JSIAM Letters Vol.6 (2014) pp.5–7 ©2014 Japan Society for Industrial and Applied Mathematics

The elliptic curve Diffie-Hellman problem and an equivalent hard problem for elliptic divisibility sequences

Junichi Yarimizu[1], Yukihiro Uchida[1] and Shigenori Uchiyama[1]

[1] Tokyo Metropolitan University, Tokyo 192-0397, Japan

E-mail *yarimizu-junichi@ed.tmu.ac.jp*

Received September 5, 2013, Accepted October 14, 2013

Abstract

In 1948, Ward defined elliptic divisibility sequences satisfying a certain recurrence relation. An elliptic divisibility sequence arises from any choice of elliptic curve and initial point on that curve. In this paper, we define a hard problem in the theory of elliptic divisibility sequences (*EDS-DH problem*), which is computationally equivalent to the elliptic curve Diffie-Hellman problem.

Keywords elliptic curve, elliptic divisibility sequence, elliptic curve Diffie-Hellman problem

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

In 1948, Ward defined the concept of an elliptic divisibility sequence (EDS for short) [1]. This is a sequence of integers, satisfying a certain divisibility property and a non-linear recurrence relation, which is related to a division polynomial. In 2008, Lauter and Stange defined some hard problems in the theory of EDSs, each of which is computationally equivalent to the elliptic curve discrete logarithm problem (ECDLP) [2]. But, they did not consider the elliptic curve Diffie-Hellman problem (ECDHP). In this paper, we define a hard problem (EDS-DH problem) for EDSs, which is computationally equivalent to the ECDHP. In Section 2, we begin with an introduction to EDSs and how to calculate general terms of EDSs. In Section 3, we introduce the ECDHP, and we define EDS-DH problem. In Section 4, we explain the equivalence of ECDHP and EDS-DH problem. Our conclusion is presented in Section 5.

2. Elliptic divisibility sequences

In this section, we briefly review EDSs according to [2]. See [1–3] for the detail.

2.1 Elliptic divisibility sequences

Let us begin the definition of an EDS.

Definition 1 ([2]) *An EDS $(W(n))$ is a sequence in a field K satisfying: $W(m+n)W(m-n) = W(m+1)W(m-1)W(n)^2 - W(n+1)W(n-1)W(m)^2$ $({}^\forall m, n \in \mathbf{Z})$.*

EDSs satisfy a relation which division polynomials of elliptic curves have. We now need two following theorems.

Theorem 2 ([4]) *If $((W(n))$ is a non-trivial EDS, then $W(0) = 0_K$, $W(1) = \pm 1_K$, and $W(-n) = -W(n)$ $({}^\forall n \in \mathbf{Z})$.*

This theorem means that we only need to consider positive subscript terms of EDS with $W(1) = 1_K$, where 1_K denotes the unit element for multiplication and 0_K denotes the unit element for addition in the field K; we assume this throughout this paper.

Theorem 3 ([4]) *If the initial five terms $W(0)$, $W(1)$, $W(2)$, $W(3)$, $W(4)$ of an EDS $(W(n))$ are known, then the whole sequence is well defined.*

Since we always have $W(0) = 0_K, W(1) = 1_K$, this is equivalent to knowing the three terms $W(2)$, $W(3)$, $W(4)$.

2.2 Calculating a general term

It is then important to know how to calculate a general term of an EDS defined by the three terms $W(2), W(3), W(4)$. For this purpose, we use the recurrence relations below.

Definition 4 *By Definition 1, we have the recurrence relations for all $k \in \mathbf{Z}$:*

- $W(2k+1)W(1) = W(k+2)W(k)^3 - W(k-1)W(k+1)^3$.
- $W(2k)W(2) = W(k)(W(k+2)W(k-1)^2 - W(k-2)W(k+1)^2)$.

These formulae are called the doubling formulae.

Let Ψ_n denote the n-th division polynomial of an elliptic curve E over a field K. The sequence $W_{E,P} : \mathbf{Z} \to K$ of the form $W_{E,P}(n) = \Psi_n(P)$ for some fixed point $P \in E(K)$ is an elliptic divisibility sequence. Ward showed that almost all elliptic divisibility sequences arise in this way for the case $K = \mathbf{Q}$. This relationship is the basis of our work here.

In this paper, we assume naive arithmetic in $\mathbf{F}_q$, namely, we bound the time to do basic $\mathbf{F}_q$ operations by $O((\log q)^2)$ for simplicity.

Theorem 5 ([4, Theorem 3.4.1]) *Let E be an elliptic curve over $K = \mathbf{F}_q$, and $P \in E(K)$ a point of order not less than 4. Given a value t, the term $W_{E,P}(t)$ in the elliptic divisibility sequence associated to E, P can be calculated in $O((\log t)(\log q)^2)$ time.*

3. ECDHP and EDS-DH problem

In this section, we introduce the ECDHP and define the EDS-DH problem.

Problem 6 *Let E be an elliptic curve over a finite field K. Suppose there are points $P, [a]P, [b]P \in E(K)$ $(a, b \in \mathbf{Z})$. Determine $[ab]P \in E(K)$.*

This problem is called the elliptic curve Diffie-Hellman problem (ECDHP). In order to define the EDS-DH problem, we need the following theorem.

Theorem 7 ([2]) *Let K be a finite field of q elements, and E an elliptic curve defined over K. For all points $P \in E(K)$ of order relatively prime to $q-1$ and greater than 3, define:*

$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))}\right)^{\frac{1}{\mathrm{ord}(P)^2}}.$$

For a point P of order relatively prime to $q-1$ and greater than 3, the sequence $\phi([n]P)$ is an EDS. Specifically:

$$\phi([n]P) = \phi(P)^{n^2} W_{E,P}(n) \quad ({}^{\forall}n \in \mathbf{Z}).$$

In light of this theorem we will use the following convenient notation:

$$\widetilde{W}_{E,P}(n) = \frac{\phi([n]P)}{\phi(P)}.$$

$\widetilde{W}_{E,P}(n)$ can be calculated *as a function of the point $[n]P$ on the curve* without knowledge of n.

Problem 8 *Let K be a finite field of q elements, and E an elliptic curve defined over K. Let $P \in E(K)$ be a point of order relatively prime to $q-1$ and greater than 3. Suppose there are points $P, [a]P, [b]P \in E(K)$ $(a, b \in \mathbf{Z})$. Determine $\widetilde{W}_{E,P}(ab) \in K$.*

We call this problem the EDS-DH problem.

4. Equivalence of two hard problems

In this section, we prove the following theorem.

Theorem 9 *Let E be an elliptic curve over a finite field $K = \mathbf{F}_q$ of characteristic $\neq 2$. For all points $P \in E(K)$ of order relatively prime to $q-1$ and greater than 3, the ECDHP is computationally equivalent to the EDS-DH problem.*

Proof ECDHP $\Longrightarrow$ EDS-DH problem:

For simplicity and cryptographical view point, we only consider the case the order of P is prime. Setting $n = ab$ in the equation of Theorem 7, we obtain an expression:

$$\widetilde{W}_{E,P}(ab) = \frac{1}{\phi(P)}\left(\frac{W_{E,[ab]P}(q-1)}{W_{E,[ab]P}(q-1+\mathrm{ord}([ab]P))}\right)^{\frac{1}{\mathrm{ord}([ab]P)^2}}.$$

Using Theorem 5 to calculate the ratio of terms inside the parentheses takes $\log(q-1+\mathrm{ord}([ab]P)) + \log(q-1)$ steps. Since $\mathrm{ord}([ab]P)$ is on the order of q, this is $O((\log q)^3)$ time at worst. The other necessary operation is to find the inverse of $\mathrm{ord}([ab]P)^2$ modulo $q-1$, and to raise to that exponent. Both these are also $O(\log q)$ finite field operations.

EDS-DH problem $\Longrightarrow$ ECDHP:

See [2, Lemma 1] for the following identity:

$$\frac{W_{E,P}(n-1)W_{E,P}(n+1)}{W_{E,P}(n)^2} = x(P) - x([n]P).$$

Set $n = ab$ in this equation, and apply Theorem 7:

$$\frac{\widetilde{W}_{E,P}(ab-1)\widetilde{W}_{E,P}(ab+1)}{\widetilde{W}_{E,P}(ab)^2} = \phi(P)^2(x(P) - x([ab]P)).$$

The term $\widetilde{W}_{E,P}(ab)$ can be calculated from the assumption that the EDS-DH problem is solvable. With knowledge of the product $\widetilde{W}_{E,P}(ab-1)\widetilde{W}_{E,P}(ab+1)$, the x-coordinate of $[ab]P$, $x([ab]P)$, can be calculated without requiring knowledge of $[ab]P$.

The sequence $\widetilde{W}_{E,P}$ satisfies the recurrence instance: $\widetilde{W}_{E,P}(i+j)\widetilde{W}_{E,P}(i-j) = \widetilde{W}_{E,P}(i+1)\widetilde{W}_{E,P}(i-1)\widetilde{W}_{E,P}(j)^2 - \widetilde{W}_{E,P}(j+1)\widetilde{W}_{E,P}(j-1)\widetilde{W}_{E,P}(i)^2$ $({}^{\forall}i, j \in \mathbf{Z})$.

Setting $i = ab$ and $j = a$ in this equation gives: $\widetilde{W}_{E,P}(a(b+1))\widetilde{W}_{E,P}(a(b-1)) = \widetilde{W}_{E,P}(ab+1)\widetilde{W}_{E,P}(ab-1)\widetilde{W}_{E,P}(a)^2 - \widetilde{W}_{E,P}(a+1)\widetilde{W}_{E,P}(a-1)\widetilde{W}_{E,P}(ab)^2$.

All of these terms can be calculated by applying the assumption that the EDS-DH problem is solvable except for $\widetilde{W}_{E,P}(ab+1)\widetilde{W}_{E,P}(ab-1)$. However, compare these terms with the recurrence relation to determine this unknown term. Also determine $x([ab]P)$ in this manner. We can calculate the corresponding possible values for y in probabilistic time $O((\log q)^4)$ [2, Theorem 9]. To determine which of the two points with this x-coordinate is actually $[ab]P$, first take one of the two candidate points, and proceed on the assumption that it is $[ab]P$. Using EDS-DH problem oracle, calculate $\widetilde{W}_{E,P}(ab)$ from the three points $P, [a]P$, and $[b]P$. Also calculate $\widetilde{W}_{E,P}(ab)$ from P and $[ab]P$ by Theorem 7. Then, if the two values are equal, our assumption about the point we chose is correct. If the two values are not equal, then the point we chose was incorrect, and the other one is the point $[ab]P$ we seek.

(QED)

5. Conclusion

We defined a hard problem in the theory of EDSs (*EDS-DH problem*), which is computationally equivalent to the ECDHP. A future work is to propose some cryptographic schemes based on our proposed hard problem.

Acknowledgments

The authors would like to thank the anonymous reviewer for his/her valuable comments. This work was supported in part by Grant-in-Aid for Scientific Research (C)(20540135).

References

[1] M. Ward, Memoir on elliptic divisibility sequences, Amer. J. Math., **70** (1948), 31–74.

[2] K. E. Lauter and K. E. Stange, The elliptic curve discrete

logarithm problem and equivalent hard problems for elliptic divisibility sequences, in: Proc. of SAC 2008, LNCS-5381, pp. 309–327, Springer-Verlag, Berlin, 2009.

[3] N. Sakurada, J. Yarimizu, N. Ogura and S. Uchiyama, An integer factoring algorithm based on elliptic divisibility sequences, JSIAM Letters, **4** (2012), 21–23.

[4] R. Shipsey, Elliptic divisibility sequences, Ph.D. thesis, The Univ. of London, London, 2000.