Efficient Algorithms to Solve the Elliptic Curve Discrete Logarithm Problem over Finite Fields of Characteristic Two

黄, 筠茹

https://doi.org/10.15017/1500510

出版情報：九州大学, 2014, 博士（機能数理学）, 課程博士
バージョン：

（様式６－２）

氏　　名	黄　筠茹
論　文　名	Efficient Algorithms to Solve the Elliptic Curve Discrete Logarithm Problem over Finite Fields of Characteristic Two (標数 2 の有限体上の楕円曲線離散対数問題の効率的な解法アルゴリズム)
論文調査委員	主査　九州大学　教授　髙木　剛 副査　九州大学　訪問教授 / 富士通研究所　穴井 宏和 副査　九州大学システム情報科学府　教授　櫻井 幸一 副査　台湾大学　准教授　鄭 振牟

論　文　審　査　の　結　果　の　要　旨

本論文では、グレブナ基底を用いた楕円曲線暗号の安全性に関する考察を行った。楕円曲線暗号は、RSA 暗号の素因数分解問題とは異なり、有限体上の楕円曲線上の離散対数問題(ECDLP)の困難性を安全性の根拠としている。ECDLP の効率的な解法として、Pollard により提案された ρ 法がある [Math.Comp.78]。Pollard の ρ 法は、一般の巡回群に対して適応可能な汎用的なアルゴリズムであり、鍵サイズ n(ビット長)に対して指数時間 $O(2^{n/2})$ の計算量が必要となる。一方、Eurocrypt2012 において Faugère-Perret-Petit-Renault は ECDLP の新たな攻撃法として、Weil 降下法と言われる Semaev 多項式を利用した指数計算法をグレブナ基底により高速化する新しい攻撃方法(FPPR 法)を提案した。その後、Asiacrypt2012 において Petit-Quisquater は、楕円曲線暗号の歴史で初めて指数時間のバリアを突破した準指数時間 $O(2^{n^{2/3}\log n})$ の計算量となる見積もりを与えた。本研究課題では、Semaev 多項式の対称性に注目し、基本対称式を用いた表現により degree of regularity が増大しない高速化を行った。

FPPR 法では、$GF(2^n)$ 上の楕円曲線上の 2 点 P,Q に対して、Q=dP を満たす d を求める離散対数問題を考える。関係探索ステップでは、Semaev 多項式を用いて、乱数 s,t に対して分解 $sP+tQ = P_1+P_2+\cdots+P_m$(ただし $P_1,P_2,\cdots,P_m$ は因子基底 F_V に含まれる)を求める。ここで、m 次 Semaev 多項式 $S_m(x_1,x_2,\cdots,x_m)$ は各変数 x_i に対して次数 2^{m-2} の対称多項式であり、楕円曲線上の点 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2),\cdots,P_m=(x_m,y_m)$ が $P_1+P_2+\cdots+P_m = \infty$ を満たす必要十分条件は $S_m(x_1,x_2,\cdots,x_m)=0$ となる。そのため、点 R=sP+tQ の x 座標 x_R に対して、$S_{m+1}(x_1,x_2,\cdots,x_m,x_R)=0$ の解から 1 個の関係式を得ることができる。もし求めた解 x_i が F_V に含まれない場合は、s,t を取り直して別の分解 sP+tQ を試みる。ここで、関係式 $s_jP+t_jQ = \Sigma P_{ij}$ を十分な個数集めることにより、$sP+tQ=\infty$ を満たす s,t を求め、結果として離散対数問題 Q=(-s/t)P を解読できる。

本博士論文では、FPPR 法の計算量と使用メモリ量を削減する手法を考察した。特に、合成数の拡大次数に対して提案された Semaev 多項式の対称性を利用した既存の高速化手法に注目し、それを素数次拡大に適応する方法を提案し、理論的な計算量の見積もりと計算機実験による評価を与えた。提案方式では、グレブナ基底の途中で多項式の次数(degree of

regularity)が増大しない拡大体の基底表現を利用することにより計算用とメモリ量を削減している。改良アルゴリズムにより、拡大次数 29 次の標数 2 の有限体上で定義される楕円曲線の離散対数問題を、計算機代数ソフトウェア Magma を用いて AMD Opteron 6276(メモリ 512GB)において約 34 日で解くことができた。

本博士論文の結果は、The 8th International Workshop on Security (IWSEC 2013),において発表を行い、Springer 社の Lecture Notes in Computer Science, Vol. 8231, pp. 115-132, 2013 として公表済である。また、同論文の Full paper は、Pacific Journal of Mathematics for Industry に受理されて 2015 年に出版予定である。この結果は、グレブナ基底を用いて楕円曲線暗号の安全性解析を詳細に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（機能数理学）の学位を受ける資格があるものと認める。