Improvement of Faugère et al.'s method to solve ECDLP

Yun-Ju, Huang
Graduate School of Mathematics, Kyushu University

Petit, Christophe
UCL Crypto Group

Shinohara, Naoyuki
NICT

Takagi, Tsuyoshi
Institute of Mathematics for Industry, Kyushu University

https://hdl.handle.net/2324/1434304

出版情報：MI lecture note series. 53, pp.145-158, 2013-12-26. 九州大学マス・フォア・インダストリ研究所
バージョン：

Improvement of Faugère *et al.*'s method to solve ECDLP

○ Huang Yun-Ju *
Christophe Petit ⋆
Naoyuki Shinohara †
Tsuyoshi Takagi ‡

*Graduate School of Mathematics, Kyushu University
⋆ UCL Crypto Group
† NICT
‡ Institute of Mathematics for Industry, Kyushu University

August 29, 2013

Abstract

- Target : ECDLP problem.
- Motivation : A new technique for index calculus method algorithm to solve ECDLP proposed by Faugère *et al.* at Eurocrypt 2012.
- Contribution :
  1. Give a new idea to improve the algorithm proposed by Faugère *et al.*
  2. Implements different strategies solving ECDLP and compares them.

Outline

Target - ECDLP

Background

Index Calculus Method with Gröbner Basis

Our Contribution

Elliptic Curve Discrete Log Problem (ECDLP)

Let F_{2^n} is a binary field of prime degree n over F_2.

Let $E_{\alpha,\beta} : y^2 + xy = x^3 + \alpha x^2 + \beta$ over field F_{2^n}, where $\alpha, \beta \in F_{2^n}$.

Given $P \in E_{\alpha,\beta}$, $Q \in \langle P \rangle$,

Target

Find smallest non-negative integer k such that $Q = [k]P$

Known Algorithm

- Exhaustive Search
  Time Complexity : $O(2^n)$
- Pollard-rho Mehod
  Time Complexity : $O(2^{\frac{n}{2}})$
- Index Calculus Method
  Time Complexity : claimed to be sub-exponential
  $O(2^{cn^{2/3}\log n})$ by Petit *et al.* at Asiacrypto 2012.

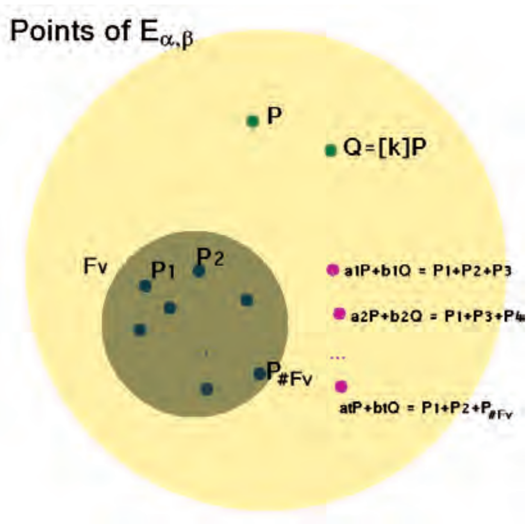
Generic Index Calculus Mehod

Generic Index Calculus Method

Input :	$P, Q \in E_{\alpha,\beta}$
Output :	$k \in N$ such that $Q = [k]P$
phase 1:	Setup factor base $F_V = \{P_i \in E_{\alpha,\beta} \mid x(P_i) \in V\}$
phase 2: Relation Search	Find sufficient relations $sol_m = \{\sum_{1 \le j \le m} P'_j = [a]P + [b]Q\}$ for random $a, b \in N$, $P'_j \in F_V$.
phase 3:	Transform the relation to matrix M.
phase 4:	Find reduced echelon form M_{-} of M.
phase 5:	Solve the relation $[a']P + [b']Q = O$ in M_{-}. $k = \frac{-a'}{b'}$.

$x(P_i)$ means x-coordinate of P_i.

Generic Index Calculus



Generic Index Calculus Method

$$\begin{array}{cccccc} P_1 & P_2 & \dots & P_{\#F_V} & P & Q \end{array}$$

$$\begin{pmatrix} 1 & 1 & & 0 & a_1 & b_1 \\ 1 & 0 & & 0 & a_2 & b_2 \\ \vdots & & \ddots & \vdots & & \vdots \\ 1 & 1 & \dots & 1 & a_t & b_t \end{pmatrix}$$

$\Downarrow$ reduced row echelon form

$$\begin{pmatrix} 1 & 0 & & 0 & & \\ 0 & 1 & & 0 & & \\ \vdots & & \ddots & \vdots & & \\ 0 & 0 & \dots & 1 & & \\ 0 & 0 & & 0 & a' & b' \end{pmatrix}$$

Semaev's Polynomials[1]

Property - Semaev's summation polynomial

For $R = [a]P + [b]Q$**, Semaev's summation polynomials** s_{m+1} are multivariate polynomials where :
$\forall x_1, \ldots, x_m \in F_{2^n}$,

$$s_{m+1}(x_1, x_2, \ldots, x_m, x_r) = 0$$

if and only if $\exists P'_j, 1 \leq j \leq m$ such that

$$\sum_{1 \leq j \leq m} P'_j + R = O,$$

where $x_j = x(P'_j)$, $x_r = x(R)$.

The problem to find P'_j s.t, $\sum P'_j = R$ is now reduced to solve $s_{m+1}(x_1, , x_m, x_r) = 0$. x_j is variable and x_r is known value.

Version by Faugère *et al.* (FPPR)

In Eurocrypt 2012, Faug'ere, Perret, Petit and Renault proposed a new version to solve the Semaev's summation polynomials by Gröbner basis for phase 2 (Relation Search).

Variable Rewritten

We can regard F_{2^n} as the vector space defined by the basis $\{v_0, v_1, \ldots, v_{n'-1}\}$.

Variable Substitution

Let $x_j = x(P_j'), P_j' \in F_v$, if we rewrite $x_j = \sum_{0 \le \ell \le n'-1} c_{j,l} v_\ell$, then

$s_{m+1}(x_1, \ldots, x_m, x_r)$
$= s_{m+1}(\sum_{0 \le \ell \le n'-1} c_{1,\ell} v_\ell, \ldots, \sum_{0 \le \ell \le n'-1} c_{m,\ell} v_\ell, \sum_{0 \le l \le n-1} r_\ell v_\ell)$

where $c_{j,\ell} \in F_2$ is unknown and r_ℓ is known.

Multivariable Polynomial System

Multivariable Polynomial System

$s_{m+1}(\sum_{0 \le \ell \le n'-1} c_{1,\ell} v_\ell, \ldots, \sum_{0 \le l \le n'-1} c_{m,\ell} v_\ell, \sum_{0 \le \ell \le n-1} r_\ell v_\ell)$
$= f_0(c_{j,\ell}) v_1 + f_1(c_{j,\ell}) v_2 + \ldots + f_{n-1}(c_{j,\ell}) v_n$
where $1 \le j \le m, 1 \le \ell \le n'$, $c_{j,\ell} \in F_2$

$s_{m+1} = 0$ over $F_{2^n} \iff f_0 = 0, f_1 = 0, f_{n-1} = 0$ over F_2.

Outline

Target - ECDLP

Background

Index Calculus Method with Gröbner Basis

Our Contribution

Symmetric function

Using the fact that Semaev's summation polynomials are symmetric, substitute the polynomials with elementary symmetric functions.

For example :

$$s_3 = (x_1x_2 + x_1x_r + x_2x_r)^2 + x_1x_2x_r + \beta$$
$$= (\sigma_2 + \sigma_1 x_r)^2 + \sigma_2 x_r + \beta$$

where
$\sigma_1 = x_1 + x_2, \sigma_2 = x_1x_2,\ \beta$ is the parameter of $E_{\alpha,\beta}$.

Rewritten system for symmetric function

- Variables rewritten
  $x_1 = c_{1,0}v_1 + c_{1,1}v_2 + \ldots + c_{1,n'-1}v_{n'}$
  $x_2 = c_{2,0}v_1 + c_{2,1}v_2 + \ldots + c_{2,n'-1}v_{n'}$
  ...
  $x_m = c_{m,0}v_1 + c_{m,1}v_2 + \ldots + c_{m,n'-1}v_{n'}$
- Symmetric function rewritten
  $\sigma_1 = d_{1,0}v_1 + d_{1,1}v_2 + \ldots + d_{1,n-1}v_n$
  $\sigma_2 = d_{2,0}v_1 + d_{2,1}v_2 + \ldots + d_{2,n-1}v_n$
  ...
  $\sigma_m = d_{m,0}v_1 + d_{m,1}v_2 + \ldots + d_{m,n-1}v_n$
- Relation of variables and symmetric function
  $d_{1,0} = f_{1,0}(c_{i,j})$
  $d_{1,1} = f_{1,1}(c_{i,j})$
  ...
  $d_{m,n-1} = f_{m,n-1}(c_{i,j})$

Symmetric function

- Using symmetric function for s_{m+1} is not a new idea. Gaudry, Diem, Joux and Vitse proposed this in composite extension degree.[2, 3, 4, 5]
- However, in prime extension degree makes the number of variables and number of polynomials grows too large. This makes it impracticable.

Special factor base V

Let $F_{2^n} = F_2[\omega]/h(\omega)$, where $h(\omega)$ is an irreducible polynomial of prime degree n over F_2.

Using the special factor base $V = \{1, \omega, ..., \omega^{n'-1}\}$.

Rewritten system for symmetric function

- Variables rewritten
  $x_1 = c_{1,0} + c_{1,1}\omega + ... + c_{1,n'-1}\omega^{n'-1}$
  $x_2 = c_{2,0} + c_{2,1}\omega + ... + c_{2,n'-1}\omega^{n'-1}$
  ...
  $x_m = c_{m,0} + c_{m,1}\omega + ... + c_{m,n'-1}\omega^{n'-1}$
- Symmetric function rewritten
  $\sigma_1 = d_{1,0} + d_{1,1}\omega + ... + d_{1,n'-1}\omega^{n'-1}$
  $\sigma_2 = d_{2,0} + d_{2,1}\omega + ... + d_{2,n'-2}\omega^{2n'-2}$
  ...
  $\sigma_2 = d_{m,0} + d_{m,1}\omega + ... + d_{m,n'-m}\omega^{n-m}$
- Relation of variables and symmetric function
  $d_{1,0} = f_{1,0}(c_{i,j})$
  $d_{1,1} = f_{1,1}(c_{i,j})$
  ...
  $d_{m,n'-m} = f_{m,n'-m}(c_{i,j})$

Symmetric function with specific vector base V

	s_{m+1}	s'_{m+1}	s'_{m+1} with specific V
#var	mn'	$mn' + mn$	$mn' + (n'-1)\frac{m(m+1)}{2} + m$
#poly	n	$n + mn$	$n + (n'-1)\frac{m(m+1)}{2} + m$
$\deg_{reg}$	7 or 6	4 or 3	4 or 3

Table: Comparison for different multivariate polynomial system

The time and memory costs are respectively roughly $\#var^{2*deg_{reg}}$ and $\#var^{3*deg_{reg}}$.

Experimental Results

CPU : AMD Opteron 6276*4, 16 cores, 2.3GHz, L3 cache 16MB
OS : CentOS 6.3
RAM : 512 GB
Platform : Magma V2.18-9 64-bit version

Experimental Results

Using Magma to finding one relation $\sum P_i = [a]P + [b]Q$.

	n	n'	sol: yes						
			D_{reg}	var	poly	mono	t_{trans}	t_{groe}	mem
Imp_{FPPR}	23	3	6	9	23	2792.97	5.47	1.06	29.10
Imp_{Ours}	23	3	3	24	38	1079.60	0.91	1.04	15.59
Imp_{FPPR}	53	3	6	9	53	6358.94	12.86	1.03	72.06
Imp_{Ours}	53	3	3	24	68	2348.50	2.12	0.79	24.89
Imp_{FPPR}	23	4	6	12	23	12059.19	21.06	6.83	95.66
Imp_{Ours}	23	4	3	33	44	2173.29	1.83	3.19	29.63
Imp_{FPPR}	53	4	6	12	53	27655.34	50.63	1.86	272.55
Imp_{Ours}	53	4	3	33	74	4701.09	4.19	1.75	40.46

Table: Comparison of the relation search ($m = 3$, $n' = 3, 4$) with two strategies, Imp_{FPPR} and Imp_{Ours}. Units are sec and MB

Target - ECDLP Background Index Calculus Method with Gröbner Basis Our Contribution

Experimental Results

Using Magma to finding one relation $\sum P_i = [a]P + [b]Q$.

	n	n'	sol: yes						
			D_{reg}	var	poly	mono	t_{trans}	t_{groe}	mem
Imp_{FPPR}	23	5	7	15	23	40168.90	64.67	70.46	475.55
Imp_{Ours}	23	5	4	42	50	3572.00	3.01	157.86	323.60
Imp_{FPPR}	53	5	6	15	53	91642.50	147.66	80.76	810.08
Imp_{Ours}	53	5	3	42	80	8034.10	6.83	6.68	59.58
Imp_{FPPR}	23	6	7	18	23	107008.67	163.45	3888.70	6656.13
Imp_{Ours}	23	6	4	51	56	5270.00	4.36	5150.12	4791.31
Imp_{FPPR}	53	6	7	18	53	245891.33	366.92	2967.03	7311.44
Imp_{Ours}	53	6	3	51	86	11748.00	10.48	34.82	151.04

Table: Comparison of the relation search ($m = 3$, $n' = 4, 5$) with two strategies, Imp_{FPPR} and Imp_{Ours}. Units are sec and MB

Experimental Results

Using Magma to solve ECDLP.

n	$\#E_{\alpha,\beta}$	Imp_{FPPR}	Imp_{Ours}
7	4*37	1.574	0.864
11	4*523	8.625	6.702
13	4*2089	49.698	31.058
17	4*32941	2454.470	1364.742
19	4*131431	22474.450	9962.861

Table: Comparison of two ECDLP strategies, Imp_{FPPR} and Imp_{Ours}. The last two columns are computing time in seconds.

Conlusion

- This work has been accepted by IWSEC2013.
- We give the experimental evidence of our improvements.
- Future work - parallization.

Thanks

Q & A

Reference I

- I. Semaev, "Summation polynomials and the discrete logarithm problem on elliptic curves," *IACR Cryptology ePrint Archive*, vol. 2004, p. 31, 2004.
- C. Diem, "An index calculus algorithm for plane curves of small degree," in Hess *et al.* [14], pp. 543–557.
- P. Gaudry, "Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1690 – 1702, 2009.
- C. Diem, "On the discrete logarithm problem in elliptic curves," *Compositio Mathematica*, vol. 147, pp. 75–104, 2011.
- A. Joux and V. Vitse, "Elliptic curve discrete logarithm problem over small degree extension fields," *Journal of Cryptology*, pp. 1–25, 2011.
- C. Petit and J.-J. Quisquater, "On polynomial systems arising from a weil descent," in *Advances in Cryptology ASIACRYPT 2012* (X. Wang and K. Sako, eds.), vol. 7658 of *Lecture Notes in Computer Science*, pp. 451–466, Springer Berlin Heidelberg, 2012.
- D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.
- I. Blake, G. Seroussi, N. Smart, and J. W. S. Cassels, *Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)*. New York, NY, USA: Cambridge University Press, 2005.
- T. Saito, S. Yokoyama, T. Kobayashi, and G. Yamamoto, "Some relations between semaev's summation polynomials and stange's elliptic nets," *Journal of Math-for-Industry*, vol. 3 (2011A-9), pp. 89–92, 2011.

Reference II

R. P. Brent, "An improved monte carlo factorization algorithm," *BIT Numerical Mathematics*, vol. 20, pp. 176–184, 1980.

J. M. Pollard, "A monte carlo method for factorization," *BIT Numerical Mathematics*, vol. 15 (3), pp. 331–334, 1975.

J.-C. Faugre, L. Perret, C. Petit, and G. Renault, "Improving the complexity of index calculus algorithms in elliptic curves over binary field," in *Proceedings of Eurocrypt 2012*, vol. 7237 of *Lecture Notes in Computer Science*, pp. 27–44, Springer Verlag, 2012.

J. H. Silverman, "The xedni calculus and the elliptic curve discrete logarithm problem," *Designs, Codes and Cryptography*, vol. 20, pp. 5–40, 1999.

F. Hess, S. Pauli, and M. E. Pohst, eds., *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, vol. 4076 of *Lecture Notes in Computer Science*, Springer, 2006.

J.-C. Faugère, "A new efficient algorithm for computing gröbner bases (f_4)," *Journal of Pure and Applied Algebra*, vol. 139, no. 1-3, pp. 61–88, 1999.

J. C. Faugère, "A new efficient algorithm for computing gröbner bases without reduction to zero (f_5)," in *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, (New York, NY, USA), pp. 75–83, ACM, 2002.

J. Faugère, P. Gianni, D. Lazard, and T. Mora, "Efficient computation of zero-dimensional gröbner bases by change of ordering," *Journal of Symbolic Computation*, vol. 16, no. 4, pp. 329 – 344, 1993.

Reference III

J. M. Pollard, "Kangaroos, monopoly and discrete logarithms," *Journal of Cryptology*, vol. 13, pp. 437–447, 2000.

D. Shanks, "Class number, a theory of factorization, and genera," in *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pp. 415–440, 1971.

D. Bernstein, H.-C. Chen, C.-M. Cheng, T. Lange, R. Niederhagen, P. Schwabe, and B.-Y. Yang, "Ecc2k-130 on nvidia gpus," in *Progress in Cryptology - INDOCRYPT 2010* (G. Gong and K. Gupta, eds.), vol. 6498 of *Lecture Notes in Computer Science*, pp. 328–346, Springer Berlin Heidelberg, 2010.

L. Judge, S. Mane, and P. Schaumont, "A hardware-accelerated ecdlp with high-performance modular multiplication," *International Journal of Reconfigurable Computing*, vol. 2012, 2012.