【 19 】

氏名	宮地充子（みやじあつこ）
博士の専攻分野の名称	博士（理学）
学位記番号	第 13479 号
学位授与年月日	平成 9 年 12 月 16 日
学位授与の要件	学位規則第 4 条第 2 項該当
学位論文名	Studies on security and efficiency of elliptic curve cryptosystems （楕円曲線暗号の安全性と効率に関する研究）
論文審査委員	（主査） 教授 山本 芳彦 （副査） 教授 伊吹山知義　教授 日比 孝之

論文内容の要旨

'86年にMillerとKoblitzにより独立に楕円曲線暗号が提案された。楕円曲線暗号は，有限体上の離散対数問題(DLP)の概念を楕円曲線上に応用した楕円曲線上の離散対数問題（EDLP）を用いる暗号である。提案当初，EDLPは効率的な解法がないことから，DLPより難しい問題である，つまり鍵サイズが小さくできると考えられていた。しかし'91年にMenezes，岡本，VanstoneによりEDLPをDLPに帰着させる解法（MOV-reduction）が提案された。MOV-reductionは，ある種の楕円曲線E/F_p上のEDLPを同じF_p上のDLPに帰着させる非常に強力な解法である。このような楕円曲線は，暗号化/復号化の実行時間の観点から，暗号に用いる利点はない。MOV-reductionは，全ての楕円曲線に効率的に適用される解法ではない。しかしながら，どのような楕円曲線に適用できないか研究されていなかった。さらに楕円曲線暗号では，楕円曲線上の加法を行なう際の計算量が多いため，鍵サイズに比較して実行時間がかかるという問題がある。

本研究では，MOV-reductionが適用できない楕円曲線について考察し，MOV-reductionが無効になる楕円曲線の構成方法を与えた。また本研究では，楕円曲線の加算を高速に実現する方法を検討し，その楕円曲線の構成方法も与えた。

論文(1)では，MOV-reductionが無効になる楕円曲線について考察した。MOV-reductionの楕円曲線暗号に対する適用結果は，3パターン考えられる。準指数時間攻撃となる場合，指数時間攻撃となる場合，そして無効になる場合である。これまでどのような場合にMOV-reductionが無効になるかがわかっていなかった。ここでは，F_p上の位数pをもつ楕円曲線では，定義体の拡大体F_{p^k}上への単射準同型が構成できないことから，MOV-reductionが無効になることを示した。さらに，MOV-reductionの$F2^r$への拡張方法を示し，これにより，提案の楕円曲線を除く全ての楕円曲線が，入力の多項式時間でMOV-reduction適用可能になることを示した。

論文(2)では，MOV-reductionが無効になる楕円曲線暗号の高速化について考察した。楕円曲線暗号の実行速度は，楕円曲線の加算に要する時間に依存し，加算の実行時間は楕円曲線及びそのベースポイントの設定により異なる。本研究ではこの点に着目し，特に楕円曲線とベースポイントという2つのパラメータを1パラメータ化し，このパラメ

ータをコントロールすることにより，処理の高速化を可能にした。これにより，楕円曲線暗号の一つの機能である署名生成において，約30％高速化が実現できた。

論文(3)では，MOV-reduction が指数時間攻撃になる場合について考察した。MOV-reduction が効率的な攻撃になるのは，準指数時間攻撃になる場合のみで，指数時間攻撃になる場合も，楕円曲線暗号の安全性に問題を与えない。そこで本論文では，この種の楕円曲線暗号を取り上げ，楕円曲線の定義体を操作することにより，その実行時間を高速にする方法を与えた。

また，楕円曲線暗号では安全性の観点から，楕円曲線を定期的に変更することが必要である。この際，楕円曲線上の離散対数問題は，独立になるように変更し，安全性，メモリサイズ，実行速度及び演算ソフトは，変更しないことが望ましい。本論文では，isogenous 楕円曲線を暗号に利用することにより，安全性，メモリサイズ，実行速度及び演算ソフトを変更せず，独立な楕円曲線上の離散対数問題に変更する方法を与えた。

論文審査の結果の要旨

本研究は，楕円曲線暗号に対して MOV-reduction が適用できる条件について考察し，有限体上に定義された楕円曲線上の任意の離散対数問題が多項式時間内で MOV-reduction が適用できる離散対数問題に帰着することを示した。また，楕円曲線暗号の署名生成や効率についても考察し，これら一連の研究は，楕円曲線暗号理論の新たな進展をもたらした。よって，本論文は，博士（理学）の学位論文として十分価値あるものと認める。