Pregled "lakih" blok-šifarskih algoritama zasnovanih na SPN mreži sa aspekta bezbednosti bežičnih senzorskih mreža

Petar Prvulović, Nemanja Radosavljević, Djordje Babić
Računarski fakultet
Univerzitet Union
Beograd, Srbija
pprvulovic@raf.rs, nradosavljevic@raf.rs, djbabic@raf.rs

Sažetak—**Bežične senzorske mreže omogućavaju komunikaciju između senzorskih čvorova. Primene su brojne: od nadgledanja saobraćaja i proizvodnih pogona, do praćenja rada automobila ili zdravstvenog stanja pacijenata. Njihov osnovni zadatak je prikupljanje i slanje očitanih vrednosti sa nadgledanog prostora do bazne stanice. Na osnovu prikupljenih podataka donose se odluke, te je u tehnologijama zasnovanim na bežičnim senzorskim mrežama potrebno posvetiti pažnju aspektu bezbednosti komunikacije između bežičnih senzorskih čvorova, kako bi prikupljeni podaci bili bezbedno preneti kroz mrežu do bazne stanice. Senzorski čvorovi imaju problem ograničenog energetskog kapaciteta čvorova. Kriptoalgoritme je potrebno izabrati tako da se potreban nivo zaštite postigne minimalnim mogućim utroškom energije na kriptovanje komunikacije. Za ove potrebe prepoznata je kategorija "lakih" kriptoalgoritama. U ovom radu poredimo blok-šifarske algoritme koji zbog male hardverske i energetske zahtevnosti svoju primenu posebno nalaze u bežičnim senzorskim mrežama. Glavni fokus ovog rada je pregled blok-šifarskih algoritama koji su zasnovani na supstitucijalno-permutacionoj mreži.**

Ključne riječi-bežične senzorske mreže; blok-šifarski algoritmi; supstituciono-permutaciona mreža (SPN); bezbednost; energetska efikasnost

I. UVOD - PROBLEM BEZBEDNOSTI U BEŽIČNIM SENZORSKIM MREŽAMA

Senzorski čvorovi u bežičnim senzorskim mrežama (BSM, eng. WSN) imaju ograničeno napajanje, memorijske i procesne kapacitete i protočnost. Izvor napajanja često su baterije, a uobičajeno je i da senzorski čvorovi nisu dostupni nakon postavljanja BSM, tako da je njihov životni vek direktno određen trajanjem izvora napajanja. Ove karakteristike ograničavaju performanse čvorova, a time i izbor protokola i algoritama koji se mogu primeniti u BSM. BSM su zasnovane na jednostavnim protokolima za upravljanje topologijom koji nisu dovoljni da obezbede bezbednost komunikacije. Kao i kod drugih vidova bežične komunikacije na otvorenom i senzorske mreže su podložne praćenju i ometanju komunikacije. [1] Mobilnost čvorova uvodi dodatni prostor za napade. [2] Otud je bezbednost jedan od osnovnih problema u primeni bežičnih senzorskih mreža [3] koji, imajući u vidu ograničene performanse čvorova, treba posmatrati sa više aspekata.

Za neometano funkcionisanje BSM potrebno je zadovoljiti kriterijume bezbednosti komunikacije i preživljavanja mreže u slučaju (očekivanih) otkaza. Bezbednost komunikacije obuhvata zahteve kao što su: poverljivost komunikacije između senzorskih čvorova, integritet podataka tokom prenosa kroz mrežu, autentifikacija legitimnih čvorova kako bi se sprečilo uključivanje zlonamernih učesnika u mrežu i zaštita bazne stanice [4]. Preživljavanje mreže zahteva obezbeđivanje mehanizama koji će omogućiti nesmetan rad mreže u slučaju otkaza određenog broja čvorova, dostupnost podataka u čvorovima u bilo kom trenutku i održavanje rada mreže u toku očekivanog vremenskog roka efikasnom upotrebom energije baterijskog napajanja čvorova. [4]

Ovako postavljeni kriterijumi zahtevaju primenu šifarskih algoritama koji nisu računski zahtevni. U skladu sa tim prepoznajemo klasu tzv. "lakih" šifarskih algoritama. Broj logičkih kola potrebnih za implementaciju algoritma u vezi je sa kompleksnošću algoritma i može se izraziti kroz gate-equivalent (GE). GE je jedinica mere kompleksnosti digitalnih elektronskih kola koja ne zavisi od tehnologije proizvodnje i izražava koliko bi pojedinačnih logičkih kola bilo potrebno povezati da bi se dobila funkcionalnost merenog digitalnog sklopa. U literaturi se kao prihvatljive granice, zavisno od vrste uređaja, navodi 250-4000 GE za potrebe bezbednosti [5].

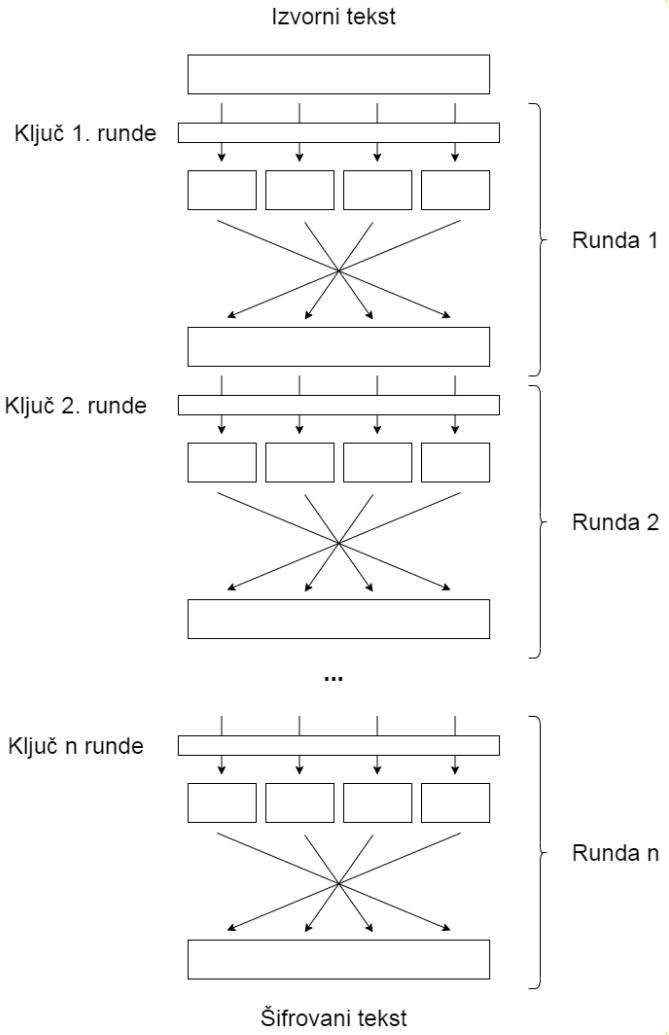
U radu je predstavljen pregled izabranih blok-šifarskih algoritama zasnovanih na SPN mreži koji se primenjuju u BSM. Algoritmi su predstavljeni sa aspekata protočnosti, kompleksnosti implementacije na hardveru i energetskim potrebama šifrovanja. Glavni doprinos rada ogleda se u definisanju i rangiranju karakteristika algoritama koje su bitan faktor u odlučivanju i izboru algoritma za primenu. Predstavljena analiza algoritama daje preporuke po adekvanosti primene u BSM, sa stanovišta postavljenih uslova bezbednosti i energetske efikasnosti.

II. "LAKI" ŠIFARSKI ALGORITMI

Pojam "laki šifarski algoritam" određuje klasu algoritama za šifrovanje koji su pogodni za upotrebu na platformama sa ograničenim resursima. Klasična kriptografija fokusira se na pružanje visokog nivoa bezbednosti. "Laka" kriptografija mora uzeti u obzir i pomenuta ograničenja, što može uticati na dizajn i implementaciju. Sveobuhvatan pregled ove teme načinili su

Hadživasilis i ostali [5]. Kod primene u BSM od interesa su nam moderni šifarski algoritmi. U ovom radu fokusirani smo na blok-šifarske algoritme: AES, PRESENT, NOEKEON, LED i PRINCE. Nabrojane algoritme ćemo predstaviti u kratkoj formi i izdvojiti one parametre koji su nam od značaja za dalje poređenje u prethodno definisanom kontekstu primene u BSM.

Postoji nekoliko tipova unutrašnje strukture blok-šifarskih algoritama. U radu razmatramo algoritme koji koriste supstitucijalno-permutacione mreže (eng. Substitution Permutation network). Supstitucijalno-permutacione mreže (SPN) ulaz dele na veći broj malih blokova nad kojima se prvo primenjuje supstitucija, kroz S-box elemente - matrice koje definišu supstituciju, a zatim se pozicije bajtova mešaju u koraku permutacije. Dodavanje ključa vrši se pre ili nakon ovih operacija, u svakoj rundi. Blok-šifarski algoritmi poruku šifruju u blokovima fiksne dužine. Ključ može biti iste dužine kao blok ili duži. Tipično se u svakoj rundi koristi drugačija vrednost - ključ runde, koji se izvodi iz ključa. Proces šifrovanja prikazan je na slici 1.



Slika 1. Proces šifrovanja algoritama zasnovanog na SPN

A. *AES*

AES poruku deli na blokove od 128 bitova - 16 bajtova i šifruje je ključem dužine 128,192 ili 256 bitova u 10, 12 odnosno 14 rundi respektivno. U svakoj rundi koristi se ključ runde dužine 128 bitova koji se generiše iz originalnog ključa. Svaka runda sastoji se od 4 koraka. U prvom koraku blok se deli na 16-bajtne delove koji se predstavljaju kao matrice 4x4 i nad njima vrši supstitucija na osnovu predefinisanih S-box matrica iste dimenzije. U drugom koraku se redovi dobijene matrice rotiraju ulevo za predefinisani broj bajtova. U trećem koraku vrši se mešanje po kolonama množenjem kolona polinomom. Poslednji korak koristi ključ runde od 128 bitova, generisan operacijom ekspanzije ključa, koji se xor operacijom primenjuje na matricu, tako što se matrica posmatra kao niz bajtova.

Postoji više implementacija ovog algoritma. U [6] je navedena hardverska implementacija koja zahteva 2400GE, čija protočnost obrade normirana na radnom taktu od 100MHz iznosi 57Kbps.

B. *PRESENT*

PRESENT [7] šifruje poruku u blokovima od 64 bita kroz 31 rundu i koristi ključ dužine 80 ili 128 bitova. Ovaj algoritam je dizajniran za potrebe uređaja ograničenih performansi. Umesto osam koristi jednu S-box a u harverskoj implementaciji difuzioni sloj se izvodi ožičavanjem, bez upotrebe algebarskih jedinica, što omogućava izuzetno nisku potrošnju energije. Kod 80-bitnog ključa moguće je postići 1030GE [5]. Iako pokazuje bitno bolje performanse od AES, u smislu protočnosti i potrošnje energije, manje je otporan na napade, što se može otkloniti po cenu povećanja kompleksnosti implementacije.

C. *NOEKEON*

NOEKEON [8] koristi 128-bitni ključ i poruku šifruje u blokovima iste te dužine. Šifrovanje se vrši u 16 jednakih rundi, u kojima se vrše sledeće operacije: dodavanje konstante runde, teta transfomacija - difuzija i dodavanje radnog ključa, Pi1 permutacija, gama transformacija - primena nelinearne operacije i Pi2 permutacija. Pi1 i Pi2 permutacije izvode se rotacijom ulevo/udesno za definisani broj bitova. Runde su potpuno iste i razlikuju se jedino u vrednosti radnog ključa. Umesto ključa runde koristi se radni ključ koji se dobija primenom XOR operacije na tekući rezultat u postupku šifrovanja. Radi dodatne uštede moguće je umesto radnog ključa koristiti ključ, čime se postiže ušteda u memorijskom prostoru ali algoritam čini podložnim pojedinim napadima. Proces dešifrovanja može se vršiti upotrebom kola za šifrovanje što u situacijama kada čvor treba da radi obe operacije stvara bitnu uštedu u veličini kola.

D. *LED*

LED - Lightweight Encryption Device [9] je dizajniran sa fokusom na primenu u uređajima ograničenih kapaciteta. Poruku šifruje u 64-bitnim blokovima primenom ključa dužine 64, 80, 96 ili 128 bitova, u 32 i 48 rundi, čime se može uticati na kompleksnost implementacije. Kod implementacija manje kompleksnosti otvara se prostor za napade na ključ i dr.

Ključevi rundi se, slično kao kod NOEKEON, ne izvode iz ključa a S-box je sličan kao u PRESENT.

E. PRINCE

PRINCE [10] je dizajniran za implementaciju na hardveru. Simetričan je pa se dekripcija vrši na isti način kao enkripcija, sa ključem koji se lako izračunava. Koristi 128-bitni ključ i 64-bitne blokove koje šifruje kroz 11 rundi: 5 "unapred", jedna, srednja, koja uvodi linearnost kroz dva sloja, i 5 "unazad". Nelinearni sloj sadrži jedan 4-bitni S-box. Linearni sloj se sastoji od množenja 64x64 matricom i rotacijom reda slično kao kod AES, ali se primenjuje na 4-bitnim niblovima, umesto nad bajtovima. Mali broj rundi i "plitka" logika rundi su strategija postizanja dobrih performansi, što se može videti iz uporednih podataka u nastavku.

III. METODOLOŠKI OKVIR POREĐENJA ALGORITAMA

Polazni osnov za analizu "lakih" blok-šifarskih algoritama je njihova upotreba u BSM i sistemima zasnovanim na "internetu stvari" (IoT). U zavisnosti od polja primene BSM sa aspekta bezbednosti analiziraju se različite karakteristike šifarskih algoritama. Karakteristike koje posmatramo u ovom radu su: protočnost algoritma, hardverska kompleksnost implementacije algoritma i utrošak energije tokom šifrovanja. Svaki od ovih kriterijuma je ograničavajući faktor u zavisnosti od polja primene senzorskih čvorova koji čine BSM.

Protočnost algoritma određujemo kao količinu podataka koja se može šifrovati u jedinici vremena. Ovaj kriterijum je od ključne važnosti kod sistema u kojima čvorovi generišu dosta saobraćaja, u smislu velikog broja poruka i velike dužine poruka. Protočnost je predstavljena normirano na radnom taktu od 100KHz.

Kompleksnost hardverske implementacije je ograničavajući faktor kod BSM koje koriste male čvorove, gde je ograničenje uzrokovano dimenzijama čvora. Kod BSM koje koriste veliki broj čvorova male uštede u hardverskoj implementaciji mogu proizvesti bitnu razliku u konačnoj ceni proizvodnje.

Potrošnja energije je od kritičnog značaja kod senzorskih čvorova sa baterijskim napajanjem. Kod BSM gde, zbog nepristupačnosti čvorova, zamena baterije nije moguća, trajanje baterije određuje životni vek čvorova i BSM. Otkaz određenog broja čvorova može dovesti do prekida komunikacije sa delom mreže ili proizvesti dodatno opterećenje preostalim čvorovima takvo da dovede do otkaza cele mreže. Potrošnju energije posmatramo u μJ po bitu šifrovanog sadržaja.

Svaki od navedenih kriterijuma posmatramo kroz hardversku implementaciju tehnologijom izrade od 0.13μm sa najdužim od podržanih dužina ključeva, a tamo gde je primenjivo navodimo i rezultate na 0.18μm i sa kraćim ključevima.

Primena BSM određuje koji od ova tri parametra su od kritičnog značaja. U skladu sa tim donosi se odluka koji od navedenih algoritama je najpogodniji za dati slučaj primene.

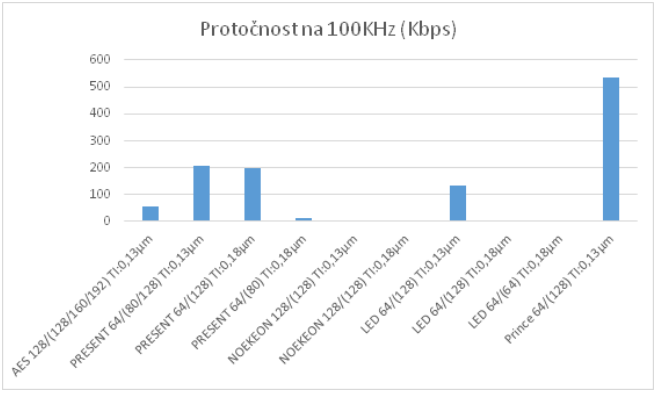
IV. UPOREDNI PREGLED IZABRANIH ALGORITAMA

U tabeli 1 prikazan je uporedni pregled hardverskih implementacija opisanih algoritama: njihovu protočnost normiranu na radnom taktu od 100MHz, GE koji se može postići na hardverskim implementacijama i procenjeni utrošak energije u μJ po šifrovanom bitu. Navedene vrednosti su prikazane za implementaciju tehnologijom od 0.13μm, a za one koji postoje i na 0.18μm.

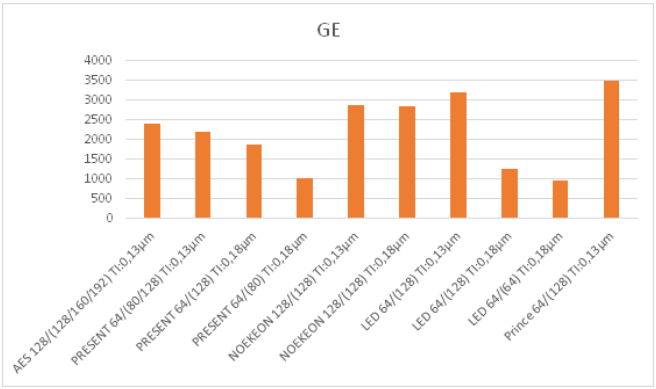
U opštem slučaju navedeni algoritmi zadovoljavaju kriterijume kompleksnosti implementacije merene po GE. Radi boljeg sagledavanja vrednosti datih u tabeli, na slici 2 grafički je prikazana protočnost algoritama na 100KHz, gde se jasno vidi da Prince značajno odstupa od ostalih algoritama, što nam govori da mali broj rundi, "plitke" runde i potpuno razvijena forma (po cenu veće kompleksnosti implementacije) zaista imaju efekta. Na slici 3 prikazan je grafik koji predstavlja broj logičkih kola potrebnih za implementaciju algoritma, na kome vidimo da algoritmi sa kraćim ključem i blokovima šifrovanja imaju nešto kompaktniju implementaciju. Slika 4 predstavlja grafički prikaz potrošnje energije neophodne za šifrovanje jednog bita otvorenih podataka, merene u μJ, gde vidimo da se po ovom kriterijumu kao lošiji kandidati izdvajaju implementacije na 18μm tehnologiji izrade.

TABELA I. UPOREDNI PRIKAZ HARDVERSKIH IMPLEMENTACIJA "LAKIH" BLOK-ŠIFARSKIH ALGORITAMA

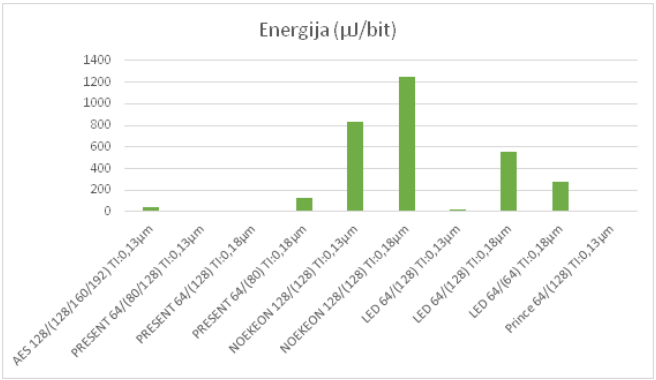
Algoritam	Dužina bloka (b)	Dužina ključa (b)	Tehnologija izrade (μm)	Protočnost na 100KHz (kbps)	GE	Energija (μJ/bit)
AES	128	128/160/192	0,13	57	2400	42,38
PRESENT	64	80/128	0,13	206	2195	10,63
PRESENT	64	128	0,18	200	1886	14,14
PRESENT	64	80	0,18	12,4	1030	124,56
NOEKEON	128	128	0,13	3,44	2880	837,90
NOEKEON	128	128	0,18	3,44	2862	1247,65
LED	64	128	0,13	133,33	3194	23,95
LED	64	128	0,18	3,4	1265	555,02
LED	64	64	0,18	5,1	966	282,55
PRINCE	64	128	0,13	533,3	3491	6,54



Slika 2. Uporedni prikaz protočnosti algoritama na 100KHz



Slika 3. Uporedni prikaz kompleksnosti implementacije algoritama



Slika 4. Uporedni prikaz algoritama sa aspekta energetske efikasnosti

Ograničavajući faktori koji mogu odstraniti neke algoritme iz razmatranja mogu biti razni, zavisno od situacije i primene. Kod radiofrekventne identifikacije (RFID – radio frequency identification) ograničavajući faktor je prostor/kompleksnost implementacije, dok utrošak energije nije od primarnog značaja jer se koristi eksterno napajanje prilikom očitavanja čipa. Kod primene u nadgledanju otvorenih područja čvorovi komuniciraju dužim porukama i dozvoljavaju fizički veću implementaciju, ali koriste baterijsko napajanje i utrošak energije predstavlja bitan kriterijum.

V. ZAKLJUČAK

U radu je predstavljen uporedni pregled izabranih blok-šifarskih algoritama iz kategorije "lakih" algoritama, koji zadovoljavaju uslove bezbednosti i energetske efikasnosti u BSM. Opisan je princip funkcionisanja svakog od izabranih algoritama kako bi se sagledale njihove zajedničke osobine i izdvojile razlike koje mogu biti faktor u odlučivanju. Algoritmi su uporedo predstavljeni po merama protočnosti algoritma na normiranih 100MHz takta, kompleksnosti implementacije izraženoj kroz GE i potrošnjom energergije tokom šifrovanja. Iz predstavljenih podataka vidi se da pomenuti algoritmi mogu da zadovolje potrebe bezbednosti i preživljavanja BSM u opštem slučaju. Kod BSM sa većim ograničenjima resursa čvorova neke od algoritama nije moguće primeniti i izbor se svodi na one algoritme koji mogu da se izvedu na tako ograničenom hardveru, iako su manje energetski efikasni. Doprinos rada se ogleda u analizi osobina algoritama u široj slici implementacije, kao što je očekivana dužina poruka i učestalost komunikacije i otvaranju prostoroa za dalju analizu manje očiglednih detalja implementacije, kao što je način na koji komunikacioni protokoli tretiraju pauze u komunikaciji koje mogu nastati latencijom u algoritmu šifrovanja. Ovakvi detalji indirektno mogu proizvesti potrošnju energije koja kumulativno može imati merljiv uticaj na dužinu životnog veka čvorova i BSM. Dalji tok istraživanja autori će usmeriti ka otkrivanju ove vrste "skrivenih troškova" šifrovanja komunikacije u BSM.

ZAHVALNICA

Ovaj rad podržalo je Ministarstvo prosvete, nauke, i tehnološkog razvoja Republike Srbije, u okviru projekta tehnološkog razvoja TR32023 – „Optimizacija performansi energetski efikasnih računarskih i komunikacionih sistema

LITERATURA

[1] N. Radosavljević, Đ. Babić, "Overview of security threats, prevention and protection mechanisms in wireless sensor networks", Journal of Mechatronics, Automation and Identification Technology, Vol. 5, No. 2, pp. 1 – 6, 2020.

[2] N. Radosavljević, Đ. Babić, "Pregled sigurnosnih pretnji i mehanizama prevencije i zaštite u bežičnim senzorskim mrežama s primenom u preciznoj poljoprivredi", 20th International Symposium INFOTEH-JAHORINA, 2020.

[3] E. Shi, & A. Perrig, "Designing secure sensor networks", Wireless Communications Magazine, 11(6), 38–43., 2004.

[4] B. Bhushan, G. Sahoo, "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks", Wireless Pers Commun DOI 10.1007/s11277-017-4962-0, Springer Science+Business Media, LLC, 2017.

[5] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, C. Manifavas, "A Review of Lightweight Block Ciphers", Journal of Cryptographic Engineering, DOI: 10.1007/s13389-017-0160-y, 2017.

[6] A. Moradi, A. Poschmann, S. Ling, C. Paar, H. Wang, "Pushing the limits: a very compact and a threshold implementation of AES", Advances in Cryptology EUROCRYPT 2011, Springer, LNCS, 6632, pp. 69–88, 2011.

[7] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, "PRESENT: An Ultra-

Lightweight Block Cipher", Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems – CHES, 2007.

[8] J. Daemen, M. Peeters, G. Van Assche, V. Rijmen, "Nessie Proposal: NOEKEON", First Open NESSIE Workshop, 2000.

[9] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw, "The LED Block Cipher, Cryptographic Hardware and Embedded Systems", CHES 2011, Springer, LNCS, 6917, 2011, pp.326341, 2011.

[10] J. Borghoff et al., "PRINCE A Low-latency Block Cipher for Pervasive Computing Applications", Advances in Cryptology ASIACRYPT 2012, Springer, LNCS, 7658, pp. 208–225, 2012.

ABSTRACT

Wireless sensor networks allow communication between sensor nodes. The applications are numerous: from monitoring traffic and production facilities, to monitoring the work of cars or the health condition of patients. Their main task is to collect and send the read values from the monitored area to the base station. Decisions are made based on the collected data, and in technologies based on wireless sensor networks, it is necessary to pay attention to the aspect of communication security between wireless sensor nodes, so that the collected data can be safely transferred through the network to the base station. Sensor nodes have a problem of limited energy capacity of nodes. Cryptoalgorithms should be chosen so that the required level of protection is achieved with the minimum possible energy consumption for communication encryption. For these purposes, the category of "light" cryptoalgorithms has been recognized. In this paper, we compare block cipher algorithms which, due to their low hardware and energy requirements, find their application especially in wireless sensor networks. The main focus of this paper is an overview of block cipher algorithms based on a substitution-permutation network.

An overview of "light" block cipher algorithms based on SPN network from the aspect of security of wireless sensor networks

Petar Prvulović, Nemanja Radosavljević, Djordje Babić