Eliptičke krivulje u kriptografiji

Filip Najman

11. predavanje

7.6.2022.

Kvantna faktorizacija

Svi kriptografski algoritmi s javnim ključem koji se danas široko koriste se baziraju na težini sljedećih problema: faktorizacija prirodnih brojeva, problem diskrentog lograitma (u konačnim poljima) i problem diskretnog logaritma na eliptičkim krivuljama.

Peter Shor je 1994. razvio **kvantni algoritam** koji faktorizira brojeve u polinomijalnom vremenu.

Tim algoritmom se mogu probiti (teoretski) svi gore navedeni kriptosustavi u polinomijanlom vremenu.

Danas postoje kvantna računala, ali s vrlo malo qubita, te nisu vrlo korisna u praksi.

2001. je Shorovim algoritmom faktoriziran broj 14, a 2012. broj 21. 2019. godine je pokušana faktorizacija broja 35, ali nije uspjela.

Post-kvantna kriptografija

2016. godine je National Institute of Standards and Technology (NIST) raspisao natječaj za predlaganje kriptografskih protokola koji bi bili otporni na napade kvantnim računalom.

Inicijalno je na natječaju predloženo 23 protokola za potpisivanje i 58 za enkirpciju.

U treću rundu je ušlo 7 finalista, 4 za enkripciju i 3 za potpisivanje, te 8 alternativa (5+3), kao rezerve za finaliste.

Od 4 enkripcijska finalista 3 se baziraju na rešetkama.

Rešteka L s bazom $B = \{b_i | 1 \leq i \leq n\}$ se definira kao $L = \{\sum_{i=1}^{n} a_i b_i | a_i \in \mathbb{Z}\} \subseteq \mathbb{R}^n$.

Kriptosustavi bazirani na rešetkama se uglavnom baziraju na problemu nalaženja najkraćeg vektora u rešetci.

Poznato je da je ovaj problem NP-težak.

Kriptografija pomoću izogenija supersingularnih EK

Jedan od alternativnih kriptosustava je SIKE (Supersingular isogeny key exchange) koji se bazira na Supersingular isogeny Diffie–Hellman key exchange (SIDH), koji se bazira na šetnjama po grafu izogenija supersingularnih eliptičkih krivulja nad konačnim poljima.

Izogenija $\phi : E \to E'$ je surjektivni (ako se gleda nad $\overline{k}$) homomorfizam algebarskih krivulja s konačnom jezgorm.

Svaka izogenija $\phi : E \to E'$ inducira *dualnu izogeniju* $\widehat{\phi} : E' \to E$ takvu da je $\phi \circ \widehat{\phi} = [m]_{E'}$ i $\widehat{\phi} \circ \phi = [m]_E$, gdje je m stupanj izogenije ϕ (i također $\widehat{\phi}$).

Kompozicija izogenija je također izogenija, te je reclacija "biti izogen" relacija ekvivalencije.

Klasa izogenije neke eliptičke krivulje E je skup elitpičkih krivulja izogenih s E.

Izopgenije eliptičkih krivulja

Definirajmo za E/k,

$$E[m] = \{P \in E(\overline{k}) | [m]P = O\} = \ker[m].$$

Teorem

Za E/k i $\operatorname{char} k \nmid m$, postoji bijekcija između izogenija stupnja m i cikličkih podrgupa od $E[m]$.

Ako $\operatorname{char} k \nmid p$, tada

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$

Ako je $\operatorname{char} k = p$, vrijedi

$$E[p] = \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{- } \textbf{obične} \text{ krivulje,} \\ \{O\}, & \text{- } \textbf{supersingularne} \text{ krivulje.} \end{cases}$$

Za supersingularne krivulje (nad $\mathbb{F}_p$) vrijedi

$$E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2,$$

što će se pokazati ključno za njihovu uporabu.

Odaberimo prost broj $p = 2^{e_A}3^{e_B} - 1$, gdje su e_A i e_B takvi da je 2^{e_A} otprilike veliko kao 3^{e_B}.

Neka je E supersingularna krivulja nad $\mathbb{F}_p$. Tada je

$$E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z} \times \mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z}.$$

Neka su P i Q generatori od $E(\mathbb{F}_{p^2})$; svaki element se može prikazati kao $[a]P + [b]Q$.

Kriptosustav pomoću supersingularnih izogenija

Protokol razmjene ključeva se bazira na sljedećem teškom problemu:

Problem

Za dane izogene krivulje E, E' izračunajte izogeniju $\phi : E \to E'$.

Fiksirajmo supersingularnu E nad $\mathbb{F}_p$ (ona je javna). Vrijednosti p, a time e_A i e_B su javne.

Alice za svoju tajni ključ izabire izogeniju ϕ_A stupnja 2^{e_A} (ili ekvivalentno cikličku podgrupu reda 2^{e_A}). Analogno Bob izabere izogeniju stupnja 3^{e_B}.

Konkretnije, neka je

$$< P_A, Q_A >= E[2^{e_A}] \simeq \mathbb{Z}/2^{e_A}\mathbb{Z} \times \mathbb{Z}/2^{e_A}\mathbb{Z},$$

$$< P_B, Q_B >= E[3^{e_B}] \simeq \mathbb{Z}/e^{e_B}\mathbb{Z} \times \mathbb{Z}/2^{e_B}\mathbb{Z}.$$

Točke P_A, Q_A, P_B, Q_B su javno poznati generatori odgovarajućih podgrupa.

Kriptosustav pomoću supersingularnih izogenija

Alice izabere slučajan $0 \leq k_A \leq 2^{e_A}$, a Bob slučajan $0 \leq k_B \leq 3^{e_B}$.

Sada Alicina tajna izogenija $\phi_A : E \to E_A$ odgovara podgrupi generiranoj s $S_A = P_A + [k_A]Q_A$.

Bobova tajna izogenija $\phi_B : E \to E_B$ odgovara podgrupi generiranoj s $S_B = P_B + [k_B]Q_B$.

Sada je Alicine javni ključ $K_A = (E_A, \phi_A(P_B), \phi_A(Q_B))$, a Bobov $K_B = (E_B, \phi_B(P_A), \phi_B(Q_A))$.

Alice izračuna $S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A) = \phi_B(S_A)$, te izogeniju $\phi'_A : E_B \to E_{AB}$ koja odgovara podgrupi geneeriranoj s S'_A.

Bov izračuna $S'_B = \phi_A(P_B) + [k_B]\phi_A(Q_B) = \phi_A(S_B)$, te izogeniju $\phi'_B : E_A \to E_{AB}$ koja odgovara podgrupi geneeriranoj s S'_B.

Sada je zajednički ključ Alice i Bob $j(E_{AB})$.

Da bi Eve probila kriptosustav, morala bi naći ϕ_A, ϕ_B, ϕ'_A ili ϕ'_B.