様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　５　月　２２　日現在

機関番号：　１１３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６３３０１５０

研究課題名（和文）一方向性関数の不動点に関する理論基盤の構築

研究課題名（英文）Constructing a theory of fixed points assciated with one-way functions

研究代表者

静谷　啓樹（Shizuya, Hiroki）

東北大学・教育情報基盤センター・教授

研究者番号：５０１９６３８３

交付決定額（研究期間全体）：（直接経費）　　1,200,000円

研究成果の概要（和文）：今日の情報セキュリティにとって一方向性関数は不可欠のものである。本研究の目的は、その一方向性関数を不動点という切り口から再検討することにある。不動点とは、関数 f について f(x)=x が成り立つような x のことであり、不動点では入出力が同じなので関数は一方向性とは見えなくなる。
本研究では特に、楕円曲線上で構成した暗号学的な関数の不動点の性質が未解決であることを踏まえ、それを部分的ではあるが解決した。具体的には、全楕円曲線のうち半数より多い曲線上の関数では自明な不動点を持ってしまうことを示し、また非自明な不動点を持つ関数を導く楕円曲線についても量的な評価を与えた。

研究成果の概要（英文）：It is clear today that the notion of one-way function is essential for us to keep information and information systems secure. The purpose of this research project is to re-investigate one-way functions from a viewpoint of fixed points. Intuitively a fixed point x of a function f is defined as f(x)=x. Since the output is the same as the input, the function looks not to be one-way as far as for the fixed point.
We especially attempted to solve an open question concerning the property of fixed points of an elliptic-curve version of a cryptographic function, and in fact have given a partial solution to the question: among all the elliptic curves, more than a half curves lead to a function that has a trivial fixed point. We have also shown quantitative estimation for non-trivial fixed points.

研究分野：　暗号理論

キーワード：　一方向性関数　不動点　楕円曲線　離散対数問題

１．研究開始当初の背景

現代暗号理論の中心的概念の一つに「一方向性関数」がある。その存在は証明されてはいないが、具体的な候補の関数の一方向性を仮定すれば、暗号系や認証系の基本構成要素が設計どおりに機能する。重要なのは、存在が証明されていないものに依存して情報社会のセキュリティが確保されているという点である。しかし、その存在証明は「P≠NP」や「擬似乱数生成器の存在」と同程度の困難さを持っており、容易には解決できない。

そこで研究代表者はこれまで、一方向性関数を逆方向に計算する難しさの具体例として、暗号系を破る関数の難しさの帰着関係(Sakurai-Shizuya1998)や、一方向性関数が定義された代数系（有限群）そのものが持つ計算量的性質(Hasegawa-Isobe-Shizuya-Tashiro 2009)などの検討を通じて、一方向性関数の存在を下支えしうる事実を証明してきた。本研究は、そのような活動の流れの中で現れた研究テーマである。

例えば、有限素体上の指数関数 $f(x)=g^{\wedge}x \pmod p$ は逆方向の計算が離散対数問題となるため、一方向性と考えられている。ただし、g はその有限体の乗法群の生成元(mod p の原始根)とする。このとき、$f(h)=h$ となる不動点 h が見つかることがある。そこで、そのような (g,h) の ペアはいつも存在するか、という問題が数論の分野で検討されてきたが、これは肯定的に解決されている(G1981, Z1995, CZ1999, H2002)。

一方、このような不動点に関する問題意識を有限体上で定義された楕円曲線上でも考えることが 2010 年に提案された(GS2010)。楕円曲線 E 上の点 $P=(u,v)$ に対して x 座標を抽出する関数を $x(P)=u$ とするとき、E 上の点 G を底とする関数 $f(t)=x(tG)$ を定義する。もし t が $f(t)=t$ を満たすとき、t は不動点となる。このような (G,t) のペアはその有限体上のどの楕円曲線にも存在するかどうかが問題として提起され、未解決である。

以上の例に見た不動点の議論は、Blum-Micali の擬似乱数生成器(BM1984)とその楕円曲線版に関する議論に深く関係しており、進展すれば単なる事実の解明以上に暗号理論に寄与することが期待される。

２．研究の目的

不動点それ自体は数学上の概念であるが、計算機科学など広範な科学／技術分野に現れている。そのような不動点を俯瞰する解説論文としては、25 年以上も前の文献があり(IPSJ1992)、そこでは様々 な分野における不動点の理論のエッセンスが紹介されている。ところが、1992 年当時にはすでに理論計算機科学で重要なコミュニティを形成していたはずの暗号理論研究者の解説がそこには収録されていない。そこで本研究では、暗号理論方面の解説がそこに収録されたと仮定して、少なくともその解説で引用され紹介されるような理論的進展を得たい。

具体的には次の 3 点を目標とする。

(1)未解決問題の解決：不動点に関して[GS2010]で提起された未解決問題を解決する。基本的には、有限体上で（前節で述べた意味での）不動点を有する楕円曲線を数え上げ、それがその有限体上の全曲線にわたるかどうかを評価することになる。また反対に、不動点を一つも持たない楕円曲線の存在の有無と性質を併せて検討する。

(2) 様々な具体例の蓄積：例えば Textbook RSA 暗号化関数にも不動点の存在は知られていた。具体的な暗号系に関係の深い一方向性関数（と見られる関数）は数多くあり、それぞれについて不動点の有無と存在条件などを具体的に解明する。

(3) 帰納的一般化の達成：以上のような事例研究を踏まえて、ある程度の抽象化を施すことで一方向性関数の不動点に関する理論をとりまとめる。おそらく、単射の一方向性関数が最初の統一モデルになるであろう。有限集合の置換と同一視し、巡回置換分解することで不動点（長さ 1 の巡回成分）の存在を明らかにするという道筋が考えられる(研究代表者は既にこのアプローチを公表している(Shizuya-Takagi1988))。

なお本研究は、不動点を含まない一方向性関数の解明とも表裏の関係にある研究である。ただし、本研究は事実の解明が主な作業であり、その成果が暗号技術を直ちに高度化するなどという実利はない。

３．研究の方法

(1) 未解決問題の解決：p を 3 より大きな素数とする。有限体 $\mathbf{F}_p$ 上で定義された楕円曲線 E 上の点 P に対して x 座標を抽出する関数を $x(P)$ とするとき、E 上の点 G を底とする関数 $f(t)=x(tG)$ を定義する。もし t が $f(t)=t$ を満たすとき、それを f の不動点と呼ぶことにする。このような (G,t) はその有限体上のどの楕円曲線にも存在するかどうかが問題として提起され(GS2010)、未解決である。その解決を目指す。

例えば $x=1$ に $\mathbf{F}_p$ 有理点 G を持つ楕円曲線は、その点に対して $t=1$ が自明な不動点になる（$x(tG)=x(1G)=1$ を自明に満たす）。そのような曲線の本数は $\mathbf{F}_p$ 上の楕円曲線全体（$p^{\wedge}2-p$ 本）のうち、どの程度の本数を占めるのかを明らかにする。また、そのような自明なものではない不動点を持つ曲線を数え上げることも検討し、特に位数 2 で x 座標が奇数 $2k+1$ $(k\geqq 0)$ の $\mathbf{F}_p$ 有理点 G を持つ曲線に注目する。というのは、この G を底として $f(2k+1)=x((2k+1)G)=x(G)=2k+1$ という不動点になるからである。問題は、そのような位数 2 の点を含む楕円曲線の本数の数え上げである。さらに、そのような非自明な不動点をまったく持たない曲線についても考察し、その密度を評価する。

(2) 様々な具体例の蓄積：他の様々な一方向性関数（と見られる関数）の不動点を検討する。不動点を調べるからには、定義域と値域が一致している（少なくとも重なっている）必要がある。そのような条件を満たす暗号化関数を具体的な多数の暗号系の中から抽出し、存在条件などを調べる。最も典型的な例は有限集合の間の全単射である。例えば、Textbook RSA 暗号は有限群の全単射になっているが、概念的には全単射は置換と同一視できても、その暗号化関数を置換として具体的に表現することは難しい（元の番号付け自体に公開鍵から秘密鍵を得るための情報がエンコードされてしまうので）。このように、置換として見るか全単射として見るかで、不動点を検討するためのアプローチは異なってくるため、具体的な関数ごとの理論にならざるを得ない。
(3)帰納的一般化の達成：以上のような事例研究を踏まえて、ある程度の範囲限定なり抽象化を施すことで、一方向性関数の不動点に関する理論をとりまとめ試みを行う。基本は有限集合間の全単射となる。その全単射を元の添字の置換と見なし、巡回置換分解することで長さ１の巡回成分（すなわちそれが不動点）の存在条件を探ることになる。このようなアプローチは研究代表者が有限体上の指数関数（離散対数問題）について既に行っている(Shizuya-Takagi1988)。

４．研究成果

特に(1)について成果を得た。(2)については、暗号化関数ではなく情報理論的に安全なカードプロトコルの不動点の考察にとどまった。しかし(3)については、一方向性単射に関する Shizuya-Takagi 1988 のような一方向性置換の巡回置換分解というアプローチに加えて、離散力学系ゼータ関数(discrete dynamical zeta function)とのリンクならびに論理回路の否定複雑度(negation complexity)とのリンク(GMOR2015)も見つかっており、今後の検討課題となっている（NOT ゲートなしに一方向性単射の回路は実現できないことが明らかになっているが、不動点の有無とその性質との関係についてはまだ検討されていない）。

このような達成状況であるため、以下では(1)に関する成果の要旨を述べる。

未解決となっているのは、有限体 $\mathbf{F}_p$ 上の楕円曲線 E の点 G を底にして $h(t)=x(tG)$ なる関数 h を定義したとき、その不動点の性質である。本研究ではこの関数をそのまま扱うのではなく、self-power map の楕円曲線版の不動点を考えることにより分析した。Self-power map とは、x を x^x に対応させる写像であり、その楕円曲線版は E 上の点 P に対して $f(P)=x(P)P$ と定義できる。もし P が f の不動点であれば、関数 h の底を P、$t=x(P)$ とおくことで $h(t)=x(tP)=x(P)=t$ となり、t は h の不動点となる。そこで本研究ではもっぱら楕円曲線版の self-power map f の不動点を検討した。以下では素数 p は 3 より大きいものとし、楕円曲線の定義体は常に有限体 $\mathbf{F}_p$ とする。

まず、「自明な不動点」と「位数に基づく不動点」を定義する。自明な不動点とは点 P について、$x(P)=1$ となっている点のことである。このとき、$f(P)=x(P)P=P$ が成り立つ。一方の位数に基づく不動点とは、点 P の位数が n のとき、$x(P)=kn+1 \quad (k>1)$ となっている点のことである。このとき、$f(P)=x(P)P=(kn+1)P=P$ が成り立つ。本研究では一般の n についてまでは解明できなかったが、$n=2$ については結果を得た。

$\mathbf{F}_p$ 上で定義された楕円曲線は同型性などを無視すれば p^2-p 本存在する。本研究では、このうち f の自明な不動点を持つ楕円曲線の本数 N_1、位数 2（$n=2$）の不動点を持つ楕円曲線の本数 N_2 を評価した。得られた結果は次のとおりである。

(i) $p(p+1)/2 > N_1 \geqq p(p-1)/2$
(ii) $N_2 \geqq (p-1)(p-2)/6$

このうち (i) については、$x=1$ に $\mathbf{F}_p$ 有理点を持つ楕円曲線の単純な数え上げであり、0 を含む平方剰余元の個数や、与えられた条件での 3 次特異曲線の数などから自然に導かれる。$\mathbf{F}_p$ 上で定義された楕円曲線の半分以上が自明な不動点を持つことを示している。(ii) については、p と $2p$ をそれぞれ 3 つの相異なる非負整数に分割する仕方の数え上げ問題に帰着されることを示した。これは、楕円曲線の 2-ねじれ群が単位元を除いてすべて F_p 有理点である場合に、少なくとも一つの点の x 座標は奇数であることを利用したものである。

上記の(i)(ii)はそのまま未解決問題の関数で不動点を持つ楕円曲線の本数になり、未解決問題に対する部分的な解となっている。今回は位数 $n=2$ の点についての評価となったが、一般の位数 n の点について解明することはもちろん今後の課題である。

＜引用文献＞

[Guy1981] Richard K. Guy, Unsolved Problems in Number Theory, Springer-Verlag (1981).
[BM1984] M. Blum, S. Micali, “How to generate cryptographically strong sequence of pseudorandom bits,” SIAM J. Compt., vol.13, no.4, pp.850-864 (1984).
[Shizuya-Takagi1988] H. Shizuya and T. Takagi, “Cyclic permutation algorithm for solving discrete logarithm problem,” Proc. 1988 Workshop on Information Security and Cryptography (July 1988).
[IPSJ1992] 『情報処理』特集：不動点をめぐって，情報処理学会，vol.33, no.4, pp. 308-399 (1992).

[Z1995] W. P. Zhang, “On a problem of Brizolis,” Pure Appl. Math., vol.11, pp.1-3 (1995).
[Sakurai-Shizuya1998] K. Sakurai, H. Shizuya, “A Structural Comparison of the Computational Difficulty of Breaking Discrete Log Cryptosystems,”Journal of Cryptology, Vol.11,No.1, pp.29-43 (1998).
[CZ1999] C. Cobeli and A. Zaharescu, “An exponential congruence with solutions in primitive roots,” Rev. Roumaine Math. Pures Appl., vol.44, no.1, pp.15-22 (1999).
[Holden2002] J. Holden, “Fixed Points and Two-Cycles of the Discrete Logarithm,” ANTS 2002, LNCS 2369, Springer-Verlag, pp.405-415 (2002).
[Hasegawa-Isobe-Shizuya-Tashiro2009] S. Hasegawa, S. Isobe, H. Shizuya, K. Tashiro, “On the Pseudo-Freeness and the CDH Assumption,”International Journal of Information Security, vol. 8, Issue 5, pp. 347-355 (2009).
[GS2010] L. Glebsky, I. Shparlinski, “Short cycles in repeated exponentiation modulo a prime,” Design, Codes and Cryptography, vol.56, pp.35-42 (2010).
[GMOR2015] S. Guo, T. Malkin, I. C. Oliveira, A. Rosen, “The power of negations in cryptography,” Theory of Cryptography Conference (TCC2015), LNCS 9014, Springer, pp.36-65 (2015).

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

① Shingo Hasegawa, Shuji Isobe, Jun-ya Iwazaki, Eisuke Koizumi, and Hiroki Shizuya, “A Strengthened Security Notion for Password-Protected Secret Sharing Schemes,” IEICE Trans. Fundamentals, Special Section on Cryptography and Information Security, vol.E98-A, no.1, pp.203-212 (2015).**【査読有】**
② Shingo Hasegawa, Shuji Isobe, Jun-ya Iwazaki, Eisuke Koizumi, and Hiroki Shizuya, “A Rigorous Security Proof for the Enhanced Version of Password-Protected Secret Sharing Scheme,” Interdisciplinary Information Sciences, vol.22, no.1, pp. 31-55 (2016). **【査読有】**
③ Takaaki Mizuki and Hiroki Shizuya, “Computational Model of Card-Based Cryptographic Protocols and Its Applications” (Invited Paper), IEICE Trans. Fundamentals, Special Section on Cryptography and Information Security, vol. E100-A, no.1, pp.3-11 (2017). **【査読有】**
④ Hiroki Shizuya, “On the fixed points of an elliptic-curve version of self-power map,” Interdisciplinary Information Sciences (accepted for publication) (2018). **【査読有】**

〔学会発表〕（計 2 件）

① M. Fukumitsu, S. Hasegawa, S. Isobe and H. Shizuya, “On the Impossibility of Proving Security of Strong-RSA Signatures via the RSA Assumption,” Proc. 19th Australasian Conference on Information Security and Privacy (ACISP 2014), LNCS 8544, Springer, pp.290-305 (2014).**【査読有】**
② S. Hasegawa, S. Isobe, J. Iwazaki, E. Koizumi, H. Shizuya, “Password-protected Secret-sharing Schemes without Random Oracles,” Proc. 2014 International Symposium on Information Theory and Its Applications (ISITA 2014), IEICE pp.579-583 (2014).**【査読有】**

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://www.isl.is.tohoku.ac.jp/~shizuya/

６．研究組織
(1)研究代表者
静谷　啓樹　（SHIZUYA, Hiroki）
東北大学・教育情報基盤センター・教授
研究者番号：50196383

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者

(　　)

研究者番号：

(4)研究協力者

(　　)