2023 암호분석경진대회

6번 문제

목차

[문제풀이 코드 개요]

* 6번 문제 관련 파일 목록

1. 6/params.sage: 문제에서 주어진 파라미터를 정의한 파일

2. 6/solver.sage: Alice가 획득한 서명값 s를 이용한 개인키 복원 공격 코드

3. 6/implementation.sage: 6번 문제에서 주어진 서명 알고리즘에 대한 sagemath 구현체

4. 6/analysis.sage: 6/implementation.sage 구현체에 대한 공격 검증 코드

문제풀이 코드는 전부 sagemath script로 작성하였으며, 코드가 2023pqc_s.txt 파일과 동일한 폴더 아래 위치할 경우 정상적으로 작동함

1, 2번 파일이 실제 문제풀이(개인키 복원)에 필요한 코드며, 3, 4번은 전자서명 알고리즘 분석을 위해 작성한 공격과 관련없는 코드기 때문에 확인하지 않아도 무방함.

[답]

주어진 전자서명 알고리즘은 생성된 서명값 중 s에서 개인키인 n_S, ϕ_S를 복원할 수 있으며, 공격자는 복원한 서명을 통하여 임의의 메세지 m을 공격자 스스로 서명할 수 있음 (**[풀이 과정]** 섹션 참고).

문제에서 복원된 개인키값은 아래와 같음.

n_S = 0x5a0c7dc0eb986a066077645b72cd4b57f9aa64608bab7ecccffc64

$\phi_S(x,y) =$

(x^2+(153266247282646412875433016919523088686109405271846163667339172350781821966953215675267029214576725168855347207390688169220953720 64*i+136240907267658649873872012304596178230435707363083510945366189975897429519523024523546250263801876326559457191549441058938831096 00)*x+625345388388242902405028983667223117019237958196899197650183364249795837991078785137137488036101146905996348775700587772035545381 1*i+1790789391986132203711096118112575397526452660172721388246349549684395705661196695020567717733229260210097347869837956861308865483 6)/(x+153266247282646412875433016919523088686109405271846163667339172350781821966953215675267029214576725168855347207390688169220953720 64*i+136240907267658649873872012304596178230435707363083510945366189975897429519523024523546250263801876326559457191549441058938831096 00,

x^2*y+(621382579518406102317745837244712411813610081060763622214202713395114315405866640908318917108672658787235041478525269450187601056 1*i+280875779218650842286525744946174202700136122885510567774743065897426466457262817873903338093175681941317241161700327244545148563 3)*x*y+(935790089749155672518295748661250024118569106325891847812069503760684151011250346163954151279834386245629892738419913507616714156 9*i+2434089422944622171294984063269639519192772016559816493960752220391481905328950772092076324584630981051308116896937354471906051733 9)*y)/(x^2+(621382579518406102317745837244712411813610081060763622214202713395114315405866640908318917108672658787235041478525269450187601056 1*i+280875779218650842286525744946174202700136122885510567774743065897426466457262817873903338093175681941317241161700327244545148563 3)*x+156113547813739857492332473232847314113780706452279104546225286801047998900232913130109163931593553315162624151412050127965225953 80*i+178093644879623221981516568023646555481064665235637823107452103645535548705694979451562237513499839667153356209748681739898344386 08)

(^: 제곱연산, *: 곱연산)

[풀이 과정]

1. e 복원

Alice가 획득한 s를 통하여 e를 복구할 수 있음

$s=(x_0,\ldots,x_{255})$에서 각각의 x_i가 E, E_S중 어느 곡선에 속하는 점인지 확인하는 것으로 e_i가 0,1중 어떤 값이었는지 알 수 있음.

즉,

$e_i=0 \Leftarrow \exists\,(x_i,y)\in E$ s.t. $y^2=x^3+6x^2+x\in F_{p^2}$,

$e_i=1 \Leftarrow \exists\,(x_i,y)\in E_S$ s.t. $y^2=x^3+A'x^2+x\in F_{p^2}$

와 같은 관계가 성립함

이 과정을 통하여 e를 복구할 뿐 아니라, E위의 점 G_i들과 E_S위의 점 $\phi_S(R_i)$들의 정보를 획득할 수 있음

2. S 복원

$G_i=S+R_i$에서 S의 order(2^n, $n\le 216$)와 R_i의 order(3^n, $n\le 137$)로 인하여 다음과 같은 관계가 성립함

$3^{137}G_i=3^{137}(S+R_i)=3^{137}S+3^{137}R_i=3^{137}S$

S를 기준으로 양변을 정리하면 다음과 같은 관계를 얻을 수 있음

$S=G_i\cdot 3^{137}\cdot(3^{-137} \bmod 2^{216})$

(S의 order가 2^{216}인 점을 고려)

e를 복원하는 과정에서 G_i의 좌표정보를 획득하였기 때문에, 임의의 G_i에 대해 $G_i\cdot 3^{137}\cdot(3^{-137} \bmod 2^{216})$를 연산할 경우 $\ker\phi_S$의 generator인 S를 복원할 수 있다는 것을 알 수 있음

3. n_S 복원

$S=P_S+n_S\cdot Q_S$를 Q_S에 대해 정리하면 다음과 같은 관계를 얻을 수 있음

$n_s\cdot Q_S=S-P_S$

위 관계에서 n_S를 찾는 문제는 전형적인 Elliptic Curve Discrete Logarithm Problem에 속하며, 곡선이 supersingular한 경우 효율적으로 문제를 해결 가능한 알고리즘이 알려져있음(**[참조]** 섹션 참고).

따라서, E가 supersingular하기 때문에 알려진 알고리즘(MOV attack 등)을 이용하여 개인키 n_S을 효율적으로 복원할 수 있음.

실제로 문제에서 주어진 서명값에 대해서 order가 일정한 특정 점들에 대해서 성공적으로 n_S가 복원됨을 확인함.

4. ϕ_S 복원

서명검증을 위하여 계산하는 isogeny $\alpha_i: E\to E_i'$에 대해서 $\ker\alpha_i=<G_i>=<S+R_i>$이기 때문에 S, R_i 각각을 kernel로 하는 함수로 합성됨을 확인함. 즉

$\alpha_i=\beta_i\circ\phi_S$

가 성립하며 (증명은 **[부록]** 섹션 참고) α_i를 degree가 2, 3인 각각의 isogeny로 분해 후 degree가 2인 isogeny만 합성하는 방식으로 ϕ_S를 복원할 수 있음.

실제로 문제에서 주어진 서명값에 대해서 order가 일정한 특정 점들에 대해서 성공적으로 ϕ_S가 복원됨을 확인함.

5. 결론

전자서명에 필요한 개인키 n_S, ϕ_S를 서명값중 s를 통하여 전부 복원할 수 있기 때문에, 임의의 메세지에 대한 서명값을 획득한 공격자는 개인키를 복원한 후 원하는 메세지에 대한 전자서명을 진행할 수 있음. 따라서 해당 서명 알고리즘은 안전하지 않음

[실행 결과]

실제로 주어진 서명값에 대해 공격 수행시(1, 2번 파일 사용) order가 일정한 특정 점들에 대해서 개인키인 n_S, ϕ_S가 성공적으로 복원되며, Macbook M1 Pro 기준 10초 이내에 효율적으로 복원되는것을 확인함.

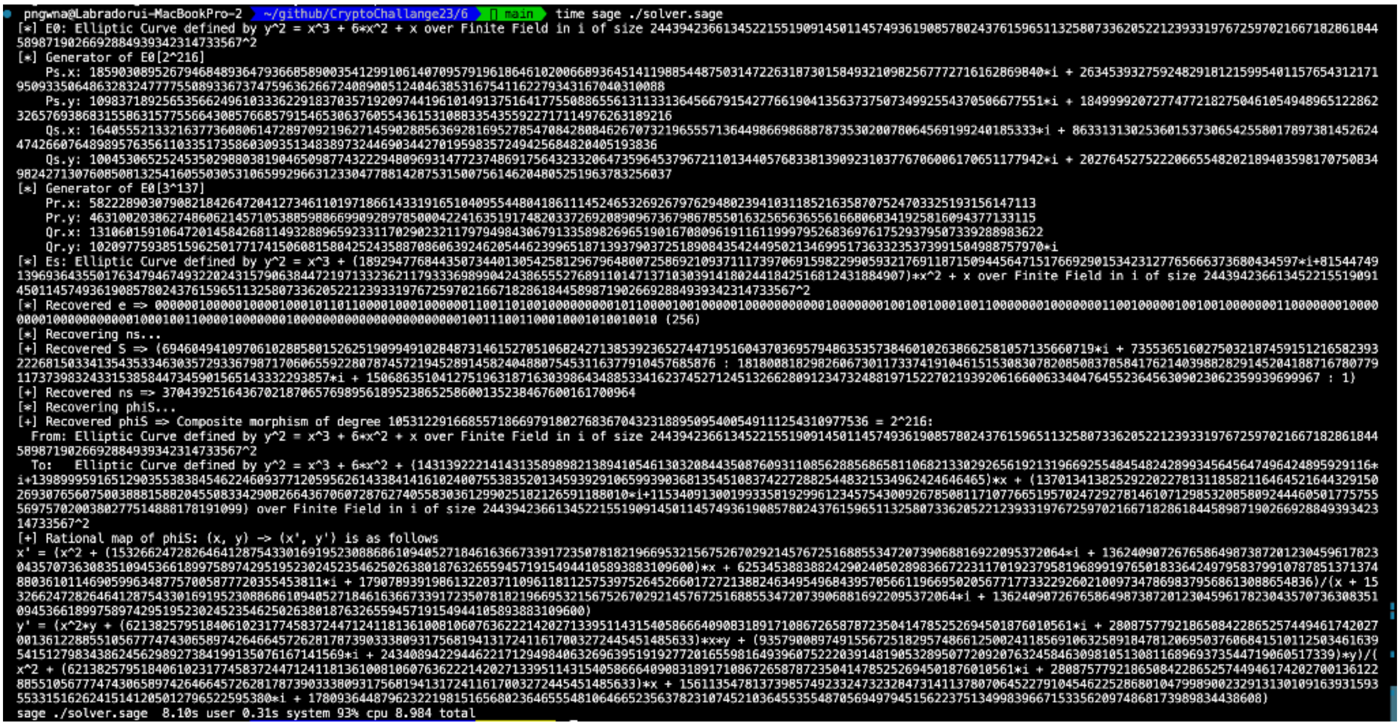

그림 1 실행 결과에 대한 스크린샷

[참조]

- Supersingular curve 상에서의 효율적인 DLP 해결 알고리즘 :https://www.dima.unige.it/~morafe/MaterialeCTC/p80-menezes.pdf
- MOV attack: :https://people.cs.nctu.edu.tw/~rjchen/ECC2009/19_MOVattack.pdf
- isogeny가 equivalent할 조건: https://www.math.auckland.ac.nz/~sgal018/crypto-book/ch25.pdf, 25-1 챕터

[부록] - $\alpha_i = \beta_i \circ \phi_S$가 성립하는 이유에 대한 증명

아래는 $< S+R_i >$를 kernel로 하는 α_i와 $< S, R_i >$를 kernel로 하는 $\beta_i \circ \phi_S$가 equivalent함을 보이고자 함.

두 isogeny의 kernel의 order가 $|< S+R_i >| = \mathrm{lcm}(\mathrm{ord}(S), \mathrm{ord}(R_i)) = 2^{136} \cdot 3^{137} = |< S, R_i >|$로 같으며 $< S+R_i > \subseteq < S, R_i >$이고 양쪽 group이 모두 abelian이기 때문에 $< S+R_i > = < S, R_i >$임.

두 isogeny의 domain, kernel, codomain이 동일하기 때문에 α_i와 $\beta_i \circ \phi_S$는 equivalent함. 끝.