NIST Curves

• 1985 – Elliptic Curve Cryptography proposed

\[ y^2 + axy + by = x^3 + cx^2 + dx + e \]

• 1999 – NIST standardized the Elliptic Curve Digital Signature Algorithm in FIPS 186-2
  – NIST recommended 15 elliptic curves of varying security levels, called \textit{NIST curves}

• 2013 – some concerns about NIST curves
Curve Concerns

• Efficiency
  – NIST curves chosen to be very efficient
  – New curves with more efficient implementations have since been found

• Security
  – The addition law for the NIST curves has special cases which can allow for side-channel attacks
  – New curves have been found which avoid this pitfall

• Do the NIST curves have hidden weakness?
Types of Curves

• Two different kinds of curves:
  – *Pseudo-random curves* - coefficients are generated from the output of a seeded cryptographic hash
  – *Special curves* - coefficients and underlying field have been selected to optimize efficiency

• Concern expressed over provenance of the parameters of pseudo-random curves
  – Where do NIST curve coefficients come from?
NIST Curve Generation

• Pseudo-random curves
  • \( y^2 = x^3 - 3x + b \) (prime fields)
  • \( y^2 + xy = x^3 + x^2 + b \) (binary fields)

• The parameter \( b \) is the output of a one-way function generated from a seed
  – Pseudo-random generation specified in ANSI X9.62 and IEEE P1363 uses SHA-1 as one-way function, i.e. \( H(\text{seed})=b \).

• Given the seed, it is easily verified that \( b \) was generated by this method

• Ensures the elliptic curve cannot be predetermined
Curve Selection

- The NIST curves were chosen by repeatedly selecting a random seed, and then checking the resulting curve against known attacks.
- In particular, the NIST curves do NOT belong to any known class of elliptic curves with weak security properties.
- Pseudo-random curves are unlikely to be susceptible to future special-purpose attacks.
Security of NIST Curves

• Assuming that SHA-1 cannot be inverted, generation process provides assurance NIST curves not intentionally constructed with hidden weaknesses

• There are NO known attacks of cryptographic significance which lessen the claimed security levels of the NIST curves