Fundamental Elliptic Curve Cryptography Algorithms

draft-mcgrew-fundamental-ecc-02

mcgrew@cisco.com

kmigoe@nsa.gov

Elliptic Curve Cryptography

- Alternative to integer-based Key Exchange and Signature algorithms
- Smaller keys and signatures
- More efficient at higher security levels

Diffie Hellman

g is number $< p$

Alice | **Bob**

x = **random**

$g^x \bmod p$ →

y = **random**

← $g^y \bmod p$

$$\boxed{(g^y)^x \bmod p \quad = \quad (g^x)^y \bmod p}$$

EC Diffie Hellman

g is element of EC group G

Alice | **Bob**

x = **random**

$\xrightarrow{\quad g^x \quad}$

y = **random**

$\xleftarrow{\quad g^y \quad}$

$(g^y)^x$ **=** $(g^x)^y$

Cryptographic Groups

Prime Group

Element is number $x < p$

- Prime modulus $\boldsymbol{p}$
- Generator $\boldsymbol{g} < p$
- Order $\boldsymbol{n}$

EC Group

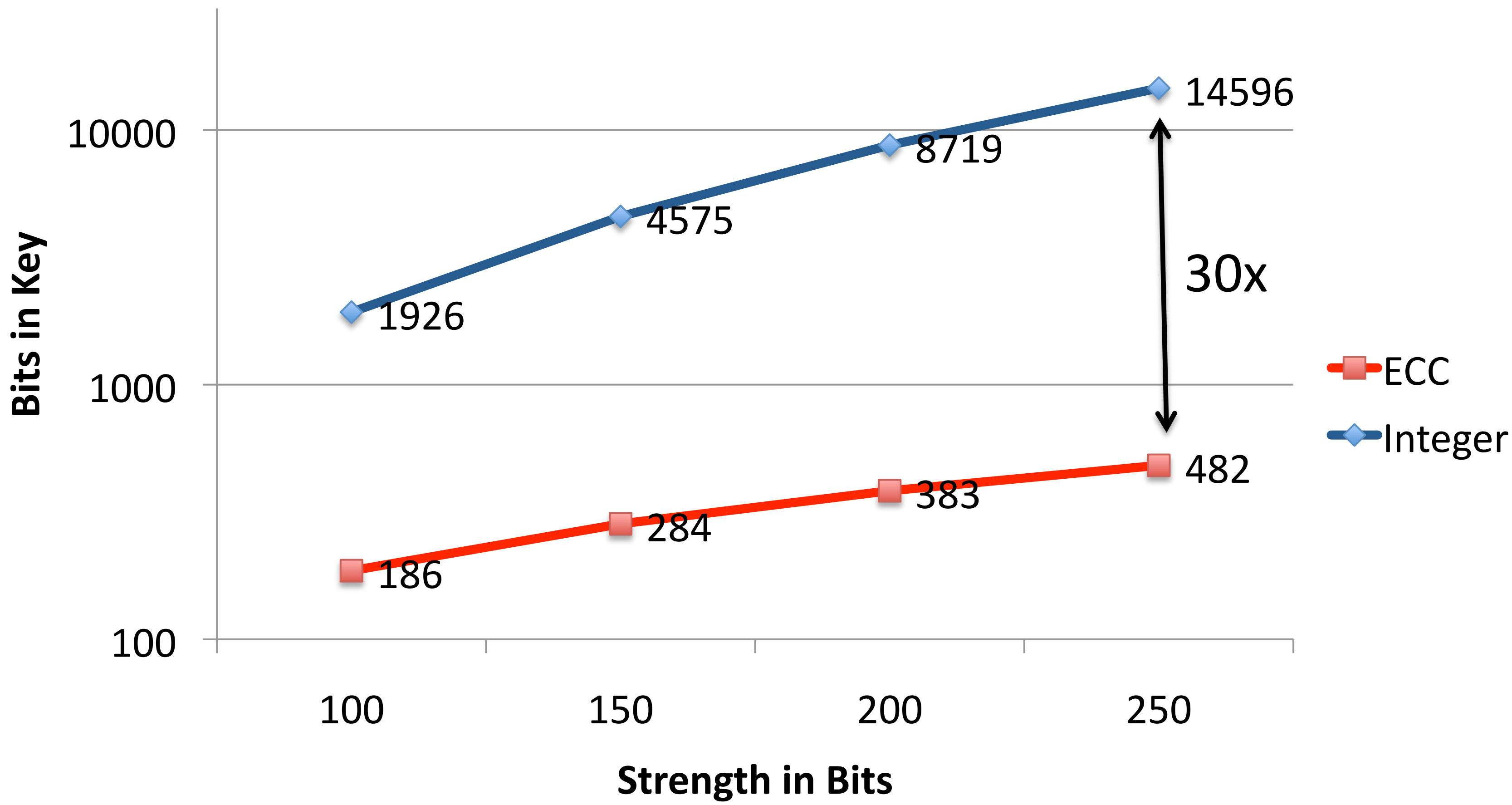
Element is (x, y) with $x, y < p$

with $y^2 = x^3 + ax + b \bmod p$

- Prime modulus $\boldsymbol{p}$
- Parameters $\boldsymbol{a}, \boldsymbol{b} < p$
- Generator $(\boldsymbol{g_x}, \boldsymbol{g_y})$
- Order $\boldsymbol{n}$

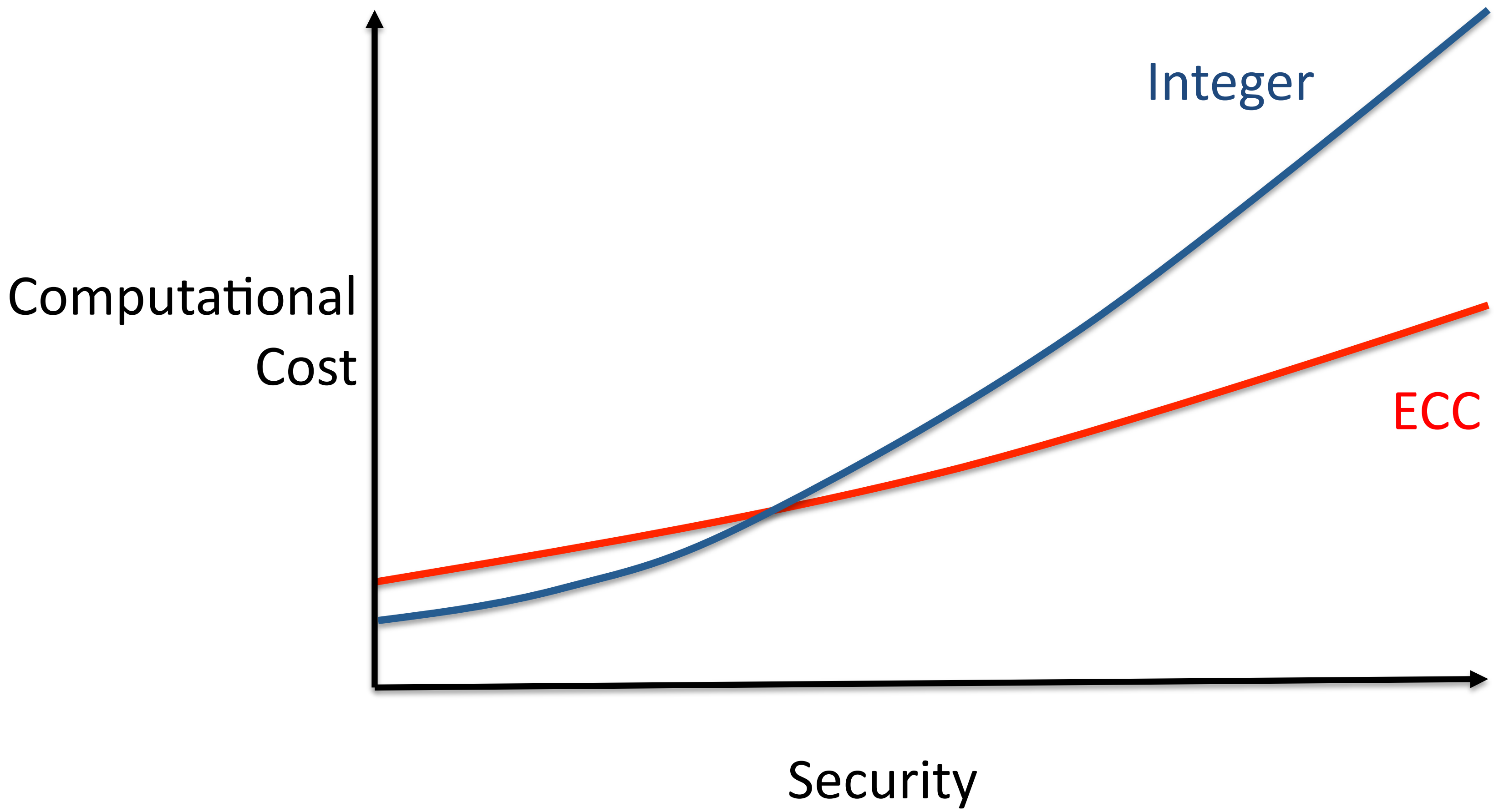
ECC Parameter Set

Public Key Sizes



From RFC3766, *Determining Strengths For Public Keys Used For Exchanging Symmetric Keys*

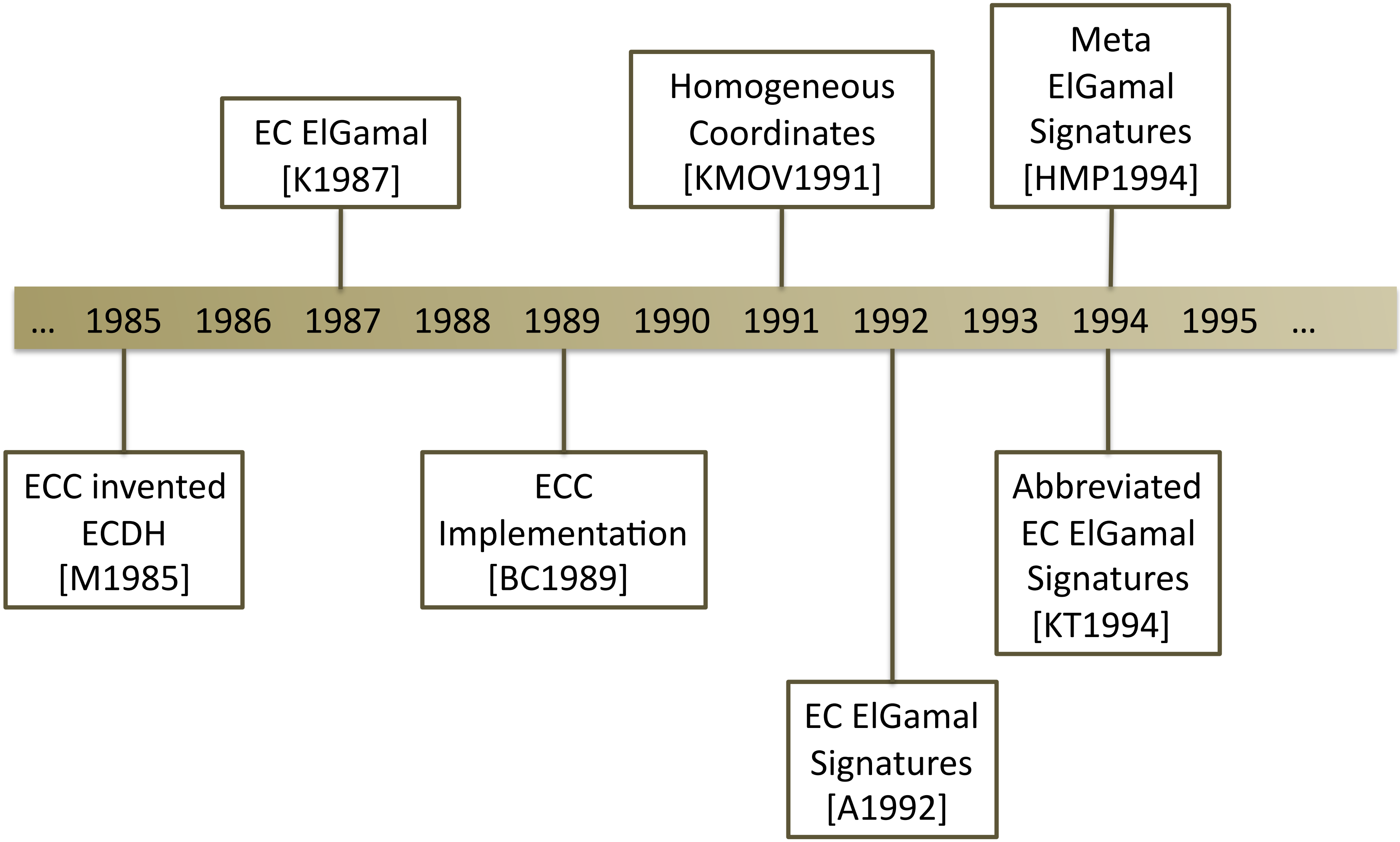
ECC Efficient at High Security



fECC

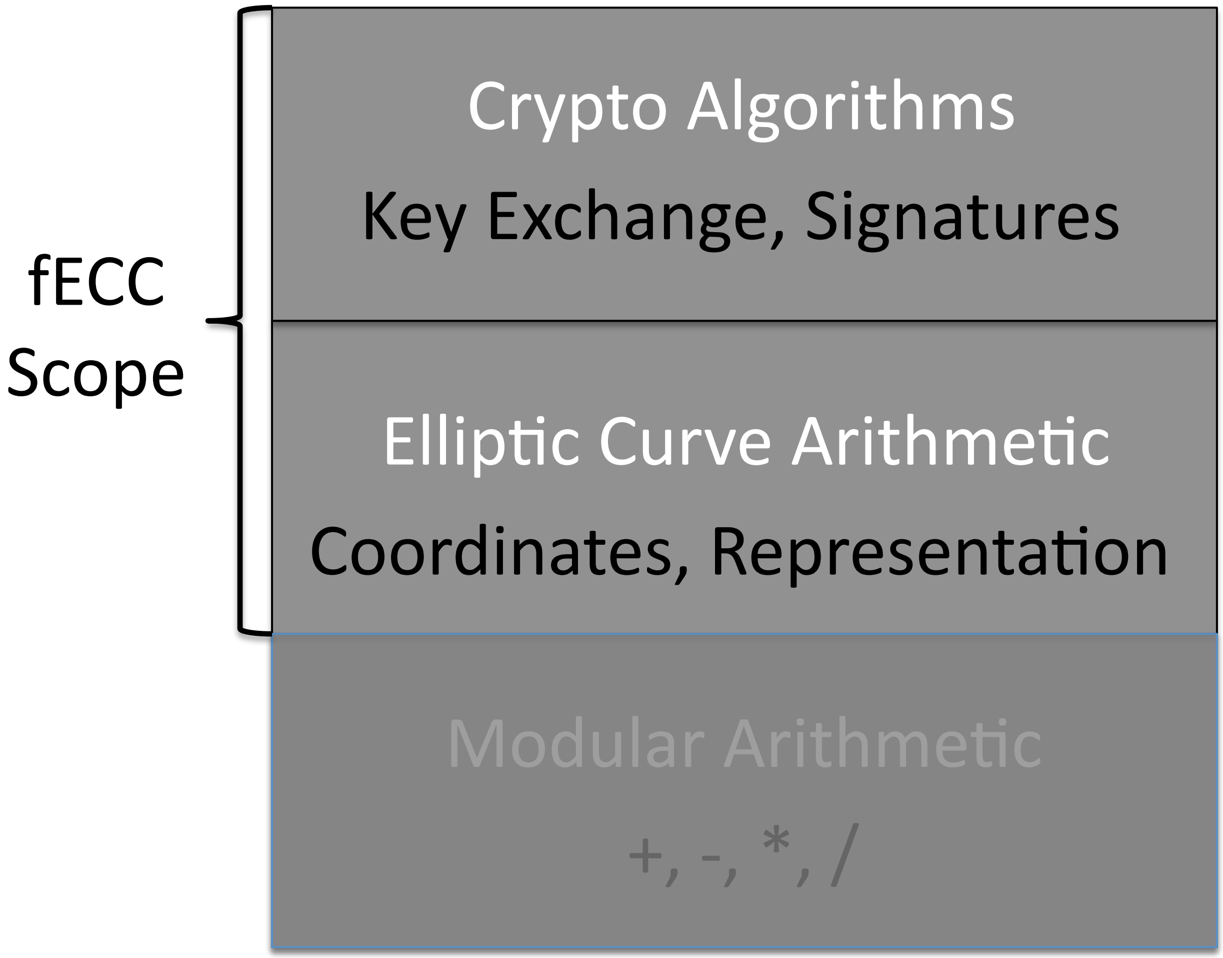
- `draft-mcgrew-fundamental-ecc`
  - Informational
  - First published 7/09
  - Comments received and incorporated in -02
- Closely based on pre-1994 references
  - Security: survived > 16 years of review
  - IPR: simplifies analysis

Timeline



EC ElGamal [K1987]
Homogeneous Coordinates [KMOV1991]
Meta ElGamal Signatures [HMP1994]
... 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 ...
ECC invented ECDH [M1985]
ECC Implementation [BC1989]
EC ElGamal Signatures [A1992]
Abbreviated EC ElGamal Signatures [KT1994]

Layers


fECC
Scope
Crypto Algorithms
Key Exchange, Signatures
Elliptic Curve Arithmetic
Coordinates, Representation
Modular Arithmetic
+, -, *, /

fECC Diffie-Hellman

- Miller 1985
- Compatible with IKE (RFC 4753)
- Compatible with ECDH (IEEE 1363, ANSI X9.62)
  - Curves over GF(*p*) with cofactor=1
  - ECSVDP-DH primitive
  - Key Derivation Function is identity function

fECC Signatures

- Koyama and Tsuruoka, 1994
- Horster, Michels, and Petersen, 1994
- KT-IV Signatures
  - Compatible with ECDSA (IEEE 1363, ANSI X9.62)
- KT-I Signatures
  - Not interoperable with standard

ECC Parameter Sets

- Compatible
  - Suite B
    - USG Cryptographic Interoperability Strategy
    - Uses NIST P256, P384, P521
  - Other NIST curves over GF(*p*)
  - RFC 5639 *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*
  - WAPI ISO/IEC JTC 1/SC 6 Proposal
- Not compatible
  - DJB's Curve25519 protocol

Not in Scope

- EC Group Parameter Generation
- Identity-based crypto
- Edwards' coordinates
- GF(2^m) curves
- Mod *p* arithmetic optimizations
- Certificate details
- Exotic groups (hyperelliptic, braids, ...)
- ...

Possible Future Drafts

- Optimizations
  - Modular arithmetic
    - Efficient primes
  - Elliptic Curve arithmetic

Priority: preserve interoperability and compatibility with standards

Conclusions

- Draft ready for RFC
- ECC deserves serious consideration
  - fECC is secure and performs well
- Recommendation: IETF work using ECC should explicitly allow fECC
  - `… implementations MAY use [fECC] …`

Questions?

$$(x3,y3) = (x1,y1) \times (x2,y2)$$

$x3 = ((y2-y1)/(x2-x1))^2 - x1 – x2$

$y3 = (x1-x3)(y2-y1)/(x2-x1) – y1$

A Group

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$5, \quad 5^2=4, \quad 5^3=6, \quad 5^4=2, \quad 5^5=3, \quad 5^6=1$

Multiplication modulo 7