

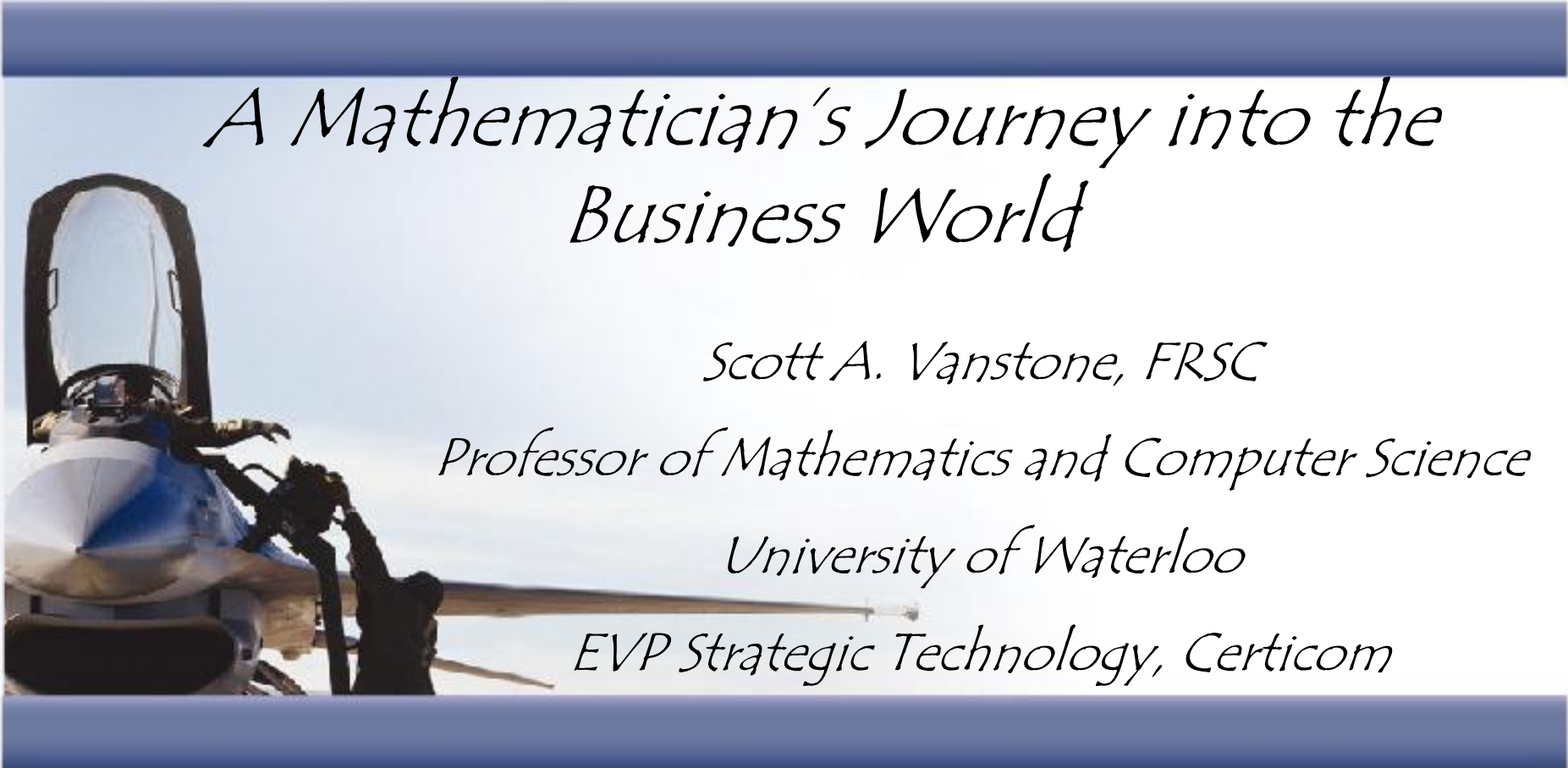


certicom

securing innovation



**protect your content,
software and devices**
with government-approved security



A Mathematician's Journey into the Business World

Scott A. Vanstone, FRSC

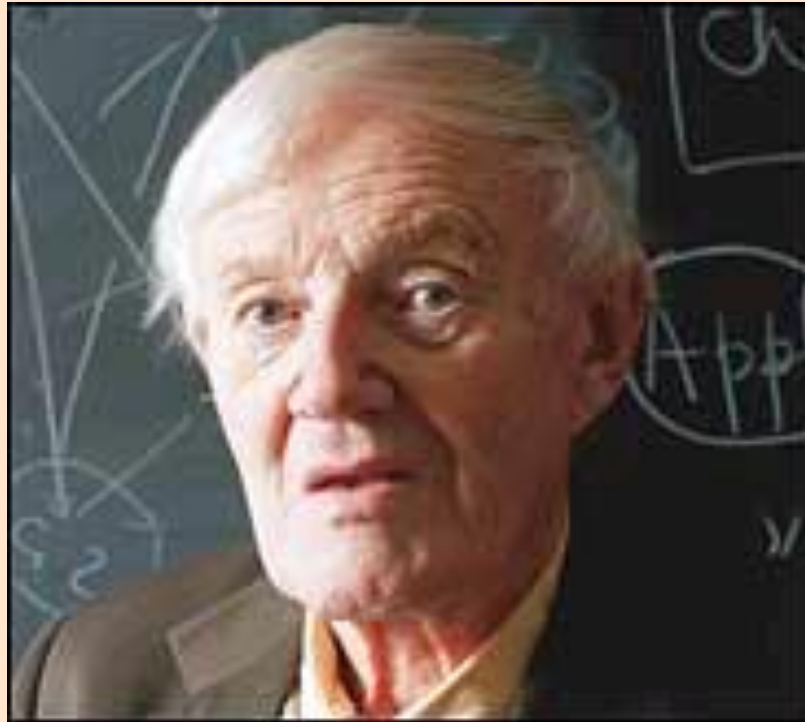
Professor of Mathematics and Computer Science

University of Waterloo

EVP Strategic Technology, Certicom

A Bit of History

- ❖ *The University of Waterloo has a long history in the area of cryptography and information security.*
- ❖ *The University was founded in 1957 but its connection to cryptography goes back to the beginnings of World War II.*
- ❖ *Professor William T. Tutte, one of the most distinguished professors at Waterloo, worked at Bletchley Park from 1941 to 1945.*



- ❖ *Tutte's work at Bletchley Park has been referred to by many as the greatest intellectual achievement of World War II.*
- ❖ *With only 4000 characters of ciphertext and matching plaintext Tutte was able to deduce how the German enciphering machine "Tuny" worked.*
- ❖ *An actual Tuny machine was never captured by the Allies until after the war.*

An Amazing Quote

- ◆ *At the opening ceremony for the Centre for Applied Cryptographic Research at the University of Waterloo (June 19, 1998) Tutte gave a lecture titled "Fish and I".*
- ◆ *"Now at my pre-Bletchley cryptographic school in London I had learned that you can sometimes get results by writing out a cipher text on a period and looking for repeats. I resolved to do this I can't say that I had much faith in this procedure but I thought it best to seem busy."*



This Lecture

- Services cryptography can supply.
- Symmetric versus public-key cryptography.
- A brief history of Certicom.
- Applications
- Government involvement.
- Conclusion.

Services Cryptography Can Provide

- Confidentiality
- Data integrity
- Authentication
- Non-repudiation

Think of the Postal Analogue

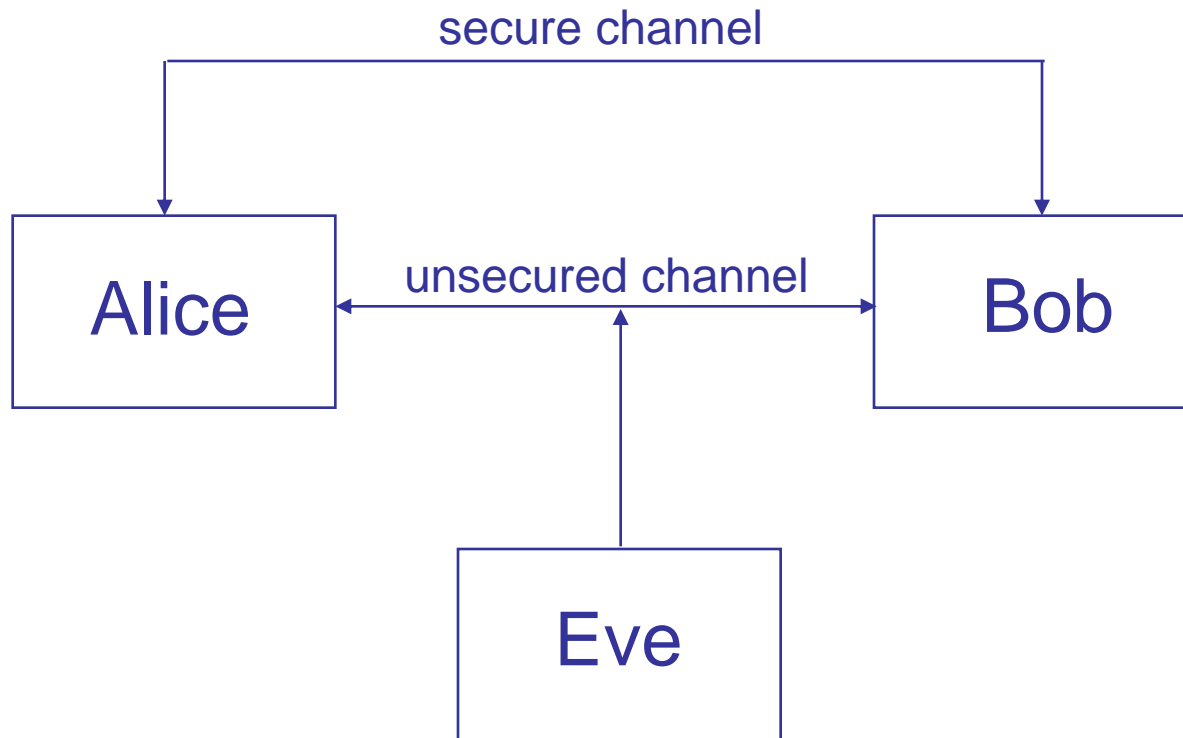
- You put a letter in an envelope to maintain the integrity of the information in the letter and keep the letter from prying eyes (integrity and encryption).
- You put your address in the upper left corner of the envelope to authenticate the sender which is you (authentication).
- You sign the letter so that at a later date you cannot say you did not send it.

The Digital World

- We want to mimic all of these services but electronically.
- This has been done and done more securely and efficiently than postal mail.
- It is all due to the advent of something called “public-key cryptography”.
- Canada is and continues to be a leader in this field.

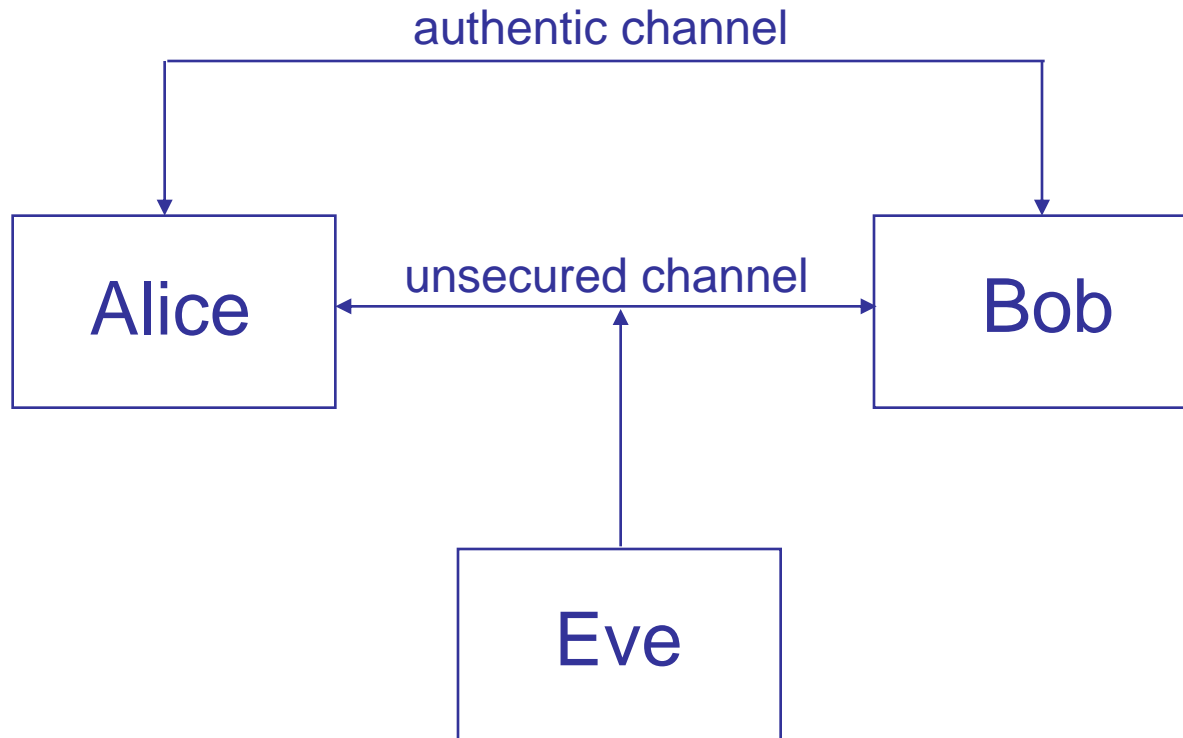
Symmetric-Key Cryptography

Communicating parties a priori share secret information.



Public-Key Cryptography

Communicating parties a priori share authentic information.



Symmetric-Key vs Public-Key

- Symmetric-Key has been used for thousands of years.
- Public -Key is relatively new dating from 1976.
- The mathematics to implement public-key existed in the 17th and 18th century but the realization came much later.

Why Symmetric-Key?

-
- Typically very fast for bulk encryption (confidentiality).
- The Advanced Encryption Standard (AES) is well accepted as a superior algorithm for symmetric-key.

Disadvantages

- Key management can be a serious problem.
- Non-repudiation (digital signature) is very difficult to realize.

Why Public-Key?

- One disadvantage of symmetric-key cryptography is key management.
- Public-Key provides an efficient method to distribute keys.
- Public-key offers a very efficient way to provide non-repudiation. This is one of the great strengths of public-key.

Disadvantages

- Public-key operations require intense mathematical calculations.
- They can be thousands of times slower to encrypt data than a well designed symmetric-key scheme.

Hybrid Schemes

- Use symmetric-key schemes to do bulk encryption.
- Use public-key techniques to pass keys so that key management is not a problem.

Basis for Public-key Schemes

- All commercially viable public-key schemes are based on hard mathematical problems.
 - Integer factorization
 - Discrete logarithms
 - Elliptic curve discrete logarithm
- The first two have primarily been used in the wired world.

Basis for Public-key Schemes

- All commercially viable public-key schemes are based on hard mathematical problems.
 - Integer factorization
 - Discrete logarithms
 - Elliptic curve discrete logarithm
- The first two have primarily been used in the wired world.

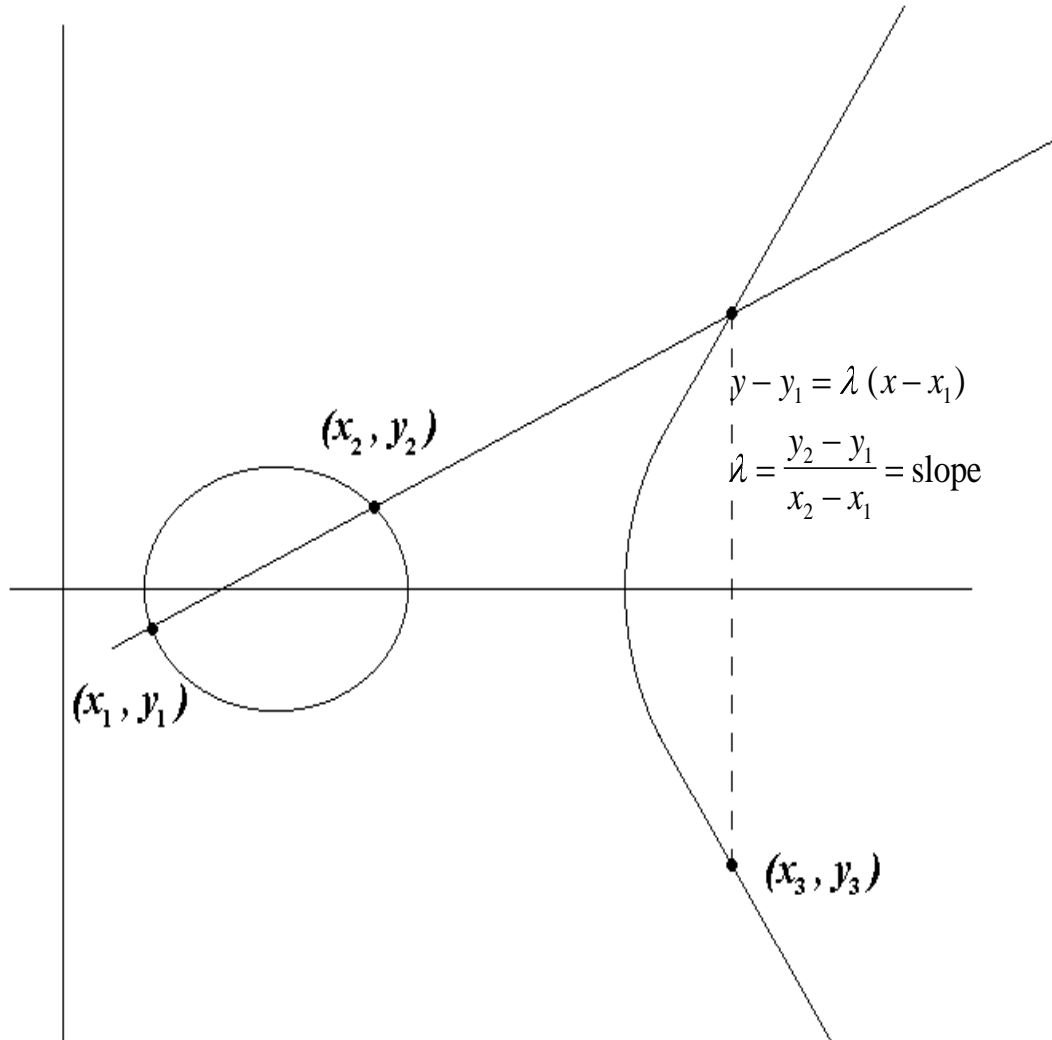
Digital Signatures

- *One of the truly great technologies that public-key cryptography can provide.*
- *Handwritten signatures are fixed to the message but not an integral part of the message.*
- *Digital signatures combine the message and private information of the signer.*

Why ECC?

- ❖ *Most security per bit of any known public-key scheme*
- ❖ *Ideally suited to constrained environments*
 - *Computationally efficient*
 - *Bandwidth efficient*
 - *Battery efficient*
- ❖ *Well studied*
- ❖ *Standardized in relevant influential international standards*

Elliptic Curve: $y^2 = x^3 + ax + b$



Brief History of Certicom

- My background is in combinatorics, finite geometries, design theory and coding theory.
- All of these areas rely heavily on finite fields.
- In 1976 public-key cryptography was discovered by Whitfield Diffie and Martin Hellman.

History (continued)

- My background was ideally suited to move into this new and exciting area of mathematics.
- Although Diffie and Hellman had the concept they did not have any practical realization of public-key cryptography.
- It was left to Rivest, Shamir and Adleman to provide a practical method to implement all of the features.

History (c0ntinued)

- In the early 80's two other researchers at the University of Waterloo and I discovered several protocols to implement encryption, key management and digital signatures.
- In 1985 we decided to commercialize this new technology.
- We originally called the company Cryptech.

History (continued)

- Coincidentally, ECC was introduced to the cryptographic research community in 1985 but Certicom was not started because of this.
- In 1990, Cryptech obtained financing from a few investors and was then able to hire people to sell the technology.
- This kept the company alive but not growing as we had hoped.

History (continued)

- At the Crypto'85 conference in Santa Barbara I attended a very interesting lecture by Victor Miller.
- Victor introduced elliptic curve cryptography (ECC) to the cryptographic research community.
- Leaving the lecture hall I knew that if ECC was secure it was superior.

History (continued)

- After Crypto'85, I returned to the University of Waterloo and began to investigate the ECDLP.
- Cryptech continued to sell the original technology into the 90's
- I felt that ECC had greater potential and a significant differentiator in the market place.

History (continued)

- After 8 years of intensive study on the security of ECC, I made the decision in 1993 that Certicom would put its energy behind this new technology.
- We would evangelize and put it into our software products.
- Having said this it was not until 1997 that we introduced our first toolkit with ECC.

History (continued)

- At this turning point we decide to correct some mistakes we had made in the first 8 years.
 - Standardization is crucial to the success of any cryptographic scheme.
 - Protect your intellectual property through the patent process procedure.
- We did not have the money to do either but we knew it was essential and we did it.

History (continued)

- As a mathematician and professor for many years I know that there are many mathematicians that frown on patenting.
- By patenting you leave yourself choices
 - You can license to others and perhaps make money.
 - You can give it away at a later date.
 - You may be able to trade for something else.

History (continued)

- By not patenting you leave yourself no choices.
- I can tell you from first hand experience that if we would not have patented what we found we would not have had the success that we ultimately realized.

History (continued)

- One of the early adopters of ECC was Motorola.
- Motorola was looking to provide a high level of security in their pagers.
- Pagers, being extremely constrained environments, were a good place to implement ECC.
- We built an ECC chip with Motorola that is used today.

History (continued)

- With the Motorola success we took the company public in 1995.
- The name was changed to Certicom.
- The company began to grow and by 2000 we had approximately 500 people
 - 200 hundred in Toronto
 - 300 hundred in Silicon Valley.
- Headquarters was moved to Silicon Valley.

History (continued)

- We wanted to address the US market and attract talented people from Silicon Valley.
- Certicom listed on the Nasdaq in 2001.
- Shortly thereafter the tech bubble burst and many high tech companies went under.
- Certicom survived the tech meltdown.

History (continued)

- Drastic changes were required.
- Headquarters moved back to Toronto.
- Major lay-offs.
- We survived because of the technology and good management in those days.

History (continued)

- The most significant event for Certicom and ECC came in October, 2003 when the NSA in the US licensed 26 of our patents for \$25,000,000.
- This allowed Certicom to become debt free and begin to grow again.

History (continued)

- The next major milestone for the technology came in February of 2005 when the NSA announced Suite B.

History (continued)

- We have come a long way since 1985.
- ECC is rapidly becoming the public-key scheme of choice.
- RIM acquired Certicom in March of 2009.
- This will drive adoption around the world much faster than we could do on our own.

RIM BlackBerry



- RIM was an early adopter of EC technology.
- RIM licensed Certicom's intellectual property and software to enhance their offerings to a wider community.

RIM (continued)

- Security on the Blackberry exceeds the security level mandated by the US Government to secure classified information.
- ECC at 521 bits

Certicom's Patent Portfolio

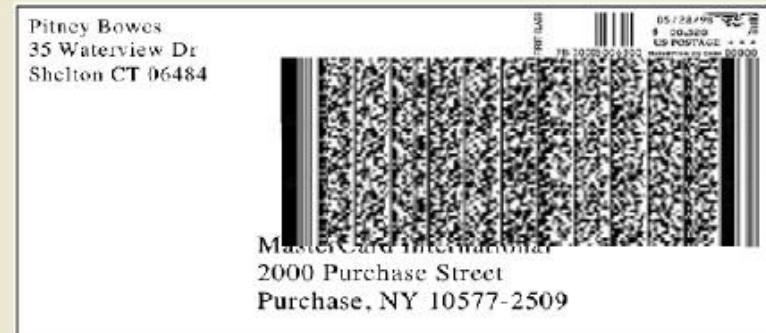
- RIM has the ability to use the portfolio defensively. They can trade patents with other companies and save money in the process.
- Certicom was never able to do this because of its size.

Digital Postage Marks

- ECDSA signature adds 40 byte appendix
 - Smaller alternative is the ECPVS scheme which adds as little as 20 bytes
- Cryptographic overhead of an equivalent DPM using RSA would add 128 bytes



ECC-based signature



RSA-based signature

6 times smaller signature with ECPVS

ECC in DPMs

- ❖ *ECC provides the smallest most efficient solution for this environment*
- ❖ *This has become a standard for Canada Post*
- ❖ *It is in a draft international standard*

QR - Codes

- Two dimensional bar codes used for advertising.
- Different from the two dimensional bar codes used in DPM.
- They are easier to read with a cell phone camera than a DPM.
- Security is required and only ECC works.

Airline Boarding Passes

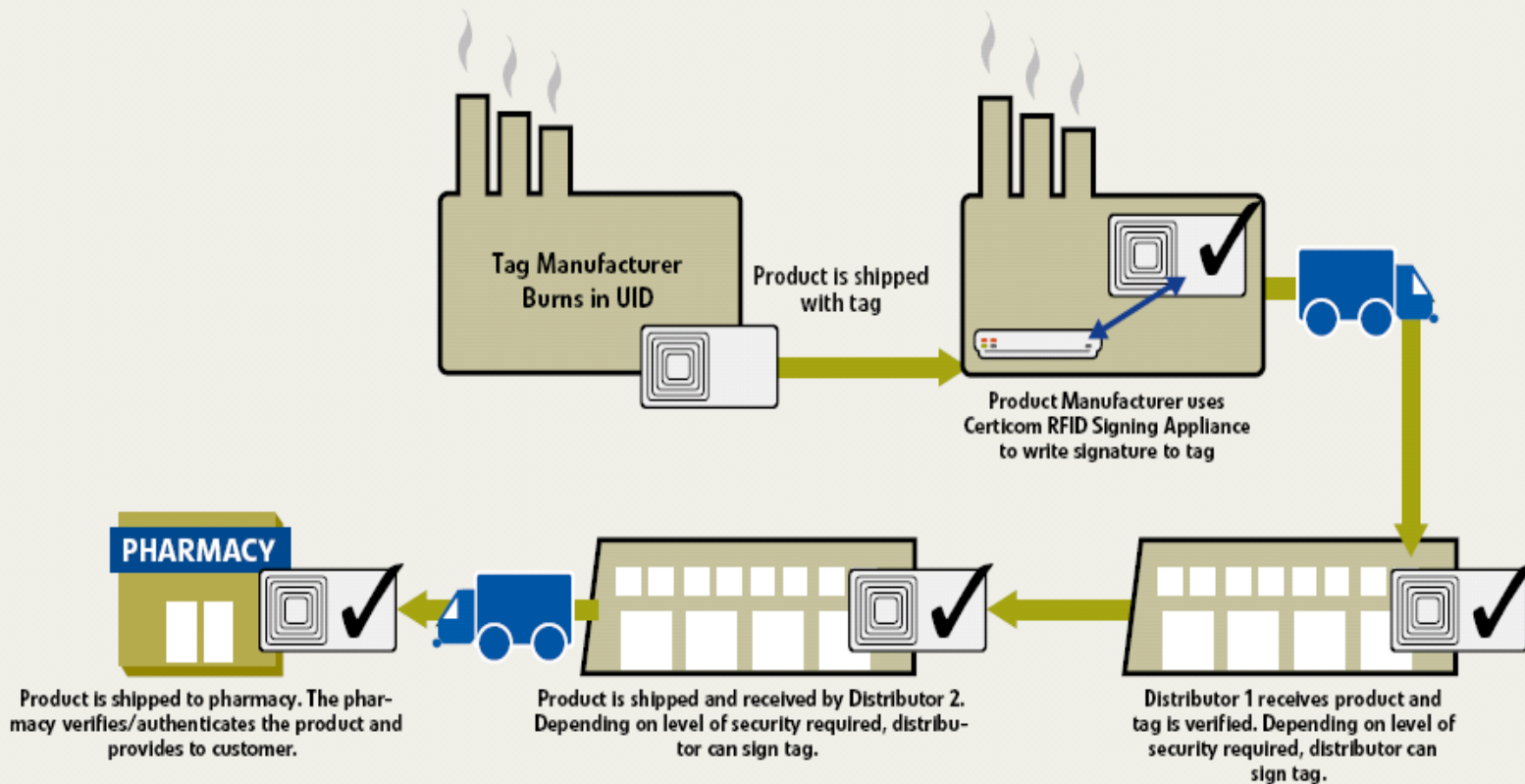
- Many boarding passes now carry a 2-dimensional bar-code.
- These passes can be paper or electronic.
- The information in the bar-code needs to be authenticated.
- This is done with an ECC digital signature.

RFID Tags

- Radio Frequency Identification tags (RFID tags).
- 3M supplies RFID tags to the pharmaceutical industry to track the distribution of certain drugs.
- These tags have at most 2000 bits.
- They want to put multiple digital signatures on the tag.

Distribution Channel Authentication

Certicom Security for RFID Product Authentication in Action



RFID Tags (continued)

- The only digital signature schemes which provide high security and provides multiple signatures per tag.

Consumer Electronics

- ECC is mandated in several consumer electronics standards.
 - DTCP
 - AACCS
 - SAFIA
- ECC is in
 - Televisions
 - DVD players
 - Blueraay disks

Consumer Electronics (continued)

- There are 5 ECDSA digital signatures on every Blu-ray disk.
- The Nintendo Wii game station uses a 283 bit binary Koblitz curve to protect their games.

Cryptographic Modernization

- ❖ *National Security Agency (NSA) commencing "Crypto Modernization Program" for mission critical information*
- ❖ *Looking for solution for next 20+ years; NSA has studied ECC as long as I have.*
- ❖ *Standardization and evangelization supporting the technology*

US Government Initiative

- The United States, the UK, Canada and certain other NATO nations have all adopted some form of elliptic curve cryptography for future systems to protect classified information throughout and between their governments.

NSA Contract

- ◇ *Signed US\$25 million agreement in October, 2003*
- ◇ *Worldwide, non-exclusive license for 26 of Certicom's ECC-based patents*
- *Manufacturers of NSA-approved end-user products required to implement ECC*



ECC becoming crucial technology for protecting mission critical national security information

Significance of Agreement

- ❖ *The NSA has endorsed Elliptic Curve Cryptography.*
- ❖ *In February 2005 the NSA announced Suite B.*
 - Public-key schemes are all ECC (no RSA)*
- ❖ *The NSA is promoting the use of ECC not only for national security but for the commercial sector.*

Industry Leading Customers



Conclusion

- RIM brings a whole new dimension to ECC adoption.
- RIM has about 60 million Blackberries in the field and about 250,000 Blackberry enterprise servers.
- RIM owns a large portion of the smartphone market and is increasing market share annually.

Conclusion (continued)

- RIM is committed to fostering ECC adoption.
- It is wonderful to see such elegant mathematics becoming widely used around the world