HIDDEN NUMBER PROBLEM
WITH HIDDEN MULTIPLIERS, TIMED-RELEASE CRYPTO,
AND NOISY EXPONENTIATION

NICK A. HOWGRAVE-GRAHAM, PHONG Q. NGUYEN, AND IGOR E. SHPARLINSKI

Abstract. We consider a generalisation of the hidden number problem recently introduced by Boneh and Venkatesan. The initial problem can be stated as follows: recover a number \( a \in \mathbb{F}_p \) such that for many known random \( t \in \mathbb{F}_p \) approximations to the values of \( \lfloor at \rfloor \) are known. Here we study a version of the problem where the “multipliers” \( t \) are not known but rather certain approximations to them are given. We present a probabilistic polynomial time solution when the error is small enough, and we show that the problem cannot be solved if the error is sufficiently large. We apply the result to the bit security of “timed-release crypto” introduced by Rivest, Shamir and Wagner, to noisy exponentiation black-boxes and to the bit security of the “inverse” exponentiation. We also show that it implies a certain bit security result for Weil pairing on elliptic curves.

1. Introduction

For an integer \( m \geq 2 \) we denote by \( \mathbb{Z}_m \) the residue ring modulo \( m \), which we identify with the set of integers \( k \in \{0, \ldots, m - 1\} \); \( \mathbb{Z}_m^* \) is the subset of \( \mathbb{Z}_m \) consisting of the integers \( k \in \mathbb{Z}_m \) with \( \gcd(k, m) = 1 \). In particular, for a prime \( p \) we denote by \( \mathbb{F}_p \) the field of \( p \) elements. For integers \( s \) and \( m \geq 1 \) we denote by \( [s]_m \) the remainder of \( s \) on division by \( m \), and we write
\[
\|r\|_m = \min\{\lfloor r \rfloor_m, m - \lfloor r \rfloor_m\}.
\]
We also use \( \log z \) to denote the binary logarithm of \( z > 0 \).

In this paper, we study a variant of the hidden number problem introduced in 1996 by Boneh and Venkatesan [4, 5]. The original problem can be stated as follows: recover a number \( a \in \mathbb{F}_p \) such that for many known random \( t \in \mathbb{F}_p \) approximations to the values of \( \lfloor at \rfloor \) are known.

It turned out that for many applications, including some results about the bit security of Diffie-Hellman, Shamir and several other cryptosystems [8, 9] and for results on attacking the DSA and DSA-like signature schemes (both heuristically [10, 19] and rigorously [6, 20, 21]), the condition that \( t \) is selected uniformly at random from \( \mathbb{F}_p \) is too restrictive. It has been systematically exploited in the aforementioned papers [6, 8, 9, 20, 21, 28] that the method of [4, 5] can be adjusted...
to the case when $t$ is selected from a sequence which has some uniformity of distribution property. Thus bounds of exponential sums of various kinds have been used in these papers, as exponential sums are a natural tool to establish uniformity results. Similar results about recovering polynomials $f \in \mathbb{F}_p[X]$ from approximations to the values of $\lfloor f(t) \rfloor_p$ are known as well [27]. However, in all the above works the values of $t$ are assumed to be known exactly.

Here we consider the situation where this is no longer the case. Namely, we consider the following problem: recover a number $a \in \mathbb{F}_p$ such that for many random $t \in \mathbb{F}_p$ approximations to the values of both $\lfloor at \rfloor_p$ and $t$ are known. In fact we consider this problem modulo an arbitrary integer $m$.

We design a probabilistic polynomial time algorithm for this problem when the absolute error of approximation is $O(m^{1/5-\varepsilon})$. We apply this result to study the bit security of “timed-release crypto” introduced by Rivest, Shamir and Wagner [24]. We also use it to design a “correction” algorithm for noisy exponentiation black-boxes. This result is similar to those known for algebraic functions over finite fields [13]. Finally, we study the bit security of the “inverse” exponentiation which has recently appeared in several cryptographic scenarios, see [17, 25].

On the other hand, we also show that even modulo a prime $p$ the problem cannot be solved in polynomial time if the absolute error of approximation is $p^{1/2+\varepsilon}$ using uniformity of distribution results. This contrasts quite dramatically to the situation with the original hidden number problem, where the multipliers are known, in which case one can recover $a$ from crude approximations to $\lfloor at \rfloor_p$ of order $\Delta = p \exp(-\log p^{1/2+\varepsilon})$, see [4]. In fact, it is possible even for larger values of $\Delta$ with a nonuniform algorithm, see [5].

Hereafter the implied constants in symbols ‘$O$’ may occasionally, where obvious, depend on the small positive parameters $\varepsilon$ and are absolute otherwise; they are all effective and can be explicitly evaluated.

2. LATTICES

As in [4, 5], our results rely on rounding techniques in lattices. We therefore review a few related results and definitions.

Let $\{b_1, \ldots, b_s\}$ be a set of linearly independent vectors in $\mathbb{R}^s$. The set of vectors

$$ L = \{ z : z = \sum_{i=1}^{s} c_i b_i, \quad c_1, \ldots, c_s \in \mathbb{Z} \} $$

is called an $s$-dimensional full-rank lattice. The set $\{b_1, \ldots, b_s\}$ is called a basis of $L$. Such a basis is not unique.

A basic lattice problem is the closest vector problem (CVP), also called the nearest lattice point problem: given a lattice basis and a vector $u \in \mathbb{R}^n$, find a lattice vector minimizing the distance to $u$. There exists a polynomial-time algorithm that can approximate the closest vector problem up to some subexponential factor (see for instance [18, Section 2.1], or [22, Section 2.4], or [23, Section 2.4]).

**Lemma 1.** There exists a polynomial time algorithm which, given a lattice $L$ and a vector $u = (u_1, \ldots, u_s) \in \mathbb{R}^s$, finds a lattice vector $w = (w_1, \ldots, w_s)$ satisfying
the inequality
\[
\sum_{i=1}^s (w_i - u_i)^2 \leq \exp\left( O\left( \frac{s \log^2 \log s}{\log s} \right) \right) \times \min \left\{ \sum_{i=1}^s (z_i - u_i)^2, \ z = (z_1, \ldots, z_s) \in L \right\}.
\]

Proof. The statement is a combination of the Schnorr modification \[20\] of the lattice basis reduction algorithm of Lenstra, Lenstra and Lovász \[16\] with a result of Kannan \[12\] about reduction of the closest vector problem to the shortest vector problem. \[\square\]

In fact, for our applications we apply it in a better-known form with the constant \(2^s\) (as found by Babai \[2\]), namely
\[
\sum_{i=1}^s (w_i - u_i)^2 \leq 2^s \min \left\{ \sum_{i=1}^s (z_i - u_i)^2, \ z = (z_1, \ldots, z_s) \in L \right\}.
\]

Moreover, because in our applications the dimension \(s\) is fixed, we can also use algorithms which find the closest vector in a lattice in polynomial time (see \[11, 1\]).

The following result can be interpreted as a statement about short vectors in a certain two-dimensional lattice, and thus has some links with Lemma 1. However, as usual with two-dimensional lattices, continued fractions provide stronger statements and shorter proofs.

**Lemma 2.** There exists a polynomial time algorithm which, for a given \(Q \in [1, m]\), for any \(A \in \mathbb{Z}_m^*\) finds \(\lambda \in \mathbb{Z}_m^*\) such that
\[
0 < \|\lambda\|_m < Q \quad \text{and} \quad \|\lambda A\|_m \leq m/Q.
\]

Proof. Let \(P_i\) and \(Q_i\) denote respectively the numerator and denominator of the \(i\)th continued fraction convergents to \(A/m\), \(i \geq 1\). There exists \(j\) such that \(Q_j < Q \leq Q_{j+1}\). Then we have
\[
\left| \frac{A}{m} - \frac{P_j}{Q_j} \right| \leq \frac{1}{Q_j Q_{j+1}}.
\]
Therefore \(|AQ_j - mP_j| \leq m/Q_{j+1}\). Selecting \(\lambda = Q_j\), we obtain the desired statement. \(\square\)

3. Algorithm

**Theorem 1.** Let \(\varepsilon > 0\) and \(1 \geq \rho > 1/2\) be fixed real numbers and let \(m\) be a sufficiently large integer. Let \(T\) be a subset of \(\mathbb{Z}_m^*\) of cardinality
\[
\#T \geq 0.5m^\rho.
\]
We define
\[
\Delta = m^{(2\rho-1)/5-\varepsilon} \quad \text{and} \quad d = \left\lfloor 4\varepsilon^{-1}/5 \right\rfloor.
\]
Assume that the smallest prime divisor \(p\) of \(m\) satisfies the inequality
\[
p \geq (m/\Delta)^{1/2}.
\]
There exists a deterministic polynomial time algorithm \(A\) such that for any \(a \in \mathbb{Z}_m^*\), given \(2d + 1\) integers \(A, T_i, S_i \in [0, m - 1]\) with
\[
|a - A| \leq \Delta, \quad |t_i - T_i| \leq \Delta, \quad |[at_i]_m - S_i| \leq \Delta, \quad i = 1, \ldots, d.
\]
where \( t_1, \ldots, t_d \) are chosen uniformly and independently at random from \( T \), it outputs \( a \) with probability at least \( 1 + O(m^{-1}) \).

**Proof.** Using Lemma 2, we find a nonzero integer \( \lambda \) with

\[
\|\lambda\|_m \leq (m/\Delta)^{1/2} \quad \text{and} \quad \|\lambda A\|_m \leq (m\Delta)^{1/2}.
\]

We define \( V_i = [\lambda T_i]_m, U_i = [\lambda S_i]_m, i = 1, \ldots, d \). Let \( T_i - t_i = \delta_i, [at_i]_m - S_i = \Delta_i, i = 1, \ldots, d, \) and \( a - A = \alpha \). We have

\[
aV_i - U_i = a\lambda T_i - \lambda S_i \equiv a\lambda(t_i + \delta_i) - a\lambda t_i + \lambda\Delta_i \\
\equiv a\lambda\delta_i + \lambda\Delta_i \equiv A\lambda\delta_i + a\lambda\delta_i + \lambda\Delta_i \mod m,
\]

for \( i = 1, \ldots, d \). Therefore

\[
\|aV_i - U_i\|_m < \|A\lambda\|_m\|\delta_i\|_m + \|\alpha\|_m\|\lambda\|_m\|\delta_i\|_m + \|\lambda\|_m\|\Delta_i\|_m \\
\leq \|A\lambda\|_m\Delta + \|\lambda\|_m\Delta^2 + \|\lambda\|_m\Delta \leq 3m^{1/2}\Delta^{3/2}.
\]

We denote by \( \mathcal{L} \) the \( d + 1 \)-dimensional lattice generated by the rows of the following \((d + 1) \times (d + 1)\) matrix:

\[
\begin{pmatrix}
  m & 0 & \ldots & 0 & 0 \\
  0 & m & \ldots & 0 & 0 \\
  \vdots & \vdots & \vdots & \vdots & \vdots \\
  0 & 0 & \ldots & m & 0 \\
  V_1 & V_2 & \ldots & V_d & 1/m
\end{pmatrix}.
\]

Then we see that this lattice contains a vector \( v = (v_1, \ldots, v_d, v_{d+1}) \) with \( v_i \equiv aV_i \) (mod \( m \)), \( i = 1, \ldots, d, 0 \leq v_{d+1} = a/m < 1 \), and such that

\[
(1) \quad \sum_{i=1}^{d+1} (v_i - U_i)^2 \leq 9dm\Delta^3 + 1 \leq 10dm\Delta^3,
\]

where \( U_{d+1} = 0 \). To find \( v \) and thus to recover \( a \) we use the algorithm of Lemma 1 getting a lattice vector \( w = (w_1, \ldots, w_d, w_{d+1}) \) with

\[
(2) \quad \sum_{i=1}^{d+1} (w_i - U_i)^2 \leq 10d^2m\Delta^3.
\]

We show that with probability \( 1 + O(m^{-1}) \) we have \( v = w \).

Let \( w = (w_1, \ldots, w_d, w_{d+1}) \), where \( w_i \equiv bV_i \) (mod \( m \)), \( i = 1, \ldots, d \), and \( w_{d+1} = b/m \) with some integer \( b \in [0, m - 1] \).

From (1) and (2) we derive

\[
(w_i - v_i)^2 \leq (v_i - U_i)^2 + (w_i - U_i)^2 \leq 20d^4m\Delta^3, \quad i = 1, \ldots, d + 1.
\]

Therefore for every \( i = 1, \ldots, d \) the inequality

\[
(3) \quad \|(a - b)\lambda T_i\|_m = \|(a - b)V_i\|_m = |w_i - v_i| \leq 5d^{1/2}2d^2m^{1/2}\Delta^{3/2}
\]

holds.

If \( a \equiv b \mod m \), then \( v = w \).

For each \( c \in \mathbb{Z}_m \) with \( \gcd(c, m) = f \) and every integer \( h \in [0, m/2) \) there are at most

\[
f \left( \frac{2h + 1}{f} \right) + 1 \leq 2h + f + 1
\]

values of \( T \in \mathbb{Z}_m \) with \( \|cT\|_m \leq h \).
because of the conditions of the theorem we have $0 < |\lambda| \leq (m/\Delta)^{1/2} < p$; thus $\gcd(\lambda, m) = 1$. Assume that $a \not\equiv b \pmod{m}$. Then
\[
\gcd((a - b)\lambda, m) \leq m/p \leq (m\Delta)^{1/2}.
\]
Hence the inequality
\[
\|(a - b)\lambda T\|_m \leq 5d^{1/2}2^{d/2}m^{1/2}\Delta^{3/2}
\]
holds for at most
\[
10d^{1/2}2^{d/2}m^{1/2}\Delta^{3/2} + (m\Delta)^{1/2} + 1 \leq 11d^{1/2}2^{d/2}m^{1/2}\Delta^{3/2}
\]
values of $T \in \mathbb{Z}_m$. For each $T$ there could be at most $2\Delta + 1 \leq 3\Delta$ values of $t \in \mathbb{Z}_m^*$ with $|t - T| \leq \Delta$.

Thus for each $i = 1, \ldots, d$ there are at most $33d^{1/2}2^{d/2}m^{1/2}\Delta^{5/2}$ values of $t_i \in \mathbb{Z}_m^*$ for which (3) holds.

Hence the probability that (3) holds for every $i = 1, \ldots, d$ when $t_1, \ldots, t_d$ are chosen uniformly and independently at random from $\mathbb{Z}_m^*$ is at most
\[
\left(\frac{33d^{1/2}2^{d/2}m^{1/2}\Delta^{5/2}}{\#T}\right)^d \leq \left(\frac{33d^{1/2}2^{d/2}m^{1/2}\Delta^{5/2}}{0.5mp}\right)^d \leq \left(\frac{66d^{1/2}2^{d/2}}{m^{-5d\varepsilon/2}}\right)^d m^{-5d\varepsilon/2}
\]
provided that $m$ is large enough. Thus the probability that this happens for at least one $b \in \mathbb{Z}_m$ is at most
\[
\left(\frac{66d^{1/2}2^{d/2}}{m^{-5d\varepsilon/2}}\right)^d m^{-1} \leq \left(\frac{66d^{1/2}2^{d/2}}{m^{-5d\varepsilon/2}}\right)^d m^{-1},
\]
and the result follows. \hfill \qed

Recalling that the smallest prime divisor $p$ of $m$ satisfies the inequality
\[
p \geq (m/\Delta)^{1/2} \geq m^{(2-\rho)/5+\varepsilon/2} \geq m^{2/5} > m^{1/3},
\]
we see that $m$ has at most two prime divisors. Therefore
\[
\#\mathbb{Z}_m^* \geq m(1 - 1/p)^{O(1)} = m + O(m^{3/5}).
\]
Hence for $T = \mathbb{Z}_m^*$ one can apply Theorem \ref{thm:main} with $\rho = 1$ and thus with $\Delta = m^{1/5-\varepsilon}$.

It is easy to see that Theorem \ref{thm:main} applies to prime values of $m = p$ as well as to RSA moduli $m = pl$ which are products of two primes $p < l < 2p$.

4. APPLICATIONS

Here we show how to apply Theorem \ref{thm:main} to the bit security of “timed-release crypto” introduced by Rivest, Shamir and Wagner in \cite{rivest1988timed}, and to noisy exponentiation black-boxes.

We recall that the construction of \cite{rivest1988timed} relies on the assumed hardness of computing the function $[\vartheta^e]_m$, where the positive integers $\vartheta, e, s, m$ are publicly known. Certainly, if the Euler function $\varphi(m)$ of $m$ is known, then it can be computed very efficiently by computing
\[
E \equiv e^s \pmod{\varphi(m)}, \quad 0 \leq E \leq \varphi(m),
\]
in $O(\log s)$ modular multiplications and then by computing
\[
\vartheta^e \equiv \vartheta^{de} \pmod{m}.
\]
Otherwise it is assumed that any algorithm to compute this value takes at least \( s \) consecutive exponentiations (even if unlimited parallelism is allowed).

We show that Theorem 1 implies a certain result about the bit security of this function. We remark that in [22] this scheme is considered with \( e = 2 \). Here we consider a slightly different case of \( \gcd(e, \varphi(m)) = 1 \). If the largest power of 2-adic order of the Carmichael function \( \lambda(m) \), is not too large (which is true for the overwhelming majority of the moduli), then the case \( e = 2 \) can be considered as well.

Let \( \mathcal{RSW}_\Delta \) denote an oracle which, given any \( v \in \mathbb{Z}_m^* \), outputs some \( V \) such that \( \left| \left[ v^e \right]_m - V \right| \leq \Delta \).

**Theorem 2.** Let \( \varepsilon > 0 \) be a fixed real number and let \( m \) be a sufficiently large integer. We define
\[
\Delta = m^{1/5-\varepsilon}.
\]
Assume that the smallest prime divisor \( p \) of \( m \) satisfies the inequality
\[
p \geq (m/\Delta)^{1/2}.
\]
Given an oracle \( \mathcal{RSW}_\Delta \), there exists a probabilistic polynomial time algorithm \( A \) such that for any \( \vartheta \in \mathbb{Z}_m^* \) it makes the expected number \( O(\varepsilon^{-1}) \) of calls of the oracle \( \mathcal{RSW}_\Delta \) and computes \( \left[ \vartheta^e \right]_m \) with probability at least \( 1 + O(m^{-1}) \).

**Proof.** First of all we remark that, because \( \gcd(e, \varphi(m)) = 1 \) when \( v \in \mathbb{Z}_m^* \) is selected uniformly at random, the value of \( \left[ v^e \right]_m \) is uniformly distributed in \( \mathbb{Z}_m^* \) as well. Now making calls of the oracle \( \mathcal{RSW}_\Delta \) with \( v = \vartheta \) and with \( v = u_i \) and \( v = \vartheta u_i, i = 1, \ldots, d \), for \( d = \lceil 4\varepsilon^{-1}/5 \rceil \) values of \( u_i \in \mathbb{Z}_m^* \) chosen uniformly at random, we apply the algorithm of Theorem 1 to derive the result.

Thus, Theorem 2 implies that \( k = \lceil (4/5 - \varepsilon) \log m \rceil \) of the most significant bits of \( \left[ \vartheta^e \right]_m \) are as secure as the whole value.

Let \( g \in \mathbb{F}_p^* \) be a fixed element of multiplicative order \( \tau \), which is the smallest positive integer \( k \) for which
\[
\vartheta^k \equiv 1 \pmod{m}.
\]

Let \( \mathcal{E\mathcal{X}\mathcal{P}}_\Delta \) denote an oracle which, given any \( v \in [0, \tau - 1] \), outputs \( V \) such that
\[
\left| \left[ g^v \right]_p - V \right| \leq \Delta.
\]

**Theorem 3.** Let \( \varepsilon > 0 \) and \( 1 \geq \rho > 1/2 \) be fixed real numbers and let \( g \) be of multiplicative order \( \tau \geq 0.5p^\rho \), where \( p \) is a sufficiently large prime. We define
\[
\Delta = p^{(2p-1)/5-\varepsilon}.
\]
Given an oracle \( \mathcal{E\mathcal{X}\mathcal{P}}_\Delta \), there exists a probabilistic polynomial time algorithm \( A \) such that for any \( s \in [0, \tau - 1] \) it makes the expected number \( O(\varepsilon^{-1}) \) of calls of the oracle and computes \( \left[ g^s \right]_p \) with probability at least \( 1 + O(p^{-1}) \).

**Proof.** Let \( G \subseteq \mathbb{F}_p^* \) be the multiplicative group generated by \( g \). First of all we remark that when \( v \in [0, \tau - 1] \) is selected uniformly at random, the value of \( \left[ g^v \right]_p \) is uniformly distributed in \( G \) and \( \#G = \tau \geq 0.5p^\rho \). Now making calls of the oracle \( \mathcal{E\mathcal{X}\mathcal{P}}_\Delta \) with \( v = s \) and with \( v = u_i \) and \( v = s + u_i, i = 1, \ldots, d \), for \( d = \lceil 4\varepsilon^{-1}/5 \rceil \) values of \( u_i \in [0, p - 2] \) chosen uniformly at random, we apply the algorithm of Theorem 1 to derive the result.
Of course the result of Theorem 3 makes sense only if \( g \) is unknown. In fact, applying Theorem 3 with \( s = 1 \), one can simply recover \( \lfloor g \rfloor_p \) first and then use repeated squaring to compute \( \lfloor g^s \rfloor_p \) for any \( s \).

Theorem 3 is also related to the reconstruction of linear congruential generators of pseudorandom numbers, see [7, 15], but has a different flavour and seems to be independent of these results.

We now assume that the multiplicative order \( \tau \) of \( g \in \mathbb{F}_p \) is prime, and for \( v \in [1, \tau - 1] \) we denote by \( \overline{v} \) the multiplicative inverse of \( v \) modulo \( \tau \), that is, \( v \overline{v} \equiv 1 \pmod{\tau} \).

Let \( \mathcal{IDH}_\Delta \) denote an oracle which, given \( \lfloor g^v \rfloor_p \) with \( v \in [1, \tau - 1] \), outputs \( V \) such that \( \left| \lfloor g^\overline{v} \rfloor_p - V \right| \leq \Delta \).

**Theorem 4.** Let \( \varepsilon > 0 \) and \( 1 \geq \rho > 1/2 \) be fixed real numbers and let \( g \) be of multiplicative order \( \tau \geq 0.6 \rho \), where \( \tau \) and \( p \) are a sufficiently large primes. We define
\[
\Delta = p^{(2\rho - 1)/5 - \varepsilon}.
\]
Given an oracle \( \mathcal{IDH}_\Delta \), there exists a probabilistic polynomial time algorithm \( A \) such that for any \( s \in [0, \tau - 1] \), given \( S = \lfloor g^s \rfloor_p \) it makes the expected number \( O(\varepsilon^{-1}) \) of calls of the oracle and computes \( \lfloor g^\overline{s} \rfloor_p \) with probability at least \( 1 + O(p^{-1}) \).

**Proof.** Let \( G \subseteq \mathbb{F}_p^\ast \) be the multiplicative group generated by \( g \). First of all we remark that when \( v \in [1, \tau - 2] \) is selected uniformly at random, then the value of \( \lfloor g^v \rfloor_p \) is uniformly distributed in \( G = G \setminus \{1, g^{-1}\} \) and \( \#G = \tau - 2 \geq 0.5 \rho \). Now making calls of the oracle \( \mathcal{IDH}_\Delta \) with
\[
\lfloor S^{v_i} \rfloor_p = \lfloor g^{sv_i} \rfloor_p \quad \text{and} \quad \lfloor S^{w_i} \rfloor_p = \lfloor g^{sw_i} \rfloor_p,
\]
where \( v_i = (u_i + 1) \) and \( w_i = u_i \), we obtain approximations to \( \lfloor g^{u_i} \rfloor_p \) and to \( \lfloor g^{w_i} \rfloor_p \), for \( d = \lfloor 4 \varepsilon^{-1}/5 \rfloor \) values of \( u_i \in [1, \tau - 2] \) chosen uniformly at random, and we apply the algorithm of Theorem 1 to derive the result. \( \square \)

It would be interesting to obtain the same result for arbitrary multiplicative orders \( \tau \) without the restriction that it must be prime, in particular for \( \tau = p - 1 \) (that is, for primitive roots \( g \)). On the other hand, typically in cryptographic applications elements of prime multiplicative order are of special interest. It can also be relevant to recall that we know from [7] that for infinitely many primes \( p \), \( p - 1 \) has a prime divisor \( \tau \geq p^{0.677} \) (thus it overlaps with the region where Theorem 4 applies).

5. **Lower bound**

Here we show that Theorem 4 cannot be substantially improved. Namely, if \( \Delta = m^{1/2 + \varepsilon} \), then for every \( a \in \mathbb{Z}_m^\ast \) there are exponentially many integers \( b \in \mathbb{Z}_m^\ast \) which cannot be distinguished from \( a \) based only on the inequalities of Theorem 4.

This lower bound is based on a result about the uniformity of distribution of the pairs \( (\tau, \lfloor b \tau \rfloor_m) \), \( \tau \in \mathbb{Z}_m \). For simplicity we obtain our lower bound for \( m = p \) prime, but the result can easily be extended to arbitrary moduli.

**Theorem 5.** Let \( \varepsilon > 0 \) be fixed and let \( p \) be a sufficiently large prime. Put
\[
\Delta = p^{1/2 + \varepsilon}.
\]
There exists a set \( \mathcal{A} \subseteq \mathbb{F}_p^* \) of cardinality \( \#\mathcal{A} \geq 4\Delta - 3 \) such that for any \( a \in \mathcal{A} \) and any \( A \in \mathbb{F}_p \) with \(|a - A| \leq \Delta\) there exists a set \( \mathcal{F}_{a,A} \) of cardinality \( \#\mathcal{F}_{a,A} = 2\Delta + O(\Delta p^{-\varepsilon}) \) which satisfies the following property. For any number \( 2d \) of integers \( T_1, S_i \in [0, p - 1] \) such that

\[
|t_i - T_i| \leq \Delta \quad \text{and} \quad |[at_i]_p - S_i| \leq \Delta, \quad i = 1, \ldots, d,
\]

for some \( t_1, \ldots, t_d \in \mathbb{F}_p^* \), for any \( b \in \mathcal{F}_{a,A} \) there are some \( \tau_1, \ldots, \tau_d \in \mathbb{F}_p^* \) for which we have

\[
|b - A| \leq \Delta, \quad |\tau_i - T_i| \leq \Delta, \quad |[b\tau_i]_p - S_i| \leq \Delta, \quad i = 1, \ldots, d.
\]

**Proof.** Let \( e_p(z) = \exp(2\pi iz/p) \). We recall the identity (see Exercise 11.a in Chapter 3 of [30])

\[
\sum_{c=0}^{p-1} e_p(cu) = \begin{cases} 
0, & \text{if } u \not\equiv 0 \pmod{p}, \\
p, & \text{if } u \equiv 0 \pmod{p},
\end{cases}
\]

which holds for any integer, and the inequality (see Exercise 11.b in Chapter 3 of [30])

\[
\left| \sum_{u=K+1}^{K+H} e_p(cu) \right| \leq \frac{p}{2||c||_m},
\]

which holds for any integer \( c \) with \( 1 \leq c \leq p - 1 \) and any integer \( H \).

Given \( b \in \mathbb{F}_p^* \) and two intervals \( I = [K + 1, K + H] \) and \( J = [L + 1, L + G] \), let us denote by \( N_b(I, J) \) the number of \( \tau \in \mathbb{F}_p^* \) such that \( \tau \equiv s \pmod{p} \) for some \( s \in I \) and \([as]_p \equiv r \pmod{p} \) for some \( r \in J \). We also put

\[
D_b = \max_{I,J} \left| N_b(I, J) - \frac{\mu(I)\mu(J)}{p} \right|,
\]

where the maximum is taken over all intervals \( I \) and \( J \), and \( \mu(I) \) and \( \mu(J) \) are the lengths of \( I \) and \( J \), respectively.

Using (4), we obtain

\[
N_b(I, J) = \frac{1}{p} \sum_{s \in I} \sum_{r \in J} \sum_{c=0}^{p-1} e_p(c(bs - r))
\]

\[
= \frac{1}{p} \sum_{c=0}^{p-1} e_p(cbs) \sum_{r \in J} e_p(-cr).
\]

Separating the term \( \mu(I)\mu(J)/p \) corresponding to \( c = 0 \) and using (4), we obtain

\[
\left| N_b(I, J) - \frac{\mu(I)\mu(J)}{p} \right| \leq \frac{1}{4} \sum_{c=1}^{p-1} \frac{1}{||c||_m||bc||_m}.
\]

Hence,

\[
\sum_{b=1}^{p-1} D_b \leq \frac{p}{4} \sum_{c=1}^{p-1} \frac{1}{||c||_m} \sum_{b=1}^{p-1} \frac{1}{||bc||_m}
\]

\[
= \frac{p}{4} \sum_{c=1}^{p-1} \frac{1}{||c||_m} \sum_{b=1}^{p-1} \frac{1}{||b||_m} = O(p \log^2 p).
\]
Let $B$ be the set of $b \in \mathbb{F}_p^*$ for which $D_b > p^{3\varepsilon/2}$. Then from the previous inequality we conclude that
\[
\#Bp^{3\varepsilon/2} < \sum_{b \in B} D_b = O\left(p \log^2 p\right).
\]

Thus $\#B = O\left(p^{1-3\varepsilon/2} \log^2 p\right) = O\left(p^{1-\varepsilon}\right)$, provided that $p$ is large enough.

Put $L = \lfloor p/2\Delta \rfloor$. Separate the interval $[0, p - 1]$ into $N$ nonintersecting half-open subintervals $[ip/L, (i + 1)p/L)$, $i = 0, \ldots, L - 1$, of length $m/L > \Delta$. Let $C = [i_0p/L, (i_0 + 1)p/L)$ be the subinterval with
\[
\#(C \cap B) \leq \#B/L = O\left(\Delta p^{-\varepsilon}\right).
\]

We put $A = [i_0m/L + 3\Delta, (i_0 + 1)m/L - 3\Delta]$. Select any $a \in A$. Thus for any $A$ with $|a - A| \leq \Delta$ the interval $[A - \Delta, A + \Delta] \subseteq A$ contains at least $2\Delta + O\left(\Delta p^{-\varepsilon}\right)$ elements $b$ with $D_b < p^{3\varepsilon/2}$. We denote the set of such elements by $F_{a,A}$.

Let $T, S \in [0, p - 1]$. We consider the intervals
\[
T = [T - \Delta, T + \Delta] \cap [0, p - 1] \quad \text{and} \quad S = [S - \Delta, S + \Delta] \cap [0, p - 1].
\]

Then for any $b \in F_{a,A}$ we have $N_b(T, S) > 0$. Indeed, because $\mu(T) \geq \Delta$ and $\mu(S) \geq \Delta$, we derive
\[
N_b(T, S) \geq \frac{\mu(T)\mu(S)}{p} - D_b > \Delta^2 p^{-1} - p^{3\varepsilon/2} = p^{2\varepsilon} - p^{3\varepsilon/2} > 0.
\]

Remark: we see from Theorem 4 that for any number $d$ of approximations $T_i$ and $S_i$, $i = 1, \ldots, d$, with absolute error $O\left(p^{1/2+\varepsilon}\right)$, exponentially many “hidden” elements $a \in \mathbb{F}_p^*$ cannot be distinguished from almost all elements of the interval $[A - \Delta, A + \Delta]$. In the next result we show that for approximations with absolute error $O\left(p^{2/3+\varepsilon}\right)$ this holds for all $a \in \mathbb{F}_p$.

**Theorem 6.** Let $\varepsilon > 0$ be fixed and let $p$ be a sufficiently large prime. Put
\[
\Delta = p^{2/3+\varepsilon}.
\]

For any $a \in \mathbb{F}_p$ and any $A \in [\Delta, p - \Delta - 1]$ with $|a - A| \leq \Delta$ there exists a set $F_{a,A}$ of cardinality $\#F_{a,A} = 2\Delta + O\left(\Delta p^{-\varepsilon}\right)$ which satisfies the following property. For any number $2d$ of integers $T_1, S_1, \ldots, T_d, S_d \in [0, p - 1]$ such that
\[
|t_i - T_i| \leq \Delta \quad \text{and} \quad \left|\left[\frac{at_i}{p}\right] - S_i\right| \leq \Delta, \quad i = 1, \ldots, d,
\]
for some $t_1, \ldots, t_d \in \mathbb{F}_p$, for any $b \in F_{a,A}$ there are some $\tau_1, \ldots, \tau_d \in \mathbb{F}_p^*$ for which we have
\[
|b - A| \leq \Delta, \quad |\tau_i - T_i| \leq \Delta, \quad \left|\left[\frac{b\tau_i}{p}\right] - S_i\right| \leq \Delta, \quad i = 1, \ldots, d.
\]

**Proof.** We use the definition of $D_b$ from the proof of Theorem 5.

Let $B$ be the set of $b \in \mathbb{F}_p^*$ for which $D_b > p^{1/3+\varepsilon}$. As in the proof of Theorem 5 we conclude that
\[
\#Bp^{1/3+3\varepsilon/2} < \sum_{b \in B} D_b = O\left(p \log^2 p\right).
\]

Thus $\#B = O\left(p^{2/3+3\varepsilon/2} \log^2 p\right) = O\left(\Delta p^{-\varepsilon}\right)$, provided that $p$ is large enough.

Thus for any $A$ with $|a - A| \leq \Delta$ the interval $[A - \Delta, A + \Delta] \subseteq A$ contains at least $2\Delta + O\left(\Delta p^{-\varepsilon}\right)$ elements $b$ with $D_b < p^{3\varepsilon/2}$. We denote the set of such elements by $F_{a,A}$.
Let $T, S \in [0, p - 1]$. We consider the intervals

$$T = [T - \Delta, T + \Delta] \cap [0, p - 1] \quad \text{and} \quad S = [S - \Delta, S + \Delta] \cap [0, p - 1].$$

Then for any $b \in F_{a,A}$ we have $N_b(T, S) > 0$. Indeed, because $\mu(T) \geq \Delta$ and $\mu(S) \geq \Delta$, we derive

$$N_b(T, S) \geq \frac{\mu(T)\mu(S)}{p} - D_b > \Delta^2 p^{-1} - p^{1/3+\varepsilon} = p^{1/3+2\varepsilon} - p^{1/3+\varepsilon} > 0,$$

and the desired result follows.

Obviously the same result holds for $A$ outside of the interval $[\Delta, p - \Delta - 1]$, but the cardinality $\#F_{a,A}$ becomes asymptotically equal to the length of the interval $[A - \Delta, A + \Delta] \cap [0, p - 1]$.

6. Generalizations and open questions

It would be very important to extend Theorem 1 to the case when the multipliers $t_i$ are selected from a sufficiently large subgroup $G$ of $\mathbb{Z}_m^\times$.

In particular, this would imply an analogue of Theorem 2 with $e = 2$ corresponding to the choice of $e$ suggested in [14]. Also, one would be able to obtain an analogue of Theorem 3 modulo a composite and when $g$ is not necessarily a primitive root but rather generates a subgroup of $\mathbb{Z}_m^\times$ of sufficiently large order.

It is easy to see that, using the exponential sums technique in the same style as it is done in [13, 14, 20, 21], one can obtain an analogue of Theorem 1 in the case when the multipliers $t_i$ are selected from a subgroup $G$ of $\mathbb{Z}_m^\times$. Using the bounds of exponential sums from [14], and some other previously known bounds, such results can be established for subgroups of size

- $\#G \geq m^{1/2+\varepsilon}$ for composite $m$,
- $\#G \geq p^{1/3+\varepsilon}$ for prime $m = p$,
- $\#G \geq p^\varepsilon$ for almost all prime $m = p$.

Certainly increasing the admissible values of $\Delta$ from $m^{1/5-\varepsilon}$ to a large value would be a very interesting result. For example, it would be very interesting to show that a certain portion $k = o(\log m)$ of the most significant bits of $[\vartheta_{2\varepsilon}]_m$ are as secure as the whole value. Here we describe another possible approach which can possibly lead to better bounds.

Assume we are given four integers $T_i$ and $S_i$ with

$$|t_i - T_i| \leq \Delta, \quad |(at_i)_m - S_i| \leq \Delta, \quad i = 1, 2,$$

where $t_1$ and $t_2$ are chosen uniformly and independently at random from $\mathbb{Z}_m^\times$.

We define $V_i = [\lambda T_i]_m$ and $U_i = [\lambda S_i]_m$, $i = 1, 2$.

Let $T_i - t_i = \delta_i$ and $|at_i)_m - S_i = \Delta_i$, $i = 1, 2$. From the congruences

$$a(T_i + \delta_i) \equiv S_i + \Delta_i \quad (\text{mod } m) \quad i = 1, 2,$$

we conclude that

$$(T_1 + \delta_1)(S_2 + \Delta_2) \equiv (T_2 + \delta_2)(S_1 + \Delta_1) \quad (\text{mod } m).$$

Therefore for some integer $k$ we have

$$S_2\delta_1 - S_1\delta_2 + T_1\Delta_2 - T_2\Delta_1 + km = T_2S_1 - T_1S_2 + \delta_2\Delta_1 - \delta_1\Delta_2.$$
We denote by $L$ the 5-dimensional lattice generated by the rows of the following $5 \times 5$ matrix:

$$
A = \begin{pmatrix}
\Delta & 0 & 0 & 0 & S_2 \\
0 & \Delta & 0 & 0 & S_1 \\
0 & 0 & \Delta & 0 & T_2 \\
0 & 0 & 0 & \Delta & T_1 \\
0 & 0 & 0 & 0 & m
\end{pmatrix}.
$$

Let us consider the vector $u \in L$ defined as follows:

$$
u = (\delta_1, -\delta_2, \Delta_2, -\Delta_1, k)A
= (\delta_1, -\delta_2, \Delta_2, -\Delta_1, \delta_1, S_2\delta_1 - S_1\delta_2 + T_1\Delta_2 - T_2\Delta_1 + km)
$$

and another vector $v = (0, 0, 0, 0, T_2S_1 - T_1S_2)$.

From (6) we see that the distance between the vectors $u$ and $v$ is $O(\Delta^2)$. Taking into account that the determinant of the lattice $L$ is $\Delta^4m$, we see that any five-dimensional ball of radius $\Delta^{4/5}m^{1/5-\varepsilon}$ is very unlikely (heuristically) to contain more than one lattice vector. Thus, if $\Delta = m^{1/6-\varepsilon}$, then $u$ is probably the only lattice vector within the distance $O(\Delta^2)$ out of $v$ and thus will be recovered by the lattice reduction algorithm. Although this approach in the above form has led to a weaker bound on $\Delta$ than that of Theorem 1, it can be generalised to, and used with, several values of $t_1, \ldots, t_d$. Also notice that the method does not need any initial approximation to $a$ and applies to arbitrary moduli $m$. It may be shown that heuristically this technique should work with $\Delta = m^{1/4-\varepsilon}$ as $d \to \infty$; however, it seems hard to turn this approach into a provable statement, as has been done in Theorem 1.

We also remark that Theorem 1 gives a certain result for the Weil pairing on elliptic curves. Namely, let $s$ be a divisor of $p - 1$. Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$ of $q$ elements, and let $E_{tor}[s]$ denote the $s$-torsion group of $E$, which consists of points $P \in E$ (including points over the extensions of $\mathbb{F}_p$) for which $sP = O$, the point at infinity. We recall that the Weil pairing of order $s$,

$$
e_s : E_{tor}[s] \times E_{tor}[s] \to \mathbb{F}_p^*,$$

mapping pairs of points from $E_{tor}[s]$ to the uniquely defined subgroup of order $s$ of $\mathbb{F}_p^*$, satisfies

$$
e_s(R, P + Q) = e_s(R, P)e_s(R, Q)
$$

for any points $P, Q, R \in E_{tor}[s]$, see [29]. Therefore, if $s \geq p^{1/2+\varepsilon}$, then, given an oracle which for an unknown point $U \in E_{tor}[s]$ and a given point $T \in E_{tor}[s]$ outputs some approximation to $e_s(U, T)$ (the required precision depends on the size of $s$, as in Theorem 1), one can compute $e_s(U, P)$ for any $P \in E_{tor}[s]$. Indeed, one can use this oracle to approximate $e_s(U, P + T)$, $e_s(U, P)$ and $e_s(U, T)$ for polynomially many random points $T \in E_{tor}[s]$, getting the situation of Theorem 1.

Finally, Theorems 5 and 6 show that one cannot obtain an analogue of Theorem 1 with substantially larger values of $\Delta$. For example, it cannot be obtained with $\Delta = p \exp(-(\log p)^{1/2+\varepsilon})$ as it was for the original hidden number problem of [4, 5]. However, it would still be very interesting to try to improve Theorems 2 and 3 in order to reduce the gap between algorithmic results and impossibility results.

Acknowledgment. The authors thank Mats Näslund for the idea of applying their results to Weil pairing.
References


IBM T. J. Watson Research Center, Hawthorne, NY 10532, USA
E-mail address: nahg@watson.ibm.com

D´epartement d’Informatique, École Normale Sup´erieure, 45, rue d’Ulm, 75230 Paris Cedex 05, France
E-mail address: pnguyen@ens.fr

Department of Computing, Macquarie University, New South Wales 2109, Australia
E-mail address: igor@ics.mq.edu.au