IEEE P1363:

Standard Specifications for Public-Key Cryptography

David Jablon
CTO Phoenix Technologies
Treasurer, IEEE P1363

NIST Key Management Workshop
November 1-2, 2001

Outline

- History to date
  - *Scope & objective of Std 1363-2000 & P1363a*
  - *Highlights of development process*
  - *Review of techniques in Std 1363-2000 & P1363a*
  - *Rationale*
  - *P1363 Study Group begins P1363.1 & P1363.2*

Outline (2)

- The present
  - *Current status of P1363a*
  - *Scope and objective of P1363.1*
  - *Contents of P1363.1*
  - *Scope and objective of P1363.2*
  - *Contents of P1363.2*

Outline (3)

- The future
  - *Schedule for completion of P1363.1 and P1363.2*
  - *Public-key techniques registry*
  - *Second amendment to Std 1363-2000: P1363b*

The History

P1363 Working Group History

- First meeting January 1994
- Up to now, 31 working group meetings
- 1997: project split into P1363 & P1363a
- 2000: began exploring additional topics
- Late 2000: began P1363.1 & P1363.2

What is IEEE Std 1363-2000 ?

- 1994: P1363 Working Group commissioned to start project
  - *Original P1363 became "IEEE Std 1363-2000"*
- IEEE standard for public-key cryptography based on three families:
  - *Discrete Logarithm (DL) systems*
  - *Elliptic Curve Discrete Logarithm (EC) systems*
  - *Integer Factorization (IF) systems*
- Sponsored by Microprocessor Standards Committee

November 1, 2001 NIST Key Management Workshop 7

Objective and Scope of P1363

- Objective
  - *Facilitate interoperable security by providing comprehensive coverage of public-key techniques*
- Scope
  - *Cryptographic parameters and keys*
  - *Key agreement, digital signatures, encryption*
  - *Recommended supporting techniques*

November 1, 2001 NIST Key Management Workshop 8

What is P1363a ?

- 1997: MSC approved P1363 WG to begin work on amendment to Std 1363-2000
- Supplements techniques in Std 1363-2000
- Intended that the two documents will be merged in future revisions
- Scope was limited to schemes in the same families and same general goals as in Std 1363-2000

November 1, 2001 NIST Key Management Workshop 9

Objective and Scope of P1363a

- Objective
  - *To facilitate the completion of the base standard while providing a forum for discussing additional techniques*
  - *To "fill in the gaps" from Std 1363-2000*
- Scope
  - *Cryptographic parameters and keys*
  - *Key agreement, digital signatures, encryption*
  - *Recommended supporting techniques*

November 1, 2001 NIST Key Management Workshop 10

IEEE Std 1363-2000 and P1363a

- IEEE Std 1363-2000 (base standard)
  - *Established techniques*
  - *Goal: timely publication (First balloted early 1999, approved as a standard January 2000)*
- P1363a (supplement)
  - *Techniques in same families that have become "established" since work ended on P1363*
  - *Call for more submissions in April 1998*
  - *Goal: fill in gaps, assure thorough study and input from the community*

November 1, 2001 NIST Key Management Workshop 11

Existing Public-Key Standards

- Standards are essential in several areas:
  - *Cryptographic schemes*
  - *Key representation*
- Some work in each area, but no single comprehensive standard ...
  - *ANSI X9.30, X9.31, X9.42, X9.44, X9.62, X9.63*
  - *ISO/IEC 9796, 10118, 14888, 15946*
  - *PKCS, SEC, EESS*
  - *FIPS 180-1, 186-2*
  - *NESSIE, CryptRec*

November 1, 2001 NIST Key Management Workshop 12

1363 Standards: A Different Kind of Standard

- A set of tools from which implementations and other standards can be built
  - *Framework with selectable components: applications are expected to "profile" the standard*
    - Example: signature scheme is based on a particular mathematical primitive (e.g., RSA) with selectable key sizes and "auxiliary" functions (hashing, message encoding)
  - *Functional specifications rather than interface specifications*

November 1, 2001 NIST Key Management Workshop 13

Highlights

- Comprehensive
  - *Three families; a variety of algorithms*
- Adoption of new developments
  - *"Unified" model of key agreement*
  - *"Provably secure" schemes*
  - *Key and parameter validation*
- A forum for discussing public-key crypto
  - *Active discussion mailing list*
  - *Web site for new research contributions*

November 1, 2001 NIST Key Management Workshop 14

Std 1363-2000 and P1363a: Contents

- Overview
- References
- Definitions
- Types of cryptographic techniques
- Math conventions
- DL primitives
- EC primitives
- IF primitives
- Key agreement schemes
- Signature schemes
- Encryption schemes
- Message encoding
- Key derivation
- Auxiliary functions
- Annexes

Primitives vs. Schemes

- Primitives:
  - *Basic mathematical operations*
    - e.g., $c = m^e \bmod n$
  - *Limited-size inputs, limited security*
- Schemes:
  - *Operations on byte strings, including hashing, formatting, other auxiliary functions*
  - *Often unlimited-size inputs, stronger security*
- Implementations can conform with either

Key Agreement Schemes

- General model
  - *Establish valid domain parameters*
  - *Select one or more valid private keys*
  - *Obtain other party's one or more "public keys"*
  - *Validate the public keys (optional)*
  - *Compute a shared secret value*
  - *Apply key derivation function*

November 1, 2001 NIST Key Management Workshop 17

Signature Schemes

- General model
  - *Signature operation*
    - Select a valid private key
    - Apply message encoding method and signature primitive to produce a signature
  - *Verification operation*
    - Obtain the signer's "public key"
    - Validate the public key (optional)
    - Apply verification primitive and message encoding method to verify the signature

November 1, 2001 NIST Key Management Workshop 18

Encryption Schemes

- General model
  - *Encryption operation*
    - Obtain the recipient's public key
    - Validate the public key (optional)
    - Apply message encoding method and encryption primitive to produce a ciphertext with optional authentication
  - *Decryption operation*
    - Select the appropriate private key
    - Apply decryption primitive and message encoding method to obtain plaintext
    - Optionally authenticate the validity of the plaintext

Summary of Schemes (1)

- Discrete Logarithm (DL) systems
  - *P1363: Diffie-Hellman, MQV key agreement*
  - *P1363: DSA, Nyberg-Rueppel signatures*
  - *P1363a: Pintsov-Vanstone signatures, signatures with message recovery (Nyberg-Rueppel 2)*
  - *P1363a: DLIES encryption*
- Elliptic Curve (EC) systems
  - *Elliptic curve analogs of DL systems*

Summary of Schemes (2)

- Integer Factorization (IF) systems
  - *P1363: RSA encryption*
  - *P1363: RSA, Rabin-Williams signatures*
  - *P1363a: EPOC encryption*
  - *P1363a: ESIGN signatures, IF signatures with message recovery*

Message Encoding and Key Derivation

- Message encoding methods
  - *For signature*
  - *For encryption*
- Key derivation function

Auxiliary Functions

- Hash functions
  - *Hash from arbitrary length input*
- Mask generation functions
  - *Arbitrary length input and output*
  - *Hash (message || 0) || hash (message || 1) || ...*

November 1, 2001 NIST Key Management Workshop 23

Annexes

- Annex A: Number-theoretic background
- Annex B: Conformance
- Annex C: Rationale
- Annex D: Security considerations
- Annex E: Formats
- Annex F: Bibliography
- Test vectors to be posted on the web

November 1, 2001 NIST Key Management Workshop 24

Annex A

- Annex A: Number-theoretic background (Informative)
  - *Supporting algorithms and methods for efficiently performing operations specified in main body*

Annex B

- Annex B: Conformance (Normative)
  - *Provide implementers with a consistent language for claiming conformance with parts of this standard*
  - *An implementation may claim conformance with one or more primitives, schemes or scheme operations*

Annex C

- Annex C: Rationale (Informative)
  - *Some questions the working group considered . . .*
  - *Why is the standard the way it is?*

General Questions

- Why three families?
  - *All are well understood, established in marketplace to varying degrees*
  - *Different attributes: performance, patents, etc.*
  - *Goal is to give standard specifications, not to give a single choice*
- Why no key sizes?
  - *Security requirements vary by application, strength of techniques vary over time*
  - *Goal is to give guidance but leave flexibility*

Annex D

- Annex D: Security Considerations (Informative)
  - *Key management (authentication, generation, validation)*
  - *Security parameters (key sizes)*
  - *Random number generation*
  - *Emphasis on common uses and secure practice*

Annex E

- Annex E: Formats (Informative)
  - *Suggested interface specifications, such as representation of mathematical objects and scheme outputs*

Annex F

- Annex F: Bibliography (Informative)
  - *Well, it's a bibliography . . .*

Annex G

- Annex G: Patent Information (Informative)
  - *Collection of information that the working group has gathered on intellectual property relating to techniques in the standard (new in P1363a)*

Study Group

- March 2000: Study Group for Future Public-Key Cryptography Standards commissioned
- Considered broader scopes for future projects relating to public-key crypto
- Determined where all previously out-of-scope submissions fit
- Completed work in 2001 with 2 new projects and additional ideas for the future

New Project Ideas

- Key and domain parameter generation and validation
- Threshold cryptosystems
- Key establishment protocols
- Entity authentication protocols
- Proof-of-possession protocols
- Guidelines for implementations
  - *updated security considerations, key size recommendations, interoperability issues, etc.*

New Project Ideas (2)

- Conformance testing
- ASN.1 syntax
- S-expression syntax
- Identification schemes
- Password-based security protocols
- Fast implementation techniques and number-theoretic algorithms
- New families of cryptosystems

The Present

P1363a: Current Status

- Document approved by working group and MSC for ballot
- IEEE is assembling ballot body
- Only minor edits and voting remain

What is P1363.1?

- MSC approved WG to begin P1363.1
  - *Standard Specifications for Public-Key Cryptography: Techniques Based on Hard Problems over Lattices*
- Grew out of Study Group work in 2000
- Public-key techniques in a fourth family
- Parallel, but independent effort to P1363a
- Submissions for new techniques close October 1, 2001

Objective and Scope of P1363.1

- Objective
  - *To continue to facilitate interoperable security by providing comprehensive coverage of public-key techniques in the "lattice family"*
- Scope
  - *Cryptographic parameters and keys*
  - *Digital signatures, encryption in lattice family*
  - *Recommended supporting techniques*
  - *Updated specification format*

November 1, 2001 NIST Key Management Workshop 39

Contents of P1363.1

- Same general contents as Std 1363-2000 (overview, references, definitions, math conventions, etc.)
- Shortest Vector Problem (SVP) Primitives
- Signature and Encryption schemes
- Message Encoding Methods
- Additional Auxiliary Functions
- Number theoretic background
- Security Considerations

November 1, 2001 NIST Key Management Workshop 40

Summary of P1363.1 Schemes

- Shortest Vector (SV) Systems
  - *NTRU encryption*
  - *NSS signatures (tentative)*

November 1, 2001 NIST Key Management Workshop 41

What is P1363.2?

- MSC approved the P1363 WG to begin work on P1363.2 – Standard Specifications for Public-Key Cryptography: Password-based Techniques
- Grew out of Study Group work in 2000
- Public-key techniques utilizing “low-grade” secrets
- Parallel, but independent effort to P1363a and P1363.1
- Submissions for new techniques close October 1, 2001

November 1, 2001 NIST Key Management Workshop 42

Objective and Scope of P1363.2

- Objective
  - *Continue to facilitate interoperable security by providing comprehensive coverage of public-key techniques using passwords and other low-grade secrets*
- Scope
  - *Cryptographic parameters and keys*
  - *Password-based key establishment & authentication*
  - *Recommended supporting techniques*

November 1, 2001 NIST Key Management Workshop 43

Contents of P1363.2

- Same general structure as Std 1363-2000
  - *overview, references, definitions, math conventions, etc.*
- Random element derivation, key derivation & secret value derivation primitives
- Password-authenticated key retrieval and key agreement schemes
  - *balanced and augmented trust models*
- Password-authenticated key agreement protocols
- Additional auxiliary functions
- Number theoretic background
- Security considerations

November 1, 2001 NIST Key Management Workshop 44

Summary of P1363.2 Schemes

- Discrete Log Systems
  - *Password-authenticated key agreement*
    - AMP, PAK, SPEKE, SRP (tentative)
    - Balanced and Augmented schemes
  - *Password-authenticated key retrieval*
    - FK (tentative)
- Elliptic Curve Systems
  - *Analogs to DL systems*

The Future

Schedule for Completion of P1363.1 and P1363.2

- October 2001: Both projects closing submissions
- 2002: Working group to review each document
- Late 2002: Balloting for P1363.1 expected
- Early 2003: Balloting for P1363.2 expected

Public-Key Registry

- Discussed at great length in study group and later in working group
- IEEE may support effort
- Three documents
  - *Process document*
  - *Format specification (Standard)*
  - *Registry of public-key cryptographic techniques*
- Continuing investigation to determine usefulness and feasibility

P1363b: A 2nd Amendment to Std 1363-2000

- Continue adding mature techniques
- Maintain the currency of the document
- Working group currently considering the project

Meetings in Late 2001

- August 23-24 (after Crypto) Santa Barbara
  - *working group presentations*
  - *working group meeting*
- October 22-24 – Seoul, Korea
  - *Cancelled*
  - *... next meeting to be announced ...*

Current IEEE P1363 Officers

- Chair: William Whyte
  - *wwhyte@ntru.com*
- Vice Chair: Don Johnson
  - *djohnson@certicom.com*
- Secretary: Ari Singer
  - *asinger@ntru.com*
- Treasurer: David Jablon
  - *david_jablon@phoenix.com*
- Primary Editor: David Stern
  - *david.l.stern@intel.com*

For More Information

- IEEE P1363 Web site
  - *http://grouper.ieee.org/groups/1363*
  - *publicly accessible research contributions and document submissions*
- Two mailing lists
  - *general announcements list, low volume*
  - *technical discussion list, high volume*
  - *everybody is welcome to subscribe*
    - web site contains subscription information