IEEE P1363:
A Comprehensive Standard for Public-Key Cryptography

Burt Kaliski
Chief Scientist, RSA Laboratories
Chair, IEEE P1363

Revised July 1997

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
- **P1363 project is sponsored by IEEE's Microprocessor Standards Committee**

Public-Key Standards

- **Standards are essential in several areas:**
  - cryptographic schemes
  - key representation
  - scheme identification
- **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, ISO / IEC 14888
  - PKCS

Objective and Scope

- **Objective**
  - to facilitate interoperable security by providing comprehensive coverage of public-key techniques
- **Scope**
  - key generation and representation
  - key agreement, encryption, digital signatures
  - all based on public-key cryptography
- **A set of tools from which implementations, other standards can be built**

A Different Kind of Standard

- **As a set of tools, P1363 is different than other public-key standards**
  - definitions with selectable components
    - example: signature scheme is defined in terms of a specific mathematical primitive with selectable key sizes and "encoding" techniques (hashing, formatting)
    - security considerations explained (but not mandated)
- **Goal: consistent implementation of public-key techniques across many applications**
  - applications are expected to "profile" the standard

Highlights

- **A comprehensive standard**
  - three families: DL, EC, IF
  - key agreement, encryption, signatures
- **Recent developments included (some in supplement)**
  - "unified" model of key agreement
  - authenticated public-key encryption, encryption of arbitrary-length messages with one operation
  - "provably secure" schemes

Base vs. Supplement

- **Base document (P1363)**
  - established techniques
  - editorial contribution available for review, comments requested
  - goal: timely publication
- **Supplement (P1363A [proposed])**
  - additional techniques
  - contributions available, more solicited
  - goal: thorough research

History and Status

- 1994: first meetings
- 1995: patent issues resolved
- 1996: technical issues settled
- 1997: body nearing completion
  final appendices in preparation
- 1998: balloting of base
  development of supplement

Base Document Outline

- Introduction
- Definitions and conventions
- DL systems, EC systems, IF systems
- Encoding techniques, auxiliary functions
- Appendices

Appendix Material

- Rationale
- Conformance
- Background
- Number-theoretic algorithms
- Security considerations, key management
- Test vectors
- ASN.1 syntax

Primitives vs. Schemes

- **Primitives**
  - mathematical operations (e.g., $c = m^e \bmod n$) on which schemes are based
- **Schemes**
  - cryptographic operations and framework, with encoding techniques, auxiliary functions
- **Schemes are intended to provide security, primitives aren't; implementations can conform with either**

Three Families

- **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

Discrete Logarithm (DL) Systems

- **Security based on discrete logarithm problem over a finite field**
- **Flexibility in field, representation**
  - GF(2^m) or GF(p) (p prime)
  - normal or polynomial basis for GF(2^m)

DL Primitives

- **Secret value derivation**
  - Diffie-Hellman and MQV: secret value from other party's public key(s), own private key(s)
- **Signature and verification**
  - DSA
  - Nyberg-Rueppel, has data recovery capability

DL Key Agreement Schemes (1)

- **Diffie-Hellman with "unified model"**
  - one or two key pairs from each party
    - typically static and / or ephemeral
  - DH secret value derivation primitive followed by key derivation function
    - parties generate one or two key pairs (at some time)
    - exchange public keys
    - compute one or two secret values with primitive
    - apply key derivation function

DL Key Agreement Schemes (2)

- **Menezes-Qu-Vanstone**
  - two key pairs from each party
    - presumably, static and ephemeral
  - MQV secret value derivation primitive followed by key derivation function

DL Signature Schemes

- **DSA with appendix**
  - formatted hash function followed by DSA primitive
  - with SHA-1, appropriate parameter sizes, conforms with Digital Signature Standard
- **Nyberg-Rueppel with appendix**
  - formatted hash function followed by Nyberg-Rueppel primitive

DL Schemes for Further Study

- **Password-based authenticated key agreement ("EKE")**
- **Encryption schemes**
  - e.g., noninteractive key agreement followed by symmetric techniques
- **Signature schemes with message recovery**
  - e.g., Nyberg-Rueppel with redundancy function
- **Signature schemes with "provable security"**

Elliptic Curve Systems

- Security based on discrete logarithm problem over an elliptic curve
- As with DL, GF(2^m) and GF(p), normal and polynomial bases
- Primitives, schemes analogous to DL

Integer Factorization (IF) Systems

- **Security based on integer factorization problem**
- **RSA and Rabin-Williams supported**
  - both with composite modulus
  - RSA has odd public exponent, RW has even public exponent

IF Primitives

- **Encryption and decryption**
  - RSA only
- **Signature and verification**
  - RSA and Rabin-Williams
  - both have message recovery capability

IF Encryption Schemes

- **RSA**
  - formatting function followed by RSA primitive
  - authenticated encryption, control information is optional input
  - limited message size

IF Signature Schemes

- **RSA, RW with appendix**
  - formatted hash function followed by primitive
- **RSA, RW with message recovery**
  - redundancy function followed by primitive
  - limited message size

IF Schemes for Further Study

- **Key agreement schemes**
- **Alternate encryption schemes**
  - arbitrary length messages, single operation
- **Signature schemes with partial message recovery**
- **Signature schemes with “provable security”**

Encoding Techniques (1)

- **Techniques for encoding "message representatives" for the various schemes**
- **Encryption**
  - OAEP formatting
  - "enhanced" OAEP (supplement?)
- **Signatures with message recovery**
  - ISO/IEC 9796-1 formatting

Encoding Techniques (2)

- **Signatures with appendix**
  - hash function only
  - X9.31 / ISO 14888 draft, with formatting and hash function identifier
  - Bellare-Rogaway PSS (supplement?)

Auxiliary Functions

- **Functions supporting the schemes and encoding techniques**
- **Hash functions**
  - SHA1, RIPEMD-160 recommended
- **Key derivation functions**
  - example: hash (secret value || parameters), where parameters may be a counter
- **OAEP and mask generation**

Rationale

- 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 definitions, 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 based on U.S. 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

Other Questions

- **Why two types of field?**
  - mod *p* arithmetic already implemented in many systems, may have performance advantages in software
  - characteristic 2 arithmetic may have advantages in hardware
- **Why more than one type of basis?**
  - different attributes: performance, flexibility, patents
  - no impact on security

Suggested Topics for Supplement (1)

- **Key agreement schemes**
  - IF family
  - password-based, authenticated (SPEKE)
- **Encryption schemes**
  - DL, EC families
  - arbitrary-length messages
- **Signature schemes**
  - DL, EC with message recovery
  - partial message recovery

Suggested Topics for Supplement (2)

- **"Provable security" schemes**
- **Additional encoding techniques**
  - PSS
  - "enhanced" OAEP
  - ...

Schedule

- **Meetings in 1997:**
  - March 24-26, Auburn, Alabama
  - May 15-16, Konstanz, Germany [Eurocrypt '97]
  - June 11-13, Chicago, Illinois
  - August 19, 21-22, Santa Barbara, CA [Crypto '97]
  - November 18-20, Albuquerque, NM
- **Ballot of base document in early 1998**
- **Contributions to supplement welcome**

For More Information

- **Web site: http://stdsbbs.ieee.org/groups/1363/**
- **Mailing list**
  - subscribe by sending message with body *subscribe stds-p1363* to majordomo@mail.ieee.org
- **Contributions to burt@rsa.com**
- **Editorial comments to lisa@rsa.com or leo@rsa.com**

Officers

- Chair: Burt Kaliski, burt@rsa.com
- Vice-chair: Terry Arnold, terry.arnold@merdan.com
- Secretary: Roger Schlafly, rschlafly@attmail.com
- Treasurer: Michael Markowitz, mjmarkowitz@attmail.com
- Editor: Yiqun Lisa Yin, lisa@rsa.com