Certicom's Bulletin of Security and Cryptography

CØDE&CIPHER

This issue of Code and Cipher reviews the second annual **Certicom ECC Conference** and summarizes some of the key discussions.

The Cryptography of Today and Tomorrow

"It's tough to make predictions, especially about the future."
–Yogi Berra
[borrowed from ECC conference presenter, Jim Dworkin]

Although no one would claim to be clairvoyant, the more than 100 attendees at the 2nd Annual Certicom ECC Conference, agreed that ECC is the cryptography of today and the future. During the three-day conference held in October, the finest minds in cryptography and security representing Australia, Canada, Europe, and the United States gathered in Toronto to discuss the many current and future applications and standards employing ECC.

Certicom ECC Visionary Award winner, Dr. Gerhard Frey, Chair for Number Theory at the Institute for Experimental Mathematics of the University of Duisburg-Essen, Germany, best summed up the value of ECC with the following: "Without doubt it is important to communicate in a secure and inexpensive way by using open networks and to be able to sign documents, authenticate persons and machines with simple protocols and clear, easy-to-follow implementation rules."

Under the conference theme of, "Smallest, Fastest, Strongest", Dr. Scott Vanstone, founder and EVP strategic technology at Certicom, set the stage by providing an overview of where ECC is being deployed. His talk was supported throughout the conference by the guest speakers who gave specifics about their use of ECC. Keynote speaker, David Maher, EVP and CTO of Intertrust, talked about digital rights management (DRM) applications, illustrating how DRM has evolved from being a roadblock to an enabler. He discussed the different layers of intellectual property and made the point that as DRM systems become more distributed and dynamic, there is a greater need for an ECC public-key system. XM Satellite Radio's senior chief engineer, Richard Michalski, gave an overview of security requirements for conditional access systems before elaborating on where and how it is used in the XM Satellite Radio system.

ECC on the move with mobile applications

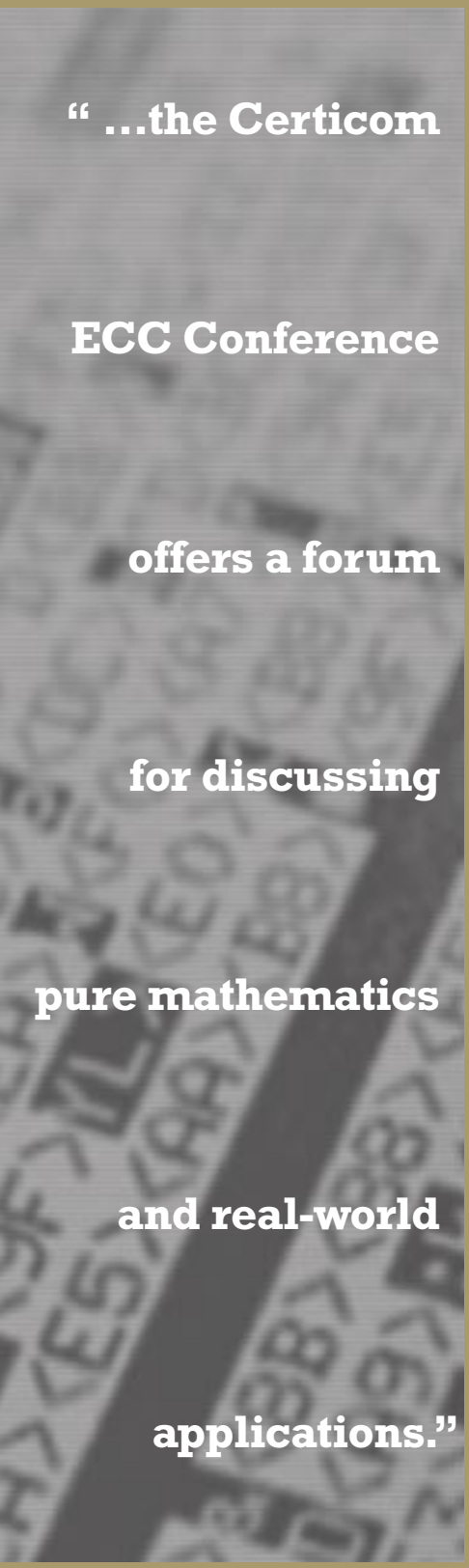
Herb Little, an early ECC adopter at Research In Motion, discussed the use of SPEKE over elliptic curves in password-based key establishment while Bill O'Brien of Bell Canada used

continues on page 5

Certicom ECC Visionary Award

One of the conference's highlights was the presentation of the Certicom ECC Visionary Award to Dr. Gerhard Frey for his contribution to the advancement of ECC. In presenting the award, Dr. Scott Vanstone described Dr. Frey as one of the foremost mathematicians of our time.

Dr. Frey is a German mathematician known for his work in number theory. In 1996, Dr. Frey was awarded the Gauss medal of the "Braunschweigische Wissenschafteliche Gesellschaft" for his work on Fermat's Last Theorem. (For over 350 years, some of the greatest minds of science struggled to prove what was known as Fermat's Last Theorem.) He is the Chair for Number Theory at the Institute for Experimental Mathematics of the University of Duisburg-Essen, Germany.



Crypto Column by Dr. Scott Vanstone

A Second Successful Certicom ECC Conference

I've always considered myself fortunate to have one foot in the commercial sector and one in academia. Not a lot of mathematicians get that opportunity. But for three days at the ECC conference, my friends, colleagues and associates got a glimpse into my world. The only one of its kind, the Certicom ECC Conference offers a forum for discussing pure mathematics and real-world applications. The conference brings together some of the best mathematicians in the world with some of the most innovative entrepreneurs and business people to discuss elliptic curve cryptography and its real-world applications.

The first day of the conference kept true to this form. It began with a discussion on the use of ECC in digital rights management, a relatively new area that uses security to promote fair use rights for music, visual artwork, computer and video games, and movies. The day ended with attendees toasting one of the foremost mathematicians of our time, Dr. Gerhard Frey, who was awarded the Certicom ECC Visionary Award 2005 in recognition of his seminal contributions to the advancement of ECC. As Gerhard deftly illustrated, there is a reciprocal relationship between pure mathematics and real-world applications, and our many speakers illustrated this relationship.

As proponents of ECC, we are confident ECC will become the de facto public key scheme. This past spring the National Security Agency specified the use of ECC algorithms in its Suite B recommendations for securing classified and unclassified communications. Of all the validations one can receive, this has to be the most significant. Not only does Suite B set guidelines for protecting government communications, it greatly influences best practices in the commercial sector. When a friend of mine heard about this endorsement he phoned to announce that I should get a lifelong achievement award for perseverance. The twenty years of perseverance is paying off.

ECC is in every major standard in the world and ECDSA is one of the most widely used signing algorithms. ECC is deployed in numerous applications–digital postage marks, electronic payment systems, consumer electronics, anti-cloning and conditional access systems, and many others. The Federal Aviation Association uses ECC to secure communications between aircraft and control towers, Research In Motion built it into the Blackberry and ECC is found in the Digital Transmission Content Protection (DTCP) standard, which is used over Firewire to secure the digital link between consumer devices that transfer digital content. And the list of applications continues to grow as we anticipate ECC being used in epassports and sensors networks.

I would like to thank the speakers and all participants for contributing their time, knowledge and experience to make the conference a great success. I found it humbling and exhilarating to be surrounded by so many intelligent and accomplished people and I look forward to seeing you at the next Certicom ECC Conference, to be held November 2006 in Toronto, Canada.

Certicom ECC Conference 2005: Snapshots of Innovation

In this review of the Certicom ECC Conference 2005, we'd like to give you detailed descriptions of each presentation given at the conference because the value of the information warrants it. But to do that we'd have to turn this six-page newsletter into a book.

Instead, we've decided to write snapshots of selected presentations with the hope that they will give you some insight into the exciting applications that are being developed and deployed using ECC.

If you'd like to learn more about a topic presented at the conference, please contact Certicom at +1-613-254-9258 or info@certicom.com.

Willam (Bill) O'Brien,
Systems Solution Architect, Corporate Security, Bell Canada

A Practical Evolution of ECC for Mobile Computing

As systems solution architect for Bell Canada, O'Brien is responsible for ensuring that any data that hits the Bell network is secure, regardless of the mobile device used. To deal with this challenge, O'Brien has a toolbox of security mechanisms that includes ECC and AES.

During his talk, O'Brien used several case studies to illustrate the importance of ECC's speed, flexibility and efficiency in mobile communications. In one of the scenarios, he discussed the challenge of maintaining secure connectivity with moving law enforcement cruisers. O'Brien and team created a datagram connection between a police cruiser and a tower using 1X-RTT. He used ECC-based certificates to authenticate sessions and ECC-public/private keys to encrypt the data. By rotating keys during a session he prevents encrypted data from being broken and there is no need to re-establish a connection should he lose a signal. The transmission resumes from where it left off.

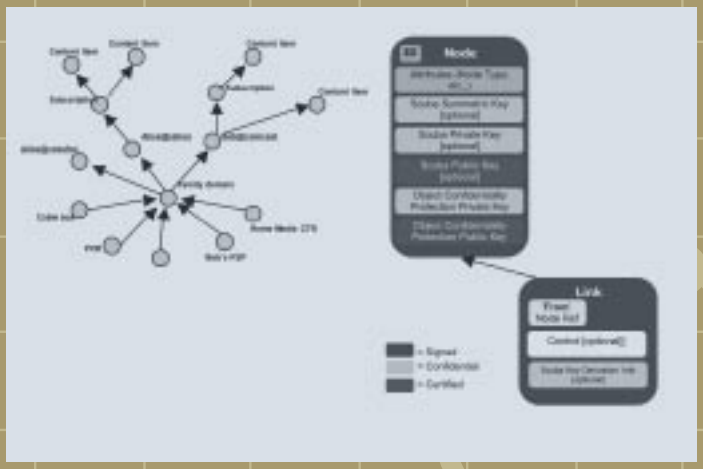
In each of his scenarios, which ranged from securing connections for moving vehicles to controlling the back door of an IP network and regulating access points in the Bell stores, O'Brien explained why ECC is vital to his security policies.

Digital Rights Management, the Real Story

David Maher
Executive Vice President and Chief Technology Officer, Intertrust

The first keynote speaker set the tone for the conference by underscoring the importance of Smallest, Fastest, Strongest, drawing parallels between what is needed in the digital rights management industry and what is needed in cryptographic systems. Maher discussed the evolution of digital rights management (DRM) and the need for efficient and strong cryptography in the new DRM model.

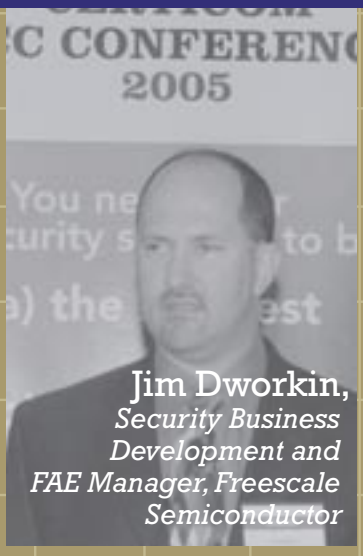
He explained how the DRM industry's early emphasis on copy protection led to roadblocks and a draconian attitude towards protecting content. Today, the industry is driving towards integration of media services with electronic commerce services. Maher explained how this shift in thinking is only possible with granularity. He showed that by breaking DRM into functional tiers and studying the relationships within the device and services tiers (what he referred to as nodes and links) industry players can better understand the issues, remove barriers and promote interoperability. Functional tiers could include 'home and enterprise gateways' and 'home and personal networks and devices'.



Essential to the node system is a signing mechanism that establishes a trusted relationship between each node. That is, at each node in the system, efficient cryptography is needed to quickly establish integrity and authentication of signed objects to determine if a user is part of the domain and if a device can use the content.

As systems become more distributed and dynamic as described above, there is a greater demand for faster, smaller and stronger public key distribution systems to secure content and rights while promoting interoperability.

CERTICOM ECC CONFERENCE 2005 SNAPSHOT



Jim Dworkin,
Security Business Development and FAE Manager, Freescale Semiconductor

Integrated Hardware Security

In his presentation, Dworkin discussed how the amount of digital content being handled by a network and the increased complexity of attacks is changing the role of the processor well beyond its original function. Traditionally, network equipment has used discrete security processors, but the security functions are merging into integrated processors as manufacturers like Freescale try to provide a single chip that performs all security functions across multiple layers of the protocol stack. But as Dworkin pointed out, this only addresses crypto-based security and content processing, which may not be enough security in some applications if the software running on a device cannot be trusted. To be truly secure, while still realizing performance benefits, organizations need a trusted embedded computing environment – a hardware-based, software security architecture that leverages the power in today's communications processors.

Dworkin explained that Freescale's PowerQUICC processors with integrated security engines are designed to accelerate industry standard algorithms in hardware. Freescale's PowerQUICC

continues on page 6

Redefining Identity, Information and Privacy with ECC

In this talk, Richard explained how he uses ECC to protect identity and privacy in electronic communications and ultimately prevent spam. He believes a fundamental flaw in today's security environment begins the moment a user shares his public-key certificate because the certificate puts context around the key, such as who issued it, who owns it, and when it expires. Consequently, anyone who has that information can use it or pass it along.

Using ECC, Avanza has created a technology that protects that information in what Richard calls 'a managed identity'. The technology creates a strong cryptography string that looks and acts like an email address but includes an encrypted certificate and private key. Every unique electronic relationship has a unique key – which makes it impossible for anyone outside of the relationship to obtain the private information. The key is simple enough that specialized servers are not needed. With its strength and efficient size, ECC, which provides authentication and key exchange, is the only public key that will work.

The Cryptography of Today and Tomorrow

continued from page 1

a series of case studies to illustrate how Bell is using ECC to protect mobile computing and Ravi Belwarl of Nokia discussed the use of cryptography in Nokia's mobile devices. Philippe Richard of Avanza Technologies discussed how his company uses public keys to protect email identify at the moment the information is created. Dr. Peter Landrock of Cryptomathic showed how ECC could be used in electronic voting, from the registration and voting stages through to the final counting of votes.

ECC hardwired

Hardware specialist, Brett Thompson of Eracom Technologies, explored the use of ECC in future electronic payment systems. Dr. Nicko van Someren, founder of nCipher, proved the value of ECC's security and scalability in his description of hardware security modules in large enterprises. Freescale's Jim Dworkin described the advantages of using ECC in hardware to establish trust and the importance of having this trust in the new reality of converged communications.

SPYRUS' chief scientist, Robert Jueneman, examined ECC from the perspective of protecting government applications, providing suggestions for building on the National Security Agency's Suite B recommendations for securing information and mitigating side channel attacks. Presentations by industry watchers Ralph Poore and Jeff Stapleton of Innove examined the how and why of transitioning to stronger cryptography systems.

Throughout the conference speakers gave presentations on mathematics to show the synergetic relationship between theory and application and how advancements in one area positively affect the other. Dr. Robert Lambert of Certicom used unorthodox props, such as jars of cranberry juice, to illustrate the new Fast ECDSA Verify algorithm. Dr. Gerhard Frey showed how pure mathematics provides data security.

Rounding out the topics was a discussion on standards by Certicom's new chief technology officer, Bill Lattin, who reviewed new and emerging standards in ECC, of which there were plenty to discuss.

Participants unanimously agreed that the 2nd Annual Certicom ECC Conference provided an exceptional forum to learn about advancements in ECC in both the commercial and academia arenas and to network with security-savvy and innovative individuals. Buoyed by this year's success, organizers have already started planning for the 2006 conference, scheduled for November 14-16 in Toronto. Register today at: www.certicom.com/conference2006

Recent Developments in ECC Standardization

Of the talks given at the conference, Lattin's presentation on standards was arguably one of the most relevant to the application of ECC. To paraphrase Lattin, you need to standardize technology or the world won't buy into it. Dr. Scott Vanstone recognized that when he first began working with ECC and today, 20 years later, ECC is in every major standards group in the world.

In his talk, Lattin summarized the many standards being updated to include ECC. For instance, ANSI is going through its five-year update and in doing so is adding new NIST curves and SHA-2 support and removing composite curves. NIST 800-56 is important because it offers guidance on key agreement and key transport schemes and on what crypto parameters to use, something FIPS 140-2 doesn't do. NIST SP800-57, which provides recommendations for key management, is targeted at government organizations but has relevance in the commercial sector too as it clearly establishes the strengths and expected lifetimes of various cryptosystems.

Of all the standards discussed, Lattin pointed to ANSI X9.82 as being one of the most important new standards as it deals with random number generation. Without true randomness, security is weak. High quality cryptographically strong random numbers are essential for keys, nonces, digital signatures and many other security mechanisms.

Other standards with recent ECC activity include:

ANSI X9.92: Pintsov-Vanstone Signatures for digital postal marks and electronic passports
IETF: the use of ECDSA in IPSec/IKE standard
IETF: ECC ciphersuites for TLS
IETF: Additional algorithms and identifiers for use of ECC with PKIX
IETF: ECMQV and ECDSA being added to MIKEY and ECDSA for XML digital signatures

Bill Lattin,
Chair of the SECG Industry Consortium and CTO, Certicom

IETF: new hash functions for S/MIME and inclusion of ECDSA, ECDH and ECMQV
SECG: The SEC 1 & 2 standards are being updated to include AES, SHA-2, and the NIST curves.

Lattin's presentation underscored the fact that cryptosystems are changing. AES is replacing TDES, NIST has published requirements to migrate to larger bit sizes and with SHA-1 under attack in signature applications, SHA-2 adoption is rapidly growing.

In security circles, one of the most significant standard-related announcements this year is the National Security Agency's (NSA) Suite B recommendations for using ECC to protect classified and unclassified communications. Not only does Suite B affect government security, but it raises the bar in the commercial industry, setting new best practices for protecting sensitive corporate data.

On October 31, Bill Lattin joined Certicom as its Chief Technology Officer to lead Certicom's technology strategy. He will continue in his role as chair of *The Standards for Efficient Cryptography Group* (SECG), an industry consortium founded to develop commercial standards that facilitate the adoption of efficient cryptography and interoperability across a wide range of computing platforms.

Integrated Hardware Security

continued from page 4

processors accelerate ECC public-key operations as a viable market alternative to RSA and other public-key schemes to enable new levels of security for services such as SSL and IPSec in those applications that demand ECC. By integrating hardware acceleration for ECC, Freescale recognizes that the market values ECC as a viable commercial public-key algorithm. Furthermore, trusted platform services such as secure software and trusted boot can be found on Freescale's i.MX series of applications processors for mobile computing environments.

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™