Secure Bilinear Diffie-Hellman Bits

Steven D. Galbraith[1], Herbie J. Hopkins[1], and Igor E. Shparlinski[2]

[1] Mathematics Department, Royal Holloway University of London
Egham, Surrey, TW20 0EX, UK
`Steven.Galbraith@rhul.ac.uk`, `H.J.Hopkins@rhul.ac.uk`
[2] Deptartment of Computing, Macquarie University
Sydney, NSW 2109, Australia
`igor@comp.mq.edu.au`

Abstract. The Weil and Tate pairings are a popular new gadget in cryptography and have found many applications, including identity-based cryptography. In particular, the pairings have been used for key exchange protocols. This paper studies the bit security of keys obtained using protocols based on pairings (that is, we show that obtaining certain bits of the common key is as hard as computing the entire key). These results are valuable as they give insight into how many "hard-core" bits can be obtained from key exchange using pairings.

1 Introduction

Let p be a prime and let $\mathbb{F}_p$ be the field of p elements, which we identify with the set $\{0, 1, \ldots, p-1\}$. Let l be a prime which is coprime to p and define m to be the smallest positive integer such that $p^m \equiv 1 \pmod{l}$. In this paper we consider a non-degenerate bilinear pairing

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathcal{G} \subseteq \mathbb{F}_{p^m}^*$$

where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathcal{G}$ are cyclic groups of order l. Such a pairing can be obtained from the *Weil* or *Tate* pairings on elliptic curves or abelian varieties [9, 10, 17, 18, 21–23, 28].

One implementation of such a pairing which has $\mathbb{G}_1 = \mathbb{G}_2$ (given by Verheul [28]) is to take a supersingular elliptic curve E over $\mathbb{F}_p$ such that $l \| \#E(\mathbb{F}_p)$ and such that E has a suitable "distortion map" φ (which is a non-$\mathbb{F}_p$-rational endomorphism on E). Let $\mathbb{G}_1 = \mathbb{G}_2$ be the unique subgroup of $E(\mathbb{F}_p)$ of order l. The pairing $e(P, Q)$ is defined to be the Weil (or Tate) pairing of P with $\varphi(Q)$. For a situation where $\mathbb{G}_1 \neq \mathbb{G}_2$ see [17]. We note that suitable groups $\mathbb{G}_1, \mathbb{G}_2$ over prime fields $\mathbb{F}_p$ for which m is large can be constructed using the methods of [2, 8].

Pairings have found many applications in cryptography including the tripartite key exchange protocol of Joux [17] (also see the variations by Al-Riyami and Paterson [1] and Verheul [28]) and the identity-based key exchange protocol of Smart [27]. These protocols enable a set of users to agree a random element K of a subgroup of $\mathbb{F}_{p^m}^*$, and the "key" is then derived from K.

We recall the *tripartite Diffie-Hellman protocol* in the original formulation of Joux [17]: To set up the system, three communicating parties A, B and C

choose suitable groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order l and points $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ with $e(P,Q) \neq 1 \in \mathbb{F}_{p^m}^*$.

To create a common secret key, A, B and C choose secret numbers $a, b, c \in [0, l-1]$ and publish pairs

$$(aP, aQ), \qquad (bP, bQ), \qquad (cP, cQ).$$

Now each of them is able to compute the common key

$$K = e(P,Q)^{abc}.$$

For example, A can compute K as follows,

$$e(bP, cQ)^a = e(P, cQ)^{ab} = e(P,Q)^{abc} = K \in \mathbb{F}_{p^m}^*.$$

Note that K is an element of order l in $\mathbb{F}_{p^m}^*$.

Since p^m is very large (at least 1024 bits), and since K is an element of a subgroup, one is inclined to only use a part of the representation of K to derive the bitstring which serves as the key. An important issue is what is meant by the "bits" of an element of an extension field $\mathbb{F}_{p^m}$ (since we usually have $m > 1$).

Since $l \approx p$ it makes sense to derive a key whose size is approximately the same as the size of p. In this paper we consider taking the trace of K with respect to $\mathbb{F}_{p^m}/\mathbb{F}_p$ to obtain an element of $\mathbb{F}_p$. We represent elements of $\mathbb{F}_p$ as integers in $[0, p-1]$ and obtain corresponding bitstrings in the usual way. We show that the trace is a secure key derivation function.

The results follow from several recently established results [19, 26] on the *hidden number problem with trace* in extension fields. Detailed surveys of bit security results and discussions of their meaning and importance are given in [11, 12]; several more recent results can be found in [5–7, 13–16, 19, 25, 26].

We obtain an almost complete analogue of the results of [7, 13] for $m = 2$ (for example, for the elliptic curves used by Joux [17] and Verheul [28]) and much weaker, but nontrivial, results for $m \geq 3$. For example, in the case that $m = 2$ and p is a 512 bit prime, our results imply that, if the bilinear-Diffie-Hellman problem is hard, then the 128 most significant bits of the trace of K can be used to derive a secure key.

Note that we allow all our constants to depend on m while p and l are growing parameters. Thoughout the paper $\log z$ denotes the binary logarithm of $z > 0$.

2 Hidden Number Problem with Trace

We denote by

$$\mathrm{Tr}(z) = \sum_{i=0}^{m-1} z^{p^i} \qquad \text{and} \qquad \mathrm{Nm}(z) = \prod_{i=0}^{m-1} z^{p^i}$$

the *trace* and *norm* of $z \in \mathbb{F}_{p^m}$ to $\mathbb{F}_p$, see Section 2.3 of [20].

For an integer x we define

$$\|x\|_p = \min_{a \in \mathbb{Z}} |x - ap|$$

and for a given $k > 0$, we denote by $\mathrm{MSB}_{k,p}(x)$ any integer u, $0 \le u \le p-1$, such that

$$\|x - u\|_p \le p/2^{k+1}.$$

Roughly speaking, a value of $\mathrm{MSB}_{k,p}(x)$ gives the k most significant bits of the residue of x modulo p. Note that in the above definition k need not be an integer.

The *hidden number problem with trace* over a subgroup $\mathcal{G} \subseteq \mathbb{F}_{p^m}^*$ can be formulated as follows: Given r elements $t_1, \ldots, t_r \in \mathcal{G} \subseteq \mathbb{F}_{p^m}^*$, chosen independently and uniformly at random, and the values $\mathrm{MSB}_{k,p}(\mathrm{Tr}(\alpha t_i))$ for $i = 1, \ldots, r$ and some $k > 0$, recover the number $\alpha \in \mathbb{F}_{p^m}$.

The case of $m = 1$ and $\mathcal{G} = \mathbb{F}_p^*$ corresponds to the hidden number problem introduced in [7] (for the case $\mathcal{G} \subset \mathbb{F}_p^*$ see [13]). The case of $m \ge 2$ is more difficult because one of the crucial ingredients, a bound on exponential sums with elements of small subgroups of $\mathbb{F}_{p^m}$, is missing. Nevertheless in some special cases results of a comparable strength have been obtained in [19]. In other cases, an alternative method from [26] can be used, leading to weaker results.

The following statement is a partial case of Theorem 2 of [19].

We denote by $\mathcal{N}$ the set of $z \in \mathbb{F}_{p^m}$ with norm equal to 1, thus $|\mathcal{N}| = (p^m - 1)/(p-1)$.

Lemma 1. *Let p be a sufficiently large prime number and let $\mathcal{G}$ be a subgroup of $\mathcal{N}$ of order l with $l \ge p^{(m-1)/2+\rho}$ for some fixed $\rho > 0$. Then for*

$$k = \left\lceil 2\sqrt{\log p} \right\rceil \qquad \textit{and} \qquad r = \left\lceil 4(m+1)\sqrt{\log p} \right\rceil$$

there is a deterministic polynomial time algorithm $\mathcal{A}$ as follows. For any $\alpha \in \mathbb{F}_{p^m}$, if $t_1, \ldots, t_r$ are chosen uniformly and independently at random from $\mathcal{G}$ and if $u_i = \mathrm{MSB}_{k,p}(\mathrm{Tr}(\alpha t_i))$ for $i = 1, \ldots, r$, the output of $\mathcal{A}$ on the $2r$ values (t_i, u_i) satisfies

$$\Pr_{t_1, \ldots, t_r \in \mathcal{G}} \left[\mathcal{A}(t_1, \ldots, t_r; u_1, \ldots, u_r) = \alpha \right] \ge 1 - p^{-1}.$$

For smaller groups a weaker result is given by Theorem 1 of [26].

Lemma 2. *Let p be a sufficiently large prime number and let $\mathcal{G}$ be a subgroup of $\mathbb{F}_{p^m}^*$ of prime order l with $l \ge p^\rho$ for some fixed $\rho > 0$. Then for any $\varepsilon > 0$, let*

$$k = \lceil (1 - \rho/m + \varepsilon) \log p \rceil \qquad \textit{and} \qquad r = \lceil 4m/\varepsilon \rceil$$

there is a deterministic polynomial time algorithm $\mathcal{A}$ as follows. For any $\alpha \in \mathbb{F}_{p^m}$, if $t_1, \ldots, t_r$ are chosen uniformly and independently at random from $\mathcal{G}$ and if $u_i = \mathrm{MSB}_{k,p}(\mathrm{Tr}(\alpha t_i))$ for $i = 1, \ldots, r$, the output of $\mathcal{A}$ on the $2r$ values (t_i, u_i) satisfies

$$\Pr_{t_1, \ldots, t_r \in \mathcal{G}} \left[\mathcal{A}(t_1, \ldots, t_r; u_1, \ldots, u_r) = \alpha \right] \ge 1 - p^{-1}.$$

3 Bit Security of Tripartite Diffie-Hellman

We have already described the tripartite Diffie-Hellman system of Joux. In that case an adversary sees $(P,Q),(aP,aQ),(bP,bQ)$ and (cP,cQ) and the key is derived from $\mathrm{Tr}(e(P,Q)^{abc}) \in \{0,1,\ldots,p-1\}$ (if distortion maps are used then $P=Q$, see [28]). In this section we study the bit security of keys obtained in this way. Later in this section we discuss the bit security of keys obtained from the protocols of Al-Riyami and Paterson [1].

Let $\omega_1,\ldots,\omega_m$ be a fixed basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and let $\vartheta_1,\ldots,\vartheta_m$ be the dual basis, that is,

$$\mathrm{Tr}(\vartheta_j\omega_i) = \begin{cases} 0, \text{ if } i \neq j; \\ 1, \text{ if } i = j; \end{cases}$$

see Section 2.3 of [20]. Then any element $\alpha \in \mathbb{F}_{p^m}$ can be represented in the basis $\omega_1,\ldots,\omega_m$ as

$$\alpha = \sum_{i=1}^{m} \mathrm{Tr}(\vartheta_i\alpha)\omega_i.$$

We now assume that there is an algorithm which can provide some information about one of the components $\mathrm{Tr}(\vartheta_i e(P,Q)^{abc})$ of the above representation and show that it leads to an efficient algorithm to compute the whole value $e(P,Q)^{abc}$ and hence the key $\mathrm{Tr}(e(P,Q)^{abc})$. It follows that the partial information about one of the components is as hard as the whole key.

To make this precise, for every $k>0$ we denote by $\mathcal{O}_k$ the oracle which, for some fixed $\vartheta \in \mathbb{F}_{p^m}^*$ and any $a,b,c \in [0,l-1]$, takes as input the pairs

$$(P,Q), \qquad (aP,aQ), \qquad (bP,bQ), \qquad (cP,cQ),$$

and outputs $\mathrm{MSB}_{k,p}\left(\mathrm{Tr}\left(\vartheta e(P,Q)^{abc}\right)\right)$.

We start with the case $m=2$ for which we obtain a result of the same strength as those known for the classical two-party Diffie–Hellman scheme over $\mathbb{F}_p$, see [7, 13]. Moreover, one can prove that there are infinitely many parameter choices to which our construction applies. Indeed, we know from [3] that there are infinitely many primes p such that $p+1$ has a prime divisor $l \geq p^{0.677}$. These arguments can be easily adjusted to show that the same holds for primes in the arithmetic progression $p \equiv 2 \pmod 3$. When $p \equiv 2 \pmod 3$, the elliptic curve given by the Weierstrass equation $Y^2 = X^3+1$ has $\#E(\mathbb{F}_p) = p+1$. Another infinite series of examples of $\#E(\mathbb{F}_p) = p+1$ can be obtained with primes $p \equiv 3 \pmod 4$ and the elliptic curve given by the Weierstrass equation $Y^2 = X^3 + X$, see [18].

Theorem 1. *Assume that p is an n-bit prime (for sufficiently large n) and l is the order of groups $\mathbb{G}_1$ and $\mathbb{G}_2$ such that $\gcd(l, p(p-1)) = 1$ and $l \geq p^{1/2+\rho}$ for some fixed $\rho > 0$. Then there exists a polynomial time algorithm which, given the pairs*

$$(P,Q), \qquad (aP,aQ), \qquad (bP,bQ), \qquad (cP,cQ)$$

for some $a,b,c \in \{0,\ldots,l-1\}$, makes $O(n^{1/2})$ calls of the oracle $\mathcal{O}_k$ with $k = \lceil 2n^{1/2} \rceil$ and computes $e(P,Q)^{abc}$ correctly with probability at least $1-p^{-1}$.

Proof. The case when $ab = 0$ is trivial. In the general case choose a random $d \in \{0, \ldots, l-1\}$ and call the oracle $\mathcal{O}_k$ on the pairs

$$(P, Q), \qquad (aP, aQ), \qquad (bP, bQ), \qquad ((c+d)P, (c+d)Q)$$

(the points $(c+d)P$ and $(c+d)Q$ can be computed from the values of cP, cQ and d). Let $\alpha = \vartheta e(P,Q)^{abc}$ be the hidden number and let $t = e(P,Q)^{abd}$ which can be computed as $t = e(aP, bQ)^d$. The oracle returns

$$\mathrm{MSB}_{k,p}\left(\mathrm{Tr}(\vartheta e(P,Q)^{ab(c+d)})\right) = \mathrm{MSB}_{k,p}\left(\mathrm{Tr}(\alpha t)\right).$$

Since l is prime and $ab \not\equiv 0 \pmod{l}$ it follows that the "multipliers" t are uniformly and independently distributed in $\mathcal{G}$, when the shifts d are chosen uniformly and independently at random from $\{0, \ldots, l-1\}$. Now from Lemma 1 we derive the result. ☐

Similarly, from Lemma 2 we derive:

Theorem 2. *Assume that p is an n-bit prime (for sufficiently large n) and l is the order of groups $\mathbb{G}_1$ and $\mathbb{G}_2$ such that $\gcd(l, p(p-1)) = 1$ and $l \geq p^\rho$ for some fixed $\rho > 0$. Then, for any $\varepsilon > 0$, there exists a polynomial time algorithm which, given the pairs*

$$(P, Q), \qquad (aP, aQ), \qquad (bP, bQ), \qquad (cP, cQ)$$

for some $a, b, c \in \{0, \ldots, l-1\}$, makes $O(\varepsilon^{-1})$ calls of the oracle $\mathcal{O}_k$ with $k = \lceil (1 - \rho/m + \varepsilon)n \rceil$ and computes $e(P,Q)^{abc}$ correctly with probability at least $1 - p^{-1}$.

We now consider the authenticated three party key agreement protocols of Al-Riyami and Paterson [1]. In this setting, users A, B and C have public keys aP, bP and cP and transmit ephemeral keys xP, yP and zP. The protocols TAK–1, TAK–2 and TAK–3 of [1] construct keys of the form

$$e(P,P)^{abc+xyz}, \qquad e(P,P)^{abz+acy+bcx}, \qquad e(P,P)^{xyc+xzb+yza}$$

respectively. If bitstrings are derived from these keys using the trace then results analogous to Theorems 1 and 2 are obtained.

We sketch the details in the case of TAK–2. Suppose $\mathcal{O}_k$ is an oracle which, on input $(P, aP, bP, cP, xP, yP, zP)$, outputs

$$\mathrm{MSB}_{k,p}(\mathrm{Tr}(\vartheta e(P,P)^{abz+acy+bcx}))$$

and let $\alpha = \vartheta e(P,P)^{abz+acy+bcx}$. Repeatedly choosing random w and calling $\mathcal{O}_k$ on $(P, aP, bP, cP, xP, yP, zP + wP)$ yields

$$\mathrm{MSB}_{k,p}(\mathrm{Tr}(\alpha t)) \qquad \text{where} \qquad t = e(aP, bP)^w.$$

It is straightforward to obtain analogues of of Theorems 1 and 2.

Al-Riyami and Paterson [1] also propose the protocol TAK–4, which is related to the MQV protocol. It is interesting to note that we are not able to give bit security results for keys obtained with this protocol.

4 Bit Security of Identity-based Key Exchange

The first identity-based key exchange protocol is due to Sakai, Ohgishi and Kasahara [24], but we consider the protocol of Smart [27] as it has better security properties.

The trusted authority defines two groups $\mathbb{G}_1$ and $\mathbb{G}_2$, chooses $P \in \mathbb{G}_2$ and a secret integer s, and publishes P and $P_{\text{pub}} = sP$. The identities of users A and B give rise to points $Q_A, Q_B \in \mathbb{G}_1$ (see Boneh and Franklin [4] for details about identity-based cryptography using pairings) and the trusted authority gives them sQ_A and sQ_B respectively.

The key agreement protocol is as follows. User A chooses a random integer a and transmits $T_A = aP$ to B. Similarly, user B transmits $T_B = bP$ to A. Both users can compute the common key

$$K = e(aQ_B + bQ_A, P_{\text{pub}})$$

for example user A computes $e(aQ_B, P_{\text{pub}})e(sQ_A, T_B)$. In practice, the key is derived from K using some key derivation function, which in this case we take to be the trace.

The bit security of this key-exchange protocol can be studied and results analogous to those above can be obtained. Suppose $\mathcal{O}_k$ is an oracle such that, for any $a, b, c \in [0, l-1]$, on input

$$(P, aP, bP, cP, Q_A, Q_B)$$

outputs $\text{MSB}_{k,p}\left(\text{Tr}(\vartheta e(aQ_B + bQ_A, cP)\right)$ for some fixed $\vartheta \in \mathbb{F}_{p^m}^*$. Let $\alpha = \vartheta e(aQ_B + bQ_A, P_{\text{pub}})$. Repeatedly choose random $d \in [0, l-1]$ and call the oracle $\mathcal{O}_k$ on

$$(P, T_A, T_B + dP, P_{\text{pub}}, Q_A, Q_B).$$

The oracle responses are of the form

$$\text{MSB}_{k,p}(\text{Tr}(\alpha t)) \quad \text{where} \quad t = e(Q_A, P_{\text{pub}})^d$$

and analogues of Theorems 1 and 2 are obtained.

5 Remarks

It remains an open problem to understand the bit security of keys obtained from the protocol TAK–4 of Al-Riyami and Paterson [1].

We remark that it would be valuable to extend our results (as well as the results of [5–7, 13, 14, 16, 19]) to case when the oracle works correctly only on a polynomially large fraction of all possible inputs. Unfortunately, at the moment it is not clear how to adjust the ideas of [7], underlying all further developments in this area, to work with such "unreliable" oracles.

It has been shown in [13] that for almost all primes p an analogue of Lemma 1 holds for subgroups $\mathcal{G} \in \mathbb{F}_p^*$ of cardinality $|\mathcal{G}| \geq p^\rho$, for any fixed $\rho > 0$. It is not immediately clear how to extend the underlying number theoretic techniques to extension fields, although this question definitely deserves further attention (see also the discussion in [26]).

Finally, we recall a different kind of bit security result (see [16]) concerning the value of the pairing $e(R,P)$ for an *unknown* point R, in case when $m = 1$ (although it is quite possible that the whole approach of [16] can be generalised to extension fields). In particular, if $l \ge p^{1/2+\rho}$ is a divisor of $p-1$, where $\rho > 0$ is fixed, then an oracle producing about $(1-\rho/5)\log p$ most significant bits of $e(R,P)$ for an *unknown* point $R \in \mathbb{G}_1$ and a *given* point $P \in \mathbb{G}_2$, can be used to construct a polynomial time algorithm to compute $e(R,P)$ exactly. It would be interesting to understand cryptographic implications of this result.

References

1. S. Al-Riyami and K. G. Paterson, 'Authenticated three party key agreement protocols from pairings', *Cryptology ePrint Archive: Report 2002/35*.
2. P. S. L. M. Barreto and B. Lynn and M. Scott, 'Constructing elliptic curves with prescribed embedding degrees', Proceedings of the Third Workshop on Security in Communication Networks (SCN'2002), Springer LNCS, to appear.
3. R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arithm.*, **83** (1998), 331–361.
4. D. Boneh and M. Franklin, 'Identity-based encryption from the Weil pairing', *Proc. Crypto'2001, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2139** (2001), 213–229.
5. D. Boneh, S. Halevi and N. A. Howgrave-Graham, 'The modular inversion hidden number problem', *Proc. Asiacrypt'2001, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2248** (2001), 36–51.
6. D. Boneh and I. E. Shparlinski, 'On the unpredictability of bits of the elliptic curve Diffie–Hellman scheme', *Proc. Crypto'2001, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2139** (2001), 201–212.
7. D. Boneh and R. Venkatesan, 'Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes', *Proc. Crypto'1996, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.
8. R. Dupont and A. Enge and F. Morain, 'Building curves with small MOV degree over finite prime fields', *Cryptology ePrint Archive, Report 2002/57*.
9. G. Frey and H.-G. Rück, 'A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves', *Math. Comp.*, **62** (1994), 865–874.
10. S. D. Galbraith, 'Supersingular curves in cryptography', *Proc. Asiacrypt'2001, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2248** (2001), 495–513 (full version is available from `http://www.isg.rhul.ac.uk/~sdg/`).
11. M. Goldman, M. Näslund and A. Russell 'Complexity bounds on general hard-core predicates', *J. Cryptology*, **14** (2001), 177–195.
12. M. I. González Vasco and M. Näslund, 'A survey of hard core functions', *Proc. Workshop on Cryptography and Computational Number Theory*, Singapore 1999, Birkhäuser, 2001, 227–256.
13. M. I. González Vasco and I. E. Shparlinski, 'On the security of Diffie–Hellman bits', *Proc. Workshop on Cryptography and Computational Number Theory*, Singapore 1999, Birkhäuser, 2001, 257–268.
14. M. I. González Vasco and I. E. Shparlinski, 'Security of the most significant bits of the Shamir message passing scheme', *Math. Comp.*, **71** (2002), 333–342.
15. J. Håstad and M. Näslund, 'The security of individual RSA and discrete log bits', *J. of the ACM*, (to appear).
16. N. A. Howgrave-Graham, P. Q. Nguyen and I. E. Shparlinski, 'Hidden number problem with hidden multipliers, timed-release crypto and noisy exponentiation', *Math. Comp.*, (to appear).
17. A. Joux, 'A one round protocol for tripartite Diffie–Hellman', *Proc. ANTS-4, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1838** (2000), 385–393.

18. A. Joux, 'The Weil and Tate pairings as building blocks for public key cryptosystems', *Proc. ANTS-5, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2369** (2002), 20–32.
19. W.-C. W. Li, M. Näslund and I. E. Shparlinski, 'The hidden number problem with the trace and bit security of XTR and LUC', *Proc. Crypto'2002, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2442** (2002) 433–448.
20. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
21. V. Miller, 'Short programs for functions on curves', *Preprint*, 1986.
22. A. J. Menezes, T. Okamoto and S. A. Vanstone, 'Reducing elliptic curve logarithms to logarithms in a finite field', *IEEE Trans. Inf. Theory*, **39** (1993) 1639–1646.
23. K. Rubin and A. Silverberg, 'Supersingular abelian varieties in cryptology', *Proc. Crypto'2002, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2442** (2002).
24. R. Sakai, K. Ohgishi and M. Kasahara, 'Cryptosystems based on pairing', Proc. of SCIS '00, Okinawa, Japan, 2000.
25. C. P. Schnorr, 'Security of almost all discrete log bits', *Electronic Colloq. on Comp. Compl.*, Univ. of Trier, **TR98-033** (1998), 1–13.
26. I. E. Shparlinski, 'On the generalized hidden number problem and bit security of XTR', *Proc. AAECC-14, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 268–277.
27. N. P. Smart, 'An identity based authenticated key agreement protocol based on the Weil pairing', *Electronics Letters*, **38** (2002), 630–632.
28. E. R. Verheul, 'Evidence that XTR is more secure than supersingular elliptic curve cryptosystems', *Proc. Eurocrypt'2001, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2045** (2001), 195–210.