Security of the Most Significant Bits of the Shamir Message Passing Scheme

Maria Isabel González Vasco
Department of Mathematics, University of Oviedo
Oviedo, 33007, Spain
mvasco@orion.ciencias.uniovi.es

and

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

Abstract

Boneh and Venkatesan have recently proposed a polynomial time algorithm for recovering a "hidden" element α of a finite field $\mathbb{F}_p$ of p elements from rather short strings of the most significant bits of the remainder modulo p of αt for several values of t selected uniformly at random from $\mathbb{F}_p^*$. Unfortunately the applications to the computational security of most significant bits of private keys of some finite field exponentiation based cryptosystems given by Boneh and Venkatesan are not quite correct. For the Diffie-Hellman cryptosystem the result of Boneh and Venkatesan has been corrected and generalized in our recent paper. Here a similar analysis is given for the Shamir message passing scheme. The results depend on some bounds of exponential sums.

1 Introduction

Let p be an n-bit prime and let $\mathbb{F}_p$ be a field of p elements.

For integers s and $q \ge 1$ we denote by $(s \operatorname{rem} q)$ the remainder of s on division by q. We also use $\log z$ to denote the binary logarithm of $z > 0$.

The *Shamir message passing scheme* can be described in the following way, see [2], as well as Protocol 12.22 from [8].

To send a message $m \in [0, p-1]$ from *Alice* to *Bob*:

- *Alice* selects a random $a \in [0, p-2]$ with $\gcd(a, p-1) = 1$, computes $A = (m^a \operatorname{rem} p)$ and sends A to *Bob*.
- *Bob* selects a random $b \in [0, p-2]$ with $\gcd(b, p-1) = 1$, computes $B = \left(A^b \operatorname{rem} p\right)$ and sends B to *Alice*.
- *Alice* finds $u \in [0, p-2]$ satisfying the congruence $au \equiv 1 \pmod{p-1}$, computes $C = (B^u \operatorname{rem} p)$ and sends C to *Bob*.
- *Bob* finds $v \in [0, p-2]$ satisfying the congruence $bv \equiv 1 \pmod{p-1}$, computes $m = (C^v \operatorname{rem} p)$.

Given a primitive root $g \in \mathbb{F}_p$, Boneh and Venkatesan [2] have proposed a method of recovering a "hidden" element $\alpha \in \mathbb{F}_p$ from about $n^{1/2}$ most significant bits of $(\alpha g^{x_i} \operatorname{rem} p)$, $i = 1, \ldots, d$, for $d = \left\lceil 2n^{1/2} \right\rceil$ integers $x_1, \ldots, x_d$, chosen uniformly and independently at random in the interval $[0, p-2]$. This result has been applied to proving security of reasonably small portions of bits of private keys of several cryptosystems. In particular, Theorem 3 of [2] claims the security of the $\left\lceil n^{1/2} \right\rceil + \lceil \log n \rceil$ most significant bits of the message in the Shamir message passing scheme. Unfortunately the proof of this result is not quite correct because the exponent x of the corresponding multiplier g^x (where g will in fact be m^b, m and b chosen in the scheme) must satisfy the additional condition $\gcd(bx+1, p-1) = 1$, thus g^x runs through some special subset of $\mathbb{F}_p^*$ (even if g is a primitive root) rather than through the whole $\mathbb{F}_p^*$ and therefore Theorem 1 of [2] does not apply. The proof of Theorem 2 in [2], dealing with security of most significant bits of the Diffie–Hellman key, suffers from a similar problem. In [4] the result of Theorem 1 of [2] has been extended to case when g is not necessary a primitive root but an element of multiplicative order T, provided that $T \ge p^{1/3+\varepsilon}$ for any prime p and $T \ge p^\varepsilon$ for almost all p. It has also been shown that this statement allows to close the gap in the proof of Theorem 2 of [2]. Namely it is shown that having an oracle which computes $\lceil n^{1/2} \rceil + \lceil \log n \rceil$ most significant bits of the private key $\left(g^{ab} \operatorname{rem} p\right)$ from the values of the public keys $A = (g^a \operatorname{rem} p)$ and $B = \left(g^b \operatorname{rem} p\right)$ one can construct a probabilistic polynomial time algorithm for computing the whole key $\left(g^{ab} \operatorname{rem} p\right)$ for all pairs $(a, b) \in [0, T-1]^2$, where T is the multiplicative order of g.

The method of [4] relies on some bounds of exponential sums and results about the distribution of exponential functions in residue classes. Here we use a similar approach to study the bit security of the Shamir message passing scheme.

A survey of similar results for other functions of cryptographic interest has recently been given in [3].

Throughout the paper the implied constants in symbols 'O' may occasionally, where obvious, depend on the small positive parameter ε and are absolute otherwise; they all are effective and can be explicitly evaluated.

2 Distribution of Exponential Functions Modulo p

As in [4] the following bound of exponential sums plays the central role in our arguments.

Let $\mathbf{e}(z) = \exp(2\pi i z/p)$.

The following estimate is well known, see the proof of Lemma 2 in [7] or Theorem 8.2 in [9].

Lemma 1 *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $\vartheta \in \mathbb{F}_p$ of multiplicative order τ the bound*

$$\max_{0 \le H \le \tau - 1} \max_{\gcd(c,p)=1} \left| \sum_{0 \le x \le H} \mathbf{e}\left(c\vartheta^x\right) \right| = O\left(p^{1/2} \log p\right)$$

holds.

We denote by $\nu(k)$ the number of prime divisors of $k \ge 2$.

Let us fix an element g of multiplicative order T modulo p. Combining Lemma 1 with the sieve of Eratosthenes we derive.

Lemma 2 *For any b with* $\gcd(b, p-1) = 1$ *the bound*

$$\max_{\gcd(c,p)=1} \left| \sum_{\substack{x\in[0,T-1] \\ \gcd(bx+1,p-1)=1}} \mathbf{e}\left(cg^x\right) \right| = O\left(2^{\nu(p-1)} p^{1/2} \log p\right)$$

holds.

Proof. Let $\mu(k)$ denote the Möbius function. We recall that $\mu(1) = 1$, $\mu(k) = 0$ if $k \geq 2$ is not sqyare-free and $\mu(k) = (-1)^{\nu(k)}$ otherwise.

Using the Möbius function $\mu(d)$ over the divisors of $p-1$ to detect the co-primality condition and interchanging the order of summation, we obtain (see Section 3.d of Chapter 2 of [12])

$$\sum_{\substack{x\in[0,T-1] \\ \gcd(bx+1,p-1)=1}} \mathbf{e}\left(cg^x\right) = \sum_{d|p-1} \mu(d) \sum_{\substack{x\in[0,T-1] \\ bx+1\equiv 0 \pmod d}} \mathbf{e}\left(cg^x\right).$$

Since $\gcd(b, p-1) = 1$, we can find for each $d|p-1$ the condition $bx+1 \equiv 0 \pmod d$ can be written in the form $x = dy + \alpha_d$ with some integer α_d, $1 \leq \alpha_d \leq d-1$. Therefore

$$\sum_{\substack{x\in[0,T-1] \\ bx+1\equiv 0 \pmod d}} \mathbf{e}\left(cg^x\right) = \sum_{0\leq dz+\alpha_d\leq T-1} \mathbf{e}\left(cg^{dz+\alpha_d}\right)$$

Denoting by τ_d the multiplicative order of $\vartheta_d = g^d$ and remarking that $\tau_d \geq T/d$, we derive from Lemma 1

$$\sum_{0\leq dz+\alpha_d\leq T-1} \mathbf{e}\left(cg^{dz+\alpha_d}\right) = \sum_{0\leq z\leq (T-1-\alpha_d)/d} \mathbf{e}\left(cg^{\alpha_d}\vartheta_d^z\right) = O\left(p^{1/2}\log p\right).$$

Taking into account that

$$\sum_{d|p-1} |\mu(d)| = 2^{\nu(p-1)}$$

(see Section 3.b of Chapter 2 of [12]), we obtain the desired result. □

For integers λ, b, r and h let us denote by $N_{\lambda,b}(r,h)$ the number of $x \in [0, T-1]$ with $\gcd(bx+1, p-1) = 1$ and such that $(\lambda g^x \operatorname{rem} p) \in [r+1, r+h]$. We also denote by N_b the the number of $x \in [0, T-1]$ with $\gcd(bx+1, p-1) = 1$. Note that if $T = p-1$ and $\gcd(b, p-1) = 1$ then $N_b = \varphi(p-1)$.

We need the following asymptotic formula which shows that $N_{\lambda,b}(r,h)$ is close to its expected value $\frac{N_b h}{p}$.

Lemma 3 *The bound*

$$\max_{0\le r,h\le p-1}\ \max_{\gcd(\lambda,p)=1}\ \max_{\gcd(b,p-1)=1}\left|N_{\lambda,b}(r,h)-\frac{N_b h}{p}\right| = O\left(2^{\nu(p-1)}p^{1/2}\log^2 p\right)$$

holds.

Proof. We remark that $N_{\lambda,b}(r,h)$ is the number of solutions $x\in\{0,\ldots,T-1\}$ of the congruence

$$\lambda g^x \equiv y \pmod p, \qquad y=r+1,\ldots,r+h,$$

provided that $\gcd(bx+1,p-1)=1$.

Using the identity (see Exercise 11.a in Chapter 3 of [12])

$$\sum_{c=0}^{p-1}\mathbf{e}\left(cu\right)=\begin{cases}0, & \text{if } u\not\equiv 0 \pmod p;\\ p, & \text{if } u\equiv 0 \pmod p;\end{cases}$$

we obtain

$$\begin{aligned} N_{\lambda,b}(r,h) &= \frac{1}{p}\sum_{\substack{x=0\\ \gcd(bx+1,p-1)=1}}^{T-1}\ \sum_{y=r+1}^{r+h}\sum_{c=0}^{p-1}\mathbf{e}\left(c\left(\lambda g^x-y\right)\right)\\ &= \frac{1}{p}\sum_{c=0}^{p-1}\ \sum_{\substack{x=0\\ \gcd(bx+1,p-1)=1}}^{T-1}\mathbf{e}\left(\lambda g^x\right)\sum_{y=r+1}^{r+h}\mathbf{e}\left(-cy\right).\end{aligned}$$

Separating the term $N_b h/p$ corresponding to $c=0$ we obtain

$$\begin{aligned}\left|N_{\lambda,b}(r,h)-\frac{N_b h}{p}\right| &\le \frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{\substack{x=0\\ \gcd(bx+1,p-1)=1}}^{T-1}\mathbf{e}\left(c\lambda g^x\right)\right|\left|\sum_{y=r+1}^{r+h}\mathbf{e}\left(-cy\right)\right|\\ &= \frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{\substack{x=0\\ \gcd(bx+1,p-1)=1}}^{T-1}\mathbf{e}\left(c\lambda g^x\right)\right|\left|\sum_{y=r+1}^{r+h}\mathbf{e}\left(cy\right)\right|.\end{aligned}$$

Using Lemma 2 and the estimate

$$\max_{0\le r,h\le p-1}\ \sum_{c=1}^{p-1}\left|\sum_{y=r+1}^{r+h}\mathbf{e}\left(cy\right)\right| = O(p\log p),$$

see Exercise 11.c in Chapter 3 of [12], we obtain the desired result. □

We also need to estimate N_b. The following statement is a simple consequence of the sieve of Eratosthenes.

Lemma 4 *For any b with* $\gcd(b, p-1) = 1$ *the bound*

$$N_b = \frac{\varphi(p-1)}{p}T + O(2^{\nu(p-1)}).$$

holds

Proof. Indeed, as in the proof of Lemma 2, using the Möbius function $\mu(d)$ over the divisors of $p-1$ to detect the co-primality condition and interchanging the order of summation, we obtain

$$\sum_{\substack{x=0 \\ \gcd(bx+1,p-1)=1}}^{T-1} 1 = \sum_{d|p-1} \mu(d) \left(\frac{T}{d} + O(1)\right) = T \sum_{d|p-1} \frac{\mu(d)}{d} + O\left(\sum_{d|p-1} |\mu(d)|\right)$$

from which the result follows at once (see Section 3.d of Chapter 2 of [12]). □

Because $\nu(p-1)! \le p-1$ we conclude that $2^{\nu(p-1)} \le p^{o(1)}$. Thus combining Lemma 3 and Lemma 4 we obtain

Lemma 5 *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for $T \ge p^{1/2+\varepsilon}$ the bound*

$$\max_{0 \le r,h \le p-1} \max_{\gcd(\lambda,p)=1} \max_{\gcd(b,p-1)=1} \left| N_{\lambda,b}(r,h) - \frac{\varphi(p-1)hT}{p^2} \right| = O\left(T^{1-\delta}\right)$$

holds.

3 Lattices

As in [2], our results rely on rounding techniques in lattices. We therefore review a few related results and definitions.

Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ be a set of linearly independent vectors in $\mathbb{R}^s$. The set of vectors

$$L = \{\mathbf{z} \ : \ \mathbf{z} = \sum_{i=1}^{s} t_i \mathbf{b}_i, \quad t_1, \ldots, t_s \in \mathbb{Z}\}$$

is called an s-dimensional full rank lattice. The set $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ is called the *basis* of L.

In [1] Babai describes a polynomial time algorithm which, for given a lattice L and a vector $\mathbf{r} = (r_1, \ldots, r_s) \in \mathbb{R}^s$, finds a lattice vector $\mathbf{v} = (v_1, \ldots, v_s)$ satisfying the inequality

$$\left(\sum_{i=1}^{s} (v_i - r_i)^2\right)^{1/2} \le 2^{s/4} \min \left\{ \left(\sum_{i=1}^{s} (z_i - r_i)^2\right)^{1/2}, \quad \mathbf{z} = (z_1, \ldots, z_s) \in L \right\}.$$

That is, a given vector can be rounded in polynomial time to an approximately closest vector in a given lattice. The above algorithm uses the lattice basis reduction algorithm of Lenstra, Lenstra and Lovász [6], see also [11] for some more recent and stronger results.

For integers g and $x_1, \ldots, x_d$, selected in the interval $[0, p-2]$, we denote by $L_g(x_1, \ldots, x_d)$ the $d+1$-dimensional lattice generated by the rows of the following $(d+1) \times (d+1)$-matrix

$$\begin{pmatrix} p & 0 & 0 & \ldots & 0 & 0 \\ 0 & p & 0 & \ldots & 0 & 0 \\ & \vdots & & & & \vdots \\ 0 & 0 & 0 & \ldots & p & 0 \\ t_1 & t_2 & t_3 & \ldots & t_d & 1/p \end{pmatrix} \qquad (1)$$

where $t_i = (g^{x_i} \operatorname{rem} p)$, $i = 1, \ldots, d$.

The following result is a generalization of Theorem 5 of [2] (which corresponds to the case $T = p-1$).

Also, for $b \in [1, p-2]$ with $\gcd(b, p-1) = 1$ we denote by $\mathcal{X}_b$ the set of integers $x \in [0, p-2]$ with $\gcd(bx+1, p-1) = 1$. In particular, $\#\mathcal{X}_b = \varphi(p-1)$.

Lemma 6 *Let $d = 2\lceil n^{1/2} \rceil$ and $\mu = n^{1/2}/2 + 3$, p sufficiently large prime number. Let α be a fixed integer in the interval $[0, p-1]$. For any $\varepsilon > 0$, any element $g \in \mathbb{F}_p$ of multiplicative order $T \ge p^{1/2+\varepsilon}$ and any $b \in [1, p-2]$ with* $\gcd(b, p-1) = 1$ *the following statement holds: Chosen integers $x_1, \ldots, x_d$ uniformly and independently at random in the set $\mathcal{X}_b$, then with probability $P \ge 1 - 2^{-n^{1/2}}$ for any vector $\mathbf{u} = (u_1, \ldots, u_d, 0)$ with*

$$\left(\sum_{i=1}^{d} \left((\alpha g^{x_i} \operatorname{rem} p) - u_i\right)^2\right)^{1/2} \le p 2^{-\mu},$$

all vectors $\mathbf{v} = (v_1, \ldots, v_d, v_{d+1}) \in L_{g,p}(x_1, \ldots, x_d)$ satisfying

$$\left(\sum_{i=1}^{d} (v_i - u_i)^2\right)^{1/2} \le p 2^{-\mu},$$

are of the form

$$\mathbf{v} = ((\beta g^{x_1} \operatorname{rem} p), \dots, (\beta g^{x_d} \operatorname{rem} p), \beta/p)$$

with some $\beta \equiv \alpha \pmod p$.

Proof. As in [2] we define the modular distance between two integers β and γ as

$$\operatorname{dist}_p(\beta, \gamma) = \min_{b \in \mathbb{Z}} |\beta - \gamma - bp| = \min \left\{ ((\beta - \gamma) \operatorname{rem} p), p - ((\beta - \gamma) \operatorname{rem} p) \right\}.$$

Let z be an integer chosen uniformly at random in the set $\mathcal{X}_b$. Because $T|p-1$ $x = (z \operatorname{rem} T)$ is also uniformly distributed in the set of integers $x \in [0, T-1]$ with $\gcd(bx+1, p-1) = 1$. Hence, it follows from Lemma 5 that for any β and γ such that $\beta \not\equiv \gamma \pmod p$ the probability $P(\beta, \gamma)$ of

$$\operatorname{dist}_p(\beta g^x, \gamma g^x) > p 2^{-\mu+1}$$

for an integer x chosen uniformly at random in the set $\mathcal{X}_b$ is

$$P(\beta, \gamma) = 1 - 2^{-\mu+2} + O\left(T^{-\delta}\right)$$

for some $\delta > 0$, depending only on ε. Thus

$$P(\beta, \gamma) \geq 1 - \frac{5}{2^\mu}$$

provided that p is large enough.

Therefore, for any $\beta \not\equiv \alpha \pmod p$,

$$\Pr\left[\exists i \in [1, d] \mid \operatorname{dist}_p(\beta g^{x_i}, \alpha g^{x_i}) > p 2^{-\mu+1}\right] = 1 - (1 - P(\alpha, \beta))^d \geq 1 - \left(\frac{5}{2^\mu}\right)^d,$$

where probability is taken over integers $x_1, \dots, x_d$ chosen uniformly and independently at random in the set $\mathcal{X}_b$.

Since for $\beta \not\equiv \alpha \pmod p$ there are only $p-1$ possible values for $(\beta \operatorname{rem} p)$ we obtain

$$\Pr\left[\exists \beta \not\equiv \alpha \pmod p, \ \exists i \in [1, d] \mid \operatorname{dist}_p(\beta g^{x_i}, \alpha g^{x_i}) > p 2^{-\mu+1}\right] \geq 1 - (p-1)\left(\frac{5}{2^\mu}\right)^d > 1 - 2^{-n^{1/2}}$$

because

$$d(\mu - \log 5) > \left\lceil n^{1/2} \right\rceil n^{1/2} + 2 \left\lceil n^{1/2} \right\rceil (3 - \log 5) > \log p + n^{1/2}.$$

The rest of the proof is identical to the proof of Theorem 5 of [2], we outline it for the sake of completeness.

Let us fix some integers $x_1, \dots, x_d$ with

$$\min_{\beta \not\equiv \alpha \pmod p} \ \min_{i \in [1,d]} \operatorname{dist}_p(\beta g^{x_i}, \alpha g^{x_i}) > p2^{-\mu+1}. \qquad (2)$$

Let $\mathbf{v}$ be a lattice point satisfying

$$\left(\sum_{i=1}^{d} (v_i - u_i)^2 \right)^{1/2} \le p2^{-\mu}.$$

Clearly, since $\mathbf{v} \in L_{g,p}(x_1, \dots, x_d)$, there are integers $\beta, z_1, \dots, z_d$ such that

$$\mathbf{v} = (\beta t_1 - z_1 p, \dots, \beta t_d - z_d p, \beta/p),$$

where, as in (1), $t_i = (g^{x_i} \operatorname{rem} p)$, $i = 1, \dots, d$.

If $\beta \equiv \alpha \pmod p$, then for all $i = 1, \dots, d$ we have $\beta t_i - z_i p = (\beta t_i \operatorname{rem} p)$, for otherwise there would be $j \in \{1, \dots, d\}$ so that $|v_j - u_j| > p2^{-\mu}$.

Now suppose that $\beta \not\equiv \alpha \pmod p$. In this case we have

$$\begin{aligned} \left(\sum_{i=1}^{d} (v_i - u_i)^2 \right)^{1/2} &\ge \min_{i \in [1,d]} \operatorname{dist}_p(\beta t_i, u_i) \\ &\ge \min_{i \in [1,d]} \left(\operatorname{dist}_p(\beta t_i, \alpha t_i) - \operatorname{dist}_p(u_i, \alpha t_i) \right) \\ &> p2^{-\mu+1} - p2^{-\mu} = p2^{-\mu} \end{aligned}$$

that contradicts to our assumption. As we have seen, the condition (2) holds with probability exceeding $1 - 2^{-n^{1/2}}$ and the result follows. □

For an integer $k \ge 1$ we define $f_k(t)$ by the inequalities

$$(f_k(t) - 1)\frac{p}{2^k} \le (t \operatorname{rem} p) < f_k(t)\frac{p}{2^k}.$$

Thus, roughly speaking, $f_k(t)$ is the integer defined by the k most significant bits of $(t \operatorname{rem} p)$.

Using Lemma 6 in the same way as in [2] Theorem 5 is used in the proof of Theorem 1, we obtain

Lemma 7 *Let* $d = 2\left\lceil n^{1/2} \right\rceil$ *and* $k = \left\lceil n^{1/2} \right\rceil + \lceil \log n \rceil$*. For any* $\varepsilon > 0$*, any element* $g \in \mathbb{F}_p$ *of multiplicative order* $T \geq p^{1/2+\varepsilon}$ *and any* $b \in [1, p-2]$ *with* $\gcd(b, p-1) = 1$ *the following statement holds: There exists a deterministic polynomial time algorithm* $\mathcal{A}$ *such that for any integer* $\alpha \in [1, p-1]$ *given* $2d$ *integers*

$$t_i = (g^{x_i} \operatorname{rem} p) \qquad \text{and} \qquad s_i = f_k(\alpha t_i), \qquad i = 1 \ldots, d,$$

its output satisfies

$$\Pr_{x_1,\ldots,x_d \in \mathcal{X}_b} \left[\mathcal{A}(t_1, \ldots, t_d; s_1, \ldots, s_d) = \alpha\right] \geq 1 - 2^{-n^{1/2}}$$

if $x_1, \ldots, x_d$ *are chosen uniformly and independently at random in the set* $\mathcal{X}_b$*.*

Proof. We follow the same arguments as in the proof Theorem 1 of [2] which we briefly outline here for the sake of completeness. We refer to the first d vectors in the defining matrix of $L_{g,p}(x_1, \ldots, x_d)$ as p-vectors.

Let us consider the vector $\mathbf{r} = (r_1, \ldots, r_d, r_{d+1})$ where

$$r_i = s_i \frac{p}{2^k}, \quad i = 1, \ldots, d, \qquad \text{and} \qquad r_{d+1} = 0.$$

Multiplying the last row vector $(t_1, \ldots, t_d, 1/p)$ of the matrix (1) by α and subtracting certain multiples of p-vectors, we obtain a lattice point

$$\mathbf{u}_\alpha = (u_1, \ldots, u_d, \alpha/p) \in L_{g,p}(x_1, \ldots, x_d)$$

such that

$$|u_i - r_i| < p2^{-k}, \qquad i = 1, \ldots, d.$$

Therefore,

$$\left(\sum_{i=1}^{d+1} (u_i - r_i)^2\right)^{1/2} \leq p(d+1)^{1/2} 2^{-k}.$$

Now we can use the Babai algorithm [1] to find in polynomial time a lattice vector $\mathbf{v} = (v_1, \ldots, v_d, v_{d+1}) \in L_{g,p}(x_1, \ldots, x_d)$ such that

$$\begin{aligned} &\left(\sum_{i=1}^{d} (v_i - r_i)^2\right)^{1/2} \\ &\quad \leq 2^{(d+1)/4} \min\left\{\left(\sum_{i=1}^{d+1} (z_i - r_i)^2\right)^{1/2}, \quad \mathbf{z} = (z_1, \ldots, z_d, z_{d+1}) \in L\right\} \\ &\quad \leq 2^{(d+1)/4} p(d+1)^{1/2} 2^{-k} \leq p2^{-\mu}, \end{aligned}$$

where $\mu = n^{1/2}/2 + 3$, provided that n is sufficiently large. We also have

$$\left(\sum_{i=1}^{d} (u_i - r_i)^2\right)^{1/2} \le pd^{1/2}2^{-k} \le p2^{-\mu}.$$

Applying Lemma 6, we see that $\mathbf{v} = \mathbf{u}_\alpha$ with probability at least $1 - 2^{-n^{1/2}}$, and therefore, α can be recovered in polynomial time. □

4 Security of the Most Significant Bits of the Shamir Scheme

We are ready to prove the main results.

For an integer k we suppose that we are given an oracle $\mathcal{O}_k$ such that for any given values of A, B, C it outputs the k most significant bits of m if the triple (A, B, C) corresponds to a proper usage of the Shamir message passing scheme and an error message, otherwise.

More precisely, given A, B and C, the oracle $\mathcal{O}_k$ outputs:

- $f_k(m)$, if $A = (m^a \operatorname{rem} p)$, $B = \left(A^b \operatorname{rem} p\right)$ and $C = (B^u \operatorname{rem} p)$, where $au \equiv 1 \pmod{p-1}$ for some $m \in [1, p-1]$ and $a, b \in [0, p-2]$ with $\gcd(ab, p-1) = 1$;
- an error message, otherwise.

Theorem 8 *Assume that we are given an oracle $\mathcal{O}_k$ as above, with*

$$k = \left\lceil n^{1/2} \right\rceil + \lceil \log n \rceil .$$

Then there exists a probabilistic polynomial time algorithm which computes the message m, for all except $O\left(p^{1/2+\varepsilon}\right)$ messages $m \in [1, p-1]$, from the values of $A = (m^a \operatorname{rem} p)$, $B = \left(A^b \operatorname{rem} p\right)$ and $C = (B^u \operatorname{rem} p)$, where $a, b \in [0, p-2]$ with $\gcd(ab, p-1) = 1$ and $au \equiv 1 \pmod{p-1}$, which uses the expected number of $O\left(n^{1/2} \log n\right)$ calls of the oracle $\mathcal{O}_k$.

Proof. We exclude from the consideration the messages $m \in [1, p-1]$ of multiplicative order less than $p^{1/2+\varepsilon}$. Obviously, the number E of such excluded messages does not exceed

$$E \le \tau(p-1)p^{1/2+\varepsilon}, \tag{3}$$

where $\tau(p-1)$ is the number of positive integer divisors of $p-1$. Indeed, for any divisor $D|p-1$ there are at most D values of $m \in [1, p-1]$ of multiplicative order D. Using the bound $\tau(p-1) = O\left(p^{\varepsilon/2}\right)$, see Theorem 5.2 of Chapter 1 of [10], we obtain from (3) that the exceptional set is of size $E = O\left(p^{1/2+\varepsilon}\right)$.

Let us consider a message m of multiplicative order $T \geq p^{1/2+\varepsilon}$.

For $x \in \mathcal{X}_b$ we put $a_x = a$ define $b_x \in [1, p-2]$ from the congruence

$$b_x(bx+1) \equiv b \pmod{p-1}.$$

We also put

$$m_x = \left(m^{1+bx} \operatorname{rem} p\right).$$

We remark that

$$A_x = \left(m_x^{a_x} \operatorname{rem} p\right), \qquad B_x = \left(m_x^{a_x b_x} \operatorname{rem} p\right), \qquad C_x = \left(m_x^{b_x} \operatorname{rem} p\right)$$

can be computed as

$$A_x = \left(AC^x \operatorname{rem} p\right), \qquad B_x = B, \qquad C_x = C.$$

Although the value of b is not known, one can select elements $x \in \mathcal{X}_b$ uniformly and independently at random by querying the oracle $\mathcal{O}_k$ with the triples (A_x, B_x, C_x) where the elements x are selected uniformly and independently at random in the interval $[0, p-2]$. If $\gcd(bx+1, p-1) > 1$ the oracle returns an error message, otherwise $x \in \mathcal{X}_b$. Now we chose $d = 2\left\lceil n^{1/2} \right\rceil$ elements $x_1, \ldots, x_d \in \mathcal{X}_b$ uniformly and independently at random. Because

$$\frac{p-1}{\#\mathcal{X}_b} = \frac{p-1}{\phi(p-1)} = O(\log\log p),$$

see Theorem 5.1 of Chapter 1 of [10], we see that the expected number of choices of $x \in [0, p-2]$ before we get d elements in $\mathcal{X}_b$ is $O(d \log\log p) = O(n^{1/2}\log n)$. We remark that these elements are independent and uniformly distributed in $\mathcal{X}_b$. Moreover, every output of the oracle provides k most significant bits of m_x. Remarking that $m_x \equiv mC^x \pmod{p}$ and that $C \equiv m^b \pmod{p}$ is of multiplicative order T (because $\gcd(b, p-1) = 1$), we see that Lemma 7 applies and the result follows. $\square$

5 Remarks

First of all we note that the constants in above estimates are effective and can be explicitly evaluated.

We also remark that one can consider an oracle which instead of returning an error message for "inconsistent" inputs (A, B, C) returns just a random element from $\mathbb{F}_p$. In this case repeating each query twice one can easily distinguish between an $x \in \mathcal{X}_b$ and other values.

Acknowledgement. We thank Consuelo Martínez for her interest and for helpful advice. We also thank Mats Näslund for fruitful discussions.

References

[1] L. Babai, *On Lovász' lattice reduction and the nearest lattice point problem,* Combinatorica, **6** (1986), 11–13.

[2] 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.

[3] M. I. González Vasco and M. Näslund, *A survey of hard core functions,* Preprint, 2000.

[4] M. I. González Vasco and I. E. Shparlinski, *On the security of Diffie-Hellman bits*, Preprint, 2000.

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

[6] A. K. Lenstra, H. W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients,* Mathematische Annalen, **261** (1982), 515–534.

[7] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Math. USSR – Sbornik*, **18** (1972), 659–676.

[8] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, Boca Raton, FL, 1996.

[9] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers,* Bull. Amer. Math. Soc., **84** (1978), 957–1041.

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

[11] C. P. Schnorr, *A hierarchy of polynomial time basis reduction algorithms,* Theor. Comp. Sci., **53** (1987) 201–224.

[12] I. M. Vinogradov, *Elements of number theory,* Dover Publ., New York, 1954.