Napadi na supersingularne kriptografske sisteme umetanjem greške

Seminarski rad u okviru kursa Kriptografija
Prof. Miodrag Živković
Matematički fakultet

Bukurov Anja

27. maj 2017.

Sažetak

Predstavljamo prvi napad umetanjem greške na kripto sisteme koji su zasnovani na supersingularnim izogenijima. Tokom računanja pomoćnih tačaka, napad cilja da promeni početnu tačku nekom slučajno odabranom tačkom na krivoj umetanjem greške. Pokazaćemo da će ovakav napad otkriti tajnu izogeniju jednom uspešnom smetnjom koja ima visoku verovatnoću uspeha.

1 Uvod

Kriptografske sisteme zasnovane na izogenijama između supersingularnih eliptičkih krivih predložili su Jao i De Feo 2011. godine kao kandidat za kriptografski protokol. Umesto da se oslanja na problem diskretnog logaritma, koji je osetljiv na Šorov (engl. Shor) algoritam, ovaj protokol zasnovan je na problemu pronalaženja izogenija između supersingularnih eliptičkih krivih.

Napad umetanjem greške iskorišćava curenje osetljivih informacija kada implementacija radi pod neočekivanim uslovima. U ovom radu ispitujemo efekte promene tačke P u neko slučajno odabranu tačku P_0 i pokušaj da se otkrije tajna, a to je u ovom slučaju izogenija ϕ. Napad bi bio u mogućnosti da otkrije celu tajnu ϕ iz jednog izlaza $\phi(P_0)$ sa visokom verovatnoćom. Predstavićemo napad sa umetanjem greške u kontekstu nekoliko signaturnih shema i protokolu razmene ključa. Napad bi radio i protiv protivmera koje je predložio Kirkvud (engl. Krikwood) koje su zasnovane na Fudžisaki-Okamoto (engl. Fujisaki-Okamoto) transformaciji. Glavno zapažanje je da korisnik nikada ne treba da otkriva sliku slučajno izabranih tačaka pod tajnom izogenijom.

2 Supersingularni izogeni kriptografski sistem

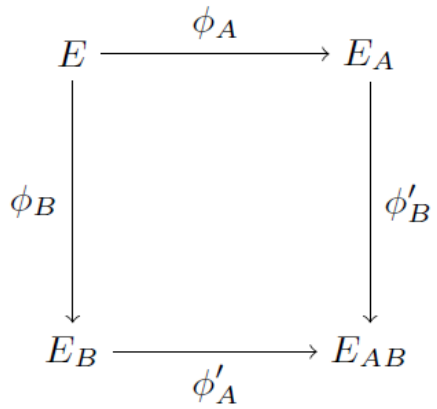
U ovom delu, upoznajemo se sa protokolom razmene ključa, interaktivnim protokolom identifikacije i raznim signaturnim shemama.

Razmena ključa Pretpostavimo da Alisa i Bob žele da uspostave zajedničku tajnu. Moraju izvršiti tri koraka kako bi to uradili:

Priprema: Bira se prost broj p oblika $p = l_A^{e_A} \cdot l_B^{e_B} \cdot f \pm 1$ gde su l_A i l_B različiti mali prosti brojevi, f je mali kofaktor, dok su e_A i e_B pozitivni celi brojevi takvi da važi $l_A^{e_A} \approx l_B^{e_B}$. Zatim je potrebno odrediti supersingularnu eliptičku krivu E u polju $\mathbb{F}_{p^2}$ i početne tačke $\{P_A, Q_A\}$ i $\{P_B, Q_B\}$.

Generisanje ključa: Alisa slučajno odabira elemente $a_1, a_2 \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$, takve da nisu oba deljiva sa l_A i određuje podgrupu $G_A =< h[a1]P_A + [a2]Q_A >$. Zatim koristi Veluovu (Vélu) formulu da odredi krivu $E_A = E/G_A$ i izogeniju $\phi_A : E \longrightarrow E_A$, gde je $ker\phi_A = G_A$. Alisa takođe računa tačke $\phi_A(P_B)$ i $\phi_A(Q_B)$. Onda Bobu šalje torku $(E_A, \phi_A(P_B), \phi_A(Q_B))$. Bob zatim vrši izračunavanja sa druge strane.

Poreklo ključa: Kada primi Bobovu torku $(E_B, \phi_B(P_A), \phi_B(Q_A))$, Alisa određuje podgrupu $G'_A =< h[a1]\phi_B(P_A) + [a2]\phi_B(Q_A) >$ i koristi Veluovu formulu da odredi krivu $E_{AB} = E_B/G'_A$. Zatim koristi j-invarijantu krive E_{AB} kao zajedničku tajnu. Bob postupa na isti način. Protokol rezimiramo na slici 1.



Slika 1: Protokol razmene ključa