Attacking Elliptic-Curve Cryptography

Ruben Niederhagen

April 15, 2010

Why cryptography?

Provide a virtual private room for conversation.

- Authentication: The process of proving one's identity.
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism that the sender cannot deny having sent this message.

This becomes complicated when you can not be in the same room physically.

Where do we encounter cryptography?

- web browser: online banking, electronic shopping, ...
- email: signatures on emails, encryption of emails, ...
- ov-chipkaart
- passport: electronic passport has eliptic curve signatures
- ...

Where do we encounter cryptography?

Therefore, a big variety of devices is in use:

- servers
- personal computers, notebooks
- smart phones (blackberry...)
- passive chip cards
- ...

How can we provide privacy and authenticity?

Use a lock:

- Easy to open with a key.
- Hard to open without the key.

Hide message in a hard problem which is easy to solve in the knowledge of a certain secret.

Currently most commonly used: integer factorization and RSA problem

Small and embedded devices: elliptic curve discrete logarithm problem (ECDLP)
only one approved by NSA for high security
$\longrightarrow$ the future of cryptographic applications?

Must be easy to solve with the key but hard without the key!
Common metric: *key length*

The Certicom challenges

1997: Certicom announces several ECDLP prizes:

> *The Challenge is to compute the ECC private keys from the given list of ECC public keys and associated system parameters. This is the type of problem facing an adversary who wishes to completely defeat an elliptic curve cryptosystem.*

Objectives:

- Increase the understanding and appreciation of the difficulty of the ECDLP.
- Enable comparisons between the security levels of cryptographic systems such as ECC, RSA and DSA.
- Provide information on suitable key lengths for a desired level of security.

The Certicom challenges, level 0: exercises

Bits	Name	"Estimated number of machine days"	Prize
79	ECCp-79	146	book
79	ECC2-79	352	book
89	ECCp-89	4360	book
89	ECC2-89	11278	book
97	ECC2K-95	8637	$5000
97	ECCp-97	71982	$5000
97	ECC2-97	180448	$5000

The Certicom challenges, level 1

Bits	Name	"Estimated number of machine days"	Prize
109	ECC2K-108	1300000	$10000
109	ECCp-109	9000000	$10000
109	ECC2-109	21000000	$10000
131	ECC2K-130	2700000000	$20000
131	ECCp-131	23000000000	$20000
131	ECC2-131	66000000000	$20000

The Certicom challenges, level 2

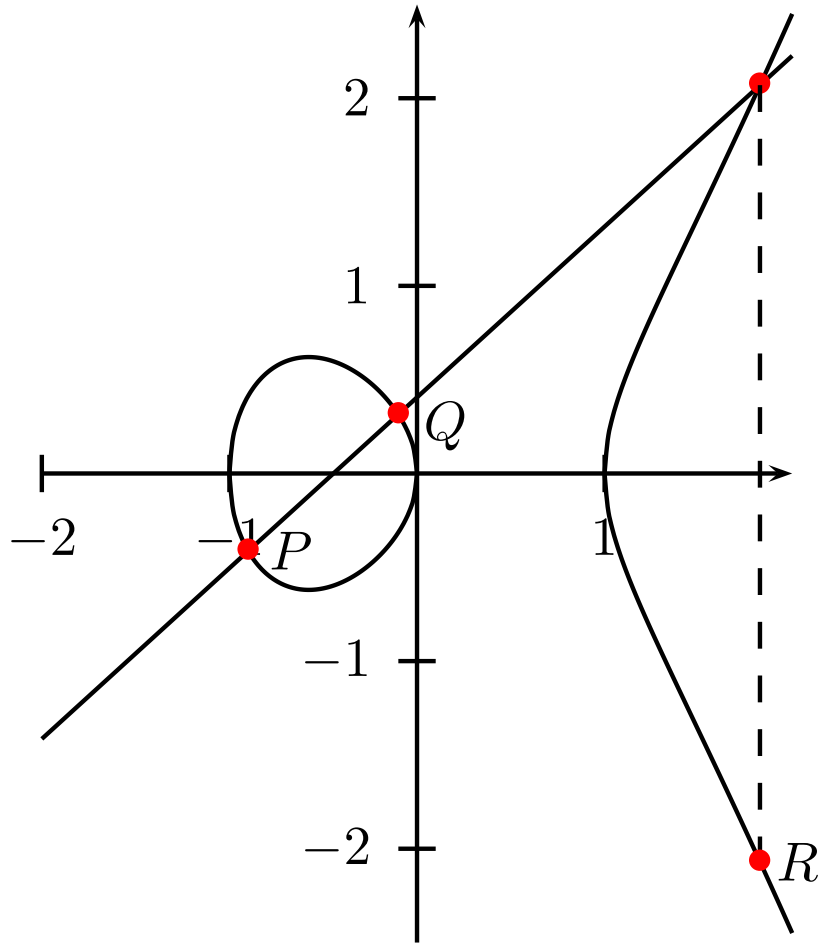
Bits	Name	"Estimated number of machine days"	Prize
163	ECC2K-163	3200000000000000	$30000
163	ECCp-163	23000000000000000	$30000
163	ECC2-163	62000000000000000	$30000
191	ECCp-191	4800000000000000000	$40000
191	ECC2-191	10000000000000000000	$40000
239	ECC2K-238	9200000000000000000000000	$50000
239	ECCp-239	14000000000000000000000000	$50000
239	ECC2-238	21000000000000000000000000	$50000
359	ECCp-359	$\approx \infty$	$100000

Broken challenges

1997: Baisley and Harley break ECCp-79.
1997: Harley et al. break ECC2-79.
1998: Harley et al. break ECCp-89.
1998: Harley et al. break ECC2-89.
1998: Harley et al. (1288 computers) break ECCp-97.
1998: Harley et al. (200 computers) break ECC2K-95.
1999: Harley et al. (740 computers) break ECC2-97.
2000: Harley et al. (9500 computers) break ECC2K-108.
2002: Monico et al. (10000 computers) break ECCp-109.
2004: Monico et al. (2600 computers) break ECC2-109.

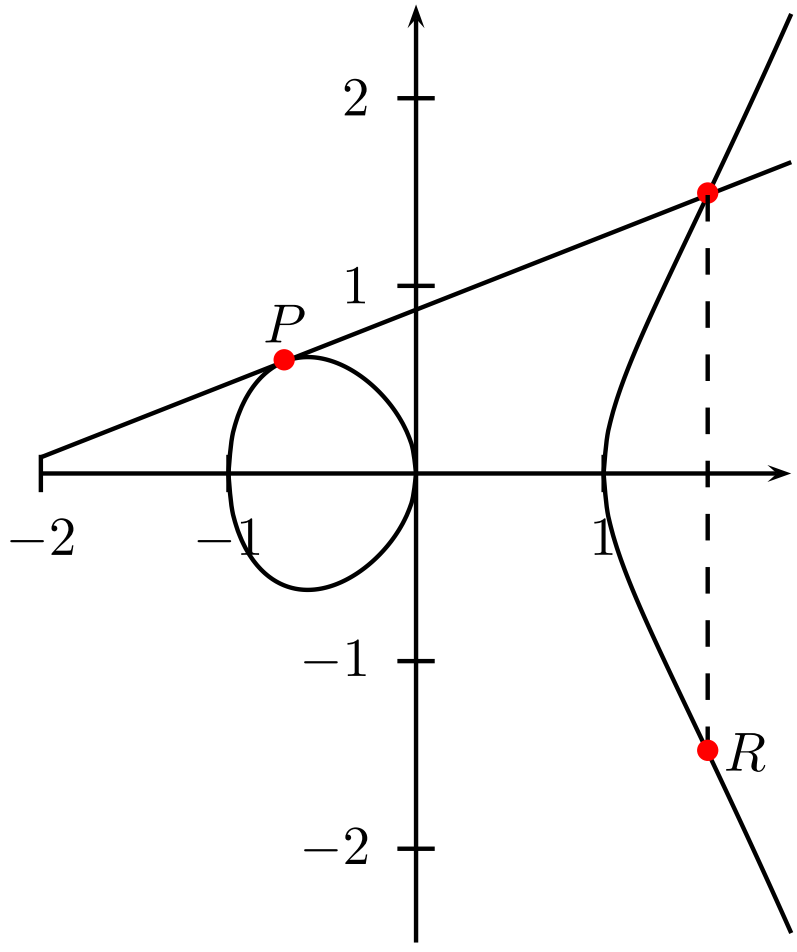
next unbroken challenge is ECC2K-130

Addition on an elliptic curve over $\mathbb{R}$



$P + Q = R$ on $C : y^2 = x^3 - x; \quad x, y \in \mathbb{R}$

Doubling on an elliptic curve over $\mathbb{R}$



$2P = P + P = R$ on $C : y^2 = x^3 - x; \quad x, y \in \mathbb{R}$

The target: ECC2K-130

The Koblitz curve $y^2 + xy = x^3 + 1$ over
$\mathbf{F}_{2^{131}} = \mathbf{F}_2[z]/(z^{131} + z^{13} + z^2 + z + 1)$

Certicom generated two random points P, Q on the curve:

P_x = 05 1C99BFA6 F18DE467 C80C23B9 8C7994AA
P_y = 04 2EA2D112 ECEC71FC F7E000D7 EFC978BD
Q_x = 06 C997F3E7 F2C66A4A 5D2FDA13 756A37B1
Q_y = 04 A38D1182 9D32D347 BD0C0F58 4D546E9A

The challenge:
Find an integer $k \in \{0, 1, \ldots, \ell - 1\}$ such that $[k]P = Q$
where ℓ is the prime
$680564733841876926932320129493409985129 \approx 2^{129}$.
$\rightarrow$ can not be broken by brute force

Breaking ECC2K-130

With our latest implementations, ECC2K-130 is breakable in a year on average

- by 3039 3GHz Core 2 CPUs,
- or by 2462 Cell CPUs,
- or by 1263 GTX 295 GPUs,
- or by 615 XC3S5000 FPGAs,
- or by (estimated) 100 ASICs costing 60000 EUR,
- or by any combination thereof.

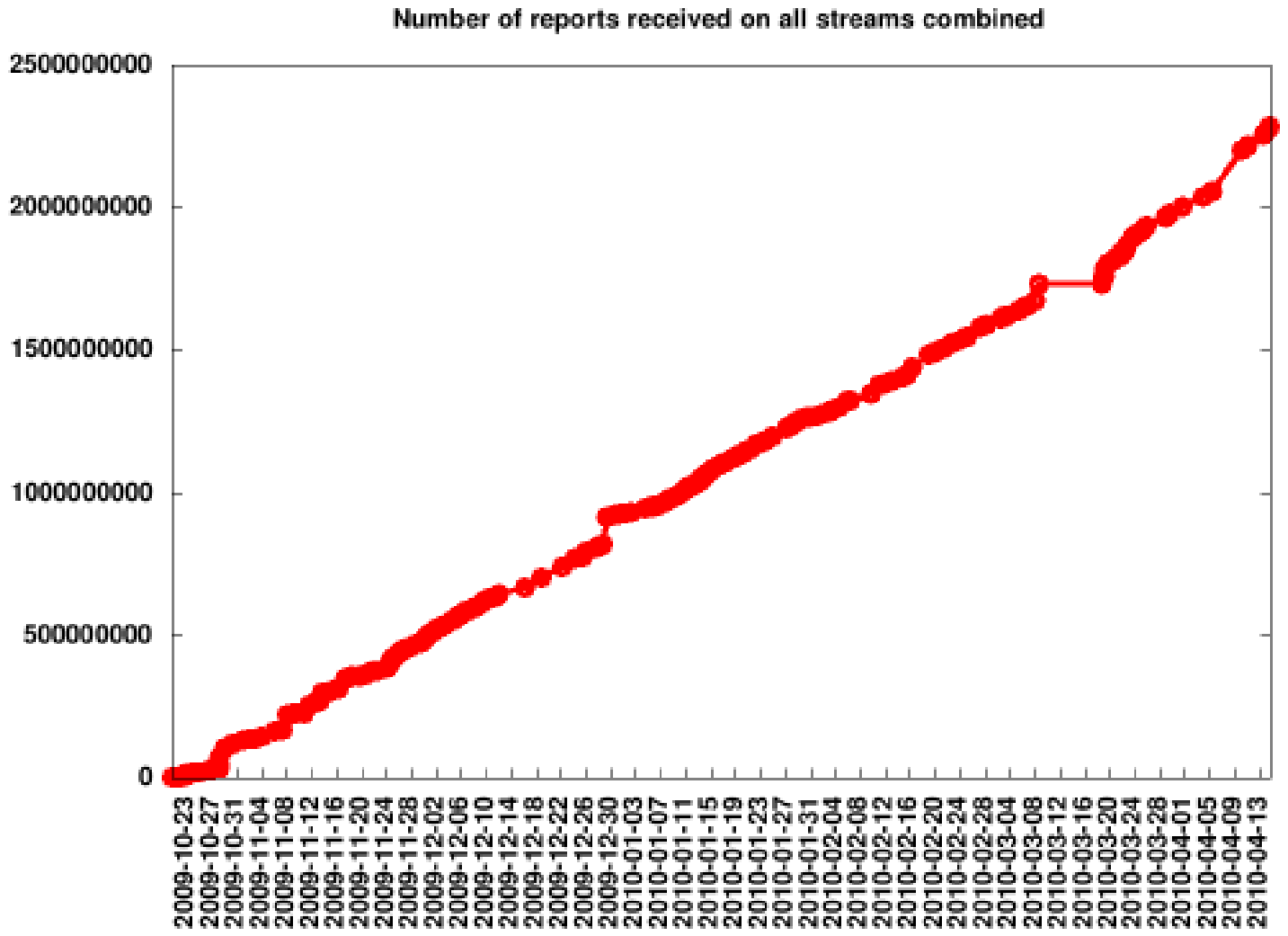
Contributors

TU/e is running several servers to collect data.

14 sites all over the world are sending data in:

- Technische Universiteit Eindhoven: x86 nodes, GPU nodes
- Ecole Polytechnique Fédérale de Lausanne: Cell and x86 nodes
- Katholieke Universiteit Leuven: x86 nodes
- Bristol University: x86 nodes
- Ireland's High-Performance Computing Centre: x86 nodes
- Jülich Supercomputing Centre: Cell nodes
- National Taiwan University: x86 nodes, GPU nodes
- University of Illinois at Chicago: x86 nodes, GPU nodes
- Ruhr University of Bochum: FPGAs
- ...

Current progress:



http://ecc-challenge.info

People involved in breaking ECC2K-130

Daniel V. Bailey, Lejla Batina, Daniel J. Bernstein, Peter Birkner,
Joppe W. Bos, Hsieh-Chung Chen, Chen-Mou Cheng,
Gauthier van Damme, Giacomo de Meulenaer,
Luis Julian Dominguez Perez, Junfeng Fan, Tim Güneysu,
Frank Gürkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens,
Ruben Niederhagen, Christof Paar, Francesco Regazzoni,
Peter Schwabe, Leif Uhsadel, Anthony Van Herrewege,
Bo-Yin Yang

Get more details, and watch our progress!

http://eprint.iacr.org/2009/466:
"The Certicom challenges ECC2-X" (SHARCS 2009)—
analysis of ECC2K-130, ECC2-131, ECC2K-163, ECC2-163 with
ASIC, FPGA, Cell, Core2 implementation details.

http://eprint.iacr.org/2009/541:
"Breaking ECC2K-130"; continues to be improved;
more platforms, better speeds, running the attack.

http://ecc-challenge.info:
graph of number of points reported to the servers.

https://twitter.com/ECCchallenge:
Twitter page with the latest announcements.