氏　　名	根・　健太
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第４７５７号
学位授与の日付	平成２５年　３月２５日
学位授与の要件	自然科学研究科　産業創成工学専攻 （学位規則第５条第１項該当）
学位論文の題目	Proposals of Multiplication and Inversion Methods in Extension Field for Scalable Asymmetric-key and Fast Symmetric-key Cryptosystems （拡張性の有る非対称鍵暗号と高速処理可能な対称鍵暗号のための拡大体での乗算および逆元計算法の提案）
論文審査委員	准教授　野上　保之　　教授　舩曳　信生　　准教授　中西　　透

学位論文内容の要旨

本論文では，次世代の非対称鍵暗号方式が課す拡大体のパラメータ制約と，同方式が求める拡大体のパラメータに対する拡張性に，より柔軟に対応できる拡大体（ガロア体）での乗算法として，ガウス周期正規基底（Gauss period Normal Basis: GNB）を適用した循環ベクトル乗算アルゴリズム（Cyclic Vector Multiplication Algorithm: CVMA）を提案し，その柔軟性を理論的に検証する。また，Advanced Encryption Standard (AES) をはじめとする対称鍵暗号方式の処理を従来実装よりも高速化するために，冗長表現基底（Redundantly Represented Basis: RRB）および複雑混合基底（More Miscellaneously Mixed Bases: MMMB）を提案する。

近年，次世代の非対称鍵暗号方式として，ペアリングベース暗号方式が注目を集めている。この暗号方式の処理を高速化する手段として，拡大体での算術計算，とくに乗算の高速化は非常に有効である。一方で，この暗号方式では拡大体のパラメータである標数および拡大次数に対して大きな制約を課す場合がある。ゆえに，ある程度の高速処理を可能とし，かつこれらのパラメータに対して柔軟に対応できる乗算法が必要とされる。この要求を満たす拡大体での乗算法として，CVMA が提案されている。この CVMA は GNB の一部である特殊な基底を適用しているが，速度面を考慮した場合，GNB 自身を適用した方が拡大体のパラメータに対する柔軟性は向上する。そこで本論文では，従来の CVMA から，GNB を適用した CVMA へ改良を行う。さらに，CVMA の柔軟性を理論的な指標で示すために， GNB の存在確率を導出するための定理を提案する。この定理から，速度面を考慮した際に，改良した CVMA のパラメータに対する柔軟性がより高いものであることを論証する。

一方で，対称鍵暗号の分野では，AES およびそれに類似する暗号方式のハードウェア実装報告が盛んに行われている。これらの実装の多くは，AES 内の処理で最も低速な処理である SubBytes および InvSubBytes を高速化するために，本来の AES で採用されているような拡大体 F_{2^8} での逆元計算に替わり，その同型な逐次拡大体（合成体）である $F_{((2^2)^2)^2}$ や $F_{(2^4)^2}$ での逆元計算を採用している。本論文では，$F_{((2^2)^2)^2}$ よりも逆元計算が高速な $F_{(2^4)^2}$ に着目し，$F_{(2^4)^2}$ での逆元計算を高速化できる RRB を提案する。その結果，$F_{(2^4)^2}$ での逆元計算を，著者が知る限りの既存研究では $4T_{\mathrm{AND}}+10T_{\mathrm{XOR}}$ で提供されるところを，$4T_{\mathrm{AND}}+7T_{\mathrm{XOR}}$ で実現する。ただし，T_{AND} および T_{XOR} は AND および XOR ゲートの遅延時間を意味している。また，上記のように $F_{(2^4)^2}$ での逆元計算を採用する場合，逆元計算前後の同型写像とその逆写像を高速化することも重要である。より高速に写像を行うためには，効率の良い F_{2^8} から $F_{(2^4)^2}$ への写像行列とその逆写像行列を準備する必要がある。そこで本論文では，AES 内の処理である MixColumns および InvMixColumns で実行される拡大体での乗算を工夫することよって，効率の良い F_{2^8} から $F_{(2^4)^2}$ への写像行列とその逆写像行列の組を選択可能にする MMMB を提案する。その結果，同型写像およびその逆写像を，著者が知る限りの既存研究では $3T_{\mathrm{XOR}}$ で提供されるところを，$2T_{\mathrm{XOR}}$ で実現する。

論文審査結果の要旨

申請者は，拡張性のある非対称鍵暗号を実現するためのベクトル乗算法，および高速に処理できる対称鍵暗号を実現するためのベクトル逆元計算法を,それぞれ奇標数体および2進体と呼ばれる有限体(拡大体）に対して提案をしている。それぞれペアリング暗号やAES暗号に代表される非対称鍵暗号および対称鍵暗号は，拡大体における演算（とりわけ乗算および逆元計算）を，様々なパラメータに対応しながら，かつ多用するため，これらをより汎用的，かつ高速に処理できるように実現することは重要である。

博士論文において申請者は，まず奇素数を法とする拡大体（奇標数体）におけるベクトル乗算法を提案している。そのベクトル乗算法の計算効率を大きく左右するものは，その拡大体の元を表現するために用いる基底であるとし，計算効率を評価の観点に含め，かつ様々なパラメータに対応できることを主たる目的として，ガウス周期正規基底（GNB）を用いることを提案している。そして，幾つかあるGNBの構成条件に基づき，これを（計算効率という観点から）最適な形で利用できる確率（そのGNBが構成できる確率）を理論的に与えている。その理論式に基づき，その計算効率への影響（計算コストの期待値）について，従来法と比較しながら評価を与えている。

続いて，標数を2とする拡大体（2進体）における高速処理可能な逆元計算法を提案している。この演算はAES暗号におけるSubBytes処理などで用いられるが，その計算を効率よく行うために，あえて冗長性を与える基底を用いることを提案し，伝送するデータビット数は増えるものの，計算効率が上がることを示している。一方で，そのために増加しがちな回路規模を，重複する計算部分を一つの回路ブロックとして実現・併用することによって，削減する方法を提案している。回路規模とバランスをとりながら，もっとも処理効率のよい逆元計算回路を，処理時間および回路規模をもって評価している。

以上，本博士（甲）申請論文は，岡山大学大学院自然科学研究科博士（工学）の要件を十分に満たすものであると判定する。