Playing “Hide-and-Seek” in Finite Fields: Hidden Number Problem and Its Applications

Igor E. Shparlinski
Centre for Advanced Computing: Algorithms and Cryptography
Macquarie University

igor@comp.mq.edu.au
Introduction

We describe a rather surprising, yet powerful, combination of

- exponential sums

- lattice reduction algorithms.

This combination has led to a number of cryptographic applications, helping to make rigorous several heuristic approaches.

It provides a two edge sword to:

- prove important security results;

- create powerful attacks
Examples:

- Bit security of the
  - Diffie–Hellman key exchange system,
  - Shamir message passing scheme,
  - XTR cryptosystem,

- Attacks on the
  - Digital Signature Scheme (DSA),
  - Nyberg–Rueppel Signature Scheme.
Notation

\[ p = \text{prime number} \]

\[ \mathbb{F}_p = \text{finite field of } p \text{ elements.} \]

\[ \lfloor s \rfloor_m = \text{the remainder of } s \text{ on division by } m. \]

For \( \ell > 0 \), \( \text{MSB}_{\ell,p}(x) \) denotes any integer \( u \) such that

\[ |\lfloor x \rfloor_p - u| \leq p/2^\ell+1. \]

\( \text{MSB}_{\ell,p}(x) \approx \ell \) most significant bits of \( x \).

However this definition is more flexible.

In particular, \( \ell \) need not be an integer.
Hidden Number Problem (HNP)

Boneh and Venkatesan, 1996

**HNP**: Recover $\alpha \in \mathbb{F}_p$ such that for many known random $t \in \mathbb{F}_p$ we are given $\operatorname{MSB}_{\ell,p}(\alpha t)$ for some $\ell > 0$.

**B&V, 1996**: a polynomial time algorithm to solve HNP with $\ell \approx \log^{1/2} p$.

The algorithm is based on lattice reduction.

**Lattices**

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

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

is called an $s$-dimensional full rank lattice. The set $\{b_1, \ldots, b_s\}$ is called a basis of $L$. 
The closest vector problem

**CVP:** Given a vector \( r \in \mathbb{R}^s \) find a lattice vector \( v \in L \) with

\[
||r - v|| = \min_{z \in L} ||r - z||.
\]

**CVP** is \textbf{NP}-complete.

Approximate solution?

Lenstra, Lenstra and Lovász, 1982
Kannan, 1987
Schnorr, 1987

**Lemma 1** There exists a deterministic polynomial time algorithm which, for a given lattice \( L \) and a vector \( r \in \mathbb{R}^s \), finds a lattice vector \( v \in L \) satisfying the inequality

\[
||r - v|| \leq \exp \left( C s \log^2 \log s \right) \min_{z \in L} ||r - z||.
\]

for some absolute constant \( C > 0 \).

LLL: stretch factor \( 2^{s/2} \) (can be used as well)

Working with \( 2^{o(s)} \) is technically easier
Let $d \geq 1$ be integer. Given $t_i$, $u_i = \text{MSB}_{\ell,p}(\alpha t_i)$, $i = 1, \ldots, d$, we build the lattice $L(p, \ell, t_1, \ldots, t_d)$ spanned by the rows of the matrix:

$$
\begin{pmatrix}
    p & 0 & \ldots & 0 & 0 \\
    0 & p & \ddots & \vdots & \vdots \\
    \vdots & \ddots & \ddots & 0 & \vdots \\
    0 & 0 & \ldots & p & 0 \\
    t_1 & t_2 & \ldots & t_d & 1/2^{\ell+1}
\end{pmatrix}.
$$

The **unknown** vector $v = ([\alpha t_1]_p, \ldots, [\alpha t_d]_p, \alpha/2^{\ell+1})$

- belongs to $L(p, \ell, t_1, \ldots, t_d)$

- is close to the **known** vector $u = (u_1, \ldots, u_d, 0)$:
  $$
  \|v - u\| = O\left(p2^{-\ell}\right).
  $$

**Idea:** Apply a CVP algorithm and hope that it will output $v$.  

How to make it rigorous?

We show that for almost all \( t_1, \ldots, t_d \), \( v \) is the only lattice vector which can be so close to \( u \).

In fact, even within the approximation factor of Lemma 1, that is within the distance of order \( p2^{-\ell + o(d)} \), this is still the only lattice vector.

Assume that \( w \equiv (\beta t_1, \ldots, \beta t_d, \beta/2^{\ell+1}) \pmod{p} \), with \( \beta \not\equiv \alpha \pmod{p} \) is another lattice vector with \( \| w - u \| \leq p2^{-\ell + o(d)} \).

Then

\[
\| w - v \| \leq p2^{-\ell + o(d)}. \quad (1)
\]

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

\[
(\alpha - \beta) t_i \in [-p2^{-\ell + o(d)}, p2^{-\ell + o(d)}] \pmod{p}
\]

For every fixed \( \gamma \not\equiv 0 \pmod{p} \)

\[
\Pr_{t \in \mathbb{F}_p} (\gamma t \in [-h, h] \pmod{p}) \leq \frac{2h + 1}{p} \quad (2)
\]
Thus
\[
\Pr_{t_1, \ldots, t_d \in \mathbb{F}_p} (\gamma t_i \in [-h, h] \pmod p, \ i = 1, \ldots, d) \leq \left( \frac{2h + 1}{p} \right)^d.
\]

In our settings
\[
\gamma = \alpha - \beta \quad \text{and} \quad h = p 2^{-\ell + o(d)}.
\]

Because \( \beta \) (and thus \( \gamma = \alpha - \beta \)) may belong to \( p - 1 \) distinct residue classes we conclude that (1) holds with probability at most
\[
P \leq p \left( 2^{-\ell + o(d)} \right)^d.
\]

Choose \( \ell = d = 2 \left\lfloor \log^{1/2} p \right\rfloor \). Then
\[
P \leq \frac{1}{p}.
\]

CVP algorithm returns \( \mathbf{v} \) with prob. \( \geq 1 - 1/p \)
Extended HNP

**HNP:** Recover $\alpha \in \mathbb{F}_p$ such that for many known random $t \in \mathbb{F}_p$ we are given $\text{MSB}_{\ell,p}(\alpha t)$ for some $\ell > 0$.

The condition that $t$ is selected uniformly at random from $\mathbb{F}_p$ is too restrictive for applications.

Typically $t$ is selected from a certain finite sequence $T$ of elements of $\mathbb{F}_p$ which

- may have a nice and well-studied number theoretic structure (bit security of Diffie–Hellman key),

- may be rather "ugly" looking (attacks on DSA and Nyberg–Rueppel).

**EHNP:** Recover $\alpha \in \mathbb{F}_p$ such that for many known random $t \in T$ we are given $\text{MSB}_{\ell,p}(\alpha t)$ for some $\ell > 0$.

The same arguments as above apply to the **EHNP** ... but one needs an analogue of (2).

\[\downarrow\]

$T$ must have some **uniformity of distribution** properties.
Distribution of Sequences

**Discrepancy** $\mathcal{D}(\Gamma)$ of an $N$-element sequence $\Gamma = \{\gamma_1, \ldots, \gamma_N\}$ of elements of the interval $[0, 1]$ is defined as

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

where $|J|$ is the length of the interval $J$ and $A(J, N) = \# \{\gamma_n \in J, \ 1 \leq n \leq N\}$.

A finite sequence $\mathcal{T}$ of integers is $\Delta$-homogeneously distributed modulo $p$ ($\Delta$-HD$_p$) if for any $a \in [1, p - 1]$,

$$\{[at]_p/p\}, \quad t \in \mathcal{T},$$

has the discrepancy at most $\Delta$. 
Putting Together

For a $\Delta$-HD$_p$ sequence $\mathcal{T}$ instead of (2) we get

$$\Pr_{t \in \mathcal{T}} (\gamma t \in [-h, h] \pmod{p}) \leq \frac{2h + 1}{p} + \Delta.$$

Nguyen & Shparlinski, 2000:

**Theorem 2** Let $\ell = \lceil \log^{1/2} p \rceil + \lceil \log \log p \rceil$ and $d = 2 \lceil \log^{1/2} p \rceil$. Let $\mathcal{T}$ be $2^{-\log^{1/2} p}$-HD$_p$. There exists a deterministic polynomial time algorithm $A$ such that for any fixed integer $\alpha \in [0, p - 1]$, given $2d$ integers $t_i$ and $u_i = \text{MSB}_{\ell,p}(\alpha t_i)$, $i = 1, \ldots, d$, its output satisfies

$$\Pr_{t_1, \ldots, t_d \in \mathcal{T}} [A(t_1, \ldots, t_d; u_1, \ldots, u_d) = \alpha] \geq 1 - 2^{-(\log p)^{1/2} \log \log p}$$

if $t_1, \ldots, t_d$ are chosen uniformly and independently at random from the elements of $\mathcal{T}$. 
Discrepancy and Exponential Sums

Polya–Vinogradov, 1918:

$T$ is $\Delta$-HD$_p$ with

$$\Delta = O \left( \frac{\log p}{\#T} \max_{1 \leq c \leq p-1} \left| \sum_{t \in T} \exp \left( 2\pi i ct/p \right) \right| \right).$$

To use it we need an improvement up on the trivial bound

$$\left| \sum_{t \in T} \exp \left( 2\pi i ct/p \right) \right| \leq \#T$$

In many situations we have such results which are quite enough... but what if only a very weak bound of the above exponential sums is known?
Using Very Weak Bounds

Shparlinski&Winterhof, 2003:

We can amplify it but considering $k$-sums

$$\{ t_1 + \ldots + t_k \mid t_1, \ldots, t_k \in T \}.$$ 

The discrepancy of this sequence:

$$\Delta_k = O \left( \frac{\log p}{\#T} \max_{1 \leq c \leq p-1} \left| \sum_{t \in T} \exp \left( \frac{2\pi i ct}{p} \right) \right|^k \right).$$

Any nontrivial saving $\gamma$ against the trivial bound

$$\left| \sum_{t \in T} \exp \left( \frac{2\pi i ct}{p} \right) \right| \leq \gamma \#T$$

will be risen to the $k$th power!
Important Example

Konyagin, 1992:

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

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

the bound

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

holds.

Konyagin&Shparlinski, 1999:

For larger subgroups stronger bounds are known.
Modifications to the Algorithm

Chose

\[ t_{11}, \ldots, t_{1k}, \ldots, t_{d1}, \ldots, t_{dk} \in \mathcal{G} \]

and get integers \( u_{ij} \) with

\[ \left| \left\lfloor \alpha r_{ij} \right\rfloor_p - u_{ij} \right| < p/2^{\ell+1}, \quad i = 1, \ldots, d, \ j = 1, \ldots, k. \]

For \( i = 1, 2, \ldots, d \) we put

\[ v_i = \sum_{j=1}^{k} \left\lfloor \alpha r_{ij} \right\rfloor_p, \quad t_i = \left\lfloor \sum_{j=1}^{k} t_{ij} \right\rfloor_p, \quad u_i = \sum_{j=1}^{k} u_{ij} \]

The rest of the algorithm remains the same.
Good News: Bit Security of the Diffie–Hellman Key

Diffie–Hellman (DH) problem:

Given an element $g$ of order $\tau$ modulo $p$, recover $K = [g^{xy}]_p$ from $[g^x]_p$ and $[g^y]_p$.

Typically, either $\tau = p - 1$ or $\tau = q$ — a large prime divisor of $p - 1$.

The size of $p$ and $\tau$ is determined by the present state of art in the discrete logarithm problem. Typically, $p$ is about 500 bits, $\tau$ is at least 160 bits.

However after the common DH key $K = g^{xy}$ is established, only a small portion of bits of $K$ will be used as a common key for some private key cryptosystem.
Assume that finding $K$ is infeasible. Is it still infeasible to find certain bits of $K$?

| Private Key | Public Key |

Boneh & Venkatesan, 1996:
for $\tau = p - 1$ (- small gap in the proof)

González Vasco & Shparlinski, 2000:
for “any” $\tau$ (+ fixing the gap in BV)

YES!!!

Assume we know how to recover $\ell$ most significant bits of $[g^{xy}]_p$ from $X = [g^x]_p$ and $Y = [g^y]_p$.

Select a random $u \in [0, \tau - 1]$ and apply this algorithm to $X = [g^x]_p$ and $U = [Y g^u]_p = [g^{y+u}]_p$:

$\text{MSB}_{\ell,p}(g^{x(y+u)}) = \text{MSB}_{\ell,p}(g^{xy}g^{xu}) = \text{MSB}_{\ell,p}(\alpha t)$

**EHNP** with $\alpha = g^{xy}$ and $t = g^{xu}$, $u \in [0, \tau - 1]$!!!
When $\gamma^u$ is $2^{-\log^{1/2}p}$-HD$_p$? \hspace{1cm} (\gamma = g^x)

Shparlinski & Winterhof, 1999:

**Theorem 3** For any $\varepsilon > 0$ there exists $c > 0$ such that for $k = c \log^2 p$ any $\gamma \in \mathbb{F}_p$ of order $\tau \geq (\log p)^{1+\varepsilon}$ the sequence

$$T_k = \{\gamma^{u_1} + \ldots + \gamma^{u_k}, \ u_1, \ldots, u_k = 0, \ldots, \tau - 1\}$$

is $p^{-\delta}$-HD$p$.

If $p$ is an $n$-bit prime and $\tau \geq (\log p)^{1+\varepsilon}$ then

$\approx n^{1/2}$ most significant bits of the DH key are as secure as the whole key.
What Else?

Similar results for the Shamir message passing scheme (has not been worked out in details).

Shparlinski, 2000:
Li, Näslund, Shparlinski, 2002:

Similar results for the XTR cryptosystem of Lenstra&Verheul

Galbraith&Hopkins&Shparlinski, 2003:

Similar results for the bilinear Diffie-Hellman bits

In both case but for much large ordes.

Open Question: Extend the range.
Bad News: Attack on DSA


**Public Data:**

\[ q \text{ and } p = \text{ primes with } q | p - 1 \]

\[ g \in \mathbb{F}_p = \text{ a fixed element of order } q. \]

\[ \mathcal{M} = \text{ set of messages to be signed} \]

\[ h : \mathcal{M} \rightarrow \mathbb{F}_q = \text{ a hash-function.} \]

The **secret key** is \( \alpha \in \mathbb{F}_q^* \) which is known only to the **signer** (and publishes \( A = \lfloor g^\alpha \rfloor_p \) – to be used for signature verification).

To sign a message \( \mu \in \mathcal{M} \), the signer chooses a random integer \( k \in \mathbb{F}_q^* \) usually called the **nonce**, and which must be kept **secret** and computes:

\[
    r(k) = \left\lfloor \left\lfloor g^k \right\rfloor_p \right\rfloor_q, \quad s(k, \mu) = \left\lfloor k^{-1} \left( h(\mu) + \alpha r(k) \right) \right\rfloor_q.
\]

\((r(k), s(k, \mu))\) is the **DSA signature** of the message \( \mu \) with a nonce \( k \).
Assume that some bits of \( k \) are “leaked”.

Howgrave-Graham&Smart, 1998: **Heuristic** lattice based attack.

Nguyen, 1999: Simpler and more powerful but still **heuristic** lattice based attack.

Nguyen&Shparlinski, 1999: **Rigorous** lattice based attack.

**Idea** (Nguyen, 1999):

\[
s(k, \mu) \equiv k^{-1} (h(\mu) + \alpha r(k)) \pmod{q}
\]

\[
\downarrow
\]

\[
\alpha r(k)s(k, \mu)^{-1} \equiv k - h(\mu)s(k, \mu)^{-1} \pmod{q}.
\]

If \( \ell \) most significant bits of \( k \) are known then we know MSB\(_{\ell,q}(\alpha r(k)s(k, \mu)^{-1})\).

**EHNP** with

\[
t(k, \mu) = \left[ r(k)s(k, \mu)^{-1} \right]_q, \quad (k, \mu) \in [1, q-1] \times \mathcal{M}.
\]
Nguyen&Shparlinski, 1999:

\[ W = \# \{ h(\mu_1) = h(\mu_2), \quad \mu_1, \mu_2 \in M \}. \]

\[ W/\#M^2 = \text{probability of collision}. \]
Typically \( W/|M|^2 \approx q^{-1} \).

**Theorem 4** Let \( Q \) be a sufficiently large integer. The following statement holds with \( \vartheta = 1/3 \) for all primes \( p \in [Q, 2Q] \), and with \( \vartheta = 0 \) for all primes \( p \in [Q, 2Q] \) except at most \( Q^{5/6+\varepsilon} \) of them. For any \( \varepsilon > 0 \) there exists \( \delta > 0 \) such that for any \( g \in \mathbb{F}_p \) of order \( q \geq p^{\vartheta + \varepsilon} \) the sequence
\[ t(k, \mu) = \left[ r(k) s(k, \mu)^{-1} \right]_q, \quad (k, \mu) \in [1, q-1] \times M. \]
is \( q^{-\delta} \)-HD\(_q\), provided
\[ W \leq \frac{\#M^2}{q^{1-\delta}}. \]
Theoretically: If $q$ is an $n$-bit prime and $\approx n^{1/2}$ most significant bits of $k$ are known for $\approx n^{1/2}$ signatures then $\alpha$ can be recovered in polynomial time.

The proof uses:

- bounds of exponential sums with exponential functions (Konyagin&Shparlinski, 1999);
- Weil’s bound;
- Vinogradov’s method of estimates of double sums.

Main difficulty: The double reduction erases any number theoretic structure among the values of $r(k)$.

Practically: 4 bits of $k$ are always enough, 3 bits are often enough, 2 bits are possibly enough as well.
Moral:

1. Do not use small $k$ (to cut the cost of exponentiation in $r(k)$).

2. Protect your software/hardware against timing/power attacks when the attacker measures the time/power consumption and selects the signatures for which this value is smaller than “on average” – these signatures are likely to correspond to small $k$ ($\sim$ faster exponentiation in $r(k)$).

3. Use quality PRNG’s to generate $k$, biased generators are dangerous.

4. Do not use Arazi’s cryptosystem which combines DSA and Diffie-Hellman protocol – it leaks some bits of $k$ (Brown & Menezes).

5. Do not buy CryptoLib from AT&T, it always uses odd values of $k$ thus one bit is leaked immediately, one more and ....
Generalizations and Open Problems

Complete analogue of the bit security results for the DH key are also known ElGamal cryptosystem, Shamir message passing scheme and several others.

For XTR some non-trivial results are known as well (Li, Näslund, Shparlinski, 2002).

Attacks on other DSA-like schemes, including the elliptic curve DSA, of the same strength as on the original DSA (ElMahassni, Nguyen, Shparlinski, 2000–2001).

For the Nyberg–Rueppel scheme the range of $p$ and $q$ in which the results are nontrivial are narrower than in practical applications. Improve... Better bounds of exponential sums are required.