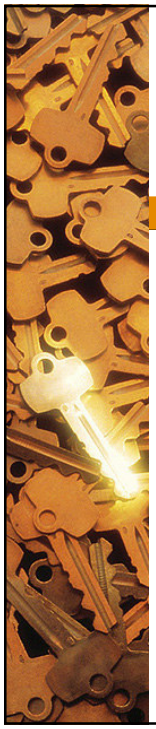


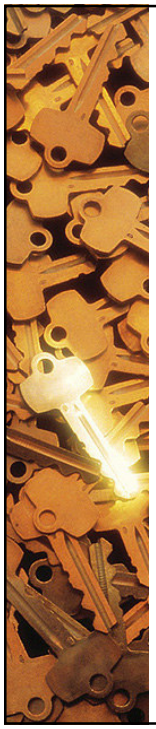
PKCS #13: Elliptic Curve Cryptography Standard

Burt Kaliski
RSA Laboratories
PKCS Workshop
October 7, 1998

Introduction

- Elliptic curve cryptography is emerging as a new public-key technique
- Some standardization underway:
  - ANSI X9.62,.63, IEEE P1363, ISO work
- PKCS #13: a profile of existing work
  - status: in preparation, this is a proposal

RSA Data Security.
A Security Dynamics Company



ECC: Primary Choices

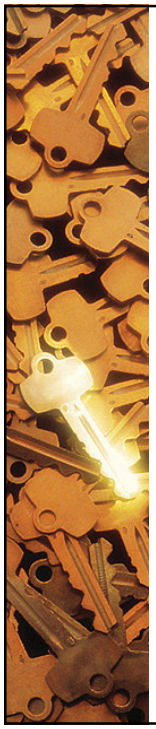
- Underlying finite field
- Cryptographic schemes
- Point representation

RSA Data Security.
A Security Dynamics Company

Finite Field

- Odd characteristic: GF(p), p odd
  - also GF(p^m), e.g., for $p = 3$
- Even characteristic: GF(2^m)
  - which field representations?
- Even generally faster (esp. in hardware), odd leverages existing modular arithmetic implementations

RSA Data Security.
A Security Dynamics Company



Key Agreement Schemes

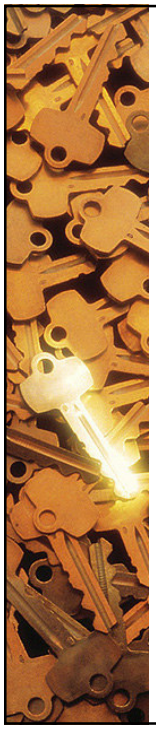
- Diffie-Hellman
- "Unified" Diffie-Hellman
- MQV
- DH basic, "unified" more flexible, MQV more efficient for joint static/ephemeral
  - P1363, X9.63 draft have all three

RSA Data Security.
A Security Dynamics Company

Signature Schemes

- DSA
- Nyberg-Rueppel
- Schnorr
- DSA "standard," NR allows message recovery, Schnorr more "provable"
  - P1363 has first two, X9.62 has DSA

RSA Data Security.
A Security Dynamics Company



Encryption Schemes

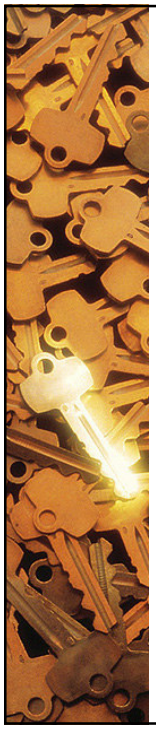
- Elgamal (= DH + multiplication)
- S/MIME approach
- Zheng-Seberry, Bellare-Rogaway schemes
- Elgamal basic, S/MIME enhanced, ZS and BR "provable", more flexible
  - ZS, BR submitted to P1363a
  - BR in X9.63 draft

RSA Data Security.
A Security Dynamics Company

Point Representation

- Uncompressed: (x,y)
- y-compressed: only one bit of y
- x-compacted: one less bit of x
- x only (with algorithm changes)
- Size, processing tradeoffs
  - P1363 supports uncompressed, y-compressed

RSA Data Security.
A Security Dynamics Company



Proposed Profile

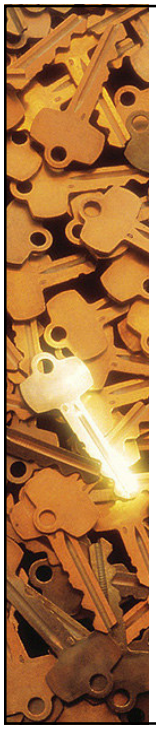
- GF(p) and GF(2^m), with rationale
- ECDH, ECDSA, P1363a ECES
- Uncompressed, with P1363 format
- Domain parameter and key generation, validation later

RSA Data Security.
A Security Dynamics Company

IP Considerations

- ECC in general is not patented, but specific choices may be, e.g.:
  - MQV key agreement
  - point compression (app.)
  - key validation (app.)
- Proposed profile is intended to be unencumbered, though some implementation techniques may be patented

RSA Data Security.
A Security Dynamics Company



Discussion

- Are the choices appropriate?
- Is the profile too general?
  - e.g., would fewer choices be better?
- Is it necessary?
  - maybe *IEEE P1363 Profile for PKCS Applications* would be a better title?
- Work plan and schedule

RSA Data Security.
A Security Dynamics Company