On the Security of Diffie–Hellman Bits

Maria Isabel González Vasco and Igor E. Shparlinski

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 $\mathbb{F}_p^*$. We use some recent bounds of exponential sums to generalize this algorithm to the case when t is selected from a quite small subgroup of $\mathbb{F}_p^*$. Namely, our results apply to subgroups of size at least $p^{1/3+\varepsilon}$ for all primes p and to subgroups of size at least p^{ε} for almost all primes p, for any fixed $\varepsilon > 0$. We also use this generalization to improve (and correct) one of the statements of the aforementioned work about the computational security of the most significant bits of the Diffie–Hellman key.

1. Introduction

Let p be an n-bit prime and let $g \in \mathbb{F}_p$ be an element of multiplicative order T, where $\mathbb{F}_p$ is the finite field of p elements.

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

In the case of $T = p - 1$, that is, when g is a primitive root, 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 $d = \lceil 2n^{1/2} \rceil$ 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, in Theorem 2 of [2] the security of the $\lceil n^{1/2} \rceil + \lceil \log n \rceil$ most significant bits of the private key $\left(g^{ab} \operatorname{rem} p\right)$ of the Diffie–Hellman cryptosystem with public keys $(g^a \operatorname{rem} p)$ and $\left(g^b \operatorname{rem} p\right)$ with $a, b \in [0, p-2]$ is considered.

Namely, a method has been given to recover, in polynomial time, the Diffie–Hellman key $\left(g^{ab} \operatorname{rem} p\right)$ from $(g^a \operatorname{rem} p)$ and $\left(g^b \operatorname{rem} p\right)$, using an oracle which gives only the $\lceil n^{1/2} \rceil + \lceil \log n \rceil$ most significant bits of the Diffie–Hellman key.

Unfortunately the proof of Theorem 2 in [2] is not quite correct. Indeed, in order to apply Theorem 1 of that paper to $h = g^b$ this element must be a primitive root of $\mathbb{F}_p$. Thus the proof of Theorem 2 of [2] is valid only if $\gcd(b, p-1) = 1$ (of course the same result holds in the case $\gcd(a, p-1) = 1$ as well). However, even in the most favourable case when $l = (p-1)/2$ is prime, only 75% of pairs (a, b) satisfy this condition. Certainly breaking a cryptosystem in 75% of the cases is already bad enough (even in 0.75% is) but unfortunately for the attacker (using the above oracle), these weak cases can easily be described and avoided by the communicating parties. The proof of Theorem 3 of [2] suffers from a similar problem.

Here we use new bounds of exponential sums from [7] to extend some results of [2] to the case of elements g of arbitrary multiplicative order T, provided that $T \geq p^{1/3+\varepsilon}$. This allows us to prove that the statement of Theorem 2 of [2] holds for all pairs (a, b). We also prove that for almost all primes p similar results hold already for $T \geq p^{\varepsilon}$.

A survey of similar results for other functions of cryptographic interest has recently been given in [5].

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 g^x Modulo p

For integers λ, r and h let us denote by $N_{\lambda,g,p}(r, h)$ the number of $x \in [0, T-1]$ for which $(\lambda g^x \operatorname{rem} p) \in [r+1, r+h]$.

We need the following asymptotic formula which shows that $N_{\lambda,g,p}(r, h)$ is close to its expected value Th/p, provided that T is of larger order than $p^{1/3}$.

Lemma 2.1. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order $T \geq p^{1/3+\varepsilon}$ the bound*

$$\max_{0 \leq r,h \leq p-1} \max_{\gcd(\lambda,p)=1} \left| N_{\lambda,g,p}(r,h) - \frac{Th}{p} \right| = O\left(T^{1-\delta}\right)$$

holds.

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

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

Using the identity (see Exercise 11.a in Chapter 3 of [17])

$$\sum_{c=0}^{p-1} \exp\left(2\pi i c u/p\right) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod p; \\ p, & \text{if } u \equiv 0 \pmod p; \end{cases}$$

we obtain

$$\begin{aligned} N_{\lambda,g,p}(r,h) &= \frac{1}{p} \sum_{x=0}^{T-1} \sum_{y=r+1}^{r+h} \sum_{c=0}^{p-1} \exp\left(2\pi i c\left(\lambda g^x - y\right)/p\right) \\ &= \frac{1}{p} \sum_{c=0}^{p-1} \sum_{x=0}^{T-1} \exp\left(2\pi i c \lambda g^x/p\right) \sum_{y=r+1}^{r+h} \exp\left(-2\pi i c y/p\right). \end{aligned}$$

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

$$\begin{aligned}\left|N_{\lambda,g,p}(r,h) - \frac{Th}{p}\right| &\le \frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{x=0}^{T-1}\exp\left(2\pi i c\lambda g^x/p\right)\right|\left|\sum_{y=r+1}^{r+h}\exp\left(-2\pi i c y/p\right)\right| \\ &= \frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{x=0}^{T-1}\exp\left(2\pi i c\lambda g^x/p\right)\right|\left|\sum_{y=r+1}^{r+h}\exp\left(2\pi i c y/p\right)\right|.\end{aligned}$$

We estimate the sum over x by using the bound

$$\max_{\gcd(c,p)=1}\left|\sum_{x=0}^{T-1}\exp\left(2\pi i c g^x/p\right)\right| = O\left(B(T,p)\right), \qquad (1)$$

where

$$B(T,p) = \begin{cases} p^{1/2}, & \text{if } T \ge p^{2/3}; \\ p^{1/4}T^{3/8}, & \text{if } p^{2/3} > T \ge p^{1/2}; \\ p^{1/8}T^{5/8}, & \text{if } p^{1/2} > T \ge p^{1/3}; \end{cases} \qquad (2)$$

which is essentially Theorem 3.4 of [7]. Using the estimate

$$\max_{0\le r,h\le p-1}\sum_{c=1}^{p-1}\left|\sum_{y=r+1}^{r+h}\exp\left(2\pi i c y/p\right)\right| = O(p\log p),$$

see Exercise 11.c in Chapter 3 of [17], we obtain

$$\max_{0\le r,h\le p-1}\left|N_{\lambda,g,p}(r,h) - \frac{Th}{p}\right| = O\left(B(T,p)\log p\right).$$

It is easy to see that for any $\varepsilon > 0$ there exists $\delta > 0$ such that $B(T,p) = O(T^{1-2\delta})$ for $T \ge p^{1/3+\varepsilon}$ and the result follows. □

In the next statement we show that for almost all primes the lower bound $T \ge p^{1/3+\varepsilon}$ can be brought down to $T \ge p^{\varepsilon}$.

Lemma 2.2. *Let Q be a sufficiently large integer. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for all primes $p \in [Q, 2Q]$, except at most $Q^{5/6+\varepsilon}$ of them, and any element $g \in \mathbb{F}_p$ of multiplicative order $T \ge p^{\varepsilon}$ the bound*

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

holds.

Proof. The proof is analogous to the proof of Lemma 2.1 using in this case Theorem 5.5 of [7] instead of (1) and (2). For each prime $p \equiv 1 \pmod T$ we fix an element $g_{p,T}$ of multiplicative order T. Then Theorem 5.5 of [7] claims that for any $U > 1$ and any integer $\nu \geq 2$, for all primes $p \equiv 1 \pmod T$ except at most $O(U/\log U)$ of them, the bound

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \exp\left(2\pi i c g_{p,T}^x / p\right) \right| = O\left(T p^{1/2\nu^2} \left(T^{-1/\nu} + U^{-1/\nu^2}\right)\right),$$

holds. We remark that the value of the above exponential sum does not depend on the particular choice of the element $g_{p,T}$.

Taking

$$\nu = \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1 \qquad \text{and} \qquad U = Q^{1/2+\varepsilon/2},$$

after simple computation we obtain that there exists some $\delta > 0$, depending only on ε, such that for any fixed $T \geq Q^{\varepsilon/2}$ the bound

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \exp\left(2\pi i c g_{p,T}^x / p\right) \right| = O\left(T^{1-2\delta}\right), \tag{3}$$

holds for all except $O(Q^{1/2+\varepsilon/2})$ primes $p \equiv 1 \pmod T$ in the interval $p \in [Q, 2Q]$. As it follows from (1) and (2), a similar bound also holds for $T \geq Q^{1/3+\varepsilon/2}$. So the total number of exceptional primes p for which (3) does not hold for at least one $T \geq p^\varepsilon > Q^{\varepsilon/2}$ is $O\left(Q^{5/6+\varepsilon}\right)$.

Using the bound (3) in the same way as we have used (1) and (2) in the proof of Lemma 2.1 we derive the desired result. □

Certainly in both Lemma 1 and Lemma 3 the dependence of δ on ε can be made explicit (as a linear function of ε).

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

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

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 [9], see also [14] for some more recent and stronger results.

For integers $x_1, \dots, x_d$, selected in the interval $[0, T-1]$, we denote by $L_{g,p}(x_1, \dots, x_d)$ the $d+1$-dimensional lattice generated by the rows of the following $(d+1) \times (d+1)$-matrix

$$\begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ 0 & p & 0 & \dots & 0 & 0 \\ & \vdots & & & & \vdots \\ 0 & 0 & 0 & \dots & p & 0 \\ t_1 & t_2 & t_3 & \dots & t_d & 1/p \end{pmatrix} \qquad (4)$$

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

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

Lemma 3.1. *Let $d = 2\lceil n^{1/2} \rceil$ and $\mu = n^{1/2}/2 + 3$. Let α be a fixed integer in the interval $[0, p-1]$. For any $\varepsilon > 0$, sufficiently large p, and any element $g \in \mathbb{F}_p$ of multiplicative order $T \ge p^{1/3+\varepsilon}$ the following statement holds. Choose integers $x_1, \dots, x_d$ uniformly and independently at random in the interval $[0, T-1]$. Then with probability $P \ge 1 - 2^{-n^{1/2}}$ for any vector $\mathbf{u} = (u_1, \dots, u_d, 0)$ 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 $\mathbf{v} = (v_1, \dots, v_d, v_{d+1}) \in L_{g,p}(x_1, \dots, x_d)$ satisfying

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

are of the form

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

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 x be an integer chosen uniformly at random in the interval $[0, T-1]$. It follows from Lemma 2.1 that for any β and γ with $\beta \not\equiv \gamma \pmod p$ 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 interval $[0, T-1]$ is

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

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

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

provided that p is large enough.

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

$$\Pr\left[\exists i \in [1, d] \mid \operatorname{dist}_p(\beta g^{x_i}, \alpha g^{x_i}) > p2^{-\mu+1}\right] = 1 - (1 - P(\alpha, \beta))^d \geq 1 - \left(\frac{5}{2^{\mu}}\right)^d,$$

where probability is taken over integers $x_1, \ldots, x_d$ chosen uniformly and independently at random in the interval $[0, T-1]$.

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

$$\Pr\left[\exists \beta \not\equiv \alpha \pmod p,\ \exists i \in [1, d] \mid \operatorname{dist}_p(\beta g^{x_i}, \alpha g^{x_i}) > p2^{-\mu+1}\right]$$
$$\geq 1 - (p-1)\left(\frac{5}{2^{\mu}}\right)^d > 1 - 2^{-n^{1/2}}$$

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 $x_1, \ldots, x_d$ with

$$\min_{\beta \not\equiv \alpha \pmod p} \ \min_{i \in [1,d]} \operatorname{dist}_p(\beta g^{x_i}, \alpha g^{x_i}) > p2^{-\mu+1}. \qquad (5)$$

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

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

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

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

where, as in (4), $t_i = (g^{x_i} \operatorname{rem} p)$, $i = 1, \ldots, d$.

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

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

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

that contradicts to our assumption. As we have seen, the condition (5) holds with probability exceeding $1 - 2^{-n^{1/2}}$ and the result follows. □

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

$$(f_k(t) - 1)\frac{p}{2^k} \leq (t \,\mathrm{rem}\, p) < f_k(t)\frac{p}{2^k}.$$

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

Using Lemma 3.1 in the same way as Theorem 5 is used in the proof of Theorem 1 of [2] we obtain

Lemma 3.2. *Let* $d = 2\lceil n^{1/2} \rceil$ *and* $k = \lceil n^{1/2} \rceil + \lceil \log n \rceil$. *For any* $\varepsilon > 0$*, sufficiently large* p *and any element* $g \in \mathbb{F}_p$ *of multiplicative order* $T \geq p^{1/3+\varepsilon}$*, there exists a deterministic polynomial time algorithm* $\mathcal{A}$ *such that for any integer* $\alpha \in [1, p-1]$ *given* $2d$ *integers*

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

its output satisfies

$$\Pr_{x_1,\ldots,x_d \in [0,T-1]} \left[\mathcal{A}(t_1, \ldots, t_d; s_1, \ldots, s_d) = \alpha\right] \geq 1 - 2^{-n^{1/2}}$$

if $x_1, \ldots, x_d$ *are chosen uniformly and independently at random in the interval* $[0, T-1]$.

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 (4) 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

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

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 3.1, 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. □

Accordingly, using Lemma 2.2 instead of Lemma 2.1, in a similar way we obtain that for almost all primes much smaller values of T can be considered.

Lemma 3.3. *Let Q be a sufficiently large integer. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for all primes $p \in [Q, 2Q]$, except at most $Q^{5/6+\varepsilon}$ of them, and any element $g \in \mathbb{F}_p$ of multiplicative order $T \ge p^\varepsilon$ 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

$$\Pr_{x_1, \ldots, x_d \in [0, T-1]} \left[\mathcal{A}(t_1, \ldots, t_d; s_1, \ldots, s_d) = \alpha\right] \ge 1 - 2^{-n^{1/2}}$$

if $x_1, \ldots, x_d$ are chosen uniformly and independently at random in the interval $[0, T-1]$.

4. Security of the Most Significant Bits of the Diffie–Hellman Key

We are ready to prove the main results.

For each integer k define the oracle $\mathcal{O}_k$ as an 'black box' which given the values of $A = (g^a \operatorname{rem} p)$ and $B = (g^b \operatorname{rem} p)$ outputs the value of $f_k(g^{xy})$.

Theorem 4.1. *Let $k = \lceil n^{1/2} \rceil + \lceil \log n \rceil$. For any $\varepsilon > 0$, sufficiently large p and any element $g \in \mathbb{F}_p$ of multiplicative order $T \ge p^{1/3+\varepsilon}$, there exists a probabilistic polynomial time algorithm which for any pair $(a, b) \in [0, T-1]^2$, given the values of $A = (g^a \operatorname{rem} p)$ and $B = (g^b \operatorname{rem} p)$, makes $O\left(n^{1/2}\right)$ calls of the oracle $\mathcal{O}_k$ and computes $\left(g^{ab} \operatorname{rem} p\right)$ correctly with probability $1 + O\left(2^{-n^{1/2}}\right)$.*

Proof. Given a pair $(a,b) \in [0, T-1]^2$ let us select an integer $r \in [0, T-1]$ uniformly at random. We compute

$$g_r = (Bg^r \operatorname{rem} p)$$

thus $g_r \equiv g^{b+r} \pmod{p}$.

The probability that $\gcd(b+r, T) \geq Tp^{-1/3-\varepsilon/3}$ is at most $\tau(T)T^{-1}p^{1/3+\varepsilon/3}$ where $\tau(T)$ is the number of positive integer divisors of T. Indeed, for any divisor $D|T$ with $D \geq Tp^{-1/3-\varepsilon/3}$ there are at most $T/D \leq p^{1/3+\varepsilon/3}$ values of $s \in [0, T-1]$ with $\gcd(s,T) = D$.

Using the bound $\tau(T) = O\left(T^{\varepsilon/3}\right)$, see Theorem 5.2 of Chapter 1 of [13], we obtain that the probability of $\gcd(b+r, T) \geq Tp^{-1/3-\varepsilon/3}$ is at most

$$O\left(T^{-1}p^{1/3+2\varepsilon/3}\right) = O\left(p^{-\varepsilon/3}\right) = O\left(2^{-n^{1/2}}\right).$$

In the opposite case, when $\gcd(a+r, T) \leq Tp^{-1/3-\varepsilon/3}$, the multiplicative order of g_r is

$$T_r = \frac{T}{\gcd(b+r,T)} \geq p^{1/3+\varepsilon/3}.$$

Let $\alpha_r \equiv g^{a(b+r)} \pmod{p}$. Then

$$f_k\left(\alpha_r g_r^x\right) = f_k\left(g_r^{(a+x)}\right) = f_k\left(g^{(a+x)(b+r)}\right).$$

Now we use the oracle $\mathcal{O}_k$ with $(g^x A \operatorname{rem} p)$ and $(g^r B \operatorname{rem} p)$ to compute $f_k\left(\alpha_r g_r^x\right)$ for an integer x chosen uniformly at random in the interval $[0, p-1]$. Because $T_r | p-1$ the values of $(x \operatorname{rem} T_r)$ are uniformly distributed in the interval $[0, T_r - 1]$ as well, thus Lemma 3.2 can be applied. Therefore, one can construct a probabilistic polynomial time algorithm that:

- Selects a random $r \in [0, T-1]$.
- Applies algorithm $\mathcal{A}$ from Lemma 3.2 (now g_r plays the role of g in the conditions of Lemma 3.2. This algorithm makes $O\left(n^{1/2}\right)$ calls to the oracle $\mathcal{O}_k$.
- Outputs the correct value α_r with probability at least $1 - O\left(2^{-n^{1/2}}\right)$.

Indeed, the only possible source of error is either the case $T_r \leq p^{1/3+\varepsilon/3}$ or the probability error of the algorithm of Lemma 3.2. The probability of both events is $O\left(2^{-n^{1/2}}\right)$.

Remarking that

$$g^{ab} \equiv \alpha_r A^{-r} \pmod{p},$$

we obtain the desired result. □

It is easy to see that Theorem 4.1 is nontrivial for any $T \geq p^{1/3+\varepsilon}$. In a similar way, Lemma 3.2 produces a result which holds for almost all primes p and is non-trivial for $T \geq p^{\varepsilon}$.

Theorem 4.2. *Let* $k = \lceil n^{1/2} \rceil + \lceil \log n \rceil$. *For any* $\varepsilon > 0$ *and for all primes* $p \in [2^{n-1}, 2^n - 1]$, *except at most* $2^{(5/6+\varepsilon)n}$ *of them, and any element* $g \in \mathbb{F}_p$ *of multiplicative order* $T \ge p^\varepsilon$ *the following statement holds: There exists a probabilistic polynomial time algorithm which for any pair* $(a, b) \in [0, T-1]^2$, *given the values of* $A = (g^a \operatorname{rem} p)$ *and* $B = (g^b \operatorname{rem} p)$, *makes* $O\left(n^{1/2}\right)$ *calls of the oracle* $\mathcal{O}_k$ *and computes* $\left(g^{ab} \operatorname{rem} p\right)$ *correctly with probability* $1 + O\left(2^{-n^{1/2}}\right)$.

5. Remarks

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

It would be very interesting to replace the condition $T \ge p^\varepsilon$ for the smallest size of the multiplicative order of g in Lemma 2.2 by a weaker condition of the form $T \ge (\log p)^c$ with some constant c. Although a more careful analysis of the proof of Theorem 5.5 of [7] should allow to replace p^ε with a slower growing function, it seems unlikely that the present method can be applied to T as small as a power of $\log p$.

Our results can also be applied to several other cryptosystems based on exponentiation in finite fields, which have been considered in [2], except the *Shamir message passing scheme*, see [2, 3] (this scheme is also described in Protocol 12.22 in [11]). Unfortunately the proof of Theorem 3 in [2] suffers from the same problem as the proof of Theorem 2 of that paper. Namely, for the ElGamal scheme, see [2, 3] as well as Section 8.4 from [11], it produces a result which applies only to at most 50% of the cases and it cannot be applied to the the Shamir message passing scheme at all. Indeed, in this scheme the exponent x of the corresponding multiplier g^x must satisfy the additional condition $\gcd(bx + 1, p - 1) = 1$, with some b, $\gcd(b, p-1) = 1$, 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 thus Theorem 1 of [2] does not apply. Our results in their present form cannot be used for this problem directly, however it has been shown in [6] that a modification of the technique of this paper, combined with some elementary sieve method produce similar results for the Shamir message passing scheme.

Besides the mentioned in [2, 3] cryptosystems several other schemes can be studied as well. For example, very similar results hold for the Matsumoto–Takachima–Imai key-agreement protocol, see Section 12.6 of [11].

The results of [3] can be generalized in a similar way. To do so one can use the bound of exponential sums of Theorem 3.4 of [7] to study the distribution of the sums $(g^{x_1} + \ldots + g^{x_r} \operatorname{rem} p)$ and thus obtain an analogue of Lemma 2.4 of [3].

One can also extend Theorem 4.1 to the case of Diffie-Hellman encryption modulo an arbitrary composite integer $m \ge 2$. Indeed, using the well-known bound

$$\max_{\gcd(c,m)=1} \left| \sum_{x=0}^{T-1} \exp\left(2\pi i c g^x / m\right) \right| \le m^{1/2},$$

see Theorem 10 of Chapter 1 in [8] or Theorem 8.2 in [12], instead of (1) and (2), one can obtain similar results for elements g, $\gcd(g, m) = 1$, of multiplicative order T modulo m such that $T \geq m^{1/2+\varepsilon}$. In fact, Lemma 3.2 can be extended to elements t_i chosen uniformly and independently at random from any subgroup $\mathcal{G}$ of the group of units modulo m, provided that the cardinality of $\mathcal{G}$ satisfies $\#\mathcal{G} \geq m^{1/2+\varepsilon}$.

As we have mentioned, similar but somewhat more involved technique can be applied to studying the bit security of the Shamir message passing scheme, see [6].

Finally, we remark that somewhat similar problem for extensions of finite fields have been considered in [16]. The results of that paper and some of their improvements in [15] have applications to the security of the new cryptosystem designed in [4, 10].

Acknowledgement. We thank Consuelo Martínez for her interest and for helpful advice. We also thank Mats Näslund for a careful reading of the manuscript and fruitful discussion.

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

[4] A. E. Brouwer, R. Pellikan, and E. R. Verheul, *Doing more with fewer bits,* Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1716**, (1999), 321–332.

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

[6] M. I. González Vasco and I. E. Shparlinski, *Security of the most significant bits of the Shamir message passing scheme, Preprint*, 2000, 1–14.

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

[8] N. M. Korobov, *Exponential sums and their applications,* Kluwer Acad. Publ., Dordrecht, 1992.

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

[10] A. K. Lenstra and E. R. Verheul, *The XTR public key system,* Proc. of Crypto'2000, Springer-Verlag, Berlin, (to appear).

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

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

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

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

[15] I. E. Shparlinski, *Security of polynomial transformations of the Diffie–Hellman key,* Preprint, 2000.

[16] E. R. Verheul, *Certificates of recoverability with scalable recovery agent security,* Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1751** (2000), 258–275.

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

Department of Mathematics, University of Oviedo,
Oviedo, 33007, Spain
E-mail address: `mvasco@orion.ciencias.uniovi.es`

Department of Computing, Macquarie University,
Sydney, NSW 2109, Australia
E-mail address: `igor@comp.mq.edu.au`