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 $G_A = \langle h[a1]P_A + [a2]Q_A \rangle$. 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 $G'_A = \langle h[a1]\phi_B(P_A) + [a2]\phi_B(Q_A) \rangle$ 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.

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi'_B"] \\ E_B \arrow[r, "\phi'_A"'] & E_{AB} \end{tikzcd}$$

Slika 1: Protokol razmene ključa

3 Napad umetanjem greške

Pretrpostavimo da je napadnuti protokol otkriva x-koordinatu slike tačke pod tajnom izogenijom. Napad umetanjem greške cilja da natera implementaciju da kao rezultat da sliku slučajno odabrane tačke pod tajnom izogenijom. Ovo bi protivniku omogućilo da otkrije tajnu. Primetimo da ova izračunavanja ne uključuju y-koordinatu tačaka.

Ako nam je daat kriva E i tačka P, promena x-koordinate tačke P rezultovaće drugom tačkom, P_0 na istoj krivoj. Ako nam je dato x možemo da dobijemo y rešavanjem kvadratne jednačine, koja u prostoru $\mathbb{F}_{p^2}$ uvek ima rešenje. Konkretno, svako $x \in \mathbb{F}_{p^2}$ odgovara tački na krivoj E ili na krivoj E', koja predstavlja njen kvadratni obrt. U najefikasnijim implementacijama kriptografskih sistema do sada, izračunavanja ne razlikuju krive E i E' tako da će izogenija biti izračunata tačno za svako $x \in \mathbb{F}_{p^2}$.

3.1 Dobijanje izogenije iz slike slučajno odabrane tačke

Neka je $E/\mathbb{F}_{p^2}$ supersingularna eliptička kriva gde je $p = l_A^{e_A} \cdot l_B^{e_B} \cdot f \pm 1$. Zatim sa tačkama ($P_A$, Q_A), (P_B, Q_B) i (P_C, Q_C) koje su generatori redom za $E[l_A^{e_A}]$, $E[l_B^{e_B}]$ i $E[f]$, slučajno odabrana tačka $X \in E(\mathbb{F}_{\not\vdash})$ ima oblik

$$X = [u]P_A + [v]Q_A + [w]P_B + [x]Q_B + [y]P_C + [z]Q_C$$

za neke $u, v, w, x, y, z \in \mathbb{Z}$

Sad pretpostavimo da nam je data slika tačke X pod izogenijom ϕ_A, onda ćemo pokazati kako neko može da iskoristi $\phi_A(X)$ da dobije ϕ_A. Pošto je ϕ_A homomorfizam grupe i znamo da X može biti izraženo linearnom kombinacijom P_A, Q_A, P_B, Q_B, P_C i Q_C imamo sledeći izraz

$$\phi_A(X) = \phi_A([u]P_A + [v]Q_A + [w]P_B + [x]Q_B + [y]P_C + [z]Q_C)$$

$$= [u]\phi_A(P_A) + [v]\phi_A(Q_A) + [w]\phi_A(P_B)$$
$$+[x]\phi_A(Q_B) + [y]\phi_A(P_C) + [z]\phi_A(Q_C)$$

Sada nam je cilj da izolujemo linearnu kombinaciju $\phi_A(P_A)$ i $\phi_A(Q_A)$. Do kraja izvodimo operaciju:

$$[l_B^{e_B} \cdot f]\phi_A(X) = [l_B^{e_B} \cdot f]([u]\phi_A(P_A) + [v]\phi_A(Q_A))$$
$$= [u']\phi_A(P_A) + [v']\phi_A(Q_A)$$

Jednom kad dobijemo $[u']\phi_A(P_A) + [v']\phi_A(Q_A)$, podgrupa generisana do sada će pomoći u konstruisanju izogenije ϕ_A.

Lema 1. Neka je E_1 supersingularna eliptička kriva u $\mathbb{F}_{p^2}$, gde je $p = l_A^{e_A} \cdot l_B^{e_B} \cdot f \pm 1$. Pretpostavimo da je $\phi : E_1 \longrightarrow E_2$ izogenija stepena $l_A^{e_A}$ i neka su $\{P, Q\}$ generatori za $E_1[l_A^{e_A}]$. Tada za bilo koje $X \in E[l_A^{e_A}]$ definiši $\psi : E_2 \longrightarrow E'$ takvo da je $ker\psi = \langle\phi(X)\rangle$, onda postoji $\theta : E' \longrightarrow E_1$ koje je stepena l_A^t, tako da je $t \leq e_A$, takvo da je

$$\phi' = \theta \circ \psi$$

.