Primena enkripcionih šema zasnovanih na identitetima u naprednoj elektroenergetskoj mreži

Srđan Đorđević, Slobodan Bojanić

Apstrakt—**Informaciona bezbednost napredne elektroenergetske mreže značajno zavisi od primenjenog metoda autentifikacije i sistema za upravljanje ključevima. U ovom radu predlaže se primena kriptografske šeme zasnovane na identitetima u naprednoj mernoj infrastrukturi zbog veoma jednostavnog sistema za upravljanje ključevima. Razmatrali smo izvesne probleme vezane za praktične i teoretske aspekte kriptografije zasnovane na identitetu i ispitivali pod kojim uslovima se ovaj tip kriptografije može primeniti za obezbeđivanje informacione zaštite napredne elektroenergetske mreže.**

Ključne reči— **napredna merna infrastruktura; napredna elektroenergetska mreža; kriptografija zasnovana na identitetima.**

I. Uvod

Jedan od ključnih problema u daljem razvoju napredne elektroenergetske mreže (*Smart Grid*, SG) je obezbeđivanje informacione sigurnosti. Dvosmerna komunikacija između potrošača i proizvođača električne energije realizuje se uz upotrebu širokog spektra fizičkih mreža na različitim delovima napredne elektroenergetske mreže što ima za posledicu povećanje ranjivosti sistema na sajber napade i havarije. Informaciona bezbednost mora da uzme u obzir ne samo namerne napade već i greške korisnika, kvarove na opremi kao i prirodne katastrofe. Sigurnost SG je usled njene kompleksnosti moguće obezbediti isključivo uz primenu mera fizičke i informacione zaštite na svim nivoima.

Enkripcione šeme koje se primenjuju u SG mreži radi postizanja informacione bezbednosti moraju pored visokog stepena sigurnosti da ispune i određene dodatne zahteve koji proističu iz ograničenja AMI sistema. Usled ograničenog propusnog opsega komunikacionih linija potrebno je smanjiti količinu podataka koji se njima prenose na najmanju moguću meru. Drugo ograničenje AMI sistema predstavlja slaba procesorska moć naprednih brojila usled čega je neophodno da procedure enkripcije i dekripcije budu maksimalno efikasne. Da bi se smanjili troškovi razvoja individualnih enkripcionih šema potrebno je da enkripcioni algoritam bude kompatibilan sa različitim platformama.

Sagledavajući karakteristike koje treba da odlikuju kriptosistem primenjen u SG proizilazi da jedno od mogućih rešenja za obezbedjivanje informacione zaštite SG predstavlja primena enkripcije zasnovane na identitetima (*Identity-based encryption* – IBE). IB enkripcija predstalja tip asimetričnog kriptivanja čije je najvažnije svojstvo da javni ključ entiteta predstavlja neku jedinstvenu informaciju kojom je opisan taj uređaj ili osoba [1]. Glavni motiv za razvoj IB kriptosistema je bio eliminacija infrastrukture javnog ključa čime je u odnosu na klasičan kriptosistem značajno pojednostavljen postupak autentifikacije.

Naredno poglavlje daje opis enkripcije zasnovane na identitetima. U okviru trećeg poglavlja dato je poređenje klasičnog kriptosistema i IB kriptosistema. Sažet prikaz implementacije IBE kriptosistema dat je u četvrtom poglavlju. Peto poglavlje posvećeno je primeni IBE kriptosistema u naprednoj elektroenergetskoj mreži.

II. Enkripcija zasnovana na identitetima

Glavni motiv za uvođenje IB kriptosistema je pojednostavljivanje distribucije ključeva s obzirom da se svi ključevi izvode iz identiteta entiteta. Uvođenjem ovakvog koncepta ukinuta je potreba za postojanjem digitalnog sertifikata odnosno distribucija ključeva se obavlja bez sertifikacionih tela i procedura za izdavanje i proveru važenja sertifikata.

Prilikom slanja podataka svaki pojedinačni paket se enkriptuje javnim ključem primaoca i potpisuje privatnim ključem pošiljaoca. Na prijemu je postupak obrnut, dekirptovanje se obavlja primenom privatnog ključa primaoca a verifikacija se obavlja primenom javnog ključa pošiljaoca.

Prilikom inicijalizacije IB kriptosistema treća strana od poverenja koja nosi naziv centar za generisanje ključeva (*Key Generator Center* - KGC) generiše glavni privatni i glavni javni ključ.

U IB kriptografskoj šemi pošiljalac enkriptuje poruku na osnovu digitalnog identiteta primaoca i glavnog javnog ključa. Ova procedura se obavlja bez prethodne interakcije sa bilo kojom komponentom sistema. S obzirom da je autentifikacija garantovana implicitno sve do trenutka dok je prenos privatnog ključa do odgovarajućeg korisnika siguran eliminisana je potreba za postojanjem infrastrukture javnog ključa kao i digitalnih potpisa.

Primalac poruke dekriptuje poruku primenom tajnog ključa koji dobija od KCG. Tokom ove procedure entitet koji dekriptuje poruku mora da obavi autentifikaciju u odnosu na KGC kao uslov za prijem tajnog ključa.

Procedura IB digitalnog potpisivanja (*Identity Based*

Srđan Đorđević– Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, Srbija (e-mail: srdjan.djordjevic@ elfak.ni.ac.rs).

Slobodan Bojanić – Escuela Técnica Superior de Ing. de Telecomunicación, Universidad Politecnica de Madrid, Madrid, Spain (e-mail: slobodan@die.upm.es).

Signature - IBS) odvija se suprotnim redosledom, pošiljalac kreira digitalni potpis primenom tajnog ključa koji je dobijen od KGC dok primalac proverava identitet pošiljaoca poruke primenom digitalno identiteta pošiljaoca i glavnog javnog ključa.

Privatni ključevi svih entiteta generišu se iz master ključa koji je smešten na jednom mestu, odnosno u KGC. Razbijanjem ovog ključa ugrozila bi se bezbednost celog sistema.

Da bi se uspešno obavila razmena podataka na komunikacionoj liniji neophodno je ostvariti uzajamnu identifikaciju (autentifikaciju) izvora informacija. Autentifikacionih protokoli koji se primenjuju u AMI mogu se podeliti u sledeće tri kategorije:

1. Protokoli koji primenjuju simetričnu kriptografiju uz primenu centra za distribuciju ključeva [3]
2. Protokoli koji se zasnivaju na primeni kriptografije javnog ključa i infrastrukture javnog ključa (*Public Key Infrastructure* - PKI) [4]
3. Protokoli koji primenjuju enkripciju zasnovanu na identitetima (*Identity-based encryption* – IBE) [5, 6]

Ukoliko se za autentifikaciju koristi tajni ključ odnosno simetrični kriptografski algoritam neophodno je obezbediti skup ključeva za svaki uređaj kao i razmenu ovih ključeva između uređaja. Distribucija ključeva u simetričnom kriptografskom sistemu obavlja se uz primenu trećeg entiteta kome veruju obe strane, takozvanog centar za distribuciju ključeva. Autentifikacioni protokoli bazirani na simetričnoj kriptografiji nisu našli širu primenu u AMI sistemima jer pored činjenice da je koordinacija ovih procedura veoma kompleksna ne postoji ni ekonomska opravdanost za njihovo korišćenje.

Postupak autentifikacije primenom digitalnog potpisa je jednostavniji za realizaciju i ekonomski opravdaniji. Svaki od uređaja ima tajni ključ koji se formira u toku postupka instalacije kao i jedan sertifikat za upravljanje ključevima. Tehnika digitalnog potpisa za kriptovanje koristi tajni ključ entiteta koji šalje poruku dok se za dekriptovanje primenjuje javni ključ istog entiteta. Ovakav pristup je opravdan jer je od primarnog značja verifikacija uređaja koji šalje poruku a ne zaštita sadržaja poruke. Uobičajena je primena HMAC (*Hash-based Message Authentication Code*) algoritma prema kome se potpisivanje (kriptovanje) obavlja nad sažetkom poruke koji se dobija primenom neke od heš fukcija. Ovako potpisani sašetak poruke (message digest) šalje se zajedno sa izvornom porukom. Na ovaj način istovremeno se obezbeđuje integritet podataka i autentifikacija poruke.

Značajna razlika između konvencionalnog i IB kripto sistema ogleda se u mehanizmu upravljanja ključevima. U konvencionalnoj infrastrukturi javnog ključa, koja je zasnovana na sertifikatima, privatne ključeve generišu sami entiteti ili sertifikaciono telo. U IB kriptografskom sistemu privatne ključeve kreira isključivo centar za generisanje ključeva, KGC, nakon verifikacije identiteta entiteta koji je poslao zahtev, primenom master ključa nad digitalnim identitetom. Centar za generisanje ključeva je kontrolisan i upravljan od strane poverljivog tela (*Thrusted Authority*) koji predstavlja treću strane od poverenja. Dok u klasičnom kriptosistemu sa trećom stranom od poverenja komunicira entitet koji šalje poruku u IB kriptosistemu entitet koji prima poruku treba da obezbedi ključ.

Značajna odlika IB kriptosistema je da obezbeđuje bolji kompromis između sigurnosti i kompleksnosti u odnosu na ostale kriptografske sisteme. Iako su mogućnosti IB kriptosistema velike ova tehnologija trenutno više postoji u teoriji i nije još testirana u praksi. Prilikom njene praktične implementacije pojavili su se izvesni problemi koji su usporili realizaciju. Sa druge strane klasičan kriptosistem zasnovan na infrastrukturi javnog ključa je već više godina široko rasprostranjena tehnologija proverena u praksi.

Prvi predlog za praktičnu realizaciju IB kriptosistema primenom uparivanja predložen je pre desetak godina.

Prvu praktičnu implementaciju IBE dali su Boneh i Franklin 2001 godine uz primenu Weil uparivanje nad eliptičkim krivama [2].

III. Poređenje kriptosistema zasnovanih na identitetu i klasične infrastrukture javnog ključa

Radi sprovođenja postupka autentifikacije, odnosno uzajamne verifikacije entiteta, neophodno je postojanje registracionog telo (*Registration Authority*, RA) čija je funkcija dodela jedinstvenog digitalnog identiteta svim entitetima. Entitet za koji je generisan digitalni identitet dostavlja se u slučaju PKI sertifikacionom telo (*Certificate Authority*, CA) a u slučaju IB kriptosistema centru za generisanje ključeva, KCG. U klasičnom kriptosistemu sertifikaciono telo dodeljuje entitetu digitalni sertifikat koji povezuje javni ključ sa digitalnim identitetom i time garantuje identitet korisnika dok u IB kriptosistemu KGC generiše tajni ključ entiteta koji je potrebno sigurnim komunikacionim kanalom dostaviti entitetu. Odavde proizilazi da je realizacija IB kriptosistem moguća u primenama gde korisnici ne zahteva često tajni ključ ili u aplikacijama gde je jednostavno uspostaviti sigurni komunikacioni kanal kao što su relativno mali sistemi.

Postupak zamene ključa usled isteka važenja ili kompromitovanja ključa je u klasičnoj infrastrukturu javnog ključa, PKI, jednostavan i svodi se na to da entitet generiše novi par ključeva za koje dobija sertifikat. Svi ključevi koji nisu važeći su dostupni u listi opoziva sertifikata (*Certification Revocation List*, CRL) koja je javno dostupna. Sa druge strane postupak zamene ključeva u u IB kriptosistemu je znatno komplikovaniji s obzirom da javni ključ entiteta u IB kriptosistemu na jedinstven način izveden iz njegovog identiteta koji treba da bude javno dostupan. Praktično je nemoguće zameniti ključ entiteta uvek kada je to potrebno. Delimično rešenje ovog problema je da se za generisanje javnih ključeva pored informacija o identitu primene i informacije opšteg tipa. Jedno praktično rešenje bi bilo da javni ključ sadrži u sebi informaciju o vremenskom periodu u toku koga je ključ važeći. Ukoliko bi ovi vremenski periodi bili suviše kratki ugrozila bi se sigurnost sistema jer bi

u tom slučaju bilo neophodno često prenositi tajni ključ između KGC i svakog pojedinačnog entiteta.

Centar za generisanje ključeva predstavlja najranjiviju tačku u IB kriptosistemu. Napadač koji dođe u posed glavnog ključa može da generiše tajne ključeve svih entiteta u sistemu i samim tim da čita sve šifrovanje poruke kao i da falsifikuje potpise svih entiteta u sistemu. Odavde proizilazi da je od velike važnosti očuvati bezbednost glavnog ključa. Jedno od rešenja ovog problema je distribucija tajnog ključa između više centara za generisanje ključeva. Drugi pristup je promena master ključa u regularnim vremenskim intervalima uz istovremeno ažuriranje privatnih ključeva svih entiteta. U klasičnoj infrastrukturi javnog ključa takođe postoji problem ranjivosti sertifikacionih tela. Ukoliko bi napadač došao u posed tajnog ključa sertifikacionog tela bio bi u mogućnosti da dekriptuje sve poruke onih entiteta kojima je izdao javni ključ, znači samo od trenutka preuzimanja ključa za razliku od napada na IB kriptosistem.

S obzirom da su u IB kriptografskom sistemu ključevi potrebni za enkripciju i dekripciju smešteni u depou pojavljuje se kao bezbednosni problem i potencijalno preuzimanje ključeva od strane treće strane od poverenja (Key escrow). Za određene aplikacije skladištenje ključeva na jednom mestu nije prihvatljivo iz bezbednosnih razloga.

U IB kriptosistemima prirodno je očekivati veliko opterećenje centara za generisanje ključeva. Ovaj nedostatak je posebno izražen ukoliko se ključevi često menjaju i ukoliko sistem ima veliki broj entiteta. U kranjem slučaju neophodno je uvesti veći broj KGC sa hijerarhijskom organizacijom. Svi ovi KGC bi obavljali istu funkciju, odnosno nebi bilo moguće iskoristiti ih za povećanje sigurnosti glavnog ključa ili za rešavanje problema deponovanja ključeva. Može se opet izvesti zaključak da je IB kriptosistem pogodniji za primene u malim sistemima.

IB kriptosistem pruža niz dodatnih mogućnosti kojima može da se poveća funkcionalnost sistema. Javni ključevi entiteta se mogu na jednostavan način povezati sa nizom drugih informacija kao na primer vremenom važenja ključa ili tajnim informacijama korisnika. Jedna od mogućnosti je i delegiranje dekripcionog ključa odnosno mogućnost da jedan od entiteta naloži drugim entitetima da mogu da primenjuju određeni ključ.

IV. Implementacija kriptosistema zasnovanog na identitetima

Koncept kriptografije zasnovane na identitetima predložio je Adi Shamir [1]. Njegova ideja je bila da se javno poznate informacije osoba koje komuniciraju kao što su e-mail adirese ili telefonski brojevi upotrebe za enkripciju i digitalni potpis umesto digitalnih sertifikata. Ovaj autor je uspešno razvio koncept digitalnog potpisa zasnovanog na identitetima (identity-based signature, IBS) primenjujući postojeći RSA algoritam ali nije uspeo da kreira enkripcionu šemu zasnovanu na identitetima (identity-based encryption, IBE). Implementacija enkripcione šeme zasnovane na digitalnim identitetima je više godina ostala otvoren problem sve dok ga nisu istovremeno rešila dva istraživačka tima Joux [7] i Boneh-Franklin [2] zahvaljujući primeni funkcija bilinearnog uparivanja. Sve postojeće implementacije kriptosistema zasnovanih na uparivanju uključujući i IB kriptosistem su realizovane primenom eliptičkih krivih.

Primenu eliptičkih krivih nad konačnim poljem u kriptografiji predložili su Kolbitz i Miller [8, 9]. Ova dva autora su nezavisno došla do zaključka da kriptosistemi zasnovani na problemu diskretnog logaritma pružaju bolju sigurnost kada se definišu na skupu tačaka eliptičke krive. Na ovaj način omogućeno je postizanje istog stepena sigurnosti sa znatno kraćim ključevima.

Eliptička kriva definisana nad poljem K predstavlja uređene parove $(x, y) \in K \times K$ koji zadovoljavaju algebarsku jednačinu eliptičke krive (Vajerštrasovu jednačinu).

$$y^2 = x^3 + ax + b \qquad (1)$$

Jedno od bitnih svojstava eliptičkih krivih je da se nad njima može jednostavno uvesti binarna operacija koja sa skupom tačaka eliptičke krive kreira Abelovu grupu. Ova operacija poznata kao metod tangente i tetive se definiše geometrijski pri čemu se za dve zadate tačke na krivoj određuje treća tačka a označava se simbolom +. Primenom analitičke geometrije dobijaju se algebarske jednačine koje definišu ovu operaciju.

Za primene u kriptografiji definiše se grupa koju čini skup tačaka na eliptičkoj krivi kao i operacija koja se obavljaju između elemenata grupe. Grupa se kreira uzastopnom primenom operacije sabiranja nad jednom tačkom i može se prikazati na sledećio način:

$$\langle P \rangle = \{P, P+P, P+P+P, ..., [n-1]P, 0\}$$

gde je: P generator grupe ili bazna tačka, n red tačke ili red generatora koji treba da bude prost broj, $[k]$P označava tačku dobijenu nakon k uzastopno obavljenih operacija nad baznom tačkom, O neutralni element koji predstavlja tačku u beskonačnosti. Neophodno je obezbediti da koordinate svake tačake koja pripada grupi budu elementi zadatog polja.

Za kreiranje konačnih polja eliptičkih krivih primenjuje se modularna aritmetika. Skup brojeva kongruentnih sa brojem a po modulu p (brojevi čija je razlika od a umnožak od p) naziva se klasa kongruencije i označava sa $[a]_p$. Za primene eliptičkih kriva u kriptografiji posebno je važan slučaj kada je odabrano konačno polje skup klasa kongruencije po modulu: $\mathbf{Z}/\, p\mathbf{Z} = \{[a]_p \mid a \in Z\}$.

Sigurnost asimetričnih kriptosistema koji primenjuju eliptičke krive zasniva se na problemu diskretnog logaritma u zadatoj grupi. Za zadate dve tačke na eliptičkoj krivoj P i Q potrebno je odrediti nenegativan broj t takav da bude ispunjeno $Q = [t]P$.

Uparivanje predstavlja funkciju čiji ulaz predstavljaju dve tačke na eliptičkoj krivoj a izlaz je element određene multiplikativne abelove grupe. Najvažnije svojstvo uparivanja je bilinearnost. Do sada su razvijena dva postupka uparivanja

Weil-ovo i Tate-ovo uparivanje.

Iako su Boneh i Franklin primenili Weil uparivanje na eliptičkim krivama da bi kreirali IB kriptosistem oni su naveli da se umesto ovog tipa uparivanja može primeniti Tate uparivanje. Za realizaciju Weil uparivanja potrebno je dvostruko više vremena procesiranja u odnosu na Tate uparivanje. Odavde proizilazi da se primenom Tate uparivanja umesto Weil uparivanja može značajno povećati efikasnost IB kriptosistema.

Sigurnosni protokoli koji primenjuju uparivanje zasnivaju se na bilinearnom Diffie-Hellman problemu koji se formanlo može izraziti na sledeći način: za zadate tačke na eliptičkoj krivoj (*P*, *aP*, *bP*, *cP*) odrediti da li je $ab = c$, gde su $a,b,c \in Z_n^*$ nepoznati celi brojevi.

Prvu praktičnu realizaciju IB kriptosistema predložili su Boneh i Franklin [2]. Oni su predložili dve enkripcione šeme sa oznakama *BasicIdent* i *Fullident*. Enkripciona šema *BasicIdent* sastoji se od četiri algoritama. Prvi algoritam odnosi se na podešavanje sistema u toku koga KGC definiše sistemske parametre i kreira glavni ključ. Sva sračunavanja obavljaju se nad dve grupe, G_1 i G_2 za koje važi bilinerno mapiranje $e: G_1 \times G_1 \to G_2$. Elementi obe grupe su tačke eliptičke krive nad poljem $\mathbf{Z} / p\mathbf{Z}$. Grupa G_1 se kreira primenom sledeće relacije

$$P: \{nP \,||\, n \cup \{0,\ldots,q-1\}\} \tag{2}$$

gde je: *P* slučajno odabrana tačka koja predstavlja generator grupe, *q* slučajno odabran prost broj koji predstavlja red grupe. U procesu incijalizacije slučajno odabran prost broj usvaja se za glavni tajni ključ $s \cup Z_q^*$. Glavni javni ključ određuje se primenom operacije skalarnog množenjem u eliptičkoj krivi kao $P_{pub} = sP$. Tokom postupka inicijalizacije potrebno je definisati dve javno dostupne heš funkcije čiji ulazni i izlazni nizovi mogu da se prikažu na sledeći način: $H_1: \{0,1\}^* \to G_1^*, H_2: G_2 \to \{0,1\}^n$. Pored toga u postupku inicijalizacije sistema definiše se i dužina otvorenih i šifrovanih poruka.

Postupak generisanja tajnog ključa entiteta određenog digitalnog identiteta $ID \cup \{0,1\}^*$ uz primenu glavnog tajnog ključa i sistemskih parametara nazvan je ekstrahovanje. Privatni ključ entiteta čiji je digitalni identitet ID definisan je sledećim izrazom:

$$d_{ID} = sH_1(ID) \tag{3}$$

Prilikom enkriptovanja i dekriptovanja primenjuje se funkcija uparivanje. Pored toga primenjuje se heš funkcija da bi se generisala maska koja se EXOR logičkom operacijom sabere sa izvornom porukom. Enkripcija je procedura kojom se od ulazne poruke i javnog ključa generiše šifrovana poruka. Entitet koji šalje poruku najpre primenom heš funkcije H_1 nad digitalnim identitetom *ID* formira sažetak $Q_{ID} = H_1(ID)$. Nakon toga se primenjuje funkcija uparivanja nad dobijenim nizom sažetka i javnim ključem $g_{ID} = e(Q_{ID}, K_{pub}) \cup G_2$. Da bi se kreirala šifrovana poruka potrebno je da entitet koji šalje poruku generiše slučajan prost broj $r \cup Z_q^*$. Na kraju se na osnovu sistemskih parametara, izvorne poruke *m* i rezultata funkcije uparivanja, g_{ID}, formira šifrovana poruka *c* na sledeći način:

$$c = (rP, m \oplus H_2(g_{ID}^r)) \cup G_2 \tag{4}$$

Dekriptovanjem se od šifrovane poruke $c = (u, v)$ uz primenu privatnog ključa entiteta d_{ID} i sistemskih parametara generiše otvorena poruka na sledeći način:

$$m = v \oplus H_2(e(d_{ID}, u)) \tag{5}$$

V. PRIMENA IB KRIPTOSISTEMA U SG

Napredna elektroenergetska mreža sadrži veliki broj uređaja različite prirode pri čemu se informacije prikupljaju sa brojnih senzora i mernih uređaja za koje često postoje energetska ograničenja. Imajući u vidu ova svojstva SG sistema proizilazi da bi primena IB kriptosistema za obezbeđivanje informacione bezbednosti SG mreže dala dobre rezultate.

Najveća količina informacija u SG mreži prenosi se u jednom smeru od senzora ka kontrolnim centrima. Imajući u vidu ovakvu arhitekturu naprednih elektro energetskih mreža pred kriptografskim algoritmima koji se primenjuju radi zaštite podataka postavlja se kao dodatan uslov smanjenje razmene podataka sa mernim uređajima koji predstavljaju pošiljaoce poruka. Primena IB kriptosistema u SG bi sa ovog aspekta dala veoma dobre rezultate jer se ne zahteva komunikacija između pošiljaoca poruke i servera za generisanje ključeva.

Jedna od dodatnih mogućnosti koju pruža IBC kriptosistem odnosi se na proceduru zamene ključeva. U ovom kriptosistemu za razliku od klasičnog svaki entitet može sam da inicira zamenu ključa zavisno od potrebe. Pojednostavljenje procedure zamene ključeva pruža mogućnost podešavanja bezbednosti u pojedinim delovima mreže. Ovo svojstvo predstavlja veliku prednost u odnosu na klasičan kriptosistem s obzirom na razlike koje postoje između mernih uređaja u pogledu učestalosti merenja i značaja merenih podataka.

Praktična implementacija IBC kritptografskog sistema postala je moguća tek nakon primene kriptografskih algoritama zasnovanih na algebarskim strukturama eliptičkih krivih u konačnom polju. U poređenju sa RSA kriptografskim algoritmom ovaj algoritam primenjuje znatno kompleksnije računske operacije ali za isti nivo tajnosti koristi ključeve znatno manje dužine. Manja dužina ključa znači manji broj neophodnih operacija, brže vreme enkripcije, manji broj tranzistora u hardverskoj implementaciji kao i manju potrošnju. Najveći broj postojećih hardverskih implementacija kriptosistema koji primenjuju eliptičke krive namenjen je

postizanju većih brzina uz upotrebu značajnijih resursa. Uprokos ovoj činjenici prirodno je očekivati da u neposrednoj budućnosti najznačajnije primene ovih algoritama budu u uređajima za koje postoje ograničenja u pogledu memorije i procesorske snage. Jedan od uslova koji treba da ispune procedure za enkripciju i dekripciju u naprednoj elektroenergetskoj mreži je veća efikasnost s obzirom na slabu procesorsku moć naprednih brojila, veliki broj drugih komponenata ograničenih resursa kao i veliki broj senzor sa baterijskim napajanjem. Proizilazi da bi upotreba algoritama sa eliptičkim krivama u SG bila dobro rešenje.

Simulacija primene IBC u SG sistemu data je u [10]. Autori ovog rada implementirali su softverski IB kriptografsku šemu primenom Tato-ovo uparivanja za enkripciju podataka i u sistemu za digitalno potpisivanje. Korišćena enkripciona šema obezbeđuje tajnosti i autentifikaciju entiteta u SG sistemu. Obavljeno je testiranje efikasnosti kriptografskog sistema za različite dužine ključeva. Dobijeni rezultati upućuju na zaključak da je postignut visok stepen efikasnosti i skalabilnosti uz zadovoljavajuću tajnost i autentifikaciju podataka. Razrada IB autentifkacionog protokola za primenu u AMI data je u radu [10].

VI. ZAKLJUČAK

Napredna elektroenergetska mreža sadrži veliki broj uređaja različite prirode pri čemu se informacije prikupljaju sa brojnih senzora i mernih uređaja za koje često postoje energetska ograničenja jer koriste baterijska napajanja. Imajući u vidu ova svojstva SG sistema proizilazi da bi primena IB kriptosistema za obezbeđivanje informacione zaštite SG mreže dala dobre rezultate. Osobine koje čine IB kriptosistem posebno atraktivnim za primenu u SG sistemu su upravljanje ključevima bez digitalnih sertifikata i infrastrukture javnog ključa kao i mogućnost razmene podataka bez prethodnog konfigurisanja softvera od strane korisnika (*Zero-configuration Sign-Cryption Scheme*).

Sigurnost SG u velikoj meri zavisi od primenjenih metoda za autentifikaciju, autorizaciju i privatnosti. Sve ove metode se oslanjaju na određeni sistem za upravljanje ključevima. Imajući u vidu veličinu i kompleksnost SG mreže proizilazi potreba da sistem za upravljanje ključevima bude skalabilan do izuzetno velikih razmera. Klasičan sistem za upravljanje ključevima koji se bazira na infrastrukturi javnog ključa ne nudi dovoljan nivo skalabilnosti. Izvesno je da će se javiti potreba za novim sistemom za upravljanje ključevima koji bi bio specijalizovan za ispunjenje zahteva napredne elektroenergetske mreže.

Rezultati softverske implementacije IBE kriptosistema u SG [10] pokazuju da bi primena ove kriptografske šeme u SG pružila visok stepen efikasnosti i skalabilnosti. Jedna od prednosti ove kriptografske šeme za primene u SG je mogućnost podešavanja nivoa bezbednosti a samim tim i troškova implementacije u pojedinim delovima sistema.

Enkripciona šema zasnovana na identitetu odlikuje se znatno jednostavnijim i efikasnijim sistemom za upravljanje ključevima u odnosu na klasičnu enkripcionu šemu. Sagledavajući svojstva ovog IB kriptografskog sistema može se zaključiti da je pored nedostataka koji ga odlikuju i i činjenice da nije zaživeo u praksi potrebno ozbiljno razmotriti njegovu primenu u SG mreži.

ZAHVALNICA

Rezultati prikazani u ovom radu ostvareni su u okviru projekta TR 32004 čiju realizaciju finansira Ministarstvo nauke Republike Srbije.

LITERATURA

[1] Adi Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science*, vol. 7, pp. 47--53, 1984.

[2] D. Boneh and M. K. Franklin "Identity-based encryption from the weil pairing," CRYPTO'01 Proceedings of the 21 st Annual International Cryptology Conference and Advances in Cryptology, London, England, pp. 213-229, 2001.

[3] M. M. Fouda, Z. M. Dadlulah, N. Kato, R. Lu, X. Shen, „Towards a light-weight message authentication mechanism tailored for smart grid communications," in Int. Workshop on Security in Computers, Networking and Communications. Shanghai, China: IEEE, pp. 1035-1040, April 2011.

[4] E. Ayday and S. Rajagopal, „Secure, intuitive and low-cost device authentication for smart grid networks," in IEEE *Consumer Communications Networking Conference*, Las Vegas, USA, pp. 1161-1165, January 2011.

[5] L. Chen, "Identity-based cryptography," International School on Foundations of Security Anayses and Design, 2006.

[6] S. Bojanić, S. Đorđević, O. Nieto-Taladriz, „Security Aspects of Advanced Metering Infrastructures," IX Symposium on Industrial Electronics INDEL 2012, Banja Luka, Bosnia and Herzegovina, pp. 205-208.

[7] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," Proc. of 8th IMA International Conference on Cryptography and Coding, LNCS 2260, Springer-Verlag (2001), pp. 360–363.

[8] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.

[9] V. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology - Crypto '85, LNCS 218, Springer-Verlag (1986), pp. 417–426, 1985.

[10] Chakib Bekara, Thomas Luckenbach, and Kheira Bekara. "A Privacy Preserving and Secure Authentication Protocol for the Advanced Metering Infrastructure with Non-Repudiation Service". Proceedings of 2012 International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, St. Maarten, The Netherlands, pp. 60-68, March 2012.

ABSTRACT

The security of the smart grid strongly depends on an authentication scheme which relays on some sort of key management. In this paper, we propose the use of an identity based cryptography scheme for the advanced metering infrastructure because of its very simple key management mechanism. We discus some problems associated with practical and theoretical aspects of identity based cryptography and examine under which conditions identity based cryptography may be used in smart grid.

The application of the identity-based encryption in the smart grid

Srđan Đorđević, Slobodan Bojanić