有限体の拡大体上の楕円曲線とその被覆曲線の離散対数問題に対する安全性評価

Security Evaluation of Elliptic Curve Discrete Logarithm Problem over Extensions of Finite Field under Cover Attack

西垣佳亮・暗号分科会・中央大学大学院

Abstract - The objective of this study is to verify the impact of cover attacks on the security of elliptic curve cryptography through actual computational experiments. It is known that there exist elliptic curves over extensions of finite fields where the security is compromised due to covering attacks. In this study, we implemented cover attacks against elliptic curves over cubic extension fields and confirmed the decrease in security.

研究背景と目的

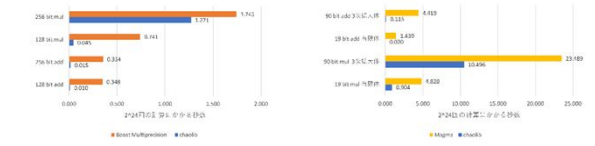
- 本研究の対象である楕円曲線暗号はそれ以前の暗号と比較して，より短い鍵長でより高い安全性を実現できる優れた暗号方式である．
- 被覆攻撃はある条件を満たす楕円曲線に対して適用することでその曲線の離散対数問題を解くコストが下がるものである．
- 被覆攻撃を実際に適用して安全性を検証した研究は少ない．
- 本研究では実際の楕円曲線暗号への攻撃を通して，暗号の安全性を評価することを目的とする．

手法

- 楕円曲線に対してλ法による並列計算で離散対数問題を解く
- 被覆攻撃を行い，被覆曲線を構成する
- 被覆曲線に対してdouble large prime 法で解く

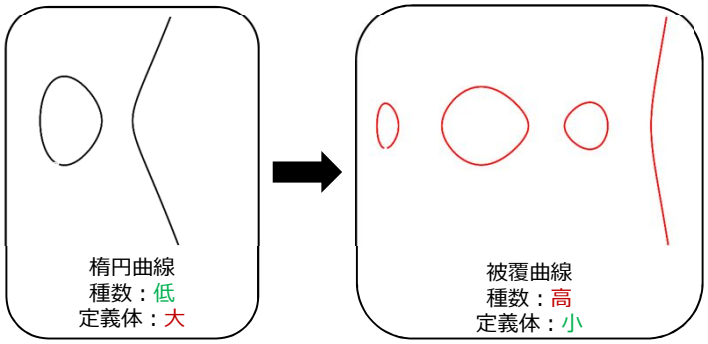
実装

可能な限り大きな問題を解くことが目標
⇒既存の物では遅いため，C++でフルスクラッチ開発を行った．



被覆攻撃

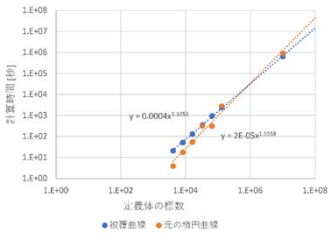
拡大体上定義された楕円曲線の離散対数問題を別の曲線に移す手法



実験

本研究では鍵長に換算して35 bitから68 bitまでの 3 次拡大体上の楕円曲線と素体上種数 3 の被覆曲線の離散対数問題を実際に解いた．

定義体の標数	$\#\mathcal{J}_C(K)$	bit	double large prime 法 関係収集	線形代数	合計	ラムダ法
4,079	67,867,385,039	36	16.94	4.16	21.10	3.91
8,147	540,745,792,523	39	44.45	7.42	51.87	17.72
16,223	4,269,662,081,567	42	126.16	3.76	129.92	54.41
32,911	35,647,012,903,144	46	356.58	2.66	359.24	320.39
65,011	356,470,129,031,444	48	915.73	24.19	939.92	317.12
129,967	2,195,327,319,715,496	51	2,394.18	6.39	2,400.57	2,750.59
10,000,019	250,001,424,987,670,554,266	68	約 622,080	約 12,960	約 635,040	約 887,040



考察

計算時間は楕円曲 線と被覆曲線の双方で理論値通りのオーダーであった．標 数が $4.4 \cdot 10^5 < 2^{19}$ を超えてからは，被覆曲線のほうが元 の曲線より離散対数問題が解き易くなることが分かった． 126 bit の楕円曲線離散対数問題は，被覆攻撃を適用で きれば 112 bit の楕円曲線暗号離散対数問題を ρ 法で解く のと変わらない時間で解くことができる．現在の λ 法に よる楕円曲線暗号の解読記録は 112 bit であるため，126 bit 以下の楕円曲線暗号は解読される危険性がある． 2008 年，山外ら [1] は 35 bit までの離散対数問題を長 尾の指数計算法を用いて解き，68 bit の離散対数問題を 解くために 230 秒の時間が必要だと見積もった．本研究で はハードウェアの進化や実装の工夫もあり $63400 < 2^{20}$ 秒で解くことができた．この結果は本研究が行われるまで の 16 年間の間に暗号の解読は 2^{10} 倍も速くなっているこ とを示している．

参考文献

- 山外一徳, 小崎俊二, 松尾和人. 拡大体上の楕円曲線暗号に対する index calculus について. 日本応用数理学会 研究部会連合発表会 数論アルリズムとその応用(JANT) セッション, 2008.