被覆攻撃の対象となる有限体拡大体上の楕円・超楕円曲線から被覆曲線の構成に関する研究

Construction of Cover Curves from Elliptic/Hyperelliptic Curves over Extension of Finite Fields Subjected to Cover Attack

登丸尚哉・暗号・認証分科会・中央大学大学院

・研究背景

拡大体上定義された楕円・超楕円曲線暗号は、鍵長を小さくしても高い安全性とともに効率的なハードウェア実装が期待され、IoT機器の暗号方式として広く利用されてる。その反面、一部の拡大体上の楕円・超楕円曲線は被覆攻撃という攻撃手法により安全性が低下する危険性があり、被覆攻撃の対象となる曲線の分類や、被覆曲線の構成、攻撃を利用した暗号解読の計算機実験等の被覆攻撃に関する解析が求められる。

・提案手法

これまでに被覆攻撃の対象になると分類された楕円・超楕円曲線に対して、関数体の生成元の最小多項式を利用したDiemの手法を元に、それぞれの曲線の形に合わせた計算機実験を行い、被覆曲線の構成を行う。

・今後の方針

・これまで被覆曲線を構成した元の楕円・超楕円曲線とは異なる種数、拡大次数の曲線に構成を行う
・研究に関連して、被覆攻撃の対象となる曲線の分類に取り組む