Kriptografski sustavi temeljeni na eliptičkim krivuljama i mogućnosti njihove primjene

Kuterovac, Marija

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

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.