# Hidden Number Problem in Small Subgroups

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

Arne Winterhof
Temasek Laboratories, National University of Singapore
10 Kent Ridge Crescent, Singapore 119260, Singapore
tslwa@nus.edu.sg

March 13, 2003

**Abstract**

Boneh and Venkatesan have proposed a polynomial time algorithm for recovering a "hidden" element $\alpha \in \mathbb{F}_p$, where $p$ is prime, from rather short strings of the most significant bits of the residue of $\alpha t$ modulo $p$ for several randomly chosen $t \in \mathbb{F}_p$. González Vasco and the first author have recently extended this result to subgroups of $\mathbb{F}_p^*$ of order at least $p^{1/3+\varepsilon}$ for all $p$ and to subgroups of order at least $p^\varepsilon$ for almost all $p$. Here we introduce a new modification in the scheme which amplifies the uniformity of distribution of the 'multipliers' $t$ and thus extend this result to subgroups of order at least $(\log p)/(\log \log p)^{1-\varepsilon}$ for all primes $p$. As in the above works, we give applications of our result to the bit security of the Diffie–Hellman secret key starting with subgroups of very small size, thus including all cryptographically interesting subgroups.

**Keywords:** Hidden number problem, Diffie-Hellman key exchange, Lattice reduction, Exponential sums, Waring problem in finite fields

# 1 Introduction

For a prime $p$, denote by $\mathbb{F}_p$ the field of $p$ elements and always assume that it is represented by the set $\{0, 1, \dots, p-1\}$. Accordingly, sometimes, where obvious, we treat elements of $\mathbb{F}_p$ as integer numbers in the above range.

For a real $\eta > 0$ and $t \in \mathbb{F}_p$ we denote by $\mathrm{MSB}_\eta(t)$ any integer which satisfies the inequality

$$|t - \mathrm{MSB}_\eta(t)| < p2^{-\eta-1}. \qquad (1)$$

Roughly speaking, $\mathrm{MSB}_\eta(t)$ is an integer having about $\eta$ most significant bits as $t$ (taking into account our convention about the elements of $\mathbb{F}_p$). However, this definition is more flexible and better suited to our purposes. In particular we remark that $\eta$ in the inequality (1) need not be an integer.

Given a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ we consider the following *hidden number problem* over $\mathcal{G}$:

> *Recover a number $\alpha \in \mathbb{F}_p$ such that for $k$ elements $t_1, \dots, t_d \in \mathcal{G}$, chosen independently and uniformly at random from $\mathcal{G}$, we are given $k$ pairs*
>
> $$(t_h, \mathrm{MSB}_\eta(\alpha t_h)), \qquad h = 1, \dots, d,$$
>
> *for some $\eta > 0$.*

For $\mathcal{G} = \mathbb{F}_p^*$ this problem has been introduced and studied by Boneh and Venkatesan [1, 2]. In [1] a polynomial time algorithm is designed which recovers $\alpha$ for some $\eta \sim (\log p)^{1/2}$ and $k = O(\log^{1/2} p)$. The algorithm of [1] has been extended in several directions. In particular, in [5] it is generalised to all sufficiently large subgroups $\mathcal{G} \subseteq \mathbb{F}_p^*$. This and other generalisations have led to a number of cryptographic applications, see [20, 21, 22]. Using bounds of exponential sums from [7, 10] it has been shown that the algorithm of [1] works for subgroups $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order $\#\mathcal{G} \geq p^{\nu+\varepsilon}$ where for any $\varepsilon > 0$ and sufficiently large $Q$ one can take

- $\nu = 1/3$ for all primes $p \in [Q, 2Q]$,
- $\nu = 0$ for all primes $p \in [Q, 2Q]$, except at most $Q^{5/6+\varepsilon}$ of them.

Using a recent improvement of [9] of the bounds of exponential sums one can obtain the same result with

- $\nu = 1/4$ for all primes $p \in [Q, 2Q]$,
- $\nu = 0$ for all primes $p \in [Q, 2Q]$, except at most $Q^{3/4+\varepsilon}$ of them.

However, in practical applications one would probably choose a subgroup of order about $\exp\left(c(\log p)^{1/3}(\log\log p)^{2/3}\right)$ for some constant $c > 0$ in order to balance complexities of the number field sieve based attacks and Pollard's rho-method based attacks, see [6, 13, 16, 17, 23].

Here we extend the algorithm of [1] to the case of almost arbitrary subgroups $\mathcal{G} \subseteq \mathbb{F}_p^*$. More precisely, our result applies to any subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of size $\#\mathcal{G} \geq \log p/(\log\log p)^{1-\varepsilon}$, thus it includes all subgroups of cryptographically interesting sizes. As in [1], our method is based on lattice reduction algorithms and also makes use of exponential sums, however not in such a direct way as in [5]. Namely, we introduce certain new arguments allowing to amplify the uniformity of distribution properties of small subgroups $\mathcal{G}$. This allows us to use the bound of exponential sums from [8] with elements of $\mathcal{G}$, which is very moderate in strength (and does not imply any uniformity of distribution properties of $\mathcal{G}$ which would be the crucial argument of the method of [5]). The bound of [8] has however the very important advantage over the bounds of [7, 9, 10] that it applies to subgroups of order $\#\mathcal{G} \geq \log p/(\log\log p)^{1-\varepsilon}$. It is interesting to note that our approach has links with the famous *Waring problem* which has been studied in number theory for several hundred years. In fact, the Waring problem in finite fields has been the main motivation of the bound of exponential sums of [8] which we use in this paper. For surveys of recent results on this problem see [3, 8, 24]. As in [1, 5] we apply our algorithm for the hidden number problem to derive a bit security result for the Diffie-Hellman scheme.

We hope that similar ideas can be used for several other variants of the hidden number problem and its applications, see [20, 21, 22]. On the other hand, it should be remarked that our approach requires an increase in the number of oracle calls (which remains polynomial nevertheless, in particular it never exceeds $(\log p)^4$).

Throughout the paper $\log x$ always denotes the binary logarithm of $x > 0$ and the constants in the 'O'-symbols may occasionally, where obvious, depend on a small positive parameter $\varepsilon$ and are absolute otherwise. We always assume that $p$ is a prime number with $p \geq 5$, thus the expressions $\log\log p$ and $\log\log\log p$ are defined (and positive).

**Acknowledgements:** The first author was supported in part by

ARC grant DP0211459. The second author was supported in part by DSTA grant R-394-000-011-422.

## 2 Exponential sums and distribution of short sums of elements of subgroups

For a complex $z$ we put $\mathbf{e}_p(z) = \exp(2\pi i z/p)$.

Let $T = \#\mathcal{G}$, $T|(p-1)$, be the cardinality of a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$. If we put $n = (p-1)/T$ then each element $r \in \mathcal{G}$ has exactly $n$ representations $r = x^n$ with $x \in \mathbb{F}_p^*$. Therefore, for any $\lambda \in \mathbb{F}_p$,

$$\sum_{r\in\mathcal{G}} \mathbf{e}_p(\lambda r) = \frac{T}{p-1} \sum_{x\in\mathbb{F}_p^*} \mathbf{e}_p(\lambda x^n).$$

Now by Theorem 1 of [8] we have the following bound, see also [3, 9, 10].

**Lemma 1.** *For any $1 > \varepsilon > 0$ there exists a constant $c(\varepsilon) > 0$ such that for any subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order*

$$T \ge \frac{\log p}{(\log\log p)^{1-\varepsilon}}$$

*the bound*

$$\max_{\gcd(\lambda,p)=1} \left| \sum_{r\in\mathcal{G}} \mathbf{e}_p(\lambda r) \right| \le T\left(1 - \frac{c(\varepsilon)}{(\log p)^{1+\varepsilon}}\right)$$

*holds.*

For an integer $k \ge 1$, a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ and $t \in \mathbb{F}_p$ we denote by $N_k(\mathcal{G}, t)$ the number of solutions of the equation

$$r_1 + \ldots + r_k \equiv t \pmod p, \qquad r_1, \ldots, r_k \in \mathcal{G}.$$

Recalling the relation between the set of $n$th powers, where $n = (p-1)/T$, we see that studying the above congruence is equivalent to studying the congruence

$$x_1^n + \ldots + x_k^n \equiv t \pmod p, \qquad x_1, \ldots, x_k \in \mathbb{F}_p^*.$$

The problem of finding the smallest possible value of $k$ for which the congruence (or in more traditional settings the corresponding equation over $\mathbb{Z}$) has a solution for any $t$ is known as the Waring problem. However for our purposes just a solvability is not enough. Rather we need an asymptotic formula for the number of solutions.

We show that Lemma 1 can be used to prove that for reasonably small $k$, $N_k(\mathcal{G}, t)$ is close to its expected value.

**Lemma 2.** *For any $1 > \varepsilon > 0$ there exists a constant $C(\varepsilon) > 0$ such that for any subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$, of order*

$$T \ge \frac{\log p}{(\log\log p)^{1-\varepsilon}}$$

*the bound*

$$\max_{t \in \mathbb{F}_p} \left| N_k(\mathcal{G}, t) - \frac{T^k}{p} \right| \le \frac{T^k}{p^2}$$

*holds for any integer $k \ge C(\varepsilon)(\log p)^{2+\varepsilon}$.*

*Proof.* The well-known identity (see for example [12, Chapter 5.1])

$$\sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda u) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod p, \\ p, & \text{if } u \equiv 0 \pmod p, \end{cases}$$

implies that

$$\begin{aligned} N_k(\mathcal{G}, a) &= \sum_{r_1, \ldots, r_k \in \mathcal{G}} \frac{1}{p} \sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(\lambda(r_1 + \ldots + r_k - t)\right) \\ &= \frac{1}{p} \sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(-\lambda t\right) \left( \sum_{r \in \mathcal{G}} \mathbf{e}_p\left(\lambda r\right) \right)^k . \end{aligned}$$

Separating the term $T^k/p$, corresponding to $\lambda = 0$, and applying Lemma 1 to other terms, we obtain

$$\max_{t \in \mathbb{F}_p} \left| N_k(\mathcal{G}, t) - \frac{T^k}{p} \right| \le T^k \left( 1 - \frac{c(\varepsilon)}{(\log p)^{1+\varepsilon}} \right)^k = T^k \exp\left( O\left( k (\log p)^{-1-\varepsilon} \right) \right)$$

and the desired result follows. $\square$

## 3 Uniform distribution and hidden number problem

First of all we recall the classical definition of the *discrepancy* $\mathcal{D}(\Gamma)$ of an $N$-element sequence $\Gamma = (\gamma_1, \dots, \gamma_N)$ of elements of the interval $[0,1]$:

$$\mathcal{D}(\Gamma) = \sup_{J \subseteq [0,1]} \left| \frac{A(J,N)}{N} - |J| \right|,$$

where the supremum is extended over all subintervals $J$ of $[0,1]$, $|J|$ is the length of $J$, and $A(J,N)$ denotes the number of points $\gamma_n$ in $J$ for $0 \le n \le N-1$. Informally speaking the discrepancy tells us how much the number of hits $A(J,N)$ of a given interval $J$ differs from its expected value $|J|N$.

Now, following [14] we say that a finite sequence $\mathcal{T}$ of elements of $\mathbb{F}_p$ is $\Delta$-*homogeneously distributed modulo* $p$ if for any integer $\lambda$ with $\gcd(\lambda, p) = 1$, the discrepancy of the sequence of fractions $(\lambda t/p)_{t \in \mathcal{T}}$ is at most $\Delta$ (we certainly assume that $\lambda t \in \mathbb{F}_p$ and thus is reduced modulo $p$ and all these points belong to $[0,1]$).

The following statement is a generalization of Theorem 1 of [1] and is given in [14] as Lemma 4.

**Lemma 3.** *Let $\omega > 0$ be an arbitrary absolute constant. For a prime $p$, define*

$$\eta = \omega \left( \frac{\log p \log\log\log p}{\log\log p} \right)^{1/2} \qquad \textit{and} \qquad d = \left\lceil 3\eta^{-1} \log p \right\rceil.$$

*Let $\mathcal{T}$ be a $2^{-\eta}$-homogeneously distributed modulo $p$ sequence of integer numbers. There exists a probabilistic polynomial-time algorithm $\mathcal{A}$ such that for any $\alpha \in \mathbb{F}_p$ given $2d$ integers*

$$t_h \qquad \textit{and} \qquad u_h = \mathrm{MSB}_\eta(\alpha t_h), \qquad h = 1, \dots, d,$$

*its output satisfies for sufficiently large $p$*

$$\Pr\left[\mathcal{A}(p, t_1, \dots, t_d; u_1, \dots, u_d) = \alpha\right] \ge 1 - \frac{1}{p}$$

*where the probability is taken over all $t_1, \dots, t_d$ chosen uniformly and independently at random from the elements of $\mathcal{T}$ and all coin tosses of the algorithm $\mathcal{A}$.*

# 4 Hidden Number Problem in Subgroups

Assume that for $\alpha \in \mathbb{F}_p^*$ and a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order $T$, generated by $g \in \mathbb{F}_p^*$, we are given an *oracle* $\mathcal{HNP}_\mu$ such that for every $x \in \{0, 1, \ldots, T-1\}$, it returns $\mathrm{MSB}_\mu(\alpha g^x)$.

**Theorem 4.** *Let $\vartheta > 0$ be an arbitrary absolute constant and let*

$$\mu = \vartheta \left( \frac{\log p \log\log\log p}{\log\log p} \right)^{1/2}.$$

*There exists a polynomial time probabilistic algorithm which, for any $1 > \varepsilon > 0$ and any $g \in \mathbb{F}_p^*$ of order*

$$T \geq \frac{\log p}{(\log\log p)^{1-\varepsilon}},$$

*makes $O\left(\mu^{-1}(\log p)^{3+\varepsilon}\right)$ calls of the oracle $\mathcal{HNP}_\mu$ and then recovers $\alpha$ with probability at least $1 + O\left(2^{-\mu/2}\right)$.*

*Proof.* For integers $w$ we denote by $\lfloor w \rfloor_p$ the remainder of $w$ on division by $p$. Take $C(\varepsilon)$ from Lemma 2, $d$ from Lemma 3, and put

$$k = \left\lceil C(\varepsilon)(\log p)^{2+\varepsilon} \right\rceil, \qquad \eta = 2\mu/3, \qquad d = \left\lceil 3\eta^{-1} \log p \right\rceil.$$

Then by Lemma 2 the sequence

$$\mathcal{T} = (r_1 + \ldots + r_k \ \mid \ r_1, \ldots, r_k \in \mathcal{G})$$

of $k$-sums of elements of $\mathcal{G}$ is $2^{-\eta}$-homogeneously distributed modulo $p$. Now we call the oracle $\mathcal{HNP}_\mu$ for $dk$ uniformly and independently at random chosen

$$r_{11}, \ldots, r_{1k}, \ldots, r_{d1}, \ldots, r_{dk} \in \mathcal{G}$$

and get integers $u_{hj}$ with

$$\left| \lfloor \alpha r_{hj} \rfloor_p - u_{hj} \right| < p/2^{\mu+1}, \qquad h = 1, \ldots, d, \ j = 1, \ldots, k.$$

For $h = 1, 2, \ldots, d$ we put

$$v_h = \sum_{j=1}^{k} \lfloor \alpha r_{hj} \rfloor_p, \qquad t_h = \left\lfloor \sum_{j=1}^{k} r_{hj} \right\rfloor_p, \qquad u_h = \sum_{j=1}^{k} u_{hj}.$$

(where we used addition over $\mathbb{Z}$).

Note that for sufficiently large $p$,

$$|v_h - u_h| < kp/2^{\mu+1} \le p/2^{\eta+1}.$$

Next, we have

$$v_h - u_h - \lfloor v_h \rfloor_p + \lfloor u_h \rfloor_p = \nu p \quad \text{with } \nu \in \{-1, 0, 1\}.$$

If $\nu = 1$ then we have

$$\lfloor v_h \rfloor_p - \lfloor u_h \rfloor_p + p = |v_h - u_h| < p/2^{\eta+1}$$

which is only possible if $\lfloor v_h \rfloor_p > p - p/2^{\eta+1}$. If $\nu = -1$ then we have

$$\lfloor u_h \rfloor_p - \lfloor v_h \rfloor_p + p = |v_h - u_h| < p/2^{\eta+1}$$

which is only possible if $\lfloor v_h \rfloor_p < p/2^{\eta+1}$. If $\nu = 0$ then we have

$$|\lfloor \alpha t_h \rfloor_p - \lfloor u_h \rfloor_p| = |\lfloor v_h \rfloor_p - \lfloor u_h \rfloor_p| = |v_h - u_h| < \frac{p}{2^{\eta+1}}.$$

By Lemma 2, the probability that $p/2^{\eta+1} \le \lfloor v_h \rfloor_p \le p - p/2^{\eta+1}$ for all $h = 1, \ldots, d$ is $1 + O\left(d2^{-\eta}\right)$. Now the algorithm of Lemma 3 yields the correct $\alpha$ with probability at least $1 + O\left(d2^{-\eta} + p^{-1}\right) = 1 + O\left(2^{-\mu/2}\right)$ if $p$ is sufficiently large. □

# 5 Bit Security of the Diffie-Hellman scheme

As in [1, 5] we now apply Theorem 4 to derive a bit security result for the Diffie-Hellman scheme.

We assume that for a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ we are given an oracle $\mathcal{DH}_\mu$ which, given the values of $X = g^x \in \mathbb{F}_p$ and $Y = g^y \in \mathbb{F}_p$, outputs the value of $\mathrm{MSB}_\mu\left(g^{xy}\right)$. Repeating the same arguments of [5] we derive the following result.

**Theorem 5.** *Let $\vartheta > 0$ be an arbitrary absolute constant and let*

$$\mu = \vartheta \left(\frac{\log p \log\log\log p}{\log\log p}\right)^{1/2}.$$

*There exists a polynomial time probabilistic algorithm which, for any $1 > \varepsilon > 0$ and any $g \in \mathbb{F}_p^*$ of order*

$$T \geq (\log p)^{1+\varepsilon}$$

*which for any pair $(a, b) \in \{0, 1, \ldots, T-1\}^2$, given the values of $A = g^a \in \mathbb{F}_p$ and $B = g^b \in \mathbb{F}_p$, makes $O\left(\mu^{-1}(\log p)^{3+\varepsilon}\right)$ calls of the oracle $\mathcal{DH}_\mu$ and computes $g^{ab}$ correctly with probability $1 + O\left(2^{-\mu/2} + T^{-\varepsilon/2}\right)$.*

*Proof.* As in [5], given a pair $(a, b) \in \{0, 1, \ldots, T-1\}^2$ let us select an integer $s \in \{0, 1, \ldots, T-1\}$ uniformly at random. We compute

$$g_s = Bg^s$$

thus $g_s = g^{b+s}$.

Let $\Delta = T^{\varepsilon/(1+\varepsilon)}$. The probability that $\gcd(b+s, T) \geq \Delta$ is at most $\tau(T)/\Delta$, where $\tau(T)$ is the number of positive integer divisors of $T$. Indeed, for any divisor $D|T$ with $D \geq \Delta$ there are at most $T/D \leq T/\Delta$ values of $x \in \{0, 1, \ldots, T-1\}$ with $\gcd(x, T) = D$.

Using the bound $\tau(T) = T^{o(1)}$, see [15, Chapter 1, Theorem 5.2], we obtain that the probability of $\gcd(b+s, T) \geq \Delta$ is at most $T^{-\varepsilon/2}$.

In the opposite case, when $\gcd(b+s, T) < \Delta$, the multiplicative order of $g_s$ is

$$T_s = \frac{T}{\gcd(b+s, T)} > \frac{\log p}{(\log\log p)^{1-\varepsilon}}.$$

Put $\alpha_s = g^{a(b+s)}$. Now we can call the oracle $\mathcal{DH}_\mu$ with $g^x A = g^{x+a}$ and $g_s$ to evaluate

$$\mathrm{MSB}_\mu\left(g^{(a+x)(b+s)}\right) = \mathrm{MSB}_\mu\left(\alpha_s g_s^x\right)$$

for an integer $x$ chosen uniformly at random in the set $\{0, 1, \ldots, T-1\}$. Because $T_s|T$ the values of $x$ are uniformly distributed modulo $T_s$ as well, thus Theorem 4 can be applied, producing the desired result. $\square$

# 6 Remarks

It seems very plausible that the same approach can be applied to the hidden number problem over extension fields which is related to proving bit security of XTR and LUC protocols, see [11, 19], as well as of some tripartite key exchange protocol on elliptic curves, see [4]. In particular, for this purpose one can probably use a very weak bound of [18] which however applies to very small subgroups.

As in [1, 5], Theorem 4 can be applied to a number of other cryptographic protocols, for example to the ElGamal cryptosystem.

In [2] a *nonuniform* algorithm has been constructed which works with much smaller values $\eta \sim \log \log p$. This means that if the points $t_1, \ldots, t_d \in \mathcal{G}$ are known in advance, one can design (in exponential time) a certain data structure, that now given $d$ values $\mathrm{MSB}_\eta(\alpha t_h)$, $h = 1, \ldots, d$, the hidden number $\alpha$ can be found in polynomial time. In principle our approach can be used to extend the algorithm of [2], as well. However, this algorithm works only for almost all $\alpha \in \mathbb{F}_p$ rather than for all of them.

# References


[1] 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.

[2] D. Boneh and R. Venkatesan, 'Rounding in lattices and its cryptographic applications', *Proc. 8th Annual ACM-SIAM Symp. on Discr. Algorithms*, SIAM, 1997, 675–681.

[3] T. Cochrane, C. Pinner and J. Rosenhouse, 'Bounds on exponential sums and the polynomial Waring's problem $\mod p$', *Proc. Lond. Math. Soc.*, (to appear).

[4] S. D. Galbraith, H. J. Hopkins and I. E. Shparlinski, 'Secure bilinear Diffie-Hellman bits', *Cryptology ePrint Archive, Report 2002/155*, 2002, 1–8.

[5] 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.

[6] R. Crandall and C. Pomerance, *Prime numbers: A Computational perspective*, Springer-Verlag, Berlin, 2001.

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

[8] S. V. Konyagin, 'On estimates of Gaussian sums and the Waring problem modulo a prime', *Trudy Matem. Inst. Acad. Nauk USSR*, Moscow, **198** (1992), 111–124 (in Russian); translation in *Proc. Steklov Inst. Math.*, **1** (1994), 105–117.

[9] S. V. Konyagin, 'Bounds of exponential sums over subgroups and Gauss sums', *Preprint*, 2002, 1–25 (in Russian).

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

[11] 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.

[12] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, (1997).

[13] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.

[14] P. Q. Nguyen and I. E. Shparlinski, 'The insecurity of the digital signature algorithm with partially known nonces', *J. Cryptology*, **15** (2002), 151–176.

[15] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

[16] O. Schirokauer, 'Discrete logarithms and local units', *Philos. Trans. Roy. Soc. London, Ser. A*, **345** (1993), 409–423.

[17] O. Schirokauer, D. Weber and T. Denny, 'Discrete logarithms: The effectiveness of the index calculus method', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1122** (1996), 337–362.

[18] I. E. Shparlinski, 'On exponential sums with sparse polynomials', *J. Number Theory*, **60** (1996), 233–244.

[19] I. E. Shparlinski, 'On the generalised hidden number problem and bit security of XTR', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 268–277.

[20] I. E. Shparlinski, 'Playing "Hide-and-Seek" in finite fields: Hidden number problem and its applications', *Proc. 7th Spanish Meeting on Cryptology and Information Security, Vol.1*, Univ. of Oviedo, 2002, 49–72.

[21] I. E. Shparlinski, 'Exponential sums and lattice reduction: Applications to cryptography', *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer-Verlag, Berlin, 2002, 286–298.

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

[23] D. R. Stinson, *Cryptography: Theory and practice*, CRC Press, Boca Raton, FL, 2002.

[24] A. Winterhof, 'On Waring's problem in finite fields', *Acta Arith.*, **87** (1998), 171–177.