Some Elliptic CUrve REsults

Elligator

by Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

MiniaLT

by W. Michael Petullo, Xu Zhang, Jon A. Solworth, Daniel J. Bernstein, and Tanja Lange

http://safecurves.cr.yp.to/

by Daniel J. Bernstein and Tanja Lange

December 3, 2013

Elligator

Your protocol sends elliptic curve points (public keys) but they need to look like random strings because

- you're fighting censorship; connection will be cut if your protocol is detected.

---

http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

Elligator

Your protocol sends elliptic curve points (public keys) but they need to look like random strings because

- you're fighting censorship; connection will be cut if your protocol is detected.
- you're evil and need random strings in your kleptography scheme.

---

http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

Elligator

Your protocol sends elliptic curve points (public keys) but they need to look like random strings because

- you're fighting censorship; connection will be cut if your protocol is detected.
- you're evil and need random strings in your kleptography scheme.

You need to map arbitrary strings to curve points because

- your PAKE scheme breaks if only half of the passwords land on curve points.

---

http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

Elligator

Your protocol sends elliptic curve points (public keys) but they need to look like random strings because

- you're fighting censorship; connection will be cut if your protocol is detected.
- you're evil and need random strings in your kleptography scheme.

You need to map arbitrary strings to curve points because

- your PAKE scheme breaks if only half of the passwords land on curve points.

You have been using an elliptic curve together with its twist for whatever reason.

---

http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

Elligator

Your protocol sends elliptic curve points (public keys) but they need to look like random strings because

- you're fighting censorship; connection will be cut if your protocol is detected.
- you're evil and need random strings in your kleptography scheme.

You need to map arbitrary strings to curve points because

- your PAKE scheme breaks if only half of the passwords land on curve points.

You have been using an elliptic curve together with its twist for whatever reason.

You might be interested in Elligator!

---

http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

Elligator

Choose prime $p = 2^n - c$ with small c, then integers $\leq (p-1)/2$ cover essentially all strings of $n-1$ bits.

---

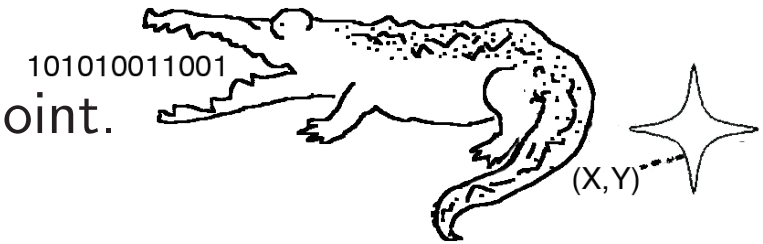
http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

Elligator

Choose prime $p = 2^n - c$ with small c, then integers $\leq (p-1)/2$ cover essentially all strings of $n-1$ bits.

Elligator map takes any integer $\leq (p-1)/2$ and produces curve point.



---

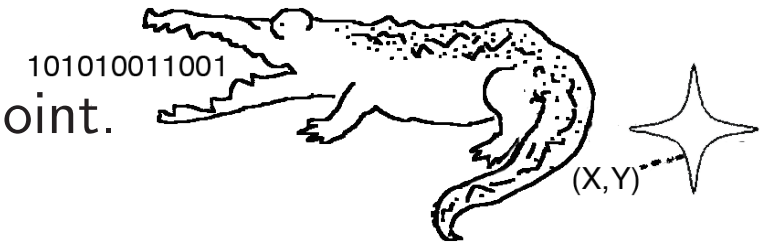
http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

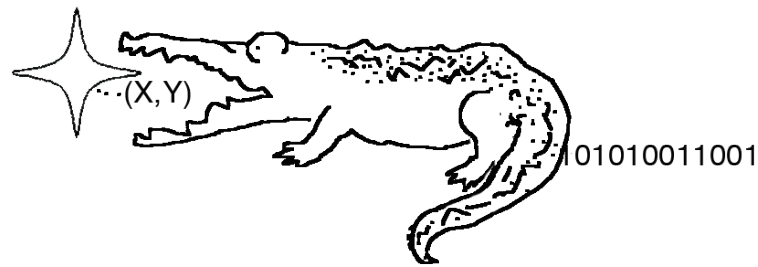
Elligator

Choose prime $p = 2^n - c$ with small c, then integers $\leq (p-1)/2$ cover essentially all strings of $n-1$ bits.

Elligator map takes any integer $\leq (p-1)/2$ and produces curve point.



Inverse elligator map defined on $(p-1)/2$ points, produces string of $n-1$ bits.



---

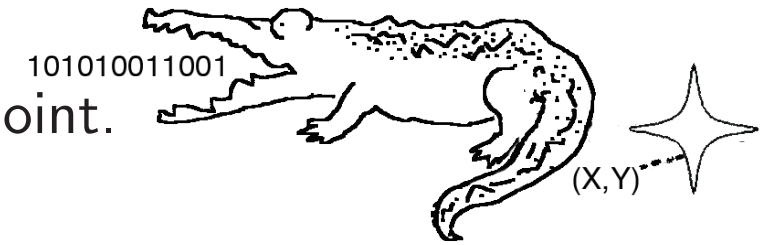
http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

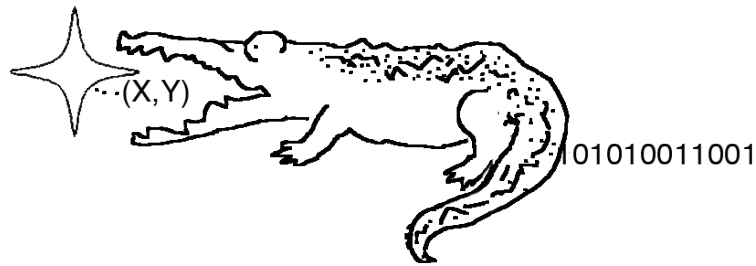
Elligator

Choose prime $p = 2^n - c$ with small c, then integers $\leq (p-1)/2$ cover essentially all strings of $n-1$ bits.

Elligator map takes any integer $\leq (p-1)/2$ and produces curve point.



Inverse elligator map defined on $(p-1)/2$ points, produces string of $n-1$ bits.



Maps are inverse of one another and efficiently computable.
Very fast test whether inverse map is defined on point
$\Rightarrow$ fast rejection of points, tweak protocol to try again.

---

http://elligator.cr.yp.to

Daniel J. Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange

MinimaLT – Minimal Latency Tunneling

- MinimaLT protocol makes secure connections
- Replaces TLS and TCP; built on top of UDP
- Advantages:
  - Stronger than TLS

---

http://www.ethos-os.org/

W. Michael Petullo, Xu Zhang, Jon A. Solworth, Daniel J. Bernstein, & me

MinimaLT – Minimal Latency Tunneling

- MinimaLT protocol makes secure connections
- Replaces TLS and TCP; built on top of UDP
- Advantages:
  - Stronger than TLS
  - Simpler than TLS

---

http://www.ethos-os.org/

W. Michael Petullo, Xu Zhang, Jon A. Solworth, Daniel J. Bernstein, & me

MinimaLT – Minimal Latency Tunneling

- MinimaLT protocol makes secure connections
- Replaces TLS and TCP; built on top of UDP
- Advantages:
  - Stronger than TLS
  - Simpler than TLS
  - Faster than TCP; even faster than QUIC

---

http://www.ethos-os.org/

W. Michael Petullo, Xu Zhang, Jon A. Solworth, Daniel J. Bernstein, & me

MinimaLT – Minimal Latency Tunneling

- MinimaLT protocol makes secure connections
- Replaces TLS and TCP; built on top of UDP
- Advantages:
  - Stronger than TLS
  - Simpler than TLS
  - Faster than TCP; even faster than QUIC
- Skips TCP handshake; authentication makes this safe
- Provides IP-address mobility: unlinkable, no handshake
- Overlaps ephemeral-key retrieval with DNS lookup
- Erases keys within minutes (TLS often takes months)
- Has strong protections against denial of service
- Fast crypto provided by NaCl.

---

http://www.ethos-os.org/

W. Michael Petullo, Xu Zhang, Jon A. Solworth, Daniel J. Bernstein, & me

MinimaLT – Minimal Latency Tunneling

- MinimaLT protocol makes secure connections
- Replaces TLS and TCP; built on top of UDP
- Advantages:
  - Stronger than TLS
  - Simpler than TLS
  - Faster than TCP; even faster than QUIC
- Skips TCP handshake; authentication makes this safe
- Provides IP-address mobility: unlinkable, no handshake
- Overlaps ephemeral-key retrieval with DNS lookup
- Erases keys within minutes (TLS often takes months)
- Has strong protections against denial of service
- Fast crypto provided by NaCl.

Extra advertisement

small (human-auditable) codebase: TweetNaCl

---

http://www.ethos-os.org/

W. Michael Petullo, Xu Zhang, Jon A. Solworth, Daniel J. Bernstein, & me

SafeCurves:
choosing safe curves for elliptic-curve cryptography

All known security criteria for elliptic curves,
machine verified.

---

http://safecurves.cr.yp.to

Daniel J. Bernstein and Tanja Lange

SafeCurves:
choosing safe curves for elliptic-curve cryptography

All known security criteria for elliptic curves,
machine verified.
Also: can the curve be backdoored?

---

http://safecurves.cr.yp.to

Daniel J. Bernstein and Tanja Lange

SafeCurves:
choosing safe curves for elliptic-curve cryptography

		Parameters:			ECDLP security:				ECC security:			
Curve	Safe?	field	equation	base	rho	transfer	disc	rigid	ladder	twist	complete	ind
Anomalous	False	True ✔	True ✔	True ✔	True ✔	False	False	True ✔	False	False	False	False
M-221	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔
E-222	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔
NIST P-224	False	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	False	False	False	False	False
Curve1174	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔
Curve25519	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔
BN(2,254)	False	True ✔	True ✔	True ✔	True ✔	False	False	True ✔	False	False	False	False
brainpoolP256t1	False	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	False	False	False	False
ANSSI FRP256v1	False	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	False	False	False	False	False
NIST P-256	False	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	False	False	True ✔	False	False
secp256k1	False	True ✔	True ✔	True ✔	True ✔	True ✔	False	True ✔	False	True ✔	False	False
M-383	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔
Curve383187	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔
brainpoolP384t1	False	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	False	True ✔	False	False
NIST P-384	False	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	False	False	True ✔	False	False
Curve3617	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔	True ✔

---

http://safecurves.cr.yp.to

Daniel J. Bernstein and Tanja Lange