IT'15
ŽABLJAK

XX

međunarodni naučno - stručni skup

INFORMACIONE TEHNOLOGIJE

SADAŠNJOST I BUDUĆNOST

Urednik
Božo Krstajić

IT'15

INFORMACIONE TEHNOLOGIJE

- SADAŠNJOST I BUDUĆNOST -

Urednik
Božo Krstajić

Zbornik radova sa XX međunarodnog naučno - stručnog skupa
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost
održanog na Žabljaku od 23. do 28. februara 2015. godine

Zbornik radova
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost 2015

Glavni urednik
Prof.dr Božo Krstajić

Izdavač
Univerzitet Crne Gore
Elektrotehnički fakultet
Džordža Vašingtona bb., Podgorica
www.etf.ucg.ac.me

Tehnička obrada
Aleksandra Radulović
Centar Informacionog Sistema
Univerziteta Crne Gore

Tiraž
150

Podgorica 2015.

Organizator
Elektrotehnički fakultet, Univerzitet Crne Gore

Suorganizatori:
Elektrotehnički fakultet, Univerzitet u Beogradu
Elektrotehnički fakultet, Univerzitet u Banja Luci
Elektronski fakultet, Univerzitet u Nišu
Fakultet tehničkih nauka, Univerzitet u Novom Sadu

Skup su podržali:
Ministarstvo za informaciono društvo i telekomunikacije
Agencija za elektronske komunikacije i poštansku djelatnost
doMEn d.o.o.
Terna Crna Gora
Pošta Crne Gore

Programski odbor

Dr Novak Jauković, Elektrotehnički fakultet, Podgorica, MNE
Dr Ljubiša Stanković, Elektrotehnički fakultet, Podgorica, MNE
Dr Zdravko Uskoković, Elektrotehnički fakultet, Podgorica, MNE
Dr Vujica Lazović, Ekonomski fakultet, Podgorica, MNE
Dr Branko Kovačević, Elektrotehnički fakultet, Beograd, SRB
Dr Milorad Božić, Elektrotehnički fakultet, Banja Luka, BIH
Dr Miroslav Bojović, Elektrotehnički fakultet, Beograd, SRB
Dr Zoran Jovanović, Elektrotehnički fakultet, Beograd, SRB
Dr Milica Pejanović-Đurišić, Elektrotehnički fakultet, Podgorica, MNE
Dr Despina Anastasiadou, Research & Development Innovation Academy, Solun, GRC
Dr Dejan Popović, Elektrotehnički fakultet, Beograd, SRB
Dr Gabriel Neagu, National Institute for Research & Development in Informatics, Bucharest, ROU
Dr Božo Krstajić, Elektrotehnički fakultet, Podgorica, MNE
Dr Tomo Popović, Texas A&M Univerzitet, College Station, TX, USA
Dr Milovan Radulović, Elektrotehnički fakultet, Podgorica, MNE
Dr Le Xie, Texas A&M University, College Station, TX, USA
Dr Sašo Gelev, Elektrotehnički fakultet, Radoviš, MKD
Dr Budimir Lutovac, Elektrotehnički fakultet, Podgorica, MNE
Dr Igor Radusinović, Elektrotehnički fakultet, Podgorica, MNE
Dr Alex Sprintson, Texas A&M University, College Station, TX, USA
Dr Igor Đurović, Elektrotehnički fakultet, Podgorica, MNE
Dr Miloš Daković, Elektrotehnički fakultet, Podgorica, MNE
Dr Milutin Radonjić, Elektrotehnički fakultet, Podgorica, MNE
Dr Ana Jovanović, Elektrotehnički fakultet, Podgorica, MNE
Dr Vesna Rubežić, Elektrotehnički fakultet, Podgorica, MNE
Dr Ramo Šendelj, Fakultet za Informacione Tehnologije, Podgorica, MNE
Dr Stevan Šćepanović, Prirodno-matematički fakultet, Podgorica, MNE

Organizacioni odbor

Dr Novak Jauković, Elektrotehnički fakultet, Podgorica
Dr Božo Krstajić,Elektrotehnički fakultet, Podgorica / CIS UCG
Dr Milovan Radulović, Elektrotehnički fakultet, Podgorica
Dr Zoran Veljović, Elektrotehnički fakultet, Podgorica
Dr Ana Jovanović, Elektrotehnički fakultet, Podgorica
Dr Saša Mujović, Elektrotehnički fakultet, Podgorica
MSc Žarko Zečević, Elektrotehnički fakultet, Podgorica
Vladan Tabaš, dipl.ing., Čikom, Podgorica

Sekretarijat

Aleksandra Radulović, CIS Univerzitet Crne Gore

P R E D G O V O R

Poštovani učesnici i čitaoci,

Pred vama je jubilarni XX zbornik radova međunarodnog naučno-stručnog skupa “INFORMACIONE TEHNOLOGIJE – sadašnjost i budućnost” (IT’15) koji je uspješno održan od 23. do 28. februara 2015. godine na Žabljaku. Programski odbor je izvršio selekciju kvalitetnih radova koji su pred vama, a najbolji među njima će biti prošireni i objavljeni u časopisu Elektrotehničkog fakulteta Univerziteta Crne Gore u Podgorici ("ETF Journal of Electrical Engineering").

Ovakav jubilej i jubilarni Zbornik je prilika da se osvrnemo i na misiju ove konferencije, na neke univerzalne vrijednosti koje smo zadržali, a i na inovacije koje smo uveli. U proteklih 20 godina IT je prepoznat kao relevantna, nekad nacionalni, sada međunarodni naučno stručni skup koji se trudio i trudi da omogući širokom spektru naučnika i stručnjaka prezentaciju, kako rezultate naučnih istraživanja i trendova, tako i uspješnih stručnih projekata i rješenja. Nijesmo se nikad ograničavali samo na ICT, već smo ostavljali prostor za sve oblasti nauke i djelatnosti u kojima se primjenjuje ICT, a teško je danas naći izuzetke. Trudili smo se da se na IT-u pojavljuju najeminentniji naučnici i stručnjaci, ali i mladi istraživači, inženjeri, a zadnje dvije godine i studenti. Uveli smo i neke nove prakse kao posledice primjene tehnologija koje promovišemo: elektronsku obradu korespodencije sa autorima, elektonski proces recenzije, objavljivanja radova na sajtu, katalogizaciju istih te online praćenje i prezentovanje radova.Proširili smo djelatnost konferencije sa učešćem kompanija i institucija sa uspješnim prijektima, a posebno smo ponosni i na studentsko učešće. Ove godine smo posvetili čitav segment samo studentima i pripremili posebna predavanja i prezentacije za njih. Konačno i tradicionalno, vjerovatno jedan od značajnih argumenata za učešće na IT-u je neponovljiva priroda Durmitora, gostoprimstvo grada i poslovnično nezaboravna druženja učesnika.

Ovdje je svakako mjesto da se pomenu i rodonačelnici ovog skupa, koji su prije 20 godina započeli ovu konferenciju: prof. dr Novak Jauković, prof. dr Srbijanka Turajlić, prof. dr Dejan Popović i prof. dr Srđan Stanković, i čije je aktivno učešće u radu jubilarnog skupa potvrda da isti ima kontinuitet, kredibilitet i budućnost.

Sve detalje o ovom, prošlim i narednom skupu možete naći na web adresi konferencoije www.it.ac.me.

Prof. dr Božo Krstajić

SADRŽAJ

PREGLED INTEGRISANE ŠEME PO ELIPTIČKOJ KIRIVULJI
OVERVIEW OF ELLIPTIC CURVE INTEGRATED SCHEME

Maja Kukuševa Paneva, Biljana Čitkuševa Dimitrovska, Goce Stefanov, *Faculty of Electrical Engineering, UGD - Štip, R.Macedonia*

Sadržaj: *U ovom radu je data integrirana šema za enkripciju po eliptičkoj krivi* (*ECIES*). *ECIES je hibridna šema bazirana na eliptičkim krivama koja uključuju u sebe kriptiranje i dekriptiranje, izračunavanje haš funkcije I autentifikaciju. U ovom radu će biti prikazana analiza potrošene energije i upotrebljene RAM i ROM memorije.*

Abstract: *This paper gives overview of integrated encryption scheme over elliptic curve* (*ECIES*). *ECIES is hybrid scheme based on elliptic curve that includes encryption and decryption algorithm, hash computation and authentication. Analysis of simulation scenarios about energy and RAM and ROM memory consumption will be represented in this paper.*

1. INTRODUCTION

Elliptic Curve Cryptography is public key cryptography proposed independently by N. Koblitz and V. Miller in 1985. Implementation of ECC include elliptic curve digital signature algorithm, Integrated Scheme and Diffie- Hellman. Elliptic Curve Integrated Scheme (ECIES) is hybrid scheme that uses public key system to transport the session key for usage in symmetric chipper. Also, ECIES provides semantic security against chosen plaintext and chosen chippertext attacks.

ECIES [1, 2] is based on elliptic curve discrete logarithm problem [3]. The difficulty of ECDLP is based on finding integer $l \in [0, n-1]$ such that for given elliptic curve E, $P \in E(K)$ and $Q \in \langle P \rangle$ defined over finite fields F_p, $Q = lP$. The integer l must be large prime in order to avoid Pohling- Hellman [4] and Pollard's rho attacks [5, 6]. The method for solving ECDLP is fully exponential which results in decreasing key size needed to achieve same level of security when using conventional public key schemes. Comparing to 1034-bit RSA the same level of security is achieved using 160 bit key [7].

In this paper analysis about memory and energy consumption of ECIES will be represented. The analysis is done using software package TinyECC in TinyOS. In sector 2 the background of ECIES is represented. In sector 3 is given description of simulation scenario (grid and random topology), measured parameters (CPU Total, Radio Total and Total Energy), obtained results and their analysis. Sector 4 concludes this paper.

2. BACKGROUND

ECIES is standard encryption algorithm a variant of ElGamal encryption scheme proposed be Rogaway and Bellare [8]. This scheme is standardized in ANSI X9.63, ISO/IEC 15946-3 and IEEE P1363a. Based on sheared secret obtained by Diffie- Hellman, ECIES derives two symmetrical keys. The first is used for encryption of the plaintext while the second is used for authentication of the received encrypted message. The functional diagram of ECIES is represented in Figure 1 and includes key derivation function (KDF), encryption and decryption and message authentication. Key derivation function KDF is constructed from hash function H. For *l*- bits key KDF(*S*) is defined as concatenation of the hash values H(*S*, *i*), where *i* is counter incremented for each hash function until *l* bits of hash values have been generated. ENC is symmetric key encryption scheme while DES is decryption function. MAC is message authentication code algorithm.

First step in using ECIES is selection of elliptic curve and domain parameters agreement between nodes Alice and Bob. Alice and Bob secretly choose random integer primes k_{rA} and k_{rB} so that $0 < k_{rA}$ and $k_{rB} < n$ (private keys). At the beginning Alice generates key pair which is consist of public key (point from the elliptic curve) obtained as multiplication of Alice's private key and the base point G. After that Alice uses key agreement function in order to obtain the sheared secret. This is performed by multiplication of Alice's private key and Bob's public key:

$$Q_{uA} = k_{rA} G \tag{1}$$

Then the value obtained from Equation 1 is used as an input in key derivation function. The output of KDF is concatenation of symmetric encryption key k_{ENC} and MAC key k_{MAC}. Alice uses the encryption key k_{ENC} to encrypt the plaintext *m* and thus to obtain the encrypted message *c*. The value *tag* is generated from the encrypted message *c* and k_{MAC}. At the end Alice sends the values of Q_{uA}, *tag* and *c* to Bob. On the other side, Bob in order to decrypts the received message multiplies its private key k_{rB} with Alice's public key and obtains the sheared secret. From the sheared secret Bob derives the same k_{ENC} and k_{MAC} as Alice. Using the MAC key k_{MAC} and encrypted message Bob generates *tag**

value. If the values of *tag* and *tag** are not the same, Bob rejects the received message due to invalid verification.

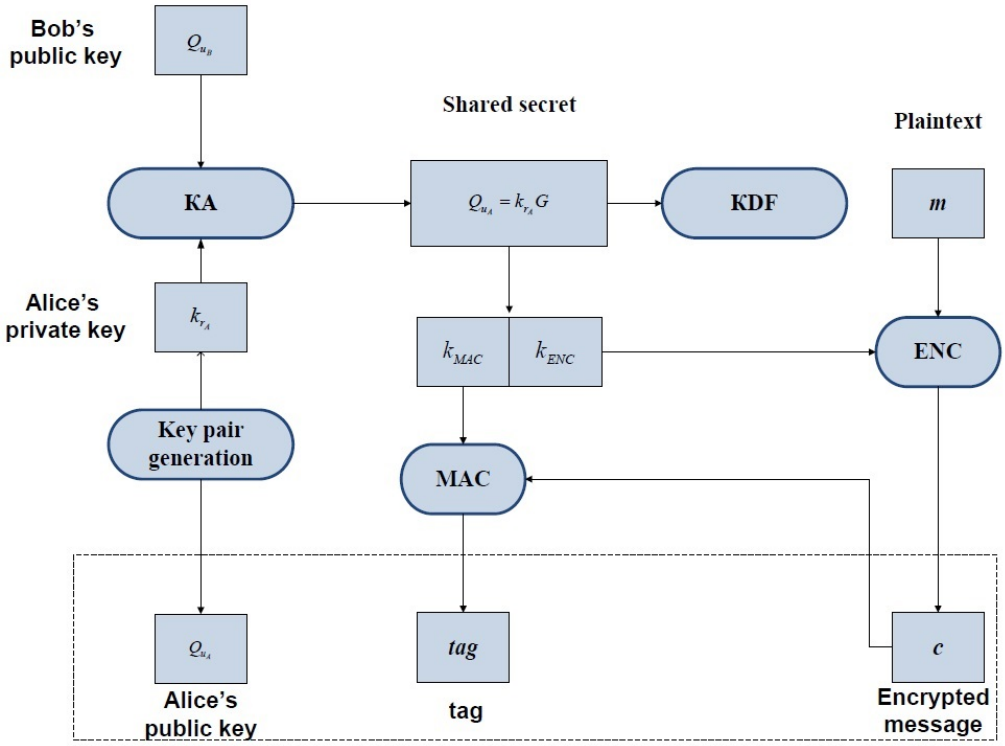

Figure 1. ECIES functional diagram

If the tag values are same, Bob decrypts the message using k_{ENC} and obtains the plaintext.

3. SIMULATION AND RESULTS

TinyOS [9] is an open source operating system for low power and limited resource applications that utilize wireless sensor networks. TinyOS has specially designed simulator TOSSIM [10] that allows debugging, testing and analyze of code written in nesC. TOSSIM has extension that provides per node estimation of power consumption and power management. The power analyze is done using the software package TinyECC1.0. TinyECC1.0 includes three elliptic curve cryptography schemes Elliptic Curve Integrated Scheme, Elliptic Curve Diffie- Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) which are not scope of this paper. The simulations are performed according NIST recommendation [11] for domain parameters $T = (p, a, b, G, n, h)$. Two curves have been analyzed secp128r1 and secp192k1 with affine coordinates. According to NIST recommendation the key size for the curve secp128r1 is 128-bits from which 64- bits are for security, while the key size for secp192k1 is 192-bits from which 96-bits are for security. Number of nodes are integer from square root from 4 up to 100 nodes. Two types of topology were deployed, random and grid as shown on Figure 2. In random topology nodes are randomly placed in working environment, unlike grid topology were nodes are placed in regular square were the distance between neighbor nodes is same. The duration of every simulation is 20 seconds.

The consumption of RAM and ROM memory after compiling IEC algorithm for both curves are represented in Table 1.

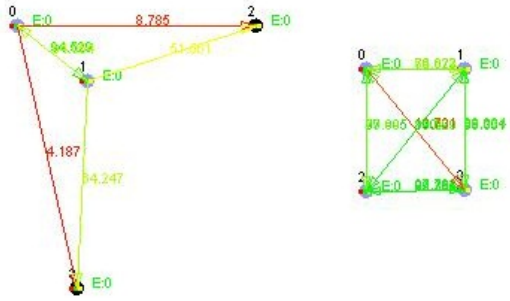

Figure 2. Simulation topology a) random b) grid

Table 1. ROM and RAM consumption

ECIES 128-bit key		ECIES 192-bits key	
1051	Bytes in ROM	1763	Bytes in ROM
28138	Bytes in RAM	28850	Bytes in RAM

The key parameters that were analyzed in term of energy consumptions are CPU Total, Radio Total and Total Energy. The parameter CPU total gives the mean energy (mJ) used for key pair derivation and generation and processing of messages. The parameter Radio Total gives the mean energy (mJ) used for transmission of the public key and communication with the other nodes in the network.

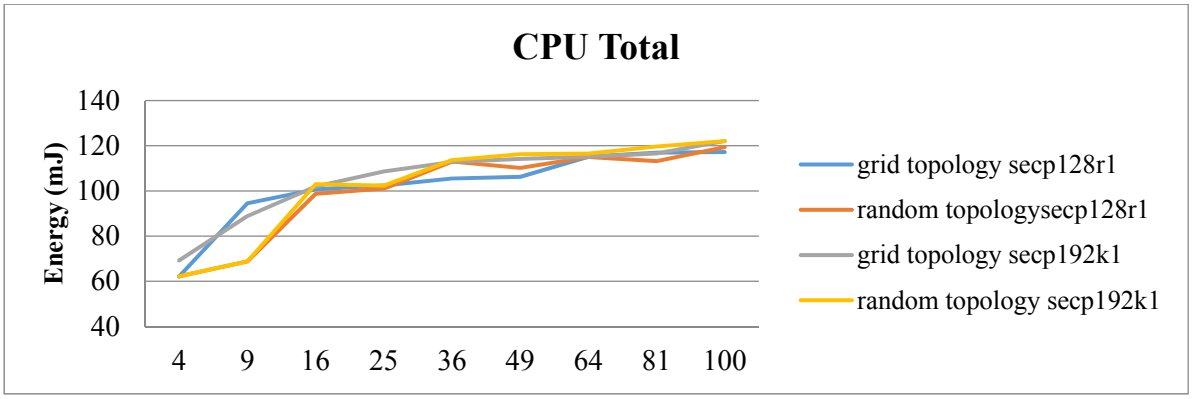

Figure 3. Parameter CPU Total

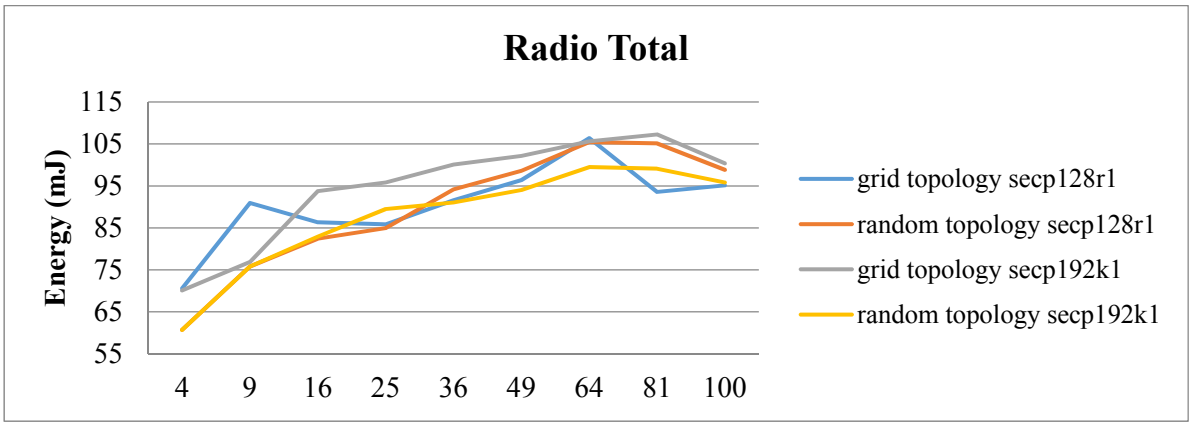

Figure 4. Parameter Radio total

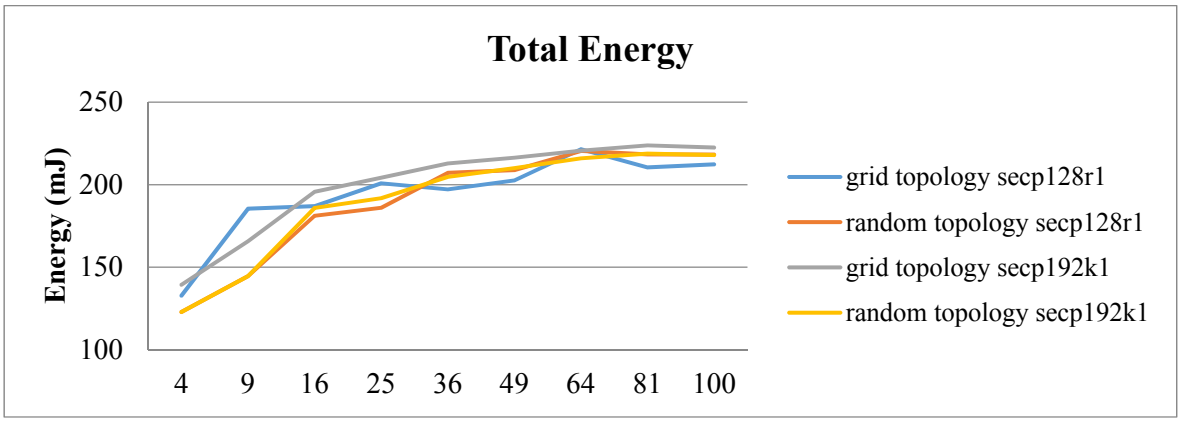

Figure 5. Parameter Total Energy

The parameter Total Energy gives the total mean energy (mJ) used and is sum of parameter CPU Total and Radio Total. The results from measurement of these parameters are shown in Figure 3, 4 and 5, appropriately.

4. CONCLUSION

ECIES is public key encryption scheme that includes public key derivation, encryption, decryption and authentication. In this paper was represented memory consumption and energy analysis in term of energy used for derivation of public key, communication with other nodes in the network, message processing and encryption and decryption process. From the obtained results can be concluded that the RAM and ROM memory consumptions depends on the key size. For longer key size the consumption of RAM and ROM memory increases**.** Also by increasing the number of nodes the energy consumption increases due to more mathematical operation that have to be performed for every node. But, the energy consumption does not depend on used curve or network topology.

Future work will involve optimization of energy consumption by introduction of projective coordinates and optimization algorithms about mathematical operation (multiplication, reduction, inversion etc.).

REFERENCES

[1] M. Abdalla, M. Bellare, P. Rogway, DHIES: An Encryption Scheme Based on the Diffie- Hellman Problem, *Contribution on IEEE* P1363a, 1998.

[2] M. Abdalla, M. Bellare, P. Rogway, DHIES: An Encryption Scheme Based on the Diffie- Hellman Problem, *Contribution on IEEE* P1363a, 1998.

[3] M. Abdalla, M. Bellare, P. Rogway, The oracle Diffie-Hellman assumptions and an analysis of DHIES, *Lecture Notes in Computer Science* 2020, 201 pp. 143-158.

[4] C. Diem, On the discrete logarithm problem in elliptic curves II, Algebra & Number Theory 7, pp. 1281-1323, 2013.

[5] S. Pohing, M. Hellman, An improved algorithm for computing logarithm over GF(p) and its cryptographic significance", IEEE Transactions on Information Theory, pp.106-110, 1978.

[6] P. van Oorshot, M.Wiener, Parallel collision search with cryptanalytic applications, Journal of Cryptology, 1-28, 1999.

[7] J.Pollard, Monte Carlo methods for index computation mod p, Mathematics of Computation, pp. 918-924, 1978.

[8] N. Gura, A. Patel, A. Wander, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, *In Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems* (CHES 2004), pp 119-132, August 2004.

[9] Bellare, Rogaway, Minimizing the use of random oracles in authenticated encryption schemes, *Information and Communication Security' 97* (INCS 1334), 1-16, 1997.

[10] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, Eric Brewer, David Culler, TinyOS: An Operating System for Sensor Networks, *In Ambient Intelligence*, Spinger- Verlag 2004.

[11] Philip Levis, Nelson Lee, Matt Welsh, David Culler, TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Application, *Proceedings of SenSys' 03 First ACM Conference on Embedded Networked Sensor Systems*, 2003.

[12] National Institute of Standards. Recommended Elliptic Curves for Federal Government Use, July 1999.

CIP - Каталогизација у публикацији
Национална библиотека Црне Горе, Цетиње

ISBN 978-86-85775-16-1
COBISS.CG-ID 27237136

ISBN 978-86-85775-16-1