Ramanujan Graphs for Post-Quantum Cryptography

Hyungrok Jo, Shingo Sugiyama, and Yoshinori Yamasaki

Abstract We introduce a cryptographic hash function based on expander graphs, suggested by Charles et al. '09, as one prominent candidate in post-quantum cryptography. We propose a generalized version of explicit constructions of Ramanujan graphs, which are seen as an optimal structure of expander graphs in a spectral sense, from the previous works of Lubotzky, Phillips, Sarnak '88 and Chiu '92. We also describe the relationship between the security of Cayley hash functions and word problems for group theory. We also give a brief comparison of LPS-type graphs and Pizer's graphs to draw attention to the underlying hard problems in cryptography.

Keywords Ramanujan graphs · Quaternion algebras · Cayley hash functions · Group word problem

1 Introduction

In the era of post-quantum cryptography, there exist four dominant research areas: Lattice-based, Code-based, Multivariate-based and Isogeny-based cryptography. Specifically, studies in the area of Isogeny-based cryptography have been numerous in the past decade, mainly due to the difficulty of finding a path in the Isogeny graph of supersingular elliptic curves.

H. Jo (✉)
Faculty of Engineering, Information and Systems, University of Tsukuba,
1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan
e-mail: jo.hyungrok.gb@u.tsukuba.ac.jp

S. Sugiyama
Department of Mathematics, College of Science and Technology, Nihon University,
1-8-14 Suruga-Dai, Kanda, Chiyoda, Tokyo 101-8308, Japan
e-mail: s-sugiyama@math.cst.nihon-u.ac.jp

Y. Yamasaki
Graduate School of Science and Engineering, Ehime University,
2-5 Bunkyo-cho, Matsuyama, Ehime 790-8577, Japan
e-mail: yamasaki.yoshinori.mh@ehime-u.ac.jp

T. Takagi et al. (eds.), *International Symposium on Mathematics, Quantum Theory, and Cryptography*, Mathematics for Industry 33,
https://doi.org/10.1007/978-981-15-5191-8_17

In 2009, Charles et al. (2009a, 2009b) introduced cryptographic hash functions from expander graphs and explained the hardness of problems behind those schemes. They proposed two kinds of hash functions based on two families of Ramanujan graphs. One of their proposals is based on Ramanujan graphs by Lubotzky et al. (1988) (in short, LPS), which are Cayley graphs over the projective group with respect to well-chosen generating sets. The other is based on Ramanujan graphs by Pizer (1990), which are not (expected to be) Cayley graphs. So far, the variants of their proposal still survive against a quantum attack except the only known exponential complexity attack (Biasse et al. 2014).

In this article, we focus on not only the background of the families of LPS's graphs and their generalization (LPS-type Jo et al. 2020, 2018) with respect to the security of their Cayley-based hash functions, but also on the relationship between the families of LPS-type graphs and Pizer's graphs.

This article is organized as follows: In Sect. 2, we present some required preliminaries of expander graphs and Ramanujan graphs, and also of quaternion algebra theory. We summarize the security on Cayley hash functions and their cryptanalysis (variants of lifting attacks) related to solving word problems in group theory. In Sect. 3, we explain a way to generalize the explicit constructions of LPS and Chiu's Ramanujan graphs, and give a proof of the Ramanujan-ness of our graphs in the special case of "$P = 13$". In Sect. 4, we describe the relationship between the families of LPS-type graphs and Pizer's graphs. In Sect. 5, we summarize the arguments in this article and expound upon some unclarified problems and the relationships between explicit families of Ramanujan graphs.

2 Ramanujan Graphs and Their Cryptographic Applications

An expander graph is well known as a ubiquitous object in various research areas, especially in computer science for designing communication networks. It is said to be a sparse, but highly connected graph. The quality of the network on expander graphs is considered as the expanding ratio. Throughout this article, we assume that all graphs are finite, undirected, simple (i.e. no loops or multi-edges) and connected. Suppose that $X = (V, E)$ is a k-regular graph, composed of a vertex set $V = V(X)$ with n vertices and an edge set $E = E(X)$. For a subset T of V, the *boundary* ∂T of T is defined as

$$\partial T = \{(x, y) \in E | x \in T \text{ and } y \in V \setminus T\},$$

where $V \setminus T$ is the complement of T in V. The *expanding constant* $h(X)$ of X, which is defined as below, is a discrete analogue of the Cheeger constant in differential geometry (Lubotzky 1994):

$$h(X) = \min_{\substack{T \subset V \\ 0 < |T| \leq n/2}} \frac{|\partial T|}{|T|}.$$

We give the definition of an *expander graph*.

Definition 1 A family of k-regular graphs $(X_j)_{j\geq 1}$ such that $|V(X_j)| \to +\infty$ as $j \to +\infty$ is called an *expander family* if there is an $\epsilon > 0$ such that the expanding constant $h(X_j)$ satisfies $h(X_j) \geq \epsilon$ for all j.

For analysis of graphs, the *adjacency matrix* A of the graph X plays an important role; it is a square matrix indexed by pairs of vertices u, v whose (u, v)-entry $A_{u,v}$ is the number of edges between u and v. Since we assume that X has n vertices, A is an n-by-n, symmetric (0, 1)-matrix without diagonal entries (i.e. $A_{u,u} = 0$). For such a graph X, the adjacency matrix A of X has the spectrum $k = \lambda_0 > \lambda_1 \geq \cdots \geq \lambda_{n-1}$. It is known (Alon and Milman 1985; Dodziuk 1984) that

$$\frac{k - \lambda_1}{2} \leq h(X) \leq \sqrt{2k(k - \lambda_1)}.$$

If the spectral gap $k - \lambda_1$ is larger, the quality of the network of X is getting better as well. However, it is shown by Alon-Boppana as follows that it cannot be too large.

Theorem 1 *Let $(X_j)_{j\geq 1}$ be a family of k-regular graphs with $|V(X_j)| \to +\infty$ as $j \to +\infty$. Then*

$$\liminf_{j\to+\infty} \lambda_1(X_j) \geq 2\sqrt{k-1}.$$

This fact motivates the definition of a *Ramanujan graph*.

Definition 2 A k-regular graph X is *Ramanujan* if, for every member λ of the spectrum of the adjacency matrix of X other than $\pm k$, one has $|\lambda| \leq 2\sqrt{k-1}$. We call $2\sqrt{k-1}$ the *Ramanujan bound* (RB).

For a more detailed exposition of the theory, see Davidoff et al. (2003), Lubotzky (1994), Terras (2010). In order to explain how to construct explicit Ramanujan graphs in the style of LPS, Chiu, LPS-type and Pizer, we recall basic facts and terminologies of quaternion algebras Vignéras (1980).

Let F be a field and $F^\times$ its unit group. Let $\mathcal{A} = \mathcal{A}_F$ be a *quaternion algebra* over F, i.e. a central simple algebra of dimension 4 over F. In this article, we always assume that F is not of characteristic 2. Then, there exist $a, b \in F^\times$ such that it can be written as $\mathcal{A} = \mathcal{A}_F(a, b) = \{\alpha = x + yi + zj + wk \mid x, y, z, w \in F\}$, where i, j, k satisfy $i^2 = a$, $j^2 = b$ and $ij = -ji = k$ (and hence $k^2 = -ab$). For $\alpha = x + yi + zj + wk \in \mathcal{A}$, its *conjugate*, the *reduced trace* and the *reduced norm* are defined by $\overline{\alpha} = x - yi - zj - wk$, $T(\alpha) = \alpha + \overline{\alpha} = 2x \in F$ and $N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = x^2 - ay^2 - bz^2 + abw^2 \in F$, respectively.

Quaternion algebras over $\mathbb{F}_q$

Throughout this article, we denote by $\mathbb{P}$ the set of all prime numbers. For a prime $p \in \mathbb{P}$ and $d \in \mathbb{N}$, let $\mathbb{F}_{p^d}$ be the field of p^d elements. Let us fix $q \in \mathbb{P} \setminus \{2\}$. It is known that, for any $a, b \in \mathbb{F}_q^\times$, the quaternion algebra $\mathcal{A} = \mathcal{A}_{\mathbb{F}_q}(a, b)$ is isomorphic to the matrix algebra $\mathrm{M}_2(\mathbb{F}_q)$ of the 2-by-2 matrices over $\mathbb{F}_q$. Let $\left(\frac{\cdot}{\cdot}\right)$ be the Kronecker symbol. When $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$, that is, $\sqrt{a}, \sqrt{-b} \in \mathbb{F}_q$, one has the following isomorphism.

Lemma 1 *Assume that* $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$. *Then, the map* $\psi_q : \mathcal{A} \to \mathrm{M}_2(\mathbb{F}_q)$ *defined by*

$$\psi_q(x + yi + zj + wk) = \begin{bmatrix} x + y\sqrt{a} & \sqrt{-b}(z + w\sqrt{a}) \\ -\sqrt{-b}(z - w\sqrt{a}) & x - y\sqrt{a} \end{bmatrix}$$

is an isomorphism satisfying $\det(\psi_q(\alpha)) = N(\alpha)$ *and* $\psi_q(\overline{\alpha}) = \overline{\psi_q(\alpha)}$ *for* $\alpha \in \mathcal{A}$. *Here,* $\overline{\begin{bmatrix} s & t \\ u & v \end{bmatrix}} = \begin{bmatrix} v & -t \\ -u & s \end{bmatrix}$ *for* $\begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \mathrm{M}_2(\mathbb{F}_q)$.

For a ring R, we denote by $R^\times$ the group of units of R. Let $\mathrm{GL}_2(\mathbb{F}_q) = \mathrm{M}_2(\mathbb{F}_q)^\times$ and $\mathrm{SL}_2(\mathbb{F}_q) = \{A \in \mathrm{GL}_2(\mathbb{F}_q) \mid \det A = 1\}$. Moreover, let $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/Z(\mathrm{GL}_2(\mathbb{F}_q))$ and $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/Z(\mathrm{SL}_2(\mathbb{F}_q))$. Here, for a group G, we denote by $Z(G)$ the *center* of G. We can naturally see that $\mathrm{PSL}_2(\mathbb{F}_q)$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ of index 2 because now q is odd. Additionally, we remark that $|\mathrm{PGL}_2(\mathbb{F}_q)| = q(q^2 - 1)$ and $|\mathrm{PSL}_2(\mathbb{F}_q)| = \frac{q(q^2-1)}{2}$. Since $\mathcal{A} \simeq \mathrm{M}_2(\mathbb{F}_q)$, we have $\mathcal{A}^\times \simeq \mathrm{GL}_2(\mathbb{F}_q)$ via (the restriction of) ψ_q and hence obtain the isomorphism $\beta_q : \mathcal{A}^\times/Z(\mathcal{A}^\times) \to \mathrm{PGL}_2(\mathbb{F}_q)$.

We need the following lemma later.

Lemma 2 (Davidoff et al. 2003, Chap. 3) *Assume that* $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$. *Let* $\alpha \in \mathcal{A}$ *with* $N(\alpha) = p \in \mathbb{P} \setminus \{q\}$, *which implies that* $\alpha \in \mathcal{A}^\times$. *Then,* $\beta_q(\alpha\mathbb{F}_q^\times) \in \mathrm{PSL}_2(\mathbb{F}_q)$ *if and only if* $\left(\frac{p}{q}\right) = 1$.

Quaternion algebras over $\mathbb{Q}$

Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}(a, b)$ be a quaternion algebra over $\mathbb{Q}$. A place v of $\mathbb{Q}$ is said to be *split* in $\mathcal{A}$ if $\mathcal{A}_v := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_v \simeq \mathrm{M}_2(\mathbb{Q}_v)$, where $\mathbb{Q}_v$ is the v-adic completion of $\mathbb{Q}$ and is said to be *ramified* if $\mathcal{A}_v$ is a division algebra. We denote by $\mathrm{Ram}(\mathcal{A})$ the set of all places which are ramified in $\mathcal{A}$. Notice that $\mathrm{Ram}(\mathcal{A})$ is a finite set, has an even cardinality, and determines an isomorphism class of quaternion algebras over $\mathbb{Q}$. The product of all primes (= finite places) in $\mathrm{Ram}(\mathcal{A})$ is called the *discriminant* of $\mathcal{A}$ and is denoted by $\mathfrak{D}$. From now on, we assume that $\mathcal{A}$ is definite, that is, the infinite place ∞ is ramified in $\mathcal{A}$, whence there are an odd number of primes which are ramified in $\mathcal{A}$. Notice that $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}(a, b)$ is definite if and only if $a < 0$ and $b < 0$.

A *lattice* $\mathcal{I} \subset \mathcal{A}$ is a free $\mathbb{Z}$-submodule of $\mathcal{A}$ of rank 4. A lattice $\mathcal{O} \subset \mathcal{A}$ is called an *order* if it is a ring with unity. In particular, it is called *maximal* if it is not properly contained in any other order. Notice that, if $\mathcal{O}$ is an order of $\mathcal{A}$, then $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is an order of $\mathcal{A}_p$ for $p \in \mathbb{P}$. Here, $\mathbb{Z}_p$ is the ring of p-adic integers. Let $\mathcal{O}$ be an order of $\mathcal{A}$. We call a lattice $\mathcal{I}$ of $\mathcal{A}$ a *left* (resp. *right*) $\mathcal{O}$- *ideal* if $\mathcal{O}_L(\mathcal{I}) = \mathcal{O}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \mathcal{O}$), where $\mathcal{O}_L(\mathcal{I}) = \{\alpha \in \mathcal{A} \mid \alpha\mathcal{I} \subset \mathcal{I}\}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \{\alpha \in \mathcal{A} \mid \mathcal{I}\alpha \subset \mathcal{I}\}$). We say that two left (resp. right) $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$ are equivalent, if there exists $\alpha \in \mathcal{A}^\times$ such that $\mathcal{I} = \mathcal{J}\alpha$ (resp. $\mathcal{I} = \alpha\mathcal{J}$). This is an equivalence relation. We denote by $H(\mathcal{O})$ the number of equivalence classes, which is shown to be finite, independent on left or right. We call $H(\mathcal{O})$ the *class number* of $\mathcal{O}$.

We next give the definition of Eichler orders. To do that, we first recall the local situations. If $p \in \mathbb{P}$ is ramified in $\mathcal{A}$, then $\mathcal{A}_p$ is a division algebra which has a maximal order $O_p = \{\alpha \in \mathcal{A}_p \mid N(\alpha) \in \mathbb{Z}_p\}$. On the other hand if $p \in \mathbb{P}$ is split in $\mathcal{A}$, then $\mathcal{A}_p$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_p)$ and a maximal order of $\mathcal{A}_p$ is isomorphic to a conjugate of the maximal order $\mathrm{M}_2(\mathbb{Z}_p) = \begin{bmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{bmatrix}$ of $\mathrm{M}_2(\mathbb{Q}_p)$ by an element of $\mathcal{A}_p^{\times}$.

Let $\mathfrak{D}$ be the discriminant of $\mathcal{A}$, and M be a positive square-free integer which is prime to $\mathfrak{D}$. An order O of $\mathcal{A}$ is called an *Eichler order* of level $(\mathfrak{D}, M)$ if the following local conditions are satisfied: For all $p \in \mathbb{P}$ being ramified in $\mathcal{A}$ (i.e., $p \mid \mathfrak{D}$), $O \otimes_{\mathbb{Z}} \mathbb{Z}_p = O_p$. On the other hand, for all $p \in \mathbb{P}$ being split in $\mathcal{A}$ (i.e. $p \nmid \mathfrak{D}$), $O \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is isomorphic to a conjugate of the order $\begin{bmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ M\mathbb{Z}_p & \mathbb{Z}_p \end{bmatrix}$ of $\mathrm{M}_2(\mathbb{Q}_p)$ by an element of $\mathcal{A}_p^{\times}$. Remark that an Eichler order is maximal when $M = 1$. If $p \mid M$, in this case we call p an *Eichler prime*. Notice that an Eichler order can be characterized as an order which is the intersection of two maximal orders. It is shown in Pizer (1976) that the class number of an Eichler order depends only on its level. Hence, we write $H(O)$ as $H(\mathfrak{D}, M)$ when O is of level $(\mathfrak{D}, M)$. Remark that $H(\mathfrak{D}, 1) = 1$ if and only if $\mathfrak{D} = 2, 3, 5, 7, 13$.

Let G be a group and S a generating set, which is symmetric (i.e. $S = S^{-1}$) and does not contain the identity of G. A *Cayley graph* over G with respect to S is a $|S|$-regular graph with a vertex set V and an edge set E, where $V = G$ and E consists of $(g_1, g_2) \in G \times G$ such that $g_1 = g_2 s$ for some $s \in S$.

The families of LPS's graphs Let p and q ($\gg 2\sqrt{p}$) be distinct primes congruent to 1 (mod 4). In Lubotzky et al. (1988), described how to construct a family of Ramanujan graphs of degree $p+1$ having $O(q^3)$ vertices as $q \to +\infty$. These graphs are Cayley graphs over the groups $G = \mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ with respect to the generating set S_{LPS} defined as

$$S_{LPS} = \left\{ \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix} \middle| a_0{}^2 + a_1{}^2 + a_2{}^2 + a_3{}^2 = p \quad \text{for odd } a_0 > 0 \text{ and even } a_1, a_2, a_3 \right\}, \tag{1}$$

where $i \in \mathbb{Z}$ such that $i^2 \equiv -1 \pmod{q}$. The diophantine Eq. (1) originally comes from the norm of their based-algebra $\mathcal{A}_{\mathbb{Q}}(-1, -1)$, where $i^2 = -1$, $j^2 = -1$ and $ij = -ji = k$, and is called the *Hamiltonian quaternion algebra*. By Jacobi's four-squares theorem Hirschhorn (1987), there are $8(p+1)$ integer solutions $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ of (1). Since there are 8 units as $\pm 1, \pm i, \pm j, \pm k$, we see $|S_{LPS}| = p + 1$.

The families of Chiu's graphs In Margulis (1988), independently of LPS, alluded to the existence of essentially the same graphs as shown by LPS, but without an explicit description. In Chiu (1992), described how to construct a family of Ramanujan graphs, and explicitly covered the case of $p = 2$. Since the Hamiltonian quaternion algebra is not split at $p = 2$, Chiu chose a specific quaternion

algebra $\mathcal{A}_{\mathbb{Q}}(-2, -13)$, which is split at 2 and has a maximal order of class number 1. Take a prime $q \in \mathbb{P} \setminus \{2, 13\}$ such that $\left(\frac{-2}{q}\right) = \left(\frac{13}{q}\right) = 1$. Chiu's cubic graphs are also Cayley graphs over the groups $G = \mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ with respect to the generating set S_C defined as

$$S_C = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 2+i' & i'j' \\ i'j' & 2-i' \end{bmatrix}, \begin{bmatrix} 2-i' & j'i' \\ j'i' & 2+i' \end{bmatrix} \right\},$$

where $i', j' \in \mathbb{Z}$ such that $i'^2 \equiv -2$, $j'^2 \equiv 13 \pmod{q}$, respectively.

The families of Morgenstern's graphs In Morgenstern (1994), described how to construct, for any prime power q, a family of Ramanujan graphs of degree $q + 1$. These graphs are given as Cayley graphs over the groups $G = \mathrm{PGL}_2(\mathbb{F}_{q^d})$ or $\mathrm{PSL}_2(\mathbb{F}_{q^d})$ for some $d \in \mathbb{N}$ with respect to the generating set $S_{M_{\mathrm{odd}}}$ when q is odd and $S_{M_{\mathrm{even}}}$ when q is even. For an odd prime power q, let ϵ be a non-square in $\mathbb{F}_q$. Let $g(x) \in \mathbb{F}_q[x]$ be irreducible of even degree d. We realize $\mathbb{F}_{q^d}$ as $\mathbb{F}_q[x]/g(x)\mathbb{F}_q[x]$. Let $\mathrm{i} \in \mathbb{F}_{q^d}$ be such that $\mathrm{i}^2 = \epsilon$. Then $S_{M_{\mathrm{odd}}}$ is defined as

$$S_{M_{\mathrm{odd}}} = \left\{ \begin{bmatrix} 1 & a - \mathrm{i}b \\ (a + \mathrm{i}b)(x-1) & 1 \end{bmatrix} \,\middle|\, b^2\epsilon - a^2 = 1 \text{ for } a, b \in \mathbb{F}_q \right\}.$$

For an even prime power q, let ϵ be a non-square in $\mathbb{F}_q$. Let $f(x) = x^2 + x + \epsilon$ be irreducible in $\mathbb{F}_q[x]$. Let $g(x) \in \mathbb{F}_q[x]$ be irreducible of even degree d. We also realize $\mathbb{F}_{q^d}$ as $\mathbb{F}_q[x]/g(x)\mathbb{F}_q[x]$. Let $\mathrm{i}' \in \mathbb{F}_{q^d}$ be a root of $f(x)$. Then $S_{M_{\mathrm{even}}}$ is defined as

$$S_{M_{\mathrm{even}}} = \left\{ \begin{bmatrix} 1 & a - \mathrm{i}'b \\ (a + \mathrm{i}'b + b)x & 1 \end{bmatrix} \,\middle|\, a^2 + ab + b^2\epsilon = 1 \text{ for } a, b \in \mathbb{F}_q \right\}.$$

2.1 Security on Cayley Hashes and Word Problems

A *hash function* is a function that accepts a message as an arbitrarily long string of bits and outputs a hash value as a finite, fixed-length string of bits. An efficiency of the hashing process is a basic requirement in a practical point. Such a function should satisfy certain properties such as *collision resistant, second preimage resistant* and *preimage resistant*.

Let $n \in \mathbb{N}$ and let $\mathcal{H} : \{0, 1\}^* \to \{0, 1\}^n$; $m \mapsto h = \mathcal{H}(m)$, where $\{0, 1\}^*$ is the set of bit strings of arbitrary length and $\{0, 1\}^n$ is the set of bit strings of a fixed length n. The function $\mathcal{H}$ is said to be

- **Collision resistant** if it is *computationally infeasible* to find $m, m' \in \{0, 1\}^*$, $m \neq m'$, such that $\mathcal{H}(m) = \mathcal{H}(m')$,
- **Second preimage resistant** if $m \in \{0, 1\}^*$ is given, it is *computationally infeasible* to find $m' \in \{0, 1\}^*$, $m \neq m'$, such that $\mathcal{H}(m) = \mathcal{H}(m')$,

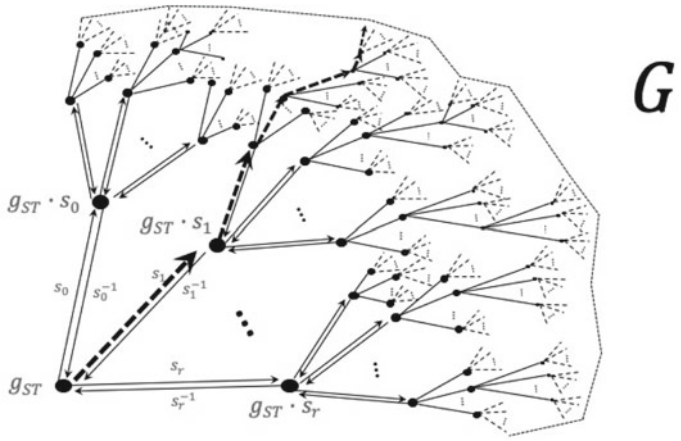

Fig. 1 Diffusion from the starting vertex g_{ST} along Cayley graphs over G with respect to $S = \{s_0, \ldots, s_r\}$

- **Preimage resistant** if $h \in \{0,1\}^n$ is given, it is *computationally infeasible* to find $m \in \{0,1\}^*$ such that $h = \mathcal{H}(m)$.

Let G be a non-commutative group and $S = \{s_0, \ldots, s_r\} \subset G$ be a generating set for the group G, symmetric and not having the identity. Charles et al. (2009a) and Petit et al. (2007), Petit and Quisquater (2010b) described a definition of Cayley hash functions, by which the input to hash is used as directions for walking around a graph, and the ending vertex is the output of the hash function as depicted in Fig. 1.

A message m is given as a string $m_1 \ldots m_\ell$, where $m_i \in \{0, \ldots, r\}$. Then the resulting hashing value h of m will be obtained as a group product

$$h := \mathcal{H}(m) = g_{ST} s_{m_1} s_{m_2} \ldots s_{m_\ell},$$

where g_{ST} is a fixed starting element in G. (We usually put g_{ST} as the identity in G.) To dispose a proper sequence of hashing bits inductively, we define a *choice function* π which assigns a next hashing bit with the bit of the message m and the previous hashing bit, while avoiding a back-tracking (i.e. ss^{-1} or $s^{-1}s$). We choose a function

$$\pi : \{0, \ldots, r\} \times S \to S \tag{2}$$

such that for any $s \in S$ the set $\pi(\{0, \ldots, r\} \times \{s\})$ is equal to $S \setminus \{s^{-1}\}$.

The security of Cayley hash functions lies on the hardness of solving *word problems* for group theory (Lubotzky 1994; Meier 2008; Petit and Quisquater 2010b), which are one of the most challenging open problems. There are three problems (*balance, representation and factorization problems*), which are related to the three properties of Cayley hash functions, respectively.

Let $L \in \mathbb{N}$ be small (approximately, $\log |G|$). We denote the product of group elements $s_{m_1}, s_{m_2}, \ldots, s_{m_\ell}$ by $\prod s_{m_i} = s_{m_1} s_{m_2} \ldots s_{m_\ell}$.

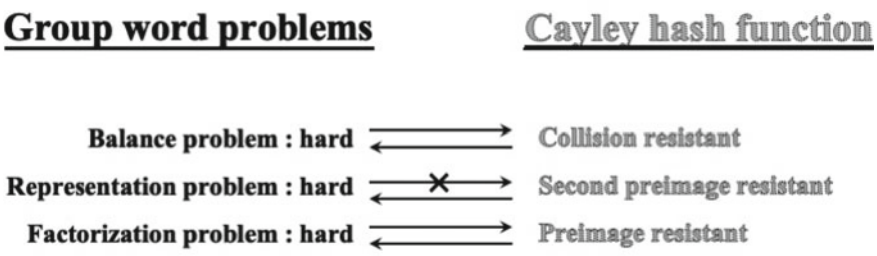

Fig. 2 Relationship between the properties of Cayley hash functions and the hardness of Group word problems

- **Balance problem** : Find an "efficient" algorithm that returns two words $m_1 \dots m_\ell$ and $m'_1 \dots m'_{\ell'}$ with $\ell, \ell' < L, m_i, m'_i \in \{0, \dots, r\}$ and $\prod s_{m_i} = \prod s_{m'_i}$.
- **Representation problem** : Find an "efficient" algorithm that returns a word $m_1 \dots m_\ell$ with $\ell < L, m_i \in \{0, \dots, r\}$ and $\prod s_{m_i} = 1$.
- **Factorization problem** : Find an "efficient" algorithm that given any element $g \in G$, returns a word $m_1 \dots m_\ell$ with $\ell < L, m_i \in \{0, \dots, r\}$ and $\prod s_{m_i} = g$.

A Cayley hash function is collision resistant if and only if the balance problem is hard; it is second preimage resistant only if the representation problem is hard; it is preimage resistant if and only if the corresponding factorization problem is hard (as described in Fig. 2).

The *diameter* of a Cayley graph over G with respect to S, which naturally came up from the problems above, is defined as the smallest ℓ such that every element of G can be expressed as a word of length at most ℓ in S. Babai and Seress (1992) conjectured that the diameter of any Cayley graph over any non-commutative simple group is polylogarithmic in the size of the group such as $\exp((|G| \log |G|)^{1/2}(1 + o(|G|)))$. Helfgott and Seress (2014) gave a quasipolynomial upper bound $\exp(\log \log |G|)^{O(1)}$, which is the best known upper bound for permutation groups.

Even after more than two decades of research in various areas (pure mathematics, computer sciences, cryptography, etc.), the hardness of the word problems is still difficult to break. For example, since suggested in Petit and Quisquater (2010b) as a challenge, it seems still open to solve the balance/representation/factorization problems for $G = \mathrm{SL}_2(\mathbb{F}_{2^n})$ with some specific generating set, which is tweaked from the generating set of Tillich and Zémor (1994). They also mentioned that it is an important challenge that we identify groups and their corresponding specific generating sets for the groups in which the balance, representation and factorization problems are difficult.

2.2 *Lifting Attacks*

In Zémor (1991), proposed the first scheme of hash functions from Cayley graphs upon SL_2 over a finite field having a large *girth*, which is the length of a shortest

cycle. Right after the advent, Tillich and Zémor found a way to break Zémor's scheme by a *lifting attack* and suggested its improved version with SL_2 over a finite field of characteristic 2. Tillich–Zémor's scheme (Tillich and Zémor 1994) in resisted being cryptanalyzed for a decade and a half until Grassl et al. (2010) and Petit et al. (2009), Petit and Quisquater (2010a) found their collisions and even preimages in practical. A critical observation for both attacks is that the hardness of balance/representation/factorization problems does not change if we replace the generators for $\mathrm{SL}_2(\mathbb{F}_{2^n})$ in order to use the Euclidean algorithm. Even Cayley hash functions based on LPS Ramanujan graphs proposed from Charles et al. (2009a) have been broken by Tillich and Zémor (2008) using a variant of a *lifting attack*.

In this subsection, we give a brief example of a lifting attack, which was used by Tillich and Zémor (2008). We have conditions on distinct prime numbers p and q that p and q satisfy $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. First, the elements of $\mathrm{PSL}_2(\mathbb{F}_q)$ are lifted to elements of $\mathrm{SL}_2(\mathbb{Z}[\mathrm{i}])$, where i is the imaginary unit. Even though the lifts of the generators do not generate the whole $\mathrm{SL}_2(\mathbb{Z}[\mathrm{i}])$ and only a subset Ω of $\mathrm{SL}_2(\mathbb{Z}[\mathrm{i}])$ with specific conditions shown in Tillich and Zèmor (2008), the lifting attack still works because Ω has a very simple nature as shown below.

$$\Omega = \left\{ \begin{bmatrix} x + \mathrm{i}y & z + \mathrm{i}w \\ -z + \mathrm{i}w & x - \mathrm{i}y \end{bmatrix} \middle| (x, y, z, w) \in E_\ell \text{ for some integer } \ell > 0 \right\},$$

where E_ℓ is the set of 4-tuples $(x, y, z, w) \in \mathbb{Z}^4$ such that

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = p^\ell & \\ x > 0, x \equiv 1 & \pmod 2 \\ y \equiv z \equiv w \equiv 0 & \pmod 2. \end{cases}$$

Tillich and Zémor solved the *representation problem* by lifting the identity to Ω, which amounts to solving the norm equation

$$(\lambda + xq)^2 + 4(yq)^2 + 4(zq)^2 + 4(wq)^2 = p^\ell \tag{3}$$

with $\lambda, x, y, z, w \in \mathbb{Z}$ and $\ell \in \mathbb{N}$ (Once the identity is lifted, reduction by q and factoring become trivial). The equation is solved as follows: we arbitrarily fix $\ell = 2\ell'$ with $p^{\ell'} > mq^2$ and $\lambda + xq = p^{\ell'} - 2mq^2$ for some m. We substitute them for each variable in the norm Eq. (3). The norm equation can be deformed by $4q^2$, resulting in the equation of the form $y^2 + z^2 + w^2 = N := m(p^{\ell'} - mq^2)$.

The last equation is solved by generating random variables for w, checking the right parity to ensure that the resulting equation $y^2 + z^2 = N' := N - w^2$ has a solution, and we finally solve this equation with the continued fraction method (or with the advanced Euclidean algorithm, Cornacchia's algorithm, Pell's equation).

Subsequently, most of the existing Cayley hash functions based on explicit Ramanujan graphs Chiu (1988), Lubotzky (1994), Morgenstern (1992) have been broken by variants of a lifting attack Jo et al. (2008), Petit et al. (2008), Tillich and Zémor (2017) as lifting attacks are able to solve the factorization/representation problems for each case. As we can see in Table 1, when we attack Cayley hash func-

Table 1 Norm equations and N to Euclidean algorithm for Cryptanalysis on Cayley hashes

Ramanujan graphs	Norm equation and N for Euclidean algorithm
LPS's Ramanujan graph (Lubotzky 1988)	$x^2 + y^2 + z^2 + w^2 = p^\ell$ $N := p^\ell - z^2 - w^2$
Chiu's Ramanujan graph ($p = 2$) (Chiu 1992)	$x^2 + 2y^2 + 13z^2 + 26w^2 = 2^\ell$ $N := 2^\ell - 13z^2 - 26w^2$
LPS-type Ramanujan graph (Jo et al. 2020)	$x^2 + Py^2 + Qz^2 + PQw^2 = p^\ell$ $N := p^\ell - Qz^2 - PQw^2$

tions, we can apply a lifting attack, which corresponds to a norm equation of their base algebra with a Euclidean algorithm.

Thus, we want to make explicit Ramanujan graphs which have more various norm equations that use P and Q as coefficients ($P \in \{2, 3, 5, 7, 13\}$ and $Q \in \mathbb{P}$ satisfying $Q \equiv 3 \pmod 8$, $\left(\frac{-Q}{P}\right) = -1$ unless $P = 2$). At the very least, for applying variants of a lifting attack, we should set up an attack corresponding to each norm equation. It is also possible to put partial information (P, Q or both) unrevealed during the process of hashing as a private key. From this, we can build the digital signature schemes which mainly resist variants of a lifting attack. This motivates the study of a generalization of LPS's and Chiu's Ramanujan graphs.

3 The Families of LPS-Type Graphs

Now we recall Ibukiyama's construction (Ibukiyama 1982) of maximal orders of definite quaternion algebras over $\mathbb{Q}$ which is ramified at given primes.

Proposition 1 (Ibukiyama 1982) *Let r be an odd positive integer and $P_1, P_2, \ldots, P_r$ distinct prime numbers. Set $M = P_1 P_2 \cdots P_r$. Take a prime number Q such that $Q \equiv 3 \pmod 8$ and $(\frac{-Q}{P_i}) = -1$ for all i except for i with $P_i = 2$. Moreover, take an integer T such that $T^2 \equiv -M \pmod Q$. Then, $\mathcal{A}_{\mathbb{Q}}(-M, -Q)$ is a definite quaternion algebra which is ramified only at $\infty, P_1, P_2, \ldots, P_r$. Moreover, let*

$$\omega_1 = \frac{1 + j}{2}, \quad \omega_2 = \frac{i + k}{2} \quad \text{and} \quad \omega_3 = \frac{Tj + k}{Q}.$$

Then, $O_{-M,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ is a maximal order of $\mathcal{A}_{\mathbb{Q}}(-M, -Q)$.

In Jo et al. (2020, 2018) a specific recipe for constructing LPS-type graphs is presented, and is shown below:

1. Fix a $p \in \mathbb{P}$.
2. Take $P \in \{2, 3, 5, 7, 13\}$ such that $P \neq p$.
3. We take a prime Q satisfying

$$Q \equiv 3 \pmod 8, \left(\frac{-Q}{P}\right) = -1 \text{ unless } P = 2$$

and an integer T satisfying $T^2 \equiv -P \pmod Q$. By Proposition 1, we have a definite quaternion algebra $\mathcal{A}_{\mathbb{Q}}(-P, -Q)$ (i.e., $i^2 = -P$, $j^2 = -Q$, $ij = -ji = k$) and its maximal order $O = O_{-P,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ with class number 1, where

$$\omega_1 = \frac{1+j}{2}, \ \omega_2 = \frac{i+k}{2} \text{ and } \omega_3 = \frac{Tj+k}{Q}.$$

4. Find all elements in $O^\times = \{\alpha \in O \mid N(\alpha) = 1\}$.
5. Find all elements in $\{\alpha \in O \mid N(\alpha) = p\}$. Moreover, seek a suitable complete representative of $\{\alpha \in O \mid N(\alpha) = p\}/O^\times$. Define S by the suitable complete representative. Then $|S|$ is exactly equal to $p + 1$, which follows by the class number 1 condition Chiu (1992, Proposition 3.4).
6. Take a $q \in \mathbb{P} \setminus \{2\}$ satisfying $q \neq p$, $\left(\frac{-P}{q}\right) = \left(\frac{Q}{q}\right) = 1$ and $\left(\frac{p}{q}\right) = 1$.
7. Via the isomorphism ψ_q in Lemma 1 and using Lemma 2, we realize S as a subset of $\mathrm{PSL}_2(\mathbb{F}_q)$. Write S_{JSY} for the subset.
8. We have a Cayley graph $X_{P,Q}^{(p,q)} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S_{JSY})$.

In Table 2, we present some numerical results by Magma and MATLAB which show the Ramanujan-ness of our constructions. Actually, we will show in the next subsection that our LPS-type graphs are Ramanujan when $P = 13$, which is the only choice of $P \in \{2, 3, 5, 7, 13\}$ such that $O^\times$ is equal to $\{\pm 1\}$. For the cases of $P \in \{2, 3, 5, 7\}$, at present, we have no ideas to prove or disprove the Ramanujan-ness of our graphs.

Table 2 Numerical results on the Ramanujan-ness of LPS-type graphs $X = X_{P,Q}^{(p,q)}$

p	Parameters (P, Q, q, T)	$\lambda_1(X)$	$2\sqrt{p}$ (RB)	$\lvert V(X)\rvert = q(q^2-1)/2$
2	(13, 11, 7, 3)	2.7253	2.8284	168
3	(2, 3, 11, 1)	3.3322	3.4641	660
5	(2, 3, 11, 1)	4.4718	4.4721	660
7	(5, 67, 3, 14)	3	5.2915	12
11	(13, 11, 7, 3)	6	6.6332	168

3.1 Proof of the Ramanujan-Ness of Graphs $X_{P,Q}^{(p,q)}$ when $P = 13$

We show that our graph $X_{P,Q}^{(p,q)}$ constructed as above is Ramanujan when $P = 13$. Let $O = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ be the maximal order we constructed as above for a fixed p, P, Q, T. Then, O has the class number 1.

Take a complete representative $S_{JSY} = \{\alpha_1, \ldots, \alpha_s\} \cup \{\bar{\alpha}_1, \ldots, \bar{\alpha}_s\} \cup \{\beta_1, \ldots, \beta_t\}$ of $\{\alpha \in O \mid N(\alpha) = p\}/O^\times$ so that $\bar{\beta}_j = \epsilon_j \beta_j$ for some $\epsilon_j \in O^\times$ for every j. In this case, $p + 1 = 2s + t$. In the same way as Coan and Perng (2012, Theorem 4.8) and Lubotzky (1988, Lemma 3.1), we have the following:

Lemma 3 *Any $\alpha \in O$ with $N(\alpha) = p^k$ for some $k \in \mathbb{N}$ is uniquely decomposed into the product*

$$\alpha = \epsilon p^r R(\alpha_1, \ldots, \alpha_s, \bar{\alpha}_1, \ldots, \bar{\alpha}_s, \beta_1, \ldots, \beta_t),$$

where $\epsilon \in O^\times$, $r \in \mathbb{N}$ and $R(\alpha_1, \ldots, \alpha_s, \bar{\alpha}_1, \ldots, \bar{\alpha}_s, \beta_1, \ldots, \beta_t)$ is a reduced word of $\alpha_1, \ldots, \alpha_s, \bar{\alpha}_1, \ldots, \bar{\alpha}_s, \beta_1, \ldots, \beta_t$ with length $m = k - 2r$.

The unit group $O^\times$ is $\{\pm 1\}$ only when $P = 13$. In such a case, we can prove the Ramanujan-ness of our graph $X_{P,Q}^{(p,q)}$ in the same way as Lubotzky (1988). For the variable $v = (x, y, z, w)$, we set

$$\begin{aligned} Q_q(v) = {} & x^2 + qxy + q^2\left(\frac{1+Q}{4}\right)y^2 + q^2 Tyz \\ & + q^2 P\left(\frac{1+Q}{4}\right)z^2 + q^2 Pzw + q^2\left(\frac{P+T^2}{Q}\right)w^2. \end{aligned}$$

It is a positive-definite quadratic form of order 4 corresponding to the reduced norm on O. Let A_q be the symmetric matrix such that $Q_q(v) = \frac{1}{2}{}^t v A_q v$, i.e.

$$A_q = \begin{bmatrix} 2 & q & 0 & 0 \\ q & \frac{q^2(1+Q)}{2} & 0 & q^2 T \\ 0 & 0 & \frac{q^2 P(1+Q)}{2} & q^2 P \\ 0 & q^2 T & q^2 P & 2q^2\frac{P+T^2}{Q} \end{bmatrix}.$$

Hence, A_q is an even matrix, i.e. $A_q \in \mathrm{M}_4(\mathbb{Z})$ and every diagonal component is contained in $2\mathbb{Z}$. The *level* of Q_q is defined as the smallest positive integer N such that NA_q^{-1} is an even matrix (cf. Schoeneberg 2012, Chap. IX). By $\det(A_q) = P^2 q^6$ and

$$A_q^{-1} = \frac{1}{P^2 q^6}\begin{bmatrix} q^6\frac{1+Q}{2}P(\frac{P+T^2}{Q}) & -q^5 P\left(\frac{P+T^2}{Q} + T^2\right) & -q^5 PT & q^5 PT\frac{1+Q}{2} \\ -q^5 P\left(\frac{P+T^2}{Q} + T^2\right) & 2q^4 P(\frac{P+T^2}{Q} + T^2) & 2q^4 PT & -q^4 PT(1+Q) \\ -q^5 PT & 2q^4 PT & 2q^4 P & -PQq^4 \\ q^5 PT\frac{1+Q}{2} & -q^4 PT(1+Q) & -PQq^4 & q^4 PQ\frac{(1+Q)}{2} \end{bmatrix},$$

the level of Q_q is equal to Pq^2.

Set $r_{Q_q}(n) := |\{\alpha \in O \mid N(\alpha) = n\}|$ for $n \in \mathbb{N}$. Then, the theta series $\Theta_{Q_q}(z) := \sum_{n=0}^{\infty} r_{Q_q}(n) e^{2\pi i n z} = \sum_{v \in \mathbb{Z}^4} e^{2\pi i Q_q(v) z}$ for $z \in \mathbb{C}$ with $\mathrm{Im}(z) > 0$ is absolutely and locally uniformly convergent by Schoeneberg (2012, Chap. IX, Sect. 1.1). Referring to Schoeneberg (2012, Chap. IX, Theorem 4) and Schoeneberg (2012, Chap. IX, Theorem 5) for $\mathbf{h} = \mathbf{0}$, the theta series $\Theta_{Q_q}(z)$ is a holomorphic modular form of weight 2 and level $\Gamma_0(Pq^2)$ with trivial nebentypus. Here, $\Gamma_0(Pq^2)$ is the Hecke congruence subgroup of level Pq^2. We remark that Q_q, A_q, Θ_{Q_q}, are valid for a general $q \in \mathbb{N}$.

Assume $P = 13$. Let Λ' be the set of all $\alpha \in O$ such that $N(\alpha) = p^k$ for some $k \in \mathbb{N}$. We define an equivalence relation on Λ so that $\alpha \sim \beta$ means $\alpha = \epsilon p^n \beta$ for some $\epsilon \in O^\times$ and $n \in \mathbb{Z}$. Since $O^\times = \{\pm 1\}$ holds, the quotient set $\Lambda := \Lambda'/\sim = \{[\alpha] \mid \alpha \in \Lambda'\}$ has a natural group structure by $[\alpha][\beta] = [\alpha\beta]$. By Lemma 3, it is generated by S_{JSY}, a complete representative of $\{\alpha \in O \mid N(\alpha) = p\}/O^\times$, and $\mathrm{Cay}(\Lambda, S_{JSY})$ is a $(p+1)$-regular tree. The homomorphism $\Lambda \to \mathrm{PSL}_2(\mathbb{F}_q)$ as a restriction of ψ_q of Lemma 1 induces $\Lambda/\Lambda(q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ with $\Lambda(q) = \ker(\psi_q|_\Lambda)$. This homomorphism $\Lambda/\Lambda(q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ is surjective as in the theory of quadratic diophantine equations applied to the quadratic form Q_1 (cf. Lubotzky et al. 1988, p. 267; Malishev 1962). Then our graph $X^{(p,q)}_{13,Q} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S_{JSY})$ is identified with $\Lambda/\Lambda(q)$ as a graph.

For proving Ramanujan-ness, let $\lambda_0 = p + 1 > \lambda_1 \geq \cdots \geq \lambda_{n-1}$ be the spectrum of the adjacency matrix of $X^{(p,q)}_{13,Q}$ (so we set $n = |X^{(p,q)}_{13,Q}| = |\mathrm{PSL}_2(\mathbb{F}_q)|$). Then, we have only to show $\theta_j \in \mathbb{R}$ for all $j \in \{1, \ldots, n-1\}$, where $\theta_j \in \mathbb{C}$ is taken so that $\lambda_j = 2\sqrt{p}\cos\theta_j$ for each $j \in \{0, \ldots, n-1\}$. By the trace formula for a regular graph as in Lubotzky (1988, p. 270–272 and p. 274, Remark 2), we have the expression

$$r_{Q_q}(p^k) = \frac{2p^{k/2}}{n} \sum_{j=0}^{n-1} \frac{\sin(k+1)\theta_j}{\sin\theta_j}.$$

Recall that this is the p^k-th Fourier coefficient of the modular form Θ_{Q_q}. Since the theta series is a sum of a linear combination of cuspidal Hecke eigenforms and that of Eisenstein series of weight 2 and level $\Gamma_0(Pq^2)$, we may take a cusp form f_1 and a non-cusp form f_2 of weight 2 so that $\Theta_{Q_q} = f_1 + f_2$. Let $a(m)$ and $C(m)$ be the m-th Fourier coefficients of f_1 and f_2 at the cusp ∞ for $m \in \mathbb{N}$, respectively. Then, $r_{Q_q}(p^k)$ has the following expression:

$$C(p^k) + a(p^k) = r_{Q_q}(p^k) = \frac{2p^{k/2}}{n} \sum_{j=0}^{n-1} \frac{\sin(k+1)\theta_j}{\sin\theta_j}.$$

By Deligne's bound as a resolution of the Ramanujan–Petersson conjecture (Deligne 1969, 1974), we have $|a(p^k)| = O_\epsilon(p^{k(1/2+\epsilon)})$. Due to the explicit nature of Fourier coefficients of Eisenstein series, $C(m)$ can be described as $C(m) = \sum_{d|m} F(d)$ for

a periodic function $F : \mathbb{N} \to \mathbb{C}$ (cf. Lubotzky 1988, p. 272). By $\left(\frac{p}{q}\right) = 1$ and $\theta_0 = i \log \sqrt{p}$, we have

$$C(p^k) = \frac{2}{n}\frac{p^{k+1}-1}{p-1} - a(p^k) + o(p^k) = \frac{2}{n}\frac{p^{k+1}-1}{p-1} + o(p^k).$$

By the Deligne bound of $a(p^k)$ and Lubotzky (1988, Lemma 4.4), we have $C(p^k) = \frac{2}{n}\frac{p^{k+1}-1}{p-1}$ because of $\left(\frac{p}{q}\right) = 1$. As a consequence, for any $\epsilon > 0$,

$$\frac{2}{n}\sum_{j=1}^{n-1}\frac{\sin(k+1)\theta_j}{\sin\theta_j} = \frac{1}{p^{k/2}}O_\epsilon(p^{k(1/2+\epsilon)}) = O_\epsilon(p^{k\epsilon}),$$

which leads us that every θ_j for $j \in \{1, \ldots, n-1\}$ is real. Therefore, we obtain $|\lambda_j| \leq 2\sqrt{p}$ for all $j = 1, \ldots, n-1$, which implies that $X^{(p,q)}_{13,Q}$ is a Ramanujan graph.

We remark an adelic approach toward Ramanujan-ness. As we see Costache et al. (2018, Sect. 7.2) (see also Lubotzky 1994, Theorem 7.1.1), we can prove the Ramanujan-ness of $X^{(p,q)}_{P,Q}$ for $P = 13$ by using an adelic interpretation as well as by using the Jacquet–Langlands correspondence between automorphic representations of the adelic group $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ and those of $\mathcal{A}^\times(\mathbb{A}_\mathbb{Q}) = (\mathcal{A} \otimes \mathbb{A}_\mathbb{Q})^\times$, which is the adelization of the anisotropic inner form $\mathcal{A}^\times$ of GL_2.

4 Relationship Between LPS-Type Graphs and Pizer's Graphs

While research in the field of Cayley-based cryptography has been declining, research in the field of Isogeny-based cryptography is quite robust, in part due to its key role in post-quantum cryptography.

However, it is also natural to investigate whether attacks on group word problems of Cayley hash functions based on LPS's graphs are related to the problem of finding a path in an isogeny graph of supersingular elliptic curves, which is explained in detail in Charles et al. (2009b).

Costache et al. (2018) described a wide range of usage of Ramanujan graphs in cryptography and also pointed out some different aspects of LPS's graphs and Pizer's graphs with specific features. They presented the construction of LPS's graphs as Cayley graphs, in terms of local double cosets. They used strong approximation (Costache et al. 2018, Sect. 7; Lubotzky 1994, Sect. 6.3) as a main tool to present the connection between local and adelic double cosets for LPS's and Pizer's graphs. They also compared the two types of graphs in an aspect of appearance by restricting the degree of the graphs (i.e. $p = 5$).

In this section, we give some comparisons between LPS-type graphs and Pizer's graphs as Costache et al. did. First, we describe Pizer's Ramanujan graphs referred to in Pizer (1990, 1998), Costache et al. (2018).

The families of Pizer's graphs Pizer (1990, 1998) showed how to construct the family of Ramanujan graphs as follows: Let $\mathcal{A}$ be the quaternion algebra over $\mathbb{Q}$ that is ramified exactly at odd $q \in \mathbb{P}$ and ∞. We shall consider special orders, which are generalizations of Eichler orders, of level $L = (q, M)$ and $L = (q^2, M)$. The vertex set of Pizer's graph $G(L, p)$ shall be in bijection with (a subset of) the isomorphism classes of left ideals of an order. Since the class number of the order depends only on its level, we may write $H(L)$ for it, which is equal to the size of such a graph. Notice that, by Pizer (1998, Proposition 4.4), we have

$$H(q, M) = \frac{q-1}{12} M \prod_{d|M} (1 + 1/d) + \begin{cases} \frac{1}{4}\left(1 - \left(\frac{-4}{q}\right)\right) \prod_{d|M} \left(1 + \left(\frac{-4}{d}\right)\right) & \text{if } 4 \nmid M \\ 0 & 4 \mid M \end{cases} + \begin{cases} \frac{1}{3}\left(1 - \left(\frac{-3}{q}\right)\right) \prod_{d|M} \left(1 + \left(\frac{-3}{d}\right)\right) & \text{if } 9 \nmid M \\ 0 & \text{if } 9 \mid M \end{cases}$$

and

$$H(q^2, M) = \frac{q^2-1}{12} M \prod_{d|M} (1 + 1/d) + \begin{cases} 0 & \text{if } q \geq 5 \\ \frac{4}{3} \prod_{d|M} \left(1 + \left(\frac{-3}{d}\right)\right) & \text{if } q = 3. \end{cases}$$

Here, the product is over all primes d dividing M.

We give a definition of a Brandt matrix. Let $\{I_1, I_2, \ldots, I_H\}$ with $H = H(L)$ be a complete representative of the left ideal classes of $\mathcal{O}$. For each $i \in \{1, \ldots, H\}$, let $\mathcal{O}_i$ be the right order of the ideal I_i, and e_i be the number of $\mathcal{O}_i^\times$. For $n \in \mathbb{N}$, the *Brandt matrix* $B(L; n) = \left[b_{i,j}^{(n)}\right]$ associated to an order of level L is a square matrix of size $H(L)$ having (i, j)-entry

$$b_{i,j}^{(n)} = e_j^{-1} \cdot |\{\alpha \in I_j^{-1} I_i \mid N(\alpha) N(I_j)/N(I_i) = n\}|,$$

where $N(I)$ is the norm of an ideal I defined as the greatest common divisor of the norms of its nonzero elements. Let p be a prime which is coprime to qM. If we restrict the parameters p and q, the edge set of $G(L, p)$ is given by a Brandt matrix $B(L; p)$, namely, the adjacency matrix of $G(L, p)$ is given by $B(L; p)$. By Pizer (1998, Proposition 4.6), we see that $G(L, p)$ is undirected (i.e. $B(L; p)$ is symmetric) when $L = (q, M)$ with $q \equiv 1 \pmod{12}$ and $L = (q^2, M)$ with $q > 3$. Moreover, it has no loops if $\mathrm{tr}\, B(L; p) = 0$ and no multiple edges if $\mathrm{tr}\, B(L; p^2) = H(L)$ (Costache et al. 2018; Pizer 1998). The regularity $p + 1$

Table 3 The families of Pizer's graphs $G(L, p)$

Conditions \ Level	$L = (q, M)$	$L = (q^2, M)$	
Coprimality	$(p, qM) = 1$		
Bipartite-ness	non-bipartite	if $\left(\frac{p}{q}\right) = -1$ bipartite	if $\left(\frac{p}{q}\right) = 1$ non-bipartite
# of vertices	$H(L)$	$H(L)$	$H(L)/2$
Undirected-ness	$q \equiv 1 \pmod{12}$	$q > 3$	
No loops	$\mathrm{tr}B(L; p) = 0$		
No multiple edges	$\mathrm{tr}B(L; p^2) = H(L)$		
Regularity	$(p + 1)$-regular		

of $G(L, p)$ and its connectedness can be obtained from using $B(L; p)$ as the adjacency matrix, as shown in Pizer (1998, Proposition 5.1). We summarize the necessary properties of the families of Pizer's graphs $G(L, p)$ in Table 3.

4.1 Similarities and Differences

As Costache et al. (2018) argued, we explicate the similarities and differences among LPS, LPS-type and Pizer's graphs from a number-theoretic perspective. These families can be viewed as sets of local double cosets, i.e. as graphs of the form

$$\Gamma \backslash \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p),$$

where Γ is a discrete cocompact subgroup.

Discrete local double cosets (LPS-type) Let p be a split prime in $\mathcal{A}$. For $N \in \mathbb{N}$, we set

$$\Gamma(N) := \ker(\mathcal{A}^\times(\mathbb{Z}[p^{-1}]) \to \mathbb{Z}[p^{-1}]^\times \backslash \mathcal{A}^\times(\mathbb{Z}[p^{-1}]/N\mathbb{Z})).$$

It is a discrete cocompact subgroup in $\mathcal{A}_p^\times$. We have

$$\mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S) \cong \Gamma(q) \backslash \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$$

for some suitable S.

For LPS-type graphs, the local double cosets are also isomorphic to adelic double cosets, but in this case the corresponding set of adelic double cosets is smaller relative to the quaternion algebra and we do not have the same chain of isomorphisms as shown below. On the other hand, Pizer's graphs, via strong approximation (Costache et al. 2018; Lubotzky 1994), can be viewed as graphs on adelic double cosets which are in turn the set of classes of an order of $\mathcal{A}$ that is related to a discrete cocompact

subgroup Γ. Moreover, the class set $\mathrm{Cl}(\mathcal{O})$ of a maximal order $\mathcal{O}$ from Pizer's graph is in bijection with supersingular elliptic curves (Charles et al. 2009b, Sect. 5.3.1) and offers convincing evidence that an isomorphism is obtained with a supersingular isogeny graph (SSIG).

The chain of isomorphisms
(**LPS**)

$$\mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S_{LPS}) \cong \Gamma(2q)\backslash \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$$

(**LPS-type with** $P = 13$)

$$\mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S_{JSY}) \cong \Gamma(q)\backslash \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$$

(**Pizer**)

$$\mathcal{O}[p^{-1}]^{\times}\backslash \mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p) \cong \mathrm{Cl}(\mathcal{O}) \cong \mathrm{SSIG}$$

Each of the underlying quaternion algebras vary with their own choice of parameters. In the case of LPS's graphs, we use the Hamiltonian quaternion algebra, ramified at 2 and ∞ and split at p. In the case of LPS-type graphs, we use the definite quaternion algebra, ramified at 13 and ∞ and split at p. Varying the parameter q, we can have different Ramanujan graphs of LPS and LPS-type, depending on the congruence subgroup $\Gamma(2q)$ and $\Gamma(q)$, respectively, without changing each of their underlying quaternion algebras. On the other hand, in the case of Pizer's graphs, we use the definite quaternion algebra, ramified at q and ∞.

5 Open Problems

It is unknown whether the link exists between the hardness of the path-finding problem in Supersingular Isogeny (Pizer) graphs and the the hardness of group word problems in Cayley-type Ramanujan graphs. If it is possible to connect those two problems theoretically or schematically, there are some expected ways to analyze the hardness of the path-finding problem in Pizer's graphs by employing the approach previously used for Cayley graphs. As a part of these approaches, it is also important to investigate much more general versions of explicit constructions of Ramanujan graphs. It is in the process to construct the family of $(2p + 1)$-regular graphs, where p is an Eichler prime based on the quaternion algebra with an explicit construction of Eichler order having class number 1 in Jo et al. (2020). We now study the Ramanujan-ness of these graphs by similar arguments in LPS-type graphs.

Additionally, even though it is difficult to predict that Pizer's graph can be represented as a Cayley graph over a group with respect to a suitable generating set (actually, all graphs with a small number of vertices, suggested as examples in Pizer

1998 are not Cayley graphs), it is not clear whether a Pizer's graph with a sufficiently large number of vertices is a Cayley graph or not.

Acknowledgements This work was supported by JST CREST Grant Number JPMJCR14D6, Japan. The authors would like to thank Meghan Delaney for pointing out grammatical errors.

References

N. Alon, V. Milman, λ_1, isoperimetric inequalities for graphs, and superconcentrators. J. Comb. Theory. B. **38**(1), 73–88 (1985)

L. Babai, Á. Seress, On the diameter of permutation groups. European. J. Combin. **13**(4), 231–243 (1992)

J.F. Basilla, On the solution of $x^2 + dy^2 = m$. P. Jpn. Acad. A-Math **80**(5), 40–41 (2004)

J.F. Biasse, D. Jao, A. Sankar, A quantum algorithm for computing isogenies between supersingular elliptic curves. Indocrypt LNCS **8885**, 428–442 (2014)

D.X. Charles, E.Z. Goren, K.E. Lauter, Cryptographic hash functions from expander graphs. J. Cryptol. **22**(1), 93–113 (2009a)

D.X. Charles, E.Z. Goren, K.E. Lauter, Families of Ramanujan graphs and quaternion algebras. Groups and symmetries, in *CRM Proceedings and Lecture Notes*, vol. 47 (American Mathematical Society, Providence, RI, 2009b), 53–80

P. Chiu, Cubic Ramanujan graphs. Combinatorica **12**(3), 275–285 (1992)

B. Coan, C. Perng, Factorization of Hurwitz quaternions. Int. Math. Forum **7**(41–44), 2143–2156 (2012)

A. Costache, B. Feigon, K.E. Lauter, M. Massierer, A. Puskás, Ramanujan graphs in cryptography. arXiv:1806.05709 (2018)

G. Davidoff, P. Sarnak, A. Valette, *Elementary Number Theory, Group Theory and Ramanujan Graphs* (Cambridge University Press, Cambridge, 2003)

L. De Feo, D. Jao, J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol. **8**(3), 209–247 (2014)

P. Deligne, Formes modulaires et représentations l-adiques, Séminaire N. Bourbaki, exp. n°, 139–172 (1968–1969)

P. Deligne, La conjecture de Weil. I, Inst. Hautes Études Sci. Publ. Math. **43**, 273–307 (1974)

J. Dodziuk, Difference equations, isoperimetric inequality and transience of certain random walks. T. Am. Math. Soc. **284**(2), 787–794 (1984)

M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren. J. Reine Angew. Math. **195**(1955), 127–151 (1956)

M. Eichler, S. Sundaravaradan, Lectures on modular correspondences. Tata Institute of Fundamental Research (1956) Available via DIALOG. http://www.math.tifr.res.in/~publ/ln/tifr09.pdf

M. Eichler, The basis problem for modular forms and the traces of the Hecke operators, in *Modular Functions of One Variable*, vol. 320 ed. by W. Kuyk (Springer, Heidelberg, 1973), 75–152

M. Grassl, I. Ilić, S. Magliveras, R. Steinwandt, Cryptanalysis of the Tillich-Zémor Hash Function. J. Cryptol. **24**(1), 148–156 (2010)

O. Goldreich, *Foundations of Cryptography* (Cambridge University Press, Cambridge, 2004)

H.A. Helfgott, Á. Seress, On the diameter of permutation groups. Ann. Math. **179**, 611–658 (2014)

M. Hirschhorn, A simple proof of Jacobi's four-square theorem. P. Am. Math. Soc. **101**(3), 436–438 (1987)

H. Hoory, N. Linial, A. Wigderson, Expander graphs and their applications. B. Am. Math. Soc. **43**(4), 439–561 (2006)

T. Ibukiyama, A basis and maximal orders of quaternion algebras over the rational number (In Japanese). MSJ, Sugaku **24**(4), 316–318 (1972) https://core.ac.uk/download/pdf/38181256.pdf

T. Ibukiyama, On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. Nagoya. Math. J. **88**, 181–195 (1982)
Y. Ihara, Discrete Subgroups of PL(2, $\mathfrak{k}_\mathfrak{p}$). Proc. Symp. Pure Math. **18**, 272–278 (1966)
H. Jo, C. Petit, T. Takagi, Full cryptanalysis of hash functions based on cubic ramanujan graphs. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **100**(9), 1891–1899 (2017)
H. Jo, S. Sugiyama, Y. Yamasaki, A general explicit construction of LPS-type Ramanujan graphs, in preparation
H. Jo, Y. Yamasaki, LPS-type Ramanujan graphs, in 2018 International Symposium on Information Theory and Its Applications, ISITA 2018, 399–403 (2018)
M. Kirschmer, J. Voight, Algorithmic enumeration of ideal classes for quaternion orders. SIAM J. Comput. **39**(5), 1714–1747 (2010)
A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan graphs. Combinatorica **8**(3), 261–277 (1988)
A. Lubotzky, Discrete groups, expanding graphs and invariant measures (Springer Science Business Mediam, Berlin, 1994)
G. Margulis, Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. Probl. Peredachi. Inf. **24**(1), 51–60 (1988)
A.I. Malishev, On the representation of integers by positive definite forms (in Russian). Trudy Mat. Inst. Steklov. **65**, 1–319 (1962)
J. Meier, *Groups, graphs and trees; an introduction to the geometry of infinite groups* (Cambridge University Press, Cambridge, 2008)
J.F. Mestre, La méthode des graphes. Exemples et applications, in *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata)*, 217–242 (1986)
J.F. Mestre, T.A. Jorza, The Method of Graphs. Examples and Applications. Notes. (2011)
M. Morgenstern, Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. J. Comb. Theory, Ser. B **62**(1), 44–62 (1994)
O. Parzanchevski, P. Sarnak, Super-golden-gates for PU(2). Adv. Math. **327**, 869–901 (2018)
C. Petit, K.E. Lauter, J.J. Quisquater, Cayley hashes: A class of efficient graph-based hash functions, preprint. (2007)
C. Petit, K.E. Lauter, J.J. Quisquater, Full cryptanalysis of LPS and Morgenstern hash functions. SCN LNCS **5229**, 263–277 (2008)
C. Petit, J.J. Quisquater, Preimages for the Tillich-Zémor hash function, in *International Workshop on Selected Areas in Cryptography*. (Springer, Berlin, Heidelberg, 2010), 282–301
C. Petit, J.J. Quisquater, Rubik's for cryptographers. IACR Cryptology ePrint Archive, vol. 638 (2010)
C. Petit, J.J. Quisquater, J.P. Tillich, G. Zémor, Hard and easy components of collision search in the Zémor-Tillich hash function: New attacks and reduced variants with equivalent security, in *Cryptographers' Track at the RSA Conference* (Springer, Berlin, Heidelberg, 2009), 182–194
A.K. Pizer, Type numbers of Eichler orders. J. Reine Angew. Math. **264**, 76–102 (1973)
A.K. Pizer, On the arithmetic of quaternion algebras. Acta Arith. **31**, 61–89 (1976)
A.K. Pizer, Ramanujan graphs and Hecke operators. B. Am. Math. Soc. **23**(1), 127–137 (1990)
A.K. Pizer, Ramanujan graphs. AMS/IP Stud. Adv. Math. **7**, 159–178 (1998)
H.J. Rosson, B.J. Ellison, J.B. Wilson, Trees, Hecke operators, and quadratic forms, preprint. https://www.math.colostate.edu/~jwilson/math/PrePrintTree.pdf
P. Sarnak, *Some Applications of Modular Forms* (Cambridge University Press, Cambridge, 1999)
B. Schoeneberg, Elliptic Modular Functions: An Introduction, vol. 203 (Springer, Berlin, 2012)
A. Terras, *Zeta functions of graphs; a stroll through the garden*, vol. 128 (Cambridge University Press, Cambridge, 2010)
J.P. Tillich, G. Zémor, Hashing with SL_2, in *Annual International Cryptology Conference* (Springer, Berlin, Heidelberg, 1994), 40–49
J.P. Tillich, G. Zèmor, Collisions for the LPS expander graph hash function. Eurocrypt LNCS **3027**, 254–269 (2008)

M.F. Vignéras, *Arithmétique des algèbres de quaternions*. Lecture Notes in Mathematical, vol. 800 (Springer, Berlin, 1980)
G. Zémor, Hash functions and graphs with large girths, in *Workshop on the Theory and Application of Cryptographic Techniques* (Springer, Berlin, Heidelberg, 1991), 508–511