On the Bit Security of the Diffie-Hellman Key

Ian F. Blake
Department of Electrical and Computer Engineering
University of Toronto, Toronto, ON M5S 3G4, Canada
ifblake@comm.toronto.edu

Theo Garefalakis
Department of Mathematics
University of Crete, 71409 Heraklion, Crete, Greece
theo@math.uoc.gr

Igor E. Shparlinski
Department of Computing
Macquarie University, Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

December 13, 2004

Abstract

Let $\mathbb{F}_p$ be a finite field of p elements, where p is prime. The bit security of the Diffie-Hellman function over subgroups of $\mathbb{F}_p^*$ and of an elliptic curve over $\mathbb{F}_p$, is considered. It is shown that if the Decision Diffie-Hellman problem is hard in these groups, then the two most significant bits of the Diffie-Hellman function are secure. Under the weaker assumption of the computational (rather than decisional) hardness of the Diffie-Hellman problems, only about $(\log p)^{1/2}$ bits are known to be secure.

Keywords Diffie-Hellman protocol, bit security, exponential sums

1 Introduction

Let $\mathcal{G}$ be a finite cyclic group of cardinality $\#\mathcal{G} = t$ with generator g. The *computational Diffie-Hellman problem*, or CDH problem, in $\mathcal{G}$ is the problem of computing g^{ab} from known values of g^a and g^b for two randomly chosen integers $a, b \in [0, t-1]$. Similarly, computing the function g^{ab} from g^a and g^b is referred to as the Diffie-Hellman function. A related problem to the CDH problem is the *decision Diffie-Hellman problem*, or DDH problem, which is the problem of deciding whether $c \equiv ab \pmod{t}$ for a given triple $\left(g^a, g^b, g^c\right)$. It is believed that in most groups of cryptographic interest, the DDH problem is not easier than the CDH problem (obviously it is not harder). This principle has however to be applied with caution, see [11].

These DH and the related discrete logarithm (DL) problems are of central importance to cryptography and in particular, to cryptographic protocols such as the DH key exchange and DL based encryption schemes. Much research has been devoted to establishing the precise nature of their complexity and relationships.

One aspect of the relationship is to note that even though the CDH or DDH problems may be hard in a certain group, it does not necessarily follow that some information on the problems, such as a few bits of the result sought, are hard to obtain. The motivation to study this question comes from private key derivation techniques. Typically, g^{ab} is hashed to a rather short bit string which constitutes the actual private key. Various approaches have been considered in the literature, and the reader is referred to [6] which establishes important results on this very question.

One however may ask what happens if instead of these sophisticated techniques one simply uses several of the most significant bits of an appropriate encoding of g^{ab}. For example, if it is only intended to use the 64 or 128 most significant bits of the Diffie-Hellman function as a key, it is of some importance to establish the difficulty of obtaining such partial information. It is vital to make sure that there is no loss of security in this procedure. Thus, it is natural to ask whether deriving some nontrivial information about the Diffie-Hellman function g^{ab} is as hard as computing the whole value g^{ab}. The above property of hardness of computing some bits of information about g^{ab} is called *bit security*.

Two specific groups which are used in cryptography for which the property of bit security is of special interest, are subgroups of $\mathbb{F}_p^*$ of prime order and subgroups of the group of points on certain elliptic curves, again of prime

order.

Let $\mathbb{F}_p$ be a finite field of p elements, where p is prime. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$, $p > 3$, given by an affine *Weierstrass equation* of the form

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

with coefficients $A, B \in \mathbb{F}_p$, such that $4A^3 + 27B^2 \neq 0$. We write every finite point $P \in \mathcal{E}(\mathbb{F}_p)$ as $P = (x(P), y(P))$ and recall that the set $\mathcal{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points on any elliptic curve $\mathcal{E}$ forms an Abelian group (with a point at infinity as the neutral element) and the cardinality of this group satisfies the Hasse–Weil bound

$$|\#\mathcal{E}(\mathbb{F}_p) - p - 1| \leq 2p^{1/2}, \tag{1}$$

see [2, 18] for this and some other general properties ofelliptic curves. Elements of $\mathbb{F}_p$ are denoted by the integers from the set $\{0, \ldots, p-1\}$.

The study of bit security of the Diffie-Hellman function g^{ab} has been pioneered by Boneh and Venkatesan [4]. Their work [4] has introduced an ingenious link between this problem and the closest vector problem in lattices, which has been used in many other works on this subject, see [1, 3, 7, 8, 9, 14, 15, 16, 17] and references therein. In order to give a brief notion of the genesis of this work, we note that [4] assumes the group of interest is the entire $\mathbb{F}_p^*$, that is, of order $p - 1$.

The results required equidistribution results for the solutions of certain equations and for smaller groups these are harder to establish. González Vasco and Shparlinski [9] have shown how the equidistribution properties can be proved in much smaller groups, specifically in subgroups of $\mathbb{F}_p^*$ of size at least $T \geq p^{1/3+\varepsilon}$, which has been a significant step forward. The proof of this result depended on obtaining suitable bounds for certain exponential sums over subgroups of $\mathbb{F}_p^*$ of interest.

In summary, the results of [4, 9, 17] show that about $(\log p)^{1/2}$ most significant bits of the Diffie-Hellman key are hard to recover if the CDH problem is hard. Certainly it is natural to try to reduce the number of bits which are hard to compute. In this direction, Blake and Garefalakis [1] have shown that already two bits are hard, however under a stronger assumption of the hardness of the DDH problem.

The proof of the central result of [1], showing that if the DDH problem is hard (in $\mathbb{F}_p^*$) then finding two bits of the Diffie-Hellman function is also hard, relied on the distribution result of [9] and hence the restriction on the size

of the group to $T \geq p^{1/3+\varepsilon}$ carried over to that work. Various improvements have been obtained on the size of the subgroup until the following surprising result of Bourgain and Konyagin [5]. This result asserts that there exist positive constants C_1 and C_2 such that for any $\varepsilon > 0$ and any subgroup G of $\mathbb{F}_p^*$ with $\#\mathcal{G} \geq p^{\varepsilon}$, we have

$$\max_{c \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{G}} \exp(2\pi i c u/p) \right| = O\left(\#\mathcal{G}\, p^{-\gamma}\right), \tag{2}$$

where $\gamma = \exp(C_1/\varepsilon^{C_2})$

This result on exponential sums can be carried over directly to extend equidistribution results, in particular of [9]. Here we use this result on smaller subgroups to reformulate and extend the results of [1] on two bits to smaller subgroups in a way that allows us to use the full power of the method of [1]. Thus the restriction in [1] to groups of size $T \geq p^{1/3+\varepsilon}$ is replaced by $T \geq p^{\varepsilon}$. Certainly this is close to the natural threshold beyond which the problem becomes void: if T is very small then CDH can be solved by the classical methods of Shank and Pollard.

We also obtain analogues of the results of [1] for subgroups $\mathcal{G}$ of point groups of elliptic curves, that is, it is shown that an oracle $\mathcal{O}_\eta$ capable of returning η of the most significant bits of $x(abQ)$ can resolve the DDH problem in k calls with probability at least $1 - 2^{-(\eta-1)k}$. This result, however, still requires an elliptic curve subgroup size of $T \geq p^{1/2+\varepsilon}$. We remark that for the Diffie-Hellman function on elliptic curves a bit security result of a slightly different flavor is given in [3].

In order to simplify the arguments and emphasize the new elements of the work, it is assumed the subgroups $\mathcal{G}$ are of prime order, which is certainly the most interesting case for cryptographic applications.

2 Distribution of Cyclic Subgroups of Finite Fields and Elliptic Curves

Let $\vartheta \in \mathbb{F}_p^*$ be a fixed element of order T. Given an element $\lambda \in \mathbb{F}_p^*$ and positive integers r, h, we denote by $N_\lambda(r, h)$ the number of solutions to the congruence

$$\lambda \vartheta^u \equiv v \pmod{p}, \qquad 0 \leq u \leq T-1,\ r+1 \leq v \leq r+h.$$

Similarly for elliptic curves, let $Q \in \mathcal{E}(\mathbb{F}_p)$ be a fixed point of order T. Given a point $L \in \mathcal{E}(\mathbb{F}_p)$ and positive integers r, h, we denote by $M_L(r,h)$ the number of solutions to the congruence

$$x(uQ + L) - x(uQ) \equiv v \pmod p, \qquad 0 \le u \le T-1,\ r+1 \le v \le r+h.$$

Results showing that both $N_\lambda(r,h)$ are $M_L(r,h)$ are close to their expected values are needed to establish the results of interest.

The following bound can be obtained from the results of [5] by using exactly the same technique of Lemma 2.1 in [9] (see also [15]) except that instead of the bound of exponential sums from [10, 13] the bound (2) is used, which applies to elements $\vartheta \in \mathbb{F}_p^*$ of extremely small orders).

Lemma 1. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $\vartheta \in \mathbb{F}_p^*$ of order $T \ge p^\varepsilon$ we have*

$$\max_{r,h} \max_{\gcd(\lambda,p)=1} \left| N_\lambda(r,h) - \frac{Th}{p} \right| = O(T^{1-\delta}).$$

For elliptic curves a similar result follows from the bound of exponential sums of [12]. Let $\mathcal{O}$ denote the point on infinity on an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$.

Lemma 2. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any point $Q \in \mathcal{E}(\mathbb{F}_p)$ of order $T \ge p^{1/2+\varepsilon}$ we have*

$$\max_{r,h} \max_{L \ne \mathcal{O}} \left| M_L(r,h) - \frac{Th}{p} \right| = O(T^{1-\delta}).$$

Proof. Let $\mathcal{H}$ be the subgroup of $\mathcal{E}(\mathbb{F}_p)$ generated by Q. We have

$$\begin{aligned} M_L(r,h) - \frac{(T-2)h}{p} & \\ = \frac{1}{p} \sum_{P \in \mathcal{H} - \{\mathcal{O}, -L\}} & \sum_{v=r+1}^{r+h} \sum_{c=1}^{p-1} \exp(2\pi i c(x(P+L) - x(P) - v)/p). \end{aligned}$$

It follows from [12] that

$$\left| \sum_{P \in \mathcal{H} - \{\mathcal{O}, -L\}} \exp(2\pi i c(x(P+L) - x(P))/p) \right| = O(p^{1/2}),$$

and

$$\sum_{c=1}^{p-1} \left| \sum_{v=r+1}^{r+h} \exp(2\pi ic(-v)/p) \right| \le p(1+\log p).$$

Therefore we get the bound

$$\left| M_L(r,h) - \frac{Th}{p} \right| = O\left(p^{1/2}\log p\right)$$

and since $T \ge p^{1/2+\varepsilon}$, the result follows. □

3 Main Results

For integers t, denote by $\lfloor t \rfloor_p$ the remainder of t on division by p.

For a real $\eta > 0$, denote by $\mathrm{APPR}_\eta(t)$ any integer u which satisfies the inequalities

$$|\lfloor t \rfloor_p - u| \le p2^{-1-\eta}. \tag{3}$$

Thus, roughly speaking, when η is large, $\mathrm{APPR}_\eta(t)$ is the integer defined by the approximately η most significant bits of $\lfloor t \rfloor_p$. However, this definition is more flexible and better suited to our purposes. In particular we remark that η in the inequality (3) need not be an integer. In fact in our applications η can be an arbitrary small positive number (although to establish meaningful probability bounds we will require $\eta > 1$).

For example, if p is an n-bit prime, and we consider that all residues modulo p have n-bit long representations (starting with extra zeros, if necessary), then two leading bits b_1, b_2 of any residue t can be used to find $\mathrm{APPR}_1(t)$:

$$|\lfloor t \rfloor_p - (2^{n-1}b_1 + 2^{n-2}b_2 + 2^{n-3})| \le 2^{n-3} \le p/4.$$

since $2^{n-1} \le p < 2^n$.

As in [1], we note that if, for example, $p = 2^n + 1$ is a Fermat prime or any other prime just a little larger than 2^n, then the traditional most significant bit of almost all residues is zero and thus carries almost no information.

Fix an element $g \in \mathbb{F}_p^*$. For a real $\eta > 0$ denote by $\mathcal{DH}_\eta$ an oracle, which given $\lfloor g^a \rfloor_p$ and $\lfloor g^b \rfloor_p$, outputs $\mathrm{APPR}_\eta(g^{ab})$. We now show that such an oracle can be used to solve the DDH problem for the group $\mathcal{G}$ of smaller order than previously established [1], generated by g.

Theorem 3. *Let $\varepsilon > 0$ be an arbitrary fixed real number. Assume $g \in \mathbb{F}_p$ is an element of multiplicative order $T \geq p^{\varepsilon}$ which is prime. There exists a probabilistic polynomial time algorithm, which for any triplet $(a, b, c) \in [1, T]^3$, given $\lfloor g^a \rfloor_p$, $\lfloor g^b \rfloor_p$, $\lfloor g^c \rfloor_p$, makes k calls to the oracle $\mathcal{DH}_\eta$, and decides if $ab \equiv c \pmod{T}$ with error probability $(1 + o(1))2^{-(\eta-1)k}$.*

Proof. Denote $\alpha = \left\lfloor g^{ab} \right\rfloor_p$, and $\gamma = \lfloor g^c \rfloor_p$. We wish to decide if $\alpha = \gamma$. The following steps are repeated k times.

1. Choose a random $u \in [1, T-1]$ and compute γg^{bu}.
2. Query the oracle $\mathcal{DH}_\eta$ on input (g^{a+u}, g^b).
3. Accept if and only if $\mathcal{DH}_\eta(g^{a+u}, g^b) = \mathrm{APPR}_\eta(\gamma g^{bu})$.

Clearly, if $\alpha = \gamma$ then $\left\lfloor \alpha g^{bu} \right\rfloor_p = \left\lfloor \gamma g^{bu} \right\rfloor_p$ for every $u \in \{1, \ldots, T-1\}$ and the algorithm always answers correctly in this case.

We now show that if $\alpha \neq \gamma$ the probability (taken over the random choices of $u \in \{1, \ldots, T-1\}$) that the algorithm errs is small. Indeed, the algorithm makes the wrong decision only if the approximations of $\left\lfloor \alpha g^{bu} \right\rfloor_p$ and $\left\lfloor \gamma g^{bu} \right\rfloor_p$ are the same, which implies that

$$\left| \left\lfloor \gamma g^{bu} \right\rfloor_p - \left\lfloor \alpha g^{bu} \right\rfloor_p \right| < p 2^{-\eta} \tag{4}$$

The inequality (4) is equivalent to

$$(\alpha - \gamma) g^{bu} \equiv v \pmod{p}, \qquad |v| < p 2^{-\eta}.$$

Since the decision problem is trivial for $b = T$ we assume that $1 \leq b < T$, so g^b has order T. Using Lemma 1, we see that the number of solutions to the last congruence is $T 2^{1-\eta} + O(T^{1-\delta})$ for some $\delta > 0$. Thus, the probability of error is $2^{1-\eta} + O(T^{-\delta})$.

Repeating the above experiment k times, with values of u chosen independently, and accepting if and only if every run accepts, we conclude that the probability of error is $2^{(1-\eta)k} + O(2^{(\eta-1)k} T^{-\delta k})$. Given the bound $T \geq p^{\varepsilon}$ the probability becomes $2^{(1-\eta)k} + O\left(2^{(\eta-1)k} p^{-\varepsilon\delta k}\right)$ which finishes the proof. $\square$

The application of the technique of [1] is now used to establish a similar result for subgroups of points on an elliptic curve. Fix a point $Q \in \mathcal{E}(\mathbb{F}_p)$ on an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$. For a real $\eta > 0$ we denote by $\mathcal{ECDH}_\eta$ an

oracle, which, given $\lfloor x(aQ) \rfloor_p$ and $\lfloor x(bQ) \rfloor_p$, outputs $\mathrm{APPR}_\eta(x(abQ))$. We now show that such an oracle can be used to solve the DDH problem for the group $\mathcal{G}$ generated by Q.

Theorem 4. *Let $\varepsilon > 0$ be an arbitrary fixed real number. Assume $Q \in \mathcal{E}(\mathbb{F}_p)$ is a point of order $T \geq p^{1/2+\varepsilon}$ which is prime. There exists a probabilistic polynomial time algorithm, which for any triplet $(a, b, c) \in [1, T]^3$, given Q, aQ, bQ, cQ, makes k calls to the oracle $\mathcal{ECDH}_\eta$, and decides if $ab \equiv c \pmod{T}$ with error probability $(1 + o(1))2^{-(\eta-1)k}$.*

Proof. Let $a, b, c \in [1, T]$, where T is prime. Then $ab \equiv c \pmod{T}$ if and only if $abQ = cQ$. If $r \in [1, T]$ then obviously $abQ = cQ$ is equivalent to $uQ + L = uQ$ where $L = abQ - cQ$ and $uQ = cQ + rbQ$, and clearly L is fixed (for any given values of a, b and c) and u runs through $[1, T]$ as r runs through the same set.

If $ab \equiv c \pmod{p}$ then $uQ + L = uQ$ and therefore $x(uQ + L) \equiv x(uQ) \pmod{p}$ for every value of $u \in [1, T]$. If, on the other hand, $ab \not\equiv c \pmod{T}$ then $x(uQ+L) \not\equiv x(uQ) \pmod{p}$ except for one value of u (for which $2uQ = -L$ since then $x(uQ) \equiv x(-uQ) \equiv x(uQ + L) \pmod{p}$). One would expect this inequality to be reflected in the most significant bits of $x(uQ + L)$ and $x(uQ)$ for many values of u. The important observation is that the point $uQ + L$ can be realized as the Diffie-Hellman function, and an approximation of its x-coordinate can be given by the oracle.

Assume now that $ab \not\equiv c \pmod{p}$, which implies that $L \neq \mathcal{O}$. Considering the values of $u \in [1, T]$ for which $\mathrm{APPR}_\eta(x(uQ + L)) = \mathrm{APPR}_\eta(x(uQ)) = B$ we have

$$x(uQ + L) \equiv v_1 \pmod{p} \quad \text{and} \quad x(uQ) \equiv v_2 \pmod{p},$$

where

$$\begin{aligned} |v_1 - B| &\leq p2^{-1-\eta} \\ |v_2 - B| &\leq p2^{-1-\eta}, \end{aligned}$$

and we have

$$\begin{aligned} x(uQ + L) - x(uQ) &\equiv v \pmod{p}, \\ 0 \leq u \leq T - 1, \quad -p2^{-\eta} &\leq v \leq p2^{-\eta}. \end{aligned} \tag{5}$$

Lemma 2 now implies that the number of u and v in the above range that satisfy (5) is $T2^{1-\eta}+O(T^{1-\delta})$. Since v is uniquely determined by u, if r (and therefore u) is chosen uniformly at random from $[1, T-1]$ the probability that v is in the range $[-p2^{\eta}, p2^{\eta}]$ is $2^{1-\eta}+O(T^{-\delta})$.

The basic steps of the algorithm are

1. Choose $r \in [1, T]$ and compute $Q_1 = cQ + rbQ$.
2. Query the oracle $\mathcal{ECDH}_{\eta}$ on input $(x(aQ + rQ), x(bQ))$.
3. Accept if and only if $\mathcal{ECDH}_{\eta}(x(aQ + rQ), x(bQ)) = \mathrm{APPR}_{\eta}(x(Q_1))$.

Repeating the above experiment k times, with values of r chosen independently, and accepting if and only if every run accepts, we conclude that the probability of error is $2^{(1-\eta)k} + O(2^{(\eta-1)k}T^{-\delta k})$. Given the bound $T \geq p^{1/2+\varepsilon}$ the probability becomes $2^{(1-\eta)k} + O\left(2^{(\eta-1)k}p^{-(1/2+\varepsilon)\delta k}\right)$ which finishes the proof. □

4 Comments

This paper has significantly extended the results of [1] in two directions:

- It is observed that the elegant result of Bourgain and Konyagin [5] on bounds for exponential sums over small subgroups, can be directly applied to obtain the necessary equidistribution results and hence extends the result of [1] to almost arbitrary subgroups of $\mathbb{F}_p^*$, in particular to groups of size $T \geq p^{\varepsilon}$ rather than $T \geq p^{1/3+\varepsilon}$ as in [1].
- Given the equidistribution result on elliptic curves, implied by [12], the technique of [1] is used to establish a similar result to resolve the DDH problem with high probability, that is, given an oracle that returns the $\eta > 1$ most significant bits of the x-coordinates of abQ, on input aQ and bQ.

It seems not known at this point how to reduce the group size for the elliptic curve problem, from $T \geq p^{1/2+\varepsilon}$ as is done for the case of $\mathbb{F}_p$. On the other hand, one can easily obtain similar results for y-coordinates and for many other natural functions on points on elliptic curves.

It seems clear that the technique of [1] can also be applied to other related Diffie-Hellman variants such as XTR and LUC. The bit security of these is considered in [14] where, in particular, the security of the $\log^{1/2} p$ most significant bits is proved for the XTR variant of the Diffie-Hellman protocol. The techniques of this work carry over to establish similarly improved results for that case. Combining the approach of [1] with the method of [8], one can consider the case of so-called noisy oracles which output a correct result only with certain probability.

Finally, it would be interested to obtain analogues of the above results for the case of binary fields $\mathbb{F}_{2^n}$ or other extension fields of small characteristic. In this case, a slightly different technique can be applied (see [7, 16]).

Acknowledgment: The authors would like to thank the two anonymous reviewers for their careful reading of the manuscript and helpful suggestions.

References

[1] I. F. Blake and T. Garefalakis, 'On the complexity of the discrete logarithm and Diffie-Hellman problems', *J. Compl.*, **20** (2004), 148–170.

[2] I. F. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc., Lecture Note Series, Vol.265, Cambridge Univ. Press, 1999.

[3] D. Boneh and I. E. Shparlinski, 'On the unpredictability of bits of the elliptic curve Diffie–Hellman scheme', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2139** (2001), 201–212.

[4] D. Boneh and R. Venkatesan, 'Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.

[5] J. Bourgain and S. V. Konyagin, 'Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order', *Comptes Rendus Mathematique*, **337** (2003), 75–80.

[6] R. Gennaro, H. Krawczyk and T. Rabin, 'Hashed Diffie-Hellman over non-DDH groups', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3027** (2004), 361–381.

[7] M. I. González Vasco, M. Näslund and I. E. Shparlinski, 'The hidden number problem in extension fields and its applications', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2286** (2002), 105–117.

[8] M. I. González Vasco, M. Näslund and I. E. Shparlinski, 'New results on the hardness of Diffie-Hellman bits', *Proc. Intern. Workshop on Public Key Cryptography, Singapore, 2004*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **2947** (2004), 159–172.

[9] 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.

[10] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Ouart. J. Math.*, **51** (2000), 221–235.

[11] A. Joux and K. Nguyen, 'Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups', *J. Cryptology*, **16** (2003), 239–247.

[12] D. R. Kohel and I. E. Shparlinski, 'Exponential sums and group generators for elliptic curves over finite fields', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1838** (2000), 395–404.

[13] S. V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[14] W.-C. W. Li, M. Näslund and I. E. Shparlinski, 'The hidden number problem with the trace and bit security of XTR and LUC', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2442** (2002), 433–448.

[15] I. E. Shparlinski, *Cryptographic applications of analytic number theory*, Birkhäuser, 2003.

[16] I. E. Shparlinski, 'Security of polynomial transformations of the Diffie–Hellman key', *Finite Fields and Their Appl.*, **10** (2004), 123–131.

[17] I. E. Shparlinski and A. Winterhof, 'Hidden number problem in small subgroups', *Cryptology ePrint Archive, Report 2003/49*, 2003, 1–12.

[18] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.