Heuristic counting of Kachisa-Schaefer-Scott curves

Yutaro Kiyomura¹, Noriyasu Iwamoto², Shun’ichi Yokoyama¹, Kenichiro Hayasaka¹, Yuntao Wang³, Takanori Yasuda³, Katsuyuki Takashima⁴ and Tsuyoshi Takagi⁵

¹Graduate School of Mathematics, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
²Graduate School of Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
³Institute of Systems, Information Technologies and Nanotechnologies, 2-1-22 Momochihama, Fukuoka 814-0001, Japan
⁴Information Technology R&D Center, Mitsubishi Electric, 5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
⁵Institute of Mathematics for Industry, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
E-mail ma212014@math.kyushu-u.ac.jp
Received March 25, 2014, Accepted June 25, 2014

Abstract
Estimating the number of pairing-friendly elliptic curves is important for obtaining such a curve with a suitable security level and high efficiency. For 128-bit security level, M. Naehrig and J. Boxall estimated the number of Barreto-Naehrig (BN) curves. For future use, we extend their results to higher security levels, that is, to count Kachisa-Schaefer-Scott (KSS) curves with 192- and 224-bit security levels. Our efficient counting is based on a number-theoretic conjecture, called the Bateman-Horn conjecture. We verify the validity of using the conjecture and confirm that an enough amount of KSS curves can be obtained for practical use.

Keywords pairing-based cryptography, pairing-friendly elliptic curve, KSS curves, Bateman-Horn conjecture

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction
Pairing-based cryptography is one of the popular topics in public key cryptography. A pairing is given as a map $e$ from $G_1 \times G_2$ to $G_T$, where $G_1$ and $G_2$ are subgroups with order $r$ on an elliptic curve over a finite field $\mathbb{F}_q$ and $G_T$ is a multiplicative group with prime order $r$ of $\mathbb{F}_{q^k}$ ($k$: embedding degree). This map $e$ has the bilinearity property i.e. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P \in G_1, Q \in G_2$ and $a, b \in \mathbb{Z}$. The schemes using such a pairing have various applications including ID-based encryption [1], keyword searchable encryption [2], and functional encryption [3]. For a secure pairing-based cryptosystem, both the discrete logarithm problems in the group of $\mathbb{F}_q$-rational points on an elliptic curve (ECDLP) and in the multiplicative group $\mathbb{F}_{q^k}$ (DLP) must be computationally infeasible. To achieve the same security level in both groups, the prime order $r$ and the size $q^k$ of the extension field should be balanced appropriately. For the purpose, the ratio $\rho = \log q/\log r$ gives an important parameter. Usually $\rho$ satisfies $1 \leq \rho \leq 2$ and $\rho \approx 1$ is the most desirable for high efficiency. For the embedding degree $k$, Freeman et al. recommended that $1 \leq k \leq 50$ [4]. For practical cryptosystems, we need suitable elliptic curves with small embedding degrees $k$ and large $r$. Curves with such properties are called “pairing-friendly elliptic curves”.

Due to the performance improvement of the hardware in the future, it is necessary to construct elliptic curves with varying embedding degrees for various security levels. In the literatures, Barreto-Naehrig (BN) curves [5] ($k = 12$) are recommended for 128-bit security level, and Kachisa-Schaefer-Scott (KSS) curves [6] are recommended for 192- and 224-bit security levels (as indicated in [7]). It is important to estimate the number of prime pairs $(q, r)$ of pairing-friendly elliptic curves for efficient curve parameters with suitable security levels. M. Naehrig and J. Boxall estimated the number of prime pairs $(q, r)$ for BN curves [8,9].

In this paper, we extend their results to KSS curves and estimate the number of prime pairs $(q, r)$ for KSS curves. Our efficient counting is based on a number-theoretic conjecture, called the Bateman-Horn conjecture [10]. For verifying the conjecture, we estimate the number of prime pairs $(q, r)$ in certain short intervals. Moreover, by calculating the Hardy-Littlewood constant given in the conjecture, we confirmed an enough amount of KSS curves with appropriate parameter sizes can be obtained for practical use.

2. Pairing-Friendly Elliptic Curves

2.1 Definition
For a random elliptic curve $E$ over a random field $\mathbb{F}_q$ and a prime $r \approx q$, the probability that $E$ has embedding degree less than $(\log q)^2$ with respect to $r$ is vanishingly small and in general the embedding degree can be expected to be around $r$ [11]. The computation of pair-
ings is infeasible since pairings on a random elliptic curve take values in a field of size $2^{160}$ if the size of $r$ and $q$ are around $2^{160}$ (80-bit security level). In order to construct practical pairing-based cryptography, we need suitable elliptic curves with such small embedding degree $k$ and large order $r$ of group. We define such an elliptic curve which is called pairing-friendly elliptic curve [4].

**Definition 1** Suppose $E$ is an elliptic curve defined over a finite field $\mathbb{F}_q$. We say that $E$ is a pairing-friendly elliptic curve if the following two conditions hold.

1. There is a prime $r \geq \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$.
2. The embedding degree of $E$ with respect to $r$ is less than $\log_2(r)/8$.

Freeman, Scott and Teske recommended that $1 \leq k \leq 50$ [4]. It is known that BN curves [5], KSS curves [6], etc. are famous pairing-friendly elliptic curves.

### 2.2 KSS Curves

Kachisa, Schaefer and Scott presented some new family of pairing-friendly elliptic curves [6]. These curves are called KSS curves. KSS curves are suitable for calculating pairings for high security levels. KSS-18 curves ($k = 18$) use the following parameters.

| $q(x) = \frac{1}{21} (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)$, |
|---------------------------------------------------------------|
| $r(x) = \frac{1}{343} (x^6 + 37x^3 + 343)$, |
| $t(x) = \frac{1}{7} (x^4 + 16x + 7)$.

We get the following polynomials $q^+(x)$ and $r^+(x)$ with integer coefficients by substituting $42x + 14$ for $x$ in $q(x)$ and $r(x)$.

\[
\begin{align*}
q^+(x) &= 461078666496x^7 + 1284433428096x^7 + 1564374047904x^6 + 108827335648x^5 + 473078255328x^4 + 131624074008x^3 + 22896702948x^2 + 2277529014x + 99213811, \\
r^+(x) &= 16003008x^6 + 32006016x^5 + 26671680x^4 + 11862072x^3 + 2971512x^2 + 397800x + 22249.
\end{align*}
\]

KSS-16 curves ($k = 16$) use the following parameters.

| $q(x) = \frac{1}{980} (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125)$, |
|---------------------------------------------------------------|
| $r(x) = \frac{1}{61250} (x^8 + 48x^4 + 625)$, |
| $t(x) = \frac{1}{35} (2x^5 + 41x + 35)$.

We get the following polynomials $q^+(x)$ and $r^+(x)$ with integer coefficient by substituting $70x + 25$ for $x$ in $q(x)$ and $r(x)$.

\[
\begin{align*}
q^+(x) &= 2882400500000000x^{10} + 1037664180000000x^9 + 1681204210000000x^8 + 1614132350000000x^7 + 10173492949900000x^6 + 4396843858680000x^5 + 1319757590130000x^4 + 2716657471500000x^3 + 36701968956250x^2 + 293862998082x + 105890880565, \\
r^+(x) &= 9411920000x^8 + 2689120000x^7 + 3361400000x^6 + 24010000000x^5 + 10718768816x^4 + 3062526880x^3 + 54689400x^2 + 55807000x + 2491537.
\end{align*}
\]

KSS-16 and KSS-18 curves are recommended for 192- and 224-bit security levels, respectively [7].

### 3. Heuristic Counting

#### 3.1 Counting $(q, r)$ Based on the Bateman-Horn Conjecture

A conjecture by Bateman and Horn [10] allows us to estimate the number of prime pairs $(q, r)$ of KSS curves.

**Conjecture 2** For large $y \in \mathbb{N}$, we heuristically expect the number of positive $x$ with $1 \leq x \leq y$ for which $(q, r) = (q^+(x), r^+(x))$ provides a prime pair of KSS curves to be

\[
Q(y) = \frac{C}{\deg q^+ \cdot \deg r^+} \int_{2}^{y} \frac{1}{(\log x)^2} dx.
\]

The constant $C$ is given as

\[
C = \prod_p \left( 1 - \frac{1}{p} \right)^{-2} \left( 1 - \frac{N_p}{p} \right),
\]

where the product is taken over all primes $p$ and $N_p$ denotes the number of solutions of $q^+(x) \cdot r^+(x) \equiv 0 \pmod{p}$. $C$ is called the Hardy-Littlewood constant.

$C$ is conditionally convergent and therefore unsuitable for numerical computation. Instead, we use the formula given by the theorem of Davenport and Schinzel [12] shown below.

**Theorem 3** Let $D_{q, r}$ be the discriminant of $q^+(x) \cdot r^+(x)$. Let $K_q$ (resp. $K_r$) be the number field generated by polynomial $q^+(x)$ (resp. $r^+(x)$), let $\rho(K_q)$ (resp. $\rho(K_r)$) be the residue of the Dedekind zeta function of number field $K_q$ (resp. $K_r$). Then the Hardy-Littlewood constant (2) is given by

\[
C = \frac{\gamma(D_{q, r})}{\rho(K_q) \cdot \rho(K_r)} \times \prod_{p | D_{q, r}} \left( 1 - \frac{N_p}{p} \right) \left( 1 - \frac{1}{p} \right)^{-N_p} \prod_{j \geq 2} \left( 1 - \frac{1}{p^j} \right)^{-N_{p(j)}}
\]

where the product is taken over all primes $p$ and $N_{p(j)}$ denotes the number of irreducible factors of $q^+(x) \cdot r^+(x)$.
Table 1. The value of each parameter for the Hardy-Littlewood constant in the case of KSS-18 curves.

| $p$ s.t. $p$ | $D_{q,r}$ | $N_p$ | $N^{q(j)}_p$ | $N^{r(j)}_p$ |
|--------------|----------------|------|-------------|-------------|
| 2            | 0              | 4    | 1           | 0           |
| 3            | 0              | 1    | 6           | 0           |
| 7            | 1              | 2    | 3           | 1           |
| 1879         | 3              | 1    | 3           | 0           |

Table 2. The value of each parameter for the Hardy-Littlewood constant in the case of KSS-16 curves.

| $p$ s.t. $p$ | $D_{q,r}$ | $N_p$ | $N^{q(j)}_p$ | $N^{r(j)}_p$ |
|--------------|----------------|------|-------------|-------------|
| 2            | 0              | 1    | 2           | 0           |
| 5            | 1              | 2    | 5           | 4           |
| 7            | 0              | 2    | 2           | 0           |
| 29           | 2              | 3    | 1           | 0           |
| 37           | 2              | 1    | 1           | 0           |
| 41           | 3              | 1    | 0           | 4           |

$(\text{mod } p)$ that are of degree $j$, and

$$\gamma(D_{q,r}) = \prod_{p \mid D_{q,r}} \left(1 - \frac{N_p}{p}\right) \prod_{j \geq 1} \left(1 - \frac{1}{p^j}\right)^{-N^{q(j)}_p - N^{r(j)}_p}$$

where $N^{q(j)}_p$ (resp. $N^{r(j)}_p$) denotes the number of distinct prime ideal factors of $p$ in $K_q$ (resp. $K_r$) that are of degree $j$.

3.2 Calculating the Hardy-Littlewood constants

For estimating the number of prime pairs $(q, r)$ of KSS curves, we calculated the Hardy-Littlewood constants by using a PC with following specifications: OS: Mac OS X Lion 10.7.5, CPU: Intel Core i7 2.7GHz, RAM: 4GB, Software with library: Magma V2.19-8 [13].

First, Table 1 shows the value of each parameter for the Hardy-Littlewood constant in the case of KSS-18 curves. We took the product over all primes $p$ with $2 \leq p < 10^4$. We calculated the Hardy-Littlewood constant $C$ by using the following intermediate values:

$$D_{q,r} = -10993687569404569692638984433145652116$$
$$47790629569259251226170319541227943$$
$$9891358479863452897892890026869871171$$
$$1616465957252142569839124675574807303$$
$$405860995536097935844131873491149953$$
$$3599336893569238811479553506704491$$
$$7418630411109678816,$$

$$\gamma(D_{q,r}) = 8.7577455178555663724757783419,$$

$$\rho(K_q) = 1.3360481512644235955504593364.$$
Table 3. Experimental results obtained by Method 1.

| Curves | $\ell$ | $P_{\ell}$ | $R_{\ell}$ | $Q_{\ell}$ | $E_{\ell}$ |
|--------|--------|-----------|-----------|-----------|-----------|
| KSS-18 | 76     | $1.38 \times 10^{-4}$ | 520089619800435929 | 571142585113572801 | 9.8% |
| KSS-16 | 50     | $1.46 \times 10^{-4}$ | 82000432115    | 94172570023    | 14.8% |

Table 4. Experimental results obtained by Method 2.

| Curves | $\ell$ | $\ell$-bit (length of $x$) | $x_{i,1}$ | $R_{I}$ | $P_{I}$ | $Q_{I}$ | $E_{I}$ | $H_{I} = 5 \times 10^{9}$ |
|--------|--------|---------------------------|----------|--------|--------|--------|--------|--------------------------|
| KSS-18 | 76     | $2^{10}$                  | 62       | 1.24 $\times 10^{-4}$ | 76.7    | 23.7%  | 413    | $1.38 \times 10^{-4}$ | 660.3 | 11.4% |
|        |        |                           | 83       | 1.66 $\times 10^{-4}$ | 75.5    | 9.0%   | 434    | $1.45 \times 10^{-4}$ | 453.2 | 4.4%  |
|        |        |                           | 51       | 1.02 $\times 10^{-4}$ | 74.7    | 46.5%  | 388    | $1.29 \times 10^{-4}$ | 448.3 | 15.5% |
| KSS-16 | 50     | $2^{10}$                  | 65       | 1.30 $\times 10^{-4}$ | 85.5    | 31.5%  | 420    | $1.40 \times 10^{-4}$ | 513.2 | 22.1% |
|        |        |                           | 84       | 1.68 $\times 10^{-4}$ | 83.5    | 0.5%   | 437    | $1.46 \times 10^{-4}$ | 401.2 | 14.7% |
|        |        |                           | 60       | 1.20 $\times 10^{-4}$ | 82.2    | 37.0%  | 405    | $1.35 \times 10^{-4}$ | 493.0 | 21.7% |

5. Conclusion

In this paper, we counted the number of prime pairs $(q, r)$ of KSS curves by using two methods, and estimated the probability of the prime pairs of KSS curves. The estimation shows that KSS curves with appropriate sizes of primes $(q, r)$ exist enough for practical use.

References

[1] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, in: Proc. of CRYPTO 2001, J. Kilian ed., LNCS, Vol. 2139, pp.213–229, Springer-Verlag, Berlin, 2001.
[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, Public key encryption with keyword search, in: Proc. of EUROCRYPT 2004, C. Cachin and J. Camenisch eds., LNCS, Vol. 3027, pp.506–522, Springer-Verlag, Berlin, 2004.
[3] T. Okamoto and K. Takashima, Fully secure functional encryption with general relations from the decisional linear assumption, in: Proc. of CRYPTO 2010, T. Rabin ed., LNCS, Vol. 6223, pp.191–208, Springer-Verlag, Berlin, 2010.
[4] D. Freeman, M. Scott and E. Teske, A taxonomy of pairing-friendly elliptic curves, J. Cryptology, 23 (2010), 224–280.
[5] P. Barreto and M. Naehrig, Pairing friendly elliptic curve of prime order, in: Proc. of SAC 2005, B. Preneel and S. Tavares eds., LNCS, Vol. 3897, pp.319–331, Springer-Verlag, Berlin, 2006.
[6] E. J. Kachisa, E. F. Schaefer and M. Scott, Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, in: Proc. of Pairing 2008, S. D. Galbraith and K. G. Paterson eds., LNCS, Vol. 5209, pp.126–135, Springer-Verlag, Berlin, 2008.
[7] C. Costello, Particularly friendly members of family trees, Cryptology ePrint Archive, Report 2012/072, 2012.
[8] J. Boxall, Heuristics on pairing-friendly elliptic curves, J. Math. Cryptol., 6 (2012), 81–104.
[9] M. Naehrig, Constructive and computational aspects of cryptographic pairings, Ph.D. thesis, Technische Universiteit Eindhoven, 2009.
[10] T. Bateman and R. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, Math. Comp., 16 (1962), 363–367.
[11] R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, J. Cryptology, 11 (1998), 141–145.
[12] H. Davenport and A. Schinzel, A note on certain arithmetical constants, Illinois J. Math., 16 (1966), 181–185.
[13] Computational Algebra Group, University of Sydney, The MAGMA Computational Algebra System for Algebra, Number Theory, and Geometry.