Polynomial interpolation of the generalized Diffie–Hellman and Naor–Reingold functions

Thierry Mefenza, Damien Vergnaud

Noname manuscript No.
(will be inserted by the editor)

Polynomial Interpolation of the Generalized Diffie-Hellman and Naor-Reingold Functions

Thierry Mefenza · Damien Vergnaud

the date of receipt and acceptance should be inserted later

Abstract In cryptography, for breaking the security of the Generalized Diffie-Hellman and Naor-Reingold functions, it would be sufficient to have polynomials with small weight and degree which interpolate these functions. We prove lower bounds on the degree and weight of polynomials interpolating these functions for many keys in several fixed points over a finite field.

Keywords. Naor-Reingold function, Generalized Diffie-Hellman function, polynomial interpolation, finite fields.

MSC2010. 11T71, 94A60

1 Introduction

The security of most cryptographic protocols relies on some unproven computational assumption which states that a well-defined computational problem is intractable (*i.e.* cannot be solved by a Turing machine in polynomial time). In group-based cryptography, we generally consider a cyclic group $\mathbb{G}$ (denoted multiplicatively) generated by some element g and the so called *computational Diffie-Hellman assumption* states that it is difficult to compute the element g^{xy} from known elements g^x and g^y (for x and y picked uniformly at random between 1 and the order $\mathbb{G}$). This assumption is the basis of the Diffie-Hellman key exchange [1] and the most efficient means known to solve this computational problem in groups used for cryptography is to solve the standard discrete logarithm problem (*i.e.* given h an element picked uniformly at random in $\mathbb{G}$, compute x such that $g^x = h$). Unfortunately, even the computational Diffie-Hellman assumption by itself is generally not sufficient to assess the security of protocols proposed and used in group-based cryptography. Cryptographers have then proposed much stronger assumptions in order to analyze the security of cryptosystems. For instance, the *decision Diffie-Hellman assumption* [2] states that given a cyclic group $\mathbb{G}$ given some elements g, g^x and g^y, no efficient algorithm can distinguish between g^{xy}

École normale supérieure, CNRS, PSL Research University · Sorbonne Universités, UPMC, CNRS, Institut Universitaire de France

and an element picked uniformly at random in $\mathbb{G}$. This assumption has been used in numerous important cryptographic applications.

In 1997, based on the decision Diffie-Hellman assumption, Naor and Reingold [3,4] proposed an efficient pseudo-random function family (*i.e.* a collection of functions that can be evaluated in polynomial time using a secret-key but for which no polynomial-time algorithm can distinguish (with significant advantage) between a function chosen randomly from the family and a truly random function). Their function takes inputs in $\{0,1\}^n$ (for some parameter n) and outputs an element in a group $\mathbb{G}$ of prime order ℓ with generator g. The secret key is an n-dimensional vector $\boldsymbol{a} = (a_1, \ldots, a_n) \in ((\mathbb{Z}/\ell\mathbb{Z})^*)^n$ and the Naor-Reingold function is defined as

$$\begin{aligned} f_{\boldsymbol{a}} : \quad \{0,1\}^n &\longrightarrow \mathbb{G} \\ (x_1, \ldots, x_n) &\longmapsto f_{\boldsymbol{a}}(x_1, \ldots, x_n) = g^{\prod_{i=1}^{n} a_i^{x_i} \bmod \ell} \end{aligned}$$

To simplify the notation, given an n-dimensional vector $\boldsymbol{a} = (a_1, \ldots, a_n) \in ((\mathbb{Z}/\ell\mathbb{Z})^*)^n$ and a variable x that will denote indifferently an n-bit string $(x_1, \ldots, x_n) \in \{0,1\}^n$ or an integer $x \in \{0, 1, \ldots, 2^n - 1\}$ (which implicitly defines $(x_1, \ldots, x_n) \in \{0,1\}^n$ the bit representation of x with extra leading zeros if necessary), we denote $\boldsymbol{a}^x$ the element in $\mathbb{F}_\ell = (\mathbb{Z}/\ell\mathbb{Z})$ defined by $\boldsymbol{a}^x = a_1^{x_1} \cdots a_n^{x_n} \bmod \ell$. In addition, when the generator g is fixed, we will denote $[x] = g^x$ for any $x \in \mathbb{F}_\ell$. With this notation, the Naor-Reingold function is simply defined by $f_{\boldsymbol{a}}(x) = g^{\boldsymbol{a}^x} = [\boldsymbol{a}^x]$.

It is shown in [3,4] that the Naor-Reingold function is pseudo-random if the decision Diffie-Hellman assumption holds in the group $\mathbb{G}$. Two interesting candidates for $\mathbb{G}$ are a subgroup of the multiplicative group of a (prime) finite field and a subgroup of the points of an elliptic curve defined over a finite field.

With the development of pairing-based cryptography, new assumptions in cyclic groups $\mathbb{G}$ were proposed to base the security of more complex or more efficient protocols. Joux [5] notably constructed a one-round tripartite key exchange whose security requires the *tripartite decision Diffie-Hellman assumption* (or *decision "Triffie-Hellman" assumption*) which states that given group[1] elements g, g^x, g^y and g^z no efficient algorithm can distinguish between g^{xyz} and an element picked uniformly at random in $\mathbb{G}$. Many generalizations of the decision Diffie-Hellman assumption were proposed (e.g. [6,7]) and can be stated as follows: given an integer n and some specific values of the Naor-Reingold function, no efficient algorithm can distinguish another value of the Naor-Reingold function from an element picked uniformly at random in $\mathbb{G}$. A salient example is the *n-partite decision Diffie-Hellman assumption*: given some elements g, g^{a_1}, ..., g^{a_n} no efficient algorithm can distinguish between $g^{a_1 \cdots a_n}$ and an element picked uniformly at random in $\mathbb{G}$.

Prior work. In order to refute the computational Diffie-Hellman assumption, it would be sufficient to know a bivariate polynomial $f(X_1, X_2)$ over a finite field of small degree or of small weight (*i.e.* a small number of its non-zero coefficients) over a finite field satisfying $f([x], [y]) = [xy]$, for all pairs $(x, y) \in S$ for a large subset $S \subseteq \{0, \ldots, \ell - 1\}^2$, where ℓ is the order of g. Lower bounds on the degree and the weight of such polynomials have been obtained (see [8–11] and references

[1] Actually, the security of Joux's key exchange relies on the stronger decision bilinear Diffie-Hellman assumption in groups equipped with a bilinear map. This assumption implies the tripartite decision Diffie-Hellman assumption in the so-called target group of the bilinear map.

therein). For the decision Diffie-Hellman assumption, it would be sufficient to know a trivariate polynomial $f(X_1, X_2, X_3)$ over a finite field of small weight (even if it is of high degree) satisfying: $f([x], [y], [xy]) = 0$, for all pairs $(x, y) \in S$ for a large subset $S \subseteq \{0, \ldots, \ell - 1\}^2$. Typically, the complexity of a polynomial is measured by its degree, but a more accurate complexity measure could also be the number of monomials (or weight). Lower bounds on degree of polynomials interpolating Diffie-Hellman triples are also known (see [11] and references therein) but there is no result on the weight of such polynomials.

Several number-theoretic properties and complexity measures have been studied for the Naor-Reingold pseudo-random functions over finite fields as well as over elliptic curves: distribution (see [12,13] and references therein), period (see [14]), linear complexity (see [15–18]) and non-linear complexity (see [19]). Recently [20], the authors of the present paper proved lower bounds on the degree of polynomials interpolating the Naor-Reingold pseudo-random function at several points for fixed keys (over a finite field and over the group of points on an elliptic curve over a finite field). They left open the problem to give lower bounds on the degree of general multivariate polynomials that interpolate the Naor-Reingold function in several fixed points for many keys. The main goal of this paper is to give such lower bounds for the Naor-Reingold and the generalized Diffie-Hellman functions over a finite field (*e.g.* given $g^{a_1}, \ldots, g^{a_n} \in \mathbb{G}$, distinguish between $g^{a_1 \cdots a_n}$ from an element picked uniformly at random in $\mathbb{G}$ [7] and other problems from the *matrix Diffie-Hellman* framework [**?**]). We prove that polynomials interpolating these functions (implicitly or explicitly) on a large set have degree and weight in $\ell^{O(1)}$ (i.e. exponential in the so-called *security parameter* in the cryptographic context).

Our contributions. In order to break the security of the Naor-Reingold pseudo-random function, it would be sufficient to have an efficiently computable k-variate polynomial $f(X_1, \ldots, X_k)$ over a finite field (of low weight) satisfying:

$$f\left([\boldsymbol{a}^{x^1}], \ldots, [\boldsymbol{a}^{x^k}]\right) = [\boldsymbol{a}^{x^{k+1}}],$$

for all $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$ for a large subset $S \subseteq (\mathbb{F}_\ell^*)^n$, for some $k \geq 1$ and for some known values $x^1, \ldots, x^{k+1} \in \{0, \cdots, 2^n - 1\}$. One can easily see that this polynomial interpolation is a generalization of the polynomial interpolation of the computational Diffie-Hellman assumption in the case $n = 2$, $k = 2$, $x^1 = (1, 0)$, $x^2 = (0, 1)$ and $x^3 = (1, 1)$. Adapting the known lower bounds on the polynomial interpolation on the discrete logarithm and the Diffie-Hellman Problem in subgroups of the multiplication group of a finite field (*e.g.* [21–25,10,11] and references therein), we prove that a low-weight multivariate polynomial cannot reveal information on the functions values. Using the same methods, we also prove that no low weight polynomial f over a finite field can satisfy: $f([a_1], \ldots, [a_n], [a_1 \ldots a_n]) = 0$, for all $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$ for a large subset $S \subseteq (\mathbb{F}_\ell^*)^n$. In particular, for $n = 2$, this means that a low weight polynomial cannot break the decision Diffie-Hellman assumption.

2 Preliminaries

Let p be an odd prime number and q a prime power of p. We denote by $\mathbb{F}_p$ the finite field with p elements and the elements of $\mathbb{F}_p$ are identified with the set of integers

$\{0, \cdots, p-1\}$ and $\mathbb{F}_q$ an extension of the prime finite field $\mathbb{F}_p$. Given $g \in \mathbb{F}_q^*$ with prime order ℓ (with $\ell \mid q-1$) we can consider the Naor-Reingold pseudo-random function defined over $\mathbb{G} = \langle g \rangle$: $f_{\boldsymbol{a}}(x) = g^{\boldsymbol{a}^x} = [\boldsymbol{a}^x] \in \mathbb{G} \subset \mathbb{F}_q^*$, for a secret key $\boldsymbol{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$ where as above x will denote indifferently an n-bit string $(x_1, \ldots, x_n) \in \{0,1\}^n$ or an integer $x \in \{0, 1, \ldots, 2^n - 1\}$ (with $x = \sum_{i=1}^n x_i 2^{i-1}$).

In the following, we will use the following lemmas (see [10]) where the *weight* $w(f)$ (or sparsity) of a polynomial $f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ is the number of its non-zero coefficients.

Lemma 1 *[[10]] Let D be an integral domain, $n \in \mathbb{N}$ and $f \in D[X_1, \ldots, X_n]$ a polynomial of total degree d with at least N zeros in T^n with components in T. If f is not the zero polynomial, then we have*

$$d \geq \frac{N}{|T|^{n-1}}.$$

Lemma 2 *[[10]] Let $\gamma \in \mathbb{F}_q$ be an element of order d, $\mathbb{G}$ the group generated by γ, n a positive integer, and $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a nonzero polynomial of local degree at most $d-1$ in each variable with at least N zeros in $\mathbb{G}^n$. If f is not the zero polynomial, then we have*

$$w(f) \geq \frac{d^n}{d^n - N}.$$

3 Polynomial Interpolation

In this section, q is a prime power, n is an integer and $g \in \mathbb{F}_q^*$ is an element of prime order ℓ (with $\ell \mid q-1$). We prove results on the multivariate polynomial interpolation of the Naor-Reingold functions over a finite field and generalized Diffie-Hellman problems. We consider polynomials that interpolate values of these functions for fixed values in $\{0, \cdots, 2^n - 1\}$ and a large set of keys. First, we consider an interpolation by a polynomial with k variables, with $k \leq n$.

Theorem 1 *Let $1 \leq k \leq n$ be an integer. Let $S \subseteq (\mathbb{F}_\ell^*)^n$, with $|S| = (\ell-1)^n - s$ with $|S| > k(\ell-1)^{n-1}$. Let $x^1, \ldots, x^{k+1} \in \{1, \cdots, 2^n - 1\}$ be pairwise distinct and let $f \in \mathbb{F}_q[X_1, \ldots, X_k]$, be a polynomial satisfying:*

$$f\left([\boldsymbol{a}^{x^1}], \ldots, [\boldsymbol{a}^{x^k}]\right) = [\boldsymbol{a}^{x^{k+1}}], \quad \text{for all } \boldsymbol{a} = (a_1, \ldots, a_n) \in S. \tag{1}$$

If the elements x^i, $i \in \{1, \ldots, k\}$ seen as vectors over $\mathbb{F}_2^n$ are linearly independent over $\mathbb{F}_2$, then:

$$\deg(f) \geq \frac{\ell-1}{2} - \frac{s}{(\ell-1)^{n-1}}$$

and if $\deg_{X_i}(f) \leq \frac{\ell-1}{2}$, for all $i \in \{1, \ldots, n\}$, we have

$$w(f) \geq \frac{\ell^{k/2}}{2^{1/2}(\ell^k - (\ell-1)^k + 2s/(\ell-1)^{n-k})^{1/2}}.$$

In particular, for $s = o(\ell^n)$, we have $\deg(f) = \Omega(\ell)$ and and if $\deg_{X_i}(f) \leq \frac{\ell-1}{2}$, for all $i \in \{1, \ldots, n\}$, we have $w(f) = \Omega(\ell^{k/2})$.

Proof For any $i \in \{1, \ldots, k+1\}$, we denote $x^i = x_1^i \ldots x_n^i$ its binary representation and put $\tilde{x^i} = x_1^i \ldots x_k^i 0 \ldots 0$ which is obtained from x^i by considering the k first positions of its binary representation and replacing the $n-k$ last positions by 0. We suppose without loss of generality that the elements $\tilde{x^i}$, $i \in \{1, \ldots, k\}$ seen as vectors over $\mathbb{F}_2^n$ are linearly independent over $\mathbb{F}_2$.

Since $|S| > k(\ell-1)^{n-1}$, we have $w(f) \geq 2$ by the following claim:

Claim If $w(f) = 1$ then (1) holds for at most $k(\ell-1)^{n-1}$ keys $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$.

Proof If $w(f) = 1$, then f is a monomial and there exists $(\alpha_1, \ldots, \alpha_k) \in \{0, \ldots, \ell-1\}^k$ such that $\alpha_1 \boldsymbol{a}^{x^1} + \cdots + \alpha_k \boldsymbol{a}^{x^k} = \boldsymbol{a}^{x^{k+1}} \bmod \ell$ (where f is the monomial $f(X_1, \ldots, X_k) = X_1^{\alpha_1} \ldots X_k^{\alpha_k}$). We prove by induction on k that the number of $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$ such that $\alpha_1 \boldsymbol{a}^{x^1} + \cdots + \alpha_k \boldsymbol{a}^{x^k} = \boldsymbol{a}^{x^{k+1}}$ does not exceed $k(\ell-1)^{n-1}$.

1. For $k = 0$, the equation $\boldsymbol{a}^{x^{k+1}} = 0$ has no solution and the statement is clearly true.
2. Otherwise, because $x^{k+1} \neq x^k$, there exists j such that the j-th component of x^{k+1} is different from the j-th component of x^k. Then the above equation can be written in the form $A = Ba_j$ where A and B do not depend on a_j. If $B \neq 0$, then for any vector $(a_1, \cdots, a_{j-1}, a_{j+1}, \cdots, a_n) \in (\mathbb{F}_\ell^*)^{n-1}$, the value of a_j is defined uniquely. If $B = 0$, then $A = 0$ and by induction, the number of $(a_1, \cdots, a_{j-1}, a_{j+1}, \cdots, a_n) \in (\mathbb{F}_\ell^*)^{n-1}$ does not exceed $(k-1)(\ell-1)^{n-2}$. Therefore, the number of solutions does not exceed $(k-1)(\ell-1)^{n-1} + (\ell-1)^{n-1} = k(\ell-1)^{n-1}$, and the result follows.

There is some $t \in \{1, \ldots, n\}$ such that $x_t^{k+1} = 1$ and let $T_0 = \{i : x_t^i = 1\} \subseteq \{1, \ldots, k\}$ that we denote $T_0 = \{i_1, \ldots, i_v\}$, with $i_j < i_{j+1}$ for $j \in \{1, \ldots, v-1\}$. Let

$$W = \left\{ \boldsymbol{a} \in (\mathbb{F}_\ell^*)^n : \begin{array}{l} \boldsymbol{a} = (a_1, \ldots, a_n) \in S \\ \text{and } (a_1, \ldots, a_{t-1}, 2a_t, a_{t+1}, \ldots, a_n) \in S \end{array} \right\},$$

then by the the union bound, $|W| \geq (\ell-1)^n - 2s$. By the pigeonhole principle, there exists $(b_{k+1}, \ldots, b_n) \in (\mathbb{F}_\ell^*)^{n-k}$ such that the set

$$T = \{(a_1, \ldots, a_k) \in (\mathbb{F}_\ell^*)^k : a' = (a_1, \ldots, a_k, b_{k+1}, \ldots, b_n) \in W\}$$

satisfies $|T| \geq (\ell-1)^k - 2s/(\ell-1)^{n-k}$. For all $\boldsymbol{a_0} = (a_1, \ldots, a_k) \in T$, putting $\boldsymbol{a'} = (a_1, \ldots, a_k, b_{k+1}, \ldots, b_n)$, we have:

$$\begin{cases} f\left([\boldsymbol{a'}^{x^1}], \ldots, [\boldsymbol{a'}^{x^k}]\right) = [\boldsymbol{a'}^{x^{k+1}}] \\ f\Big([\boldsymbol{a'}^{x^1}], \ldots, [\boldsymbol{a'}^{x^{i_1-1}}], [2\boldsymbol{a'}^{x^{i_1}}], [\boldsymbol{a'}^{x^{i_1+1}}], \ldots \\ \qquad \ldots, [\boldsymbol{a}^{x^{i_v-1}}], [2\boldsymbol{a}^{x^{i_v}}], [\boldsymbol{a}^{x^{i_v+1}}], \ldots, [\boldsymbol{a}^{x^n}]\Big) = [2\boldsymbol{a'}^{x^{k+1}}] \end{cases}$$

Since the elements $\tilde{x^i}$, $i \in \{1, \ldots, k\}$ seen as vectors over $\mathbb{F}_2^n$ are linearly independent over $\mathbb{F}_2$, one can verify that the set

$$T_1 = \left\{ \left([\boldsymbol{a'}^{x^1}], \ldots, [\boldsymbol{a'}^{x^k}]\right) \in (\mathbb{F}_q^*)^k : \boldsymbol{a'} = (\boldsymbol{a_0}, b_{k+1}, \ldots, b_n) \in W, \text{ and } \boldsymbol{a_0} \in T \right\}$$

is of the same cardinality as T. Hence the polynomial

$$F(X_1, \ldots, X_k) = f(X_1, \ldots, X_{i_1}^2, \ldots, \ldots, X_{i_v}^2, \ldots, X_k) - f^2(X_1, \ldots, X_k)$$

has at least $|T| \geq (\ell-1)^k - 2s/(\ell-1)^{n-k}$ zeros. Since $w(f) \geq 2$, one can see that F is a nonzero polynomial and $\deg F \leq 2 \deg f$. By Lemma 1, we obtain:

$$\deg(f) \geq \frac{\ell-1}{2} - \frac{s}{(\ell-1)^{n-1}}.$$

Furthermore if $\deg_{X_i}(f) \leq \frac{\ell-1}{2}$, for all $i \in \{1, \ldots, n\}$, and since $w(F) \leq 2w(f)^2$, then by applying Lemma 2 we have:

$$w(f) \geq \frac{\ell^{k/2}}{2^{1/2}(\ell^k - (\ell-1)^k + 2s/(\ell-1)^{n-k})^{1/2}}.$$

Remark 1 The previous proof uses only the fact that the $\tilde{x^i}$ are linearly independent and we need this assumption to prove that the set T_1 has the same cardinality as T. Note that if $\tilde{x^i} = 2^{n+i-k-1}$ for $i \in \{1, \ldots, k\}$, then the set T_1 is of the same cardinality as T and Theorem 1 holds. Theorem 1 is more general and applies to numerous settings. For instance for $k = 3$, $\tilde{x^1} = 1000\ldots0$, $\tilde{x^2} = 1100\ldots0$ and $\tilde{x^3} = 1010\ldots0$, the set T_1 is of the same cardinality as T and the vectors $\tilde{x^1}, \tilde{x^2}, \tilde{x^3}$ are linearly independent.

Remark 2 In Equation (1), if we replace each $[\boldsymbol{a}^{x^i}]$ by X_i, for $i \in \{1, \ldots, k+1\}$, the polynomial $f(X_1, \ldots, X_k) - X_{k+1}$ has $k+1$ indeterminates and has at least N zeros in $\mathbb{G}^{k+1}$, where N is the cardinality of the set

$$\left\{(\boldsymbol{a}^{x^1}, \ldots, \boldsymbol{a}^{x^{k+1}}) \in (\mathbb{F}_\ell^*)^{k+1} : \boldsymbol{a} \in S\right\}.$$

We do not know a lower bound on N but obviously we have $N \leq (\ell-1)^{k+1}$. By applying Lemma 1, we obtain

$$\deg(f) \geq \frac{N}{(\ell-1)^k}.$$

If the vectors x^i, for $i \in \{1, \ldots, k\}$ are linearly independent, then $N \geq (\ell-1)^n$. Thus we have $n \leq k+1$ and $\deg(f) \geq (\ell-1)^{n-k}$. The result is non-trivial only for $k = n-1$ (and in this case we obtain $\deg(f) \geq \ell - 1$) but is much less general than Theorem 1.

Remark 3 Note that all the previous results on the polynomial interpolation of the Diffie-Hellman function dealt with $k = n = 2$, $x^1 = 10$, $x^2 = 01$ and $x^3 = 11$ while our results are more general and holds for many k, n and x^i, for $i \in \{1, \ldots, k\}$. In the special case, $k = n = 2$, $x^1 = 10$, $x^2 = 01$, $x^3 = 11$ and $s = o(\ell^n)$, Mahassni and Shparlinski obtained in [8] the bound $\deg(f) \geq \ell/128$ while we obtain the bound $\deg(f) \geq \ell/2$. The remainding theorems of the paper cannot be compared with the known results on the polynomial interpolation of the Diffie-Hellman map (since $k > n$).

Now we consider an interpolation by a polynomial with k variables and $k > n$ with some technical conditions on the input values $x^i \in \{0, \cdots, 2^n - 1\}$ for $i \in \{1, \ldots, k\}$.

Theorem 2 *Let $k > n$ be some integer. Let $S \subseteq (\mathbb{F}_\ell^*)^n$, with $|S| = (\ell-1)^n - s$. Let $x^1, \ldots, x^{k+1} \in \{0, \cdots, 2^n - 1\}$ be pairwise distinct such that $x^1 = 2^{n-1} = (1, 0, \ldots, 0)$, $x_1^{k+1} = 1$ and $x_1^i = 0$ for $i \in \{2, \ldots, k\}$ and let $f \in \mathbb{F}_q[X_1, \ldots, X_k]$, with $k > n$ be a polynomial satisfying:*

$$f\left([\boldsymbol{a}^{x^1}], \ldots, [\boldsymbol{a}^{x^k}]\right) = [\boldsymbol{a}^{x^{k+1}}], \quad \text{for all } \boldsymbol{a} = (a_1, \ldots, a_n) \in S.$$

We have

$$\deg(f) \geq \frac{\ell - 1}{2} - \frac{s}{(\ell-1)^{n-1}}.$$

Proof Let W be the set of vectors $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$ such that $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$, $(a_1 + 1, \ldots, a_n) \in S$ and $\boldsymbol{a'} = (1, a_2, \ldots, a_n)$ satisfies $\boldsymbol{a'}^{x^{k+1}} \neq \alpha \mod \ell$ for all $\alpha \in \{1, \ldots, d\}$, where d denotes the degree of f.

Claim We have

$$|W| \geq (\ell-1)^n - 2s - \deg(f)(\ell-1)^{n-1}.$$

Proof It is worth noting that, since $k > n$, we cannot prove Theorem 2 in the same way as we proved Theorem 1. Let $\alpha \in \{1, \ldots, d\}$, the number of $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$ such that $\boldsymbol{a'}^{x^{k+1}} = \alpha \mod \ell$ does not exceed $(\ell-1)^{n-1}$.

Indeed, since $x^k \neq x^1$, there exists $j \in \{2, \ldots, n\}$ such that $x_j^{k+1} = 1$, then for any vector $(a_1, \ldots, a_{j-1}, a_{j+1}, \cdots, a_n) \in (\mathbb{F}_\ell^*)^{n-1}$, the value of a_j is defined uniquely by this equation. Since the number of vectors $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$ such that $(a_1 + 1, \ldots, a_n) \notin S$ does not exceed s, the result follows.

By the pigeonhole principle, there exists $\boldsymbol{b} = (1, b_2, \ldots, b_n) \in (\mathbb{F}_\ell^*)^n$ such that the set

$$T = \{a_1 \in \mathbb{F}_\ell : \boldsymbol{a} = (a_1, b_2, \ldots, b_n) \in W\}$$

satisfies $|T| \geq \ell - 1 - \deg(f) - \frac{2s}{(\ell-1)^{n-1}}$. Then for all $a_1 \in T$, putting $\boldsymbol{a} = (a_1, b_2, \ldots, b_n)$, we have:

$$\begin{cases} f\left([a_1], [\boldsymbol{b}^{x^2}] \ldots, [\boldsymbol{b}^{x^k}]\right) = [\boldsymbol{a}^{x^{k+1}}] \\ f\left([a_1 + 1], [\boldsymbol{b}^{x^2}], \ldots, [\boldsymbol{b}^{x^k}]\right) = [(a_1 + 1, b_2, \ldots, b_n)^{x^{k+1}}] = [\boldsymbol{b}^{x^{k+1}}].[\boldsymbol{a}^{x^{k+1}}] \end{cases}$$

We have for all $a_1 \in T$

$$f\left(g.[a_1], [\boldsymbol{b}^{x^2}], \ldots, [\boldsymbol{b}^{x^k}]\right) - [\boldsymbol{b}^{x^{k+1}}] f\left([a_1], [\boldsymbol{b}^{x^2}] \ldots, [\boldsymbol{b}^{x^k}]\right) = 0$$

and the polynomial

$$F(X) = f\left(gX, [\boldsymbol{b}^{x^2}], \ldots, [\boldsymbol{b}^{x^k}]\right) - [\boldsymbol{b}^{x^{k+1}}] f\left(X, [\boldsymbol{b}^{x^2}] \ldots, [\boldsymbol{b}^{x^k}]\right)$$

has at least $\ell - 1 - \deg(f) - \frac{2s}{(\ell-1)^{n-1}}$ zeros.

The polynomial $f(X, [\boldsymbol{b}^{x^2}], \ldots, [\boldsymbol{b}^{x^k}])$ is a nonzero polynomial by the first equation of the previous system and has degree smaller than $\deg(f)$. Let d_0 its degree, then $\boldsymbol{b}^{x^{k+1}} \neq d_0 \mod \ell$ by construction of W and it follows that the leading

monomial of F is nonzero which implies that the polynomial F is nonzero. We also have $\deg(F) \leq \deg(f)$ and hence, by Lemma 1, we obtain:

$$\deg(f) \geq \ell - 1 - \deg(f) - \frac{2s}{(\ell-1)^{n-1}},$$

and the result follows.

Remark 4 The technical condition on x^1 seems necessary since using another x^1, we obtain the polynomial

$$F(X) = f\left(X^2, [\boldsymbol{b}^{x^2}], \ldots, [\boldsymbol{b}^{x^k}]\right) - f^2\left(X, [\boldsymbol{b}^{x^2}] \ldots, [\boldsymbol{b}^{x^k}]\right),$$

and it is unknown how to show that this polynomial is nonzero (without adding new technical conditions on the $\boldsymbol{b}$'s and thus on the $\boldsymbol{a}$'s).

Theorem 2 can be applied to give lower bounds on the degree of interpolating polynomials for several generalized Diffie-Hellman problems (with $k > n$ variables) from [7].

Since the weight of a polynomial is a more discerning complexity estimate, we now prove a lower bound on the weight of an interpolation by a polynomial with k variables and $k > n$ (and without any condition on the input values $x^i \in \{0, \cdots, 2^n - 1\}$ for $i \in \{1, \ldots, k\}$).

Theorem 3 *Let $k > n$ be some integer. Let $S \subseteq (\mathbb{F}_\ell^*)^n$, with $|S| = (\ell-1)^n - s$. Let $x^1, \ldots, x^{k+1} \in \{1, \cdots, 2^n - 1\}$ be pairwise distinct and let $f \in \mathbb{F}_q[X_1, \ldots, X_k]$ be a polynomial satisfying:*

$$f\left([\boldsymbol{a}^{x^1}], \ldots, [\boldsymbol{a}^{x^k}]\right) = [\boldsymbol{a}^{x^{k+1}}], \quad \textit{for all } \boldsymbol{a} = (a_1, \ldots, a_n) \in S,$$

for some different values $x^1, \ldots, x^{k+1} \in \{1, \cdots, 2^n - 1\}$. Then

$$w(f) \geq \left(\frac{\ell - 3 - \frac{s}{(\ell-1)^{n-1}}}{2 + 2k + \frac{s}{(\ell-1)^{n-1}}}\right)^{1/2}.$$

Proof Let $I = \{i \in \{1, \ldots, k\} : x_n^i = 1\}$ that we denote $I = \{i_1, \ldots, i_v\}$ with $i_1 < i_2 < \cdots < i_v$. Let $A = \{\alpha_i = (\alpha_i^1, \ldots, \alpha_i^v) \in \{0, \ldots, \deg(f)\}^v\}$ be a set of cardinality at most $w(f)$ which will be given explicitly later in the proof and W_A be the set of vectors $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$ such that:

1. $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$
2. $\boldsymbol{a}$ satisfies $\alpha_i^1 \boldsymbol{a}^{x^{i_1}-1} + \cdots + \alpha_i^v \boldsymbol{a}^{x^{i_v}-1} \neq \boldsymbol{a}^{x^{k+1}-1}$ for all $\alpha_i \in A$

Claim We have $|W_A| \geq (\ell-1)^n - T_0$, where $T_0 = s + w(f)k(\ell-1)^{n-1}$.

Proof For a fixed tuple $\alpha_i \in A$, by proceeding exactly as in the proof of Claim 1 one can prove by induction in v that the number of $a \in (\mathbb{F}_\ell^*)^n$ such that $\alpha_i^1 \boldsymbol{a}^{x^{i_1}-1} + \cdots + \alpha_i^v \boldsymbol{a}^{x^{i_v}-1} \neq \boldsymbol{a}^{x^{k+1}-1}$ does not exceed $v(\ell-1)^{n-1}$. Since the cardinality of A is at most $w(f)$ and $v \leq k$, we thus have $|W_A| \geq |S| - kw(f)(\ell-1)^{n-1}$.

There exists by the pigeonhole principle $\boldsymbol{b} = (b_1, \ldots, b_{n-1}, 1) \in (\mathbb{F}_\ell^*)^n$ such that

$$T = \{a_n \in \mathbb{F}_\ell \,:\, \boldsymbol{a} = (b_1, \ldots, b_{n-1}, a_n) \in W_A\}$$

satisfies $|T| \geq \ell - 1 - \frac{T_0}{(\ell-1)^{n-1}}$. Then for all $a_n \in T$, we have:

$$f\left([\boldsymbol{b}^{x^1}], \ldots, [\boldsymbol{b}^{x^{i_1-1}}], [\boldsymbol{b}^{x^{i_1}} a_n], [\boldsymbol{b}^{x^{i_1+1}}], \ldots \right.$$
$$\left. \ldots, [\boldsymbol{b}^{x^{i_v-1}}], [\boldsymbol{b}^{x^{i_v}-1} a_n], [\boldsymbol{b}^{x^{i_v+1}}], \ldots, [\boldsymbol{b}^{x^k}]\right) = [\boldsymbol{b}^{x^{k+1}-1} a_n].$$

Let

$$H(X) = f\left([\boldsymbol{b}^{x^1}], \ldots, [\boldsymbol{b}^{x^{i_1-1}}], X^{\boldsymbol{b}^{x^{i_1}-1}}, [\boldsymbol{b}^{x^{i_1+1}}], \ldots \right.$$
$$\left. \ldots, , [\boldsymbol{b}^{x^{i_v-1}}], X^{\boldsymbol{b}^{x^{i_v}-1}}, [\boldsymbol{b}^{x^{i_v+1}}], \ldots, [\boldsymbol{b}^{x^k}]\right) - X^{\boldsymbol{b}^{x^{k+1}-1}}$$

and $K(X)$ the polynomial obtained from $H(X)$ by reducing the exponents of every monomial modulo ℓ. If we choose A to be the set of vectors obtained from the multivariate polynomial f by considering the monomials with variables $X_{i_1}, \ldots, X_{i_v}$ from each monomial of f, then A is of cardinality at most $w(f)$ and does not depend on $\boldsymbol{b}$. One can see that $K(X)$ is a nonzero polynomial by the choice of $\boldsymbol{b}$ and has degree less than ℓ with at least $|T|$ zeros. Hence by Lemma 2, we obtain:

$$w(f) + 1 \geq w(K) \geq \frac{\ell}{1 + \frac{T_0}{(\ell-1)^{n-1}}},$$

and $(w(f)+1)\left(2(\ell-1)^{n-1} + s + w(f)k(\ell-1)^{n-1}\right) \geq (\ell-1)^n$. We thus have:

$$w(f)^2\left(2(\ell-1)^{n-1} + s + 2k(\ell-1)^{n-1}\right) \geq (\ell-1)^n - 2(\ell-1)^{n-1} - s,$$

and the result follows.

Theorem 3 gives a lower bound on the weight of explicit polynomials interpolating the Naor-Reingold pseudo-random function and it immediately gives a lower bound on the weight of explicit polynomials interpolating the n-partite Diffie-Hellman problem by some well chosen inputs:

Corollary 1 *Let $S \subseteq (\mathbb{F}_\ell^*)^n$, with $|S| = (\ell-1)^n - s$.*
Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a polynomial satisfying $f([a_1], \ldots, [a_n]) = [a_1 \ldots a_n]$ for all $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$. We have

$$w(f) \geq \left(\frac{\ell - 3 - \frac{s}{(\ell-1)^{n-1}}}{2 + 2n + \frac{s}{(\ell-1)^{n-1}}}\right)^{1/2}.$$

The next theorem extends the previous approach and gives a lower bound on the weight of implicit polynomials interpolating the generalized Diffie-Hellman problem.

Theorem 4 *Let $S \subseteq (\mathbb{F}_\ell^*)^n$, with $|S| = (\ell-1)^n - s$.*
Let $f \in \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ be a polynomial satisfying:

$$f([a_1], \ldots, [a_n], [a_1 \ldots a_n]) = 0, \quad \textit{for all } \boldsymbol{a} = (a_1, \ldots, a_n) \in S,$$

then

$$w(f) \geq \left(\frac{\ell(\ell-1)^{n-1}}{2(\ell-1)^{n-1} + s} \right)^{1/2}.$$

Proof Let $(\alpha, \beta) \in \{0, \ldots, \deg(f)\}^2\}$ with $(\alpha, \beta) \neq (0, 0)$.
Let $A = \{(\alpha', \beta') \in \{0, \ldots, \deg(f)\}^2\}$ be a set of cardinality at most $w(f)$ with $(\alpha, \beta) \notin A$ and let W_A be the set of vectors $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$ such that:

1. $\boldsymbol{a} = (a_1, \ldots, a_n) \in S$
2. $\boldsymbol{a}$ satisfies $\alpha + \beta(a_2 \ldots a_n) \neq \alpha' + \beta'(a_2 \ldots a_n) \mod \ell$ for all $(\alpha', \beta') \in A$

Claim We have $|W_A| \geq (\ell-1)^n - s - w(f)(\ell-1)^{n-1}$.

Proof Given $(\alpha', \beta') \in A$, the number of $\boldsymbol{a} \in (\mathbb{F}_\ell^*)^n$ such that

$$\alpha + \beta(a_2 \ldots a_n) = \alpha' + \beta'(a_2 \ldots a_n) \bmod \ell$$

does not exceed $(\ell-1)^{n-1}$. Indeed, we have

$$\alpha - \alpha' + (\beta - \beta')(a_2 \ldots a_n) = 0 \mod \ell,$$

and we can easily see that $\beta - \beta' \neq 0 \mod \ell$ (since otherwise, we have $\alpha - \alpha' = 0 \mod \ell$). Therefore, for any vector $(a_1, a_3, \cdots, a_n) \in (\mathbb{F}_\ell^*)^{n-1}$, the value of a_2 is defined uniquely.

Since the total number of couples (α', β') does not exceed $w(f)$, the number of $\boldsymbol{a} \in S$ such that $\boldsymbol{a} \notin W_A$ does not exceed $w(f)(\ell-1)^{n-1}$.

There exists by the pigeonhole principle $\boldsymbol{b} = (b_2, \ldots, b_n) \in (\mathbb{F}_\ell^*)^{n-1}$ such that $T = \{a_1 \in \mathbb{F}_\ell : \boldsymbol{a} = (a_1, \boldsymbol{b}) \in W_A\}$ satisfies $|T| \geq \ell - 1 - w(f) - \frac{s}{(\ell-1)^{n-1}}$. Then for all $a_1 \in T$, we have:

$$f([a_1], [b_2], \ldots [b_n], [a_1 b_2 \ldots b_n]) = 0.$$

Let $H(X) = f(X, [b_2], \ldots [b_n], X^{b_2 \ldots b_n})$ and $K(X)$ the polynomial obtained from $H(X)$ by reducing the exponents of every monomial modulo ℓ. If we choose A independent of $\boldsymbol{b}$ and of cardinality at most $w(f)$, as in the proof of Theorem 3 (but this time with variables X_1 and X_{n+1}) , then $K(X)$ is not a zero polynomial by the choice of $\boldsymbol{b}$ and has degree less than ℓ with at least $|T|$ zeros. Hence by Lemma 2, we obtain:

$$w(f) \geq w(K) \geq \frac{\ell}{1 + w(f) + \frac{s}{(\ell-1)^{n-1}}},$$

and the result follows.

4 Conclusion

In this paper, we proved lower bounds on the degree of multivariate polynomial representations of the Naor-Reingold function in several fixed points for many keys over a finite field. We also proved such bounds on the generalized Diffie-Hellman function over a finite field. It is interesting to extend these results to the group of rational points of an elliptic curve over a finite field. Using techniques from [20], one can extend the results of Theorem 2 to this setting but is unclear how to adapt the techniques from Theorem 1, Theorem 3, and Theorem 4 for elliptic curves. Another natural open problem is to generalize our bounds to a smaller set of keys.

Acknowledgments. The authors are supported in part by the French ANR JCJC ROMAnTIC project (ANR-12-JS02-0004) and by the Simons foundation Pole PRMAIS.

References

1. W. Diffie, M. E. Hellman, New directions in cryptography, IEEE Trans. Information Theory 22 (6) (1976) 644–654.
2. D. Boneh, The decision Diffie-Hellman problem, in: J. Buhler (Ed.), Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings, Vol. 1423 of Lecture Notes in Computer Science, Springer, 1998, pp. 48–63.
3. M. Naor, O. Reingold, Number-theoretic constructions of efficient pseudo-random functions, in: 38th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Miami Beach, Florida, 1997, pp. 458–467.
4. M. Naor, O. Reingold, Number-theoretic constructions of efficient pseudo-random functions, J. ACM 51 (2) (2004) 231–262.
5. A. Joux, A one round protocol for tripartite Diffie-Hellman, Journal of Cryptology 17 (4) (2004) 263–276.
6. A. Escala, G. Herold, E. Kiltz, C. Ràfols, J. L. Villar, An algebraic framework for Diffie-Hellman assumptions, Journal of Cryptology 30 (1) (2017) 242–288.
7. E. Bresson, O. Chevassut, D. Pointcheval, Provably secure authenticated group diffie-hellman key exchange, ACM Trans. Inf. Syst. Secur. 10 (3) (2007) 10.
8. E. E. Mahassni, I. Shparlinski, Polynomial representations of the Diffie-Hellman mapping., Bull. Austral. Math. Soc. 63 (2001) 467–473.
9. A. Winterhof, A note on the interpolation of the Diffie-Hellman mapping., Bull. Austral. Math. Soc.
10. E. Kiltz, A. Winterhof, On the interpolation of bivariate polynomials related to Diffie-Hellman mapping., Bull. Austral. Math. Soc. 69 (2004) 305–315.
11. I. Shparlinski, Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness . , Birkhauser Verlag, Basel, 2003.
12. S. Ling, I. E. Shparlinski, H. Wang, On the multidimensional distribution of the Naor-Reingold pseudo-random function, Math. Comput. 83 (289).
13. I. E. Shparlinski, On the Naor-Reingold pseudo-random function from elliptic curves, Appl. Algebra Eng. Commun. Comput. 11 (1) (2000) 27–34.
14. À. Ibeas, On the period of the Naor-Reingold sequence, Information Processing Letters 108 (5) (2008) 304–307.
15. D. Gómez, J. Gutierrez, A. Ibeas, On the linear complexity of the Naor-Reingold sequence., Inf. Process. Lett. 111 (17) (2011) 854–856.
16. I. E. Shparlinski, Linear complexity of the Naor-Reingold pseudo-random function, Inf. Process. Lett. 76 (3) (2000) 95–99.
17. I. E. Shparlinski, J. H. Silverman, On the linear complexity of the Naor-Reingold pseudo-random function from elliptic curves, Des. Codes Cryptography 24 (3) (2001) 279–289.

18. M. Cruz, D. Gómez, D. Sadornil, On the linear complexity of the Naor-Reingold sequence with elliptic curves., Finite Fields Appl. 16 (5) (2010) 329–333.
19. W. D. Banks, F. Griffin, D. Lieman, I. Shparlinski, Non-linear complexity of the Naor-Reingold pseudo-random function, in: J. Song (Ed.), ICISC 99: 2nd International Conference on Information Security and Cryptology, Vol. 1787 of Lecture Notes in Computer Science, Springer, Heidelberg, Germany, Seoul, Korea, 2000, pp. 53–59.
20. T. Mefenza, D. Vergnaud, Polynomial interpolation of the Naor–Reingold pseudo-random function, Applicable Algebra in Engineering, Communication and Computing 28 (2017) 237–255.
21. D. Coppersmith, I. Shparlinski, On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping, Journal of Cryptology 13 (3) (2000) 339–360.
22. E. Kiltz, A. Winterhof, Polynomial interpolation of cryptographic functions related to Diffie-Hellman and discrete logarithm problem., Discrete Appl. Math. 154 (2) (2006) 326–336.
23. T. Lange, A. Winterhof, Polynomial interpolation of the elliptic curve and XTR discrete logarithm, in: O. H. Ibarra, L. Zhang (Eds.), Computing and Combinatorics, 8th Annual International Conference, COCOON 2002, Singapore, August 15-17, 2002, Proceedings, Vol. 2387 of Lecture Notes in Computer Science, Springer, 2002, pp. 137–143.
24. T. Lange, A. Winterhof, Interpolation of the discrete logarithm in $\mathbb{F}_q$ by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$., Discrete Appl. Math. 128 (1) (2003) 193–206.
25. G. C. Meletiou, A. Winterhof, Interpolation of the double discrete logarithm, in: J. von zur Gathen, J. L. Imaña, Ç. K. Koç (Eds.), Arithmetic of Finite Fields, 2nd International Workshop, WAIFI 2008, Siena, Italy, July 6-9, 2008, Proceedings, Vol. 5130 of Lecture Notes in Computer Science, Springer, 2008, pp. 1–10.