2022 암호분석경진대회

7번 문제

양자 내성 암호 중 isogeny 기반 암호는 유한체 위의 두 타원곡선 E, E' 사이의 isogeny를 연산하는 어려움에 기반을 두어, isogeny $\phi : E \to E'$에 대해 ϕ를 비밀값으로 한다. 한편, Velu의 공식을 이용해 $\ker\phi$를 이용해 isogeny를 연산할 수 있으므로 $\ker\phi$ 도 비밀로 하며, 일반적인 구현에서는 isogeny를 저장하는 대신 $\ker\phi$를 저장한다.

한편, n차 isogeny ϕ에 대해서 dual isogeny는 차수가 같고 $\hat{\phi} \circ \phi = [n]$ 를 만족하는 isogeny $\hat{\phi}: E' \to E$ 이다. 여기에서 $[n]$은 multiplication-by-n map을 의미한다. 마찬가지로 dual isogeny를 알면 해당 isogeny를 복원할 수 있으므로 dual isogeny도 isogeny와 동일하게 비밀 값으로 한다.

다음은 양자 내성 암호 중 하나인 isogeny 기반 암호의 키 교환 프로토콜인 SIDH에 관한 설명이다

[Setup]

- $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$, $E: y^2 = x^3 + Ax^2 + x \in F_{p^2}$
- $P_A, Q_A \in E[\ell_A^{e_A}]$, generator of $E[\ell_A^{e_A}]$, $P_B, Q_B \in E[\ell_B^{e_B}]$, generator of $E[\ell_B^{e_B}]$

[Key generation]

<Alice>

- 개인키 n_A로 $R_A = P_A + n_A Q_A$ 연산한다
- $\langle R_A \rangle$를 커널로하는 isogeny $\phi_A : E \to E_A$를 연산하고 Bob에게 $E_A, \phi_A(P_B), \phi_A(Q_B)$를 전달한다

<Bob>

- 개인키 n_B로 $R_B = P_B + n_B Q_B$를 연산한다
- $\langle R_B \rangle$를 커널로하는 isogeny $\phi_B : E \to E_B$를 연산하고 Alice에게 $E_B, \phi_B(P_A), \phi_B(Q_A)$를 전달한다

[Key agreement]

<Alice>

- Bob에게 받은 값을 이용해 $R_A' = \phi_B(P_A) + n_A \phi_B(Q_A)$를 연산한다
- $\langle R_A' \rangle$를 커널로 하는 isogeny $\phi_{A'} : E_B \to E_{AB}$ 를 연산한다

<Bob>

- Alice에게 받은 값을 이용해 $R_B' = \phi_A(P_B) + n_B \phi_A(Q_B)$를 연산한다
- $\langle R_B' \rangle$를 커널로 하는 isogeny $\phi_{B'} : E_A \to E_{BA}$를 연산한다

Shared secret key는 $j(E_{AB}) = j(E_{BA})$ 이다.

[문제]

SIDHp434 파라미터를 활용해서 Alice가 Bob에게 다음과 같이 전달했을 때, Alice의 개인키 ϕ_A에 대응되는 dual isogeny $\hat{\phi}_A$를 구하시오. (표에서 Re는 실수부를, Im은 허수부를 의미하며 제시된 $\phi_A(P_B)$, $\phi_A(Q_B)$는 x좌표임)

E_A	Re	0000C2D29711365E 5AC6CB621574EC6D 2EFAD33760BD5DB3 B74E01533E6E978B D2A992929C0A36D7 32B6AE51D0397225 B6FAC262931F77CD
	Im	00003CAABA21E68C 10C9ADD816980B1D 73822C2CC8D18BCE 22B0904CA99C1A57 8D39CA029E7D28E2 55F2A19941112230 89832831644D66E6
$\phi_A(P_B)$	Re	000133617DF3EEDE E09DA13528F184DF E8BD912929AC949A F8A887EE9B3A3E43 C6035F5B88E2D82A 2D5AD3C7B1243578 F33CC6C74346FB64
	Im	00000AA8F2D61712 05D359582EEFE035 5E9BA5DC169B0B66 7FCA9EBFF266C138 D7C174B258A561CE FC33AB3DC20AF224 4E4C0FD338EE4C84
$\phi_A(Q_B)$	Re	0001A646437477E6 1DFD02DA472AC83C B439354D9F1F7879 9AFFEECD96028D6B E82E73C364291362 AB1F800A9DC4BFF5 58AABED07AE90E39
	Im	0000547960A0A8BA DE1E7B67DC14C850 81150853FEFD48BD 4B3F4F304B29D680 C7D2827C402A222C DB006F3FC8D7A13C 30B9DB783E6B463B

(자세한 SIDH 설명과 구현은 NIST Round 3 SIKE documentation 및 소스코드 참조)

2022 암호분석경진대회

7번 문제

[참고] : SIDHp434 파라미터

- $p = 2^{216}3^{137} - 1$
- $E: y^2 = x^3 + 6x^2 + x \in F_{p^2}$
- $P_A, Q_A \in E[2^{216}]$, generator of $E[2^{216}]$, $P_B, Q_B \in E[3^{137}]$, generator of $E[3^{137}]$

Point	좌표		값
P_A	x	Re	00003CCFC5E1F050 030363E6920A0F7A 4C6C71E63DE63A0E 6475AF621995705F 7C84500CB2BB61E9 50E19EAB8661D25C 4A50ED279646CB48
		Im	0001AD1C1CAE7840 EDDA6D8A924520F6 0E573D3B9DFAC6D1 89941CB22326D284 A8816CC4249410FE 80D68047D823C97D 705246F869E3EA50
	y	Re	0001AB066B849495 82E3F66688452B92 55E72A017C45B148 D719D9A63CDB7BE6 F48C812E33B68161 D5AB3A0A36906F04 A6A6957E6F4FB2E0
		Im	0000FD87F67EA576 CE97FF65BF9F4F76 88C4C752DCE9F8BD 2B36AD66E04249AA F8337C01E6E4E1A8 44267BA1A1887B43 3729E1DD90C7DD2F
Q_A	x	Re	0000C7461738340E FCF09CE388F666EB 38F7F3AFD42DC0B6 64D9F461F31AA2ED C6B4AB71BD42F4D7 C058E13F64B237EF 7DDD2ABC0DEB0C6C
		Im	000025DE37157F50 D75D320DD0682AB4 A67E471586FBC2D3 1AA32E6957FA2B26 14C4CD40A1E27283 EAAF4272AE517847 197432E2D61C85F5
	y	Re	0001D407B70B01E4 AEE172EDF491F4EF 32144F03F5E054CE F9FDE5A35EFA3642 A11817905ED0D4F1 93F31124264924A5 F64EFE14B6EC97E5
		Im	0000E7DEC8C32F50 A4E735A839DCDB89 FE0763A184C525F7 B7D0EBC0E84E9D83 E9AC53A572A25D19 E1464B509D97272A E761657B4765B3D6
$P_A - Q_A$	x	Re	0000F37AB34BA0CE AD94F43CDC50DE06 AD19C67CE4928346 E829CB92580DA84D 7C36506A2516696B BE3AEB523AD7172A 6D239513C5FD2516
		Im	000196CA2ED06A65 7E90A73543F3902C 208F410895B49CF8 4CD89BE9ED6E4EE7 E8DF90B05F3FDB8B DFE489D1B3558E98 7013F9806036C5AC
	y	Re	00007F65B303A50E F1B4192237611E22 6A3D13384EF608A6 B117365A16E0EB51 12156F2012CB029C 819F3330F69BD5C7 3CCC9A1F1C06CD15
		Im	0000749095AB8A36 C841FBF25A5671A6 7FDE5023131C73F0 EC6031C7E472DAE1 38FBED0A0BE63C67 06CD893EF88D32CC 766EC67EC056ED33
P_B	x	Re	00008664865EA7D8 16F03B31E223C26D 406A2C6CD0C3D667 466056AAE85895EC 37368BFC009DFAFC B3D97E639F65E9E4 5F46573B0637B7A9
		Im	0
	y	Re	00006AE515593E73 976091978DFBD70B DA0DD6BCAEEBFDD4 FB1E748DDD9ED3FD CF679726C67A3B2C C12B39805B32B612 E058A4280764443B
		Im	0
Q_B	x	Re	00012E84D7652558 E694BF84C1FBDAAF 99B83B4266C32EC6 5B10457BCAF94C63 EB063681E8B1E739 8C0B241C19B9665F DB9E1406DA3D3846
		Im	0
	y	Re	0
		Im	0000EBAAA6C73127 1673BEECE467FD5E D9CC29AB564BDED7 BDEAA86DD1E0FDDF 399EDCC9B49C829E F53C7D7A35C3A074 5D73C424FB4A5FD2
$P_B - Q_B$	x	Re	0001CD28597256D4 FFE7E002E8787075 2A8F8A64A1CC78B5 A2122074783F51B4 FDE90E89C48ED91A 8F4A0CCBACBFA7F5 1A89CE518A52B76C
		Im	000147073290D78D D0CC8420B1188187 D1A49DBFA24F26AA D46B2D9BB547DBB6 F63A760ECB0C2B20 BE52FB77BD2776C3 D14BCBC404736AE4
	y	Re	0000DA7A98EA2646 9B843EBF8D1EE0F0 0E6786E680AC535F 5FF26D25819549C9 59497D8E8FB14B1B F6764BD27BAE970D 0791AF091E344F22
		Im	000048704FEC03D0 5B06D8A8197DF08D 4946E465099F31B7 5C63A865A23CA2AD 41A74F05074E9DC3 F45C5A26F741A0EA 1F3C2E6CDA0BB344