Computer Security Symposium 2019
21 - 24 October 2019

Cayley hash function-map based on LPS-type Ramanujan graphs

Hyungrok Jo[1,a)] Noboru Kunihiro[1,b)] Yoshinori Yamasaki[2,c)]

Abstract: We propose a Cayley hash function-map based on LPS-type Ramanujan graphs, which is expected to resist a variant of a lifting attack. A security of a Cayley hash function-map is inherited from one of Charles et al.'s proposal in '09. We also give an agenda to extend the families of a Cayley hash function-map along the expected theoretical improvements of how to construct explicit LPS-type Ramanujan graphs in general.

Keywords: Cayley hash function, Cayley hash function-map, Ramanujan graph.

1. Introduction

Including the advent of Shor's algorithm [44] in '94, many variants of quantum algorithms have appeared to mainly solve integer factorization, discrete logarithm problem, and elliptic curve discrete logarithm problem. These facts are assumed to threaten the standard cryptographic usages in real life. From these contexts, National Institute of Standards and Technology (NIST) suggests to standardize post-quantum cryptography [33] in '16. Many researchers are investigating on various kinds of cryptographic schemes and their underlying mathematical hard problems which avoid the existing attacks by quantum algorithms.

In 2009, Charles, Goren, and Lauter [5], [6] 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, Phillips, and Sarnak (in short, LPS) [26], which are Cayley graphs over the projective group with respect to well-chosen generating sets. Petit et al. [35] presented the quasi-polynomial time algorithms to find their preimages and collisions via a variant of "lifting attacks". Jo et al. [21] showed that the cryptanalyisis of Cayley hash functions based on Chiu's Ramanujan graphs in a similar way to Petit et al.'s and also suggested the possibilities to avoid lifting attacks and the extension to the explicit Ramanujan graphs as open problems.

This study leads to construct LPS-type Ramanujan graphs [23], [24] whose norm equations are composed of sums of four squares with larger coefficients, not fixed ones as LPS's case and Chiu's case. These facts not only add up a new parameter which can affect the security of their Cayley hash functions but also produce affluent classes for constructing a new generation of a Cayley hash function. In this article, we suggest Cayley hash function-map using infinitely many candidates of LPS-type graphs [23], [24] whose distinct norm equations of based quaternion algebras. A Cayley hash function-map has a potential way to be extended more in general along the expected improvement [23] of LPS-type Ramanujan graphs.

This article is organized as follows: In Section 2, we present some required preliminaries of expander graphs and Ramanujan graphs, and also of quaternion algebra theory. In Section 3, we explain a way to generalize the explicit constructions of LPS-type Ramanujan graphs in the case of "$P = 13$". In Section 4, we design a Cayley hash function-map, primarily, based on Cayley hash function upon LPS-type Ramanujan graphs in the case of "$P = 13$". In Section 5, we mention a security of a Cayley hash function-map against the most powerful cryptanalysis tool "lifting attack". In Section 6, we summarize the arguments in this article and specify some unclarifed problems and the expected follow-up works.

2. Preliminaries: Ramanujan graph and quaternion algebra

2.1 Ramanujan graph

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

[1] Faculty of Engineering, Information and Systems, University of Tsukuba
[2] Graduate School of Science and Engineering, Ehime University
[a)] jo.hyungrok.gb@u.tsukuba.ac.jp
[b)] kunihiro@cs.tsukuba.ac.jp
[c)] yamasaki.yoshinori.mh@ehime-u.ac.jp

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* $e(X)$ of X, which is defined as below, is a discrete analogue of the Cheeger constant in differential geometry [27]:

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

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 $e(X_j)$ satisfies $e(X_j) \geq \epsilon$ 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 [1], [11] that

$$\tfrac{k - \lambda_1}{2} \leq e(X) \leq \sqrt{2k(k - \lambda_1)}.$$

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 [9], [27], [45].

2.2 Quaternion algebra

In order to explain how to construct the families of LPS-type Ramanujan graphs, we recall basic facts and terminologies of quaternion algebras [48].

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 $\mathcal{A} = \mathcal{A}_F(a, b) = \{\alpha = x + yi + zj + wk \,|\, x, y, z, w \in F\}$, 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.

2.2.1 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, $\begin{bmatrix} s & t \\ u & v \end{bmatrix} = \begin{bmatrix} v & -t \\ -u & s \end{bmatrix}$ 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 $\mathrm{SL}_2(\mathbb{F}_q) = \{A \in \mathrm{GL}_2(\mathbb{F}_q) \,|\, \det A = 1\}$. 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. *[9], Chapter 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 $\left(\frac{p}{q}\right) = 1$.*

2.2.2 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 $\mathcal{O}_L(\mathcal{I}) = \{\alpha \in \mathcal{A} \,|\, \alpha\mathcal{I} \subset \mathcal{I}\}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \{\alpha \in \mathcal{A} \,|\, \mathcal{I}\alpha \subset \mathcal{I}\}$). 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 $\mathfrak{h}(\mathcal{O})$ the number of equivalence classes, which is shown to be finite, independent on left or right. We call $\mathfrak{h}(\mathcal{O})$ the *class number* of $\mathcal{O}$.

3. The families of LPS-type graphs

We give the definition of a Cayley graph. 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 $s \in S$. We denote a Cayley graph over G with respect to S as $\mathrm{Cay}(G, S)$.

Now we recall Ibukiyama's construction [19] of maximal orders of definite quaternion algebras over $\mathbb{Q}$ which is ramified at given primes.

Proposition 1 ([19]). *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, $\mathcal{O}_{-M,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ is a maximal order of $\mathcal{A}_{\mathbb{Q}}(-M, -Q)$.

3.1 The recipe

In [23], [24] 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 $\mathcal{O} = \mathcal{O}_{-P,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ 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 $\mathcal{O}^{\times} = \{\alpha \in \mathcal{O} \mid N(\alpha) = 1\}$.
5. Find all elements in $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}$. Moreover, seek a suitable complete representative of $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}/\mathcal{O}^{\times}$. Define S by the suitable complete representative. Then $|S|$ is exactly equal to $p+1$, which follows by $\mathfrak{h} = 1$ condition [7], 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 $X^{(p,q)}_{P,Q} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S_{JSY})$.

4. Cayley hash function-map

4.1 Hash function

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

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

4.2 Cayley hash function

Let G be a non-commutative group and $S = \{s_0, \ldots, s_p\} \subset G$ be a generating set for the group G, symmetric ($S = S^{-1}$) and not having the identity ($1_G \notin S$). Charles et al. [5] and Petit et al. [34], [37] 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.

A message m is given as a string $m_1 \cdots m_\ell$, where $m_i \in \{0, \ldots, p-1\}$. (i.e. m is a p-base number.) Then the resulting hashing value h of m will be obtained as a group product

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

where g_{ST} is a fixed starting element in G. (We usually put g_{ST} as the identity 1_G in G.) To dispose a proper sequence of hashing bits inductively, we define a *choice func-*

tion 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

$$\pi : \{0, \ldots, p-1\} \times S \to S \tag{1}$$

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

The security of Cayley hash functions lies on the hardness of solving *word problems* for group theory, which are one of the most challenging open problems. It is described in datail in [22], [27], [29], [37].

4.3 Cayley hash function-map

By following the recipe in Section 3, we set up n numbers of LPS-type Ramanujan graphs (the case of $P = 13$) for constructing *Cayley hash function-map*, for an arbitrary $n \in \mathbb{N}$. In other words, we construct n numbers of $X^{(p,q)}_{13,Q^{(i)}} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S^{(i)}_{JSY})$ for $i \in \{1, \ldots, n\}$.

1. We fix $p \in \mathbb{P}$, which determines the regularity $(p+1)$ of LPS-type Ramanujan graphs.
2. We choose n numbers of distinct $Q^{(i)} \in \mathbb{P}$ which satisfies with $Q^{(i)} \equiv 3 \pmod 8$ and $\left(\frac{-Q^{(i)}}{P}\right) = -1$.
3. We fix $q \in \mathbb{P} \setminus \{2, p\}$ which satisfies with $\left(\frac{-13}{q}\right) = \left(\frac{Q^{(i)}}{q}\right) = 1$ and $\left(\frac{p}{q}\right) = 1$ for all $i \in \{1, \ldots, n\}$.

Then we have the same group $\mathrm{PSL}_2(\mathbb{F}_q)$ of the size $\frac{q(q^2-1)}{2}$ and n numbers of corresponding generating sets $S^{(i)}_{JSY}$ for each $X^{(p,q)}_{13,Q^{(i)}}$.

Let M be the set $\{X^{(p,q)}_{13,Q^{(1)}}, X^{(p,q)}_{13,Q^{(2)}}, \ldots, X^{(p,q)}_{13,Q^{(n)}}\}$.

A *Cayley hash function-map* H is a composition of n numbers of Cayley hash functions $H^{(i)}$ with each individual choice function $\pi^{(i)}$, which will be described as shown below. In the case of $n = 1$, we consider it as an original Cayley hash function.

From here, we assume that $n > 1$ and $\ell > n$, where ℓ is a length of bits of the message. A message bit is hashing through each $H^{(i)}$ cyclically. Thus, for a brief notation of a uppercase indices of H, S_{JSY} and π, we denote '$i \pmod n$' as $\tau_n(i)$.

We re-arrange the elements of the set M as M' in order, satisfying with the condition:

$$S^{(\tau_n(i))}_{JSY} \cap S^{(\tau_n(i+1))}_{JSY} = \phi \text{ for all } i \in \{1, \ldots, n\}. \tag{2}$$

We construct a Cayley hash function-map H as $\{H^{(1)}, H^{(2)}, \ldots, H^{(n)}\}$ with an ordered set M' and corresponding individual consecutive choice function $\pi^{(1)}, \pi^{(2)}, \ldots, \pi^{(n)}$ in the same order of indices as shown below:

We consider that a message m is given as a string $m_1 \cdots m_\ell$, where $m_i \in \{0, \ldots, p\}$. Because of the condition in (2), a message is $(p+1)$-base number, which is different from one of an original Cayley hash function.

Then the resulting hashing value h of m will be obtained

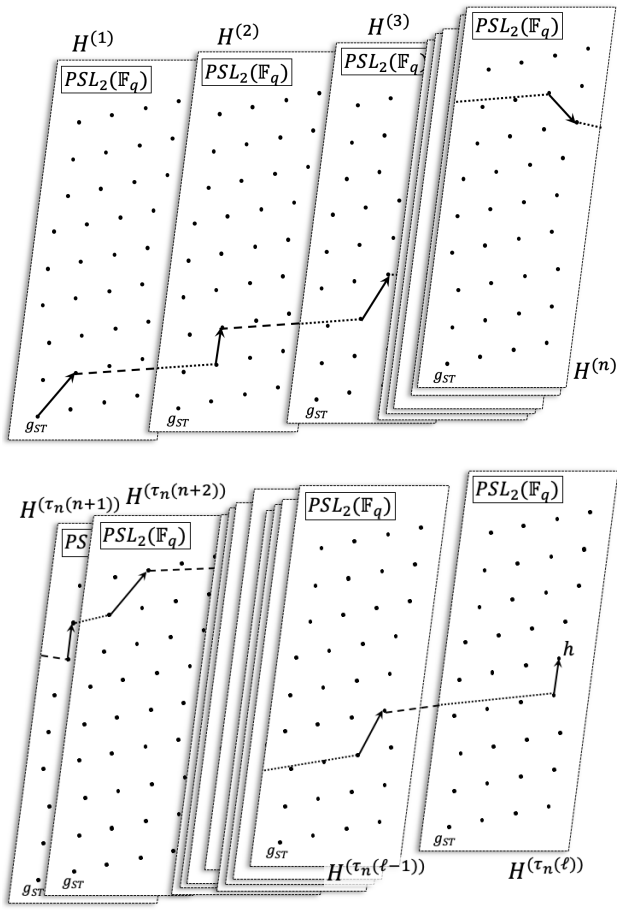

Fig. 0 Cayley hash function-map.

as a group product

$$\begin{aligned} h &:= H(m) \\ &= H^{(\tau_n(\ell))}(H^{(\tau_n(\ell-1))}(\ldots(H^{(1)}, g_{ST}), \ldots), m_{\ell-1}), m_\ell) \\ &= g_{ST} s_{m_1} s_{m_2} \cdots s_{m_\ell}, \end{aligned}$$

where g_{ST} is a fixed starting element as 1_G in G.

To dispose a proper sequence of hashing bits inductively as depicted in Fig. 4.3, we define a *choice function* $\pi^{(\tau_n(i))}$ which assigns a next hashing bit with the bit of the message m from $S^{(\tau_n(i+1))}_{JSY}$ and the previous hashing bit from $S^{(\tau_n(i))}_{JSY}$. We choose a function

$$\pi^{(\tau_n(i))} : \{0, \ldots, p\} \times S^{(\tau_n(i))}_{JSY} \to S^{(\tau_n(i+1))}_{JSY} \tag{3}$$

such that for any $s \in S^{(\tau_n(i))}_{JSY}$ the set $\pi^{(\tau_n(i))}(\{0, \ldots, p\} \times \{s\})$ is equal to $S^{(\tau_n(i+1))}_{JSY}$. In this procedule, the condition (2) guarantees a Cayley hash function-map to avoid a back-tracking (i.e. $s^{(\tau_n(i))} s^{(\tau_n(i+1))} \neq 1_G$).

5. Possible attacks

5.1 Generic attack

In general, brute-force attacks and birthday attacks against a Cayley hash function-map are expected to find a preimage in time $(p+1)p^{2\log_p q - 1}$ and $\sqrt{\frac{\pi}{2}(p+1)(\frac{q\pm1}{2}p^{2\log_p q - 2})}$, respectively.

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 [26]	$x^2+y^2+z^2+w^2=p^\ell$ $N:=p^\ell-z^2-w^2$
Chiu's ($p=2$) [7]	$x^2+2y^2+13z^2+26w^2=2^\ell$ $N:=2^\ell-13z^2-26w^2$
LPS-type [23]	$x^2+Py^2+Qz^2+PQw^2=p^\ell$ $N:=p^\ell-Qz^2-PQw^2$

5.2 Lifting attack

It is the most powerful cryptanalysis tool (at most, quasi-polynomial time algorithm) against a Cayley hash function so far. Essentially, if the norm equations of based quaternion algebra is revealed, it is vulnerable to use those Cayley hash functions by solving the specific solutions of its norm (diophantine) equations. It is well explained in [36], [38], [46], [47], [49].

We can summarize the core of the procedure of a lifting attack with Table 1, very briefly. Each norm equation can be deformed in Table 1, and we choose some random variables for z and w under the individual restricted conditions. We solve these equations for x and y with the continued fraction method (or with the advanced Euclidean algorithm, Cornacchia's algorithm, Pell's equation). However, as we can see in the case of LPS-type Ramanujan graphs in Table 1, it is unpredictable to know the exact form of a norm equation which is used for constructing a Cayley hash function-map. As a definition of a Cayley hash function-map, the norm equation is mixed up with n numbers of generators involved in each graph $X^{(p,q)}_{13,Q^{(i)}}$.

6. Conclusion

In this article, we suggest a Cayley hash function-map based on LPS-type Ramanujan graphs in the case of "$P=13$". Even if we choose n for the smallest number ($n=2$), it seems hard enough to find a collision or a preimage of a Cayley hash function-map. It is unclear if there exists a small cycle (i.e. a collision) over a sequence of hashing bits, since a hashing bit walks along each of the different Cayley graphs with respect to its individual generating set. It is necessary to implement the suggested hashing scheme by restricted parameters.

As a part of these approaches, it is also important to investigate much more general versions of explicit constructions of Ramanujan graphs. For example, when $P=2,3,5$ or 7, we can also construct explicit Ramanujan graphs along the recipe in subsection 3.1. However, it is not fully proved, yet and is still in the process. Moreover, we 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 [23]. It is in the progress to study the Ramanujan-ness of these graphs by similar arguments in LPS-type graphs. These theoretical appoaches enlarge the class of Ramanujan graphs for a cryptographic applications, mainly, this Cayley hash function-map.

Acknowledgments This work was supported by JST CREST Grant Number JPMJCR14D6, Japan.

References

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

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

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

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

[5] Charles, D. X., Goren, E. Z., Lauter, K. E.: Cryptographic hash functions from expander graphs. J. Cryptology. **22(1)**, 93–113 (2009)

[6] Charles, D. X., Goren, E. Z., Lauter, K. E.: Families of Ramanujan graphs and quaternion algebras. Groups and symmetries, **47**, CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, 53–80 (2009)

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

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

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

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

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

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

[13] Eichler, M.: The basis problem for modular forms and the traces of the Hecke operators. In: Willem Kuyk (eds.) Modular Functions of One Variable, **320**, 75–152, Springer, Heidelberg (1973)

[14] Grassl, M., Ilić, I., Magliveras, S., Steinwandt, R.: Cryptanalysis of the Tillich–Zémor Hash Function. Journal of cryptology, **24(1)**, 148–156 (2010)

[15] Goldreich, O.: Foundations of Cryptography. Cambridge University Press (2004)

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

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

[18] 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`

[19] Ibukiyama, T.: On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. Nagoya. Math. J., **88**, 181–195 (1982)

[20] Ihara, Y.: Discrete Subgroups of PL($2,\mathfrak{k}_\mathfrak{p}$). In Proc. Symp. Pure Math. 272–278, (1966)

[21] Jo, H., Petit, C., Takagi, T.: Full cryptanalysis of hash functions based on cubic ramanujan graphs. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, **100(9)**, 1891–1899 (2017)

[22] Jo, H., Sugiyama, S., Yamasaki, Y.: Ramanujan graphs for post-quantum cryptography, International Symposium on Mathematics, Quantum Theory, and Cryptography (MQC 2019), in submission.

[23] Jo, H., Sugiyama, S., Yamasaki, Y.: A general explicit construction of LPS-type Ramanujan graphs, in preparation.

[24] Jo, H., Yamasaki, Y.: LPS-type Ramanujan graphs. In 2018 International Symposium on Information Theory and Its Applications, ISITA 2018, 399–403 (2018)

[25] Kirschmer, M., Voight, J.: Algorithmic enumeration of ideal classes for quaternion orders. SIAM Journal on Computing,

39(5), 1714–1747 (2010)
[26] Lubotzky, A., Phillips, R., Sarnak, P.: Ramanujan graphs. Combinatorica **8(3)**, 261–277 (1988)
[27] Lubotzky, A.: Discrete groups, expanding graphs and invariant measures. Springer Science Business Media. (1994)
[28] Margulis, G.: 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)
[29] Meier, J.: Groups, graphs and trees; an introduction to the geometry of infinite groups. Cambridge University Press, (2008)
[30] Mestre, J. F.: 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)
[31] Mestre, J. F., Jorza, T. A.: The Method of Graphs. Examples and Applications. Notes. (2011)
[32] Morgenstern, M.: Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. Journal of Combinatorial Theory, Series B, **62(1)**, 44–62 (1994)
[33] NIST : Call for Proposals; Post-Quantum Cryptography Standardization, (2017) `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`
[34] Petit, C., Lauter, K. E., Quisquater, J. J.: Cayley hashes: A class of efficient graph-based hash functions, preprint. (2007)
[35] Petit, C., Lauter, K. E., Quisquater, J. J.: Full cryptanalysis of LPS and Morgenstern hash functions. SCN **LNCS 5229**, 263-277 (2008)
[36] Petit, C., Quisquater, J. J.: Preimages for the Tillich-Zémor hash function. In International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 282–301 (2010)
[37] Petit, C., Quisquater, J. J.: Rubik's for cryptographers. IACR Cryptology ePrint Archive,638 (2010)
[38] Petit, C., Quisquater, J. J., Tillich, J. P., Zémor, G.: 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. 182–194 (2009)
[39] Pizer, A. K.: On the arithmetic of quaternion algebras. Acta Arithmetica, 31, 61–89 (1976)
[40] Pizer, A. K.: Ramanujan graphs and Hecke operators. B. Am. Math. Soc., **23(1)**, 127–137 (1990)
[41] Pizer, A. K.: Ramanujan graphs. AMS/IP Studies in Advanced Mathematics, 7, 159–178 (1998)
[42] Sarnak, P.: Some Applications of Modular Forms. Cambridge University Press (1999)
[43] Schoeneberg, P.: Elliptic Modular Functions: An Introduction, Springer-Verlag, **203**, (2012)
[44] Shor, P. W.: Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science. (1994)
[45] Terras, A.: Zeta functions of graphs; a stroll through the garden, vol. 128, Cambridge University Press (2010)
[46] Tillich, J. P., Zémor, G.: Hashing with SL_2. In Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 40–49 (1994)
[47] Tillich, J. P., Zèmor, G.: Collisions for the LPS expander graph hash function. EUROCRYPT **LNCS 3027**, 254–269 (2008)
[48] Vignéras, M., F.: Arithmétique des algèbres de quaternions, Lecture Notes in Math., vol. 800, Springer, Berlin (1980)
[49] Zémor, G.: Hash functions and graphs with large girths. In Workshop on the Theory and Application of of Cryptographic Techniques, Springer, Berlin, Heidelberg., 508–511 (1991)