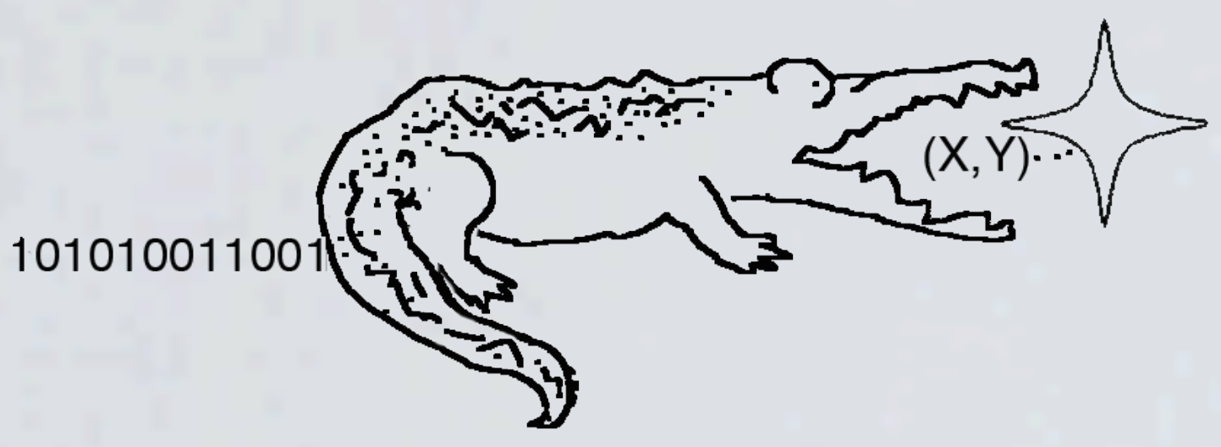
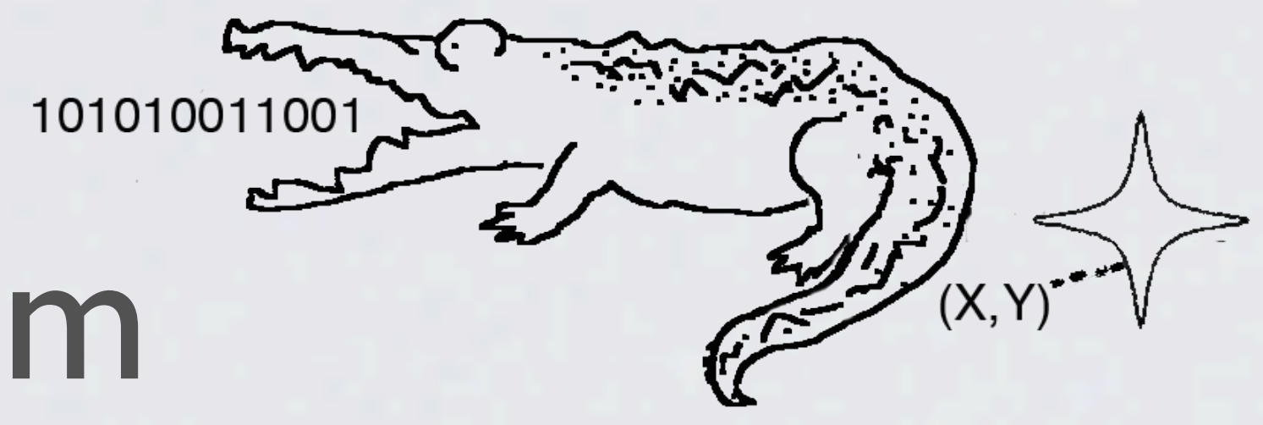


Elligator

Elliptic curve points indistinguishable from random strings



http://elligator.cr.yp.to

Censorship sucks!

How would you feel if you could not access Youtube, Facebook, Twitter anymore? How about Google only presenting highly filtered results? No independent news websites written in your native language?

Crypto protocol without Elligator:

- **Curve point (key exchange) followed by random string (ciphertext)**
- **Censor recognizes curve point, terminates connection**

Perfectly hide in the crowd

Our goal is to make anticensorship protocols undetectable. Make sure that *each sent string corresponds to an EC point.*

Crypto protocol with Elligator: Random string (key exchange) followed by random string (ciphertext)

Elligator!

Elligator makes curve point indistinguishable from uniform random strings!

Crypto protocol without Elligator: FLAGGED, CENSORED

Crypto protocol with Elligator: UNDETECTABLE

Crypto as a red flag

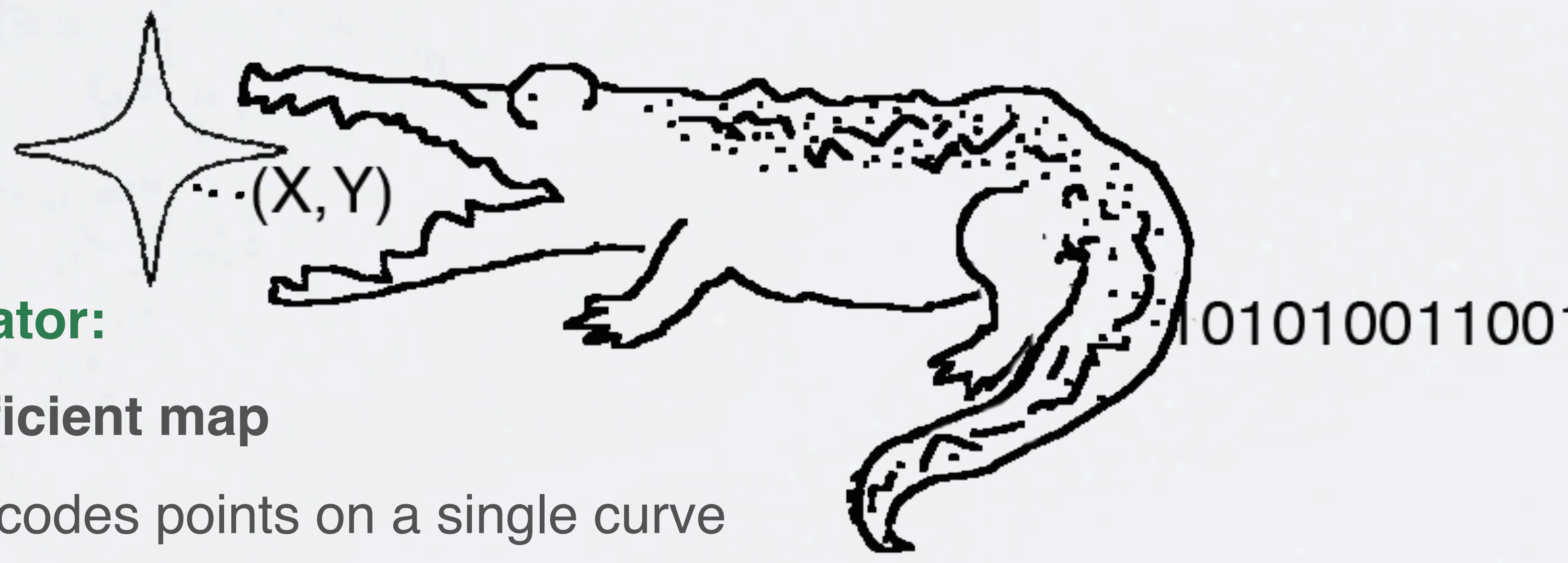
Transform traffic to look like something else:

- Censorship-circumvention protocols encrypt traffic to make it look random.
- For this users and a server need to share keys
- They are sending public keys

Without elligator: it's easy to distinguish curve points from random strings:

- Elliptic curve (EC) cryptography is a state-of-the-art tool providing speed and strong security
- Public keys are EC points
- EC points are easy to distinguish from random strings
- E.g. Check if *(x, y)* coordinates satisfy EC equation

$$y^2 = x^3 - 3x + b$$



Elligator:

- **Efficient map**
- Encodes points on a single curve
- Points indistinguishable from random
- On average every second point can be mapped
- **Fast check** whether a point can be mapped
- **Efficient inverse map**: from strings to points

Elligator 1: Edwards curves $E(\mathbf{F}_q)$, $q \equiv 3 \bmod 4$

- *Curve1174 specifically designed for Elligator 1*

Elligator 2: **Any** curve with a point of order 2, any odd *q*

- *Curve25519* is suitable for Elligator 2

Daniel J. Bernstein
Department of
Computer Science
University of Illinois at
Chicago
USA

Anna Krasnova
Privacy & Identity lab
Institute for Computing
and Information
Sciences
Radboud University
Nijmegen
The Netherlands

Mike Hamburg
Cryptography Research
A division of Rambus
USA

Tanja Lange
Department of
Mathematics and
Computer Science
Technische Universiteit
Eindhoven
The Netherlands

Acknowledgements:

This work was supported by the National Science Foundation under grant 1018836, by the Netherlands Organisation for Scientific Research (NWO) under grants 639.073.005 and 040.09.003, by the National Science Council of Taiwan under NSC 101-2915-I-001-019, by the European Commission under Contract ICT-2007-216676 ECRYPT II, and by SIDN.nl (http://www.sidn.nl/). Part of this work was done while Bernstein, Krasnova, and Lange visited Academia Sinica; they wish to thank Bo-Yin Yang for his hospitality.