**SCIS 2022** 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers



# 超特別アーベル多様体によるエクスパンダー族の構成とその暗号応用に向けて
# Construction of expander families from superspecial abelian varieties toward cryptgraphic applications

相川勇輔 * 田中亮吉 † 山内卓也 ‡
Yusuke Aikawa Ryokichi Tanaka Takuya Yamauchi

**キーワード** エクスパンダーグラフ、超特別アーベル多様体、同種写像暗号

## あらまし

頂点集合を超特異楕円曲線とし、同種写像を用いて辺を定義することで得られるグラフを超特異同種写像グラフとよぶ。Pizer[6] は、これらのグラフがエクスパンダー族をなすこと、より強くラマヌジャングラフの族であることを証明した。

エクスパンダー族は連結な無向正則グラフの族で、疎で高い連結性および疑似ランダム性を持ち、理論計算機科学において幅広い応用を持つ。ラマヌジャングラフはその中でも最適なグラフとして定義される。実際、ラマヌジャングラフの構成として Pizer[6] による超特異同種写像グラフの他に Lubotzky-Phillips-Sarnak による LPS グラフ [5] などが知られているが、Charls-Lauter-Goren[2] はこれらのグラフを利用した暗号学的ハッシュ関数を構成した（ただし、LPS グラフに基づく暗号学的ハッシュ関数は現在では破られている）。その後、Pizer によるラマヌジャングラフは、与えれら他 2 つの楕円曲線間の同種写像の計算困難性に基づく鍵共有方式である SIDH の構成に応用され、今日における同種写像暗号分野の確立に本質的に寄与した。

しかしながら、このような著しい性質を持つグラフの構成は数学的に困難なタスクであり、知られている例も多くない。一方で、数学的な観点から、Pizer による超特異楕円曲線に対する結果を、高次元化した対象である超特別アーベル多様体に拡張できるかどうかを問うことは自然である。近年、[3] や [4] 等で、超特別アーベル多様体によるグラフの研究が行われているが、非自明な自己同型の存在によって、これらのグラフの構成では有向なグラフにならざるを得なかった。そこで本研究では、

アーベル多様体とそれらの間の同種写像から
エクスパンダー族を構成できるか？

という問いを立てる。

本研究で我々は、超特別アーベル多様体のグラフをシンプレクティック群のダブルコセットと解釈することで、肯定的な解答を与える。すなわち、我々は超特別アーベル多様体から無向正則グラフの族を構成し、それらがエクスパンダー族であることを証明した [1]。

## 参考文献

[1] Y.Aikawa, R.Tanaka, T.Yamauchi, Expander graphs from superspecial abelian varieties, in preparation.

[2] D-X. Charles, K. Lauter, and E-Z. Goren, Cryptographic hash functions from expander graphs. J. Cryptology 22 (2009), no. 1, 93113.

[3] E. Florit and B.Smith, Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph, arXiv:2101.00919.

[4] B-W. Jordan and Y. Zaytman, Isogeny graphs of superspecial abelian varieties and Brandt matrices, arXiv:2005.09031.

[5] A. Lubotzky, R. Phillips, and P. Sarnak, Ramanujan graphs. Combinatorica 8 (1988), no. 3, 261277.

[6] A-K. Pizer, Ramanujan graphs and Hecke operators. Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 1, 127137.

* 三菱電機 情報技術総合研究所, 〒 247-8501, 神奈川県鎌倉市大船 5-1-1, Aikawa.Yusuke@bc.mitsubishiElectric.co.jp
† 京都大学大学院理学研究科, 〒 606-8502, 京都府京都市左京区北白川追分町 rtanaka@math.kyoto-u.ac.jp
‡ 東北大学大学院理学研究科, 〒 980-8578, 宮城県仙台市青葉区荒巻時青葉 6-3 takuya.yamauchi.c3@tohoku.ac.jp