Path-finding algorithms in LPS/LPS-type Ramanujan graphs

Hyungrok JO (University of Tsukuba)

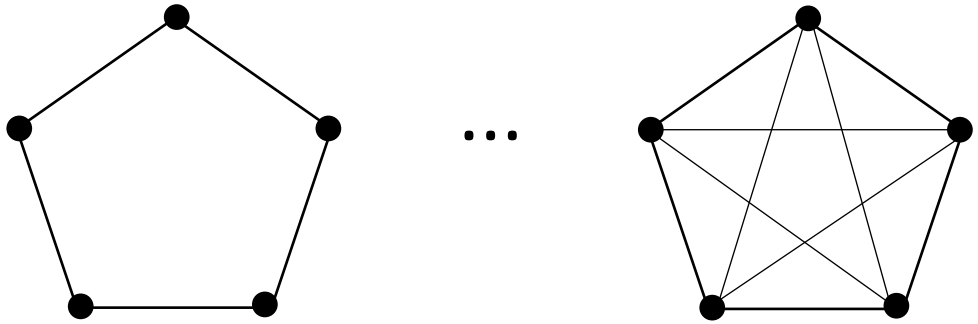
WAIS 2020 (C-4)

Febuary 21

Background

Ramanujan graphs

- Ramanujan graph (k-regular)
  - "Sparse graphs with strong connectivity".



  - Optimal expander graphs in a spectral view. (*Alon-Boppana*)
    - $|\lambda| \leq 2\sqrt{k-1}$, where λ are non-trivial eigenvalues of an adjacency matrix of a graph.
  - Random walk on graphs ⇒ uniform distribution (quickly)

    (Rapidly mixing lemma).
  - Guarantee enlarging cycles in a graph with $|V| \to \infty$.

Background

Cayley-type Ramanujan graphs

- **Lubotzky-Phillips-Sarnak** (LPS) '88 ($p \geq 5$)
  : $(p+1)$-regular graph /*Hamiton's quaternion algebra*
  - *Cayley graph over* $PSL_2(\mathbb{F}_q)$ *with its* $p+1$ *generators* S_{LPS}.
    - $B_{2,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, where $i^2 = -1, j^2 = -1,$ and $ij = -ji$
    - $\mathcal{O}_{2,\infty} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}$
    - $\mathcal{O}_{2,\infty}(p) \coloneqq \{\alpha \in \mathcal{O}_{2,\infty} | N(\alpha) = p\}/\mathcal{O}_{2,\infty}^{\times}$
    - $\forall \alpha \in B_{p,\infty}, \alpha = x + yi + zj + wij,$
      $\exists \psi_{iso}: B_{p,\infty} \to M_2(\mathbb{F}_q)$ defined by

$$\alpha = x + yi + zj + wij \mapsto \begin{bmatrix} x + yi_q & zj_q + wi_q j_q \\ -zj_q + wi_q j_q & x - yi_q \end{bmatrix},$$

where $i_q \coloneqq i \ (mod\ q), j_q \coloneqq j\ (mod\ q)$.

- Fact : $N(\alpha) = \det(\psi(\alpha))$.
- $S_{LPS} \coloneqq \{\psi(\alpha) | \alpha \in \mathcal{O}_{2,\infty}(p)\}$. ($|S_{LPS}| = p + 1$)

[LPS_1988] A. Lubotzky, R. Phillips, P. Sarnak, "Ramanujan graphs", Combinatorica, 8(3):pages 261-277, 1988.

Background

Cayley-type Ramanujan graphs

- **Chiu** '92 ($p = 2$)
  : 3-regular graph / *quaternion algebra which is split at* 2.
  - *Cayley graph over* $PSL_2(\mathbb{F}_q)$ *with its* 3 *generators* S_C.
    - $B_{13,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, where $i^2 = -2, j^2 = -13,$ and $ij = -ji$.
    - $\mathcal{O}_{13,\infty} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{2+i+ij}{4} + \mathbb{Z}\frac{2-i-ij}{4}$
    - $\mathcal{O}_{13,\infty}(2) \coloneqq \{\alpha \in \mathcal{O}_{13,\infty} | N(\alpha) = 2\}/\mathcal{O}_{13,\infty}^{\times}$
    - $S_C \coloneqq \{\psi(\alpha) | \alpha \in \mathcal{O}_{13,\infty}(2)\}$. ($|S_C| = 3$)

[Chiu_1992] P. Chiu, "Cubic Ramanujan graphs", Combinatorica 12(3) p 275-285. 1992.

Background

Cayley-type Ramanujan graphs

○ **J, Sugiyama, Yamasaki** '19 ($p \geq 2, p \neq 13$) **(LPS-type)**
: $(p+1)$-regular graph / *quaternion algebra*

- *Cayley graph over* $PSL_2(\mathbb{F}_q)$ *with its* $(p+1)$ *generators* S_{JSY}.
  - $B_{13,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, where $i^2 = -13, j^2 = -Q,$ and $ij = -ji$, where $Q(prime) \equiv 3\ (mod\ 8)$ and $\left(\frac{-Q}{13}\right) = -1$.
  - ${\mathcal{O}'}_{13,\infty} = \mathbb{Z} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}\frac{Tj+k}{Q}$, where $T \in \mathbb{Z}$ such that $T^2 \equiv -13\ (mod\ Q)$.
  - ${\mathcal{O}'}_{13,\infty}(p) \coloneqq \{\alpha \in \mathcal{O}_{13,\infty} | N(\alpha) = p\}/{\mathcal{O}'}^{\times}_{13,\infty}$
  - $S_{JSY} \coloneqq \{\psi(\alpha) | \alpha \in {\mathcal{O}'}_{13,\infty}(p)\}$. ($|S_{JSY}| = p+1$)

Remark

1) In LPS-type case, we have infinite families of Ramanujan graphs which norm also has infinite candidates depending on Q.
2) For each generator, $\langle S_{LPS} \rangle = \langle S_C \rangle = \langle S_{JSY} \rangle = PSL_2(\mathbb{F}_q)$.

[JSY_2019] H. Jo, S. Sugiyama, Y. Yamasaki, "Ramanujan graphs for post-quantum cryptography", International Symposium on Mathematics, Quantum Theory, and Cryptography. 2019.

Background

CGL hash function ‘09

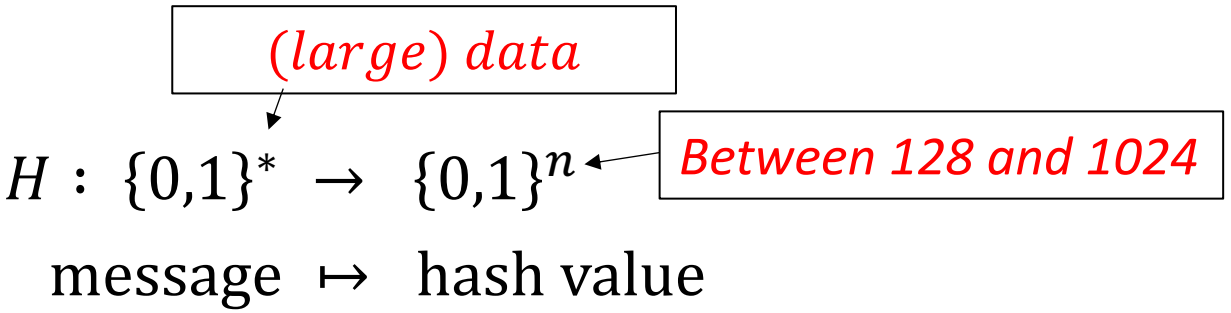
- Charles, Goren, Lauter ‘09
  - Charles et al. suggested provable cryptographic hash functions
    - based on Cayley-type graphs (LPS)
    - based on Non-Cayley-type graphs
      (Pizer’s graphs; Supersingular-Isogeny graph)

- Security analysis of CGL hash function.
  - It is revealed by path-finding algorithms in each Cayley-type graph.
  (quasi-polynomial times) LPS, Chiu, Morgenstern, etc.
  - path-finding algorithms (Cayley) => solving *norm Diophantine equation* of based quaternion algebra.

- Supersingular-Isogeny graphs are still alive
  - Diffie-Hellman Key Exchange (David Jao et al. 2011)
  - SIKE (one of candidates for PQC standardization by NIST)

CGL hash function

hash function



- **Collision resistance**
  : if it is "*computationally infeasible*" to find any two distinct preimage m, m' such that $H(m) = H(m')$.
- **Second preimage resistance**
  : if given any message $m \in \{0,1\}^*$, it is "*computationally infeasible*" to find any second preimage $m' (\neq m)$ such that $H(m) = H(m')$.
- **Preimage resistance**
  : if given any hash value $h \in \{0,1\}^n$, it is "*computationally infeasible*" to find any preimage (message) $m \in \{0,1\}^*$ such that $h = H(m)$.

CGL hash function

Cayley graph

G : a finite group

$S(\subset G)$: a *generating set* of G satisfying the followings

(1) $G = \langle S \rangle$,

(2) $S^{-1} = S$ (i.e., $\forall s \in S, s^{-1} \in S$),

(3) $id \notin S$.

$\mathrm{Cay}(G, S) = (V, E)$: *Cayley graph* over G with respect to S.

- Vertex-set V : $\{v_g | g \in G\}$
- Edge-set E : $\left\{\left(v_{g_i}, v_{g_j}\right) \middle| g_j = g_i s,\ s \in S\right\}$

❖ $\left|\mathrm{PSL}_2(\mathbb{F}_q)\right| = \frac{q^3 - q}{2}$.

CGL hash function

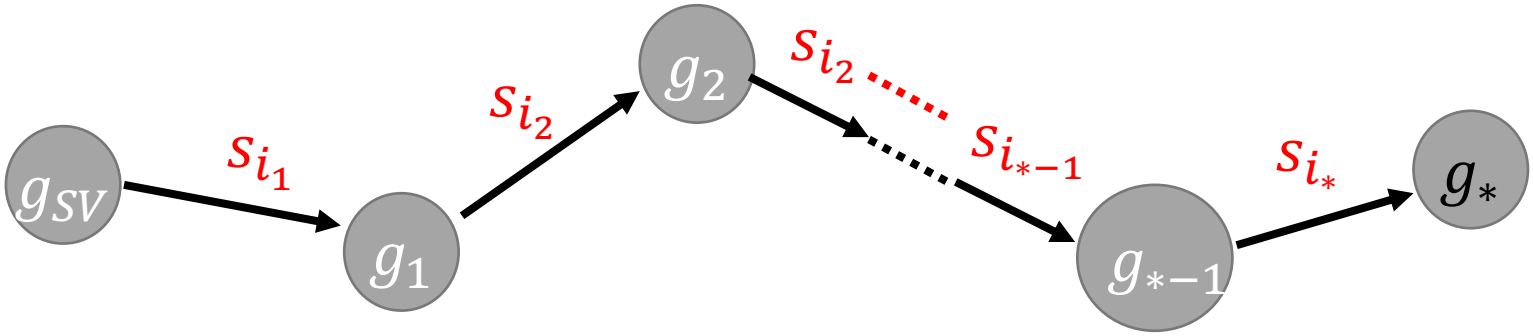
Cayley hash function

$p \stackrel{\text{def}}{=} |S| - 1.$

$$H^c : \{0, \ldots, p-1\}^* \rightarrow G$$

$$x_1 x_2 \ldots x_* \mapsto g$$

Message's bits x_j transform into $s_{i_j} \in S$ to walk around $\mathrm{Cay}(G, S)$, and its hash value is $g_* \in G$ s.t. $g_* = g_{SV} s_{i_1} s_{i_2} \cdots s_{i_*}$ for some $* \in \mathbb{N}$.



[CGL_2009] D. Charles, E. Goren, K. Lauter, "Cryptographic hash functions from expander graphs", Journal of Cryptology, 22(1) :pages 93-113, 2009.

CGL hash function

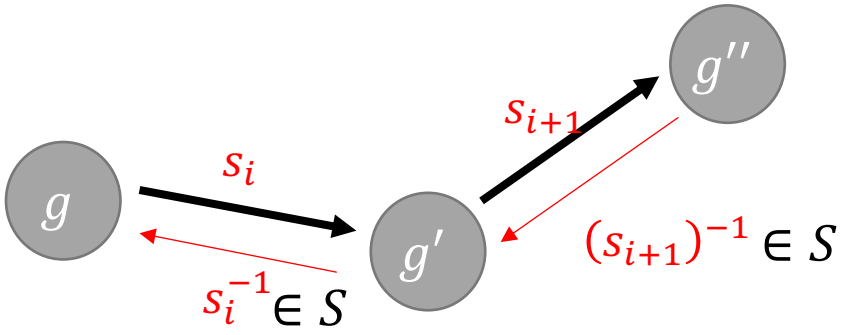
Cayley hash function

a *choice function*

$$\pi: \{0,1,\dots,p-1\} \times S \longrightarrow S$$

such that, $\forall s \in S, \pi(\{0,1,\dots,p-1\} \times \{s\}) = S \setminus \{s^{-1}\}.$

(To avoid trivial collisions $s_i s_{i+1}$ where $s_{i+1} = {s_i}^{-1}$.)

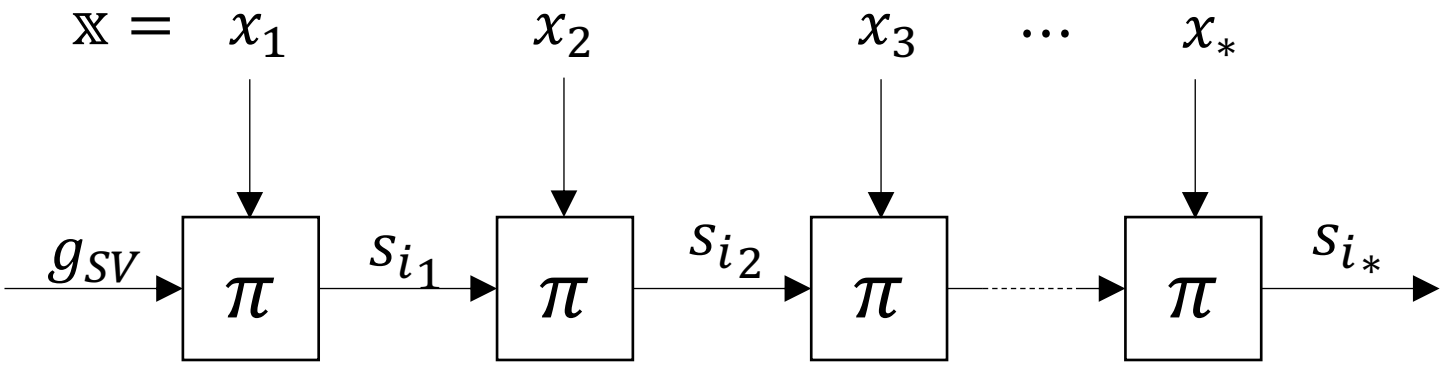


[CGL_2009] D. Charles, E. Goren, K. Lauter, "Cryptographic hash functions from expander graphs", Journal of Cryptology, 22(1) :pages 93-113, 2009.

CGL hash function

Cayley hash function

message $\mathbb{X}$



hash value of $\mathbb{X}$

$$H^c(\pi, \mathbb{X}) = H^c(\pi, x_1 \dots x_*) = g_{SV}\, s_{i_1} \dots s_{i_*} = g, \text{ for some } g \in G.$$

[CGL_2009] D. Charles, E. Goren, K. Lauter, "Cryptographic hash functions from expander graphs", Journal of Cryptology, 22(1) :pages 93-113, 2009.

Cayley hash function

Security (overall)

Recall

- **Preimage resistance of Cayley hash function** H^c
  : if given any hash value $h \in G$, it is "*computationally infeasible*" to find any preimage (message) $\mathbb{x}$ such that
  $h = H^c(\pi, \mathbb{x}) = g_{SV}\, s_{i_1} \dots s_{i_{\ell-1}}$.

$\Rightarrow$ Path-finding problem in Cayley graph with its group generators. ($G = PSL_2(\mathbb{F}_q)$)

1) LPS's case : $s = \begin{bmatrix} x + yi_q & zj_q + wi_qj_q \\ -zj_q + wi_qj_q & x - yi_q \end{bmatrix}$,
   where $x^2 + y^2 + z^2 + w^2 = p, x > 0$:odd, y, z, w : even.

   Norm of $\mathcal{O}_{2,\infty}(p)$

2) Chiu's case : $s = \begin{bmatrix} x + yi'_q & zj'_q + wi'_qj'_q \\ -zj'_q + wi'_qj'_q & x - yi'_q \end{bmatrix}$,
   where $x^2 + xw + 2y^2 + yw + 13z^2 + 2w^2 = 2$.

   Norm of $\mathcal{O}_{13,\infty}(2)$

3) LPS-type case : $s = \begin{bmatrix} x + yi''_q & zj''_q + wi''_qj''_q \\ -zj''_q + wi''_qj''_q & x - yi''_q \end{bmatrix}$,
   where $x^2 - \left(\frac{1+Q}{4}\right)y^2 - 13\left(\frac{1+Q}{4}\right)z^2 + \left(\frac{13+T^2}{Q}\right)w^2 + xy + Tyw + 13zw = p$.

   Norm of $\mathcal{O}'_{13,\infty}(p)$

Cayley hash function

Security (overall)

By using a fact $N(\alpha) = \det(\psi(\alpha))$,

assume that the targeting preimage $h = H^c(\pi, \mathbb{X}) = g_{SV}\, s_{i_1} \ldots s_{i_{\ell-1}}$ having $\det(h) = p^\ell$.

1) LPS's case : $x^2 + y^2 + z^2 + w^2 = p^\ell, x > 0$:odd, y, z, w : even.

2) Chiu's case : $x^2 + xw + 2y^2 + yw + 13z^2 + 2w^2 = 2^\ell$.

3) LPS-type case :

$$x^2 - \left(\frac{1+Q}{4}\right)y^2 - 13\left(\frac{1+Q}{4}\right)z^2 + \left(\frac{13+T^2}{Q}\right)w^2 + xy + Tyw + 13zw = p^\ell$$

Not easy to solve each norm Diophantine equation, because of many variables.

Re-assume that $h = s \cdot D \cdot s \cdot D' \cdot s \cdot D''$, $(D, D', D''$ are diagonal matrices).

So we focus on finding specific solution on diagonal matrices $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$, where $\lambda \equiv 1\ (mod\ q)$.

Cayley hash function

Security (LPS's case)

Input : a length of message ℓ, a generating set $\boldsymbol{S_{LPS}}$ for $G(=\mathrm{PSL}_2(\mathbb{F}_q))$.
Output : a ℓ-factorization of id_G composed of $\boldsymbol{S_{LPS}}$.

STEP 1. Lift-up.

$$s_{i_1}s_{i_2}\cdots s_{i_\ell} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} (\mathrm{mod}\ q)$$

$$\Rightarrow \widehat{s_{i_1}}\widehat{s_{i_2}}\cdots\widehat{s_{i_\ell}} = \begin{pmatrix}\lambda A + aq & bq\\ cq & \lambda A + dq\end{pmatrix} \text{ for some } \lambda, a, b, c, d, A \in \mathbb{Z}$$

STEP 2. Choose parameters λ, A, a by $(\mathrm{mod}\ q)$ and $(\mathrm{mod}\ q^2)$.

Since $\det(s_{i_1}s_{i_2}\cdots s_{i_\ell}) = p^\ell\ (\mathrm{mod}\ q)$,

$$\det\begin{pmatrix}\lambda A + aq & bq\\ cq & \lambda A + dq\end{pmatrix}$$
$$= (\lambda A + aq)^2 + (bq)^2 + (cq)^2 + (\lambda A + aq)^2 = p^\ell$$

Cayley hash function

Security (LPS's case)

STEP 2. Choose parameters λ, A, a by $(\mathrm{mod}\ q)$ and $(\mathrm{mod}\ q^2)$.

From $(\lambda A + aq)^2 + (bq)^2 + (cq)^2 + (\lambda A + aq)^2 = p^\ell \pmod{q}$,
choose $\lambda A \in \mathbb{Z}$ s.t. $2(\lambda A)^2 \equiv p^\ell \pmod{q}$
From $(\lambda A + aq)^2 + (bq)^2 + (cq)^2 + (\lambda A + aq)^2 = p^\ell \pmod{q^2}$,
choose $a \in \mathbb{Z}$ s.t. $2(\lambda A)^2 + 4aq \equiv p^\ell \pmod{q^2}$

STEP 3. Find the solution $(\boldsymbol{b}, \boldsymbol{c})$ with $m \coloneqq \lambda A + aq$.

$$b^2 + c^2 = p^\ell - 2m^2/q^2$$

,using Euclidean algorithms.

STEP 4. Find the sequence $(\boldsymbol{s_{i_1}}, \boldsymbol{s_{i_2}}, \cdots, \boldsymbol{s_{i_\ell}})$.

Multiply on the right $\begin{pmatrix} \lambda A + aq & bq \\ cq & \lambda A + dq \end{pmatrix}$ by each lifted generator $\widehat{s_i}$.

Check if the matrix is divisible by p, then $\widehat{s_i}$ is the inverse.

Cayley hash function

Security (Chiu's case)

Deform $x^2 + xw + 2y^2 + yw + 13z^2 + 2w^2 = 2^\ell$.

$$\Longrightarrow \left(x^2 + xw + \frac{1}{4}w^2\right) + 2\left(y^2 + \frac{1}{2}yw + \frac{1}{16}w^2\right) + 13z^2 + \frac{13}{8}w^2 = 2^\ell.$$

$$\Longrightarrow \left(x + \frac{1}{2}w\right)^2 + 2\left(y + \frac{1}{4}w\right)^2 + 13z^2 + \frac{13}{8}w^2 = 2^\ell.$$

$$\Longrightarrow \underbrace{\left(x + \frac{1}{2}w\right)}_{x'}^2 + 2\underbrace{\left(y + \frac{1}{4}w\right)}_{y'}^2 = \underbrace{2^\ell - 13z^2 - \frac{13}{8}w^2}_{N}.$$

$\Longrightarrow x'^2 + 2y'^2 = N.$

$\Longrightarrow$ Check if $(2, N) = 1$. If not, go back to (2).

$\Longrightarrow$ Cornacchia's algorithm gives x' and y'.

Cayley hash function

Security (LPS-type case)

$$x^2 - \left(\frac{1+Q}{4}\right)y^2 - 13\left(\frac{1+Q}{4}\right)z^2 + \left(\frac{13+T^2}{Q}\right)w^2 + xy + Tyw + 13zw = p^{\ell}$$

For finding a preimage in LPS-type, we should carefully choose random variables to avoid the Q. (still open)

For finding a collision in LPS-type [JY_2019], we used a fact

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij \subset \mathcal{O'}_{13,\infty} = \mathbb{Z} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}\frac{Tj+k}{Q}$$

$$x^2 - 13y^2 - Qz^2 + 13Qw^2 = p^{\ell}$$

[JY_2019] H. Jo, Y. Yamasaki, “On the security of Cayley hash functions based on LPS-type Ramanujan graphs.”, SCIS2019.

Conclusion

Towards quantum circuit design

1) The path-finding algorithms in cases of LPS, Chiu in quasi-polynomial time.

2) In a case of LPS-type, the deformation of norm equation avoiding infinite candidates of Q is not succeeded.

In the theory of quantum computation,

[Solovoy-Kitaev Theorem]

It is possible to obtain good approximations to any desired gate using surprisingly short sequences of gates from the given generating set.

Path finding algorithm in LPS Ramanujan graphs is directly used for quantum design circuit.

[Sardari_2019] Sardari, Naser T. "Complexity of strong approximation on the sphere." International Mathematics Research Notices.

[PS_2018] Parzanchevski, Ori, and Peter Sarnak. "Super-golden-gates for PU (2)." *Advances in Mathematics* 327 (2018): 869-901.

[EP_2018] Pinto, Eduardo Carvalho, and Christophe Petit. "Better path-finding algorithms in LPS Ramanujan graphs." *Journal of Mathematical Cryptology* 12.4 (2018): 191-202.

Thank you