptic curve cryptography (ECC), which appeared on the scene in 1985.

The discovery of Elliptic Curve Cryptography

ECC was discovered in the 1980s by Dr. Victor Miller (today of Princeton's Center for Communications Research) and Dr. Neal Koblitz (currently Professor of Mathematics at the University of Washington). As both recall, elliptic curves had belonged to a fairly arcane area of pure mathematics until that time and few people—including themselves—had considered elliptic curves might have practical applications.

Yet the idea had begun to circulate that elliptic curves could be used to attack cryptosystems, with the Lenstra manuscript of 1984 on

continued on page 6

A Brief History

continued from page 5

integer factorization being an intellectual catalyst in this respect. Koblitz and Miller each wondered if elliptic curves might not also form the basis of a potential cryptosystem.

There were good mathematical reasons for this conjecture. With finite fields, there is only ever one multiplicative group for a given prime. At the same time, there are many elliptic curves, of varying sizes for any given prime. This is important because, as research by Pohlig and Hellman showed, the largest prime factor of the group size governs the hardness of the discrete logarithm problem. In other words, elliptic curves offer ample opportunity to be extremely hard. Most importantly, index calculus–a method that breaks the 'square root bound' and reduces the amount of work an eavesdropper has to do to break a public-key cryptosystem–doesn't work on elliptic curves.

Phase III and beyond

Throughout the 1990s, much research was carried out and numerous standards which incorporate ECC emerged; including PKCS, SSL, NIST, ISO, IEEE, ANSI and others. Public-key infrastructures (PKIs) were devised to deal with the burdens of large-scale certificate management in public-key cryptosystems.

Since the turn of the millennium, several new developments have taken place. AES, the Advanced Encryption Standard, was introduced to meet short-, medium- and long-term symmetric-key crypto needs. NIST, the National Institute for Standards in Technology, has insisted that the strength and scalability of AES be matched on the public-key side; criteria that, of all options, ECC meets best.

ECC has also shown itself as extremely well suited to the unique demands of the wireless communications environment where bandwidth is at a premium and device power and processing resources are constrained.

Because of its advantages, ECC was chosen by the U.S. National Security Agency to meet the new, stronger public-key requirements of its crypto modernization program. Specifically, the NSA selected ECC to protect mission-critical national security information by providing authenticated key agreement, digital signatures and encryption systems.

Researchers have been working very hard on finding alternative public-key systems. So far most of their efforts have failed in that the new systems are either less secure than ECC or significantly slower. Much effort has been expended on studying hyperelliptic curves, which are generalizations of elliptic curves. (Elliptic curves are the hyperelliptic curves of genus one.) So far, it has been shown that while hyperelliptic curves of genus greater than 2 are less secure than elliptic curves, genus 2 hyperelliptic curves have comparable security. However, genus 2 curves are slower than elliptic curves so there is no compelling reason to use them.

In a relatively short space of time since its introduction, ECC has moved from the province of pure-math Number Theory into the mainstream of cryptography. And, as Dr. Neal Koblitz observes, over the course of the last three decades, cryptography itself has changed–from what used to be almost exclusively a military concern into something at the core of modern business and the daily lives of consumers. Koblitz, however credits Dr. Scott Vanstone, founder of Certicom, for his role in helping move ECC to more practical applications: "It was entirely Scott Vanstone and his students and collaborators who transformed [ECC] from a gleam in two mathematicians' eyes to something that was ready for prime time." ■

For more information about ECC, download the Certicom *"Catch the Curve"* white paper series, available at:
www.certicom.com/catchthecurve/cc21

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

certicom™