More Discriminants with the Brezing-Weng Method

Gaetan Bisson[1,2] and Takakazu Satoh[3]

[1] LORIA, 54506 Vandoeuvre-lès-Nancy, France
[2] Technische Universiteit, 5600 Eindhoven, Netherlands
[3] Tokyo Institute of Technology, 152-8551 Tokyo, Japan

Abstract. The Brezing-Weng method is a general framework to generate families of pairing-friendly elliptic curves. Here, we introduce an improvement which can be used to generate more curves with larger discriminants. Apart from the number of curves this yields, it provides an easy way to avoid endomorphism rings with small class number.

Keywords: Pairing-friendly curve generation, Brezing-Weng method.

1 Introduction

Since its birth in 2000, pairing-based cryptography has solved famous open problems in public key cryptography: the identity-based key-exchange [8], the one-round tripartite key-exchange [6] and the practical identity-based encryption scheme [3]. Pairings are now considered not only as tools for attacking the discrete logarithm problem in elliptic curves [7] but as building blocks for cryptographic protocols.

However, for these cryptosystems to be practical, elliptic curves with an efficiently computable pairing and whose discrete logarithm problem is intractable are required.

There are two general methods for the generation of such curves: the Cocks-Pinch method, which generates individual curves, and the Brezing-Weng method, which generates families of curves while achieving better ρ-values.

Our improvement extends constructions based on these methods by providing more curves with discriminants larger than what the constructions would normally provide (by a factor typically up to 10^9 given current complexity of algorithms for computing the Hilbert class polynomial). In the Cocks-Pinch method the discriminant can be freely chosen so our improvement is of little interest in this case; however, the Cocks-Pinch method is limited to $\rho \approx 2$. To achieve smaller ρ-values, one has to use the Brezing-Weng method where known efficient constructions mostly deal with small (one digit) discriminants; our improvement then provides an easy and efficient way to generate several curves with a wide range of discriminants, extending known constructions while preserving their efficiency (in particular, the ρ-value).

Curves generated by our improvement, having a larger discriminant, are possibly be more secure than curves whose endomorphism ring has small class number (even though, at the time of this writing, no attack taking advantage of a small class number is known).

In Section 2, we recall the general framework for pairing-friendly elliptic curve generation. Then, in Section 3, we present the Brezing-Weng algorithm and our improvement. Eventually, in Section 4, we study practical constructions and their efficiency; we also present a few examples.

2 Framework

2.1 The Embedding Degree

Let $\mathcal{E}$ be an elliptic curve defined over a prime finite field $\mathbb{F}_p$. We consider the discrete logarithm problem in some subgroup $\mathcal{H}$ of $\mathcal{E}$ of large prime order r. In addition, we assume that r is different from p.

For security reasons, the size of r should be large enough to avoid generic discrete logarithm attacks. For efficiency reasons, it should also not be too small when compared to the size of the ground field; indeed, it would be impractical to use the arithmetic of a very large field to provide the security level that could be achieved with a much smaller one. Therefore, the so-called ρ-value

$$\rho := \frac{\log p}{\log r}$$

must be as small as possible

We wish to generate such an elliptic curve and ensure that it has an efficiently computable pairing, that is a non-degenerate bilinear map from $\mathcal{H}^2$ to some cyclic group.

Known pairings on elliptic curves, i.e. the Weil and Tate pairings, map to the multiplicative group of an extension of the ground field. By linearity, the non-degeneracy of the pairing (on the subgroup of order r) forces the extension to contain primitive r^{th} roots of unity. Let $\mathbb{F}_{p^k}$ be the minimal such extension; the integer k is called the embedding degree. It can also be defined elementarily as

$$k = \min\{i \in \mathbb{N} : r | p^i - 1\}.$$

There are different ways of evaluating pairings, each featuring specific implementation optimizations. However, all known efficient methods are based on Miller's algorithm which relies on the arithmetic of $\mathbb{F}_{p^k}$. Therefore, the evaluation of a pairing can only be carried out when k is reasonably small.

In addition, the discrete logarithm problem must be practically intractable in both the subgroup of the curve and the multiplicative group of the embedding field. At the time of this writing, minimal security can be provided by the bounds

$$\log_2 r \geq 160 \text{ and } k \log_2 p \geq 1024.$$

However, these are to evolve and, as the bound on $k \log_2 p$ is expected to grow faster than that on $\log_2 r$ (mainly because of improvements on the index-calculus attack), we have to consider larger embedding degrees in order to preserve small ρ-values.

2.2 Curve Generation

In order to generate an ordinary elliptic curve with a large prime order subgroup and an efficiently computable pairing, we look for suitable values of the parameters:

- p, the cardinality of the ground field;
- t, the trace of the Frobenius endomorphism of the curve (such that the curve has $p + 1 - t$ rational points);
- r, the order of the subgroup;
- k, its embedding degree.

Here, "suitable" means that there exists a curve achieving those values. This consistency of the parameters can be written as the following list of conditions:

1. p is prime.
2. t is an integer relatively prime to p.
3. $|t| \leq 2\sqrt{p}$.
4. r is a prime factor of $p + 1 - t$.
5. k is the smallest integer such that $r \mid p^k - 1$.

By a theorem of Waterhouse [10], Conditions 1–3 ensure that there exists an ordinary elliptic curve over $\mathbb{F}_p$ with trace t. The last conditions then imply that its subgroup of order r has embedding degree k.

When r does not divide k —which is always the case in cryptographic applications as we want k to be small (for the pairing to be computable) and r to be large (to avoid generic discrete logarithm attacks)— Condition 5 is equivalent to $r \mid \Phi_k(p)$, which is a much more handy equation; therefore, assuming Condition 4, it is also equivalent to

$$r \mid \Phi_k(t-1).$$

To retrieve the Weierstrass equation of a curve with such parameters using the complex multiplication method, we need to look at $-D$, the discriminant (which need not be squarefree) of the quadratic order in which the curve has complex multiplication. Indeed, the complex multiplication method is only effective when the order has reasonably small class number. In practice, it is enough for D to be a small positive integer.

Writing the Frobenius endomorphism as an element of the complex multiplication order leads to the very simple condition

$$\exists y \in \mathbb{N}, 4p = t^2 + Dy^2$$

which ensures that $-D$ is the actual discriminant. It is referred to as the complex multiplication equation. Note that, instead of being added to the list, this condition may supersede Condition 3 as it is, in fact, stronger.

Using the cofactor of r, namely the integer h such that $p+1-t = hr$, the complex multiplication equation can also be written as

$$Dy^2 = 4p - t^2 = 4hr - (t-2)^2.$$

A remarkable fact is that if both the above equation considered modulo r and the "original" complex multiplication equation hold, the curve has a subgroup of order r.

Assuming that $p > 5$, the third condition implies that $p \mid t$ if and only if $t = 0$. Therefore, as p is expected to be large, we only have to check whether $t \neq 0$. This condition is omitted from the list below as it (mostly) always holds in practical constructions; bear in mind that it is required, though.

Finally, we can summarize the requirements to generate a pairing-friendly elliptic curve; we are looking for:

$$\begin{cases} p, r \text{ primes} \\ t, y \text{ integers} \\ D, k \text{ positive integers} \end{cases} \quad \text{such that} \quad \begin{cases} r \mid Dy^2 + (t-2)^2 \\ r \mid \Phi_k(t-1) \\ t^2 + Dy^2 = 4p \end{cases}$$

Note that, in the above equations, r can actually be allowed to be a prime times a small cofactor. Of course, this leads to equivalent conditions and is thus of little theoritical interest but, in some practical calculations, r appears to be of such a form and it would be too bad to miss the corresponding curves.

3 Algorithms

Let us fix D and k as small positive integers. The Cocks-Pinch method consists in solving the above equations to retrieve values of p, r, t and y; it proceeds in the following way:

1. Choose a prime r such that the finite field $\mathbb{F}_r$ contains $\sqrt{-D}$ and z, some primitive k^{th} root of unity.
2. Put $t = 1 + z$ and $y = \frac{t-2}{\sqrt{-D}} \mod r$.
3. Take lifts of t and y in $\mathbb{Z}$ and put $p = \frac{1}{4}\left(t^2 + Dy^2\right)$.

This algorithm has to be run for different parameters r and z until the output p is a prime integer; then, the complex multiplication method can be used to generate an elliptic curve over $\mathbb{F}_p$ with $p + 1 - t$ points, a subgroup of order r and embedding degree k.

Asymptotically, pairing-friendly elliptic curves generated by this algorithm have ρ-value 2.

3.1 The Brezing-Weng Method

The Brezing-Weng method starts similarly by fixing small positive integers D and k. Then, it looks for solutions to these equations as polynomials p, r, t and y in $\mathbb{Q}[x]$. Once a solution is found, for any integer x, an elliptic curve with parameters $(p(x), r(x), t(x), y(x), D, k)$ can be generated provided that $p(x)$ and $r(x)$ are prime and that $t(x)$ and $y(x)$ are integers.

To enable this, we expect polynomials p and r to have infinitely many simultaneous prime values. There is actually a very precise conjecture on the density of prime values of a family of polynomials:

Conjecture 1 (Bateman and Horn [1]). *Let $f_1, \ldots, f_s$ be s distinct (non-constant) irreducible integer polynomials in one variable with positive leading coefficient. The cardinality of R_N, the set of positive integers*

x less that N such that the $f_i(x)$'s are all prime, has the following asymptotic behavior:

$$\operatorname{card} R_N \sim \frac{C(f_1,\dots,f_s)}{\prod_i \deg f_i} \int_2^N \frac{du}{(\log u)^s} \qquad \textit{when } N \to \infty,$$

the constant $C(f_1,\dots,f_s)$ being defined as

$$\prod_{p\in\mathcal{P}} \left(1-\frac{1}{p}\right)^{-s} \left(1-\frac{1}{p}\operatorname{card}\left\{x\in\mathbb{F}_p : \prod_i f_i(x)=0\right\}\right)$$

where $\mathcal{P}$ denotes the set of prime numbers.

The latter constant quantifies how much the f_i's differ from independent random number generators, based on their behavior over finite fields.

As we only need a quick computational way of checking polynomials p and r, we use a weaker corollary, earlier conjectured by Schinzel [9] and known as *hypothesis H*, which just consists in assuming that the constant $C(f_i)$ is non-zero. Consider two polynomials, p and r; in that case, the corollary states that, provided that

$$\gcd\{p(x)\,r(x) : x\in\mathbb{Z}\} = 1,$$

the polynomials p and r have infinitely many simultaneous prime values.

Actually, there is a subtle difference with the polynomials we are dealing with here: they might have rational coefficients. However, we believe that the hypothesis of the above conjecture can be slightly weakened as

$$\gcd\{p(x)\,r(x) : x\in\mathbb{Z} \text{ such that } p(x)\in\mathbb{Z} \text{ and } r(x)\in\mathbb{Z}\} = 1$$

so to work with families of rational polynomials. Of course, we use the convention $\gcd\emptyset = 0$ (in case there is no x such that both $p(x)$ and $r(x)$ are integers).

Given small positive integers D and k, the Brezing-Weng method works as follows:

1. Choose a polynomial r with positive leading coefficient such that $\mathbb{Q}[x]/(r)$ is a field containing $\sqrt{-D}$ and z, some primitive k^{th} root of unity.
2. Put $t = 1+z$ and $y = \frac{t-2}{\sqrt{-D}}$ (represented as polynomials modulo r).
3. Take lifts of t and y in $\mathbb{Q}[x]$ and put $p = \frac{1}{4}\left(t^2+Dy^2\right)$.

This algorithm has to be run for different parameters r and z until the polynomials p and r satisfy the above conjecture. Then, we might be able to find values of x at which the instantiation of the polynomials yields a suitable set of parameters and thus generate an elliptic curve.

To heuristically check whether p and r satisfy the above conjecture, we compute the gcd of the product $p(x)\, r(x)$ for those $x \in \left\{1, \ldots, 10^2\right\}$ such that $p(x)$ and $r(x)$ are both integers. If this gcd is 1, the hypothesis of the conjecture is satisfied; otherwise, we assume it is not.

The main feature of this algorithm is that the ρ-value of the generated curves is asymptotically equal to $\frac{\deg p}{\deg r}$; therefore, a good ρ-value will be achieved if the parameters (D, k, r, z) can be chosen so that the polynomial p is of degree close to that of r. Because of the way p is defined, the larger the degree of r is, the more unlikely this is to happen.

Such wise choices are rare and mainly concerned with small discriminants; indeed, when D is a small positive integer, $\sqrt{-D}$ is contained in a cyclotomic extension of small degree which can therefore be taken as $\mathbb{Q}[x] / (r)$, thus providing a r-polynomial with small degree.

There exist a few wise choices for large D (cf. Paragraph 6.4 of [4]) but those are restricted to a small number of polynomials (p, r, t, y) and do not provide as many families as we would like.

3.2 Our Improvement

The key observation is that, if there exists an elliptic curve with parameters (p, r, t, y, D, k), then for every divisor n of y there also exists an elliptic curve with parameters $\left(p, r, t, \frac{1}{n}y, Dn^2, k\right)$. Note that this transformation preserves the ground field and the number of point of the curve, and therefore its ρ-value.

For one-shot Cocks-Pinch-like methods, this is of little interest since we could have set the discriminant to be $-Dn^2$ in the first place. However, for the Brezing-Weng method where good choices of the parameters (D, k, r, z) are not easily found, it provides a way to generate curves with a wider range of discriminants with the same machinery that we already have.

This improvement works as follows:

1. Generate a family (p, r, t, y, D, k) using the Brezing-Weng method.
2. Choose an integer x such that $p(x)$ and $r(x)$ are prime, and $t(x)$ and $y(x)$ are integers.

3. Compute the factorization of $y(x)$.
4. Choose a divisor n of $y(x)$ and generate a curve with parameters $\left(p(x), r(x), t(x), \frac{1}{n}y(x), Dn^2, k\right)$ using the complex multiplication method.

In Step 3, we do not actually have to compute the complete factorization of $y(x)$. Indeed, n cannot be too large in order for the complex multiplication method with discriminant $-Dn^2$ to be practical. So, we only have to deal with the smooth part of $y(x)$.

However, to avoid efficiently computable isogenies between the original curve (with $n = 1$, as generated by the standard Brezing-Weng method) and our curve, n must have a sufficiently large prime factor [5]. Indeed, such an isogeny would reduce the discrete logarithm problem from our curve to the original curve.

Therefore, we recommend to choose a prime factor n of $y(x)$ as large as possible among those n such that the complex multiplication method with discriminant $-Dn^2$ is still practical —i.e. the Hilbert class polynomial is computable in reasonable time. Nowadays, the computation of the Hilbert class polynomial for a discriminant with class number approximately 10^4 is a matter of minutes; we refer to [2] for quantitative statements. As the class number for discriminant $-Dn^2$ is roughly n, we advise to choose n in the integer interval $\left[10^3; 10^5\right]$, depending on the available processing power.

With such an n, the class number of the quadratic order with discriminant $-Dn^2$ will be reasonably large. This helps avoiding potential (though not yet known) attacks on curves with principal or nearly-principal endomorphism ring.

A toy example. Let $D = 8$, $k = 48$ and $r = \Phi_k$ (the cyclotomic polynomial of order k).

As x is a primitive k^{th} root of unity in $\mathbb{Q}[x]/(r)$, put

$$t(x) = 1 + x \text{ and } \sqrt{-D} = 2\left(x^6 + x^{18}\right).$$

The Brezing-Weng method outputs polynomials

$$y(x) = \frac{1}{4}\left(-x^{11} + x^{10} - x^7 + x^6 + x^3 - x^2\right) \text{ and } p = \frac{1}{4}\left(t^2 + Dy^2\right)$$

and the degree of p is such that this family has ρ-value 1.375.

For example, if $x = 137$ then

$$p(x) = 125429351059163205052743035650972214424622957\,13$$

which is a prime number and $r(x)$ is a prime number as well. The next step is to factor $y(x)$ as

$$y(x) = -1 \cdot 2 \cdot 17 \cdot 137^2 \cdot 229 \cdot 9109 \cdot 84191 \cdot 706631$$

and n can possibly be any product of these factors.

Take for instance $n = 17$, which results in discriminant -2312 with class number 16 (as opposed to class number one which would be provided by the standard Brezing-Weng method, i.e. with $n = 1$). The Weierstrass equation of a curve with parameters $\left(p(x), r(x), t(x), \frac{1}{n} y(x), Dn^2, k\right)$ is given by the complex multiplication method as

$$\begin{aligned} Y^2 = X^3 &+ 935824186433623028047894899424144532036848777X \\ &+ 898583952823329568888146564301424398299942966 0; \end{aligned}$$

this being, of course, an equation over $\mathbb{F}_{p(x)}$.

4 Constructions

We already mentioned that n should have a large prime factor. To increase chances for y to have such factors, we seek constructions where y is a nearly-irreducible polynomial, i.e. of degree close to that of its biggest (in terms of degree) irreducible factor.

Many constructions based on the Brezing-Weng method can be found in Section 6 of the survey article [4]. However, only few involve a nearly-irreducible y (most of those y are divisible by a power of x). Here, we describe a generic construction that is likely to provide nearly-irreducible y's.

4.1 Generic Construction

Fix an odd prime D and a positive integer k.

The extension $\mathbb{Q}[x]/(r)$ has to contain primitive k^{th} roots of unity; the simplest choice is therefore to consider a cyclotomic extension.

So, let us put $r = \Phi_{ke}$ for some integer e to be determined. Let ζ_D be a primitive D^{th} root of unity; the Gauss sum

$$\sqrt{\left(\frac{-1}{D}\right) D} = \sum_{i=1}^{D-1} \left(\frac{i}{D}\right) \zeta_D^i$$

shows that, for $\sqrt{-D}$ to be in $\mathbb{Q}[x]/(r)$, the product ke may be any multiple of εD where $\varepsilon = 4$ if -1 is a square modulo D, $\varepsilon = 1$ otherwise.

Therefore, we can use the following setting for the Brezing-Weng method:

1. Choose an odd prime D and a positive integer k.
2. Put $\varepsilon = 4$ if -1 is a square modulo D, $\varepsilon = 1$ otherwise.
3. Choose a positive integer e such that $\varepsilon D \mid ke$.
4. Choose a positive integer f relatively prime to k.
5. Put $r = \Phi_{ke}$, $z = x^{ef}$.
6. Use the expression

$$\sqrt{-D} = x^{\frac{ke}{\varepsilon}} \sum_{i=1}^{D-1} \left(\frac{i}{D}\right) x^{i\frac{ke}{D}} \mod r$$

   for the computation of y in the Brezing-Weng method.

As the latter polynomial is of large degree, it can be expected to be quite random once reduced modulo r. Therefore, it is likely to be nearly-irreducible and so the polynomial y given by the Brezing-Weng method might also be nearly-irreducible.

To support this expectation, we have computed $\delta := \frac{\deg m}{\deg y}$ where m is the biggest irreducible factor of $y = \frac{-1}{D}(z-1)\sqrt{-D}$, the polynomials for z and $\sqrt{-D}$ being given by the above algorithm. There are 4670 valid quadruplets $(D, k, e, f) \in \{1, \ldots, 20\}^4$ (i.e. for which D is an odd prime and $\varepsilon D \mid ke$); the following table gives the number of valid quadruplets in this range leading to values of δ with prescribed first decimal.

δ	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
	79	27	51	72	26	309	388	320	807	1127	1464

We see that, in this range, more than 70% of valid quadruplets lead to a y-polynomial whose largest irreducible factor is of degree at least $0.8 \deg y$.

4.2 Examples

Discriminant 3. Let $k = 9$, $D = 3$, $e = 1$ and $f = 4$.

The Brezing-Weng method outputs the polynomials

$$\begin{aligned} p(x) &= \tfrac{1}{3}\left(x^8 + x^7 + x^6 + x^5 + 4x^4 + x^3 + x^2 + x + 1\right) \\ y(x) &= \tfrac{1}{3}\left(x^4 + 2x^3 + 2x + 1\right) \end{aligned}$$

which represent a family of elliptic curves with ρ-value 1.33.

To generate a cryptographically useful curve from this family, we look for an integer x such that $p(x)$ is a prime, $r(x)$ is nearly-prime and $y(x)$ is an integer; we also have to make sure that $p(x)^k$ and $r(x)$ are of appropriate size for both security and efficiency.

Many such x's are easily found by successive trials; for instance, in the integer interval $\left[10^8; 10^8 + 2\cdot 10^6\right]$, there are 925 of them, which is only 6 times less than what a pair of independent random number generators would be expected to achieve (calculated as $\int_{10^8}^{10^8+2\cdot 10^6} \log^{-2}(x)\, dx \simeq 5888$); 364 of these x's have a prime factor in the integer interval $\left[10^3; 10^5\right]$, which can therefore be used as n in our algorithm.

For example, let us put $x = 100026508$; we obtain:

$$\begin{aligned}
p(x) &= 33404087284979282356159367134485\backslash\\
&\quad\; 14719712300943298532712491943583\\
r(x) &= 3 \cdot 33386384479456658408320968387432935440597815421 9\\
y(x) &= 47 \cdot 227 \cdot 3529 \cdot 27759659 \cdot 31926380379504181
\end{aligned}$$

If we choose $n = 3529$, the discriminant is -37361523 and has class number 1176; computations give a Weierstrass equation for the curve:

$$\begin{aligned}
Y^2 = X^3 &+ 32465585675528475154686711463989\backslash\\
&\quad\; 30389227646675927893599247518644X\\
&+ 10509028022025889317738018597831\backslash\\
&\quad\; 15352914330802852418162001031235
\end{aligned}$$

Discriminant 7. Let $k = D = 7$, $r = \Phi_7$ (i.e. $e = 1$) and $f = 3$. The Brezing-Weng method outputs the polynomials

$$\begin{aligned}
y(x) &= \tfrac{1}{7}\left(-2x^5 - x^3 + 2x^2 + 2x - 1\right)\\
p(x) &= \tfrac{1}{7}\left(x^{10} + x^8 - 2x^7 + 6x^3 - x + 2\right)
\end{aligned}$$

which represent a family of elliptic curves with ρ-value 1.66.

For instance, if $x = 100082571$, we obtain:

$$\begin{aligned}
p(x) &= 1440411212169845436143835468640473323570\backslash\\
&\quad\; 4509305009333005793207022595657279270011\\
r(x) &= 7 \cdot 71 \cdot 2022061384834451573585157936381299162262633341\\
y(x) &= -2 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 43 \cdot 2713 \cdot 331997537687 \cdot 2007994204551194071
\end{aligned}$$

If we choose $n = 2713$, the discriminant is -51522583 and has class number 2712; computations give a Weierstrass equation for the curve:

$$\begin{aligned}
Y^2 = X^3 &+ 5480003837932136059109680288524914164616\backslash\\
&\quad\; 4273898355113452168903506939196020801 85X\\
&+ 1075077622974369698869856782738812379262\backslash\\
&\quad\; 6891045118992108981946788799710877883221
\end{aligned}$$

Acknowledgements

We would like to thank Andreas Enge and Pierrick Gaudry for helpful discussions. Our gratitude also goes to Tanja Lange for her comments and suggestions on a draft version of this paper.

References

1. Paul T. Bateman and Roger A. Horn. Primes represented by irreducible polynomials in one variable. In *Proceedings of Symposia in Pure Mathematics*, volume 3, pages 119–132. American Mathematical Society, 1965.
2. Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Proceedings of the 8th International Symposium on Algorithmic Number Theory*. Springer LNCS, 2008.
3. Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.
4. David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006.
5. Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *The London Mathematical Society Journal of Computation and Mathematics*, 2:118–138, 1999.
6. Antoine Joux. A one round protocol for tripartite Diffie-Hellman. In *Proceedings of the 4th International Symposium on Algorithmic Number Theory*, volume 1838, pages 385–394. Springer LNCS, 2000.
7. Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.
8. Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing. In *Proceedings of the Symposium on Cryptography and Information Security*, page ref. C20, 2000.
9. Andrzej Schinzel and Wacław Sierpinski. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, 4:185–208, 1958.
10. William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École normale supérieure*, 2(4):521–560, 1969.