

Kriptografski sustavi temeljeni na eliptičkim krivuljama i mogućnosti njihove primjene

Kuterovac, Marija

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:200:476466>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-12-24**

Repository / Repozitorij:

[Faculty of Electrical Engineering, Computer Science and Information Technology Osijek](#)



**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ELEKTROTEHNIČKI FAKULTET**

Sveučilišni studij

**KRIPTOGRAFSKI SUSTAVI TEMELJENI NA
ELIPTIČKIM KRIVULJAMA I MOGUĆNOSTI
NJIHOVE PRIMJENE**

Diplomski rad

Marija Kuterovac

Osijek, 2015.

SADRŽAJ

1. UVOD	1
2. OSNOVE KRIPTOGRAFIJE	2
2. 1. Kriptografija	2
2. 2. Kriptografski sustav	4
2. 3. Primjena kriptografije	6
2. 4. Sažetak poruke	7
2. 5. Digitalni potpis	7
2. 6. Digitalna otmotnica	8
2. 7. Digitalni pečat	9
2. 8. Kriptografska analiza	9
3. ELIPTIČNE KRIVULJE	11
3. 1. Osnove eliptičnih krivulja	11
3. 1. 1. Zbrajanje na eliptičnoj krivulji	13
3. 1. 2. Skalarno množenje	15
3. 2. Eliptične krivulje nad poljem racionalnih brojeva	15
3. 2. 1. Računanje ranga	16
3. 3. Eliptične krivulje nad konačnim poljem	17
3. 3. 1. Eliptične krivulje nad konačnim poljem F_q	17
3. 3. 2. Eliptične krivulje nad konačnim poljem F_p	19
3. 3. 3. Eliptične krivulje nad konačnim poljem F_{2^m}	21
3. 3. 4. Singularne eliptične krivulje	24
3. 3. 5. Koblitzove krivulje	24
3. 4. Problem diskretnog logaritma za eliptične krivulje	25
3. 4. 1. Index calculus metoda	25
3. 4. 2. Problem diskretnog logaritma za eliptične krivulje	25
3. 5. Kriptografski sustavi koji koriste eliptične krivulje	26
3. 5. 1. ElGamalov kriptografski sustav	27
3. 5. 2. Menzes-Vanstoneov kriptografski sustav	28
3. 5. 3. Elliptic curve encryption system	29
3. 5. 4. Demytkov kriptografski sustav	31
3. 5. 5. KMOV kriptografski sustav	32
3. 5. 6. Kuwokado-Koyama kriptografski sustav	33
3. 6. Digitalni potpis temeljen na eliptičnim krivuljama	34
3. 6. 1. DSA algoritam koji koristi eliptične krivulje	35
3. 6. 2. ECDSA algoritam	36
3. 6. 3. ECSS shema digitalnog potpisa	38
3. 6. 4. EC Nyberg – Rueppelova shema digitalnog potpisa	40
3. 6. 5. OFF shema digitalnog potpisa	41
3. 7. Protokoli za razmjenu tajnog ključa	42
3. 7. 1. ECDH (engl. <i>Elliptic Curve Diffie – Hellman protocol</i>)	43
3. 7. 2. EC Nyberg – Rueppelov protokol	45
3. 8. Sustavi za raspodjelu ključeva	46
3. 8. 1. Sakazaki – Okamoto – Mamba sustav za raspodjelu ključeva temeljen na identifikatoru koji koristi eliptične krivulje	47
3. 9. Specifičnosti eliptičnih krivulja	49
3. 9. 1. Performanse i sigurnost	49
3. 9. 2. Kompleksnost diskretnog logaritamskog problema	50

3. 9. 3. Generiranje krivulja.....	50
3. 9. 4. Nekompatibilni sistemi	51
3. 9. 5. Procesiranje	51
3. 9. 6. Utrošak energije na bežičnim mrežama	52
4. USPOREDBA S DRUGIM KRIPTOGRAFSKIM SUSTAVIMA	53
5. SIMULACIJA KRIPTOGRAFSKOG SUSTAVA TEMENLJENOG NA ELIPTIČNIM KRIVULJAMA.....	57
5. 1. ECDSA algoritam	57
5. 2. ElGamalov kriptografski sustav	62
5. 2. 1. RSA algoritam.....	71
6. ZAKLJUČAK	73
LITERATURA.....	74
SAŽETAK.....	77
ABSTRACT	78
ŽIVOTOPIS	79
PRILOZI.....	80

SAŽETAK

Širenjem različitih varijanti ugrađenih računalnih sustava s mogućnostima komunikacije javlja se potreba za kriptografskim sustavima temeljenim na eliptičkim krivuljama zbog toga što su prikladniji od drugih asimetričnih kriptografskih sustava. Glavni razlog zbog kojeg se javlja potreba za zamjenom postojećih kriptografskih sustava je ta da su s napretkom tehnologije napredovale i razvijale se metode za presretanje i otkrivanje podataka iz šifrata, a sami napadi su postajali sve učinkovitiji. Neprekidnim mijenjanjem duljine ključeva, radi povećanja sigurnosti prijenosa podataka, pojavio se problem zahtjevnosti ključa, pohrane i brzine obrade podataka kod konvencionalnih kriptografskih sustava. Stoga se rješenje pronalazi u kriptografskim sustavima temeljenima na eliptičnim krivuljama jer osiguravaju manju hardversku zahtjevnost, veću brzinu i visoku sigurnost podataka i komunikacije nesigurnim komunikacijskim kanalom. Važno je napomenuti da je teško izvršiti napad na kriptografske sustave temeljene na eliptičnim krivuljama i otkriti privatne ključeve članova koji se nalaze u sjednici upravo zbog same složenosti krivulje i digitalnog potpisa koji se koriste. Kao novo razvijena metoda koja se pojavila u kriptografiji predstavlja problem napadačima zbog nepoznavanja metoda za napad na ovakve sustave i upravo zbog toga javlja se potreba za sve većom implementacijom u računalne sustave.

Ključne riječi: kriptografija, kriptografski sustavi, kriptografski sustavi temeljeni na eliptičnim krivuljama, eliptične krivulje, problem diskretnog logaritma, ElGamal, Menzes-Vanstone, KMOV, Demytkov, digitalni potpis, ECDSA, Diffie-Hellman protokol za razmjenu tajnog ključa

ABSTRACT

As the different sorts of computer systems with possibility of communication have appeared, there is a greater need for crypto systems based on elliptic curves, because they are more appropriate than other asymmetric crypto systems. With the development of technology, the methods for cipher text content interception and acquisition have also been developed, and that is the main reason for the fact that existing crypto systems had to be changed. The attacks themselves have become more efficient. By continuously changing the length of the keys to improve security of data transmission, conventional crypto systems have faced the problem with the key complexity, data storage and data processing rate. The solution has been found in crypto systems based on elliptic curves, because they ensure less hardware complexity, higher rates, and high level of data security. It is important to mention that creation of efficient attack on crypto system based on elliptic curves and finding private keys of session members is extremely hard task, because elliptic curves and digital signature that are used are extremely complex. As a newly developed method that has appeared in crypto systems, it is pretty difficult for attackers, because the methods to attack these systems are still unknown, and that is the main reason for increasing need to implement these systems in computer systems.

Keywords: cryptology, crypto systems, elliptic curve cryptology, elliptic curves, discrete logarithm problem, ElGamal, Menzes-Vanstone, KMOV, Demytkov, digital signature, ECDSA, Diffie-Hellman secret key exchange protocol.