

Pairing-Friendly Curves with Minimal Security Loss by Cheon's Algorithm

Cheol-Min Park and Hyang-Sook Lee

In ICISC 2007, Comuta and others showed that among the methods for constructing pairing-friendly curves, those using cyclotomic polynomials, that is, the Brezing-Weng method and the Freeman-Scott-Teske method, are affected by Cheon's algorithm. This paper proposes a method for searching parameters of pairing-friendly elliptic curves that induces minimal security loss by Cheon's algorithm. We also provide a sample set of parameters of BN-curves, FST-curves, and KSS-curves for pairing-based cryptography.

Keywords: Cheon's algorithm, cyclotomic polynomial, pairing-friendly elliptic curve.

I. Introduction

The security of many public key cryptosystems relies on the computational hardness of the discrete logarithm problem and the Diffie-Hellman problem. Cheon [1] proposed a new efficient algorithm for computing the discrete logarithm of the l -strong Diffie-Hellman problem. Let g be a generator of a group G of the prime order p and let $\alpha \in \mathbb{Z}_p^*$. If g, g^α , and g^{α^d} are given for a divisor d of $p-1$, then the secret key α can be computed in $O(\sqrt{p/d} + \sqrt{d})$ exponentiations by Cheon's algorithm. Cheon also proposed a method for computing α from g^{α^i} ($i=0,1,\dots,2d$) for a divisor d of $p+1$ in $O(\sqrt{p/d} + d)$ exponentiations. Therefore, if $p-1$ or $p+1$ has a divisor d less than 2^L and g^{α^i} are given for $i=0,1,\dots,2d$, Cheon's algorithm results in an additional $L/2$ -bit security loss in comparison with

other methods in solving the discrete logarithm problems such as the square root attack. Refer to [1] for details of Cheon's algorithm.

When $p \pm 1 = (\text{positive integer} \leq 2^{c_{\pm}}) \cdot \prod(\text{prime} > l)$ (plus-minus sign in same order), we define a security loss L in G with respect to the l -strong Diffie-Hellman problem by Cheon's algorithm as

$$L = \lceil \max\{c_-, c_+\}/2 \rceil.$$

In [2], Sun investigated Miyaji-Nakabayashi-Takano (MNT) [3] and generalized MNT curves [4] and identified some parameters with small security loss by Cheon's algorithm. In ICISC 2007, Comuta and others showed that among the methods for constructing pairing-friendly elliptic curves, those using cyclotomic polynomials, such as the Brezing-Weng method [5], cause heavy security loss because $r(x) \pm 1$ is reducible where $r(x)$ is an irreducible polynomial defining the prime order of the subgroup [6]. For example, $\Phi_k(x) - 1$ always has a factor of x , where $\Phi_k(x)$ is the k -th cyclotomic polynomial and φ is the Euler phi function. Hence, $\Phi_k(x_i) \pm 1$ has a factor less than $2^{160/\varphi(k)}$, at least for the 160-bit prime $\Phi_k(x_i)$. In the case of a Freeman curve [7], $r(x)$ is given by $25x^4 + 25x^3 + 15x^2 + 5x + 1$ and $r(x) \pm 1$ are factorized as

$$\begin{aligned} r(x) - 1 &= 5x(5x^3 + 5x^2 + 3x + 1), \\ r(x) + 1 &= (5x^2 + 1)(5x^2 + 5x + 2). \end{aligned}$$

Therefore, even if we choose any integer x_i for the 160-bit prime $r(x_i)$, then $r(x_i) - 1$ and $r(x_i) + 1$ have factors less than 2^{40} and 2^{80} , respectively. This implies that a subgroup of a Freeman curve with prime order $r(x_i)$ has at least 20-bit security loss with respect to 2^{40} -strong Diffie-Hellman problem by Cheon's algorithm.

In this regard, we propose a method for searching parameters of pairing-friendly elliptic curves that induces little security loss by Cheon's algorithm. We also provide parameters to induce

Manuscript received Sept. 8, 2010; revised Nov. 10, 2010; accepted Dec. 9, 2010.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MEST) (No. 2009-0000402).

Cheol-Min Park (phon: +82 42 717 5747, email: mpcm@nims.re.kr) was with the Institute of Mathematical Sciences, Ewha Womans University, Seoul, Rep. of Korea, and is now with the National Institute for Mathematical Sciences, Daejeon, Rep. of Korea.

Hyang-Sook Lee (email: hsl@ewha.ac.kr) is with the Department of Mathematics, Ewha Womans University, Seoul, Rep. of Korea.

doi:10.4218/etrij.11.0210.0338

security loss in some elliptic curves E with a small embedding degree k which is minimal in the following sense. Let G_i be a prime order subgroup of E defined over a finite field F_{p_i} and r_i be a prime order of G_i . Let L_{ij} be a security loss in G_i with respect to the j -strong Diffie-Hellman problem by Cheon's algorithm. Then, the minimal security loss is defined by a minimum of $\{L_{ij} \mid r_i > 2^{2w}, j = 2^w\}$, where w is a security level such as $w=80, 128, 192$. Note that if G has minimal security loss L , then security loss L in G remains unchanged for any l -strong Diffie-Hellman problem with $2^{2l} \leq l \leq 2^w$. If G also has a prime order r which is close to 2^{2w} , r has the following form:

$$r \pm 1 = (\text{positive integer} \leq 2^{2l}) \cdot (\text{prime} \geq 2^{2w}).$$

Therefore, we will find parameters of elliptic curves having prime order of this form.

II. Main Algorithm

We call an elliptic curve with a small embedding degree and a large prime-order subgroup a pairing-friendly curve. We consider families of pairing-friendly curves for which the curve parameters r and q are given as polynomials $r(x)$ and $q(x)$, where r is a large prime divisor of the order of elliptic curve group and q is a size of finite field. In most algorithms for constructing pairing-friendly curves, such as the Brezing-Weng method, $r(x)$ and $q(x)$ are taken as irreducible polynomial, and the prime numbers $r(x_i)$ and $q(x_i)$ are selected for some integer x_i . However, the observation of Comuta and others indicates that the choice of $r(x)$ can result in heavy security loss by Cheon's algorithm. Our proposed method overcomes this problem by using a large prime factor of $r(x_i)$ for some integer x_i . Because the irreducibility of $r(x)$ does not imply that $r(x_i)$ is a prime number for any integer x_i , we can find x_i so that $r(x_i)$ is a composite number and the largest prime factor of $r(x_i)$ results in minimal security loss. Furthermore, we have the following theorem.

Theorem 1. Consider a family of pairing-friendly curves $q(x)$, $r(x)$, and $t(x)$ with the embedding degree k and the CM-discriminant D from definition 2.6 in [8]. If $q(x_0)$ is a prime and $t(x_0)$ is an integer for some integer x_0 , then we can construct an elliptic curve $E/F_{q(x_0)}$ having a subgroup of prime order $\tilde{r}(x_0)$ and the embedding degree k by using the CM-discriminant D , where $\tilde{r}(x_0)$ is the largest prime factor of $r(x_0)$.

Proof. Because $q(x)$, $r(x)$, and $t(x)$ satisfy the condition of embedding degree k , proposition 2.4 in [8] implies that $E/F_{q(x_0)}$ has embedding degree k with respect to $\tilde{r}(x_0)$. Since $r(x)$ is a factor of $q(x)+1-t(x)$, $\tilde{r}(x_0)$ is a factor of $q(x_0)+1-t(x_0)$ and E has a subgroup of prime order $\tilde{r}(x_0)$. Since the choice of $\tilde{r}(x_0)$ does not affect $q(x)$ and $t(x)$, CM-discriminant D remains unchanged. \square

When a composite number $r(x_i)$ is selected, it needs to be a

small cofactor times a prime. Let $\tilde{\rho}$ be the ratio of the bit length between $q(x_0)$ and $\tilde{r}(x_0)$, and let ρ be the ratio of the degree between $q(x)$ and $r(x)$. If $r(x_0) = c\tilde{r}(x_0)$ where $\tilde{r}(x_0)$ is a large prime and c is an integer less than 2^α , then we have the following relation between ρ and $\tilde{\rho}$:

$$\begin{aligned} \tilde{\rho} &= \log_2 q(x_0) / (\log_2 \tilde{r}(x_0)) \leq \log_2 q(x_0) / (\log_2 r(x_0) - \alpha) \\ &= \lceil \log_2 q(x_0) / \log_2 r(x_0) \rceil \lceil \log_2 r(x_0) / (\log_2 r(x_0) - \alpha) \rceil \\ &\approx \lceil \deg q(x) / \deg r(x) \rceil \lceil 1 + \alpha / (\log_2 r(x_0) - \alpha) \rceil \\ &\leq \rho \lceil 1 + \alpha / (\log_2 r(x_0) - \alpha) \rceil. \end{aligned}$$

Given a family of pairing-friendly curve $(q(x), r(x), t(x))$, the following algorithm will output parameters with security loss $C/2$ and $\tilde{\rho}$ which is less than or equal to $\rho \lceil 1 + \alpha / (\log_2 r(x_0) - \alpha) \rceil$.

Algorithm 1: Searching for parameters of pairing-friendly curves.

Input: $q(x)$, $r(x)$, $t(x)$, C , α

Output: prime numbers $q(x_0)$, $\tilde{r}(x_0)$.

- (i) Find an integer x_0 so that $q(x_0)$ is a prime, $t(x_0)$ is an integer, and $r(x_0)$ is a large prime times a cofactor less than 2^α .
- (ii) For the largest prime factor $\tilde{r}(x_0)$ of $r(x_0)$, factorize $\tilde{r}(x_0) \pm 1$.
- (iii) For the largest prime factor d_\pm of $\tilde{r}(x_0) \pm 1$, if $(\tilde{r}(x_0) \pm 1) / d_\pm$ is greater than 2^C , then return to step 1.
- (iv) Output $q(x_0)$, $\tilde{r}(x_0)$.

In algorithm 1, finding $r(x_0)$ and factorizing $\tilde{r}(x_0) \pm 1$ require $r(x_0)$ and $\tilde{r}(x_0) \pm 1$ to have only small factors less than 2^α and 2^C , respectively. If we use the elliptic curve factorization method [9], the complexity of this process will be $O(L_{1/2, \sqrt{2}}(2^\alpha)M(\log r(x_0)))$ and $O(L_{1/2, \sqrt{2}}(2^C)M(\log \tilde{r}(x_0) \pm 1))$, where $M(\log x)$ is the complexity of multiplication mod x and $L_{m,n}(p)$ is $\exp(n(\log p)^m(\log \log p)^{1-m})$. In step (i), the primality test of $q(x_0)$ has a running time of $O(\log q(x_0)^{4+\epsilon})$ for $0 < \epsilon < 1$ by using the elliptic curve primality proving method [10]. Therefore, the total complexity of algorithm 1 is $O(\log q(x_0)^{4+\epsilon}) + O(L_{1/2, \sqrt{2}}(2^\alpha)M(\log r(x_0))) + O(L_{1/2, \sqrt{2}}(2^C)M(\log \tilde{r}(x_0) \pm 1))$.

In algorithm 1, we need to find an integer x_0 satisfying the condition. There are two approaches to this problem. One is the exhaustive search for x_0 , and another is the random selection of x_0 . We assume $r(x_0)$ is in $[2^{(2w+\alpha-1)}, 2^{(2w+\alpha+10)}]$ for w -bit security level because $r(x_0)$ must have a factor less than 2^α and a prime factor greater than 2^{2w} in algorithm 1. Then the number of integer x_0 for exhaustive search is about $2^{(2w+\alpha+10)/\deg(r)}$. By the prime number theorem or argument in [1], the probability that p , $(p-1)/2^C$, and $(p+1)/2^C$ are prime for small C is approximately $O(1/\log^3 p)$ if we assume three conditions are independent. Thus, the probability that integer x_0 satisfies the condition of algorithm 1 is less than $O(1/\log^3 \tilde{r}(x_0))$ if we assume all conditions in algorithm 1 are independent. Because $\tilde{r}(x_0)$ is greater than 2^{2w} , the expected number of x_0 for random search is about less than $2^{(2w+\alpha+10)/\deg(r)} / (2w)^3$. We summarize the

Table 1. Expected number of x_0 in algorithm 1.

$\alpha=15$	# for exhaustive search	# for random search
$w=80, \deg(r)=4$	2^{46}	2^{22}
$w=128, \deg(r)=6$	2^{46}	2^{23}
$w=192, \deg(r)=8$	2^{51}	2^{27}

Table 2. Pairing-friendly elliptic curves.

BN curve ($k = 12$)	
$q(x)$	$36x^4 + 36x^3 + 24x^2 + 6x + 1$
$r(x)$	$36x^4 + 36x^3 + 18x^2 + 6x + 1$
KSS curve ($k = 18$)	
$q(x)$	$(x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21$
$r(x)$	$x^6 + 37x^3 + 343$
FST curve ($k = 24$)	
$q(x)$	$(x-1)^2(x^8 - x^4 + 1)/3 + x$
$r(x)$	$x^8 - x^4 + 1$

expected number of x_0 for exhaustive search and random search under some conditions in Table 1.

III. Examples

Consider the following three well-known pairing-friendly elliptic curves: the Freeman-Scott-Teske (FST) curve [8], Barreto-Naehrig (BN) curve [11], and Kachisa-Schaefer-Scott (KSS) curve [12]. The polynomials defining each curve are shown in Table 2.

All of these curves have CM-discriminant $D=3$. Therefore, the curves are given by $y^2=x^3+A$, and A can be easily found by using algorithm 1 in [11]. Since k is a multiple of 6, these curves have a sextic twist. Consider the following bit security levels: AES-80, AES-128 ($k=12, 18$), and AES-192 ($k=24$).

In each table, k , p , n , \tilde{r} , and \tilde{p} represent the embedding degree, the size of finite fields, the order of elliptic curves, the prime order of subgroups of elliptic curves, and the ratio of the bit length between p and \tilde{r} , respectively. In each curve, $\tilde{r} \pm 1$ is a prime times a small cofactor less than 2^{2L} .

Note that by lemma 1 in [6], if $\Phi_k(x)$ has a prime factor p , then $p=k$ or $p \equiv 1 \pmod{k}$. Because $r(x)$ in FST curve, BN curve, and the KSS curve is a factor of $\Phi_k(u(x))$ for some polynomial $u(x)$, we have $\tilde{r}=k$ or $\tilde{r} \equiv 1 \pmod{k}$ for a prime divisor \tilde{r} of $r(x)$. In KSS curve, if \tilde{r} is a prime of the form $18t+1$, then t must be a large odd prime for \tilde{r} to induce minimal security loss by Cheon's algorithm. This implies that $\tilde{r}+1=4s$ where s is a large prime. Therefore, each curve has as minimal security loss as shown in Table 6.

Table 3. Parameters of BN curve.

$k=12$	\tilde{r} : 162-bit prime, $L=2$, $\tilde{p}=1.07$, $y^2=x^3+10$
p	30044516319073486542338136244413186924491721508017673
n	30044516319073486542338136071079646260637812277386409
\tilde{r}	8048356903046741640058434522121523241531693618373
$\tilde{r}-1$	$2^2 \cdot 3 \cdot 670696408587228470004869543510126936794307801531$
$\tilde{r}+1$	$2 \cdot 4024178451523370820029217261060761620765846809187$
$k=12$	\tilde{r} : 266-bit prime, $L=2$, $\tilde{p}=1.04$, $y^2=x^3+2$
p	168117645147302822689933583299826302980183409639586768617985750798949133918522866373
n	168117645147302822689933583299826302980182999618068860956433850534919814584565135469
\tilde{r}	74487215395349057461202296544008109428525919192764227273563956816535141597060317
$\tilde{r}-1$	$2^2 \cdot 3 \cdot 6207267949612421455100191378667342452377159932730352272796996401377928466421693$
$\tilde{r}+1$	$2 \cdot 37243607697674528730601148272004054714262959596382113636781978408267570798530159$

Table 4. Parameters of KSS curve.

$k=18$	\tilde{r} : 162-bit prime, $L=3$, $\tilde{p}=1.41$, $y^2=x^3+15$
p	455565061885682046945119712171961255245560626663728567842656966003939
n	455565061885682046945119712171961241272652281084156741040827623564883
\tilde{r}	4693853757592073921597797107950839091753062864723
$\tilde{r}-1$	$2 \cdot 3^2 \cdot 260769653199559662310988728219491060652947936929$
$\tilde{r}+1$	$2^2 \cdot 1173463439398018480399449276987709772938265716181$
$k=18$	\tilde{r} : 262-bit prime, $L=3$, $\tilde{p}=1.38$, $y^2=x^3+13$
p	4190852828852838073198134637600446681572342216015854270904760027145718973065366962510130127051107405094739099
n	4190852828852838073198134637600446681572342216015854269564581015299079238120548169246970817388213113768028043
\tilde{r}	4409035112591057406686174540082721573572055151316564253993183503108303714414643
$\tilde{r}-1$	$2 \cdot 3^2 \cdot 244946395143947633704787474449040087420669730628698014110732416839350206356369$
$\tilde{r}+1$	$2^2 \cdot 1102258778147764351671543635020680393393013787829141063498295875777075928603661$

Table 5. Parameters of FST curve.

$k=24$	\tilde{r} : 173-bit prime, $L=3$, $\tilde{\rho}=1.33$, $y^2=x^3+3$
p	13374171350320546228612795187785960215360802 16803117468963832384367817
n	13374171350320546228612795187785960215360802 16803117468963832393495043
\tilde{r}	11597075993145642609104593362754747103486457 265418617
$\tilde{r}-1$	$2^3 \cdot 3 \cdot 4832114997144017753793580567814477959786$ 02386059109
$\tilde{r}+1$	$2 \cdot 579853799657282130455229668137737355174322$ 8632709309
$k=24$	\tilde{r} : 395-bit prime, $L=3$, $\tilde{\rho}=1.27$, $y^2=x^3+10$
p	34988959101369960326660128421263641796102887 16896841664612415025282748557287389764701382 92949449163227474599377357447706985689242725 65947999262774106637
n	34988959101369960326660128421263641796102887 16896841664612415025282748557287389764701382 92949449163227474599377357447706985689242725 65949591857333433243
\tilde{r}	90557749661667749903990677782104836298807865 80663129690953220847577622501207867202813795 1479865457762597440087882392553
$\tilde{r}-1$	$2^3 \cdot 3 \cdot 3773239569236156245999611574254368179116$ 99440860963737123050868649067604216994466783 9081311661060740108226670328433023
$\tilde{r}+1$	$2 \cdot 452788748308338749519953388910524181494039$ 32903315648454766104237888112506039336014068 975739932728881298720043941196277

Table 6. Minimal security loss L of each curve.

Curve	$\tilde{r}+1$	$\tilde{r}-1$	L	
BN ($k=12$)	$2s_1$	$12t_1$	2	s_i, t_i : large primes
KSS ($k=18$)	$4s_2$	$18t_2$	3	
FST ($k=24$)	$2s_3$	$24t_3$	3	

By 2^{30} times of random selection of integer x_0 in $[2^{(2w+\alpha-1)\deg(r)}, 2^{(2w+\alpha+10)\deg(r)}]$, where w is security level and $\alpha=15$, we found parameters of each curve in Tables 3, 4, and 5 which induced minimal security loss by Cheon's algorithm.

IV. Conclusion

The results show that the proposed method for searching parameters of pairing-friendly elliptic curves induces minimal security loss by Cheon's algorithm. The sample set of parameters of BN, FST, and KSS curves for pairing-based cryptography verifies the performance of the proposed method.

Finally, we remark that although Freeman and others investigated all of the construction of pairing-friendly curves in [8], they did not consider the security against Cheon's algorithm but focused on the construction with a small ρ -value. Our proposed method also verifies the existence of parameters of pairing-friendly elliptic curves with minimal security loss by Cheon's algorithm using parameters with a ρ -value slightly larger than that of Freeman and others.

References

- [1] J.H. Cheon, "Discrete Logarithm Problems with Auxiliary Inputs," *J. Cryptology*, vol. 23, no. 3, 2010, pp. 457-476.
- [2] D. Sun, *Elliptic Curves with the Minimized Security Loss of the Strong Diffie-Hellman Problem*, Doctoral Dissertation, Seoul National University, 2007.
- [3] A. Miyaji, M. Nakabayashi, and S. Takano, "New Explicit Conditions of Elliptic Curve Traces for FR-Reduction," *IEICE Trans. Fundamentals*, E84-A(5), 2001, pp.1234-1243.
- [4] P.S.L.M. Barreto, B. Lynn, and M. Scott, "Constructing Elliptic Curves with Prescribed Embedding Degrees," *Proc. SCN, LNCS*, vol. 2576, 2002, pp. 263-273.
- [5] F. Brezing, and A. Weng, "Elliptic Curves Suitable for Pairing Based Cryptography," *Designs, Codes, Cryptography*, vol. 37, no. 1, 2005, pp. 133-141.
- [6] A. Comuta, M. Kawazoe, and T. Takahashi, "Pairing-Friendly Elliptic Curves with Small Security Loss by Cheon's Algorithm," *Proc. ICISC, LNCS*, vol. 4817, 2007, pp. 297-308.
- [7] D. Freeman, "Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10," *Proc. ANTS-VII, LNCS*, vol. 4076, 2006, pp. 452-465.
- [8] D. Freeman, M. Scott, and E. Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves," *J. Cryptology*, vol. 23, no. 2, 2010, pp. 224-280.
- [9] H.W. Lenstra Jr., "Factoring Integers with Elliptic Curves," *Annals of Mathematics*, vol. 126, no. 3, 1987, pp. 649-673.
- [10] A.O.L. Atkin and F. Morain, "Elliptic Curves and Primality Proving," *Mathematics of Computation*, vol. 61, 1993, pp. 29-68.
- [11] P.S.L.M. Barreto and M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order," *Proc. SAC, LNCS*, vol. 3897, 2005, pp. 319-331.
- [12] E. Kachisa, E. Schaefer, and M. Scott, "Constructing Brezing-Weng Pairing Friendly Elliptic Curves Using Elements in the Cyclotomic Field," *Proc. Pairing, LNCS*, vol. 5209, 2008, pp. 126-135.