A brief discussion on selecting new elliptic curves

Craig Costello
Microsoft Research

http://research.microsoft.com/pubs/246915/NIST.pdf

A brief discussion on selecting new elliptic curves
with Patrick Longa and Michael Naehrig

Based on "*Selecting elliptic curves for cryptography*" [J. Crypt. Eng.] – joint work with Joppe Bos

[VCAT] Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology
http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

NUMS Curves

- Rigidly generated primes and constants
- Simplified generation: largest prime and smallest curve constant
- Match standard security levels

Security	Prime (p)	Weierstrass (b) $y^2=x^3-3x+b$	Edwards (d) $x^2+y^2=1+dx^2y^2$
128	$2^{256}-189$	152961	-15342
192	$2^{384}-317$	-34568	-11556
256	$2^{512}-569$	121243	-78296

Curve models: relative benefits

- **Weierstrass:**
  - general
  - prime order possible
  - backwards compatible

- **Edwards:**
  - one addition formula (complete)
  - easier constant-time code
  - speed (≈1.2x)

Twist security

Our position

- Importance should not be overstated: e.g., should not be used to dismiss previous standard curves (they are prime order anyway)
- If generating new curves once-and-for-all, may as well have it

Rigidity and curve constants

> *"NIST should ensure that there are no secret or undocumented components or constants in its cryptographic standards whose origin and effectiveness cannot be explained."*
>
> Steve Lipner [VCAT, p.49]

- Popular curve instantiations specified by one constant
- Size of constant has no influence on ECDLP difficulty
- Over a given prime, find smallest constant such that E and E’ have optimal group orders

Deterministic generation algorithms

"NIST should consider the publication of a standard algorithm and corresponding software to generate additional elliptic curves and should consider to use this tool to also publish some new curves."

Bart Preneel [VCAT, p.65]

Weierstrass E: $y^2=x^3-3x+b$

```
On input of prime $p$:

for $b$ in $\{1,-1, 3,-3,4,-4,\ldots\}$
    if #E and #E' are both prime
        return $b$
```

Edwards E: $x^2+y^2=1+dx^2y^2$

```
On input of prime $p = 3 \pmod 4$:

for $d$ in $\{-1, 2,-2,3,-3,\ldots\}$
    if $\#E=4r$ and $\#E'=4r'$ and $r,r'$ both prime
        return $d$
```

… and of course, check large MOV degree, large discriminant, trace not in {0,1}, etc…

NUMS Curves

- On input of 3 primes below, these algorithms give:

Security	Prime (p)	Weierstrass (b) $y^2=x^3-3x+b$	Edwards (d) $x^2+y^2=1+dx^2y^2$
128	$2^{256}-189$	152961	-15342
192	$2^{384}-317$	-34568	-11556
256	$2^{512}-569$	121243	-78296

- Why these primes?… deterministic prime generation is a good idea too

```
On input of target level of bit-security s, do:
        return smallest c such that $2^{2s}-c$ is prime and 3 mod 4
```

Why these primes?

"Security first: When NIST issues a standard or guideline whose primary purpose is security, the security of that standard or guideline should be treated as top priority… This principal also requires that design of security standards be conservative with minimal assumptions…"

Steve Lipner [VCAT, p.47]

- Full-length primes maximize ECDLP difficulty for a given security level (without unnecessary spillover)
- Our pseudo-Mersenne primes facilitate efficient ECC at all three target security levels

– see [ECCLib] v2.0

Why not different bit-length primes?

- We implemented a range of prime shapes and prime bit-lengths
- There is *some* performance to be gained by using primes of smaller bit-length, but not too much (TBC tomorrow)
- Current metrics of security vs. performance (e.g., “bang-for-your-buck”) are ad-hoc
- Performance of primes is highly sensitive to architecture

Our position

- Moving the goalposts is unnecessary, could compromise transparency, and is a slippery slope!

Why those three security levels?

Our position

- We have yet to see a reason to deviate from traditional security levels (research continues…)
- Agrees with **[NIST2012]:**
  128, 192, 256-bit levels using 256, 384 and 512-bit curves
- Choose curves consistently (same prime/curve generation algorithms) across security levels to ease implementation

[VCAT] *Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology*, July 2014. http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

[CLN'15] C-Longa-Naehrig. *A brief discussion on selecting new elliptic curves*, June 2015. http://research.microsoft.com/pubs/246915/NIST.pdf

[BCLN'15] Bos-C-Longa-Naehrig. *Selecting elliptic curves for cryptography: an efficiency and security analysis*, May 2015. http://link.springer.com/article/10.1007%2Fs13389-015-0097-y

[ECCLib] MSR ECC Library. http://research.microsoft.com/en-us/downloads/149804d4-b5f5-496f-9a17-a013b242c02d/default.aspx

[NIST2012] *Recommendations for Key Management*, Special Publication 800-57 Part 1 Rev. 3, 2012.

Questions?