

# Napad na supersingularne izogene kriptografske sisteme umetanjem greške

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

Bukurov Anja 1082/2016

27. maj 2017.

## Sažetak

U ovom radu biće predstavljen prvi napad umetanjem greške na kriptografske sisteme koji su zasnovani na supersingularnim izogenijama. Tokom računanja pomoćnih tačaka, napad cilja da promeni početnu tačku nekom slučajno odabranom tačkom na krivoj umetanjem greške. Biće pokazano da ovakav napad može otkriti tajnu izogeniju jednom uspešnom smetnjom koja ima visoku verovatnoću uspeha.

## Sadržaj

<b>1</b>	<b>Uvod</b>	<b>2</b>
<b>2</b>	<b>Supersingularni izogeni kriptografski sistem</b>	<b>2</b>
<b>3</b>	<b>Napad umetanjem greške</b>	<b>3</b>
3.1	Dobijanje izogenije iz slike slučajno odabrane tačke . . . . .	3
3.2	Izvodljivost napada na protokol razmene ključeva . . . . .	4

# 1 Uvod

Kriptografske sisteme zasnovane na izogenijama između supersingularnih eliptičkih krivih predložili su Jao i De Feo 2011. godine [2] kao kandidat za kriptografski protokol. Umesto da se oslanja na problem diskretnog logaritma, koji je osetljiv na Šorov (engl. Shor) algoritam [3], 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 ispitani su efekti promene tačke  $P$  u neku slučajno odabranu tačku  $P'$  i pokušaj da se otkrije tajna, a to je u ovom slučaju izogenija  $\phi$ . Napad bi bio u mogućnosti da otkrije celu tajnu  $\phi$  iz jednog izlaza  $\phi(P')$  sa visokom verovatnoćom. Napad sa umetanjem greške biće predstavljen u kontekstu protokola razmene ključa. Napad bi radio i protiv protivmera koje je predložio Kirkvud (engl. Krikwood)[4] 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

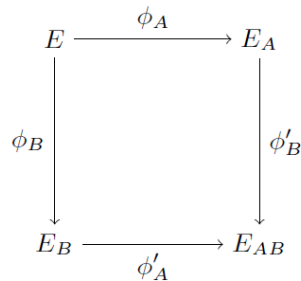
U ovom delu, upoznajemo se sa protokolom razmene ključa.

**Razmena ključa** Pretpostavimo da Alisa i Bob žele da uspostave zajedničku tajnu. Oni moraju izvršiti tri koraka kako bi to učinili:

**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  $G_A = \langle h[a_1]P_A + [a_2]Q_A \rangle$ . Zatim koristi Veluovu (fran. Vélu) [5] formulu da odredi krivu  $E_A = E/G_A$  i izogeniju  $\phi_A : E \rightarrow E_A$ , 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  $G'_A = \langle h[a_1]\phi_B(P_A) + [a_2]\phi_B(Q_A) \rangle$  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.



Slika 1: Protokol razmene ključa

### 3 Napad umetanjem greške

Pretpostavimo da 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 data kriva  $E$  i tačka  $P$ , promena  $x$ -koordinate tačke  $P$  rezultovaće drugom tačkom,  $P'$  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, pošto su tačke  $(P_A, Q_A)$ ,  $(P_B, Q_B)$  i  $(P_C, Q_C)$  redom generatori za  $E[l_A^{e_A}]$ ,  $E[l_B^{e_B}]$  i  $E[f]$ , slučajno odabrana tačka  $X \in E(\mathbb{F}_{p^2})$  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  $\phi_A$ , onda ćemo pokazati kako neko može da iskoristi  $\phi_A(X)$  da dobije  $\phi_A$ . Pošto je  $\phi_A$  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

$$\begin{aligned} \phi_A(X) &= \phi_A([u]P_A + [v]Q_A + [w]P_B + [x]Q_B + [y]P_C + [z]Q_C) \\ &= [u]\phi_A(P_A) + [v]\phi_A(Q_A) + [w]\phi_A(P_B) \\ &\quad + [x]\phi_A(Q_B) + [y]\phi_A(P_C) + [z]\phi_A(Q_C) \end{aligned}$$

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

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

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

**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  $\phi : E_1 \rightarrow E_2$  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  $\psi : E_2 \rightarrow E'$  takvo da je  $\ker \psi = \langle \phi(X) \rangle$ , onda postoji  $\theta : E' \rightarrow E_1$  koje je stepena  $l_A^t$ , tako da je  $t \leq e_A$ , takvo da je

$$\hat{\phi} = \theta \circ \psi$$

Lema nam govori da ako nam je data slika tačke na krivoj  $E_1[l_A^{e_A}]$  u izogeniji  $\phi$ , onda možemo da pronademo izogeniju  $\psi$  koja je približna izogeniji  $\phi$ . Kako bismo dobili  $\psi$  prvo moramo da otkrijemo  $\theta$ . Ako je  $t$  dovoljno malo, onda možemo dobiti  $\theta$  grubom silom. U većini slučajeva  $t$  jeste dovoljno malo. U nastavku je dat algoritam za dobijanje izogenije za slučajno odabranu tačku.

---

**Algorithm 1:** Dobijanje izogenije nakon napada umetanjem greške

---

**Data** :  $\phi(X)$   
**Output:**  $\hat{\phi}$   
1 Postavi  $\lambda \leftarrow l_B^{e_B} \cdot f$  ;  
2 Postavi  $T \leftarrow [\lambda]\phi(X)$  ;  
3 Postavi  $\psi : E_2 \rightarrow E'$  kao izogeniju sa jezgrom  $T$ ;  
4 **if**  $\text{ord}(T) = l_A^{e_A}$  **then**  
5 | return  $\psi$   
6 **else**  
7 | Gruba sila za računanje  $\theta$   
8 **end**  
9 return  $\theta \circ \psi$

---

### 3.2 Izvodljivost napada na protokol razmene ključeva

Razmotrimo protokol razmene ključa opisanog u 2. Pretpostavimo da protivnik pokušava da sazna Alisinu tajnu izogeniju i ima mogućnost da izazove grešku u Alisinom računu. Nakon računanja sa greškom, Alisa objavljuje ključ  $(E_A, \phi_A(X), \phi_A(Q_B))$ . Protivnik će onda biti u mogućnosti da otkrije  $\phi_A$  pomoću Algoritma 1.

Pretpostavimo da jedna strana koristi statički ključ u protokolu razmene ključeva. Protivnik bi bio u mogućnosti da otkrije tajnu izogeniju ako se statički javni ključ preračunava za svaku razmenu. Ipak, to nije verovatno da se desi jer se  $\phi_A(P_B)$  i  $\phi_A(Q_B)$  fiksiraju u programu (engl. *hardcode*) zbog efikasnosti.

Sada pretpostavimo da protivnik napada protokol razmene ključa sa kratkotrajnim ključevima. Ako tajne nisu autentifikovane, protivnik je u mogućnosti da izračuna  $\phi_A(P_B)$  i pošalje to umesto  $\phi_A(X)$ . Na ovaj način, obe strane mogu izvesti istu deljenu tajnu. Pošto se otkrivanje  $\phi_A$  pomoću  $\phi_A(X)$  može izvesti efikasno i računanje  $\phi_A(P_B)$  je efikasno, izvođenje zamene pre nego što istekne vreme za konekciju je veoma izvodljivo. Ipak, treba primetiti da je, ako tajne nisu autentifikovane, bolje koristiti napad „čovjek u sredini” (engl. *man-in-the-middle attack*).

## Literatura

- [1] Yan Bo Ti, *Fault Attack On Supersingular Isogeny Cryptosystems*, Mathematics Department, University of Auckland, 2017.
- [2] David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, PQCrypto '11 Proceedings, 2011.
- [3] Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. 26, 1997.
- [4] Daniel Kirkwood, Bradley C. Lackey, John McVey, Mark Motley, Jerome A. Solinas, and David Tuller, *Failure is not an option: Standardization issues for post-quantum key agreement*, 2015, Workshop on Cybersecurity in a Post-Quantum World.
- [5] Jacques Vélú, *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris, Série A. 273, 1971.