LINEAR APPROXIMATIONS OF THE FLYSTEL CONSTRUCTION

TIM BEYNE AND CLÉMENCE BOUVIER

ABSTRACT. Using a purity theorem for exponential sums due to Rojas-Léon [5], we upper bound the absolute correlations of linear approximations of the `Flystel` construction used in `Anemoi` [3]. This resolves open problem 7.1 in [2].

`Anemoi` is a family of hash functions based on the `Flystel` construction. Since the open and closed `Flystel` variants are CCZ-equivalent, we can focus on the closed variant. The closed `Flystel` construction is shown in Figure 1a, with Q_γ and Q_δ two quadratic functions on $\mathbf{F}_q$ defined by $\mathsf{Q}_\lambda\colon x \mapsto \beta x^2 + \lambda$, where β is a non-zero constant in $\mathbf{F}_q$. Assume that $d \geq 3$ is coprime to $q-1$ so that $x \mapsto x^d$ is a permutation. Up to addition by a constant, we can assume $\gamma = \delta = 0$. Hence, the closed `Flystel` construction $\mathsf{F}\colon \mathbf{F}_q^2 \to \mathbf{F}_q^2$ is given by $\mathsf{F}(x_1, x_2) = (y_1, y_2)$, where

$$y_1 = (x_1 - x_2)^d + \beta x_1^2$$
$$y_2 = (x_1 - x_2)^d + \beta x_2^2 \,.$$

Let (ψ, χ) be a linear approximation of F, with $\psi = (\psi_1, \psi_2)$ and $\chi = (\chi_1, \chi_2)$ nontrivial additive characters of $\mathbf{F}_q^2$. If $\chi_1\chi_2 = 1$, then there is one linear trail with nonzero correlation, so the result follows from the properties of quadratic Gauss sums (assume $\chi \neq 1$):

$$\left|C^{\mathsf{F}}_{\chi,\psi}\right| = \left|C^{\mathsf{Q}_\gamma}_{\chi_1,\psi_1}\right| \times 1 \times \left|C^{\mathsf{Q}_\delta}_{\chi_2,\psi_2}\right| = 1/\sqrt{q} \times 1/\sqrt{q} = 1/q \,.$$

Let ω be a principal additive character of $\mathbf{F}_q$ and write $\psi_i(x) = \omega(u_i x)$ and $\chi_i(x) = \omega(v_i x)$ with u_1, u_2, v_1 and v_2 in $\mathbf{F}_q$. If $\chi_1\chi_2 \neq 1$, then upper bounding the absolute correlation of (ψ, χ) amounts to estimating an exponential sum of the form

$$S(f) = \sum_{x \in \mathbf{F}_q^2} \omega(f(x)) \,,$$

with $f(x) = (v_1 + v_2)(x_1 - x_2)^d + \beta(v_1 x_1^2 + v_2 x_2^2) - u_1 x_1 - u_2 x_2$. To upper bound $|S(f)|$, we follow the strategy that was used for `Rescue` in [1, §3.2]. Let $\mathcal{L}_\omega$ be the Artin-Schreier sheaf on the affine line $\mathbf{A}^1$ over $\overline{\mathbf{F}}_q$ associated to the character ω, and $f^*\mathcal{L}_\omega$ its pullback to $\mathbf{A}^n$ along f (in our case, $n = 2$). Let $H^i_c(\mathbf{A}^n, f^*\mathcal{L}_\omega)$ denote cohomology with compact supports and coefficients in the ℓ-adic sheaf $f^*\mathcal{L}_\omega$ It follows from Grothendieck's trace formula that

$$S(f) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\left(\sigma, H^i_c(\mathbf{A}^n, f^*\mathcal{L}_\omega)\right) ,$$

Date: September 19, 2024.

Tim Beyne is supported by the Research Foundation – Flanders (FWO) reference № 1274724N.
Clémence Bouvier is supported by the European Research Council (ERC, grant №101097056 "SymTrust").

where σ is the geometric Frobenius action on $H_c^i(\mathbf{A}^n, f^*\mathcal{L}_\omega)$. The approach introduced in [1] is to use Deligne's theorem [4, Théorème 8.4], which shows that $H_c^i(\mathbf{A}^n, f^*\mathcal{L}) = 0$ for all $i \neq n$ and $H_c^n(\mathbf{A}^n, f^*\mathcal{L})$ is pure of weight n. That is, the eigenvalues of the geometric Frobenius action on $H_c^n(\mathbf{A}^n, f^*\mathcal{L})$ all have absolute value $q^{n/2}$. This implies the bound $|S(f)| \leq q^{n/2} \dim H_c^n(\mathbf{A}^n, f^*\mathcal{L}) \leq (d-1)^n\, q^{n/2}$. Deligne's theorem requires that the maximum-degree homogeneous component of f defines a smooth hypersurface in $\mathbf{P}^{n-1}$, but this is not the case for the `Flystel` construction. Nevertheless, the following result of Rojas-Léon is applicable.

Theorem 1 (Rojas-Léon [5, Theorem 2]). *Let f be a degree-d polynomial over $\mathbf{F}_q$ in n variables with $f = f_d + f_{d'} + \cdots$, where f_d is the degree-d homogeneous component of f and $f_{d'}$ is its homogeneous component of degree $d' = \deg f - f_d$. Let ω be a non-trivial additive character of $\mathbf{F}_q$ and $\mathcal{L}_\omega$ the corresponding Artin-Schreier sheaf on $\mathbf{A}^1$. Suppose that d and d' are coprime to the characteristic p of $\mathbf{F}_q$ and $d'/d > p/(p+(p-1)^2)$. If the projective hypersurface in $\mathbf{P}^{n-1}$ defined by $f_d = 0$ has at worst quasi-homogeneous isolated hypersurface singularities of degrees prime to p with Milnor numbers $\mu_1, \ldots, \mu_s$, and if the projective hypersurface in $\mathbf{P}^{n-1}$ defined by $f_{d'} = 0$ contains none of these singularities, then*

(1) *For all $i \neq n$, we have vanishing cohomology $H_c^i(\mathbf{A}^n, f^*\mathcal{L}_\omega) = 0$.*
(2) *$H_c^n(\mathbf{A}^n, f^*\mathcal{L}_\omega)$ is pure of weight n with dimension $(d-1)^n - (d-d')\sum_{i=1}^{s} \mu_i$.*

Since $\chi_1\chi_2 \neq 1$, we have $v_1 + v_2 \neq 0$ so that $d' = 2$. Theorem 1 is applicable for all d coprime to $p \neq 2$ with $d < (p-1)/2$. The projective hypersurface defined by $f_d(x_1, x_2) = (v_1+v_2)(x_1-x_2)^d = 0$ has one singular point $[1:1]$. This is an isolated quasi-homogeneous hypersurface singularity of degree d with Milnor number $\mu_1 = d-1$. Furthermore, the hypersurface defined by $f_{d'}(x_1, x_2) = \beta(v_1 x_1^2 + v_2 x_2^2) = 0$ does not contain the point $[1:1]$ because $v_1 + v_2 \neq 0$. By Theorem 1, it follows that $H_c^2(\mathbf{A}^2, f^*\mathcal{L}_\omega)$ is pure of weight two and

$$\dim H_c^2(\mathbf{A}^2, f^*\mathcal{L}_\omega) = (d-1)^2 - (d-2)(d-1) = d-1\,.$$

Summarizing the results above, if $p \neq 2$ and $d < 2(p-1)$ is coprime to $q-1$ and p, then the correlation matrix of the `Flystel` construction satisfies (if $\chi \neq 1$)

$$\left|C^{\mathsf{F}}_{\chi,\psi}\right| \leq \begin{cases} 1/q & \text{if } \chi_1\chi_2 = 1\,, \\ (d-1)/q & \text{otherwise}\,. \end{cases}$$

For low values of d this is close to the experimental results, as shown in Figure 1b for $d = 3$ and $d = 5$.

References

[1] Beyne, T., Canteaut, A., Leander, G., Naya-Plasencia, M., Perrin, L., Wiemer, F.: On the security of the Rescue hash function. Cryptology ePrint Archive, Paper 2020/820 (2020), `https://eprint.iacr.org/2020/820`

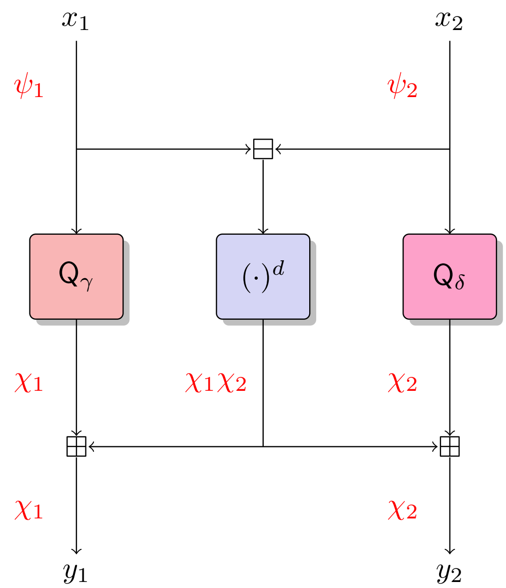
[2] Bouvier, C.: Cryptanalysis and design of symmetric primitives defined over large finite fields. Theses, Sorbonne Université (Nov 2023), `https://inria.hal.science/tel-04327955`

[3] Bouvier, C., Briaud, P., Chaidos, P., Perrin, L., Salen, R., Velichkov, V., Willems, D.: New design techniques for efficient arithmetization-oriented hash functions: Anemoi permutations and Jive compression mode. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023, Part III. Lecture Notes in Computer Science, vol. 14083, pp. 507–539. Springer, Cham, Switzerland, Santa Barbara, CA, USA (Aug 20–24, 2023)

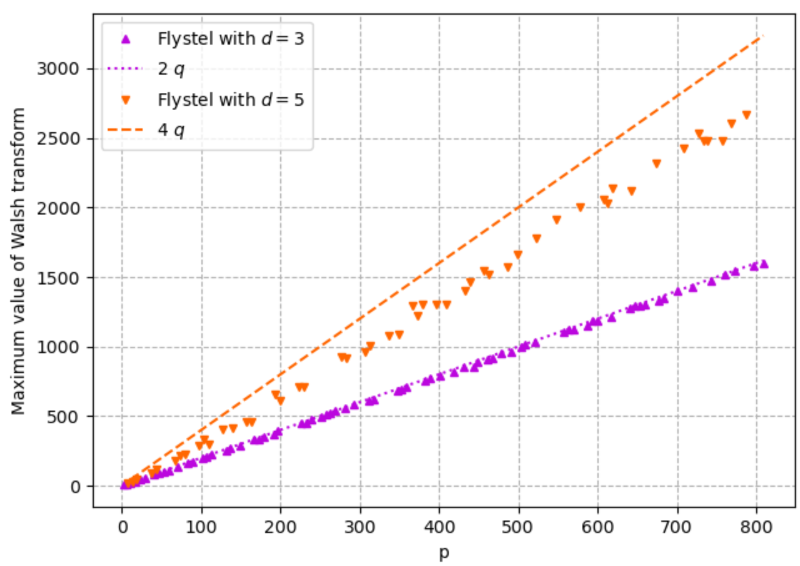
[4] Deligne, P.: La conjecture de Weil: I. Publ. Math. de l'IHÉS 43, 273–307 (1974)

[5] Rojas-León, A.: Purity of exponential sums on $\mathbb{A}^n$. Comp. Math. 142(2), 295–306 (2006)

COSIC, KU Leuven and Ruhr University Bochum, Ruhr University Bochum
Email address: `tim.beyne@esat.kuleuven.be, clemence.bouvier@rub.de`



(A) Closed `Flystel` construction F.



(B) Our bound.

FIGURE 1. `Flystel` construction and our upper bound.