

# IEEE P1363: A Comprehensive Standard for Public- Key Cryptography

Burt Kaliski  
*Chief Scientist, RSA Laboratories*  
*Chair, IEEE P1363*

RSA Data Security Conference  
January 28-31, 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**



# Existing 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**



# Highlights

- **Comprehensive**
  - families: DL, EC, IF
  - algorithms: key generation, key agreement, encryption, signatures
- **New developments (mostly “version 2”):**
  - “unified” model of key agreement
  - authenticated public-key encryption, encryption of arbitrary-length messages with one operation
  - “provably secure” schemes



# History and Status

- **First meeting January 1994**
- **1995:**
  - patent issues resolved
  - EC material drafted
- **1996:**
  - technical issues settled
  - comprehensive version 1 document drafted
- **Balloting of version 1 in 1997, version 2 TBD**



# Version 1 vs. Version 2

## ■ Version 1

- more established techniques
- draft available for review, comments requested
- goal: timely publication

## ■ Version 2

- more advanced techniques
- contributions available, more solicited
- goal: thorough research



# Version 1 Outline

- Introduction
- Definitions
- DL systems, EC systems, IF systems
- Auxiliary functions
- ASN.1 syntax
- Appendices



# Appendices

- **Rationale**
- **Conformance**
- **Background**
- **Number-theoretic algorithms**
- **Cryptographic random numbers**
- **Test vectors**
- **Application notes**



# 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



# 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, ISO/IEC 9796 format



# Discrete Logarithm (DL) Systems

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



# DL Primitives

- **Parameter setup**
- **Key generation**
- **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
  - key generation and DH secret value derivation primitives 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
- key generation and MQV secret value derivation primitives optionally followed by key derivation function



# DL Signature Schemes

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



# DL Schemes for Further Study

- Password-based authenticated key agreement (“EKE”)
- Encryption schemes
  - noninteractive DH key agreement followed by symmetric techniques? (several proposals under consideration)
- Signature schemes with message recovery
  - 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 basis
- 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

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



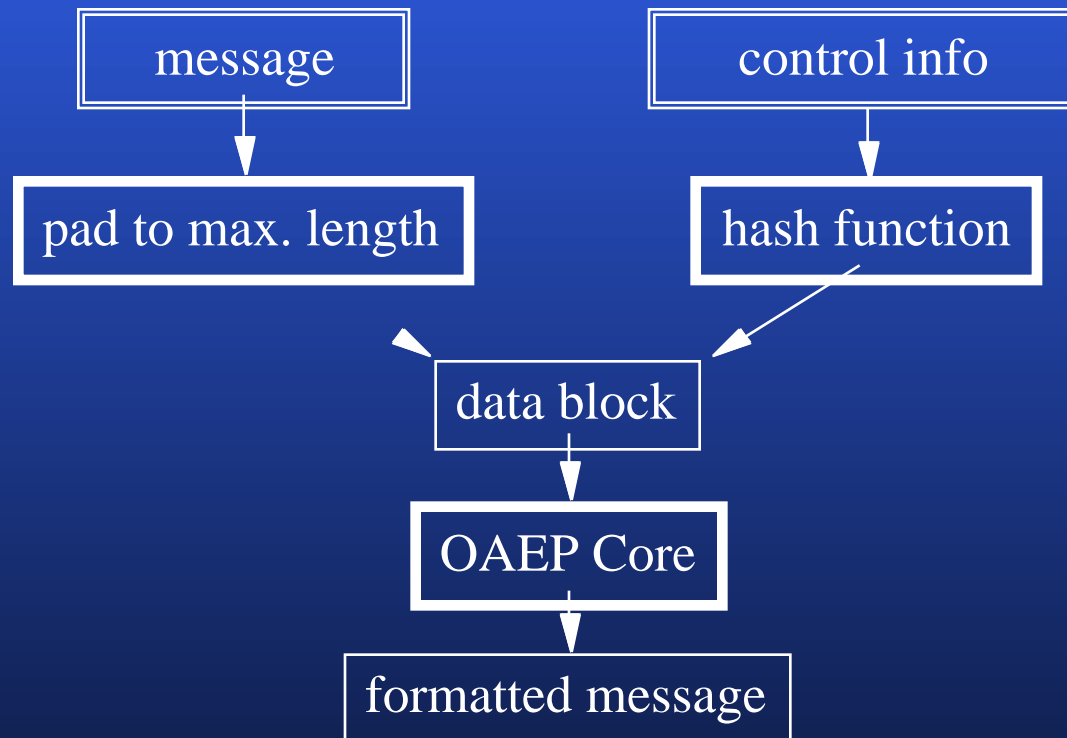
# IF Encryption Schemes

## ■ RSA-OAEP

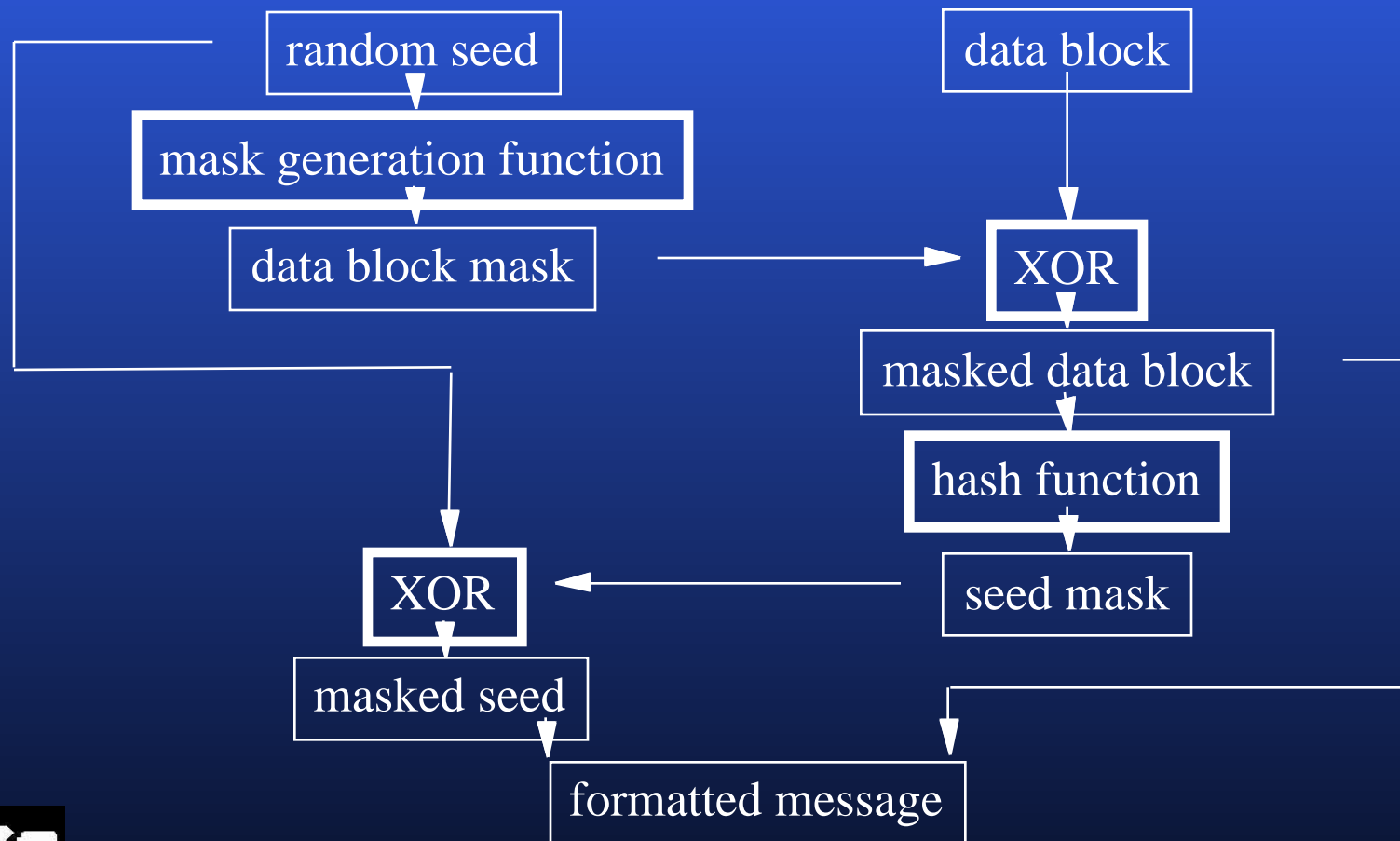
- “Optimal Asymmetric Encryption Padding” followed by RSA primitive
- authenticated encryption, control information is optional input
- limited message size



# RSA-OAEP Formatting



# OAEP Core



# IF Signature Schemes

- **RSA-9796, RW-9796 with appendix**
  - hash function, ISO/IEC 9796 formatting, followed by primitive
- **RSA-9796, RW-9796 with message recovery**
  - ISO/IEC 9796 formatting 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”



# Auxiliary Functions

- **Hash functions**

- hash from arbitrary length input
- example: SHA-1, RIPEMD-160

- **Key derivation functions**

- symmetric key from secret value, parameters (e.g., counter)
- example:  $\text{hash}(\text{secret value} \parallel \text{parameters})$

- **Mask generation functions**



# 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 ISO/IEC 9796?**
  - international standard, provides for message recovery
- **Why RSA and RW?**
  - RSA established, also supports encryption
  - RW signature verification faster with  $e = 2$ , supported along with RSA by ISO/IEC 9796
- **Why OAEP?**
  - established technique (SET, etc.), designed particularly for RSA



# Other Questions

- **Why two types of field?**
  - $\text{mod } p$  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



# Summary of Version 2 Topics

- **Key agreement schemes**
  - IF schemes
  - password-based authenticated schemes (“EKE”)
- **Encryption schemes**
  - DL, EC schemes, alternate IF schemes
  - arbitrary length messages with single operation
- **Signature schemes**
  - DL, EC with message recovery
  - partial message recovery, provable security



# Schedule

- **Meetings in 1997:**
  - March 24-26, Auburn, Alabama
  - May 15-16, Konstanz, Germany, after Eurocrypt
  - August 21-22, Santa Barbara, CA, after Crypto
  - November, TBD
- **Ballot of version 1 expected after May meeting**
- **Version 2 contributions throughout year**



# For More Information

- **FTP site:** <ftp://stdsbbs.ieee.org/pub/p1363/>
  - also available via <http://stdsbbs.ieee.org/>
- **Mailing list:** [stds-p1363@mail.ieee.org](mailto:stds-p1363@mail.ieee.org)
  - subscribe by sending message with body  
*subscribe stds-p1363*  
to [majordomo@mail.ieee.org](mailto:majordomo@mail.ieee.org) (not to the list)
- **Contributions to** [burt@rsa.com](mailto:burt@rsa.com)
- **Editorial comments to** [lisa@rsa.com](mailto:lisa@rsa.com) or  
[leo@rsa.com](mailto:leo@rsa.com)



# Officers

- **Chair: Burt Kaliski, [burt@rsa.com](mailto:burt@rsa.com)**
- **Vice-chair: Terry Arnold, [merdan@merdan.com](mailto:merdan@merdan.com)**
- **Secretary: Roger Schlafly, [rschlafly@attmail.com](mailto:rschlafly@attmail.com)**
- **Treasurer: Michael Markowitz, [mjmarkowitz@attmail.com](mailto:mjmarkowitz@attmail.com)**
- **Editor: Yiqun Lisa Yin, [lisa@rsa.com](mailto:lisa@rsa.com)**

