Research Status of the ECDLP

ZHANG Fangguo(张方国)

School of Data and Computer Science

Sun Yat-sen University, China

Email: isszhfg@mail.sysu.edu.cn

2019.11.07 Guangzhou

Outline

– 1976 : Public-Key Cryptography (Whitfield Diffie and Martin Hellman) *New Directions in Cryptography*. IEEE.IT,1976

Win 2015

Discrete Logarithm Cryptosystem

- $G=\langle g\rangle$, $|G|=n$
  (i) group elements can be compactly represented;
  (ii) the group operation can be performed efficiently;
  (iii) DLP is hard: given g, $y=g^x$, find x
- Many applications:
  Diffie-Hellman Key Exchange;
  ElGamal encryption;
  DSA ……
- Group: Fp*

1985, ECC
Victor S. Miller and Neal Koblitz

Replacing Fp* with elliptic group!

Elliptic Curve

Let k be a finite field. Consider an **elliptic curve** over k defined by

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

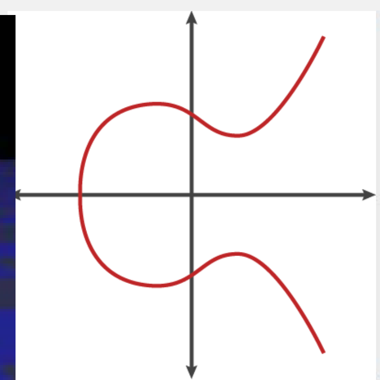
The set

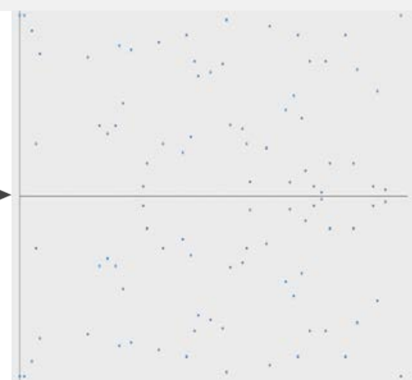
$$E(k) = \{(x, y) \in k^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \sqcup \{\infty\}$$

has a natural addition law $+$ which makes $E(k)$ into a *finite abelian group* with identity element ∞.

When Char(k) is not 2,3, after a change of variables, the equation takes the simpler form

$$\boxed{E : y^2 = x^3 + A\,x + B}$$



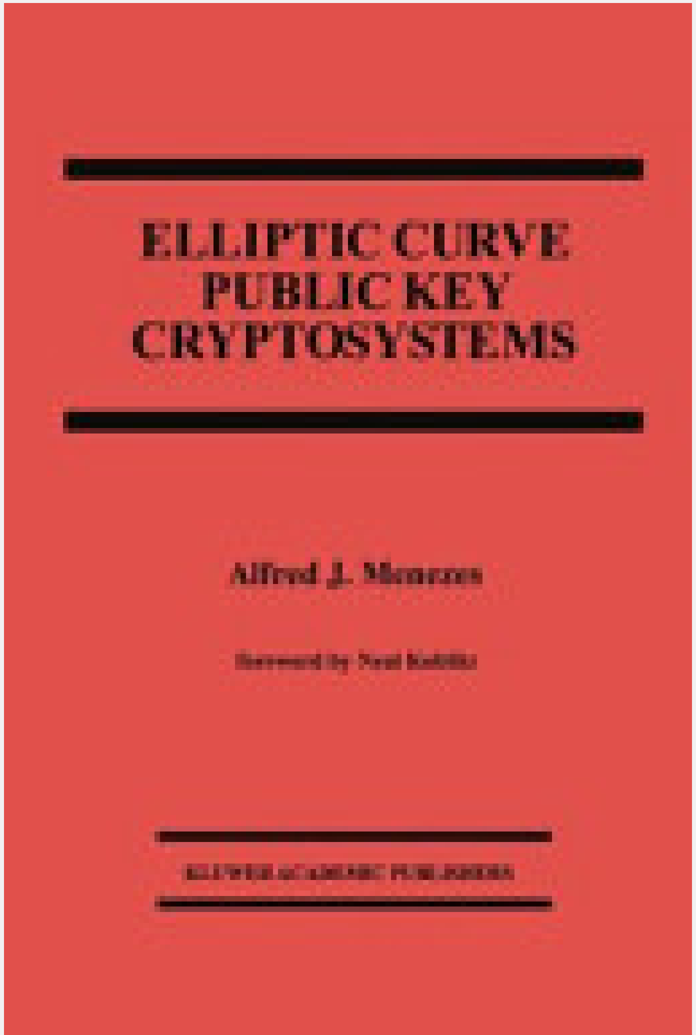


ECC

ECC Parameters

- Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$.
- Suppose $\#E(\mathbb{F}_q) = nh$, where n is prime and h is small. (By Hasse's Theorem, we have $n \approx q$.)
- Let $P \in E(\mathbb{F}_q)$ be a base point of order n.
- Key generation: Each user selects a random integer $d \in [0, n-1]$. The user's public key is $Q = dP$, and its private key is d.
- A necessary condition for the security of any ECC protocol is that the ECDLP be intractable:
  - Given E, n, P and Q, find d.

ECC is a mainstream primitive for cryptographic protocols and applications



ECDH for key exchange

ECDSA

Secure Shell (SSH)

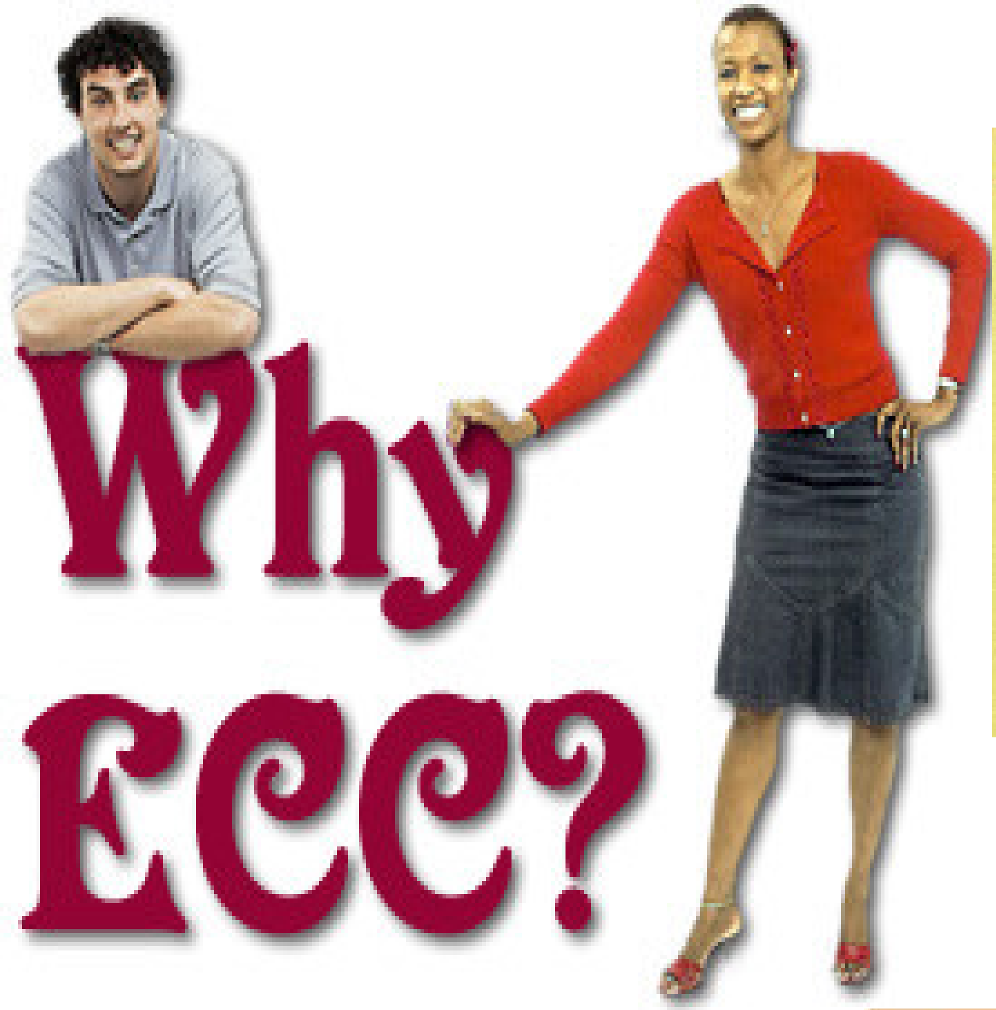
Transport Layer Security (TLS)

Bitcoin

$E : y^2 = x^3 + 7$ *over* F_p, $p=2^{256} - 2^{32} - 977$

Austrian Citizen Card(e-ID)

……



ECC key (bits)	RSA key (bits)	Ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

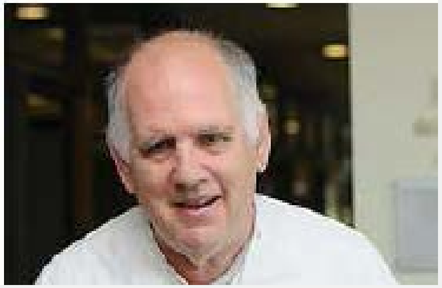
We want shorter keys!

ECC in Standards

- ANSI X9: 62, 63, 92, …
- IEEE: 1363-2000, P1363a, P1363.2, P802.15.3/4, …
- ISO: 14888-3, 9496, 15496, 18033-2, …
- FIPS: 186-2, 2XX, …
- NESSIE, IPA Cryptrec, …
- SECG: SEC1, SEC2, …
- IETF: PKIX, IPSec, SMIME, TLS, …
- SET, MediaPlayer, 5C, WAP, …
- China: SM2

Current research status of ECC

- Faster implementation：
  New algorithm**(Edwards curves)**， **software, hardware**
- Standards and more new applications
  Certicom, RSA, NIST, IEEE P1363, RFID, Blockchain……



Montgomery

$p = 2^{255} - 19,$

$E: y^2 = x^3 + 486662x^2 + x$

Ed25519

$p = 2^{255} - 19,$

$$E: -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2,$$

ECDLP： Security of ECC

Elliptic curve discrete logarithm problem (ECDLP):
Given $P, Q \in E(\mathbb{F}_q)$ to find an integer a, if it exists, such that $Q = aP$.

Attack on ECDLP

- Pohlig and Hellman Reduction
- Square Root Attacks: Generic algorithms
  Pollard Rho(Parallel), Pollard Lambda Attack
- Special cases:
  Additive Reduction (1998Semaev, Araki/Satoh, Smart),
  Multiplicative Reduction (MOV 1993, Frey-Ruck1994),
- Index calculus:
  Weil Descent (Frey1998, Hess, Gaudry, Diem, Scholten)
  Summation polynomial(Semaev2004)

Steven Galbraith, 2010.8

For the past 5 years or more there have been no significant new results on the elliptic curve discrete logarithm problem. There are at least 3 possible interpretations of this fact:

- Everyone has been working **on pairing-based cryptography** and has stopped looking at the ECDLP.
- Everyone is now interested **in lattices** and no-one is looking at elliptic curves any more.
- Research progress on the ECDLP has stabilised, in much the same way that progress on factoring has been stable for the last 15 or more years. This interpretation suggests that the ECDLP is indeed a hard computational problem.

From 2010

- **Speeding up Square Root Attacks**
  Baby-Step-Giant-Step, Pollard Rho Algorithm
- **Effort on index calculation**
  index calculus using summation polynomial method
- **Practice attacks**

Improving Baby step Giant step

- Q=aP, ord(P)=n
- M= $\lfloor \sqrt{n} \rfloor$

Then $a = a_0 + Ma_1$ with $0 \le a_0, a_1 < M$

Compute stored list of **Baby step**

(aP, a) for $0 \le a < M$.

Let $P' = MP$. Compute "giant steps" $Q - bP'$ for $b = 0, 1, 2, \ldots$ until get a match.

Baby step Giant step

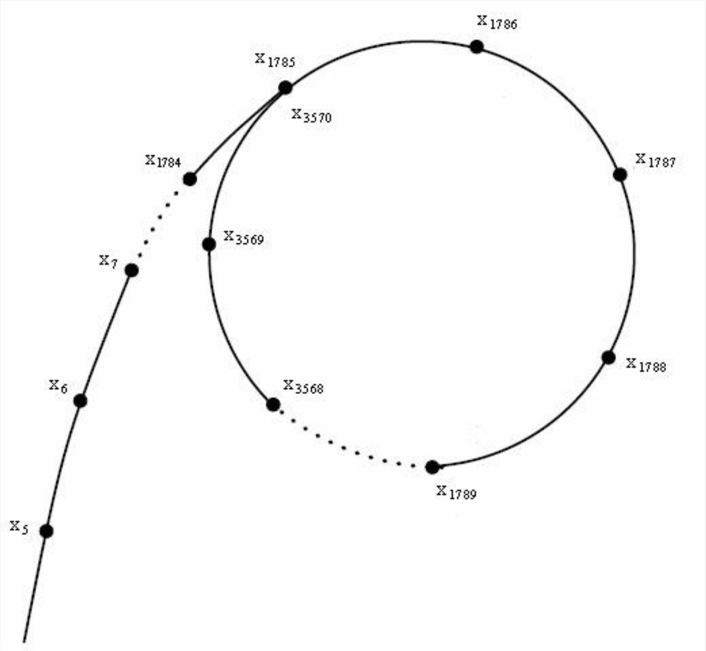
Algorithm	Average-case	Worst-case
Textbook BSGS [19]	1.5	2.0
Textbook BSGS optimised for average-case [18]	1.414	2.121
Pollard interleaving BSGS [17]	1.333	2.0
Grumpy giants [2]	1.25*	≤ 3
Pollard rho using distinguished points [20]	1.253	∞
Gaudry-Schost [7]	1.661	∞
BSGS with negation	1.0	1.5
Pollard interleaving BSGS with negation	0.943	1.414
Grumpy giants with negation	0.9*	≤ 2.7
Pollard rho using negation [3, 21]	$0.886(1 + o(1))$	∞
Gaudry-Schost using negation [8]	1.36	∞
Interleaved BSGS with block computation	0.38	0.57
Grumpy giants with block computation	0.36*	≤ 1.08
Pollard rho with Montgomery trick	0.47	∞
Gaudry-Schost with Montgomery trick	0.72	∞

Steven Galbraith, Ping Wang and Fangguo Zhang, Computing Elliptic Curve Discrete Logarithms with Improved Baby-step Giant-step Algorithm. Advances in Mathematics of Communications, Volume 11, No. 3, 2017, 453-469

Speeding up Pollard Rho Method

Pollard, J. M. (1978). "Monte Carlo methods for index computation (mod p)". Mathematics of Computation ***32*** *(143): 918–924.*

$$X_{i+1} = f(X_i) = \begin{cases} Q + X_i & X_i \in S_1, \\ 2X_i & X_i \in S_2, \\ P + X_i & X_i \in S_3. \end{cases}$$



– Pollard rho and its parallelized variants are at present known as the best generic algorithms for ECDLP

EC over GF(2^n) and Point Halving

$$\boxed{y^2 + xy = x^3 + ax^2 + b}$$

Input: $Q = (x_2, y_2) \in \langle P \rangle$.

Output: $H = (x_1, y_1) \in \langle P \rangle$, where $Q = 2H$.

1: compute λ such that $\lambda^2 + \lambda = x_2 + a$.

2: $w \leftarrow x_2(\lambda + 1) + y_2$.

3: **if** $\mathrm{Tr}(w + a^2) = 0$ **then**

4: $\quad x_1 \leftarrow \sqrt{w}$, $y_1 \leftarrow x_1(x_1 + \lambda)$.

5: **else**

6: $\quad x_1 \leftarrow \sqrt{w + x_2}$, $y_1 \leftarrow x_1(x_1 + \lambda + 1)$.

7: **end if**

PH cost: [2.6M, 3.2M]

Doubling cost: I+2M (>10M)

Iteration Function from PH

$$Y_{i+1} = F(Y_i) = \begin{cases} Y_i + M_j & j \in \{1, \ldots, r\} \\ \frac{1}{2} Y_i & j \in \{r+1, \ldots, r+h\} \end{cases}$$

For certain NIST-recommended curves over binary fields, the new method is about 12–17% faster than the previous best methods.

Fangguo Zhang and Ping Wang, Speeding Up Elliptic Curve Discrete Logarithm Computations with Point Halving, Designs, Codes and Cryptography (2013) 67:197–208

Index calculus for ECDLP

- Xedni Calculus Method

  J. Silverman, 2000.

  Jacobson, N. Koblitz, J.H. Silverman, A. Stein, E. Teske, 2000.

- Weil Descent

  Gaudry P, **H**ess F, **S**mart N P. Constructive and destructive facets of Weil descent on elliptic curves. Journal of Cryptology, 2002, 15(1):19-46 (GF(2^{nm}))

- Summation polynomials

  Semaev, I.: *Summation polynomials and the discrete logarithm problem on elliptic curves, Preprint, 2004.*

Definition 1 *Let $\overline{\mathbb{K}}$ be the algebraic closure of the field $\mathbb{K}$. For any integer $m \geq 2$, the m-th summation polynomial S_m is an element of $\mathbb{K}[X_1, \ldots, X_m]$ and it is such that, given $x_1, \ldots, x_m \in \overline{\mathbb{K}}$, then $S_m(x_1, \ldots, x_m) = 0$ if and only if there exist $y_1, \ldots, y_m \in \overline{\mathbb{K}}$ for which $(x_1, y_1), \ldots, (x_m, y_m) \in E(\overline{\mathbb{K}})$ and*

$$(x_1, y_1) + \ldots + (x_m, y_m) = \infty$$

Weil Descent+ Summation

- Gaudry and Diem explored how to use this idea in the context of Weil descent and the ECDLP on elliptic curves over **GF(p^n)** .
- Diem showed there exists a sequence of finite fields GF(p^n) (not of prime degree) such that the ECDLP along this sequence is provably **subexponential**.
- A Joux, V Vitse, Cover and Decomposition Index Calculus on Elliptic Curves made practical,EUROCRYPT 2012 (151ecdlp over GF(p^6))
- Jean-Charles Faugère, Ludovic Perret, Christophe Petit, and Guénaël Renault. Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields. *EUROCRYPT 2012*, LNCS 7237 , pages 27-44.

ECDLP in characteristic 2

- Igor Semaev, New algorithm for the discrete logarithm problem on elliptic curves, eprint 2015/310
- Karabina, Huang-Petit-Shinohara-Takagi, Yeo
- Instead of Sm, one can introduce a system with more variables which only involve (many)S3

The time and memory complexity of computing summation polynomial zeroes under the assumption is polynomial in n. The overall time complexity of computing discrete logarithms on elliptic curves over F_{2^n} becomes proportional to

$$2^{c\sqrt{n \ln n}}, \tag{1}$$

where $c = \frac{2}{(2\ln\, 2)^{1/2}} \approx 1.69$. The asymptotical bound is still correct if $d_{F4} = o(\sqrt{\frac{n}{\ln n}})$. The

Under a
first fall
degree assumption

I can break ECDLP!!!

However, we believe that elliptic curves over characteristi
2 fields of prime degree n are not threatened by
Such methods and are still safe for use.

A New Method

- Construct an elliptic code from ECDLP;
- The minimum distance codewords of elliptic code and ECDLP;
- Finding minimum distance codewords for elliptic codes using list decoding.

This new algorithm is not efficient currently, and it is even not of square-root time algorithm.
However, this is the first method of solving ECDLP via list decoding, which is of theoretical significance

Fangguo Zhang and Shengli Liu, **Solving ECDLP via List Decoding,** Cryptology ePrint Archive: Report 2018/795, published at ProvSec2019.

The Certicom ECC Challenge

- 1997.11, Certicom announces several ECDLP prizes:
- The exercises
  79-bit: SOLVED December 1997(Book)
  89-bit: SOLVED February 1998(book)
  97-bit: SOLVED September 1999($5000)
- Level I
  ECC2K-108: SOLVED April 2000($10000)
  ECCp-109: SOLVED Nov. 2002($10000)
  ECC2-109: SOLVED April 2004($10000)
  131-bit: (ECC2K-130, ECC2-131, ECCp-131) still open($20000)
- Level II
  163-bit: (ECC2K-163, ECC2-163, ECCp-162) still open($30000)
  191-bit($40000), 239-bit($50000), 359-bit($100000): still open

ECDLP record

- 2009.07，EPFL
  Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra and Peter L. Montgomery, Solving a 112-bit Prime Elliptic Curve Discrete Logarithm Problem on Game Consoles using Sloppy Reduction, International Journal of Applied Cryptography, 2(3), 2012 , pp. 212-228.

- SAC2014

  Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster

  Erich Wenger and Paul Wolfger

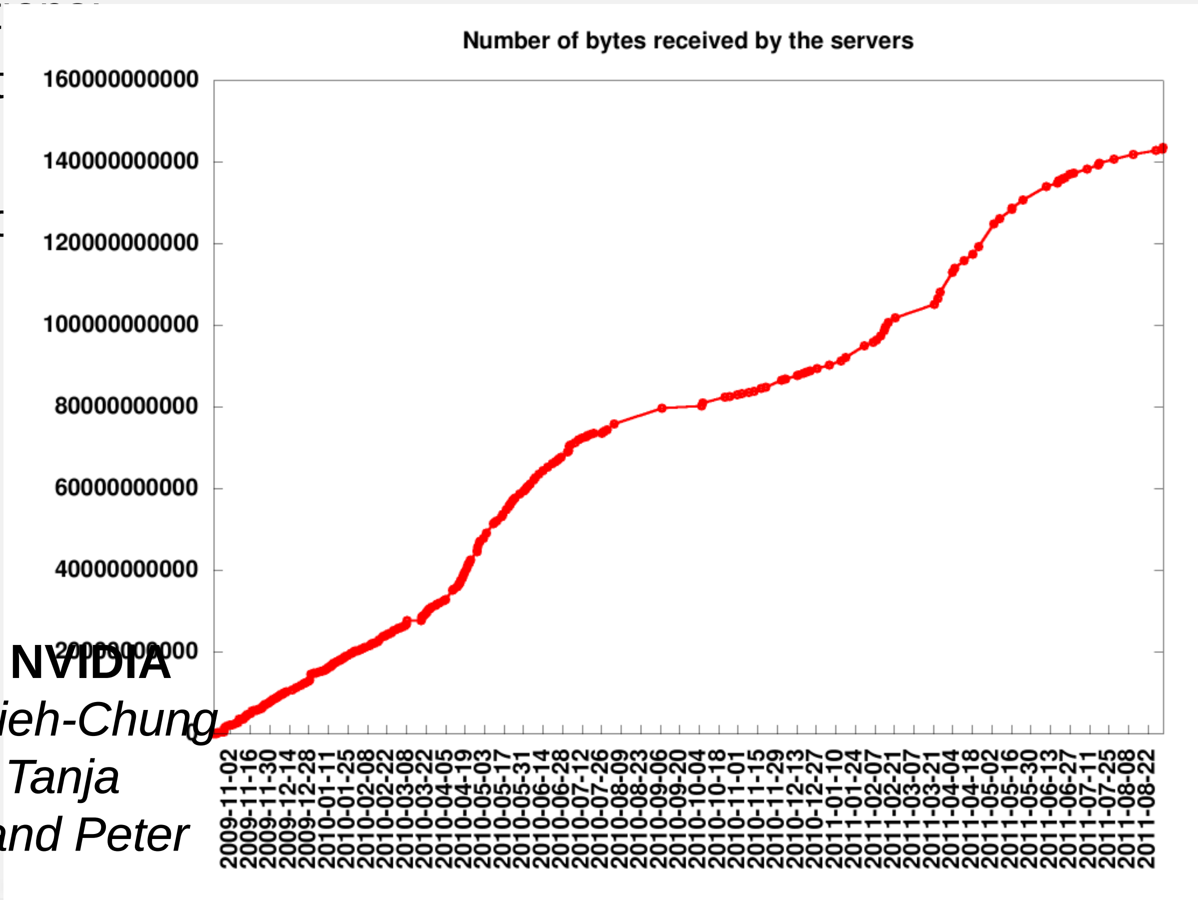
  Graz University of Technology
  Institute for Applied Information Processing and Communications
  Inffeldgasse 16a, 8010 Graz, Austria

- Erich Wenger and Paul Wolfger:new ECDLP record computation: ECC2-113, https://eprint.iacr.org/2015/143.pdf

Breaking ECC2K-130

http://ecc-challenge.info

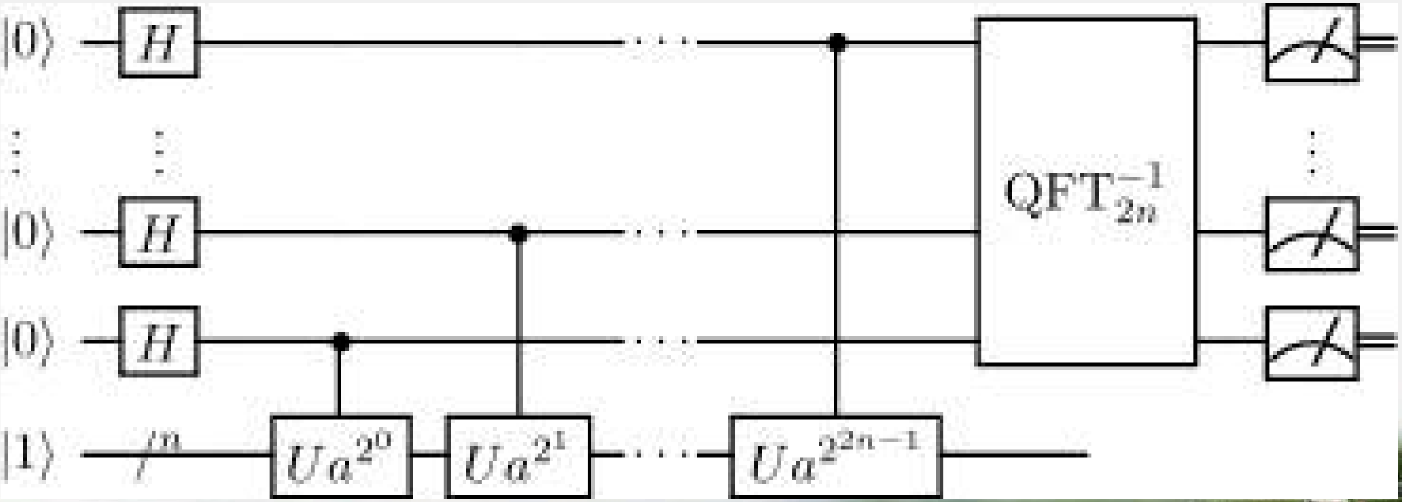
Finding a distinguished point takes on average $2^{25.27}$ iterat… we estimate a total computat… time of $2^{60.9}$ iterations (corresponding to finding abo… $2^{35.63}$ distinguished points)



2012/002 (PDF)**ECC2K-130 on NVIDIA GPUs***Daniel J. Bernstein and Hsieh-Chung Chen and Chen-Mou Cheng and Tanja Lange and Ruben Niederhagen and Peter Schwabe and Bo-Yin Yang*

Quantum computing on ECDLP

- Shor 94: Quantum computers can
  - Factor integers
  - Calculate DLP (in any group)
- **This breaks two common PKC**
  - RSA
  - ECC



Quantum computers!

- Quantum computers are on the way!
- Google quantum supremacy

nature > articles > article

MENU

nature

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature (2019) | Download Citation

1044 Altmetric | Metrics »

Cryptographic Key Length Recommendation

- NSA Suite B(2005), NIST, SM
  AES128, Hash256, ECC 256, RSA 2048

- IAD-NSA CNSA
  Suite (2016)

Cryptographic algorithms	
RSA **3072**-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) **3072**-bit or larger	Key Establishment
ECDH with NIST P-**384**	Key Establishment
ECDSA with NIST P-**384**	Digital Signature
SHA-**384**	Integrity
AES-**256**	Confidentiality

Quantum Resource Estimates for ECDLP

Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin Lauter, **Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms,** ASIACRYPT 2017, Part II, LNCS 10625, pp. 241–270, 2017.

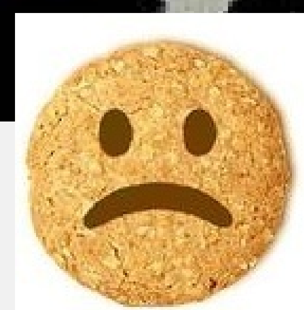
ECDLP in $E(\mathbb{F}_p)$ simulation results					Factoring of RSA modulus N interpolation from [21]		
$\lceil \log_2(p) \rceil$ bits	#Qubits	#Toffoli gates	Toffoli depth	Sim time sec	$\lceil \log_2(N) \rceil$ bits	#Qubits	#Toffoli gates
110	1014	$9.44 \cdot 10^9$	$8.66 \cdot 10^9$	273	512	1026	$6.41 \cdot 10^{10}$
160	1466	$2.97 \cdot 10^{10}$	$2.73 \cdot 10^{10}$	711	1024	2050	$5.81 \cdot 10^{11}$
192	1754	$5.30 \cdot 10^{10}$	$4.86 \cdot 10^{10}$	1 149	–	–	–
224	2042	$8.43 \cdot 10^{10}$	$7.73 \cdot 10^{10}$	1 881	2048	4098	$5.20 \cdot 10^{12}$
256	2330	$1.26 \cdot 10^{11}$	$1.16 \cdot 10^{11}$	3 848	3072	6146	$1.86 \cdot 10^{13}$
384	3484	$4.52 \cdot 10^{11}$	$4.15 \cdot 10^{11}$	17 003	7680	15362	$3.30 \cdot 10^{14}$
521	4719	$1.14 \cdot 10^{12}$	$1.05 \cdot 10^{12}$	42 888	15360	30722	$2.87 \cdot 10^{15}$

Table 2: Resource estimates of Shor's algorithm for computing elliptic curve discrete logarithms in $E(\mathbb{F}_p)$ versus Shor's algorithm for factoring an RSA modulus N.

Next…

一切皆有可能

Anything is possible!!!



Until Quantum computer

Find out efficient solution for ECDLP

Conclusions

- ECC and ECDLP
- State-of-the-art of ECDLP

  a).There is no practical attack on random curve on GF(2^n) (n is prime) and GF(p)!
  b). ECDLP on GF(p) is more secure than that on GF (2^n)!
  c). The current quantum computing is not a threat! But, in the future……
- Possible method for speed up or break ECDLP:

  elementary: too many related aspects
  advanced: ec is too rich

Thanks for your attention!