Expander Graphs in Cryptography

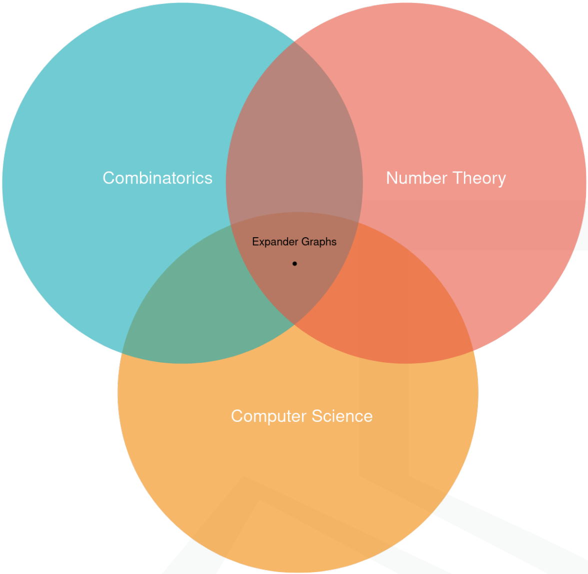
Shai Levin

Supervisor: Steven Galbraith

January, 2023

University of Auckland, New Zealand

Expander Graphs



Two Important Properties

On a 'good' expander graph:

- Path finding is hard when the number of vertices is (exponentially) large.
- Random walks converge to the uniform distribution.

Some Applications

In Computer Science:

- Efficient error correcting codes
- Fault-tolerant networks
- Cryptographic pseudorandom behaviour:
  - Cryptographic hash functions or one way functions.
  - pseudorandom functions (?)

Overview

- We want a family of graphs $\{G_i\}$
- Choose a graph from this family and a starting vertex.
- Compute a path 'randomly'.

Overview

- We want a family of graphs $\{G_i\}$
- Choose a graph from this family and a starting vertex.
- Compute a path 'randomly'.

Intuition:

1. When the path is long enough, the end point could be anywhere (pseudorandom).
2. Given starting and ending vertices, finding a path is hard.

Overview

- We want a family of graphs $\{G_i\}$
- Choose a graph from this family and a starting vertex.
- Compute a path 'randomly'.

Intuition:

1. When the path is long enough, the end point could be anywhere (pseudorandom).
2. Given starting and ending vertices, finding a path is hard.

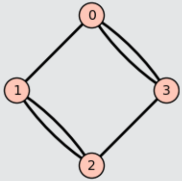
Question

What does a suitable family of graphs look like?

Adjacency Matrix, Regular graphs

An *adjacency matrix* A of a graph on n vertices is an $n \times n$ matrix where each $a_{i,j} = \#$ edges from i-th vertex to j-th vertex.

Example



For G above, $A = \begin{bmatrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{bmatrix}$.

- A graph is d-regular if each vertex is adjacent to d others.
- We call a d-regular graph on n vertices an $[n, d]$-graph.

Graph Spectrum

- If a graph G is undirected, the adjacency matrix A is symmetric and real $\implies$ n eigenvalues.

Definition (Graph Spectrum)

The *spectrum* of a graph is the set of eigenvalues $\lambda_1, ...\lambda_n$ of adjacency matrix A where:

$$d \geq \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n \geq -d$$

for $d \in \mathbb{Z}$.

Graph Spectrum

- If a graph G is undirected, the adjacency matrix A is symmetric and real $\implies$ n eigenvalues.

Definition (Graph Spectrum)

The *spectrum* of a graph is the set of eigenvalues $\lambda_1, ...\lambda_n$ of adjacency matrix A where:

$$d \geq \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n \geq -d$$

for $d \in \mathbb{Z}$.

Some useful properties of graph spectrum:

- If G is d-regular, then $\lambda_1 = d$.
- G is bipartite if.f $\lambda_1 = -\lambda_n$.
- G is connected if.f $\lambda_1 > \lambda_2$.

Algebraic Definition: Spectral Gap

Given an $[n, d]$-graph G with spectrum
$d = \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n \geq -d$:

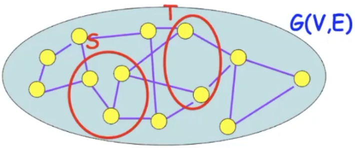
- Let $\lambda(G) := max(\{|\lambda_2|, ..., |\lambda_n|\})$ (usually just λ_2).
- $d - \lambda(G)$ is the *spectral gap*.
- If non-zero, this graph is called an *expander*.
- $\{G_i\}$ is an *expander family* (increasing in size) if for all G_i, $d - \lambda(G_i)$ meets some fixed lower bound.

Expander Mixing Lemma

Theorem

The number of edges between any two large vertex subsets in a good expander graph, is close to the average amount of edges between two vertex subsets in a random $[n, d]$-graph.

- Corollary: random walks on the graph converge to uniform distribution in $O(log(n))$ steps.



Ramanujan Graphs

Definition (Ramanujan Graphs)

If G is an $[n, d]$-graph, then it is Ramanujan if:

$$d - 2\sqrt{d-1} \leq d - \lambda(G) \leq d - 2\sqrt{d-1} + \epsilon.$$

for $\epsilon > 0$ where $\epsilon \to 0$ as $n \to \infty$.

- All expander graphs satisfy the upper bound.
- Bigger $d - \lambda(G)$ term $\implies$ better expander.
- Ramanujan graphs are (asymptotically) the best expanders - but hard to come by.

Problem

Does there exist infinite families of d-regular Ramanujan graphs for each $d \geq 3$?

Constructing Expander Graphs

Two types of construction. Given an infinite family $\{G_i\}$ of expander-graphs:

- **Weakly Explicit**: G_i can be constructed in polynomial time. (Polynomial in $\#$ vertices).
- **Strongly Explicit**: Given $i \in \mathbb{N}$, a vertex $v \in V(G_i)$, the neighbours of v can be computed in polynomial time. (Polynomial in length of input (i, v)).

Expanders: What we know so far

- Ramanujan graphs are optimal expanders.
- Good expanders are sparse and finding paths on them is 'hard'.
- Can we use them in cryptography?

One Way Functions, Pseudorandom Generators and Pseudorandom Functions

Let $f : \mathcal{X} \to \mathcal{Y}$ be a function that is efficient to compute.

- f is a *one-way* function, if given f, some $f(x) \in \mathcal{Y}$, it is hard to compute an $x' \in \mathcal{X}$ such that $f(x') = f(x)$.
- f is a *pseudorandom function*, if f is indistinguishable from a uniform function when queried. (instantiated with a secret key)

One Way Function from Expanders

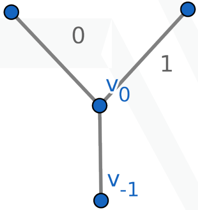
- On a 'good' $[n, d]$ expander graph G. Pick a starting adjacent vertex pair (v_{-1}, v_0).

One Way Function from Expanders

- On a 'good' $[n, d]$ expander graph G. Pick a starting adjacent vertex pair (v_{-1}, v_0).
- **Input**: string $x_1 x_2 .. x_k$ of alphabet $\{0, .., d-2\}$.

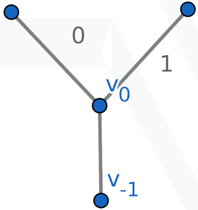
One Way Function from Expanders

- On a 'good' $[n, d]$ expander graph G. Pick a starting adjacent vertex pair (v_{-1}, v_0).
- **Input**: string $x_1 x_2 .. x_k$ of alphabet $\{0, .., d-2\}$.
- for i in $\{1, ..., k\}$:
  - Set v_i to be the x_ith vertex adjacent to v_{i-1} (not including v_{i-2}).



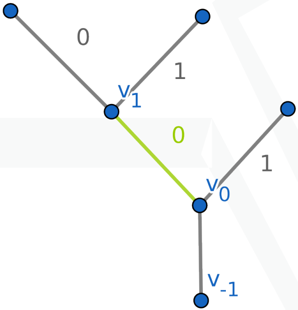
One Way Function from Expanders

- On a 'good' $[n, d]$ expander graph G. Pick a starting adjacent vertex pair (v_{-1}, v_0).
- **Input**: string $x_1 x_2 .. x_k$ of alphabet $\{0, .., d-2\}$.
- for i in $\{1, ..., k\}$:
  - Set v_i to be the x_ith vertex adjacent to v_{i-1} (not including v_{i-2}).
- **Output:** v_k.



One Way Function from Expanders

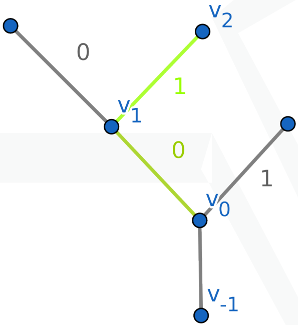
- On a 'good' $[n, d]$ expander graph G. Pick a starting adjacent vertex pair (v_{-1}, v_0).
- **Input**: string $x_1 x_2 .. x_k$ of alphabet $\{0, .., d-2\}$.
- for i in $\{1, ..., k\}$:
  - Set v_i to be the x_ith vertex adjacent to v_{i-1} (not including v_{i-2}).
- **Output:** v_k.



Example: Traversing $f(''01'')$ on a 3-regular graph

One Way Function from Expanders

- On a 'good' $[n, d]$ expander graph G. Pick a starting adjacent vertex pair (v_{-1}, v_0).
- **Input**: string $x_1 x_2 .. x_k$ of alphabet $\{0, .., d-2\}$.
- for i in $\{1, ..., k\}$:
  - Set v_i to be the x_ith vertex adjacent to v_{i-1} (not including v_{i-2}).
- **Output:** v_k.



Example: Traversing f("01") on a 3-regular graph

Choosing Our 'Good' Graph

Ramanujan graph G is 'good' if:

- strongly explicit,
- exponentially large vertex set,
- little symmetry,
- hard to find cycles on.

Proposals:

- **LPS graphs:** Cayley graph of $PSL(2, p)$. Pre-image resistance broken by Petit 2008.
- **Supersingular Isogeny Graphs:** still (believed) secure!

Elliptic Curves and Isogenies

- **Elliptic curves**.
  $y^2 = x^3 + ax + b$ Algebraic and geometric structure. Set of solutions over a field form a group.
- Maps between elliptic curves are called **isogenies**.
  Isogenies preserve group & geometric structure.
- Degree of an isogeny is the size of it's kernel (as a group homomorphism).

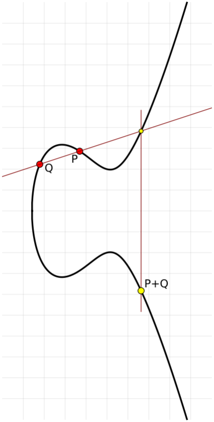


Figure 1: Group operation on $y^2 = x^3 - 4x + 7$

Supersingular ℓ-Isogeny graphs

- An elliptic curve is ordinary or supersingular.
- **$G_\ell(p)$:** Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ (up to isomorphism) form a graph with degree ℓ isogenies as edges.
- The graph is 'good'. Ramanujan, $\lfloor \frac{p}{12} \rfloor$ vertices, $\ell + 1$ regular (for prime ℓ) and strongly explicit.
- Vertices are usually represented by the j-invariant, which corresponds to a single field element in $\mathbb{F}_{p^2}$ (1-1 correspondence)

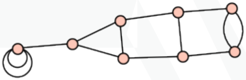


Figure 2: Supersingular isogeny graph $G_2(97)$

Computational Assumption: Isogeny Paths

Problem (IsoPath)

Given j-invariants of two elliptic curves defined over $G_\ell(p)$, find a path between them.

- Closely related to the strong expansion properties of the graph.
- Cryptanalysis: best quantum attacks are still exponential time. $\sim \tilde{O}(p^{\frac{1}{3}})$

The CGL One Way Function

The CGL function below, where $G_2(p)$ is a 3-regular family of expanders for increasing p. For security, $p \gg 2^{256}$.

Algorithm 1 $h(m, j_0, j_{-1}, \mathrm{Sqr}(.))$

Input: An n bit binary string $m = m_{n-1}||...||m_0$, adjacent vertices j_0, j_{-1} in $G_2(p)$, and a deterministic square root algorithm Sqr for $\mathbb{F}_{p^2}$.

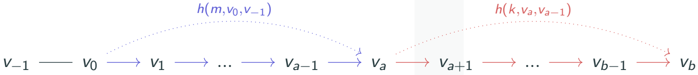
Output: Vertex j_n corresponding to the end point of the walk given by m.

for i in 0, ..., $n-1$ **do**
    $s_i \leftarrow +1$ if $m_i = 1$, -1 if $m_i = 0$
    $a_i \leftarrow -j_i^2 + 1488 j_i - 162000$
    $b_i \leftarrow 1488 j_i^2 + 40773375 j_i + 8748000000$
    $D_i \leftarrow (a_i + j_{i-1})^2 - 4(b_i + a_i j_{i-1} + j_{i-1}^2)$
    $S_i \leftarrow \mathrm{Sqr}(D_i)$
    $j_{i+1} \leftarrow 2^{-1}(-a_i - j_{i-1} + s_i S_i)$
end for
return j_n

An idea: Pseudorandom Function Candidate from CGL

Given $G_2(p)$ and a starting vertex v_0, $F_k(m)$ is computed as follows:

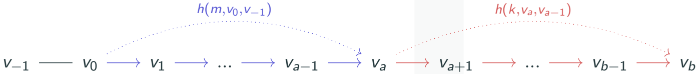
1. Walk the graph starting at v_0, based on the base-2 encoding of m, finishing on v_a
2. Walk the graph again, starting at v_a based on the base-2 encoding of k, finishing on v_b.



An idea: Pseudorandom Function Candidate from CGL

Given $G_2(p)$ and a starting vertex v_0, $F_k(m)$ is computed as follows:

1. Walk the graph starting at v_0, based on the base-2 encoding of m, finishing on v_a
2. Walk the graph again, starting at v_a based on the base-2 encoding of k, finishing on v_b.



Question

Why doesn't this work if you switch the steps around?

Applications of OWFs and PRFs: Signatures

Given a zero-knowledge, non-interactive proof system and uniformly random secret key sk:

- **OWF:** $\mathsf{pk} = OWF(\mathsf{sk})$ and signature is a proof:

  "I know a sk ***such that*** $OWF(\mathsf{sk}) = \mathsf{pk}$***"***

  with m incorporated into the randomness of the proof.

Applications of OWFs and PRFs: Signatures

Given a zero-knowledge, non-interactive proof system and uniformly random secret key sk:

- **OWF:** $\mathsf{pk} = OWF(\mathsf{sk})$ and signature is a proof:

  "I know a sk ***such that*** $OWF(\mathsf{sk}) = \mathsf{pk}$***"***

  with m incorporated into the randomness of the proof.
- **PRF:** $\mathsf{pk} = \mathrm{PRF}_{\mathsf{sk}}(\mathbf{0}))$, and signature is $\mathrm{PRF}_{\mathsf{sk}}(m)$ attached with a proof:

  "I know a sk ***such that I can compute both*** $PRF_{\mathsf{sk}}(m)$ ***and*** $PRF_{\mathsf{sk}}(\mathbf{0})$***".***

Our work - generic proof systems

- *Efficient Isogeny Proofs Using Generic Techniques* - Cong, Lai, Levin - Submitted to ACNS 2023.
- Apply generic proof systems (Aurora, Ligero, Limbo) to isogeny paths:

"I know a path between the two elliptic curves"

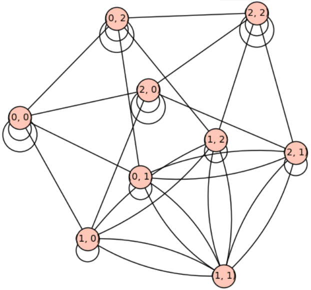
~~with message incorporated into the randomness of the proof~~

Thank you!

Example: A Strongly Explicit Family of Expanders

Margulis Construction (Discrete Torus Expanders): A family of 8-regular graphs $G_i = (V_i, E_i)$ for $i \in \mathbb{Z}^+$:

- $V_i = \mathbb{Z}_i \times \mathbb{Z}_i$
- An edge from each vertex (x, y) to $(x \pm y, y)$, $(x, y \pm x)$, $(x \pm y + 1, y)$, $(x, y \pm x + 1)$. (arithmetic mod i)
- G_i is a $[i^2, 8, \frac{5\sqrt{2}}{8}]$ family of expanders where $\lambda(G_i) \to 2\sqrt{8-1}$ as $i \to \infty$.



PRF Reformulated: Vélu Formula Approach

We can reformulate the PRF in a similar way:

- Starting with an Elliptic Curve E over $\mathbb{F}_{p^2}$ where $p = 2^a \pm 1$
- Let P_0, Q_0 be a basis for the torsion subgroup $E[2^a]$.
- Define

$$F_k(m) : \mathcal{K} \times \mathcal{M} \to \mathbb{F}_{p^2}$$
$$(k, m) \mapsto E/\langle P_0 + [2^{\frac{a}{2}} k + m] Q_0 \rangle$$

- With message and key space $\mathcal{M} = \mathcal{K} = \mathbb{Z}_{2^{a/2}}$