A GOLDWASSER-KILIAN APPROACH TO CERTIFICATES FOR RSA MODULII

IAN F. BLAKE AND ANNA POPIVANOVA

ABSTRACT. A non-interactive proof with certificates, that a given positive integer n is an RSA modulus, is given. It is based on a modification of the Goldwasser-Kilian method for primality proving.

1. INTRODUCTION

The paper gives a method for certifying that a given positive integer is the product of two suitably large primes. More specifically, a prover creates a certificate that a verifier can use to efficiently and deterministically verify that the given integer n is the product of two suitably large primes, without learning of the factorization. The method relies on a simple modification of the Goldwasser-Kilian technique [8]. The term 'suitably large' will mean that both primes in the factorization of n are at least as large as n^a, for some $a \in (1/3, 1/2)$.

Two recent contributions to the problem of verifying RSA modulii are [5] and [14]. Both produce efficient statistical zero-knowledge interactive proofs of the factorization of the given modulus. Both papers contain an interesting array of results beyond the RSA certification problem, although that problem appears to be their main motivation. It is felt that the deterministic nature of this work, once given the certificate, is of interest and complements the approach of these papers.

In the next section some background material on elliptic curves over the integers modulo a composite integer n is given. Section 3 recalls the Goldwasser-Kilian method of primality proving. Its extension to RSA modulii is given in Section 4 and the final two sections consider the complexity of the method and comment on other aspects of the problem.

2. ELLIPTIC CURVES OVER $\mathbb{Z}_n$

For an odd prime $p > 3$ denote by $E_p(A, B)$ the set of solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ to an equation of the form

$$y^2 = x^3 + Ax + B.$$

By the Hasse-Weil theorem it is known that

$$p + 1 - 2\sqrt{p} \leq \#E_p(A, B) \leq p + 1 + 2\sqrt{p}$$

and several results are available (eg. [11]) on the distribution of $\#E_p(A, B)$ as A, B are chosen at random in $\mathbb{F}_p$. Denote by $\mathcal{O}_p$ the point at infinity of the curve. There is a natural addition on $E_p(A, B)$ under which it forms a commutative group and

Date: August 3, 2001.

Key words and phrases. Cryptography, computational number theory.

this has been a rich source of groups for a variety of applications in cryptography and number theory.

Of interest here is in the extension of the set of solutions to this equation to $\mathbb{Z}_n$ ie. Any solution $(x, y) \in E_n(A_n, B_n)$ to the equation over $\mathbb{Z}_n$ can also be seen to be seen a solution to the equation modulo a prime, by restriction of the scalars. This is expressed as $(x_p, y_p) \in E_p(A_p, B_p)$ where subscripts on points and coefficients will be used to indicate the modular ring or field of definition under consideration. The operation of point addition in $E_n(A_n, B_n)$ is as in $E_p(A_p, B_p)$ with all operations in $\mathbb{F}_p$ replaced by those in $\mathbb{Z}_n$. There is a very small probability that some required arithmetic operation, such as inversion, may not be possible in which case a factorization of n would be produced. There is a bijection between $E_n(A_n, B_n)$ and E_p and E_q given by:

$$\begin{gathered} P = (x, y) \in E_n(A_n, B_n) \iff \\ (P_p, P_q) = \{(x_p, y_p) \in E_p(A_p, B_p), (x_q, y_q) \in E_q(A_q, B_q)\} \ n = pq. \end{gathered} \tag{1}$$

A point in $E_p(A_p, B_p)$ and one in $E_q(A_q, B_q)$ can yield one in $\mathbb{Z}_n$ using the Chinese Remainder Theorem (CRT) in the usual manner. If $\mathcal{O}_p$, $\mathcal{O}_q$ and $\mathcal{O}_n$ are the points at infinity in the respective modular fields and ring, then $\mathcal{O}_n$ corresponds to $(\mathcal{O}_p, \mathcal{O}_q)$ and the addition operation on $E_n(A_n, B_n)$ is equivalent to component-wise addition on $E_p(A_p, B_p) \times E_q(A_q, B_q)$ and this operation is undefined precisely when one of the points chosen is a point at infinity ([20]).

From the fact that if $Q = k \cdot P$, $P.Q \in E_n(A_n, B_n)$, $Q_p = k \cdot P_p$ and $Q_q = k \cdot P_q$ the order of $Q \in E_n(A_n, B_n)$ is the lcm of the orders if $\mathbb{F}_p$ and $\mathbb{F}_q$, it seems that the order $\#E_n(A_n, B_n)$ is the $\text{lcm}(\#E_p(A_p, B_p), \#E_q(A_q, B_q)$ (see [20], [12], [10] for further details on $E_n(A_n, B_n)$), although this is not needed here.

Finally denote the order of a point $P \in E_n(A_n, B_n)$ by $O_n(P)$, the smallest positive integer such that $k \cdot P = \mathcal{O}_n$, and similarly for points in E_p and E_q.

3. Goldwasser-Kilian certificates

The Goldwasser-Kilian technique for deterministically verifying a prime, given a certificate, depends on the following simple and elegant result (Lemma 2 of [8]). As it is central to this work it is reproduced here.

Lemma 3.1 (Goldwasser and Kilian [8]). *For all positive integers n not divisible by 2 or 3, if there exists a point P_n on an elliptic curve $E_n(A_n, B_n)$, $\gcd(n, 4A^3 + 27B^2) = 1$, of prime order q, where $q > (n^{1/4} + 1)^2$, then n is a prime.*

Proof. Suppose to the contrary that n is composite. Then there exists a prime p, $p|n$, $p < \sqrt{n}$. Since $q \cdot P_n = \mathcal{O}_n$. By restriction of scalars to $\mathbb{F}_p$, the order of P mod p must divide q, $O_p(P_p)|q$. Since $O_p(P_p) \leq \#E_p(A_p, B_p) \leq p + 1 + 2p^{1/2} < n^{1/2} + 1 + 2n^{1/2} < q$. Since q is prime then $O_p(P_p) = 1$ which implies that $P_p = \mathcal{O}_p$ which implies that $P_n = \mathcal{O}_n$ giving a contradiction. □

(XX Explain the condition $\gcd(n, 4A^3 + 27B^2) = 1$XX

The Lemma says that in order to demonstrate that n is prime it is sufficient to find an elliptic curve over $\mathbb{Z}_n$ which has a prime order subgroup of size at least $(n^{1/4} + 1)^2$. Note that the order of the subgroup, beyond the property noted, is unrelated in any other way to the integer n.

By means of this Lemma, generating a suitable prime q and an elliptic curve with the desired properties will show that n is prime. Goldwasser and Kilian [8]

apply the lemma to successively generate a sequence of primes and elliptic curves, randomly and using a probabilistic primality test, with decreasing orders, to create a 'certificate', a process referred to as a 'run-down' process [2]. In the final stage of the certificate generation, a deterministic primality test is applied to a relatively small number. With the certificate a user can, by successive applications of the lemma, verify each step of the 'run-up' process and be convinced, in a deterministic manner, that the original number is indeed a prime, since at each step the satisfaction of the Lemma will be verified. During the certificate generation phase it is sufficient to use probabilistic primality tests to determine the likelihood of a given integer being a prime. Should one of these tests in fact give a false prime, (indicate a number is prime when it is composite) it will show up when the final integer is deterministically shown to be a composite. The interesting notion of using probabilistic tests to derive a deterministic one is commented on in [8].

The Goldwasser-Kilian technique for generating certificates for a prime is given in algorithm form below, using our own notation and minor embellishments. In the original work, elliptic curves were sought at each stage of the algorithm such that their order was of the form twice a prime. The order of a randomly chosen curve is found by point counting methods. Goldwasser and Kilian suggested the original algorithm of Schoof [18], an operation of $O(\log p^9)$ (or less, depending on the type of arithmetic used). Since that work appeared other more efficient algorithms have been found and these are commented on in a later Section 5. It has also been suggested [1] that using the complex multiplication (CM) technique of generating an elliptic curve of given order over a prime field would also make the algorithm more efficient and this is also commented upon.

A way to make the algorithm more efficient is to find a prime divisor q of the curve order as close to $(n^{1/4}+1)^2$ as possible to reduce the sequence of primes (and speed up the down-run process) as quickly as possible, to result in fewer steps of the algorithm and a smaller certificate. This is perhaps more difficult to implement since it would require a factoring algorithm, precisely which we assume is not available. As noted, the CM method of curve generation will be useful in this regard.

For the moment we note that it is relatively easy to include a trial divide step on the order of a curve generated, to some appropriate bound of perhaps a few million, which would reduce the number of curves that would have to be generated to achieve one with the desired property i.e. in the original version of the algorithm, a curve whose order was not of the form twice a prime was discarded and another curve tried. With a trial divide included, some of these discarded curves might be suitable, containing a subgroup of an appropriate prime order. Thus after the trial divide routine the remainder of the order is tested for being a prime that satisfies the requirement. These issues are also discussed in [2] where the elliptic curve primality proving algorithm of Lenstra, Atkin and Morain are considered.

The following algorithm uses a few standard routines. In choosing an elliptic curve at random, we want one whose order $\#E_{p_i}(A_i, B_i)$, for some given integer p_i that has passed a probabilistic primality test, is divisible by a prime q_i greater than $(p_i^{1/4}+1)^2$ for two suitable (probabilistic) primes p_i and q_i (which will become p_{i+1} at the next stage - the primes form a decreasing sequence).

The routine `TrialDivide`(n, bd) returns an integer n' which is n divided by all primes (and all their powers) less than bd. It is possible that suitable curves will

still be rejected by this routine as well but some suitable curves will be found that the original test would have rejected.

The routine `ProbPrime(n)` returns `true` if the integer n passes a standard probabilistic primality test (eg. Miller-Rabin, Solovay-Strassen) for some fixed number of rounds. Otherwise it returns `false`. It is assumed that at the last stage of the algorithm both the prover and verifier have available a deterministic primality test for the last prime used in the certificate - this step is omitted. (e.g. [11]) run on small numbers at the last stage of certificate generation that guarantees at the start of certificate verification the initial number is a prime. It also returns either `true` or `false`.

Finally by the notation ϵ_R is meant a random choice, uniform over the set being considered.

ALGORITHM 3.1: **Goldwasser-Kilian certificate generation for the prime p**

INPUT: A prime number p
OUTPUT: A certificate for the primality of p, CERT_PRIME(p)
1. Initialization: $i = 0$, $p_0 = p$, lower bound = bd, FLAG1 = false:
   FLAG2 = false, CERT_PRIME(p) = ϕ
2. While $p_i > bd$:
3. Repeat the steps until FLAG1 = true:
4. Choose $A_i, B_i \epsilon_R \mathbb{Z}_{p_i}$, $\gcd(4A_i^3 + 27B_i^2, p_i) = 1$
5. Compute $\#E_{p_i}(A_i, B_i)$ and let $N_i = \text{TrialDivide}(\#E_{p_i}(A_i, B_i, bd)$
6. If ProbPrime(N_i) = true and $N_i > (p_i^{1/4} + 1)^2$ Set FLAG1 = true
7. Repeat the steps until FLAG2 = true:
8. Choose $P_{p_i} \epsilon_R E_{p_i}(A_i, B_i)$ until $N_i \cdot P_{p_i} = \mathcal{O}_{p_i}$
9. Set FLAG2 = true
10. $p_{i+1} = N_i$, CERT_PRIME(p) = CERT_PRIME(p) $\cup \{p_i, A_i, B_i, P_{p_i}, p_{i+1}\}$
11. $i = i + 1$
12. Return CERT_PRIME(p)

As commented on in [8], this test terminates in expected polynomial time on all but at most a vanishingly small fraction of inputs, where the step requiring the determination of a suitable elliptic curve might not decide within some finite time. However, given a certificate, the test verifies primality in deterministic polynomial time. Given a certificate, the correctness of the primality is certain, even though probabilistic tests are used in the certificate generation.

Notice that if, at any stage, the probabilistic primality test gave a false answer, i.e. it declares an integer to be a prime when it is a composite, then the final deterministic primality test would fail and the whole procedure would be repeated.

It is straightforward now to recursively check the information in the certificate to verify deterministically that the original integer p is a prime.

The next section shows how this approach can be generalized for RSA modulii.

4. CERTIFICATES FOR RSA MODULII

The Goldwasser-Kilian Lemma of the previous section is emulated to provide a result that will be used to generate RSA certificates. We have in mind to generate a certificate for the RSA modulus n_0, a product of the primes p_0, q_0.

Lemma 4.1. *Let n_0 be a positive integer not divisible by 2 or 3. Suppose the positive integer n_1 ($< n_0$) is the product of two prime numbers, both of which are greater than $(n_0^{1/6}+1)^2$. Then if there exists a point P_{n_0} on an elliptic curve $E_{n_0}(A_{n_0}, B_{n_0})$, $\gcd(n_0, 4An_0{}^3+27B_{n_0}^2) = 1$ of order n_1 then n_0 can have no divisors less than $n_0{}^{1/3}$.*

Proof. Suppose to the contrary that n_0 has a divisor r less than $n_0^{1/3}$. By assumption

$$n_1 P_{n_0} = \mathcal{O}_{n_0} \;\Rightarrow\; n_1 P_r = \mathcal{O}_r \;\Rightarrow O_{E_r}(P_r) \mid n_1.$$

But

$$\begin{aligned} O_{E_r}(P_r) \leq &\quad \#E_r(A_r, B_r) \leq r + 1 + 2r^{1/2} \\ < &\quad n_0^{1/3} + 2n_0^{1/6} + 1 \end{aligned}$$

which is strictly less, by assumption, than either of the prime factors of n_1. Hence, $P_r = \mathcal{O}_r$ which implies that $P_n = \mathcal{O}_n$ which gives a contradiction. □

The conditions of Lemma are sufficient to verify that the integer n_0 is a product of at most two primes. In the final algorithm we will remove the possibility that it is prime by providing a witness to the compositeness of n ie. an integer a such that $a^n \not\equiv a \pmod{n}$. We designate such a witness by $w_n(a)$. The generation of witnesses will be discussed in Section 5. Again, such witnesses will be found by repeated random selection, but once found they provide deterministic evidence of the compositeness n. Since n is a product of at most two primes there must exist such witnesses since it cannot be a Carmichael number (a composite integer n for which $a^n \equiv a \pmod{n}$) which always has at least three prime factors [13].

The certificate generation process for the RSA modulus $n_0 = p_0 q_0$ will generate two primes p_1 and q_1 that satisfy the above Lemma. It then provides a witness for the compositeness of n_0 and two GK certificates for the primes p_1 and q_1 to complete the evidence that n_0 is an RSA modulus.

ALGORITHM 4.1: **GK certificate generation for the RSA modulus $n_0 = p_0 q_o$**

```
INPUT:  An RSA number n_0 = p_0 q_0
OUTPUT: A certificate for the RSA modulus CERT_RSA(n_0)
1.  Initialization:  FLAG1 = false:  FLAG2 = false, CERT_RSA(n_0) = φ
2.      Repeat until FLAG1 = true:
3.          Choose A_{p_0}, B_{p_0} ε_R Z_{p_0},  gcd(4A_{p_0}^3 + 27B_{p_0}^2, p_0) = 1 until
4.              Compute #E_{p_0}(A_{p_0}, B_{p_0}),  N_0^(1) = TrialDivide(#E_{p_0}(A_{p_0}, B_{p_0}))
5.              If ProbPrime(N_0^(1)) = true and N_0^(1) > (n_0^{1/6} + 1)^2
6.                      p_1 = N_0^(1),  continue
7.          Choose A_{q_0}, B_{q_0} ε_R Z_{q_0},  gcd(4A_{q_0}^3 + 27B_{q_0}^2, q_i) = 1 until
8.              Compute #E_{q_0}(A_{q_0}, B_{q_0}),  N_0^(2) = TrialDivide(#E_{q_0}(A_{q_0}, B_{p_0})
9.              If ProbPrime(N_0^(2)) = true and N_0^(2) > (n_0^{1/6} + 1)^2
10.                     q_1 = N_0^(2),  continue
11.         Set FLAG1 = true
12.     Repeat until FLAG2 = true:
13.         Choose P_{p_0} ε_R E_{p_0}(A_{p_0}, B_{p_0}) until p_1 · P_{p_0} = O_{p_0}
14.         Choose P_{q_0} ε_R E_{q_0}(A_{q_0}, B_{q_0}) until q_1 · P_{q_0} = O_{q_0}
15.         Determine the point P_{n_0} and A_{n_0}, B_{n_0} using bijection of Equation 1.
```

```
16.          Set FLAG2 = true
17.      n_1 = p_1 · q_1, CERT_RSA(n) = CERT_RSA(n) ∪{n_1 = p_1 · q_1, A_{n_0}, B_{n_0}, P_{n_0}, w_{n_0}(a)}
18.      CERT_RSA(n) = CERT_RSA(n) ∪ { CERT_PRIME (p_1) , CERT_PRIME (q_1) }
19. Return CERT_RSA(n)
```

The verification process first verifies, through the standard Goldwasser-Kilian process, that the numbers p_1 and q_1 are primes and that they satisfy the condition of both being greater than $(n_0^{1/6}+1)^2$. The compositeness of n_0 is checked by verifying that $a^{n_0} \not\equiv a \pmod{n_0}$. Finally it is verified that the point $P_{n_0} \in E_{n_0}$ has order $n_1 = p_1 q_1$ by showing that $n_1 \cdot P_{n_0} = \mathcal{O}_{n_0}$.

5. Complexity

(In this section we will give comments on the complexity of point counting, SEA, Satoh, Kedlaya etc.) as well as a brief outline of the CM method.) I will do this.

The complexity of finding a witness for compositeness for numbers of the form $n = pq$ will be discussed - I think this is standard. The standard Miller-Rabin test actually gives estimates for the number of these I think.

6. Comments

Some aspects of the method of certifying RSA modulii given in the previous section, are noted in this section.

Note that the Lemma of the previous Section limited the primes to be greater than approximately $n_0^{1/3}$ (and hence also less than $n^{2/3}$). It is straightforward to narrow the range and we state the following variation of the Lemma without proof:

Lemma 6.1. *Let n_0 be a positive integer not divisible by 2 or 3. Suppose the positive integer n_1 is the product of two prime numbers, both of which are greater than $(n_0^{a/2}+1)^2$ for $a \in (0,1/2)$. Then if there exists a point P_{n_0} on an elliptic curve $E_{n_0}(A_{n_0}, B_{n_0})$, $\gcd(n_0, 4A_0^3 + 27B_0^2) = 1$ of order n_1 then n_0 can have no divisors less than ${n_0}^a$.*

Arguing informally, choosing $a \sim 1/2 - \epsilon$ restricts the factors of n_0 to be in the interval $(n_0^{a/2}+1)^2, n_0/(n_0^{a/2}+1)^2$ as long as $(n_o^{a/2}+1)^4 > n_0$. Thus if the modulus n_0 is to be 1024 bits, by choosing an appropriate value for a one could ensure the primes p_0 and q_0 have as close to an equal number of bits as possible.

We are tempted to label our test zero-knowledge as we know of no method to glean any information on the factorization of the RSA modulus from the knowledge of the primes p_1 and q_1. Unfortunately we are unable to verify that no information is leaking in this process, beyond knowledge that the given integer n is a composite with two factors each on the order of $\sqrt{n}$.

An interesting feature of the work of [5] is that it is able to verify that the RSA modulus is composed of safe primes i.e. primes p and q such that $(p-1)/2$ and $(q-1)/2$ are also primes. It would be interesting if the technique of the previous section could be modified to include that situation as well but at this point it is unclear how this could be achieved. (It is interesting to note however, the work of Rivest and Silverman [17] that questions the need for using such safe primes).

It seems that a variation of the scheme mentioned might yield a test that an integer is the product of three suitably large primes. The obvious extension to the basic Lemma then is:

Lemma 6.2. *Let n_0 be a positive integer not divisible by 2 or 3. Suppose the positive integer n_1 is the product of three prime numbers, all of which are greater than $(n_0^{1/4}+1)^2$. Then if there exists a point P_{n_0} on an elliptic curve $E_{n_0}(A_{n_0}, B_{n_0})$, $\gcd(n_0, 4A_0^3+27B_0^2) = 1$ of order n_1 then n_0 can have no divisors less than ${n_0}^{1/4}$.*

The Lemma gives a condition that will ensure n_0 has at most three prime factors. Perhaps it is possible to derive further conditions that will ensure it has exactly three distinct factors.

Boneh at al [3] considered the problem of how to generate an RSA modulus in a distributed manner so that the final RSA modulus and encryption exponent is known by all parties but the factorization of the modulus is unknown and parties receive only a share of the decryption exponent i.e. a distributed secret sharing scheme. It would be interesting if the approach taken here might be of use in such a scenario.

References

[1] A.O.L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.*, vol. 61, pp. 29-67, 1993.

[2] Ian F. Blake, G. Seroussi and N.P. Smart, *Elliptic curves in cryptography*, Cambridge University Press, LMS Lecture Note Series, vol. 265, 1999.

[3] D. Boneh and M. Franklin, Efficient generation of shared RSA keys, *Advances in Cryptology, Crypto '97* LNCS vol. 1233, pp. 425-439 1997.

[4] J. Boyar, K. Friedl and C. Lund, Practical zero knowledge proofs: Giving hints and using deficiencies, *J. Cryptology*, vol. 4, pp. 185-206, 1991.

[5] J. Camenisch and M. Michels, Proving in zero-knowledge that a number is the product of two safe primes, in *Advances in Cryptology, Eurocrypt '99* LNCS vol. 1592, J. Stern (Ed.), pp. 107-122, 1999.

[6] Z. Galil, S. Huber and M. Yung, A private interactive test of a Boolean predicate and minimum-knowledge public key cryptosystems, in *Proc. 26th FOCS*, pp. 360-371, 1985.

[7] R. Gennaro, D. Micciancio and T. Rabin, An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products, in *Proc. 5th CCCS*, pp. 67-72, 1998.

[8] S. Goldwasser and J. Kilian, Almost all primes can be quickly certified, in *Proc. 18th STOC*, pp. 316-329, 1986.

[9] J. van der Graaf and R. Peralta, A simple and secure way to show the validity of your public key, *Advances in Cryptology, Crypto '87* LNCS vol. 293, C. Pomerance (Ed.), pp. 128-134, 1988.

[10] N. Kunihiro and K. Koyama, Equivalence of counting the number of points on elliptic curve over the ring $\mathbb{Z}_n$ and factoring n, *Advances in Cryptology, Eurocrypt '98* LNCS vol. 1403, R. Nyberg (Ed.), pp. 47-58, 1998.

[11] H.K. Lenstra, Factoring with elliptic curves, *Ann. Math.*, vol. 126, pp. 649-673, 1987.

[12] B. Meyer and V. Müller, A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring, *Advances in Cryptology, Crypto '96* LNCS vol. 1070, U. Maurer (Ed.), pp. 49-59, 1996.

[13] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Berlin, Heidelberg: Springer-Verlag, 2001.

[14] G. Poupard and J. Stern, Short proofs of knowledge for factoring, in Proc. PKC 2000, LNCS vol. 1751, pp. 147-166, 2000.

[15] V. Pratt, Every prime has a succinct certificate, *SIAM J. Computing*, vol. , pp.214-220, 1975.

[16] M. Rabin, Probabilistic algorithms for testing primality, *J. Number Theory*, vol. 12, pp. 128-138, 1980.

[17] R. Rivest and R. Silverman, Are 'strong' primes needed for RSA?, RSA Labs Technical report, December 1, 1998.

[18] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.*, vol. 44, pp. 483-494, 1985.

[19] Solovay and Strassen, A fast Monte-Carlo test for primality, *SIAM J. Computing*, vol. 23, pp. 179-206, 1974.

[20] S.A. Vanstone and R. Zuccherato, Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$, *IEEE Trans. Information Theory*, vol. 43, pp. 1231- 1237, 1997.

Department of Electrical and Computer Engineering, Toronto, M5S 3G4, Canada
E-mail address: ifblake@comm.toronto.edu

Department of Computer Science, Toronto, M5S 3G4, Canada
E-mail address: anna@cs.toronto.edu