九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Cryptanalysis on Hash Functions Based on Ramanujan Graphs

趙, 亨騄

https://doi.org/10.15017/1806832

出版情報：九州大学, 2016, 博士（数理学）, 課程博士
バージョン：
権利関係：全文ファイル公表済

（様式６－２）

氏　　名	趙 亨ロク
論　文　名	Cryptanalysis on Hash Functions Based on Ramanujan Graphs （ラマヌジャングラフを用いたハッシュ関数の暗号解析）
論文調査委員	主査　九州大学　　教授　高木 剛 副査　九州大学　　准教授　安田 雅哉 副査　東京大学　　准教授　國廣 昇

論　文　審　査　の　結　果　の　要　旨

本博士論文では，線形群上のラマヌジャングラフを用いた暗号学的ハッシュ関数の安全性の評価を行い，3-regular グラフを用いた場合の一方向性が完全解読可能となる暗号解析理論を構築した．

暗号学的ハッシュ関数 $H:\{0,1\}^* \rightarrow \{0,1\}^\lambda$は，任意長のデータを固定長 λ に圧縮する関数であり，ディジタル署名で利用されるなど暗号理論における基本的な研究対象である．暗号学的ハッシュ関数の安全性としては，逆像 H^{-1} の計算が困難である一方向性と，H(x)=H(y)を満たす x,y を求めることが難しい衝突困難性を満たす必要がある．

Charles, Lauter, Goren は，2009 年に Journal of Cryptology において，Lubotzky, Phillips, Sarnak の特殊線形群上の Cayley グラフ(LPS グラフ)を用いた暗号学的ハッシュ関数を構成した．LPS グラフ上のランダムウォークは急速攪拌性を有するため，高い乱数性を持つと考えられている．有限群 G とその部分集合 S の Cayley グラフは，G の元 g を Vertex として，Vertex={g}に対する Edge は gs (s∈S)で定義される．また，Cayley グラフの中で，隣接行列の固有値のスペクトル･ギャップが Alon-Boppana の不等式を満たす最適なクラスは，ラマヌジャングラフと言われる．上記の LPS グラフは，q = 1 mod 4 となる素数に対して，q-regular となるラマヌジャングラフの無限族である．

群 G と部分集合 S 上の Cayley グラフによる暗号学的ハッシュ関数は，次のように構成される．集合 S の濃度を q として，S の元に番号 $s_0,s_1,\ldots,s_{q-1}$を付け，初期の Vertex を $V_0=\{g_0\}$, $g_0\in G$ とする．整数値のデータ x に対して，x の q 進展開を$(x_0,x_1,\ldots,x_k)\in\{0,1,\ldots,q-1\}^{k+1}$とする．各 x_i (i=0,1,…,k-1)に s_{x_i}を対応させて，Vertex $V_i=\{g_i\}$に繋がる Edge g_is (s∈S)の中から次の Vertex を $V_{i+1}=\{g_is_{x_i}\}$で選択することにより，Vertex の列 $V_0,V_1,\ldots,V_k$ を計算し，終端の Vertex $V_k=\{g_k\}$の値をハッシュ値 H(x)とする．そのため，暗号学的ハッシュ関数の安全性は，グラフ上の比較的短いサイクルを求める問題の困難性を根拠としている．Petit, Lauter, Quisquater は，LPS グラフを用いたハッシュ関数の一方向性を，四元数体のノルム表現 $a^2 + b^2 + c^2 + d^2 = p^k$ (p は 2 以上の素数，k は自然数)の整数解(a,b,c,d)を求める問題に帰着することにより，多項式時間で解読できることを証明した．

本博士論文は，暗号利用に適する 3-regular ラマヌジャングラフ(Chiu, Cubic Ramanujan graphs, Combinatorica 12, pp.275-285, 1992)を用いた暗号学的ハッシュ関数の安全性を考察した．3-regular ラマヌジャングラフでは四元数体のノルム表現が LPS グラフによるハッシュ関数とは異なり，その解読には不定方程式 $a^2 + 2b^2 + 13c^2 + 26d^2 = 2^k$ (k は自然数)を満たす整数解(a,b,c,d)を求める必要がある．ここで，$\omega^2 = -2$, $\Omega^2 = -13$, $\omega\Omega + \Omega\omega = 0$ を満たす ω, Ω に対して，有理数体上の四元数体 D=[1,ω,Ω,ωΩ]の元 α= a + b ω + c Ω + d ωΩ のノルムは $N(\alpha) = a^2 + 2b^2 + 13c^2 + 26d^2$ となる．また，3-regular ラマヌジャングラフは，特殊線形群の元 M を Vertex として持つ．本博士論文では，暗号学的ハッシュ関数の一方向性の解読問題を，行列 M を四元数体 D 上へのリフトすることにより，

ハッシュ関数の生成元 S と反対角行列との積からなる分解問題に帰着する暗号解析法を考察した．実際，素数 2 は四元数体 D の最大整数環において分解して，D の右イデアル類群の類数は 1 であるため，$a^2 + 2b^2 + 13c^2 + 26d^2 = 2^k$ (k は自然数)と表現できる整数(a,b,c,d)が存在する．また，正の自然数 N,d に対して不定方式 $X^2 + dY^2 = N$ の整数解は Cornacchia アルゴリズムより多項式時間で計算可能である．本博士論文では，$(a^2 + 2b^2) + 13(c^2 + 2d^2) = 2^k$ において，$d = 13$, $N = 2^k$ とした場合に Cornacchia アルゴリズムによりハッシュ関数の原像が求まる条件を考察し，3-regular グラフを用いたハッシュ関数に対する一方向性が多項式時間で解読可能であることを証明した．更に，素数 $p \neq 2$ が最大整数環で分解する場合や最大整数環の類数が 2 以上となる四元数体 D を持つラマヌジャングラフを利用した暗号学的ハッシュ関数の攻撃可能性も考察している．

本博士論文の結果は，IEICE Transaction on Fundamentals, Special Section on Discrete Mathematics and its Applications および Mathematics for Industry Special Issue on Mathematical Modelling for Next-Generation Cryptography, Springer において投稿済である．また，平成 27 年 10 月には, Forum Math-for-Industry 2015 においてポスター発表 "Hash Functions from Expander Graphs" に対して Excellent Poster Award を受賞している．

以上の結果は，ラマヌジャングラフを用いた暗号学的ハッシュ関数の安全性評価理論を考察したものであり，暗号理論の分野において学術的に高く評価できる研究業績である．

よって，本研究者は博士（数理学）の学位を受ける資格があるものと認める．