3 値論理による公開暗号ハードウェアの研究

白勢 政明
北陸先端科学技術大学院大学

2006 年 1 月 10 日

論文の内容の要旨

公開鍵暗号の主要なタイプに RSA 暗号と ElGamal 暗号とがある。RSA 暗号の暗号化/復号化処理には公開鍵 N を法とする剰余乗算が多数必要であり、ElGamal タイプではある有限体での乗算を繰り返し必要になる。本研究は ElGamal 暗号の一種である XTR に着目している。XTR は従来の ElGamal 暗号と較べて、公開鍵のサイズを 1/3 にでき、処理に暗号化/復号化に必要な処理も効率的になる。本研究では、標数 3 の体を用いると、更に公開鍵のサイズを半分にできることを示し、標数 3 の体での XTR のハードウェア実装が主題の一つである。

標数 3 の体を実装するために、3 値論理ゲートの構成法である TG 法を提案する。TG 法は現時点での最良と思われる 3 値論理ゲートの構成法である。TG 法は Olson 法による 1 変数関数ゲートと T ゲートをモジュールとして、任意の関数のゲート構成する方法である。Olson 法だけを用いる方法より、性能や任意の関数のゲートの構成の容易さから、TG 法が優れている。TG 法や Olson 法の長所は、CMOS と同様に定常時には電流が流れない (つまり消費電力が少ない) ことと、現在の CMOS の加工技術で製造できることである。実際にバイナリのゲートと、TG 法と Olson 法での 3 値論理ゲートの違いは、閾値の異なる MOSFET を複数用意することと複数の電源を用意するだけである。しかし、これらは消費電力の削減のために、バイナリの CMOS にも行われるようになっている。

TG 法によるゲートは、従来の CMOS と構造的にほとんど同じなので、HSPICE でシミュレーションすることができる。本論文で、TG 法による 3 値論理ゲートを用いた、標数 3 の体での XTR のハードウェアを設計し、性能評価を行う。

次に 3 値論理ゲートを用いて、大規模な Wallace tree 乗算器を設計することを提案する。対称 3 進表現を用いると、Wallace tree の構造が著しく単純になり、Wallace tree 乗算器の設計が容易になる。標数が大きな体を用いる ElGamal 暗号と RSA 暗号は、暗号化/復号化の処理に多ビットの乗算が必要であり、3 値論理で設計した大規模乗算器は、これらの暗号の処理に有効である。暗号処理には、他に加算や、「Montgomery 乗算」、「擬 Mersenne 素数を法とする剰余計算」というアルゴリズムも用いられるため、これらが対称 3 進表現でも行うことができなければならないが、本論文ではこれらが可能であることを示す。TG 法を用いた 3 値論理ゲートでの、加算器、乗算器、これらのアルゴリズムのためのハードウェアの設計法について説明する。

キーワード:　3 値論理, 公開鍵暗号, 対称 3 進表現, 標数 3 の有限体, TG 法