# Hidden Number Problem with the Trace and Bit Security of XTR and LUC

Wen-Ching W. Li[1,⋆], Mats Näslund[2,⋆⋆], and Igor E. Shparlinski[3,⋆⋆⋆]

[1] Department of Mathematics, Penn State University
University Park, PA 16802, USA
wli@math.psu.edu
[2] Ericsson Research
SE-16480 Stockholm, Sweden
mats.naslund@era.ericsson.se
[3] Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

**Abstract.** We consider a certain generalization of the hidden number problem introduced by Boneh and Venkatesan in 1996. Considering the XTR variation of Diffie-Hellman, we apply our results to show security of the $\log^{1/2} p$ most significant bits of the secret, in analogy to the results known for the classical Diffie-Hellman scheme. Our method is based on bounds of exponential sums which were introduced by Deligne in 1977. We proceed to show that the results are also applicable to the LUC scheme. Here, assuming the LUC function is one-way, we can in addition show that each single bit of the argument is a hard-core bit.

## 1 Introduction

When a new cryptosystem is proposed, some maturity period is normally needed before we see practical deployment. This is natural since some amount of public scrutiny is needed before we feel confident that there are no (serious) attacks possible. We can for instance see this in the case of elliptic curve cryptography where it is not until now, almost twenty years after the introduction by Koblitz and Miller [18,31], that we start to see commercial use. For this reason, a formal proof of security for a brand new scheme speeds up acceptance.

In 1994, Smith and Skinner [47] proposed a public key scheme, LUC, based on Lucas sequences modulo $p$. One reason for introducing LUC was a hope that there would not be any sub-exponential attacks on it. Although, this hope has failed, see [2] and the discussion below, LUC still seems to have both better speed and higher security than the classical Diffie-Hellman scheme [20].

While Lucas sequences have a rich mathematical theory, and have seen applications in computer science, for example, primality testing, there has been no formal proof of security relative to for example, discrete logarithms. Indeed,

⋆ Supported in part by NSF grant DMS 997-0651.
⋆⋆ Part of work done while visiting Macquarie University.
⋆⋆⋆ Supported in part by ARC grant A69700294.

M. Yung (Ed.): CRYPTO 2002, LNCS 2442, pp. 433–448, 2002.

shortly after publication, Bleichenbacher et al. showed in [2] that the very parameter settings that made LUC so efficient, also made it possible to reduce the security to discrete logarithms in $\mathbb{F}_{p^2}$, implying sub-exponential attacks. A natural question turns up: does LUC have other (worse) defects, not present in standard discrete logarithm based schemes?

One of the most recently proposed schemes is XTR, invented in 2000 by Lenstra and Verheul [23]. XTR can be thought of as a generalization of LUC to an extension field of degree six rather than two, and is based on initial ideas by Brouwer et al. [6]. The idea is to get a security against attackers corresponding to discrete logarithms in $\mathbb{F}_{p^6}$ while the actual computation and messages exchanged are in $\mathbb{F}_{p^2}$. For XTR, a proof of security exists; breaking XTR is computationally equivalent to computing discrete logarithms in $\mathbb{F}_{p^6}$, see also [23].

Still, even if completely breaking the respective schemes (LUC, XTR) requires finite field discrete logarithm computation, it is not clear what other security properties these schemes have. For instance, one can ask the natural question on "partial breaking", for example, in terms of computing certain bits of the XTR/LUC-secrets (the "logarithms").

The perhaps most interesting application of XTR (and LUC) is the Diffie-Hellman (DH) analogues; the exchanged messages are small, and, according to the recent evaluation [20,22] of the relative performance of various cryptosystems, XTR and LUC are the fastest non-elliptic curve schemes. Hence, it would be important to establish bit-security results for the DH version; given the exchanged DH messages, can certain parts or bits of the DH secret key be computed? For the conventional DH scheme over $\mathbb{F}_p$, such results were shown by Boneh and Venkatesan [4], as consequences of a generalization of the *hidden number problem* introduced in the same paper [4]: given polynomially many $t_i$ and approximations to $t_i\alpha \pmod p$, recover $\alpha$. Their results roughly state that if one can compute all of the $\lceil \log^{1/2} p \rceil$ most significant bits of the DH secret without errors, then the remaining bits can be found as well.

In fact, the original security proof of the Diffie-Hellman bits in [4] contained a slight gap, corrected in a later work by Shparlinski and González-Vasco [11]. That paper [11] is based on using bounds on certain *exponential sums* to establish approximate uniformity for some distributions over $\mathbb{F}_p$.

For XTR, Shparlinski [45] has recently extended the techniques to show security also for the XTR Diffie-Hellman secret. We here improve these results and also extend the techniques to LUC Diffie-Hellman. Our results follow from bounds on exponential sums, established using algebraic-geometric means.

For prime fields $\mathbb{F}_p$, or cyclic multiplicative groups of prime order, the security of all individual bits (except possibly the the least significant bits, depending on group order) of the discrete logarithms follows from the works [3,13,29,38,42], showing that computing any single bit with non-negligible advantage (over the trivial 1/2) implies polynomial time discrete logarithm computations. In this paper we show that the results can be carried over to LUC in a natural way. Further, when the generator has even order, the predictability for the least significant bits also applies.

## 2 Preliminaries

### 2.1 Notation

Let $p$ be a prime. To ease notation, we write $\mathbb{F}$ for the prime field $\mathbb{F}_p$, and $\mathbb{K}$ for a degree $m$ extension $\mathbb{F}_{p^m}$ of $\mathbb{F}$. As usual we assume that $\mathbb{F}$ is represented by $\{0, \ldots, p-1\}$. For integers $s$ and $r \geq 1$ denote by $\lfloor s \rfloor_r$ the remainder of $s$ on division by $r$. We also use $\log z$ to denote the binary logarithm of $z > 0$. Let

$$\mathrm{Tr}(z) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(z) = z + z^p + \ldots + z^{p^{m-1}}$$

be the trace of $z \in \mathbb{K}$ in $\mathbb{F}$, see [28] for basics of the theory of finite fields.

For a prime $p$ and $k \geq 0$ we denote by $\mathrm{MSB}_{k,p}(x)$ any integer $u$ such that

$$\left| \lfloor x \rfloor_p - u \right| \leq p/2^{k+1}. \tag{1}$$

Roughly speaking $\mathrm{MSB}_{k,p}(x)$ gives $k$ most significant bits of $x$, however this definition is more flexible and suits better our purposes. In particular, in (1), $k$ need not be integer. Also, the notion of most significant bits is tailored to modular residues and does not match the usual definition for integers.

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

We now give a short introduction to the XTR and LUC cryptosystem, as well as to the hidden number problem and its use of lattices. The reader familiar with these can proceed directly to Sect. 3.

### 2.2 The XTR and LUC Cryptosystems

Below, we concentrate only on the details relevant to this work.

Let $m = 2$ so that $\mathbb{K} = \mathbb{F}_{p^2}$ and let $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(u) = \mathrm{Tr}(u)$ as above. Let $g \in \mathbb{K}$ be a root of an irreducible quadratic polynomial $f(X) = X^2 - PX + 1 \in \mathbb{F}_p[X]$, thus $P^2 - 4$ is a quadratic non-residue of $\mathbb{F}_p$. It is easy to show that such elements exist. For example, for any root $\vartheta \in \mathbb{K}$ of an arbitrary irreducible quadratic polynomial over $\mathbb{F}$, $g = \vartheta^{p-1}$ is such an element. Note also that $f$ above is the characteristic polynomial of the recurrence $V_n(P) \equiv PV_{n-1}(P) - V_{n-2}(P) \pmod p$, $V_0 = 2, V_1 = P$, and that $V_n(P) = \mathrm{Tr}(g^n)$.

In the LUC variant of Diffie–Hellman (known as LUCDIF) the communicating parties exchange $\mathrm{Tr}\,(g^x)$ and $\mathrm{Tr}\,(g^y)$ (that is, $V_x(P)$ and $V_y(P)$), then, using $V_{xy}(P) = V_x(V_y(P)) = V_y(V_x(P))$, compute the common secret $\mathrm{Tr}\,(g^{xy})$. For details refer to [2,47].

XTR can be thought of as a generalization of LUC and has been introduced by Lenstra and Verheul, see [6,23,24,25,43,48] for basic properties and ideas behind XTR. Let $m = 6$ so that $\mathbb{K} = \mathbb{F}_{p^6}$. We also consider the field $\mathbb{L} = \mathbb{F}_{p^2}$, thus we have a tower of extensions $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$. Accordingly, we denote by $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(u)$ and $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(v)$ the trace of $u \in \mathbb{K}$ in $\mathbb{L}$ and the trace of $v \in \mathbb{L}$ in $\mathbb{F}$. In particular, $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(u)\right) = \mathrm{Tr}(u)$ for $u \in \mathbb{K}$.

The idea of XTR is based on the observation that for some specially selected element $g \in \mathbb{K}^*$, *the XTR generator*, of prime order $l > 3$ such that $l|p^2 - p + 1$, one can also here efficiently compute $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^{xy})$ from the values of $x$ and $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^y)$ (alternatively from $y$ and $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^x)$). This reduces the size of the Diffie-Hellman messages to exchange (namely, $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^x)$ and $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^y)$ rather than $g^x$ and $g^y$) to create a common key $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^{xy})$.

### 2.3 The Hidden Number Problem

We shall be interested in a variant of the *hidden number problem* introduced by Boneh and Venkatesan [4,5]. The problem can be stated as follows: recover an unknown $\alpha \in \mathbb{F}$, given approximations to $\lfloor \alpha t \rfloor_p$ for polynomially many known random $t \in \mathbb{F}$.

Let $\mathcal{G}$ be a subgroup of the multiplicative group $\mathbb{K}^*$. Motivated by the application of bit security for XTR and LUC, we consider the following question: recover $\alpha \in \mathbb{K}$, given approximations of $\mathrm{Tr}(\alpha t)$ for polynomially many known random $t \in \mathcal{G}$. Then we apply our results to obtain a statement about the bit security of the XTR and LUC cryptosystems.

For the general hidden number problem, it has turned out that for many applications (as we shall see, including the one at hand) the condition that $t$ is selected uniformly at random is too restrictive. Examples include the earlier bit security results for the Diffie-Hellman, Shamir, and several other cryptosystems [11,12] and rigorous results on attacks (following the heuristic arguments of [14,32]) on the DSA(-like) signature schemes [9,33,34].

The aforementioned papers [9,11,12,33,34] have exploited that the method of [4] can be adjusted to the case when $t$ is selected from a sequence which has some uniformity of distribution property. Thus, a central ingredient is bounds on exponential sums; a natural tool to establish such properties.

### 2.4 Bounds on Exponential Sums

The case when $t$ is selected from a small subgroup of $\mathbb{F}^*$ was studied in [11] to generalize (and correct) the results of [4] on the bit security of the Diffie-Hellman key in $\mathbb{F}_p$. The results of [11] are based on bounds of exponential sums with elements of subgroups of $\mathbb{F}^*$, namely on Theorems 3.4, 5.5 of [19].

Unfortunately, analogues of the bounds of exponential sums of Theorems 3.4, 5.5 of [19] are not known for non-prime fields. However, in [45] an alternative method of [44] has been used, which applies to very small subgroups $\mathcal{G}$ and is based on bounds of [7,10] for the number of solutions of certain equations in finite fields. Unfortunately it produces much weaker results.

It is remarked in [45] that for subgroups $\mathcal{G}$ of cardinality $|\mathcal{G}| \geq p^{m/2+\delta}$, with any fixed $\delta > 0$, the bound of exponential sums given by Theorem 8.78 in [28] combined with Theorem 8.24 of the same work (see also (3.15) in [19]) can be used. These bounds would provide analogues of the results [4,11] but, unfortunately, the subgroups $\mathcal{G}$ associated with XTR and LUC fall below this square-root threshold.

Nevertheless, thanks to the special property of these subgroup, we show in Sect. 3 how one can use an approach from [8], developed in [26,27], to apply the exponential sum technique to studying the subgroups related to XTR and LUC. We get a substantial improvement to the results of [45] on the bit-security for XTR (from $\alpha n$ bits for a constant $0 < \alpha < 1$, to $\log^{1/2}$ n bits), and a new equally strong result for LUC.

### 2.5 Lattices

As in [4,5], our results related to the hidden number problem rely on rounding techniques in lattices. We 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

$$L = \{\mathbf{z} \ : \ \mathbf{z} = c_1\mathbf{b}_1 + \ldots + c_s\mathbf{b}_s, \quad c_1, \ldots, c_s \in \mathbb{Z}\}$$

is called an *s-dimensional full rank lattice* with *basis* $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$. For a vector $\mathbf{u}$, let $\|\mathbf{u}\|$ denote its *Euclidean norm*.

It has been remarked in [30], and then in [35,36] that the following statement holds, which is somewhat stronger than that usually used in the literature. It follows from the lattice basis reduction algorithm of [21] and results of [41,15].

**Lemma 1.** *There exists a deterministic polynomial time algorithm which, for a given s-dimensional full rank lattice $L$ and $\mathbf{r} \in \mathbb{R}^s$, finds $\mathbf{v} \in L$ with*

$$\|\mathbf{v} - \mathbf{r}\| \le \exp\left(O\left(\frac{s\log^2\log s}{\log s}\right)\right)\min\{\|\mathbf{z} - \mathbf{r}\|, \quad \mathbf{z} \in L\}.$$

## 3 Distribution of Trace

First, we need the following result which, as mentioned, is essentially Theorem 8.78 of [28] (combined with Theorem 8.24 of the same work) or the bound (3.15) of [19]. Let $\mathcal{G}$ be a subgroup of $\mathbb{K} = \mathbb{F}_{p^m}$.

**Lemma 2.** *For any $\gamma \in \mathbb{K}^*$, we have*

$$\left|\sum_{t\in\mathcal{G}} \exp\left(2\pi i \mathrm{Tr}\left(\gamma t\right)/p\right)\right| \le p^{m/2}.$$

Lemma 2 is nontrivial when $|\mathcal{G}| \ge p^{m/2+\delta}$. Much less is known when $\mathcal{G}$ has size less than $p^{m/2}$. For prime finite fields, $m = 1$, Theorems 3.4, 5.5 of [19] provide a nontrivial upper bound for $|\mathcal{G}| \ge p^{1/3+\delta}$ for all primes $p$ and for $|\mathcal{G}| \ge p^{\delta}$ for almost all primes $p$, respectively, which underlies the result of [11]. However these results have not been extended to composite fields (and it seems that such extensions will require some substantially new ideas).

Nevertheless, applying the results of [8,26,27] for some special subgroups we obtain non-trivial estimates beyond the $p^{m/2}$-threshold.

For a divisor $s|m$ let $\mathcal{N}_s$ be the set of $z \in \mathbb{K}$ with $\mathrm{Nm}_s(z) = 1$, where

$$\mathrm{Nm}_s(z) = z^{1+p^{m/s}+\ldots+p^{m-m/s}}$$

is the norm of $z \in \mathbb{K} = \mathbb{F}_{p^m}$ in $\mathbb{F}_{p^{m/s}} \subseteq \mathbb{K}$. Thus $|\mathcal{N}_s| = (p^m - 1)/(p^{m/s} - 1)$.

Our results depend on the following estimate conjectured by Deligne in [8] (and proved in the case of the trivial character $\chi = \chi_0$). In the full generality it has been proved by Katz [17] (to be precise Theorem 4.1.1 of [17] and some standard transformations). For the cases relevant to XTR and LUC, we may also refer to the simpler and more explicit statements of [26,27].

**Lemma 3.** *For any divisor $s|m$, any $\gamma \in \mathbb{K}^*$, and any multiplicative character $\chi$ of $\mathbb{K}$, we have*

$$\left| \sum_{t \in \mathcal{N}_s} \chi(t) \exp\left(2\pi i \mathrm{Tr}\left(\gamma t\right)/p\right) \right| \le s p^{(m-m/s)/2}.$$

To proceed, recall the following property of the group of characters of an abelian group.

**Lemma 4.** *Let $\mathcal{H}$ be an abelian group and let $\widehat{\mathcal{H}} = \mathrm{Hom}(\mathcal{H}, \mathbb{C}^*)$ be its dual group. Then for any character $\chi$ of $\mathcal{H}$,*

$$\frac{1}{|\mathcal{H}|} \sum_{h \in \mathcal{H}} \chi(h) = \begin{cases} 1, & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \ne \chi_0, \end{cases}$$

*where $\chi_0 \in \widehat{\mathcal{H}}$ is the trivial character.*

**Lemma 5.** *For any divisor $s|m$, any subgroup $\mathcal{G}$ of $\mathcal{N}_s$ and any $\gamma \in \mathbb{K}^*$,*

$$\left| \sum_{t \in \mathcal{G}} \exp\left(2\pi i \mathrm{Tr}\left(\gamma t\right)/p\right) \right| \le s p^{(m-m/s)/2}.$$

*Proof.* Let $\Omega_{\mathcal{G}}$ be the set of all multiplicative characters of $\mathcal{N}_s$, trivial on $\mathcal{G}$. Using Lemma 4, we write

$$\begin{aligned} \sum_{t \in \mathcal{G}} \exp\left(2\pi i \mathrm{Tr}\left(\gamma t\right)/p\right) &= \frac{1}{|\Omega_{\mathcal{G}}|} \sum_{t \in \mathcal{N}_s} \exp\left(2\pi i \mathrm{Tr}\left(\gamma t\right)/p\right) \sum_{\chi \in \Omega_{\mathcal{G}}} \chi(t) \\ &= \frac{1}{|\Omega_{\mathcal{G}}|} \sum_{\chi \in \Omega_{\mathcal{G}}} \sum_{t \in \mathcal{N}_s} \chi(t) \exp\left(2\pi i \mathrm{Tr}\left(\gamma t\right)/p\right). \end{aligned}$$

Applying the inequality of Lemma 3, we obtain the desired estimate. □

For $\gamma \in \mathbb{K}$ and integers $r$ and $h$, denote by $N_\gamma(\mathcal{G}, r, h)$ the number of solutions of the congruence

$$\mathrm{Tr}(\gamma t) \equiv r + y \pmod p, \qquad t \in \mathcal{G},\ y = 0, \ldots, h-1.$$

Using standard relations between the uniformity of distribution and bounds of exponential sums, for example, see Corollary 3.11 of [37], from Lemma 2 and Lemma 5 one immediately derives the following asymptotic formulas for $N_\gamma(\mathcal{G}, r, h)$.

**Lemma 6.** *For any $\gamma \in \mathbb{K}^*$ and any subgroup $\mathcal{G} \subseteq \mathbb{K}^*$, we have*

$$N_\gamma(\mathcal{G}, r, h) = \frac{h}{p}|\mathcal{G}| + O(p^{m/2}\log p).$$

**Lemma 7.** *For any divisor $s|m$, any subgroup $\mathcal{G} \subseteq \mathcal{N}_s$, and any $\gamma \in \mathbb{K}^*$,*

$$N_\gamma(\mathcal{G}, r, h) = \frac{h}{p}|\mathcal{G}| + O(p^{(m-m/s)/2}\log p).$$

These bounds can be turned into statements on the form of the shortest vector in certain lattices. Let $\omega_1, \ldots, \omega_m$ be a fixed basis of $\mathbb{K}$ over $\mathbb{F}$. For an integer $k \geq 0$ and $d(\geq 1)$ elements $t_1, \ldots, t_d \in \mathbb{K}$, let $\mathcal{L}_k(t_1, \ldots, t_d)$ be the $d+m$-dimensional lattice generated by the rows of the $(d+m)\times(d+m)$-matrix:

$$\begin{pmatrix} p & \ldots 0 & 0 & \ldots 0 \\ 0 & \ldots 0 & 0 & \ldots 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots p & 0 & \ldots 0 \\ \mathrm{Tr}(\omega_1 t_1) & \ldots \mathrm{Tr}(\omega_1 t_d) & 1/2^{k+1} & \ldots 0 \\ \vdots & \vdots & \vdots & \ddots \vdots \\ \mathrm{Tr}(\omega_m t_1) & \ldots \mathrm{Tr}(\omega_m t_d) & 0 & \ldots 1/2^{k+1} \end{pmatrix}. \tag{2}$$

**Lemma 8.** *Let $p$ be a sufficiently large prime number and let $\mathcal{G}$ be a subgroup of $\mathbb{K}^*$ with $|\mathcal{G}| \geq p^{m/2+\delta}$ for some fixed $\delta > 0$. Then for*

$$\eta = \left\lceil \log^{1/2} p \right\rceil \qquad \text{and} \qquad d = \left\lceil \frac{m+1}{\eta - 3}\log p \right\rceil,$$

*the following holds. Let $\alpha = a_1\omega_1 + \ldots + a_m\omega_m$, $a_1, \ldots, a_m \in \mathbb{F}$, be a fixed element of $\mathbb{K}$. Assume that $t_1, \ldots, t_d \in \mathcal{G}$ are chosen uniformly and independently at random. Then with probability exceeding $1 - p^{-1}$ for any $\mathbf{s} = (s_1, \ldots, s_d, 0, \ldots, 0)$ with*

$$\left(\sum_{i=1}^{d} \left(\mathrm{Tr}(\alpha t_i) - s_i\right)^2\right)^{1/2} \leq 2^{-\eta}p,$$

*all vectors $\mathbf{v} = (v_1, \ldots, v_d, v_{d+1}, \ldots, v_{d+m}) \in \mathcal{L}_k(t_1, \ldots, t_d)$ satisfying*

$$\left(\sum_{i=1}^{d} \left(v_i - s_i\right)^2\right)^{1/2} \leq 2^{-\eta}p,$$

*are of the form*

$$\mathbf{v} = \left( \left\lfloor \sum_{j=1}^{m} b_j \mathrm{Tr}\left(\omega_j t_1\right) \right\rfloor_p, \ldots, \left\lfloor \sum_{j=1}^{m} b_j \mathrm{Tr}\left(\omega_j t_d\right) \right\rfloor_p, \frac{b_1}{2^{k+1}}, \ldots, \frac{b_m}{2^{k+1}} \right)$$

*with some integers* $b_j \equiv a_j \pmod p$, $j = 1, \ldots, m$.

*Proof.* As in [4] we define the modular distance between two integers $r$ and $l$ as

$$\mathrm{dist}_p(r,l) = \min_{b \in \mathbb{Z}} |r - l - bp| = \min \left\{ \lfloor r - l \rfloor_p, p - \lfloor r - l \rfloor_p \right\}.$$

We see from Lemma 6 that for any $\beta \in \mathbb{K}$ with $\beta \neq \alpha$ the probability $P(\beta)$ that

$$\mathrm{dist}_p\left(\mathrm{Tr}(\alpha t), \mathrm{Tr}(\beta t)\right) \le 2^{-\eta+1} p$$

for $t \in \mathcal{G}$ selected uniformly at random is

$$P(\beta) \le 2^{-\eta+2} + O(p^{m/2} |\mathcal{G}|^{-1} \log p) \le 2^{-\eta+2} + O(p^{-\delta} \log p) \le 2^{-\eta+3},$$

for large enough $p$. Therefore, with $d = \lceil (m+1)/(\eta-3) \rceil$, for any $\beta \in \mathbb{K}$,

$$\Pr\left[\forall i \in [1,d] \mid \mathrm{dist}_p\left(\mathrm{Tr}(\alpha t_i), \mathrm{Tr}(\beta t_i)\right) \le 2^{-\eta+1} p\right] = P(\beta)^d \le p^{-m-1},$$

where the probability is taken over $t_1, \ldots, t_d \in \mathcal{G}$ chosen uniformly and independently at random. From here, we derive

$$\Pr\left[\forall \beta \in \mathbb{K} \backslash \{\alpha\},\ \forall i \in [1,d] \mid \mathrm{dist}_p\left(\mathrm{Tr}(\alpha t_i), \mathrm{Tr}(\beta t_i)\right) \le 2^{-\eta+1} p\right] \le p^{-1}.$$

The rest of the proof is identical to the proof of Theorem 5 of [4]. Indeed, we fix some $t_1, \ldots, t_d \in \mathcal{G}$ with

$$\min_{\beta \in \mathbb{K} \backslash \{\alpha\}} \max_{i \in [1,d]} \mathrm{dist}_p\left(\mathrm{Tr}(\alpha t_i), \mathrm{Tr}(\beta t_i)\right) > 2^{-\eta+1} p. \tag{3}$$

Let $\mathbf{v} \in \mathcal{L}_k(t_1, \ldots, t_d)$ be a lattice point satisfying

$$\left( \sum_{i=1}^{d} \left(v_i - s_i\right)^2 \right)^{1/2} \le 2^{-\eta} p.$$

Since $\mathbf{v} \in \mathcal{L}_k(t_1, \ldots, t_d)$, there are integers $b_1, \ldots, b_m, z_1, \ldots, z_d$ such that

$$\mathbf{v} = \left( \sum_{j=1}^{m} b_j \mathrm{Tr}\left(\omega_j t_1\right) - z_1 p, \ldots, \sum_{j=1}^{m} b_j \mathrm{Tr}\left(\omega_j t_d\right) - z_d p, \frac{b_1}{2^{k+1}}, \ldots, \frac{b_m}{2^{k+1}} \right).$$

If $b_j \equiv a_j \pmod p$, $j = 1, \ldots, m$, then for all $i = 1, \ldots, d$ we have

$$\sum_{j=1}^{m} b_j \mathrm{Tr}\left(\omega_j t_i\right) - z_i p = \left\lfloor \sum_{j=1}^{m} b_j \mathrm{Tr}\left(\omega_j t_i\right) \right\rfloor_p = \mathrm{Tr}(\alpha t_i),$$

since otherwise there would be $i \in \{1, \ldots, d\}$ such that $|v_i - s_i| > 2^{-\eta} p$.

Now suppose that $b_j \not\equiv a_j \pmod p$ for some $j = 1, \ldots, m$. Put $\beta = b_1\omega_1 + \ldots + b_m\omega_m$. In this case we have

$$\begin{aligned}
\left(\sum_{i=1}^{d} \left(v_i - s_i\right)^2\right)^{1/2} &\geq \max_{i \in [1,d]} \operatorname{dist}_p \left(\sum_{j=1}^{m} b_j \operatorname{Tr}\left(\omega_j t_i\right), s_i\right) \\
&\geq \max_{i \in [1,d]} \left(\operatorname{dist}_p \left(\operatorname{Tr}(\alpha t_i), \sum_{j=1}^{m} b_j \operatorname{Tr}\left(\omega_j t_i\right)\right) - \operatorname{dist}_p\left(s_i, \operatorname{Tr}(\alpha t_i)\right)\right) \\
&\geq \max_{i \in [1,d]} \left(\operatorname{dist}_p\left(\operatorname{Tr}(\alpha t_i), \operatorname{Tr}\left(\beta t_i\right)\right) - \operatorname{dist}_p\left(s_i, \operatorname{Tr}(\alpha t_i)\right)\right) \\
&> 2^{-\eta+1} p - 2^{-\eta} p = 2^{-\eta} p
\end{aligned}$$

that contradicts our assumption. As we have seen, the condition (3) holds with probability exceeding $1 - p^{-1}$ and the result follows. □

Accordingly, using Lemma 7 instead of Lemma 6 we obtain:

**Lemma 9.** *Let $p$ be a sufficiently large prime number and let $s$ be a divisor of $m$. Let $\mathcal{G}$ be a subgroup of $\mathcal{N}_s$ with $|\mathcal{G}| \geq |\mathcal{N}_s|^{1/2} p^{\delta}$ for some fixed $\delta > 0$. Then for*

$$\eta = \left\lceil \log^{1/2} p \right\rceil \qquad \text{and} \qquad d = \left\lceil \frac{m+1}{\eta - 3} \log p \right\rceil,$$

*the following holds. Let $\alpha = a_1\omega_1 + \ldots + a_m\omega_m$, $a_1, \ldots, a_m \in \mathbb{F}$, be a fixed element of $\mathbb{K}$. Assume that $t_1, \ldots, t_d \in \mathcal{G}$ are chosen uniformly and independently at random. Then with probability exceeding $1 - p^{-1}$ for any $\mathbf{s} = (s_1, \ldots, s_d, 0, \ldots, 0)$ with*

$$\left(\sum_{i=1}^{d} \left(\operatorname{Tr}(\alpha t_i) - s_i\right)^2\right)^{1/2} \leq 2^{-\eta} p,$$

*all vectors $\mathbf{v} = (v_1, \ldots, v_d, v_{d+1}, \ldots, v_{d+m}) \in \mathcal{L}_k\left(t_1, \ldots, t_d\right)$ satisfying*

$$\left(\sum_{i=1}^{d} \left(v_i - s_i\right)^2\right)^{1/2} \leq 2^{-\eta} p,$$

*are of the form*

$$\mathbf{v} = \left(\left\lfloor \sum_{j=1}^{m} b_j \operatorname{Tr}\left(\omega_j t_1\right) \right\rfloor_p, \ldots, \left\lfloor \sum_{j=1}^{m} b_j \operatorname{Tr}\left(\omega_j t_d\right) \right\rfloor_p, \frac{b_1}{2^{k+1}}, \ldots, \frac{b_m}{2^{k+1}}\right)$$

*with some integers $b_j \equiv a_j \pmod p$, $j = 1, \ldots, m$.*

## 4 Hidden Number Problem for the Trace

Using Lemma 8 in the same way as Theorem 5 of [4] was used in the proof of Theorem 1 of that paper, we obtain

**Theorem 1.** *Let $p$ be a sufficiently large prime number and let $\mathcal{G}$ be a subgroup of $\mathbb{K}^*$ with $|\mathcal{G}| \ge p^{m/2+\delta}$ for some fixed $\delta > 0$. Then for $k = \lceil 2\log^{1/2} p \rceil$, $d = \lceil 4(m+1)\log^{1/2} p \rceil$, the following holds. There exists a deterministic polynomial time algorithm $\mathcal{A}$ such that for any $\alpha \in \mathbb{K}$ given $2d$ values $t_i \in \mathcal{G}$ and $s_i = \mathrm{MSB}_{k,p}(\mathrm{Tr}(\alpha t_i))$, $i = 1, \ldots, d$, its output satisfies*

$$\Pr_{t_1,\ldots,t_d \in \mathcal{G}} [\mathcal{A}(t_1, \ldots, t_d; s_1, \ldots, s_d) = \alpha] \ge 1 - p^{-1}$$

*if $t_1, \ldots, t_d$ are chosen uniformly and independently at random from $\mathcal{G}$.*

*Proof.* We follow the arguments in the proof of Theorem 1 in [4], here briefly outlined for completeness. We refer to the first $d$ vectors in the matrix (2) as $p$-vectors and the remaining $m$ vectors as trace-vectors. Write

$$\alpha = \sum_{j=1}^{m} a_j \omega_j \in \mathbb{K}, \qquad a_1, \ldots, a_m \in \mathbb{F}.$$

We consider the vector $\mathbf{s} = (s_1, \ldots, s_d, s_{d+1}, \ldots, s_{d+m})$ where $s_{d+j} = 0$, for $j = 1, \ldots, m$. Multiplying the $j$th trace-vector of the matrix (2) by $a_j$ and subtracting a certain multiple of the $j$th $p$-vector for $j = 1, \ldots, m$, we obtain a lattice point

$$\mathbf{u}_\alpha = (u_1, \ldots, u_d, a_1/2^{k+1}, \ldots, a_m/2^{k+1}) \in \mathcal{L}_k(t_1, \ldots, t_d)$$

such that $|u_i - s_i| \le p2^{-k-1}$, $i = 1, \ldots, d+m$, where $u_{d+j} = a_j/2^{k+1}$ for $j = 1, \ldots, m$. Therefore,

$$\|\mathbf{u}_\alpha - \mathbf{s}\| \le (d+m)^{1/2} 2^{-k-1} p.$$

Let $\eta = \lceil \log^{1/2} p \rceil$. By Lemma 1 (with a slightly rougher constant $2^{(d+m)/4}$) in polynomial time we find $\mathbf{v} = (v_1, \ldots, v_d, v_{d+1}, \ldots, v_{d+m}) \in \mathcal{L}_k(t_1, \ldots, t_d)$ such that

$$\|\mathbf{v} - \mathbf{s}\| \le 2^{o(d+m)} \min\{\|\mathbf{z} - \mathbf{s}\|, \quad \mathbf{z} \in \mathcal{L}_k(t_1, \ldots, t_d)\} \le 2^{-k+o(d)} p \le 2^{-\eta-1} p,$$

provided that $p$ is large enough. We also have

$$\left( \sum_{i=1}^{d} (u_i - s_i)^2 \right)^{1/2} \le d^{1/2} 2^{-k-1} p \le 2^{-\eta-1} p.$$

Therefore,

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

Applying Lemma 8, we see that $\mathbf{v} = \mathbf{u}_\alpha$ with probability at least $1 - p^{-1}$, and therefore the components $a_1, \ldots, a_m$ of $\alpha$ can be recovered from the last $m$ components of $\mathbf{v} = \mathbf{u}_\alpha$. □

Accordingly, Lemma 9 implies:

**Theorem 2.** *Let $p$ be a sufficiently large prime number and let $s$ be a divisor of $m$, $s|m$. Let $\mathcal{G}$ be a subgroup of of $\mathcal{N}_s$ with $|\mathcal{G}| \geq |\mathcal{N}_s|^{1/2} p^\delta$ for some fixed $\delta > 0$. Then for $k = \lceil 2 \log^{1/2} p \rceil$, $d = \lceil 4(m+1) \log^{1/2} p \rceil$ the following holds. There exists a deterministic polynomial time algorithm $\mathcal{A}$ such that for any $\alpha \in \mathbb{K}$ given $2d$ values $t_i \in \mathcal{G}$ and $s_i = \mathrm{MSB}_{k,p}(\mathrm{Tr}(\alpha t_i))$, $i = 1, \ldots, d$, its output satisfies*

$$\Pr_{t_1,\ldots,t_d \in \mathcal{G}} [\mathcal{A}(t_1, \ldots, t_d; s_1, \ldots, s_d) = \alpha] \geq 1 - p^{-1}$$

*if $t_1, \ldots, t_d$ are chosen uniformly and independently at random from $\mathcal{G}$.*

## 5 Bit Security of XTR

From Theorem 24 of [48] (see also [6,23,25]), any efficient algorithm to compute $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^{xy})$ from $g^x$ and $g^y$ can be used to construct an efficient algorithm to compute $g^{xy}$ from the same information. In [43] the same result was obtained with an algorithm which computes $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^{xy})$ only for a positive proportion of pairs $g^x, g^y$. Furthermore, the same results hold even for algorithms which compute only $\mathrm{Tr}(g^{xy})$. Any $v \in \mathbb{L}$ can be represented by a pair $\big(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(v), \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\vartheta v)\big)$ where $\vartheta$ is a root of an irreducible quadratic polynomial over $\mathbb{F}$, so $\mathrm{Tr}(g^{xy})$ is a part of the representation of $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^{xy})$. In fact the same result holds for $\mathrm{Tr}(\omega g^{xy})$ with any fixed $\omega \in \mathbb{K}^*$.

Thus the above results suggest that breaking XTR is not easier than breaking the classical Diffie–Hellman scheme. Here we obtain one more result of this kind. We would like to show that an oracle computing a certain proportion of bits of $\mathrm{Tr}(g^{xy})$ from $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^x)$ and $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(g^y)$ can be used to break classical Diffie–Hellman. However, we instead prove that an oracle that computes a certain proportion of bits of $\mathrm{Tr}(g^{xy})$ from $g^x, g^y$ can be used to compute $g^{xy}$ from $g^x, g^y$. This is stronger; the former oracle could be used to simulate the latter so if the latter oracle cannot exist, neither can the former.

Thus, to really benefit from our results, one would need to use the trace over $\mathbb{F}_p$ rather than $\mathbb{F}_{p^2}$ in XTR based systems. As $\mathrm{Tr}(z) = \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(z) + \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(z)^p$ and as $p$th powers are "free" in XTR (due to the specific representation of $\mathbb{F}_{p^2}$) this could easily be done.

For a positive integer $k$ we denote by $\mathcal{XTR}_k$ the oracle such that for any given values of $g^x$ and $g^y$, it outputs $\mathrm{MSB}_{k,p}(\mathrm{Tr}(g^{xy}))$.

**Theorem 3.** *Let $p$ be a sufficiently large $n$-bit prime number. Suppose the XTR generator $g$ has prime order $l$ satisfying $l|p^2 - p + 1$ and $l \geq p^{3/2+\delta}$ for some fixed $\delta > 0$. Then there exists a polynomial time algorithm which, given $U = g^u$ and $V = g^v$, for some $u, v \in \{0, \ldots, l-1\}$, makes $O(\log^{1/2} p)$ calls of the oracle $\mathcal{XTR}_k$ with $k = \lceil 2 \log^{1/2} p \rceil$ and computes $g^{uv}$ correctly with probability at least $1 - p^{-1}$.*

*Proof.* The case $u = 0$ is trivial. Now assume that $1 \le u \le l-1$. Then $g_u = g^u$ is an element of order $l$ (because $l$ is prime).

Select random $r \in \{0, \ldots, l-1\}$. Applying the oracle $\mathcal{XTR}_k$ to $U$ and $V_r = g^{v+r} = Vg^r$ we obtain $\mathrm{MSB}_{k,p}\left(\mathrm{Tr}\left(g^{u(v+r)}\right)\right) = \mathrm{MSB}_{k,p}\left(\mathrm{Tr}\left(g^{vu}t\right)\right)$ where $t = g_u^r$.

For $d = O(\log^{1/2} p)$ independent, random $r_1, \ldots, r_d \in [0, l-1]$, we can now apply Theorem 2 with $\alpha = g^{uv}$, $m = 6$, and the group $\mathcal{G}$ generated by $g_u$ (equal to the group generated by $g$). Indeed, we see that

$$\mathrm{Nm}_2(g) = g^{1+p^3} = g^{(p+1)(p^2-p+1)} = 1$$

thus $\mathcal{G} \in \mathcal{N}_2$ and from Theorem 2 we obtain the desired result. □

## 6 Bit Security of LUC

For a positive integer $k$ we denote by $\mathcal{LUC}_k$ an oracle that for any given values of $g^x, g^y$, outputs $\mathrm{MSB}_{k,p}\left(\mathrm{Tr}\left(g^{xy}\right)\right)$. In complete analogy with the proof of Theorem 3 we establish the following.

**Theorem 4.** *Let $p$ be a sufficiently large $n$-bit prime number. Suppose the LUC generator $g$ has prime order $l$ satisfying $l|p+1$ and $l \ge p^{1/2+\delta}$ for some fixed $\delta > 0$. Then there exists a polynomial time algorithm which, given $U = g^u$ and $V = g^v$, for some $u, v \in \{0, \ldots, l-1\}$, makes $O(\log^{1/2} p)$ calls of the oracle $\mathcal{LUC}_k$ with $k = \lceil 2\log^{1/2} p \rceil$ and outputs $g^{uv}$ with probability at least $1 - p^{-\delta/2}$.*

## 7 Hard-Core Bits of LUC

The security of LUC clearly depends on the hardness of inverting the function

$$x \mapsto f_g(x) = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(g^x) = \mathrm{Tr}(g^x),$$

where, as above, $g$ is the LUC generator of order $l|p+1$. That is, it is necessary that this is a *one-way function*, otherwise the LUCDIF scheme would clearly be insecure. Even if this is true, the function could still have other undesirable properties in the form of "leakage", for example, it may be possible to determine individual bits of $x$. Note that Theorem 4 roughly says that, unless $f_g(x)$ can be efficiently inverted, it cannot be the case that *all of* the $\log^{1/2} p$ most significant bits of $x$ can be simultaneously computed *without errors* from $f_g(x)$. Still, it does not exclude the possibility of computing in polynomial time a single bit of $x$, with probability, say, $1/2 + \varepsilon(\log p)$ for a non-negligible function $\varepsilon(n)$. (Recall that $\nu(n)$ is negligible if for any $c > 0$, $\nu(n) = o(n^{-c})$.)

As usual let $\{0,1\}^*$ denote the set of all finite binary strings and let $G^n, G^*$ be some subsets of $\{0,1\}^n, \{0,1\}^*$, respectively. Suppose $f : G^* \mapsto \{0,1\}^*$ and $b : G^* \mapsto \{0,1\}$. Then $b$ is called a *hard-core function* for $f$ if for all non-negligible $\varepsilon(n)$ and all probabilistic polynomial time algorithms, for sufficiently large $n$,

$$\Pr[\mathcal{A}(f(x)) = b(x)] \le \frac{1}{2} + \varepsilon(n),$$

probability taken over $x \in G^n$ and the random coin tosses required by $\mathcal{A}$.

We are interested in the case that $f(x) = V_x(P) = \mathrm{Tr}(g^x)$ and $b(x) = \mathrm{bit}_i(x)$, the $i$th bit of $x$ (where $\mathrm{bit}_0(x) = \mathrm{lsb}(x)$ is the least significant bit). A problem is that $V_x(P)$ is not uniquely invertible. Note however that $V_x(P) = V_z(P)$, precisely when $z = l - x$. To make "the $i$th bit of $x$" well-defined by $V_x(P)$, we restrict the domain to $\{x \mid x < l/2\}$. (This hurts the group structure, but not our proofs.) Hence, we also assume that the oracle's advantage is averaged over this smaller set.

In Sect. 6, we assumed the existence of an oracle that returned $\mathrm{Tr}(tg^x)$, where the oracle took care of selecting $t$ (and computing the answer). Here we need that we from $\mathrm{Tr}(g^x)$ can ourselves efficiently compute values of form $\mathrm{Tr}(g^{wx+s})$ for $w$, $s$ of our own choice. Note that by the Diffie-Hellman-like properties of LUC, the case $s = 0$ is easy. We thus start with a certain technical statement. Why traces of this form is of interest will shortly be made clear.

**Lemma 10.** *Given* $\mathrm{Tr}(g^x)$*, for any set of* $N = (\log p)^{O(1)}$ *triples* $(k_j, r_j, s_j) \in \mathbb{Z}_l^* \times \mathbb{Z}_l \times \mathbb{Z}_l$*, we can in polynomial time compute two sets* $\mathcal{T}_\nu = \{T_{\nu,1}, \ldots T_{\nu,N}\}$*, so that for at least one* $\nu = 1, 2$*,* $T_{\nu,j} = \mathrm{Tr}(g^{k_j^{-1} r_j x + s_j})$ *for* $j = 1, \ldots, N$*.*

*Proof.* As observed in [2], the conjugates of $g^x$ are the roots, $H_0, H_1$, of $X^2 - \mathrm{Tr}(g^x)X + 1$, and they can be found in polynomial time. The conjugates $h_0, h_1$ of $g$ are trivial to compute and $H_i = h_{\pi(i)}^x$ for some permutation $\pi \in S_2$. Thus, for any $w = k^{-1}r$ and $s$,

$$\mathrm{Tr}(g^{wx+s}) = h_{\pi(0)}^s H_0^w + h_{\pi(1)}^s H_1^w.$$

Now, we do not know $\pi$, but there are only two possibilities. We thus obtain two candidates $\mathcal{T}_\nu$, $\nu = 1, 2$. □

As noted, as with conventional discrete logarithm not all bits are secure.

**Theorem 5.** *Suppose* $l = 2^s r$*,* $s > 0$*,* $r$ *odd. There is a polynomial time algorithm to determine* $\mathrm{bit}_i(x)$ *from* $V_x(P)$ *for every* $i = 0, \ldots, s - 1$*.*

*Proof.* For the least significant bit, note that $V_{xl/2}(P) = (-1)^{\mathrm{lsb}(x)} V_0(P)$, a condition that can be easily checked. Using Lemma 10, the rest follows from a straight-forward generalization of the Pohlig-Hellman algorithm [39] to decide $x \pmod{2^s}$. □

All other bits are, however, hard:

**Theorem 6.** *Let* $c > 0$ *be a constant. Except with probability* $o(1)$ *over random choices of* $n$*-bit prime* $p = 2^s r - 1$*,* $r$ *odd, and* $g$ *the LUC generator of order* $l = p + 1$*, the following holds. If for some* $i$*,* $0 \le i \le n - c \log n$ *there is an algorithm that given* $V_x(P)$ *for random* $x$*, computes* $\mathrm{bit}_i(x)$ *with probability at least* $1/2 + \varepsilon(n)$*, then there is a probabilistic algorithm that in time polynomial in* $n\varepsilon(n)^{-1}$ *computes* $x$ *with non-negligible probability.*

*Proof.* In [38,13], reductions are given from discrete logarithms in $\mathbb{F}_p$ to computing $\mathrm{bit}_i(x)$ from $g^x$, for any $i$. The reduction only uses operations transforming $y = g^x$ into values of form $y^{k^{-1}a}g^b = g^{k^{-1}ax+b}$. By Lemma 10, the same transformations can be applied to $\mathrm{Tr}(g^x)$, for invertible $k$ (as will be the case).

The only complication that arise is that we have here restricted the domain of $V_x(P) = \mathrm{Tr}(g^x)$ to $x < l/2$. However, a closer look at [13] we see that in each step of the reduction, a good approximation to the relative magnitude of each $k^{-1}ax + b$ (modulo the order of $g$) is maintained. Using this information, we simply discard all samples on $k^{-1}ax + b > l/2$. As the samples are uniformly distributed, this increases the complexity by a factor two. Taking into account the two choices for the list of samples from Lemma 10, we loose another (non-critical) factor of two, trying both possibilities. □

For prime $l$, $l|p + 1$, the same result follows for all $i$ and all large $p$ from [42].

We note that the $k = O(\log n)$ *most significant bits* of $x$ can also be shown to be hard by [13] and a security notion for biased functions from [46]. For such $k$, from [3,29] also follows hardness for the "related" function $\mathrm{MSB}_{k,p}$.

### 7.1 Hard-Core Bits of XTR

Superficially, all details (for example, a generalization of Lemma 10) seem to go through for XTR. However, problems are encountered by the fact that the XTR function, $\mathrm{Tr}_{\mathbb{F}_{p^6}/\mathbb{F}_{p^2}}(g^x)$, is three-to-one, rather than two-to-one, and there seems to be no obvious way to restrict the domain to a set on which: (a) XTR is 1–1, (b) the set has non-negligible density, and, (c) the set is an interval, $[a..b] \subset \mathbb{Z}_l$. These properties seem necessary to apply the techniques of [13].

## 8 Summary and Open Problems

Establishing security of new cryptosystems is important. We have shown that LUC and XTR share security properties with the more well-established discrete logarithm based systems. The Diffie-Hellman variant enjoys security features as of the original Diffie-Hellman key exchange. To this end, we have seen a new application for exponential sums; we believe there are more such in store. This paper is the most recent in a series studying variants of the hidden number problem, using such exponential sums. One can ask if there is a "general" theorem to be sought, rather than treating each special case. Such generalization seem difficult though: make the group a little smaller (for example, the proposed XTR-extensions to $\mathbb{F}_{p^{2\cdot 3\cdot 5}}$) and everything breaks down.

For the LUC scheme, we also showed that no non-trivial information about individual bits leak. Though likely to be true, the analogue for XTR is left open.

## References

1. M. Ajtai, R. Kumar and D. Sivakumar, *A sieve algorithm for the shortest lattice vector problem,* Proc. 33rd ACM Symp. on Theory of Comput., Crete, Greece, July 6-8, 2001, 601–610.

2. D. Bleichenbacher, W. Bosma and A. K. Lenstra, *Some remarks on Lucas-based Cryptograph,* Lect. Notes in Comp. Sci., Springer-Verlag, **963** (1995), 386–396.
3. M. Blum and S. Micali, *How to Generate Cryptographically Strong Sequences of Pseudo-random Bits,* SIAM J. on Computing, **13**(4), 850–864, 1984.
4. 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, **1109** (1996), 129–142.
5. D. Boneh and R. Venkatesan, *Rounding in lattices and its cryptographic applications,* Proc. 8th Annual ACM-SIAM Symp. on Discr. Algorithms, ACM, NY, 1997, 675–681.
6. A. E. Brouwer, R. Pellikaan and E. R. Verheul, *Doing more with fewer bits,* Lect. Notes in Comp. Sci., Springer-Verlag, **1716** (1999), 321–332.
7. R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, *On the statistical properties of Diffie–Hellman distributions,* Israel J. Math., **120** (2000), 23–46.
8. P. Deligne, *Cohomologie 'etale (SGA* $4\frac{1}{2}$*),* Lect. Notes in Math., Springer-Verlag, **569** (1977).
9. E. El Mahassni, P. Q. Nguyen and I. E. Shparlinski, *The insecurity of Nyberg–Rueppel and other DSA-like signature schemes with partially known nonces,* Lect. Notes in Comp. Sci., Springer-Verlag, **2146** (2001), 97–109.
10. J. B. Friedlander, M. Larsen, D. Lieman and I. E. Shparlinski, *On correlation of binary M-sequences,* Designs, Codes and Cryptography, **16** (1999), 249–256.
11. M. I. González Vasco and I. E. Shparlinski, *On the security of Diffie-Hellman bits,* Proc. Workshop on Cryptography and Computational Number Theory, Singapore 1999, Birkhäuser, 2001, 257–268.
12. M. I. González Vasco and I. E. Shparlinski, *Security of the most significant bits of the Shamir message passing scheme,* Math. Comp., **71** (2002), 333–342.
13. J. Håstad and M. Näslund, *The Security of all RSA and discrete log bits,* Electronic Colloquium on Computational Complexity, Report TR99-037, 1999. (To appear in Jorunal of the ACM)
14. N. A. Howgrave-Graham and N. P. Smart, *Lattice attacks on digital signature schemes,* Designs, Codes and Cryptography, **23** (2001), 283–290.
15. R. Kannan, *Algorithmic geometry of numbers,* Annual Review of Comp. Sci., **2** (1987), 231–267.
16. R. Kannan, *Minkowski's convex body theorem and integer programming,* Math. of Oper. Research, **12** (1987), 231–267.
17. N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups,* Ann. of Math. Studies, **116**, Princeton Univ. Press, 1988.
18. N. Koblitz, *Elliptic curve cryptosystems,* Math. Comp., **48**, 203–209, 1987.
19. S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications,* Cambridge Univ. Press, Cambridge, 1999.
20. A. K. Lenstra *Unbelievable security. Matching AES security using public key systems,* Lect. Notes in Comp. Sci., Springer-Verlag, **2248** (2001), 67–86.
21. A. K. Lenstra, H. W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients,* Mathematische Annalen, **261** (1982), 515–534.
22. A. K. Lenstra and M. Stam, *Speeding up XTR,* Lect. Notes in Comp. Sci., Springer-Verlag, **2248** (2001), pp. 125–143.
23. A. K. Lenstra and E. R. Verheul, *The XTR public key system,* Lect. Notes in Comp. Sci., Springer-Verlag, **1880** (2000), 1–19.
24. A. K. Lenstra and E. R. Verheul, *Key improvements to XTR,* Lect. Notes in Comp. Sci., Springer-Verlag, **1976** (2000), 220–233.

25. A. K. Lenstra and E. R. Verheul, *An overview of the XTR public key system,* Proc. the Conf. on Public Key Cryptography and Computational Number Theory, Warsaw 2000, Walter de Gruyter, 2001, 151–180.
26. W.-C. W. Li, *Character sums and abelian Ramanujan graphs,* J. Number Theory, **41** (1992), 199–217.
27. W.-C. W. Li, *Number theory with applications,* World Scientific, Singapore, 1996.
28. R. Lidl and H. Niederreiter, *Finite fields,* Cambridge University Press, Cambridge, 1997.
29. D. L. Long and A. Wigderson, *The discrete log hides $O(\log n)$ bits,* SIAM J. on Computing, **17**(2):413–420, 1988.
30. D. Micciancio, *On the hardness of the shortest vector problem,* PhD Thesis, MIT, 1998.
31. V. Miller, *Uses of elliptic curves in cryptography,* Lect. Notes in Comp. Sci., Springer-Verlag, **218** (1986), 417–426.
32. P. Q. Nguyen, *The dark side of the Hidden Number Problem: Lattice attacks on DSA,* Proc. Workshop on Cryptography and Computational Number Theory, Singapore 1999, Birkhäuser, 2001, 321–330.
33. P. Q. Nguyen and I. E. Shparlinski, *The insecurity of the Digital Signature Algorithm with partially known nonces,* J. Cryptology, (to appear).
34. P. Q. Nguyen and I. E. Shparlinski, *The insecurity of the elliptic curve Digital Signature Algorithm with partially known nonces,* Designs, Codes and Cryptography, (to appear).
35. P. Q. Nguyen and J. Stern, *Lattice reduction in cryptology: An update,* Lect. Notes in Comp. Sci., Springer-Verlag, **1838** (2000), 85–112.
36. P. Q. Nguyen and J. Stern, *The two faces of lattices in cryptology,* Springer-Verlag, **2146** (2001), 146–180.
37. H. Niederreiter, *Random number generation and Quasi–Monte Carlo methods,* SIAM Press, 1992.
38. R. Peralta, *Simultaneous security of bits in the discrete log,* Lect. Notes in Comp. Sci., Springer-Verlag, **219** (1986), 62–72.
39. S. C. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over* GF($p$)*,* IEEE Transactions on Information Theory, **IT-24**(1):106–110, 1978.
40. K. Prachar, *Primzahlverteilung,* Springer-Verlag, 1957.
41. C. P. Schnorr, *A hierarchy of polynomial time basis reduction algorithms,* Theor. Comp. Sci., **53** (1987), 201–224.
42. C. P. Schnorr, *Security of almost all discrete log bits,* Electronic Colloquium on Computational Complexity, Report TR98-033, 1998.
43. I. E. Shparlinski, *Security of polynomial transformations of the Diffie–Hellman key,* Preprint, 2000, 1–8.
44. I. E. Shparlinski, *Sparse polynomial approximation in finite fields,* Proc. 33rd ACM Symp. on Theory of Comput., Crete, Greece, July 6-8, 2001, 209–215.
45. I. E. Shparlinski, *On the generalised hidden number problem and bit security of XTR,* Lect. Notes in Comp. Sci., Springer-Verlag, **2227** (2001), 268–277.
46. A. W. Schrift and A. Shamir, *On the universality of the next bit test,* Lect. Notes in Comp. Sci., Springer-Verlag, **537** (1990), 394–408.
47. P. J. Smith and C. T. Skinner, *A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms,* Lect. Notes in Comp. Sci., Springer-Verlag, **917** (1995), 357-364.
48. E. R. Verheul, *Certificates of recoverability with scalable recovery agent security,* Lect. Notes in Comp. Sci., Springer-Verlag, **1751** (2000), 258–275.