様式 C-7-2

自己評価報告書

平成 21 年 3 月 31 日現在

研究種目：基盤研究（B）
研究期間：２００６～２００９
課題番号：１８３４０００５
研究課題名（和文）　ペアリングに基づく楕円暗号の安全性の数論的研究

研究課題名（英文）　On security of pairing based elliptic curve cryptosystems in view of number theory

研究代表者：
佐藤　孝和 (SATOH　TAKAKAZU)
東京工業大学・大学院理工学研究科・准教授
研究者番号：７０２１５７９７

研究分野：数論
科研費の分科・細目：数学・代数学
キーワード：ペアリング、楕円曲線、公開鍵暗号

1. 研究計画の概要

(1) 本研究ではペアリングを用いた楕円曲線暗号に用いられる楕円曲線の離散対数問題および関連する諸問題の難しさ（時間計算量）を評価するための最初の研究としてそれらの上からおよび下からの何らかの非自明な評価を得ることを目標とした。

(2) 一般的な楕円曲線上の離散対数問題が困難であろうことは数学・暗号両サイドでのコンセンサスが得られているが、ペアリング暗号に適する曲線に限定した場合の離散対数問題の困難性を調べるために、数論的代数幾何、計算代数学、などの種々の手法を用いて計算量評価を得るための考察を行い、離散対数問題を解くことに結び付くアルゴリズムを作成し、暗号サイズの問題への影響を分析する計画であった。

2. 研究の進捗状況

(1) ペアリング反転ができればその値域を共有するすべてのペアリングを用いた暗号は多項式時間で解読されることは従前より知られていたが、ペアリング反転自体の困難性については本研究ではそれまで知られていた結果よりも良い結果が得られた。具体的にはペアリング反転の多項式補間について、従来は次数のみの評価しか得られていなかったが、本研究の結果として、そのような多項式の係数を明示的に与え特に重みについては最良の結果を得た。楕円曲線が関連する多項式補間で簡明な明示公式はないだろうというおおかたの予想を覆す研究成果である。Lagrange 分解式を用いて Kummer 理論をペアリング反転に適用するという着想により従来の組み合わせ論的手法では到底得られなかった成果をあげることができた。

(2) 算術演算ライブラリーのメモリー管理を改良した。この過程で、副産物として整数環上の Euclid 素数列に関する Shanks 予想の有限体上の一変数多項式環版を否定的な解決し、他方、もとの整数環上の場合の Shanks 予想の正しさを示唆する計算例を得た。

(3) 頂切離散附値環の拡大についての Deligne の定理を、剰余体が必ずしも完全でない場合に一般化した。これは例へば一般の完備離散附値環上のアーベル多様体の等分点から生ずる分岐の研究などに応用が期待される。

(4) 直近の研究成果として楕円曲線を介して種数 2 の超楕円曲線暗号の安全性評価、ペアリング暗号に適する曲線の構成法を得た。

3. 現在までの達成度

① 当初の計画以上に進展している

（理由）

本研究により既にいくつかの研究成果が得られている。しかも (1) ～ (3) は査読の有る

国際会議、査読の有る論文誌、国際会議の招待講演などにより発表が行われた。(4) も査読の有る国際会議および国際会議の招待講演で発表することが決まっている（プログラムまたは発表者名が既に公表されている）など、質の高い研究成果である。研究計画時点では楕円曲線に関する結果を主眼としたが、本自己評価時点では超楕円曲線、アーベル多様体などに関する研究成果も得られはじめており、本研究は当初の計画以上に進展していると判断される。

4. 今後の研究の推進方策

(1) 平成 21 年度は本研究の最終年度である。平成 20 年度に得られた研究成果を積極的に国際会議、論文誌等に発表し、内外の研究者との交流を通して研究の一層の進展を目指す。

(2) 楕円曲線離散対数問題の困難性を分析する際に、それが多項式時間で計算可能な同種の意味で含まれているアーベル多様体の等分点を使うことが有効であるかもしれないことが示された。これが本当に有効な手法であるのか、あるいは有効ではないのかについて検討する。

5. 代表的な研究成果

（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 3 件）

① N. Kurokawa, T. Satoh, Euclid prime sequences over unique factorization domains, 17, 145-152(2008), 査読有

② T. Satoh, Closed formulae for the Weil pairing inversion, Finite fields and their appl., 14, 743-765(2008), 査読有

③ T. Hiranouchi, Y. Taguchi, Extensions of truncated discrete valuation rings, Pure and Applied Mathematics Quarterly, 4, 1205-1214(2008), 査読有

〔学会発表〕（計 3 件）

① 佐藤孝和、超楕円暗号に適したある種の種数 2 の超楕円曲線の生成法、2009 暗号と情報セキュリティーシンポジウム、2009.01.23, 大津、日本

② Y. Taguchi, Extensions of truncated discrete valuation rings (joint work with Toshiro Hiranouchi) Pan Asian Number Theory Conference, 2009.01.10, Pohang, Korea

③ T. Satoh, On Pairing Inversion Problems, Pairing Conference 2007, 2007.07.04, Tokyo, Japan.