楕円曲線暗号解読で 10 時間を 1 秒に短縮する学習λ 法

後　保範（インダストリスパコン推進センター）

公開鍵暗号は RSA 暗号から楕円曲線暗号(ECC)に移行している。ECC 解読のλ 法(ρ 法の並列版)が学習できることを発見。パソコンで 44 件の 60 ビット ECC (70 ビット相当)の解読実験をした。解読時間はρ 法の 10 時間が、学習λ 法で 1 秒に短縮した。学習は ECC 上の固定点を間に挟むことで可能にした。そのため今後、AI により更に高速化も期待できる。

Learning λ　method for reducing elliptic curve cryptanalysis from 10 hours to 1 second.

Yasunori Ushiro (ISCPC)

1. はじめに

暗号の 2010 年問題で、1024 ビット RSA 暗号(RSA-1024)は RSA-2048 か 256 ビットの楕円曲線暗号(ECC-256)に移行した。ECC は高度な解法がなく、ρ法(並列はλ法)が最速である。ECC-256 は RSA-2048 より数万倍強固な暗号と言われている。しかし、λ法は学習する(学習λ法)ことで 4 万倍高速化できた。数十 TB の SSD なら百万倍の高速化も可能である。学習λ法は、毎回異なる ECC 上の点を固定点の導入で実現した。固定点なので AI による初期値選択で更に高速化の可能性がある。また、解読は多倍長整数演算で、FPGA(Field Program Gate Array,最終的には ASIC 化で暗号専用 LSI)でも高速化可能である。AI での高速化(AI 学習λ法)が上手く行けば、合計 1 兆倍の高速化も可能になる。その場合は ECC-256 は暗号としては黄信号(2010 年問題と同じ状態)である。米国 NSA(国家安全保障局)は研究陣の規模から既に実用化している可能性もある。

2. ECC のρ法とλ法による解読の例

$y^2=x^3+ax+b \pmod p$ なる ECC を解読する、ρ法とλ法の解読の軌跡例を示す。p=10007, r(位数)=10091, a=9773, b=8108 の例で示す。図 1 はρ法による解読の例で、図 2 は 8 並列λ法の解読の例である。ρ法は 1 個の初期値より出発し、口の点を円周の方に進みながら、円周を一周して同じ点に戻ると解読できる。この軌跡がρの文字に似ているため、ρ法と言われている。ρ法はシリアルな計算なので並列計算できない。そのため、プロセッサー毎に異なる初期値を使用し、各初期値からの計算はρ法と同じ計算を並列にする。これをλ法と呼ぶ。λ法は任意の二つの初期値の軌跡が交わると解読できる。交わる軌跡の形からλ法と言われる。ρ法とλ法は確率的収束速度は同じである。λ法は並列計算用に開発された解法であるが、PC でのシリアル計算も可能である。今回の学習λ法の解読は PC で行っている。一方学習は GPU で並列計算した。

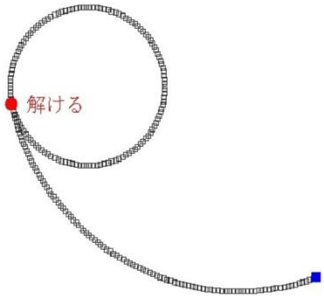

図 1. ρ法解読の軌跡

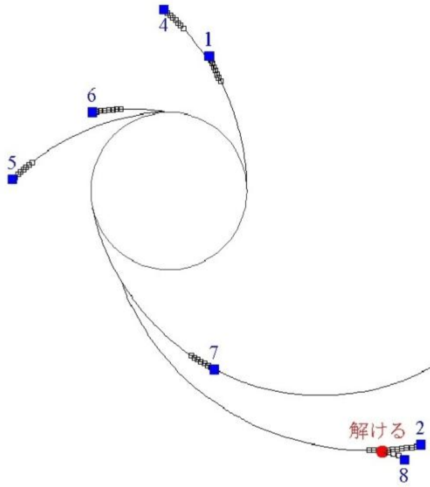

図 2. λ法解読の軌跡

3. 学習λ法の発見

ECC 上の 2 点 Q,R を与え、R=n×Q となる整数 n をρ法で求める。点 Q,R は固定し、初期値を色々変更し解読までの軌跡を同じ図の中に記載していた。この軌跡群は全て同じ円周を通り、多数に枝分かれすることが分かった。この図を見て、軌跡群の一部の点を先に計算(学習)しておけば、解読は高速化可能と考えた。しかし、ECC では点 Q と R は固定されていない。そこで、ρ法やλ法の計算ステップを色々検討し、点 Q が固定なら、R は変わっても、軌跡群全体は固定できることが分かった。その方法は計算ステップで「点 T_k から T_{k+1} に移るとき、R に依存させない」と分かった。一方、点 Q は変わるものなのにどのように固定するかの問題が残った。これを解決する方法として、任意の固定点 B を導入する。R=n×Q から直接整数 n を求めるのではなく、Q=n_1×B 及び R=n_2×B から整数 n_1 と n_2 を求めればよい。ECC の交換則から n_1×R=n_1×n_2×B=n_2×n_1×B=n_2×Q が成立する。これより、R=(n_2/n_1)×Q (mod r)となる。ここで、r は位数である。従って、n=n_2/n_1 (mod r)で求められる。

4. 学習λ法の学習と解読の例

ECC 上の 2 点 Q,R を与え、R=n×Q となる整数 n を学習λ法で学習及び解読する方法を図で示す。学習λ法では、R=n×Q を直接解読することは諦め、任意の固定点 B を導入する。そして、R=n×Q を解読する代わりに、Q=n_1×B と R=n_2×B から整数 n_1 と n_2 を求める。Q が同一で R が異なる場合は n_1 は一回だけ求めればよい。更に、学習及び解読の計算ステップで「点 T_k から T_{k+1} に移るとき、Q や R に依存させない」方式を採用させることにより、軌跡は初期値にだけ依存し、点 Q,R に依存しない固定の軌跡群を構成できる。図 3 に学習λ法の学習軌跡群を示す。細い線は軌跡群を示し、太い線は学習λ法の学習により得られた軌跡である。学習が多くなれば、太い線が多くなる。学習λ法の学習は

点Qと点Rに無関係に事前に計算しておく。図4は学習λ法により$Q=n_1\times B$から学習軌跡群を使用して、整数n_1を求めるものである。星印の軌跡をたどり、太字の線(学習済み)に到達すると整数n_1は求められる。次に、同様にして$R=n_2\times B$から学習軌跡群を使用してn_2を求める。$R=n\times Q$の関係を満たす整数nは$n=n_2/n_1 \pmod r$で求められる。予め記憶(学習)してある学習軌跡群の点の値を使用して解読するため、学習λ法の解読はρ法やλ法に比べ、少ない点の計算で済む。これが学習λ法にりECCが高速に解読できる要因である。

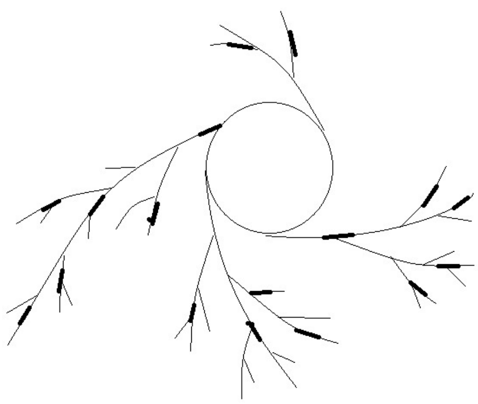

図3. 学習λ法による学習

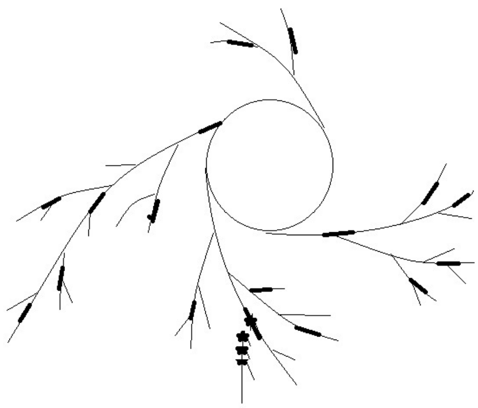

図4. 学習λ法による解読

5. 数値実験結果

　学習λ法の効果を調べるため、同じECCの問題をρ法での解読時間と比較した。比較には70ビットのECC解読に相当する44件の60ビットECCを使用した。解読はランダムにECC上の点Q,Rを与え$R=n\times Q$からnを求める時間を測定した。公平におこなうため、A,B,C,D,Eの5ケースで各60ビット44件の解読を行いその平均値で比較した。
下記に解読対象としたECCを示す。数値は16進数表示。

　ECC-60:　$y^2 = x^3 + ax + b \pmod p$,　rは位数

　　p = b98cc7dffc8ebbf,　r=b98cc7e0020c6af

　　a = 3dd997f5542f826,　b=7bb32feaa873e61

　固定の基準点BはB=(1,123)を使用した。

ρ法と学習λ法の解読は4GhzのPCの1コアで行った。一方、学習λ法による学習はGPU(GTX1080)で行った。ρ法の多倍長計算は汎用最速ライブラリと言われるgnuのgmpを使用した。一方、学習λ法はGPUでも動作させる必要があり、C及びCudaで自作した。学習λ法は学習結果が8GBのメモリに入るケースと入らないケースの2種類で評価した。メモリ入らないケースは学習データはSSDに記憶した。メモリ内のケースは学習データ取得にGPUで約1日を費やし、SSDのケースは約4日費やした。それぞれの学習量(記憶量)は2GBと36GBである。表1にρ法と学習λ法によるECCの解読実験結果を

示す。60 ビットの ECC を 44 件(70 ビット相当)解読する時間はρ法だと 10 時間を超える、一方、学習λ法だと、学習量が 2GB で 3.2 秒を切り、36GB なら 0.9 秒を切り大幅な性能向上になる。表 2. に学習量と高速化の関係を示す。数十 TB の SSD が用意できれば学習λ法により 100 万倍の高速化も可能である。

表 1. ρ法と学習λ法による 44 件の 60 ビット ECC の解読結果

データ	ρ法計算時間(s)	学習λ法時間(s)		ρ法/学習λ法(倍)	
		メモリ内	SSD	メモリ内	SSD
A	38295	3.27	0.94	11700	40700
B	35813	3.27	0.81	11000	44200
C	36729	2.98	0.92	12300	39900
D	34661	3.06	0.92	11300	37700
E	38183	3.28	0.86	11600	44400
平均	36736	3.17	0.89	11600	41400

表 2. 学習λ法による学習量と高速化の関係

高速化(対ρ法, λ法)	ECC のビット数(以下)		
	64 ビット	128 ビット	256 ビット
1 万倍	2.5 GB	4.5 GB	8.5 GB
4 万倍	36 GB	70 GB	140 GB
10 万倍	220 GB	430 GB	850 GB
100 万倍	20 TB	40 TB	80 TB

6. おわりに

楕円曲線暗号(ECC)は RSA 暗号の様に数学的に高度な解法が見つかっていない。そのため 2048 ビット RSA 暗号より、8 倍も短い 256 ビット ECC の方が強固な暗号と言われている。ECC の解読は現在ρ法(λ法)が最速と言われている。これに対し、数学的にはρ法と同じ計算で、学習により高速化する方式を考案した。その方式を学習λ法と名付けた。学習λ法は学習するほど高速化する。学習λ法の効果を 44 件の 60 ビット ECC(70 ビット相当)で評価した。その結果、2GB の学習量でρ法に比較し 1 万倍高速化した。36GB の学習量にすると 4 万倍高速化できた。学習量を増やせば、ρ法の 100 万倍も可能である。学習λ法は、任意に選んだ ECC 上の点 B を基点として計算し、軌跡は初期値にだけ依存する。そのため、ランダムな ECC 上の点 R,Q に対し R=n×Q となる整数 n を求めるのに、点 R,Q には依存しない軌跡群となる。軌跡群が固定できたので、学習λ法に人口知能(AI)機能を付けて、学習と解読で共によく通る軌跡群となる初期値の選定が可能と思われる。学習λ法に AI を働かせると学習と解読が共に高速する。もし AI で更に学習λ法と同等の高速化が可能なら、現在の 256 ビット ECC は黄信号である。AI 付き学習λ法が完成したら、国の暗号政策の根幹にかかわる。アメリカの国家安全保障局(NSA)は研究人員の多さから既に、AI 付き学習λ法を発見し、実用研究段階の可能性も否定できない。日本も AI 付き学習λ法を国主導で研究が必要と考える。