

**IEEE P1363:
Standard Specifications for
Public-Key Cryptography**

Burt Kaliski
Chair, IEEE P1363

August 17, 1999

Outline

- **The history**
 - scope and objective of P1363
 - highlights of the development process
- **The present**
 - review of techniques in the P1363 document
 - some rationale
- **The future**
 - preview of P1363a effort
 - new officers, new projects

The History

What is P1363 ?

- **Emerging 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**

Objective and Scope

■ Objective

- to facilitate interoperable security by providing comprehensive coverage of public-key techniques

■ Scope

- cryptographic parameters and keys
- key agreement, digital signatures, encryption

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
 - PKCS
 - FIPS 180-1, 186-1

P1363: 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

Highlights

- **Comprehensive**
 - three families; a variety of algorithms
- **Adoption of new developments**
 - “unified” model of key agreement
 - “provably secure” encryption
 - key and parameter validation
- **A forum for discussing public-key crypto**
 - active discussion mailing list
 - web site for new research contributions

History and Status

- **First meeting January 1994**
- **Up to now, 23 working group meetings**
- **In 1997, the project split into P1363 and P1363a**
 - to facilitate the completion of established techniques
 - to provide a forum for discussion of newer techniques without the pressures of immediate standardization

P1363 vs. P1363a

- **P1363 (base standard)**
 - established techniques
 - goal: timely publication (balloting nearly complete)
- **P1363a (supplement)**
 - some items in need of more research deferred from P1363
 - outline currently being developed
 - goal: thorough study and input from the community

The Present

P1363 Outline

- Overview
- References
- Definitions
- Type of crypto tech.
- Math conventions
- DL primitives
- EC primitives
- IF primitives
- Key agreement schemes
- Signature schemes
- Encryption schemes
- Message encoding
- Key derivation
- Auxiliary functions
- Annexes

Summary of Techniques

- **Discrete Logarithm (DL) systems**
 - Diffie-Hellman, MQV key agreement
 - DSA, Nyberg-Rueppel signatures
- **Elliptic Curve (EC) systems**
 - elliptic curve analogs of DL systems
- **Integer Factorization (IF) systems**
 - RSA encryption
 - RSA, Rabin-Williams signatures

Primitives vs. Schemes

- **Primitives:**
 - basic mathematical operations (e.g., $c = me \bmod n$)
 - 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**

DL Primitives

- **DL systems**

- security based on discrete logarithm problem over a finite field ($GF(p)$ or $GF(2^m)$)

- **Secret value derivation**

- Diffie-Hellman and MQV
- two flavors: with or without cofactor multiplication

- **Signature and verification**

- DSA
- Nyberg-Rueppel, has message recovery capability

EC Primitives

- **EC systems**
 - security based on discrete logarithm problem over an elliptic curve
 - choices of field: $GF(2^m)$ and $GF(p)$
 - representation of $GF(2^m)$: normal and polynomial basis
- **Primitives are analogous to DL**

IF Primitives

- **IF systems**
 - security based on integer factorization problem
 - RSA has odd public exponent, RW has even public exponent
- **Encryption and decryption**
 - RSA
- **Signature and verification**
 - RSA and Rabin-Williams
 - both have message recovery capability

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"
 - (optional) validate the public keys
 - compute a shared secret value
 - apply key derivation function

DL/EC Key Agreement Schemes

- **DH1**

- “traditional” Diffie-Hellman
- one key pair from each party

- **DH2**

- Diffie-Hellman with “unified model”
- two key pairs from each party

- **MQV**

- two key pairs from each party

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"
- (optional) validate the public key
- apply verification primitive and message encoding method to verify the signature (and recover the message in certain schemes)

DL/EC Signature Schemes

- **DSA with appendix**
 - hash function followed by DSA primitive
 - with SHA-1, appropriate parameter sizes, consistent with Digital Signature Standard
- **Nyberg-Rueppel with appendix**
 - hash function followed by Nyberg-Rueppel primitive
- **EC analogs of the above**

IF Signature Schemes

- **RSA, RW with appendix**
 - ANSI X9.31 message encoding followed by primitive
- **RSA, RW with message recovery**
 - ISO/IEC 9796-1 message encoding followed by primitive
 - limited message size

IF Encryption Scheme

- **RSA**
 - Bellare-Rogaway “Optimal Asymmetric Encryption Padding” followed by RSA primitive
 - authenticated encryption, control information is optional input
 - limited message size
- **General model for encryption to be included in later version**

Message Encoding and Key Derivation

- **Message encoding methods**

- for signature

- hashing, ANSI X9.31, ISO/IEC 9796

- for encryption

- OAEP

- **Key derivation function**

- follows ANSI X9.42

- Hash (secret value | | parameters)

Auxiliary Functions

- **Hash functions**
 - hash from arbitrary length input
 - SHA-1, RIPEMD-160
- **Mask generation functions**
 - arbitrary length input and output
 - Hash (message, 0), Hash (message, 1), ...

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**

Annex A

- **Annex A: Number-Theoretic Background (Informative)**
 - many number-theoretic algorithms for prime-order and binary finite fields
 - complex multiplication (CM) method for elliptic curve generation
 - primality testing and proving

Annex B

■ Annex B: Conformance (Normative)

- language for claiming conformance with parts of the 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

DL/EC Questions

- **Why DH and MQV?**
 - DH established, more flexible with unified model
 - MQV optimized for ephemeral/static case
- **Why DSA and NR?**
 - DSA in U.S. federal standard
 - NR involves less hardware in some implementations, provides for message recovery

IF Questions

- **Why RSA and RW?**
 - RSA established, also supports encryption
 - RW signature verification faster with $e = 2$, supported along with RSA by ISO/IEC 9796, ANSI X9.31

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

Ballot Status

- **IEEE P1363 ballot started February 1999**
- **Ballot passed, many comments received**
- **Recirculation ballot in progress**
 - based on revised document, response to negative votes
- **Document submitted for IEEE RevCom approval at its September meeting**

The Future

Preview of P1363a

- **P1363a will provide “missing pieces” of P1363**
- **It is intended that the two documents will be merged during future revisions**
- **Working group has received numerous submissions (see web site)**
- **Four submissions will be presented on Thursday afternoon (Aug. 19)**
 - **some may be more appropriate for other P1363 projects**

Proposed Outline for P1363a

- **Key agreement schemes (TBD)**
- **Signature schemes**
 - DL/EC scheme with message recovery
 - PSS, FDH, PKCS #1 encoding methods for IF family
 - PSS-R for message recovery in IF family
- **Encryption schemes**
 - Abdalla-Bellare-Rogaway DHAES for DL/EC family

Beyond P1363a

- **Simple, self-contained projects**
 - each separately authorized by IEEE, developed and balloted
 - same working group oversees
- **Another supplement: P1363b for similar techniques**
 - e.g., “provably secure” schemes, other families
- **New projects: P1363.1, .2, .3, ... for other types of technique**

New Project Ideas (1)

- **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**
- ***Editors needed!***

Officers

- **New slate of officers to be elected in September for two-year terms, under new bylaws**
 - Chair
 - Vice-chair
 - Primary editor
 - Secretary
 - Treasurer
- **Send nominations to Burt Kaliski -- self-nominations accepted**

Meetings in 1990

- **August 19-20, University Center State Street Room, UC Santa Barbara**
 - Thursday 2:00-5:30pm
 - Friday 8:30-5:00pm
- **November (?) to be announced**

For More Information

■ Web site

- grouper.ieee.org/groups/1363
- publicly accessible research contributions and P1363a submissions

■ Two mailing lists

- general announcements list, low volume
- technical discussion list, high volume
- everybody is welcome to subscribe
 - web site contains subscription information

Current Officers

- **Chair: Burt Kaliski, burt@rsa.com**
 - officer nominations, P1363a submissions, new project ideas
- **Vice-chair: Terry Arnold, Terry.Arnold@merdan.com**
- **Secretary: Roger Schlafly, real@ieee.org**
- **Treasurer: Michael Markowitz, markowitz@infosseccorp.com**
- **Editor: Yiqun Lisa Yin, yiqun@nttmcl.com**
 - P1363 comments