Tatra Mt. Math. Publ. **29** (2004), 123–135

TATRA MOUNTAINS
Mathematical Publications

DISCRETE LOGARITHM PROBLEM IN GH AND XTR SCHEME

Otokar Grošek — Július Šiška

ABSTRACT. The discrete logarithm problem in a group G can be viewed as a problem of finding the index of an element in a given sequence generated as powers of some element of the group G. In the presented paper we use this approach to obtain some frequentative properties of GH and XTR sequences. We also present results of experiments on small instances of GH and XTR schemes using NTL library.

1. Introduction

In cryptography much effort is spent on solving discrete logarithm problem in various groups. The most prominent ones are:

1. multiplicative subgroups of finite fields,
2. multiplicative group of linear matrices $GL(F,n)$ over a field F,
3. group generated by a point of an elliptic curve.

A new public key cryptosystem called GH was proposed by Gong and Harn [2] in 1999. It is based on fast indexing of elements of the third order characteristic sequences from a finite field. Lenstra and Verheul in [4] proposed XTR cryptosystem based on similar mathematical principles in 2000.

GH and XTR schemes can be used to implement Diffie–Hellman key exchange scheme. Let $\{s_k\}$ be a sequence used in the GH or XTR scheme. The following attack can be applied to Diffie-Hellman's key exchange scheme: subjects A and B commit to some secret value (s_{er}, s_{-er}). Let us suppose that the frequencies of sequence elements are known, and elements $s_{i_1}, s_{i_2}, s_{i_3}, \dots$ occur with the highest probability. Then an attacker can substitute value s_{i_1} for observed value s_{er} and try to decipher communication between subjects A and B. If he fails, he substitutes value s_{i_2} and again tries to decipher communication. The attacker can continue in guessing of the secret value with the next most probable

2000 Mathematics Subject Classification: 94A60, 11T71.
Keywords: GH schemes, XTR schemes, discrete logarithm problem, GH and XTR sequences.

sequence elements. It is obvious that such sequences must have good (uniform) frequentative distributions of elements to prevent similar types of attack. In general they must fulfill well known randomness postulates [8].

The rest of paper is organized as follows. We start with a short description of GH and XTR schemes and their mathematical background. Then we present a generalization of the discrete logarithm problem suitable for searching elements in sequences. Next parts deal with frequencies of sequence elements and experiments on small instances of GH and XTR public cryptosystems.

2. GH and XTR overview

Let $q = p^2$ for some chosen prime p. Let $\mathbb{E} = GF(q^3)$, $\mathbb{F} = GF(q)$, and denote its prime field as $\mathbb{K} = GF(p)$. Let $f(x) = x^3 - ax^2 + bx - 1$ be an irreducible polynomial with coefficients in $\mathbb{F}$, and let α be one of its roots in the field extension $\mathbb{E}$. A sequence $\{s_k\}_{k\geq 0}$ is said to be the 3rd order characteristic sequence for polynomial f, if s_k satisfies a recurrent relation:

$$s_{k+3} = as_{k+2} - bs_{k+1} + s_k\,, \qquad \text{for} \quad k = 0, 1, \dots\,,$$

and some initial state s_0, s_1, s_2, or equivalently

$$s_k = \mathrm{Tr}_{E/F}\left(\theta\alpha^k\right), \qquad \text{for} \quad k = 0, 1, \dots, \tag{1}$$

where $\theta \in \mathbb{E}$ is a suitable element [7].

Let the multiplicative subgroup of $\mathbb{E}^*$ generated by the root α of $f(x)$ be $G = \langle\alpha\rangle$. Then the multiplicative order r of α in the field $\mathbb{E}$ is the period of the sequence $\{s_k\}_{k\geq 0} = \left\{\mathrm{Tr}_{E/F}\left(\theta\alpha^k\right)\right\}_{k\geq 0}$. It is also the order of the subgroup G.

Both schemes, GH and XTR, make use of a specific initial state:

$$s_0 = 3\,, \quad s_1 = a\,, \quad s_2 = a^2 - 2b\,.$$

This initial state corresponds to $\theta = 1$ in (2). For GH, the coefficients a, b of polynomial f are chosen in such a way, that the period of the sequence is $r = q^2 + q + 1$. For XTR, the coefficients are such that the period r divides $p^2 - p + 1$, and is greater than 3. To be conform with [4] hereafter we denote the period of the XTR sequence as $r = q_X$ and assume that $p > 3$.

3. Discrete logarithm problem for sequences

Now we describe a general approach to the discrete logarithm problem for finite fields as follows. Let $\mathbb{F}$ be any finite field with q elements and prime characteristic p. Let $\mathbb{E} = GF(q^k)$ be its extension, and $G = \langle g \rangle$ for an element $g \in \mathbb{E}^*$. Let m be some function $m\colon \mathbb{E} \to \mathbb{F}$. For a given element $x \in \mathbb{F}$, the problem of finding the set of all indices i, $0 \le i < |G|$ satisfying $m(g^i) = x$ we call m-DLP. The set of all indices i that satisfies previous equation we denote $\log_g(x)$. In general, $\log_g(x)$ is a relation, or equivalently a subset of $\mathbb{F} \times Z_{|G|}$.

Various strategies can be used to make m-DLP problem computationally hard. If $|G| \approx \big|m(G)\big|$ then the sets $\log_g(x)$ can be small—even these sets could have cardinality 1 or 0. If $\big|m(G)\big| \ll |G|$ then discrete logarithm sets could be large enough, so that an attacker has no possibility to distinguish among indices from that set.

This problem is a generalization of the well known discrete logarithm problem. In fact, for $G \subset \mathbb{E}$, $\mathbb{E} = \mathbb{F}$ and m being the identity function, we obtain the discrete logarithm problem.

In the case of GH and XTR schemes the trace function $\mathrm{Tr}_{E/F}\colon \mathbb{E} \to \mathbb{F}$ is used as function m, providing $k = 3$. The subgroup $G \subset \mathbb{E}^*$ is generated by the root α of the characteristic polynomial f of GH and XTR sequence.

In the following sections we will study frequentative and distribution properties of the 3rd order characteristic sequences. By this approach we obtain information about the cardinalities of the Tr-DLP sets of indices.

4. Frequentional analysis

Let $Z(b)$ denote number of occurrences of the element $b \in GF(q)$ among the first r elements $s_0, s_1, \ldots, s_{r-1}$ of a sequence (2). In fact, $Z(b)$ is the cardinality of the discrete logarithm $\log_\alpha(b)$.

Obviously, the period r is a trivial upper bound for $Z(b)$, i.e., for XTR it is q_X dividing $p^2 - p + 1$. A better bound can be obtained from the following theorem.

Theorem 1. ([6] Theorem 6.84). *Let $s_0, s_1, \ldots$ be a homogeneous linear recurring sequence in $GF(q)$ with least period r. Let the minimal polynomial $m(x)$ of the sequence be irreducible over $GF(q)$ and have degree k and satisfy $m(0) \neq 0$. Let $h = \mathrm{lcm}(r, q-1)$. Then*

$$\left| Z(0) - \frac{(q^{k-1}-1)r}{q^k - 1} \right| \le \left(1 - \frac{1}{q}\right)\left(\frac{r}{h} - \frac{r}{q^k - 1}\right) q^{k/2}, \tag{3}$$

and for $b \in GF(q) \setminus \{0\}$ there holds

$$\left| Z(b) - \frac{q^{k-1} r}{q^k - 1} \right| \le \left(\frac{r}{h} - \frac{r}{q^k - 1} + \frac{h-r}{h} \cdot q^{1/2}\right) q^{k/2-1}. \tag{4}$$

Next we need a technical lemma.

LEMMA 1. *Let p be a prime, and $q = p^2$. Then*

a) $\gcd(p^2 - p + 1,\, p^2 - 1) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 3 \ \textit{ or } \ p = 3\,, \\ 3 & \textit{if } p \equiv 2 \pmod 3\,. \end{cases}$

b) $\gcd(q^2 + q + 1,\, p^2 - 1) = \begin{cases} 1 & \textit{if } p = 3\,, \\ 3 & \textit{if } p \neq 3\,. \end{cases}$

Proof.

a) Let $d = \gcd(p^2 - p + 1,\, p^2 - 1) = \gcd(p^2 - 1, p - 2) = \gcd(p - 2, 3)$ what proves the first part of this lemma.

b) Let $d = \gcd(q^2 + q + 1,\, q - 1) = \gcd\big((q-1)^2 + 3q, q - 1\big) = \gcd(3, q - 1) = 1$ or 3, and $p = 3k \pm 1$ or $p = 3$. In the first case $3|q - 1$ which yields $d = 3$. If $p = 3$, then $q - 1 = 8$ which yields $d = 1$. □

For GH and XTR characteristic sequences their minimal characteristic polynomials are irreducible. Hence the following two corollaries can be derived.

COROLLARY 1. *Let $\{s_k\}_{k \geq 0}$ be a* GH *characteristic sequence over field $GF(q)$ (i.e., $k = 3$) with period equal to $r = q^2 + q + 1$ and $b \in GF(q) \setminus \{0\}$.*

a) *If* $\gcd(q^2 + q + 1, q - 1) = 1$ *then there holds*

$$Z(0) = 10\,, \tag{5}$$

$$3 \leq Z(b) \leq 18\,. \tag{6}$$

b) *If* $\gcd(q^2 + q + 1, q - 1) = 3$ *then there holds*

$$\big|Z(0) - (q + 1)\big| \leq 2q^{1/2}\,, \tag{7}$$

$$\big|Z(b) - (q + 1)\big| \leq q - 1\,. \tag{8}$$

Proof. If $\gcd(q^2 + q + 1, q - 1) = 1$ (i.e., $q = 9$, see Lemma 1) then $h = \operatorname{lcm}(r, q - 1) = (q^2 + q + 1)(q - 1) = q^3 - 1$. If we replace h in the right side of (3) we obtain

$$\left|Z(0) - \frac{(q^{3-1} - 1)r}{q^3 - 1}\right| = \left|Z(0) - \frac{q^2 - 1}{q^3 - 1}(q^2 + q + 1)\right| = \big|Z(0) - (q + 1)\big|$$

and

$$\left(1 - \frac{1}{q}\right)\left(\frac{r}{h} - \frac{r}{q^3 - 1}\right)q^{3/2} = \left(1 - \frac{1}{q}\right)\left(\frac{1}{q - 1} - \frac{1}{q - 1}\right)q^{3/2} = 0\,,$$

what proves the equation (5). The equation (6) follows from equations

$$\begin{aligned} \left|Z(b) - \frac{q^2 r}{q^3 - 1}\right| &= \left|Z(b) - \frac{q^2(q^2 + q + 1)}{q^3 - 1}\right| = \left|Z(b) - \frac{q^2}{q - 1}\right| \\ &= \left|Z(b) - (q + 1) - \frac{1}{q - 1}\right| = \left|Z(b) - 10\frac{1}{8}\right|. \end{aligned}$$

The right side of the second inequality in Theorem 1 is

$$\begin{aligned}\Big(\frac{r}{h}-\frac{r}{q^3-1}+\frac{h-r}{h}\cdot q^{1/2}\Big)q^{1/2}\\ &=\left(\frac{q^2+q+1}{q^3-1}-\frac{q^2+q+1}{q^3-1}+\Big(1-\frac{1}{q-1}\Big)q^{1/2}\right)q^{1/2}\\ &=\Big(1-\frac{1}{q-1}\Big)q=q-1-\frac{1}{q-1}=7\frac{7}{8}\,.\end{aligned}$$

If $\gcd(q^2+q+1,q-1)=3$ then $h=\frac{q^3-1}{3}$. The left side of the inequality (7) is $\big|Z(0)-(q+1)\big|$. This can be obtained by the same reasoning as for the inequality (5). The left side of (8) is the same as in the inequality (6). The right side of (7) is

$$\begin{aligned}\Big(1-\frac{1}{q}\Big)\Big(\frac{r}{h}-\frac{r}{q^3-1}\Big)q^{3/2}\\ &=\Big(1-\frac{1}{q}\Big)\Big(\frac{3(q^2+q+1)}{q^3-1}-\frac{(q^2+q+1)}{q^3-1}\Big)q^{3/2}\\ &=2\Big(1-\frac{1}{q}\Big)\frac{1}{q-1}q^{3/2}=2q^{1/2}.\end{aligned}$$

The right side of (8) is

$$\begin{aligned}\Big(\frac{r}{h}-\frac{r}{q^k-1}+\frac{h-r}{h}\cdot q^{1/2}\Big)q^{k/2-1}\\ &=\left(\frac{2}{q-1}+\Big(1-\frac{3}{q-1}\Big)q^{1/2}\right)q^{1/2}\\ &=q-3+\frac{3+2\sqrt{q}}{q-1}\le q-\frac{2}{3}\,.\end{aligned}$$

□

Corollary 2. *Let $p>3$ and $p\equiv 1 \pmod 3$. For* XTR *characteristic sequence with period $r|(p^2-p+1)$, and any nonzero element $b\in GF(q)\setminus\{0\}$ there holds*

$$\left|Z(0)-\frac{r}{p^2-1}\right|\le p\,, \tag{9}$$

$$\left|Z(b)-\frac{p^4 r}{p^6-1}\right|\le p^2\,. \tag{10}$$

P r o o f. Let $q=p^2$. From $\gcd(p^2-p+1,q-1)=1$ it follows that $\gcd(r,q-1)=1$, and hence $h=\operatorname{lcm}(r,q-1)=r(q-1)$. Now

$$\left|Z(0)-\frac{(q^2-1)r}{q^3-1}\right|=\left|Z(0)-\frac{r}{p^2-1}\right|,$$

and

$$\begin{aligned}\left(1-\frac{1}{q}\right)\left(\frac{r}{h}-\frac{r}{q^3-1}\right)q^{3/2} &= \left(1-\frac{1}{q}\right)\left(\frac{1}{q-1}-\frac{r}{q^3-1}\right)p^3\\ &= p(p^2-1)\left(\frac{1}{p^2-1}-\frac{r}{p^6-1}\right)\\ &\le p\,.\end{aligned}$$

The proof of (10) follows from the following inequalities:

$$\begin{aligned}&\left(\frac{r}{h}-\frac{r}{q^k-1}+\frac{h-r}{h}\cdot q^{1/2}\right)q^{1/2}\\ &\qquad=\left(\frac{1}{p^2-1}-\frac{r}{p^6-1}+p-\frac{p}{p^2-1}\right)p\\ &\qquad\le p^2.\end{aligned}$$

□

A similar corollary can be proved for $p \equiv 2 \pmod 3$.

COROLLARY 3. *Let $p \equiv 2 \pmod 3$. For* XTR *characteristic sequence with period $r|(p^2-p+1)$, and any nonzero element $b \in GF(q)\setminus\{0\}$ there holds*

$$\left|Z(0)-\frac{r}{p^2-1}\right| \le 3p\,, \tag{11}$$

$$\left|Z(b)-\frac{p^4 r}{p^6-1}\right| \le p^2. \tag{12}$$

In the case of $b \neq 0$ the previous corollary does not give a better estimation for the upper bound than trivial one. Also for $b = 0$ experiments show that 0 does not appear in the sequence at all.

However, for XTR sequences we prove better estimations.

LEMMA 2. *Let $s_k \in GF(q)$ be an element of an* XTR *sequence with period q_X where $0 \le k < q_X$. Then $s_k = s_{kp^2 (\mathrm{mod}\ q_X)} = s_{kp^4 (\mathrm{mod}\ q_X)}$.*

P r o o f. Let α be a root of its characteristic polynomial, and $s_k = \mathrm{Tr}_{E/F}(\alpha^k)$. Since $\alpha^k, (\alpha^k)^{p^2}, (\alpha^k)^{p^4}$ are conjugates we have $\mathrm{Tr}_{E/F}(\alpha^k) = \mathrm{Tr}_{E/F}\big((\alpha^k)^{p^2}\big) = \mathrm{Tr}_{E/F}\big((\alpha^k)^{p^4}\big)$. The lemma follows from the fact that $s_{kp^2\ (\mathrm{mod}\ q_X)} = \mathrm{Tr}_{E/F}\big((\alpha^k)^{p^2}\big)$, $s_{kp^4\ (\mathrm{mod}\ q_X)} = \mathrm{Tr}_{E/F}\big((\alpha^k)^{p^4}\big)$ and q_X is the period of the sequence $\{s_k\}_{k\ge 0}$. □

LEMMA 3. *Let $s_k \in GF(q)$ be an element of an* XTR *sequence with period q_X where $0 \le k < q_X$. Then indices k, $kp^2 (\bmod\ q_X)$ and $kp^4 (\bmod\ q_X)$ are pairwise distinct if and only if $k \neq 0$.*

P r o o f . The lemma follows from the fact that there exists only the trivial solution $k = 0$ for any of two congruences $k \equiv kp^2 (\bmod\ p^2 - p + 1)$, $k \equiv kp^4$ $(\bmod\ p^2 - p + 1)$ and $kp^2 \equiv kp^4 (\bmod\ p^2 - p + 1)$. □

COROLLARY 4. *The element $s_0 = 3$ of an* XTR *sequence with period q_X appears exactly once in one period of the sequence.*

P r o o f . Let $s_k = s_0$ for some $0 < k < q_X$. Then from $s_0 = \mathrm{Tr}_{E/F}(\alpha^0) = \mathrm{Tr}_{E/F}(1) = \mathrm{Tr}_{E/F}(\alpha^k)$ it follows that $\mathrm{Tr}_{E/F}(\alpha^k - 1) = 0$, and this is possible if and only if $\alpha^k - 1 = 0$. Since α is a generator, this is a contradiction with the period of the sequence. □

LEMMA 4. *Let $s_k = s_{kp^2 (\bmod\ q_X)} = s_{kp^4 (\bmod\ q_X)} = s_l = s_{lp^2 (\bmod\ q_X)} = s_{lp^4 (\bmod\ q_X)}$ be elements of an* XTR *sequence with period q_X and $l \notin \{k,\ kp^2$ $(\bmod\ q_X),\ kp^4 (\bmod\ q_X)\}$ where $0 \le l, k < q_X$. Then $\{k, kp^2 (\bmod\ q_X),\ kp^4$ $(\bmod\ q_X)\} \cap \{l, lp^2 (\bmod\ q_X),\ lp^4 (\bmod\ q_X)\} = \emptyset$.*

P r o o f . We show, that $lp^2 (\bmod\ q_X) \notin \{k, kp^2 (\bmod\ q_X), kp^4 (\bmod\ q_X)\}$ and $lp^4 (\bmod\ q_X) \notin \{k, kp^2 (\bmod\ q_X), kp^4 (\bmod\ q_X)\}$. If $lp^2 \equiv kp^2 (\bmod\ q_X)$ or $lp^2 \equiv kp^4 (\bmod\ q_X)$ we have a contradiction with $l \notin \{k, kp^2 (\bmod\ q_X),\ kp^4$ $(\bmod\ q_X)\}$ since $\gcd(p^2, p^2 - p + 1) = \gcd(p^2, q_X) = 1$. The second part is straightforward. □

Previous lemmas show that the number of appearances of any element except for s_0 is a multiple of 3.

NOTE. In the case of the kth order maximal period sequence corresponding to a primitive minimal polynomial the number of elements for any $c \in GF(q^m)$ is exactly known:

$$Z(c) = \begin{cases} q^{k-m} - 1 & \text{for } c = 0\,, \\ q^{k-m} & \text{for } c \neq 0\,. \end{cases}$$

In the case we do not have a maximum-length sequence, the situation is unknown. Next theorem states, that the distribution of $Z(c)$ is the same even for different sequences with the same period.

THEOREM 2. *For any element $a \in GF(q)$ and all elements $\beta, \gamma \in GF(q^3)$ for which $\mathrm{ord}(\beta) = \mathrm{ord}(\gamma)$ there holds:*

$$\left|\{i:\ \mathrm{Tr}_{E/F}(\beta^i) = a\}\right| = \left|\{j:\ \mathrm{Tr}_{E/F}(\gamma^j) = a\}\right|.$$

Proof. Let α be a primitive element of $GF(q^3)$. Let $\operatorname{ord}(\beta) = \operatorname{ord}(\gamma) = r$. Then by M we denote the set of all elements of $GF(q^3)$ with the same order r. They are all powers of α. Let k be the smallest integer for which $\operatorname{ord}(\alpha^k) = r$. Then all elements in M can be written in the form $(\alpha^k)^i$, where $\gcd(i,r) = 1$ and $1 \le i \le q^3 - 1$. To make expressions shorter, we denote $\omega = \alpha^k$. Then

$$\langle\omega\rangle = \left\{\alpha^k, \alpha^{2k}, \dots, \alpha^{rk}\right\}.$$

Let us consider any fixed i and ω^i. Then there holds

$$\begin{aligned}\langle\omega^i\rangle &= \left\{\alpha^{ki}, (\alpha^{ki})^2, \dots, (\alpha^{ik})^r\right\} \\ &= \left\{(\alpha^k)^i, (\alpha^{2k})^i, (\alpha^{3k})^i, \dots, (\alpha^{rk})^i\right\}.\end{aligned}$$

As $\gcd(i,r) = 1$, the set $\langle\omega^i\rangle$ is just a permutation of the set $\langle\omega\rangle$ and thus there holds

$$\langle\omega^i\rangle = \langle\omega\rangle. \tag{13}$$

Now, as β and γ are both of order r, it is possible to write them in the form $\beta = \omega^i$ and $\gamma = \omega^j$ for some i, j for which $\gcd(i,r) = 1$, $\gcd(j,r) = 1$. Then from the equation (13) it must hold

$$\langle\beta\rangle = \langle\omega\rangle = \langle\gamma\rangle.$$

If the sets of the trace function images are the same, then also distribution of the trace function must be the same and this proves the theorem. $\square$

THEOREM 3. *Any* GH *and* XTR *characteristic sequence can be obtained from some maximal period sequence (with period $p^6 - 1$) by decimation.*

Proof. Let $u_0, u_1, \dots$ be a maximal sequence given by equation

$$u_n = \operatorname{Tr}_{E/F}(\gamma^n),$$

where γ is any of primitive elements of the $GF(q^3)$. Let

$$\{s_k\}_{k\ge 0}$$

be the 3rd order characteristic sequence with an irreducible minimal polynomial $f(x)$ and root α in E. Then we can write $\alpha = \gamma^d$ for some integer $1 < d < p^6 - 1$ and there holds

$$s_n = \operatorname{Tr}_{E/F}(\alpha^n) = \operatorname{Tr}_{E/F}\big((\gamma^d)^n\big) = \operatorname{Tr}_{E/F}\big(\gamma^{nd}\big) = u_{nd}.$$

$\square$

COROLLARY 5. *For any* GH *and* XTR *sequences with the same periods, frequentative properties over the same finite field $GF(q)$ are the same. Moreover, for a given order they do not depend on the selection of the characteristic polynomial.*

5. Differential cryptanalysis

Consider any sequence $s_0, s_1, \dots$ over $GF(q)$ with the least period N. For each $g \in GF(q)$ let

$$C_g = \{i \in Z_N \colon s_i = g\}.$$

Differential cryptanalysis of the sequence $\{s_k\}_{k\geq 0}$ as defined in [1] is the analysis of the following difference parameters:

$$d_s(x, y, w) = \left|C_x \cap (C_y - w)\right|, \qquad x, y \in GF(q),\ w \in Z_N.$$

Let α be a root of the irreducible characteristic polynomial $f(x)$ of the sequence $\{s_k\}_{k\geq 0}$. Then

$$d_s(x, y, w) = \left|\{i\colon\ \mathrm{Tr}_{E/F}(\alpha^i) = x,\ \mathrm{Tr}_{E/F}(\alpha^{i+w}) = y\}\right|.$$

Hence any information about mappings of powers of α by the trace function Tr would be valuable.

Let $a \in GF(q)$, $T(a) = \{x \in GF(q^3)\colon \mathrm{Tr}(x) = a\}$. Let α be any element of the field $GF(q^3)$. Then $B = \{\alpha, \alpha^q, \alpha^{q^2}\}$ is a normal base, and for any $\gamma = a_1\alpha + a_2\alpha^q + a_3\alpha^{q^2}$ there holds

$$\mathrm{Tr}_{E/F}(\gamma) = (a_1 + a_2 + a_3)\,\mathrm{Tr}_{E/F}(\alpha).$$

Thus the set $T(a)$ is a hyperplane of dimension 2 over $GF(q)$. In fact this is the set of all points $x = (x_1, x_2, x_3)$ such that $(x_1 + x_2 + x_3)\,\mathrm{Tr}_{E/F}(\alpha) = a$.

From the point of view of differential properties we need to know, how $T(a)$ intersects with the subgroup G.

For binary sequences and $p = 2$ it is known from [1], that indices of nonzero elements in the characteristic sequence form a difference set, and hence they have good cryptographic properties.

For a prime $p \neq 2$ (which is our case) the problem of description $\langle\beta\rangle \cap T(a)$ remains open for all $a \in GF(q)$. This problem leads to another problem, namely how to describe coordinates of β^i in some normal base.

6. Autocorrelation properties

Autocorrelation function of the sequence $\{s_k\}_{k\geq 0} = s_0, s_1, \dots$ is defined as

$$AC_s(l) = \sum_{i=0}^{N-1} \chi(s_i - s_{i+l}),$$

where N is the period of the sequence and χ is the additive character with values

$$\chi(g) = \exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{F/K}(g)\right).$$

It is well known, that the autocorrelation is a simpler version of a differential cryptanalysis.

Clearly for $l = 0$ $AC_s(0) = N$. Therefore we exclude this case from our considerations.

For autocorrelation function of the sequence $\{s_k\}_{k\geq 0}$ there holds

$$\begin{aligned}
AC_s(l) &= \sum_{j=0}^{N-1}\chi(s_j - s_{j+l}) = \sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{F/K}(s_j - s_{j+l})\right)\\
&= \sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{F/K}\bigl(\operatorname{Tr}_{E/F}(\theta\alpha^j) - \operatorname{Tr}_{E/F}(\theta\alpha^{j+l})\bigr)\right)\\
&= \sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{F/K}\bigl(\operatorname{Tr}_{E/F}(\theta\alpha^j - \theta\alpha^{j+l})\bigr)\right)\\
&= \sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{E/K}\bigl(\theta(1-\alpha^l)\alpha^j\bigr)\right).
\end{aligned}$$

If we denote by θ' the expression $\theta(1-\alpha^l)$, which is a constant for a given l, then we have an exponential sum

$$AC_s(l) = \sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{E/K}(\theta'\alpha^j)\right). \tag{14}$$

It is not much known about this type of sums to our best knowledge. This sum can be bounded by the following lemma which is a consequence of Theorems 8.24 and 8.78 from [7] and [10].

Lemma 5. *For subgroup $G = \langle\alpha\rangle$ of the order $|G| \geq p^{3+\varepsilon}$, where $\varepsilon > 0$ is any constant, the following bound holds*

$$\max_{\theta\in E^*}\left|\sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{p}\operatorname{Tr}_{E/K}(\theta\alpha^j)\right)\right| \leq p^3,$$

In the case of GH sequences the previous lemma yields

$$|AC_s(l)| \leq p^3$$

for $l \neq 0$.

Due to the relatively small order of an XTR subgroup the lemma is not applicable in this case.

7. Experiments

We executed several tests to obtain an overview of GH and XTR sequences. The tests were implemented in C++ programming language using NTL library [9]. NTL provides functions for modular arithmetic and computing in finite fields.

7.1 Properties of XTR sequences

- $p = 13$ and XTR subgroup of order $q_X = 157$. Finite field $GF(13^2)$ was represented as $GF(13)/(x^2 + 11x + 8)$ with the root of polynomial denoted by α. The selected third degree characteristic polynomial was $f(x) = x^3 + (2\alpha + 2)x^2 + (2\alpha + 7)x + 12$. From all elements of $GF(13^2)$ in one period of sequence, 116 elements do not appear at all, one element ($s_0 = 3$) appears exactly once, and 52 elements appear three times.
- $p = 29$ and $q_X = 271$. Finite field $GF(29^2)$ was represented as $GF(29)/(x^2 + 13x + 16)$ with the root of polynomial denoted by α. The selected characteristic polynomial was $f(x) = x^3 + (\alpha + 6)x^2 + (\alpha + 7)x + 28$. From all elements of $GF(29^2)$ in one period of sequence, 750 elements do not appear at all, the element 3 appears exactly once, and 90 elements appear three times.
- $p = 53$ and $q_X = 919$. Finite field $GF(53^2)$ was represented as $GF(53)/(x^2 + 52x + 1)$ with the root of polynomial denoted by α. The selected characteristic polynomial was $f(x) = x^3 + (49\alpha + 45)x^2 + (49\alpha + 12)x + 52$. From all elements of $GF(53^2)$ in one period of sequence, 2502 elements do not appear at all, the element 3 appears exactly once, and 306 elements appear three times.

Since in the XTR system the order of the subgroup G is smaller than the number of elements of the field $\mathbb{F}$, and assuming our Lemmas 2, 3, 4 as well as results of our experiments, it is possible to formulate the following hypothesis.

Hypothesis 1. For any XTR sequence there holds $Z(b) \in \{0, 3\}$ for $b \neq 3$.

To prove this hypothesis one needs to show e.g., that two different non-conjugate elements of $\mathbb{E}$ are mapped to different values by the trace function. The rest follows from Lemmas 2, 3, and 4.

7.2 Properties of GH sequences

We examined an instance of GH sequence for $p = 13$ and $q = p^2 = 169$ over the field $GF(13)[\alpha]$, where α is a root of the polynomial $x^2 + 7x + 4$. The chosen characteristic polynomial is $f(x) = x^3 - (5\alpha + 9)x^2 + (11\alpha + 11)x - 1$. Table 1 shows occurrences of elements in this GH sequence. For each number

TABLE 1. Number of elements with the same frequencies for $q = 169$.

Number of occurrences	144	153	162	169	171	180	189
Number of elements	12	12	48	3	28	42	24

of occurrences, the number of elements with such a number of occurrences is displayed. For example, in the chosen sequence, 12 different elements appear exactly 144 times.

Elements appeared in GH characteristic sequence from 144 to 189 times. In our case the expected value, given by Theorem 1, is $\lfloor(169^2+169+1)/169\rfloor = 170$.

Another example is an instance of GH sequence for $p = 29$ and $q = 841$ over the field $GF(29)[\alpha]$ where α is a root of the polynomial $x^2 + 15x + 4$. The chosen characteristic polynomial is $f(x) = x^3 - 25x^2 + (27\alpha + 27)x - 1$. Tables 2 and 3 have the same meaning as Table 1.

TABLE 2. Number of elements with the same frequencies for $q = 841$.

Number of occurrences	792	801	810	819	828	837	841
Number of elements	72	24	96	72	72	96	3

TABLE 3. Continuation of Table 2.

Number of occurrences	846	855	864	873	882	891	900
Number of elements	48	48	168	24	54	36	28

Element 0 (zero) appears 900 times. Expected value of $Z(b)$ is 850. Frequencies of elements are in the range from 792 to 900, close to the expected value.

8. Conclusion

We investigated distribution of elements in GH and XTR sequences. We proved some theoretical bounds (Corollary 1, 2, 3 and 4). We also performed several experiments to show the behaviour of XTR and GH sequences. They showed good frequentative properties and led to Hypothesis 1.

REFERENCES

[1] CUSICK, T.—DING, C.—RENVALL, A.: *Stream Ciphers and Number Theory*, North Holland, Amsterdam, 1998.

[2] GONG, G.—HARN, L.: *A new approach on public key distribution*, ChinaCRYPT '98, 1988, pp. 50–55.

[3] JUNGNICKEL, D.: *Finite Fields*, Wissenschaftverlag, 1993.

[4] LENSTRA, A. K.—VERHEUL, E. R.: *The XTR public key system*, in: CRYPTO '00, Lecture Notes in Comput. Sci. 1880, Springer-Verlag, Berlin, 2000, pp. 1–19.

[5] LENSTRA, A. K.—VERHEUL, E. R.: *An overview of the XTR public key system*, in: The proceedings of the Public Key Cryptography and Computational Number Theory Conference, Berlin de Gruyter, 2001, pp. 151–180.

[6] LIDL, R.—NIEDERREITER, H.: *Introduction to Finite Fields and their Applications*, Oxford University Press, Oxford, 1986.

[7] LIDL, R.—NIEDERREITER, H.: *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[8] MENEZES, A.—van OORSCHOT, P.—VANSTONE, S.: *Handbook of Applied Cryptography*, CRC Press, Inc. Singapore, 1996.

[9] SHOUP, V.: *NTL A library for doing number theory*, `http://shoup.net/ntl`.

[10] SHPARLINSKI, I. E.: *On the generalized hidden number problem and bit security of XTR*, Preprint, 2000, 1–14.

Received January 12, 2004

Otokar Grošek
Department of Mathematics
Faculty of Electrical Engineering
and Information Technology
Slovak University of Technology
Ilkovičova 3
SK–812 19 Bratislava
SLOVAKIA
E-mail: grosek@elf.stuba.sk

Július Šiška
KPMG Slovensko, spol. s r.o.
Mostová 2
SK–811 02 Bratislava
SLOVAKIA
E-mail: jsiska@kpmg.sk