Distribution and Polynomial Interpolation of the Dodis-Yampolskiy Pseudo-Random Function

Thierry Mefenza, Damien Vergnaud

Distribution and Polynomial Interpolation of the Dodis-Yampolskiy Pseudo-Random Function

Thierry Mefenza[1,2] and Damien Vergnaud[1]

[1] ENS, CNRS, INRIA, and PSL, Paris, France
[2] Department of Mathematics, University of Yaounde 1, Cameroon

Abstract. We give some theoretical support to the security of the cryptographic pseudo-random function proposed by Dodis and Yampolskiy in 2005. We study the distribution of the function values over general finite fields and over elliptic curves defined over prime finite fields. We also prove lower bounds on the degree of polynomials interpolating the values of these functions in these two settings.

Keywords. Dodis-Yampolskiy pseudo-random function, discrepancy, polynomial interpolation, finite fields, elliptic curves.

1 Introduction

A cryptographic pseudo-random function family is 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 (*i.e.* whose outputs are sampled uniformly and independently at random). In 2005, Dodis and Yampolskiy [DY05] proposed an efficient pseudo-random function family which takes inputs in $\{1, \ldots, d\}$ (for some parameter $d \in \mathbb{N}$) and outputs an element in a group $\mathbb{G}$ (multiplicatively written) of prime order t with generator g. The secret key is a scalar $x \in \mathbb{Z}_t^*$ and the pseudo-random function is defined by:

$$\begin{aligned} V_x : \{1, \ldots, d\} &\longrightarrow \mathbb{G} \\ m &\longmapsto V_x(m) = g^{\frac{1}{x+m}} \quad \text{if } x + m \neq 0 \bmod t \text{ and } 1_{\mathbb{G}} \text{ otherwise.} \end{aligned}$$

The Dodis-Yampolskiy pseudo-random function family has found numerous applications in cryptography (e.g., for compact e-cash [CHL05] or anonymous authentication [CHK+06]). Dodis and Yampolskiy showed that their construction has some very attractive security properties, provided that some assumption about the hardness of breaking the so-called *Decision Diffie-Hellman Inversion* problem holds in $\mathbb{G}$ [DY05]. This assumption is non-standard and Cheon [Che10] proved that it is stronger than the classical discrete logarithm assumption in $\mathbb{G}$.

In practice, two interesting choices for the group $\mathbb{G}$ are a subgroup of the multiplicative group of any finite field (in particular, for the so-called *verifiable* Dodis-Yampolskiy pseudo-random function in groups equipped with a bilinear

map [DY05]) or a subgroup of points of an elliptic curve defined over a prime finite field. Very few results supporting the Decision Diffie-Hellman Inversion assumption hardness were proven in these settings (contrary to the Naor-Reingold pseudo-random function family [NR04] for which numerous results are known, e.g. distribution [LSW14], linear complexity [GGI11] and non-linear complexity [BGLS00]). This paper deals with the distribution of the Dodis-Yampolskiy pseudo-random function over finite fields and over elliptic curves and proves lower bounds on the degree of polynomials which interpolate these functions.

Contributions of the paper. As a first contribution, we prove that for almost all values of parameters, the Dodis-Yampolskiy pseudo-random function produces a uniformly distributed sequence. This simple result is based on some recent bounds on character sums with exponential functions. Shparlinski [Shp11] has obtained in 2011 an explicit bound for exponential sums with consecutive modular roots over a prime finite field. Ostafe and Shparlinski [OS11] obtained an analoguous result for exponential sums over multiples of a point on an elliptic curve defined over a prime finite field. Following the method from [Shp11], we obtain readily a bound for such sums over any extension of a prime finite field (Proposition 1). This new bound allows us to give results on the distribution of the Dodis-Yampolskiy pseudo-random functions over finite fields (Theorem 1). We use the bounds from [OS11] to give results on the distribution of the Dodis-Yampolskiy pseudo-random functions over elliptic curves (Theorem 2).

In order to break the security of the Dodis-Yampolskiy pseudo-random function, it would be sufficient to have a polynomial over a finite field of low degree which reveals information on the function values. From the known lower bounds on the polynomial interpolation on the discrete logarithm in finite fields and elliptic curves (*e.g.* [CS00,LW02,KW06])), one can prove that a low-degree univariate polynomial cannot reveal the secret key x when evaluated at $V_x(m)$ (for some integer $m \in \{1, \ldots, d\}$) for all x. However, the security of the Dodis-Yampolskiy pseudo-random function would also be broken if such low-degree polynomial revealing a value $V_x(m')$ were proved to exist (for some integer $m' \in \{1, \ldots, d\} \setminus \{m\}$ and many different keys x). Our main contribution is to prove lower bounds on the degree of polynomials interpolating the values of these functions over finite fields (Theorem 3) and elliptic curves (Theorem 4 and Theorem 5). These results can be regarded as first complexity lower bounds on the pseudo-randomness of the Dodis-Yampolskiy function families.

Both contributions are motivated by earlier results of the same flavour on the Naor-Reingold pseudo-random function family.

2 Auxiliary Results

In this section, we collect some statements about finite fields, exponential sums over finite fields and elliptic curves. We provide explicit upper-bounds for exponential sums with consecutive modular roots over a finite field and for analogous exponential sums over elliptic curves [Shp11,OS11]. The bound for exponential

sums with consecutive modular roots over a general finite field is easily derived from [Shp11] and may be of independent interest.

2.1 Finite Fields and Exponential Sums

Let p be an odd prime number. We denote $\mathbb{F}_q = \mathbb{F}_{p^r}$ the finite field with $q = p^r$ elements ($r \geq 1$). For an integer t, denote by $\mathbb{Z}_t$ the residue ring modulo t and by $\mathbb{Z}_t^*$ the group of units of $\mathbb{Z}_t$. For an integer $m > 0$, we put $e_m(z) = \exp(2\pi iz/m)$. Let $g \in \mathbb{F}_{p^r}^*$ of order t (with $t \mid p^r - 1$), and ψ be a non-trivial character of $\mathbb{F}_{p^r}$. For $a \in \mathbb{F}_{p^r}^*$ and $b \in \mathbb{Z}_t$, we define the sum:

$$S_{a,b} = \sum_{n \in \mathbb{Z}_t^*} \psi(ag^{1/n}) e_t(bn).$$

Throughout the paper, the notation $U \ll V$ is equivalent to the inequality $|U| \leq cV$ with some constant $c > 0$. In the following lemmas, the implied constants in the symbols "$\ll$" may occasionally depend on the integer parameters k, ℓ and are absolute otherwise.

In [BS08] Bourgain and Shparlinski proved, when $r = 1$, that for any $\varepsilon > 0$, there exists $\delta > 0$ such that for $t \geq p^{\varepsilon}$, we have the bound $S_{a,b} \ll t^{1-\delta}$. Shparlinski [Shp11](Theorem 3.1) gave an explicit form of this result (again when $r = 1$) for relatively large values of t; in the case $t = p^{1+o(1)}$, it takes the form $S_{a,b} \ll t^{127/128+o(1)}$. Using Shparlinski's methods, we generalize this bound on $S_{a,b}$ for any $r \geq 1$ (see Appendix A for a proof which follows [Shp11]):

Proposition 1. *For any integers $k \geq 2$, $\ell \geq 1$ we have for $t \geq q^{1/2}(\log q)^2$:*

$$S_{a,b} \leq t^{1-\alpha_{k,\ell}} q^{\beta_{k,\ell}+o(1)},$$

where $\alpha_{k,\ell} = \frac{1}{2(2k+\ell)} - \frac{1}{4k\ell}$ *and* $\beta_{k,\ell} = \frac{1}{4(2k+\ell)}$.

2.2 Elliptic Curves and Exponential Sums

We will also consider the setting of an elliptic curve E defined over $\mathbb{F}_p$ (where p is a prime number), that is a rational curve given by the following Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_p$ and $4A^3 + 27B^2 \neq 0$. The set $E(\mathbb{F}_p)$ of the points of the curve defined over $\mathbb{F}_p$ (including the special point O at infinity) has a group structure (denoted additively) with an appropriate composition rule where O is the neutral element. Given P a point of the curve E with prime order ℓ (with $\ell \mid |E(\mathbb{F}_p)|$), we denote $[n]P$ the scalar multiplication, i.e. in fact the adding of the point P to itself n times (for $n \geq 0$).

Let E be an elliptic curve and $G \in E(\mathbb{F}_p)$ be a point of order $t \geq 1$. For $a \in \mathbb{F}_p^*$ and $b \in \mathbb{Z}_t$, we define the sum:

$$\hat{S}_{a,b} = \sum_{n \in \mathbb{Z}_t^*} e_p\left(aX\left(\left[\frac{1}{n}\right]G\right)\right) e_t(bn),$$

where $X(P)$ denotes the abscissa of a point $P \in E(\mathbb{F}_p)$.

In [OS11, Theorem 6], Ostafe and Shparlinski obtained an upper-bound on $\hat{S}_{a,b}$ (with $H(X) = X^{-1}$ following the notation from [OS11]):

Proposition 2 ([OS11],). *For any integers $k \geq 2$, $\ell \geq 1$ we have for $t \geq q^{1/2}(\log q)^2$:*

$$\hat{S}_{a,b} \leq t^{1-\alpha_{k,\ell}} p^{\beta_{k,\ell}+o(1)},$$

where $\alpha_{k,\ell} = \frac{1}{2(4k+\ell)} - \frac{1}{4k\ell}$ and $\beta_{k,\ell} = \frac{1}{4(4k+\ell)}$.

2.3 Division Polynomials over Elliptic Curves

In this section, we recall some basic facts on division polynomials of elliptic curves (see [Was08,BSS99]). The *division polynomials* $\psi_m(X,Y) \in \mathbb{F}_p[X,Y]/(Y^2 - X^3 - AX - B)$, $m \geq 0$, are recursively defined by:

$$\begin{aligned}
\psi_0 &= 0\\
\psi_1 &= 1\\
\psi_2 &= 2Y\\
\psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2\\
\psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3)\\
\psi_{2m+1} &= \psi_m + 2\psi_m^3 - \psi_{m-1}\psi_{m+1}^3\,, \quad m \geq 2\\
\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/\psi_2\,, \quad m \geq 3,
\end{aligned}$$

where ψ_m is an abbreviation for $\psi_m(X,Y)$. If m is odd, then $\psi_m(X,Y) \in \mathbb{F}_p[X]$ is univariate and if m is even then $\psi_m(X,Y) \in 2Y\mathbb{F}_p[X]$. Therefore, we have $\psi_m^2(X,Y) \in \mathbb{F}_p[X]$ and $\psi_{m-1}(X,Y)\psi_{m+1}(X,Y) \in \mathbb{F}_p[X]$. In particular, we may write $\psi_{2m+1}(X)$ and $\psi_m^2(X)$.

The division polynomials can be used to calculate multiples of a point on the elliptic curve E. Let $P = (x,y) \in E$ with $P \neq O$, then the abscissa of $[m]P$ is given by $\theta_m(x)/\psi_m^2(x)$ where $\theta_m(X) = X\psi_m^2 - \psi_{m-1}\psi_{m+1}$. The zeros of the denominator $\psi_m^2(X)$ are exactly the first coordinates of the non-trivial m-torsion points, i.e, the points $Q = (x,y) \in \overline{\mathbb{F}_p}^2 \setminus \{O\}$ on E with $[m]Q = O$. Note, that these points occur in pairs $Q = (x,y)$ and $-Q = (x,-y)$, which coincide only if $2Q = O$, i.e, if x is a zero of $\psi_2^2(X)$.

We recall that the group of m-torsion points $E[m]$, for an elliptic curve E defined over a field of characteristic p, is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$ if $p \nmid m$ and to a proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^2$ if $p \mid m$. If m is a power of p then $E[m]$ is either isomorphic to $(\mathbb{Z}/m\mathbb{Z})$ or to $\{O\}$. Accordingly, the degree of $\psi_m^2(X)$ is $m^2 - 1$ if $p \nmid m$ and strictly less than $m^2 - 1$ otherwise. In particular, for $p = 2$ and m a power of 2 we have $\deg(\psi_m^2) = m - 1$ if E is not supersingular and $\deg(\psi_m^2) = 0$ otherwise. By induction one can show that $\theta_m(X) \in \mathbb{F}_p[X]$ is monic of degree m^2.

3 Distribution of the Dodis-Yampolskiy Pseudo-Random Functions

For a real z, we use the notation $e(z) = exp(2\pi iz)$. For a sequence of N points $\Gamma = (\gamma_{0,n}, \ldots, \gamma_{s-1,n})_{n\in\{1,\ldots,N\}}$ in the s-dimensional unit cube, we denote its *discrepancy* by D_Γ:

$$D_\Gamma = \sup_{B\subseteq[0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ denotes the number of points of the sequence Γ in a box B (i.e. a polyhedron $[\alpha_0, \beta_0)\times\cdots\times[\alpha_{s-1}, \beta_{s-1}) \subseteq [0,1)^s$) of volume $|B|$ and the supremum is taken over all such boxes. For an integer vector $a = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$, we define $|a| = max_{\nu\in\{0,\ldots,s-1\}}|a_\nu|$ and $r(a) = \prod_{\nu=0}^{s-1} \max\{|a_\nu|, 1\}$.

In order to show that a sequence Γ is uniformly distributed, we need to show that its discrepancy D_Γ is very small (i.e. tends to 0). The following lemma is our main tool for finding non-trivial upper bound for the discrepancy. It is a slightly weaker form of the Koksma-Szüsz inequality [DT97, Theorem 1.21]. The implied constant in the symbol "$\ll$" depends on the integer s.

Lemma 1. *For any integer $L > 1$ and any sequence Γ of N points, we have*

$$D_\Gamma \ll \frac{1}{L} + \frac{1}{N} \sum_{0<|a|<L} \frac{1}{r(a)} \left| \sum_{n=1}^{N} e\left(\sum_{\nu=0}^{s-1} a_\nu \gamma_{\nu,n} \right) \right|,$$

where the sum is taken over all integer vectors $a \in \mathbb{Z}^s$ with $0 < |a| < L$.

We also need the well-known orthogonality relation:

$$\sum_{\eta=0}^{m-1} e_m(\eta\lambda) = \begin{cases} 0 & \text{if } \lambda \neq 0 \bmod m \\ m & \text{otherwise} \end{cases} \tag{1}$$

and the inequality [[IK04], Bound (8.6)] (which holds for any integers m and M with $1 \le M \le m$):

$$\sum_{\eta=0}^{m-1} \left| \sum_{\lambda=1}^{M} e_m(\eta\lambda) \right| \ll m \log\, m. \tag{2}$$

3.1 Distribution of the Dodis-Yampolskiy Pseudo-Random Function over Finite Fields

Let $q = p^r$ be a prime power for some integer $r > 1$, let $g \in \mathbb{F}_q^*$ be an element of prime order t. For $x \in \mathbb{Z}_t$ and $d \le t$, we denote by $D_x(d)$ the discrepancy of the points $(V_{x,1}(n)/p, \ldots, V_{x,r}(n)/p)$ for $1 \le n \le d$, where $V_x(n) = g^{\frac{1}{x+n}} \in \mathbb{F}_{p^r}$ and $V_x(n) = V_{x,1}(n)\beta_1 + \cdots + V_{x,r}(n)\beta_r$, where $\{\beta_1, \ldots, \beta_r\}$ is an ordered basis of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$. We identify $\mathbb{F}_p$ with the set of integers $\{0, 1, \ldots, p-1\}$.

Theorem 1. *For any $x \in \mathbb{Z}_t$, any integers $k \geq 2$, $\ell \geq 1$ and $1 \leq d \leq t$, we have:*

$$D_x(d) \leq \frac{t^{1-\alpha_{k,l}} q^{\beta_{k,l}+o(1)}}{d},$$

where $\alpha_{k,l} = \frac{1}{2(2k+l)} - \frac{1}{4kl}$ *and* $\beta_{k,l} = \frac{1}{4(2k+l)}$.

Proof. From Lemma 1, we derive

$$D_x(d) \ll \frac{1}{p} + \frac{1}{d} \sum_{0<|a|<p} \frac{1}{r(a)} \left| \sum_{n=1}^{d} e_p \left(\sum_{j=1}^{r} a_j V_{x,j}(n) \right) \right|,$$

where $a = (a_1, \ldots, a_r)$. Set

$$S_d(a) = \sum_{n=1}^{d} e_p(\sum_{j=1}^{r} a_j V_{x,j}(n)).$$

Let $\{\delta_1, \ldots, \delta_r\}$ be the dual basis of the given ordered basis $\{\beta_1, \ldots, \beta_r\}$. For $j \in \{1, \ldots, r\}$ and $n \in \{1, \ldots, d\}$, we have $V_{x,j}(n) = \mathrm{Tr}(\delta_j V_x(n))$, where Tr denotes the trace of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$ (namely $\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}}$). Therefore,

$$S_d(a) = \sum_{n=1}^{d} e_p \left(\mathrm{Tr} \left(\sum_{j=1}^{r} a_j \delta_j V_x(n) \right) \right) = \sum_{n=1}^{d} e_p(\mathrm{Tr}(\alpha_a V_x(n)))$$

where $\alpha_a = \sum_{j=1}^{r} a_j \delta_j \in \mathbb{F}_{p^r}$.
Let χ be defined by $\chi(z) = e_p(\mathrm{Tr}(z))$. Then χ is a non trivial additive character on $\mathbb{F}_{p^r}$. Since there exists $j \in \{1, \ldots, r\}$ such that $a_j \neq 0$, then $\alpha_a \neq 0$. We have:

$$S_d(a) = \sum_{n=1}^{d} \chi(\alpha_a V_x(n)) \text{ with } \alpha_a \neq 0.$$

We have

$$\begin{aligned} S_d(a) = \sum_{\substack{n=x+1 \\ n \in \mathbb{Z}_t^*}}^{x+d} \chi(\alpha_a g^{1/n}) &= \frac{1}{t} \sum_{n \in \mathbb{Z}_t^*} \chi(\alpha_a g^{1/n}) \times \sum_{c=0}^{t-1} \sum_{\substack{v=x+1 \\ v \in \mathbb{Z}_t^*}}^{x+d} e_t(c(n-v)) \\ &= \frac{1}{t} \sum_{c=0}^{t-1} \left(\sum_{n \in \mathbb{Z}_t^*} \chi\left(\alpha_a g^{1/n}\right) e_t(cn) \right) \times \sum_{\substack{v=x+1 \\ v \in \mathbb{Z}_t^*}}^{x+d} e_t(-cv). \end{aligned}$$

By applying Proposition 1 and (2), we obtain

$$S_d(a) \leq \frac{1}{t} \sum_{c=0}^{t-1} \left| \sum_{\substack{v=x+1 \\ v \in \mathbb{Z}_t^*}}^{x+d} e_t(-cv) \right| \times t^{1-\alpha_{k,\ell}} q^{\beta_{k,\ell}+o(1)} \leq t^{1-\alpha_{k,\ell}} q^{\beta_{k,\ell}+o(1)}.$$

By applying this bound to $D_x(d)$, we have

$$D_x(d) \ll \frac{1}{p} + \frac{t^{1-\alpha_{k,l}} q^{\beta_{k,\ell}+o(1)}}{d} \sum_{0<|a|<p} \frac{1}{r(a)} \ll \frac{1}{p} + \frac{t^{1-\alpha_{k,\ell}} q^{\beta_{k,\ell}+o(1)}}{d} \log^r p$$
$$\leq \frac{t^{1-\alpha_{k,\ell}} q^{\beta_{k,\ell}+o(1)}}{d}$$

□

With the choice $k = 4$, $l = 8$, $t = q^{1+o(1)}$ and $d = t^{\frac{127}{128}+\varepsilon}$, we obtain

$$D_x(d) \leq p^{r(-\varepsilon+o(1))} = q^{-\varepsilon+o(1)}.$$

3.2 Distribution of the Dodis-Yampolskiy Pseudo-Random Function over Elliptic Curves

Let $E : y^2 = x^3 + Ax + B$, be an elliptic curve over $\mathbb{F}_p$. For $P \in E(\mathbb{F}_p)$ of prime order t, for $x \in \mathbb{Z}_t$, and for $1 \leq d \leq t$ we denote by $D_x(d)$ the discrepancy of the points $(X(V_x(n))/p)$ for $n \in \{1, \ldots, d\}$ where $V_x(n) = \left[\frac{1}{x+n}\right] P \in E(\mathbb{F}_p)$. We obtain the following theorem.

Theorem 2. *For any $x \in \mathbb{Z}_t$, any integers $k \geq 2$, $l \geq 1$ and $1 \leq d \leq t$, we have:*

$$D_x(d) \leq \frac{t^{1-\alpha_{k,\ell}} p^{\beta_{k,\ell}+o(1)}}{d},$$

where $\alpha_{k,\ell} = \frac{1}{2(4k+\ell)} - \frac{1}{4k\ell}$ *and* $\beta_{k,\ell} = \frac{1}{4(4k+\ell)}$.

Proof. From Lemma 1, we derive

$$D_x(d) \ll \frac{1}{p} + \frac{1}{d} \sum_{0<|a|<p} \frac{1}{|a|} \left| \sum_{n=1}^{d} e_p\left(aX(W_x(n))\right) \right|,$$

where a is an integer. Set $S_d(a) = \sum_{n=1}^{d} e_p(aX(W_x(n)))$, we have

$$\begin{aligned} S_d(a) &= \sum_{\substack{n=x+1 \\ n\in\mathbb{Z}_t^*}}^{x+d} e_p\left(aX\left(\left[\frac{1}{n}\right] P\right)\right) \\ &= \frac{1}{t} \sum_{n\in\mathbb{Z}_t^*} e_p\left(aX\left(\left[\frac{1}{n}\right] P\right)\right) \times \sum_{c=0}^{t-1} \sum_{\substack{v=x+1 \\ v\in\mathbb{Z}_t^*}}^{x+d} e_t\left(c(n-v)\right) \\ &= \frac{1}{t} \sum_{c=0}^{t-1} \left(\sum_{n\in\mathbb{Z}_t^*} e_p\left(aX\left(\left[\frac{1}{n}\right] P\right)\right) e_t(cn) \right) \times \sum_{\substack{v=x+1 \\ v\in\mathbb{Z}_t^*}}^{x+d} e_t(-cv) \end{aligned}$$

By applying Lemma 6 and (3), we obtain

$$\begin{aligned} S_d(a) &\leq \frac{1}{t}\sum_{c=0}^{t-1}\left|\sum_{\substack{v=x+1\\ v\in\mathbb{Z}_t^*}}^{x+d} e_t(-cv)\right| \times t^{1-\alpha_{k,\ell}}p^{\beta_{k,\ell}+o(1)} \\ &\leq t^{1-\alpha_{k,\ell}}p^{\beta_{k,\ell}+o(1)} \end{aligned}$$

By applying this bound to $D_x(d)$, we have

$$\begin{aligned} D_x(d) &\ll \frac{1}{p} + t^{1-\alpha_{k,\ell}}p^{\beta_{k,\ell}+o(1)} \times \frac{1}{d}\sum_{0<|a|<p}\frac{1}{|a|} \\ &\ll \frac{1}{p} + t^{1-\alpha_{k,\ell}}p^{\beta_{k,l}+o(1)} \times \frac{1}{d}\log p \\ &\leq t^{1-\alpha_{k,\ell}}p^{\beta_{k,\ell}+o(1)} \times \frac{1}{d} \end{aligned}$$

□

With the choice $k = 4$, $\ell = 16$, $t = p^{1+o(1)}$ and $d = t^{\frac{255}{256}+\varepsilon}$, we obtain $D_x(d) \ll p^{-\varepsilon+o(1)}$.

4 Polynomial Interpolation of the Dodis-Yampolskiy Pseudo-Random Function over Finite Fields

Let $g \in \mathbb{F}_{p^r}^*$ for some integer $r > 1$, be an element of prime order $t \mid p^r - 1$. In this section, we prove a lower bound on the degree of univariate polynomial interpolation of the Dodis-Yampolskiy pseudo-random function over finite fields. We consider polynomials that interpolates values of the Dodis-Yampolskiy pseudo-random function for a fixed secret key $x \in \mathbb{F}_t^*$. The values considered are evaluation of the function at integers $n \in \{1, \ldots, d\}$ for some integer $1 \leq d \leq t$ and translates of these values by some fixed constants $\lambda \in \mathbb{N}$. This setting is interesting for applications in cryptography [CHL05,CHK+06]. Note that if one value n is larger than d then, the Dodis-Yampolskiy function is not necessarily defined at $n + \lambda$. In the following, we consider simple sets where all translates belong to the function domain but our method can be adapted to other settings.

Theorem 3. *Let λ be a fixed integer and let $A \subseteq \{1, \ldots, d\}$. For some $x \in \mathbb{F}_t^*$, let $F(X) \in \mathbb{F}_p[X]$ be such that $F(g^{\frac{1}{x+n}}) = g^{\frac{1}{x+n+\lambda}}$ for all $n \in A$. We have*

$$\deg(F) \geq \frac{t-2s}{4} \quad \textit{and} \quad w(F) \geq \left(\frac{t}{4s}\right)^{1/2} \quad \textit{where } \sharp A = t - s.$$

In the proof of Theorem 3, we use the following lemma [LW02] where the *weight* $w(F)$ (or sparsity) of a polynomial $F(X) \in \mathbb{F}_p[X]$ is the number of its non-zero coefficients.

Lemma 2 ([LW02]). *Let $\gamma \in \mathbb{F}_p$ be an element of order ℓ and $F(X) \in \mathbb{F}_p[X]$ be a non-zero polynomial of degree at most $\ell - 1$ with at least b zeros of the form γ^x with $0 \leq x \leq \ell - 1$. The weight of $F(X)$ satisfies $w(F) \geq \ell/(\ell - b)$.*

Proof (Theorem 3). Let $R = \{(n + x) \bmod t \ : n \in A\}$. Then $R \subseteq \mathbb{F}_t$ and $\sharp R = t - s$. We have $F(g^{\frac{1}{n}}) = g^{\frac{1}{n+\lambda}}$ for all $n \in R$. Noticing that $\frac{1}{n+\lambda} = \frac{1}{\lambda}(1 - \frac{1}{\frac{\lambda}{n}+1})$, we obtain $F(g^{\frac{u}{\lambda}}) = g^{\frac{1}{\lambda}(1-\frac{1}{u+1})}$ for all $u = \frac{\lambda}{n}$, $n \in R$.

Let $R_0 = \{u = \frac{\lambda}{n} : n \in R \setminus \{0\}\}$ and $T = \{u \in R_0 : 2u + 1 \in R_0\}$. Since $\sharp R_0 = t - s$, we have $\sharp T \geq t - 2s$. Then

$$F\left(g^{\frac{2u+1}{\lambda}}\right) = g^{\frac{1}{\lambda}(1-\frac{1}{2u+2})} = g^{\frac{1}{\lambda}(\frac{1}{2}+\frac{1}{2}(1-\frac{1}{u+1}))} = g^{\frac{1}{2\lambda}} \times g^{\frac{1}{2\lambda}(1-\frac{1}{u+1})}$$

for all $u \in T$. We thus have

$$F^2\left(g^{\frac{2u+1}{\lambda}}\right) = g^{\frac{1}{\lambda}} \times g^{\frac{1}{\lambda}(1-\frac{1}{u+1})} = g^{\frac{1}{\lambda}} \times F(g^{\frac{u}{\lambda}}), \quad \text{for all } u \in T.$$

Let $H(X) = F^2(g^{\frac{1}{\lambda}}X^2) - g^{\frac{1}{\lambda}}F(X)$. The polynomial $H(X)$ is a non-zero polynomial and $\deg(H) \leq 4\deg(F)$. Since $H(X)$ has at least $\sharp T = t - 2s$ zeros, we have $4\deg(F) \geq t - 2s$ and then $\deg(F) \geq \frac{t-2s}{4}$. Moreover, if $\deg(H) \leq t - 1$, since the zeros of H are the powers of $g^{\frac{1}{\lambda}}$, then we have by Lemma 2, $w(H) \geq t/(t - (t - 2s))$, and since $w(H) \leq 2(w(F))^2$, it follows that $w(F) \geq (t/4s)^{1/2}$. □

Remark 1. Theorem 3 is non-trivial only when $\sharp A > t/2$. It remains an open question to obtain non-trivial lowers bounds for smaller sets A.

5 Polynomial Interpolation of the Dodis-Yampolskiy Pseudo-Random Function over Elliptic Curves

In this section, p is an odd prime number, E is an elliptic curve defined over $\mathbb{F}_p$ and P is a point of the curve $E(\mathbb{F}_p)$ with prime order t. We prove lower bounds on the degree of polynomial interpolation of the Dodis-Yampolskiy pseudo-random function over elliptic curves defined by $V_x(n) = X\left(\left[\frac{1}{x+n}\right]P\right)$ for a secret key $x \in \mathbb{F}_t^*$ and an integer $n \in \{1, \ldots, d\}$, with $1 \leq d \leq t$.

Theorem 4. *Let $S \subseteq \{1, \ldots, d\}$, $\sharp S = t - s$. We suppose $X(P) \neq 0$. For some $x \in \mathbb{F}_t^*$, let $F(X) \in \mathbb{F}_p[X]$ be such that $\psi_2^2(F(X(P))) \neq 0$ and $F(V_x(n)) = V_x(n + 1)$ for all $n \in S$. We have*

$$\deg(F) \geq \frac{t - 2s}{176}.$$

Proof. Let $R = \{(n + x) \bmod t \ : n \in S\} \subseteq \mathbb{F}_t$. We have $\sharp R = t - s$. Let us denote $x_k = X([k]P)$ and $R_0 = \{\frac{1}{n} : n \in R\}$, then we have $F(x_u) = x_{1-\frac{1}{1+u}}$ for

all $u \in R_0$. We consider the set $T = \{u \in R_0 : 2u+1 \in R_0\}$, then $\sharp T \geq t - 2s$. For all $u \in T$, we have:

$$F(x_{2u+1}) = x_{1-\frac{1}{2(u+1)}} = x_{1/2+1/2(1-1/(u+1))} \quad \text{and} \quad F(x_u) = x_{1-1/(u+1)} \tag{3}$$

Using division polynomials (see Section 2.3), we can write:

$$x_{1+1-\frac{1}{(u+1)}} = \frac{\theta_2(F(x_{2u+1}))}{\psi_2^2(F(x_{2u+1}))} \tag{4}$$

Using the elliptic curve addition law, we have

$$x_{1+\alpha} = \frac{a(x_\alpha) - 2y_1 y_\alpha}{(x_\alpha - x_1)^2} \text{ where } a(X) = x_1 X^2 + (x_1^2 + A)X + Ax_1 + 2B,$$

and for any polynomial G of degree $m \geq 1$, we have

$$G(x_{1+\alpha}) = \frac{u(x_\alpha) - y_\alpha v(x_\alpha)}{(x_\alpha - x_1)^{2m}} \text{ and } lc(u) = G(x_1)$$

with uniquely determined polynomials $u(X)$ and $v(X)$ with $\deg(u) \leq 2m$ ($\deg(u) = 2m$ if $G(x_1) \neq 0$) and $\deg(v) \leq 2m-2$ and where $lc(u)$ is the leading coefficient of the polynomial $u(X)$. Since $F(x_u) = x_{1-\frac{1}{u+1}}$, we can rewrite (4) as:

$$\frac{a(F(x_u)) - y_1 y_{1-\frac{1}{u+1}}}{(F(x_u) - x_1)^2} = \frac{\theta_2(F(x_{2u+1}))}{\psi_2^2(F(x_{2u+1}))}.$$

Since the point $(x_{1-\frac{1}{u+1}}, y_{1-\frac{1}{u+1}}) \in E(\mathbb{F}_p)$ and $F(x_u) = x_{1-\frac{1}{u+1}}$, the polynomial $y_1^2(F(x_u)^3 + A \cdot F(x_u) + B)\psi_2^4(F(x_{2u+1}))$ is equal to the polynomial $[(F(x_u) - x_1)^2\theta_2(F(x_{2u+1})) - a(F(x_u))\psi_2^2(F(x_{2u+1}))]^2$. We thus obtain

$$y_1^2(F(x_u)^3 + A \cdot F(x_u) + B) \times \frac{p_1(x_{2u}) - y_{2u}p_2(x_{2u})}{(x_{2u} - x_1)^{12d_0}} = Q(x_u, x_{2u}, y_{2u}),$$

where $d_0 = \deg(F)$ and $Q(x_u, x_{2u}, y_{2u})$ denotes a polynomial of the form

$$\left[(F(x_u) - x_1)^2 \frac{p_3(x_{2u}) - y_{2u}p_4(x_{2u})}{(x_{2u} - x_1)^{8d_0}} - a(F(x_u)) \frac{p_5(x_{2u}) - y_{2u}p_6(x_{2u})}{(x_{2u} - x_1)^{6d_0}}\right]^2$$

such that $\deg(p_1) \leq 6d_0$, $\deg(p_2) \leq 6d_0 - 2$, $\deg(p_3) \leq 4d_0$, $\deg(p_4) \leq 4d_0 - 2$, $\deg(p_5) \leq 3d_0$ and $\deg(p_6) \leq 3d_0 - 2$. We obtain:

$$y_1^2(F(x_u)^3 + AF(x_u) + B)(x_{2u} - x_1)^{4d_0}(p_1(x_{2u}) - y_{2u}p_2(x_{2u})) = P(x_u, x_{2u}, y_{2u}),$$

where $P(x_u, x_{2u}, y_{2u}) = [(F(x_u) - x_1)^2 p_3(x_{2u}) - a(F(x_u))(x_{2u} - x_1)^{2d_0} p_5(x_{2u})$ $- y_{2u}((F(x_u) - x_1)^2 p_4(x_{2u}) - a(F(x_u))(x_{2u} - x_1)^{2d_0} p_6(x_{2u}))]^2$.

We then proceed as previously by trying to eliminate y_{2u}. We obtain an expression in function of x_u and x_{2u} and we replace x_{2u} by $\frac{\theta_2(x_u)}{\psi_2^2(x_u)}$. We finally obtain a rational function in x_u of the form:

$$\frac{Q(x_u)}{\psi_2^{40d_0}(x_u)} = 0, \text{ where } Q(X) \in \mathbb{F}_p[X] \text{ and } \deg(Q) \leq 88d_0.$$

Claim. $Q(X) \neq 0$ if $\psi_2^2(F(x_1)) \neq 0$ and $x_1 \neq 0$

Proof (Claim). We have $\deg(P_5) = 3d_0$ iff $\psi_2^2(F(x_1)) \neq 0$. If $\deg(P_5) = 3d_0$, One can then verify that the leading coefficient of Q is the leading coefficient of the numerator of the rational function obtained from $[(F(x_u) - x_1)^2 p_3(x_{2u}) - a(F(x_u))(x_{2u} - x_1)^{2d_0} p_5(x_{2u})]^4$ after replacing x_{2u} by $\frac{\theta_2(x_u)}{\psi_2^2(x_u)}$.

Therefore, if $\deg(P_5) = 3d_0$, then the leading coefficient of Q is $(f^2 \times x_1 \times \psi_2^2(F(x_1)))^4$ which is non zero if $x_1 \neq 0$ since $\deg(P_5) = 3d_0$ iff $\psi_2^2(F(x_1)) \neq 0$, where f is the leading coefficient of F. Then if $\psi_2^2(F(x_1)) \neq 0$ and $x_1 \neq 0$, $Q(X)$ is a non-zero polynomial. □

If $\psi_2^2(F(x_1)) \neq 0$ and $x_1 \neq 0$, $Q(X)$ is a non-zero polynomial with at least $\sharp T/2$ different zeros. We thus have $88d_0 \geq (t - 2s)/2$ and the claimed result. □

The condition $X(P) \neq 0$ in the statement of Theorem 4 holds obviously for almost all point P. The lower bound then holds if the group order $\sharp E(\mathbb{F}_p)$ is odd since in this case, the technical condition $\psi_2^2(F(X(P))) \neq 0$ is always satisfied. However, we obtain a weaker lower bound for the polynomial degree which holds for every curve E.

Theorem 5. *Let $1 \leq d \leq t$ be a fixed integer and let $A \subseteq \{1, \ldots, d\}$, $\sharp A = t - s$. For some $x \in \mathbb{F}_t^*$, let $F(X) \in \mathbb{F}_p[X]$ such that $F(V_x(n)) = V_x(n+1)$ for all $x \in A$. We have* $\deg(F) \geq (t - 3s)^{1/2}/6$.

In the proof of Theorem 5, we use the following simple lemma:

Lemma 3. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$ with $A \neq 0$ and $B \neq 0$. Let $F(X) \in \mathbb{F}_p[X]$ be a non-constant polynomial with $F(X) \neq X$. Then there exists $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_2^2(F(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$.*

Proof. There are exactly three distinct zeros $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbb{F}_p}$ of $\psi_2^2(X)$. For all index $i \in \{1, 2, 3\}$, there exists at least one $\beta_i \in \overline{\mathbb{F}_p}$ such that $F(\beta_i) = \alpha_i$, because F is not a constant polynomial. Since for all $i, j \in \{1, 2, 3\}$, $i \neq j$, we have $\alpha_i \neq \alpha_j$, then the system $F(X) = \alpha_i$ and $F(X) = \alpha_j$ has no solution. It follows that the polynomial $\psi_2^2(F(X))$ has at least three different zeros.

Let d denote the degree of F and let us suppose that there does not exist $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_2^2(F(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$. Then we have that $\psi_2^2(F(X))$ has exactly three zeros which are the zeros of $\psi_2^2(X)$. If $d = 1$, then it will imply that $F(X) = X$ which is impossible. If $d \geq 2$, for all $i \in \{1, 2, 3\}$, the equation $F(X) = \alpha_i$ has exactly one solution γ_i of multiplicity d which is one of $\{\alpha_1, \alpha_2, \alpha_3\}$. Then γ_1 and γ_2 are the zeros of the $(d-1)$-derivative of $F(X)$ which is of degree 1 and this is impossible because $\gamma_1 \neq \gamma_2$. Hence in all cases, we obtain a contradiction. So there exists $\alpha \in \overline{\mathbb{F}_p}$ such that: $\psi_2^2(F(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$.

Proof (Theorem). Let $R = \{(n+x) \bmod t : n \in A\}$. Then $R \subseteq \mathbb{F}_t$ and $\sharp R = t - s$. The equation $F(V_x(n)) = V_x(n+1)$ then becomes:

$$F\left(X\left(\left[\frac{1}{n}\right]P\right)\right) = X\left(\left[\frac{1}{n+1}\right]P\right),$$

for all $n \in R$. Denoting $x_k = X([k]P) = X([k \bmod t]P)$ and considering the set $T = \{n \in R/n/2, n+1 \in R\}$, we have

$$\begin{aligned} F\left(x_{\frac{2}{n}}\right) = F\left(x_{\frac{1}{n/2}}\right) = x_{\frac{1}{n/2+1}} = x_{\frac{2}{n+2}} &= \frac{\theta_2(x_{\frac{1}{n+2}})}{\psi_2^2(x_{\frac{1}{n+2}})} \\ &= \frac{\theta_2(F(x_{\frac{1}{n+1}}))}{\psi_2^2(F(x_{\frac{1}{n+1}}))} \\ &= \frac{\theta_2(F(F(x_{\frac{1}{n}})))}{\psi_2^2(F(F(x_{\frac{1}{n}})))}, \end{aligned}$$

hence we have

$$F\left(\frac{\theta_2(x_{\frac{1}{n}})}{\psi_2^2(x_{\frac{1}{n}})}\right) = \frac{\theta_2(F(F(x_{\frac{1}{n}})))}{\psi_2^2(F(F(x_{\frac{1}{n}})))}, \text{ for all } n \in T.$$

Finally, we consider the polynomial

$$H(X) = \psi_2^{2d_0}(X)\psi_2^2(F(F(X)))\left(F\left(\frac{\theta_2(X)}{\psi_2^2(X)}\right) - \frac{\theta_2(F(F(X)))}{\psi_2^2(F(F(X)))}\right).$$

The polynomial $H(X)$ has at least $\sharp T/2$ zeros. We have $F(F(X)) \neq X$ and by Lemma 3, it will imply that there exists $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_2^2(F(F(\alpha))) = 0$ and $\psi_2^2(\alpha) \neq 0$. Hence, we have $H(\alpha) = -\theta_2(F(F(\alpha)))\psi_2^{2d_0}(\alpha) \neq 0$, since $\theta_2(X)$ and $\psi_2^2(X)$ have no common zeros. Therefore, $H(X)$ is a non-zero polynomial and $\deg(H) \leq 9d_0^2$. Then we get that $9d_0^2 \geq \sharp R/2$ and the result follows. □

6 Conclusion

We studied the distribution of the Dodis-Yampolskiy pseudo-random function values over finite fields and over elliptic curves. We also proved lower bounds on the degree of polynomials interpolating the values of these functions in this two settings of practical interest. As future works, it would be interesting to study the distribution of k-tuples $(V_x(m), \ldots, V_x(m+k))_m$ and to study the linear complexity and minimal polynomials of the sequence generated by the Dodis-Yampolskiy functions over finite fields and over elliptic curves.

Acknowledgments. The authors would like to thank the reviewers for their detailed comments and suggestions for the manuscript. The authors were supported in part by the French ANR JCJC ROMAnTIC project (ANR-12-JS02-0004) and by the Simons foundation Pole PRMAIS.

References

[BGLS00] W. D. Banks, F. Griffin, D. Lieman, and I. Shparlinski. Non-linear complexity of the Naor-Reingold pseudo-random function. In *ICISC 99: 2nd International Conference on Information Security and Cryptology*, *Lecture Notes in Computer Science* 1787, pages 53–59, Seoul, Korea, December 9–10, 2000. Springer, Heidelberg, Germany.

[BS08] J. Bourgain and I. E. Shparlinski. Distribution of consecutive modular roots of an integer. *Acta Arith.*, 134(1):83–91, 2008.

[BSS99] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography.* Cambridge: Cambridge University Press, 1999.

[Che10] J. H. Cheon. Discrete logarithm problems with auxiliary inputs. *Journal of Cryptology*, 23(3):457–476, July 2010.

[CHK+06] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to win the clonewars: Efficient periodic n-times anonymous authentication. In *ACM CCS 06: 13th Conference on Computer and Communications Security*, pages 201–210, Alexandria, Virginia, USA, October 30 – November 3, 2006. ACM Press.

[CHL05] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact e-cash. In *Advances in Cryptology – EUROCRYPT 2005*, *Lecture Notes in Computer Science* 3494, pages 302–321, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

[CS00] D. Coppersmith and I. Shparlinski. On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping. *Journal of Cryptology*, 13(3):339–360, 2000.

[DT97] M. Drmota and R. Tichy. *Discrepancies and applications.* Springer-Verlag, Berlin, 1997.

[DY05] Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In *PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography*, *Lecture Notes in Computer Science* 3386, pages 416–431, Les Diablerets, Switzerland, January 23–26, 2005. Springer, Heidelberg, Germany.

[GGI11] D. Gómez, J. Gutierrez, and A. Ibeas. On the linear complexity of the Naor-Reingold sequence. *Inf. Process. Lett.*, 111(17):854–856, 2011.

[IK04] H. Iwaniec and E. Kowalski. *Analytic number theory.* Amer. Math.Soc., Providence, RI, 2004.

[KW06] E. Kiltz and A. Winterhof. Polynomial interpolation of cryptographic functions related to Diffie-Hellman and discrete logarithm problem. *Discrete Appl. Math.*, 154(2):326–336, 2006.

[LSW14] S. Ling, I. E. Shparlinski, and H. Wang. On the multidimensional distribution of the Naor-Reingold pseudo-random function. *Math. Comput.*, 83(289), 2014.

[LW02] T. Lange and A. Winterhof. Polynomial interpolation of the elliptic curve and XTR discrete logarithm. In *Computing and Combinatorics, 8th Annual International Conference, COCOON 2002, Singapore, August 15-17, 2002, Proceedings*, *Lecture Notes in Computer Science* 2387, pages 137–143. Springer, 2002.

[NR04] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, 2004.

[NW00] H. Niederreiter and A. Winterhof. Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. *Acta. Arith.*, 93(4):387–399, 2000.

[OS11] A. Ostafe and I. E. Shparlinski. Twisted exponential sums over points of elliptic curves. *Acta Arith.*, 148(1):77–92, 2011.

[Shp11] I. E. Shparlinski. Exponential sums with consecutive modular roots of an integer. *Q. J. Math.*, 62(1):207–213, 2011.

[Was08] L. C. Washington. *Elliptic curves. Number theory and cryptography.* . Boca Raton, FL: Chapman and Hall/CRC, 2nd ed. edition, 2008.

[Wei48] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A*, 34:204–207, 1948.

A Proof of Proposition 1

The classical Weil bound for exponential sums can be found in [Wei48,NW00].

Lemma 4. *Let $F(x)$ be a non constant polynomial in $\mathbb{F}_q[x]$ such that $F(x) \neq h(x)^p - h(x)$ for any $h(x) \in \overline{\mathbb{F}_q}(x)$. We have*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(F(x)) \right| \leq (\deg(F) - 1) q^{1/2}$$

We deduce the following simple lemma:

Lemma 5. *For any pairwise distinct positive integers $1 \leq r_1, \ldots, r_\upsilon \leq R$, we have*

$$\max_{\substack{(a_1,\ldots,a_\upsilon) \in \mathbb{F}_{p^r}^\upsilon \\ (a_1,\ldots,a_\upsilon) \neq (0,\ldots,0)}} \left| \sum_{n=1}^{t} \psi\left(\sum_{i=1}^{\upsilon} a_i g^{r_i n} \right) \right| \leq R q^{1/2}.$$

Proof. Let $s = (q-1)/t$. We have $g = \theta^s$, where θ is a primitive root in $\mathbb{F}_q$ and

$$\begin{aligned} \sum_{n=1}^{t} \psi\left(\sum_{i=1}^{\upsilon} a_i g^{r_i n} \right) = \sum_{n=1}^{t} \psi\left(\sum_{i=1}^{\upsilon} a_i \theta^{s r_i n} \right) &= \frac{1}{s} \sum_{n=1}^{q-1} \psi\left(\sum_{i=1}^{\upsilon} a_i \theta^{s r_i n} \right) \\ &= \frac{1}{s} \left(\sum_{x \in \mathbb{F}_q} \psi\left(\sum_{i=1}^{\upsilon} a_i x^{s r_i} \right) - 1 \right) \end{aligned}$$

Applying Lemma 4, we obtain :

$$\max_{\substack{(a_1,\ldots,a_\upsilon) \in \mathbb{F}_{p^r}^\upsilon \\ (a_1,\ldots,a_\upsilon) \neq (0,\ldots,0)}} \left| \sum_{n=1}^{t} \psi\left(\sum_{i=1}^{\upsilon} a_i g^{r_i n} \right) \right| \leq \frac{1}{s}((Rs-1)q^{1/2} + 1) \leq R q^{1/2}.$$

□

Proof (Proposition 1). For any integer $k \geq 2$, we have

$$S_{a,b}{}^k = \sum_{n_1,\ldots,n_k \in \mathbb{Z}_t^*} \psi\left(a \sum_{j=1}^{k} g^{1/n_j}\right) e_t\left(b \sum_{j=1}^{k} n_j\right).$$

For $m \in \mathbb{Z}_t$, we collect together the terms with $n_1 + \cdots + n_k \equiv m \bmod t$, getting:

$$|S_{a,b}|^k \leq \sum_{m \in \mathbb{Z}_t} \left| \sum_{\substack{n_1,\ldots,n_k \in \mathbb{Z}_t^* \\ n_1+\cdots+n_k \equiv m \bmod t}} \psi\left(a \sum_{j=1}^{k} g^{1/n_j}\right) \right|.$$

By the Cauchy inequality, we can upper-bound $|S_{a,b}|^{2k}$ by

$$t \sum_{m \in \mathbb{Z}_t} \left| \sum_{\substack{n_1,\ldots,n_k \in \mathbb{Z}_t^* \\ n_1+\cdots+n_k \equiv m \bmod t}} \psi\left(a \sum_{j=1}^{k} g^{1/n_j}\right) \right|^2 = t \sum_{(n_1,\ldots,n_{2k}) \in N_k} \psi\left(a \sum_{j=1}^{2k} (-1)^j g^{1/n_j}\right)$$

where the outside summation is taken over the set of vectors

$$N_k = \{(n_1, \ldots, n_{2k}) \in (\mathbb{Z}_t^*)^{2k} \ : n_1 + \cdots + n_{2k-1} \equiv n_2 + n_4 + \cdots + n_{2k} \bmod t)\}.$$

One can see that for any $m \in \mathbb{N}$ with $\gcd(m, t) = 1$, we have

$$\sum_{(n_1,\ldots,n_{2k}) \in N_k} \psi\left(a \sum_{j=1}^{2k} (-1)^j g^{1/n_j}\right) = \sum_{(n_1,\ldots,n_{2k}) \in N_k} \psi\left(a \sum_{j=1}^{2k} (-1)^j g^{m/n_j}\right).$$

Let us fix some parameter Q with $Q \geq 2 \log t$. Let $\mathcal{Q}$ be the set of primes $m \leq Q$ with $\gcd(m, t) = 1$. Averaging over all $m \in \mathcal{Q}$, we obtain

$$|S_{a,b}|^{2k} \leq \frac{t}{\sharp \mathcal{Q}} \sum_{m \in \mathcal{Q}} \sum_{(n_1,\ldots,n_{2k}) \in N_k} \psi\left(a \sum_{j=1}^{2k} (-1)^j g^{m/n_j}\right).$$

The number $w(t)$ of prime divisors of t satisfies $w(t) \leq (1+o(1))(\log t)/(\log\log t)$ (which can be seen from the trivial inequality $w(t)! \leq t$ and the Stirling formula). By the prime number theorem, we have (since $Q \geq 2 \log t$):

$$\sharp \mathcal{Q} \geq (1 + o(1)) \frac{Q}{\log Q} - (1 + o(1)) \frac{\log t}{\log(\log t)} \geq 0.5 \frac{Q}{\log Q},$$

provided that t is large enough. We have $\sharp N_k \leq t^{2k-1}$. Using the Hölder inequality and then extending the region of summation, we obtain that for any integer

$\ell \geq 1$, we have:

$$\begin{aligned}
|S_{a,b}|^{4k\ell} &\leq \frac{t^{2\ell}}{\sharp\mathcal{Q}^{2\ell}}(\sharp N_k)^{2\ell-1} \sum_{n_1,\ldots,n_{2k}\in\mathbb{Z}_t^*} \left|\sum_{m\in\mathcal{Q}} \psi\left(a\sum_{j=1}^{2k}(-1)^j g^{m/n_j}\right)\right|^{2\ell} \\
&\ll \frac{t^{4k\ell-2k+1}\log^{2\ell} Q}{Q^{2\ell}} \sum_{n_1,\ldots,n_{2k}=1}^{t} \left|\sum_{m\in\mathcal{Q}} \psi\left(a\sum_{j=1}^{2k}(-1)^j g^{mn_j}\right)\right|^{2\ell} \\
&= \frac{t^{4k\ell-2k+1}\log^{2\ell} Q}{Q^{2l}} \sum_{n_1,\ldots,n_{2k}=1}^{t} \sum_{m_1,\ldots,m_{2\ell}\in\mathcal{Q}} \psi\left(a\sum_{j=1}^{2k}\sum_{h=1}^{2\ell}(-1)^{j+h} g^{m_h n_j}\right) \\
&= \frac{t^{4k\ell-2k+1}\log^{2\ell} Q}{Q^{2\ell}} \sum_{m_1,\ldots,m_{2\ell}\in\mathcal{Q}} \left|\sum_{n=1}^{t} \psi\left(a\sum_{h=1}^{2\ell}(-1)^h g^{m_h n}\right)\right|^{2k}.
\end{aligned}$$

For $O(\sharp\mathcal{Q}^\ell)$=$O(Q^\ell \log^{-\ell} Q)$ tuples $(m_1,\ldots,m_{2\ell}) \in \mathcal{Q}^{2\ell}$ such that the tuple of the elements on the odd positions $(m_1,\ldots,m_{2\ell-1})$ is a permutation of the elements on the even positions $(m_2,\ldots,m_{2\ell})$, we estimate the inner sum trivially as t. For the remaining $O((\sharp Q)^{2\ell}) = O(Q^{2\ell}(\log Q)^{-2\ell})$ tuples, we use the bound of Lemma 5. Therefore,

$$\begin{aligned}
|S_{a,b}|^{4k\ell} &\ll \frac{t^{4k\ell-2k+1}\log^{2\ell} Q}{Q^{2l}}(Q^\ell \log^{-\ell} Q t^{2k} + Q^{2\ell}\log^{-2\ell} Q (Qq^{1/2})^{2k}) \\
&= t^{4k\ell-2k+1}(Q^{-\ell}\log^\ell Q t^{2k} + Q^{2k} q^k).
\end{aligned}$$

Taking $Q = 2t^{2k/(2k+\ell)} q^{-k/(2k+\ell)} (\log q)^{\ell/(2k+\ell)}$ and if $t \geq q^{1/2}(\log q)^2$, one can see that $Q \geq 2\log t$ and we obtain

$$|S_{a,b}|^{4k\ell} \ll t^{4k\ell-(2k\ell-2k-\ell)/(2k+\ell)} q^{k\ell/(2k+\ell)} (\log q)^{\ell/(2k+\ell)}$$

and the result follows. □