LETTER

Using C_{ab} Curves in the Function Field Sieve

Ryutaroh MATSUMOTO[†], ***Member***

SUMMARY In Adleman's Function Field Sieve algorithm solving the discrete logarithm problem in a finite field, it is assumed that a random bivariate polynomial in the certain class is absolutely irreducible with high probability. In this letter we point out that if we use C_{ab} type random polynomials then we always get absolutely irreducible polynomials. We can also simplify the calculation of a product of many rational functions on a curve that belongs to the field of definition by the use of a C_{ab} curve.

key words: *discrete logarithm problem, function field sieve, C_{ab} curve*

Adleman proposed the Function Field Sieve (FFS) algorithm [1] solving the discrete logarithm problem in the multiplicative group of a finite field $\mathbb{F}_{p^n}$ with p^n elements for a prime p relatively small to the extension degree n. Suppose that $\mathbb{F}_{p^n}$ is defined by a irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n. In the FFS we first choose a random polynomial $m(x) \in \mathbb{F}_p[x]$ of certain degree, then find a bivariate polynomial $H(x,y) = \sum_{i=0}^{d} \sum_{j=0}^{d'-1} h_{i,j} y^i x^j \in \mathbb{F}_p[x,y]$ satisfying the following 8 conditions:

1. H is absolutely irreducible.
2. $H(x,m)$ is divisible by f.
3. $h_{d,d'-1} = 1$.
4. $\sum_{i=0}^{d} h_{i,d'-1} y^i \in \mathbb{F}_p[y]$ is square-free.
5. $h_{0,d'-1} \neq 0$.
6. $\sum_{j=0}^{d'-1} h_{d,j} x^j \in \mathbb{F}_p[x]$ is square-free.
7. $h_{d,0} \neq 0$.
8. The order of the Jacobian of the curve defined by $H(x,y)$ is relatively prime to $(p^n-1)/(p-1)$.

In the running time analysis Adleman assumed that we can find an absolutely irreducible polynomial satisfying the conditions above with sufficiently high probability, and the assumption was not verified rigorously. That assumption is easily satisfied if we use a C_{ab} curve.

Proposition-Definition 1: [2, Proposition 12] [3], [4] Let K be a perfect field, $\bar{K}$ the algebraic closure of K, $\chi \subset \bar{K}^2$ be a possibly reducible affine algebraic set defined over K, x, y be the coordinates of the affine space, and a, b relatively prime positive integers. Then the following conditions are equivalent.

- χ is an absolutely irreducible affine algebraic curve with exactly one K-rational place Q at infinity, and the pole divisors of x and y are aQ and bQ respectively.
- χ is defined by a bivariate polynomial of form

$$G(x,y) := \alpha_{b,0} x^b + \alpha_{0,a} y^a + \sum_{ia+jb<ab} \alpha_{i,j} x^i y^j, \tag{1}$$

  where $\alpha_{i,j} \in K$ for all i, j and $\alpha_{b,0}, \alpha_{0,a}$ are nonzero.

A plane algebraic curve defined by a bivariate polynomial of form (1) is said to be a C_{ab} *curve*.

A K-basis of the affine coordinate ring $K[x,y]/(G(x,y))$ of a C_{ab} curve is

$$\{x^i y^j \mid 0 \leq i, 0 \leq j \leq a-1\},$$

and elements in the basis have pairwise distinct discrete valuations at Q.

Any algebraic curve defined over a perfect field K that has at least one K-rational place is birationally equivalent to a C_{ab} curve defined over K. □

If we use a polynomial of form (1) in the FFS then the absolute irreducibility condition is always satisfied. An algebraic curve used in the FFS is assumed to have at least one $\mathbb{F}_p$-rational place, and using C_{ab} curves in the FFS does not narrow the class of curves used in the FFS.

Proposition 2: Let z be a nonzero rational function on an absolutely irreducible algebraic curve defined over a perfect field K and Q a place in the curve. Then $z \in K$ iff $v_P(z) = 0$ for all place $P \neq Q$ in the curve, where $v_P(z)$ denotes the discrete valuation of z at a place P.

Proof: The assertion follows from [6, Corollary 1.1.19, Theorem 1.4.11 and Corollary 3.6.7]. □

In the FFS we deal with an absolutely irreducible curve defined over the field $\mathbb{F}_p$ and we have to find a product of many rational functions belonging to $\mathbb{F}_p$. To find such a product in Adleman's original method, we compute the discrete valuation of each rational function at all place, including places at infinity, then solve the system of linear equations. If we use a C_{ab} curve then we do not have to calculate the discrete valuation at

Manuscript received September 30, 1998.

[†]The author is in the Sakaniwa Lab., the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo, 152–8552 Japan. E-mail: ryutaroh@ss.titech.ac.jp

infinity, because a C_{ab} curve has exactly one place at infinity, and we can remove the conditions 3, 4, and 6 that simplify calculation of the discrete valuations at infinity. Note that we can easily calculate the discrete valuation of a rational functions on a C_{ab} curve at the place at infinity by the division algorithm of a Gröbner basis [5, Proposition 14], [4, Appendix C].

To find a polynomial $H(x, y)$ of form (1) satisfying the condition 2, let

$$H(x,y) := \alpha_{b,0}x^b + \alpha_{0,a}y^a + \sum_{ia+jb<ab} \alpha_{i,j}x^i y^j,$$

and $g(x) := H(x, m(x)) \bmod f(x)$. $g(x) = 0$ gives the system of n linear equations in variables $\alpha_{i,j}$. Substituting $\alpha_{i,j}$ in $H(x, y)$ with a solution gives a desired polynomial.

References

[1] L.M. Adleman, "The function field sieve," Proc. Algorithmic Number Theory Symposium, Lect. Notes in Comp. Sci., vol.877, pp.108–121. Springer-Verlag, 1995.
[2] T. Høholdt, J.H. van Lint, and R. Pellikaan, "Order functions and evaluation codes," Proc. AAECC-12, Lect. Notes in Comp. Sci., vol.1255, pp.138–150, 1997.
[3] S. Miura, "Algebraic geometric codes on certain plane curves," IEICE Trans., vol.J75-A, no.11, pp.1735–1745, Nov. 1992.
[4] S. Miura, "Linear codes on affine algebraic curves," IEICE Trans., vol.J81-A, no.10, pp.1398–1421, Oct. 1998.
[5] K. Saints and C. Heegard, "Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using gröbner bases," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1733–1751, Nov. 1995.
[6] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin, 1993.