CLOSE VALUES OF SHIFTED MODULAR INVERSIONS
AND THE DECISIONAL MODULAR INVERSION
HIDDEN NUMBER PROBLEM

IGOR E. SHPARLINSKI
Department of Pure Mathematics
University of New South Wales
Sydney, NSW 2052, Australia

(Communicated by Marcus Greferath)

Abstract. We give deterministic polynomial time algorithms for two different decision version the modular inversion hidden number problem introduced by D. Boneh, S. Halevi and N. A. Howgrave-Graham in 2001. For example, for one of our algorithms we need to be given about 1/2 of the bits of each inversion, while for the computational version the best known algorithm requires about 2/3 of the bits and is probabilistic.

1. Introduction

The hidden number problem, introduced and studied by Boneh and Venkatesan [3, 4], has played an important role in several cryptographic algorithms and has been generalised in a number of directions, see [17] for a survey of relevant results and also [1] for some recent developments within a new approach. Here we consider a modification of the original problem which has been suggested by Boneh, Halevi and Howgrave-Graham [2].

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

Motivated by several cryptographic applications, such as constructions of efficient and reliable pseudorandom number generators, and an analogy with the original hidden number problem of [3, 4], Boneh, Halevi and Howgrave-Graham [2] have introduced the modular inversion hidden number problem, where the goal is to recover a “hidden” shift \( s \in \mathbb{F}_p \) from approximations to the inversions \( (s + x)^{-1} \in \mathbb{F}_p \) for several field elements \( x \in \mathbb{F}_p \), where hereafter we set

\[
0^{-1} = 0
\]

(thus, alternatively one can say that we are given approximations to \( (s + x)^{p-2} \)).

More precisely, for \( z \in \mathbb{F}_p \) we denote by \( \text{MSB}_\ell(z) \) any \( u \in \mathbb{F}_p \) such that

\[
|z - u| \leq p/2^{\ell+1}.
\]

We then extend this definition to integer values of \( z \) in a natural way. Roughly speaking, \( \text{MSB}_\ell(z) \) gives \( \ell \) most significant bits of the remainder on division of \( z \) by \( p \). However, this definition is more flexible and suits better our purposes. In particular we remark that \( \ell \) in the above inequality need not be an integer.

2010 Mathematics Subject Classification: Primary: 11T71; Secondary: 11D85, 94A60.
Key words and phrases: Shifted inversion, hidden number problem, congruences, small solutions.
Boneh, Halevi and Howgrave-Graham [2] have introduced and studied the following problem, which is natural to call Computational Modular Inversion Hidden Number Problem:

\[ \text{CMIHNP: Given an oracle } \mathcal{O}_{\ell,s}, \text{ that for } x \in \mathbb{F}_p \text{ outputs } \mathcal{O}_{\ell,s}(x) = \text{MSB}_\ell \left( (s + x)^{-1} \right), \text{ recover } s \in \mathbb{F}_p. \]

Let

\[ n = \left\lceil \frac{\log p}{\log 2} \right\rceil \]

be the bit length of \( p \).

Developing and extending some ideas of [2], Ling, Shparlinski, Steinfeld and Wang [14] have given a rigorously analysed algorithm for the CMIHNP, that, for any fixed \( \varepsilon > 0 \), a sufficiently large \( p \) and \( \ell > (2/3 + \varepsilon)n \), with overwhelming probability recovers \( s \) in polynomial time, by querying \( \mathcal{O}_{\ell,s} \) at randomly chosen elements \( x \in \mathbb{F}_p \). We remark, that although the oracle queries are randomised, rest of the algorithm of [2] is deterministic.

Here we consider two modification of the CMIHNP, which we call the Decisional Modular Inversion Hidden Number Problems. More precisely, we consider:

\[ \text{DMIHNP-1: Given } t \in \mathbb{F}_p \text{ and an oracle } \mathcal{O}_{\ell,s}, \text{ that for } x \in \mathbb{F}_p \text{ outputs } \mathcal{O}_{\ell,s}(x) = \text{MSB}_\ell \left( (s + x)^{-1} \right), \text{ decide whether } s = t; \]

and

\[ \text{DMIHNP-2: Given two oracles } \mathcal{O}_{\ell,s} \text{ and } \mathcal{O}_{\ell,t}, \text{ that for } x \in \mathbb{F}_p \text{ output } \mathcal{O}_{\ell,s}(x) = \text{MSB}_\ell \left( (s + x)^{-1} \right) \text{ and } \mathcal{O}_{\ell,t}(x) = \text{MSB}_\ell \left( (t + x)^{-1} \right), \text{ respectively, decide whether } s = t. \]

For example, for DMIHNP-1, we give a polynomial time deterministic algorithm which works for less precise oracles \( \mathcal{O}_{\ell,s} \) than those in [14], namely for oracles \( \mathcal{O}_{\ell,s} \) with \( \ell > (1/2 + \varepsilon)n \). We remark that such an algorithm can also be considered as a deterministic verification of the output of the algorithm of [14] which may occasionally output wrong answers.

For DMIHNP-2, we need the oracle of the same strength as in [14], however the algorithm is deterministic.

The previously known heuristic [2] and rigorous [14] algorithms have been based on lattice algorithms. Here we use a very different approach which is based on studying the frequency of close values of two rational function \( (X+s)^{-1}, (X+t)^{-1} \in \mathbb{F}_p(X) \), computed on a short interval \( I \) of consecutive values \( \{u+1, \ldots, u+h\} \subseteq \mathbb{F}_p \). In turn, these number theoretic results are based on the method introduced by Cilleruelo and Garaev [6], and then extended in several more works [5, 7, 8]. We believe that these results can be of independent interest, and can also be used for several modifications of the DMIHNP-1 and DMIHNP-2, for example, with “noisy” oracles, see Section 5.

Throughout the paper, all implied constants in the symbols ‘\( O \)’ are absolute, unless stated otherwise.

2. Preparations

Here we collect some number theoretic results.

For an integer \( a \) we used \( \|a\|_p \) to denote the smallest by absolute value residue of \( a \) modulo \( p \), that is

\[ \|a\|_p = \min_{k \in \mathbb{Z}} \left| a - kp \right|. \]
First, we recall [8, Lemma 3.2], which follows easily from the Dirichlet pigeon-hole principle.

**Lemma 2.1.** For any real numbers $U_1, \ldots, U_\nu$ with
\[ p > U_1, \ldots, U_\nu \geq 1 \quad \text{and} \quad U_1 \ldots U_\nu \geq p^{\nu - 1} \]
and any integers $a_1, \ldots, a_\nu$ there exists an integer $u$ with $\gcd(u, p) = 1$ and such that
\[ \|a_iu\|_p = O(U_i), \quad i = 1, \ldots, \nu, \]
where the implied constant depends only on $\nu$.

Let $\tau(m)$ denote the number of positive integer divisors of an integer $m \geq 1$.

The following result follows immediately from a stronger and much more general estimate of Shiu [16, Theorem 2] (taken with $\lambda = 1$ and $x = y$), which in turn is a very special case of [16, Theorem 1]; even more general results are given by Nair and Tenenbaum [15].

**Lemma 2.2.** For any fixed real $\varepsilon > 0$, and integers $M \geq p^{1+\varepsilon}$ and $a \not\equiv 0 \pmod{p}$,
\[ \sum_{m \leq M \atop m \equiv a \pmod{p}} \tau(m) = O(Mp^{-1} \log M), \]
where the implied constant depends only on $\varepsilon$.

Finally, we need the following result, established in [9, Lemma 4.9].

Let $\omega(m)$ denote the number of prime divisors of an integer $m \geq 1$.

**Lemma 2.3.** There are absolute constants $c_1, c_2 > 0$ such that for any polynomial $f(X) \in \mathbb{Z}[X]$ of degree $d \geq 1$ with coefficients of size at most $B \geq 2$ and any integer $h \geq 1$, for the product
\[ W(h) = \prod_{f(x) \neq 0} f(x), \]
we have
\[ \omega(W(h)) \geq \min \left\{ c_1 \frac{h}{\log B}, h^{c_2/d} \right\}. \]

3. FREQUENCY OF SMALL VALUES OF SHIFTED INVERSIONS

Given $s, t \in \mathbb{F}_p$ and two positive integers $h$ and $H$, we denote by $T_{s,t}(h, H)$ the number of $x \in \{1, \ldots, h\}$ such that
\[ (x + s)^{-1} \equiv (x + t)^{-1} + y \pmod{p}, \]
for some $y \in \{0, \pm 1, \ldots, \pm H\}$.

The case when one of the shifts $s, t$ is zero is of special interest to us. Furthermore, we denote $T_r(h, H) = T_{r,0}(h, H)$.

For $s \neq t$, rewriting the congruence (1) as
\[ (x + s)(x + t)y \equiv t - s \pmod{p}, \]
we see that $y \neq 0$ and furthermore we have the trivial bound
\[ T_{s,t}(h, H) \leq \min\{h, 4H\}. \]

First we study the case when the bound $T_r(h, H) \leq h$ is attained, which is the main tool in our study of the DMIHNP.
Theorem 3.1. There is an absolute constant $c > 0$ such that for any $\delta > 0$ and sufficiently large $p$, if

\[ H^2 h^3 \leq cp \quad \text{and} \quad h \geq (1/2 + \delta) \log p \]

then for any integer $r \not\equiv 0 \pmod{p}$ we have $T_r(h, H) < h$.

Proof. For $s = r$, and $t = 0$ we derive from (2)

\[ x^2y + rxy + r \equiv 0 \pmod{p}. \]

We now apply Lemma 2.1 with $\nu = 2$ and

\[ a_1 = 1, \quad a_2 = r, \quad U_1 = (p/h)^{1/2}, \quad U_2 = (ph)^{1/2}. \]

Let $v \in [-\frac{(p-1) / 2}{(p-1) / 2}]$ be the residue of $ru$ modulo $p$. Thus

\[ u = O(U_1) \quad \text{and} \quad v = O(U_2). \]

Then

\[ ux^2y + vxy + v \equiv 0 \pmod{p} \quad (3) \]

and

\[ |ux^2y + vxy| \leq |u|h^2H + |v|hH = O\left(p^{1/2}Hh^{3/2}\right). \quad (4) \]

Therefore, for a sufficiently small constant $c$ and $H^2 h^3 \leq cp$, we obtain $|ux^2y + vxy| < p/2$. Hence, from (3) and the inequality $|v| < p/2$, we conclude that

\[ ux^2y + vxy + v = 0. \]

Clearly $v \neq 0$. In particular,

\[ x \mid v \quad (5) \]

for every solution $(x, y)$ to the congruence (3). Now, assume that $T_r(h, H) = h$, then we have (5) for very $x = 1, \ldots, h$. Hence

\[ \text{lcm}[1, \ldots, h] \mid v. \quad (6) \]

Since $1 \leq |v| = O((ph)^{1/2})$ and also by the prime number theorem we have

\[ \text{lcm}[1, \ldots, h] = \exp(h + o(h)), \]

we see that the divisibility condition (6) implies

\[ \exp(h + o(h)) \leq (ph)^{1/2} \]

which is impossible for $h \geq (1/2 + \delta) \log p$ and a sufficiently large $p$. \qed

We now obtain a similar but weaker result for $T_{s,t}(h, H)$.

Theorem 3.2. There are an absolute constants $c, C > 0$ such that for any $\delta > 0$ and sufficiently large $p$, if

\[ H^2 h^3 \leq cp \quad \text{and} \quad h \geq (\log p)^C \]

then for any integers $s \not\equiv t \pmod{p}$ we have $T_{s,t}(h, H) < h$. 

Advances in Mathematics of Communications Volume 9, No. 2 (2015), 169–176
Proof. As in the proof of Theorem 3.1 we transform (2) into
\[ x^2y + (s + t)xy + sty + s - t \equiv 0 \pmod{p}. \]
We now apply Lemma 2.1 with \( \nu = 3 \) and
\[
\begin{align*}
    a_1 &= 1, \quad a_2 = s + t, \quad a_3 = st, \\
    U_1 &= p^{2/3}h^{-1}, \quad U_2 = p^{2/3}, \quad U_3 = p^{2/3}h.
\end{align*}
\]
Let \( v, w \) and \( z \) be the smallest by absolute value residues of \((s + t)u, stu \) and \((s - t)u \) modulo \( p \), respectively. Then
\[
\begin{align*}
    (7) \quad &ux^2y + vxy + wy + z \equiv 0 \pmod{p} \\
    \text{and} \quad &|ux^2y + vxy + wy| \leq |u|h^2H + |v|hH + |w|H = O\left(p^{2/3}Hh\right).
\end{align*}
\]
Therefore, for a sufficiently small constant \( c > 0 \) and \( H^3h^3 \leq cp \), we obtain \(|ux^2y + vxy + wy| < p/2\). Hence, from (7) and the inequality \(|z| < p/2\), we conclude that
\[ ux^2y + vxy + wy + z = 0 \]
Clearly \( z \neq 0 \). In particular,
\[
\begin{align*}
    (8) \quad &\left(ux^2 + vx + w\right) \mid z \\
\end{align*}
\]
for every solution \((x, y)\) to the congruence (7). Now, assume that \( T_{r,s}(h, H) = h \), then we have (8) for every \( x = 1, \ldots, h \). Hence
\[
\omega \left( \prod_{x=1}^{h} \left(ux^2 + vx + w\right) \right) \leq \omega(z).
\]
Since \( \omega(z) = O(\log z) = O(\log p) \), using Lemma 2.3 we see that \( h = (\log p)^O(1) \). \( \Box \)

It is also clear that the method of proof of Theorems 3.1 and 3.2, and the well-known bound
\[ \tau(m) = m^o(1) \]
lead to the estimates
\[ T_r(h, H) \leq p^o(1) \quad \text{and} \quad T_{s,t}(h, H) \leq p^o(1), \]
provided that
\[ H^2h^3 \leq p \quad \text{and} \quad H^3h^3 \leq p, \]
respectively.

We now obtain upper bounds on \( T_r(h, H) \) and \( T_{s,t}(h, H) \) for slightly large values of \( h \) and \( H \).

**Theorem 3.3.** Assume that
\[ H^2h^3 \geq p^{1+\varepsilon} \]
for a fixed real \( \varepsilon > 0 \). Then for any integer \( r \not\equiv 0 \pmod{p} \) we have
\[ T_r(h, H) = O\left(p^{-1/2}H h^{3/2} \log p\right). \]
Proof. We see from (3) and (4) that for every solution \((x, y)\) to (2) we have
\[ux^2y + vxy = -v + kp\]
with some integer \(k\). Thus
\[T_r(h, H) \leq \sum_{|m| \leq M, m \equiv -v \pmod{p}} \tau(|m|)\]
for \(M = \lceil CH^{3/2}p^{1/2} \rceil\) and an appropriate absolute constant \(C > 0\). Since \(v \neq 0\) \((\mod p)\) and \(M \geq H^{3/2}p^{1/2} \geq p^{1+\varepsilon/2}\), Lemma 2.2 applies and leads to the desired result.

\[\Box\]

Theorem 3.3 is nontrivial if
\[h = o \left(p^{1/3}(\log p)^{-2/3}\right)\]
and \(H^2h = o \left(p(\log p)^{-2}\right)\).

Similarly, we also derive

**Theorem 3.4.** Assume that
\[H^3h^3 \geq p^{1+\varepsilon}\]
for a fixed real \(\varepsilon > 0\). Then for any integers \(s \neq t \pmod{p}\) we have
\[T_{s,t}(h, H) = O \left(p^{-1/3}Hh\log p\right)\].

Theorem 3.4 is nontrivial if
\[h = o \left(p^{1/3}(\log p)^{-1}\right)\]
and \(H = o \left(p^{1/3}(\log p)^{-1}\right)\).

4. Testing the hidden shift in modular inversion

We first present an algorithm for DMIHNP-1, that is, when \(t\) is known.

**Theorem 4.1.** For any fixed real \(\varepsilon > 0\), and \(\ell > (1/2 + \varepsilon)n\) given \(t \in \mathbb{F}_p\) and an oracle \(O_{t,s}\), that for \(x \in \mathbb{F}_p\) outputs \(O_{t,s}(x) = \text{MSB}_\ell((s + x)^{-1})\) one can decide whether \(s = t\) in \(O(\log p)\) oracle calls and arithmetic operations in \(\mathbb{F}_p\), where the implied constant depends only on \(\varepsilon\).

**Proof.** We set \(h = [\log p]\) and query \(O_{t,s}\) for \(x = -t + 1, \ldots, -t + h\). Clearly if \(s = t\) then for every \(x \in \mathbb{F}_p\) we have
\[|\text{MSB}_\ell((s + x)^{-1}) - (t + x)^{-1}| \leq p/2^{\ell+1}\]
Otherwise, that is, if \(s \neq t\), we see from Theorem 3.1 applied with \(H = \lceil p/2^{\ell+1} \rceil\) that for at least one of the above values of \(x\) the inequality (9) fails. \(\Box\)

We see that compared with the result of [14], the algorithm of Theorem 4.1 works with weaker oracles (that is, returning weaker approximations) and is also fully deterministic. However, of course it addresses an easier problem.

Using Theorem 3.2 instead of Theorem 3.1 in the argument of the proof of Theorem 4.1, we obtain an analogue of Theorem 4.1 for DMIHNP-2, that is, when \(t\) is unknown.

**Theorem 4.2.** For any fixed real \(\varepsilon > 0\), and \(\ell > (2/3 + \varepsilon)n\) given two oracles \(O_{t,s}\) and \(O_{t,t}\) that for \(x \in \mathbb{F}_p\) output \(O_{t,s}(x) = \text{MSB}_\ell((s + x)^{-1})\) and \(O_{t,t}(x) = \text{MSB}_\ell((t + x)^{-1})\), respectively, one decide whether \(s = t\) in \(O(\log p)^{O(1)}\) oracle calls and arithmetic operations in \(\mathbb{F}_p\), where the implied constant depends only on \(\varepsilon\).
Unfortunately the algorithm of Theorem 4.1 requires the oracle of the same strength as in [14], however it is deterministic (and is certainly faster than that of [14]).

5. Comments

It is also natural to consider the case of a noisy oracle \( \tilde{O}_\ell(s) \) that returns MSB_\ell((s+x)^{-1}) only with a certain non-negligible probability and returns a random element of \( \mathbb{F}_p \) otherwise. Unfortunately the algorithm of [14] does not apply to such oracles (and neither do the heuristic algorithms of [2]). One can however obtain efficient algorithms for such analogues of DMIHNP-1 and DMIHNP-2, which are based on Theorem 3.3 and Theorem 3.4, respectively.

Our results also provide some information about the entropy of the pseudorandom generators based on the function \( x \mapsto \text{MSB}_\ell((s+x)^{-1}) \). In particular, Theorem 3.2 implies that there is an absolute constant \( C \) such that for any \( s \in \mathbb{F}_p, \ell > (2/3+\varepsilon)n \) and \( h > (\log p)^C \) all \( h \)-tuples

\[
(\text{MSB}_\ell((s+k+1)^{-1}), \ldots, \text{MSB}_\ell((s+k+h)^{-1}))
\]

are pairwise distinct for \( k = 0, 1, \ldots, p-1 \), provided that \( p \) is large enough.

Finally, we note that for \( Hh > p^{3/4+\varepsilon} \), with some fixed \( \varepsilon \), one can immediately derive an asymptotic formula for \( T_{s,t}(h,H) \) from the more general results of [13, 19], see also [18] for survey of results about the distribution of inverses.

Acknowledgements

The author is very grateful to Gérald Tenenbaum for useful discussions and literature references related to Lemma 2.2 and also to the referee for the very careful reading and finding some imprecisions in the original version of this paper.

This paper was initiated during a very enjoyable visit of I. S. to School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, whose hospitality, support and stimulating research atmosphere are gratefully appreciated.

This research was supported by NRF Grant CRP2-2007-03, Singapore and by ARC Grant DP130100237, Australia.

References

[1] A. Akavia, Solving hidden number problem with one bit oracle and advice, in Adv. Crypt. — CRYPTO 2009, Springer-Verlag, Berlin, 2010, 337–354.
[2] D. Boneh, S. Halevi and N. A. Howgrave-Graham, The modular inversion hidden number problem, in Adv. Crypt. — ASIACRYPT 2001, Springer-Verlag, Berlin, 2001, 36–51.
[3] D. Boneh and R. Venkatesan, Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes, in Adv. Crypt. — CRYPTO ’96, Springer-Verlag, Berlin, 1996, 129–142.
[4] D. Boneh and R. Venkatesan, Rounding in lattices and its cryptographic applications, in Proc. 8th Annual ACM-SIAM Symp. Discr. Algorithms, SIAM, 1997, 675–681.
[5] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, Points on curves in small boxes and applications, Michigan Math. J., 63 (2014), 503–534.
[6] J. Cilleruelo and M. Z. Garaev, Concentration of points on two and three dimensional modular hyperbolas and applications, Geom. Funct. Anal., 21 (2011), 892–904.
[7] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, On the concentration of points of polynomial maps and applications, Math. Zeit., 272 (2012), 825–837.
[8] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, Isomorphism classes of elliptic curves over a finite field in some thin families, Math. Res. Letters, 19 (2012), 335–343.
[9] A. Dubickas, M. Sha and I. E. Shparlinski, Explicit form of Cassels’ $p$-adic embedding theorem for number fields, *Canad. J. Math.*, to appear.

[10] O. Garcia-Morchon, D. Gómez-Pérez, J. Gutierrez, R. Rietman, B. Schoenmakers and L. Tolhuizen, HIMMO: A lightweight collusion-resistant key predistribution scheme, Cryptology ePrint Archive: Report 2014/698, available at [http://eprint.iacr.org/2014/698](http://eprint.iacr.org/2014/698)

[11] O. Garcia-Morchon, D. Gómez-Pérez, J. Gutierrez, R. Rietman and L. Tolhuizen, The MMO problem, in *Proc. 39th Int. Symp. Symbol. Algebr. Comput. — ISSAC’14*, ACM, 2014, 186–193.

[12] O. Garcia-Morchon, R. Rietman, I. E. Shparlinski and L. Tolhuizen, Interpolation and approximation of polynomials in finite fields over a short interval from noisy values, *Experim. Math.*, 23 (2014), 241–260.

[13] A. Granville, I. E. Shparlinski and A. Zaharescu, On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races, *J. Number Theory*, 112 (2005), 216–237.

[14] S. Ling, I. E. Shparlinski, R. Steinfeld and H. Wang, On the modular inversion hidden number problem, *J. Symb. Comp.*, 47 (2012), 358–367.

[15] M. Nair and G. Tenenbaum, Short sums of certain arithmetic functions, *Acta Math.*, 180 (1998), 119–144.

[16] P. Shiu, A Brun–Titchmarsh theorem for multiplicative functions, *J. Reine Angew. Math.*, 313 (1980), 161–170.

[17] I. E. Shparlinski, Playing “Hide-and-Seek” with numbers: The hidden number problem, lattices and exponential sums, *Proc. Symp. Appl. Math.*, Amer. Math. Soc., 62 (2005), 153–177.

[18] I. E. Shparlinski, Modular hyperbolas, *Jap. J. Math.*, 7 (2012), 235–294.

[19] M. Văjăitu and A. Zaharescu, Distribution of values of rational maps on the $\mathbb{F}_p$-points on an affine curve, *Monatsh. Math.*, 136 (2002), 81–86.

Received for publication September 2013.

*E-mail address:* igor.shparlinski@unsw.edu.au