MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA
ISSN 2029-2341 / eISSN 2029-2252
http://www.mla.vgtu.lt

ELEKTRONIKA IR ELEKTROTECHNIKA
ELECTRONICS AND ELECTRICAL ENGINEERING

2016 8(3): 321–326

http://dx.doi.org/10.3846/mla.2016.927

KRIPTOGRAFINIŲ MAIŠOS FUNKCIJŲ ĮGYVENDINIMO PROGRAMUOJAMOSIOS LOGIKOS LUSTUOSE TYRIMAS

Tautvydas BRUKŠTUS

Vilniaus Gedimino technikos universitetas, Vilnius, Lietuva
El. paštas: tautvydas.brukstus@stud.vgtu.lt

Santrauka. Vis daugiau dėmesio skiriama duomenų apsaugai – duomenų apsaugai skirta net atskira kriptografijos mokslo šaka. Taip pat yra svarbi slaptažodžių sauga, kurioje naudojamos kriptografinės maišos funkcijos. Darbe parinkta įgyvendinimui ir ištirta šiuo metu populiari bei saugi SHA-2 kriptografinė maišos funkcija. Ji naudojama kriptografinėse valiutose. SHA-2 kriptografinės funkcijos analizės metu nepavyko rasti teorinių spragų ar kolizijos atvejų. Tyrimams pasirinkti *Altera* programuojamos logikos integriniai grandynai, kurie efektyvumu nusileidžia tik specializuotiems integriniams grandynams. Skaičiavimo sparta ir stabilumas buvo tiriama trijuose programuojamos logikos integrinuose grandynuose, priklausančiuose tai pačiai šeimai ir pagamintais skirtingų kartų technologijomis – naudojant 65 nm, 60 nm ir 28 nm KMOP technologijas. Tirtų grandynų kodiniai žymenys EP3C16, EP4CE115 ir 5CSEMA5F31.

Reikšminiai žodžiai: kriptografinė maišos funkcija, kriptografinės maišos funkcijos santrauka, programuojamos logikos integrinis grandynas.

Įvadas

Pasaulyje vis daugiau paslaugų perkeliama į elektroninę erdvę. Sparčiai vystosi internetinė bankininkystė, elektroninė prekyba, kriptografinės valiutos ir e-valdžios paslaugos. Naudojantis internetu vis daugiau kasdienių darbų galima atlikti neišėjus iš namų, tačiau reikia užtikrinti vartotojo autentifikavimą. Šiai problemai spręsti naudojamas elektroninis parašas arba sudėtingi slaptažodžiai. Jeigu jungiantis prie paslaugų tinklalapių naudojamas elektroninis parašas, nereikia naudoti sudėtingų slaptažodžių. Daugumoje atvejų dėl plataus slaptažodžių paplitimo jų atsisakyti negalima. Slaptažodžiams saugoti naudojamos maišos funkcijos.

Maiša – tai matematinė transformacija, vykdoma paverčiant tam tikro dydžio duomenų masyvą fiksuoto dydžio, dažniausiai mažesnio, duomenų masyvu (Tilborg 2011). Gautas rezultatas vadinamas maišos funkcijos santrauka. Tai panašu į piršto antspaudą realiame gyvenime, nes kiekvienam duomenų masyvui gaunama unikali santrauka. Taigi maišos funkcijos santrauką galima naudoti kaip autentiškumo patikrinimo priemonę, nes, pasikeitus duomenims duomenų masyve, maišos funkcijos santrauka pasikeis ir nebus tokia pati kaip originalių duomenų (Kavaliūnas 2008).

Maišos funkcijos taip pat naudojamos elektroniniame paraše. Čia maišos funkcija sukuria santrauką, kuri atitinka parašą. Viso failo ar duomenų masyvo pasirašymas gali trukti ilgai, dėl šios priežasties ir buvo pradėta naudoti maišos funkcija (Stakėnas 2006).

SHA-2 kriptografinė maišos funkcija plačiai naudojama slaptažodžiams saugoti, pranešimo autentifikavimo kodo sistemoje, elektroninio parašo sistemoje, kriptografinėse valiutose ir t. t. (Gauravaram 2012). IBM korporacija kuria sistemą, kuri panaudoja kriptografinės valiutos privalumus ir pašalina jos trūkumus. Kriptografinių valiutų trūkumas – naudojami virtualūs pinigai. Taigi, IBM korporacijos kuriama sistema naudos realius pinigus, o operacijos su jais bus vykdomos kaip su kriptografinės valiutos pinigais (Panaer, Werhoven 2007).

Darbe tiriamas SHA-2 kriptografinės maišos funkcijos algoritmas, nes juo grindžiama plačiausiai naudojama kriptografinė maišos funkcija. Algoritmas programuojamos logikos integriniame grandyne įgyvendinamas naudojant VHDL programavimo kalbą. SHA-2 algoritmui įgyvendinti pasirinkta VHDL programavimo kalba leidžia suprojektuoti sistemą, kuri vykdys lygiagrečiuosius skaičiavimus.

Tyrimų tikslas – ištirti SHA-2 kriptografinės maišos funkcijos skaičiavimo spartą programuojamos logikos integriniuose grandynuose. Eksperimentams naudoti trys programuojamos logikos integriniai grandynai. Pagal tyrimo rezultatus turi būti projektuojami specializuoti integriniai grandynai.

Tyrimo metodika

Tyrime panaudoti trys programuojamos logikos integriniai grandynai. Visuose programuojamos logikos grandynuose suprojektuota ta pati sistema. Tyrimo rezultatų palyginimas leidžia įvertinti programuojamos logikos integrinio grandyno įtaką skaičiavimo spartai.

Kiekviename programuojamos logikos integriniame grandyne atlikti tokie trys eksperimentai:

- naudojant vienos gijos sistemas su skirtingais taktiniais dažniais;
- naudojant vienos gijos sistemą, kurios taktinis dažnis yra maksimalus;
- naudojant maksimalų gijų skaičių ir maksimalų taktinį dažnį.

Dažniui keisti panaudota faze užrakinama kilpa. Atraminis faze užrakinamos kilpos dažnis yra 50 MHz. Matavimų metu keičiamas dažnis nuo 50 MHz taktinio dažnio iki maksimalaus dažnio, kurį pasieks programuojamos logikos integrinis grandynas.

Nustačius maksimalų taktinį dažnį, toliau eksperimentuojama esant šiam dažniui. Antrame eksperimente patikrinamas sistemos stabilumas dirbant maksimaliu taktiniu dažniu. Apdorojant eksperimento rezultatus, apskaičiuojama vidutinio nuokrypio vertė kiekvienam programuojamos logikos integriniam grandynui.

Trečias eksperimentas skirtas nustatyti, kokią maksimalią skaičiavimo spartą galima pasiekti kiekviename programuojamos logikos integriniame grandyne, esant maksimaliam dažniui, ir SHA-256 IP blokų skaičių. Taip pat patikrinama, ar suprojektuota architektūra veikloje panaudoja didžiąją loginių elementų dalį.

Eksperimentavimui buvo sukurta programa, kuri valdo programuojamos logikos integrinį grandyną. Programa valdo skaičiavimus ir matuoja skaičiavimų trukmę. Eksperimentų pabaigoje programa apskaičiuoja skaičiavimo spartą ir rezultatus pavaizduoja grafinėje vartotojo sąsajoje. Sparta pateikiama milijonais kriptografinės maišos funkcijos santraukų per sekundę (Mhash/s).

Mažinant matavimų paklaidą, kiekvieno matavimo metu, skaičiavimas kartojamas 80 000 000 kartų. Taip pat kiekvienas matavimas kartojamas 10 kartų ir apskaičiuojamas visų matavimų aritmetinis vidurkis. Taigi kiekviename matavime skaičiavimai vykdomi 800 000 000 kartų. Gauti vidurkiai yra eksperimento rezultatas.

Aritmetinis vidurkis apskaičiuojamas taip:

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \,, \qquad (1)$$

čia – i-tojo matavimo rezultatas; n – matavimų skaičius, esant vienodoms sąlygoms.

Eksperimentuose naudotų programuojamos logikos integrinių grandynų parametrai

Tyrime panaudotų trijų programuojamos logikos integriniai grandynų pagrindiniai parametrai pateikti 1 lentelėje. Panaudoti programuojamos logikos integriniai grandynai yra vieno gamintojo – *Altera*.

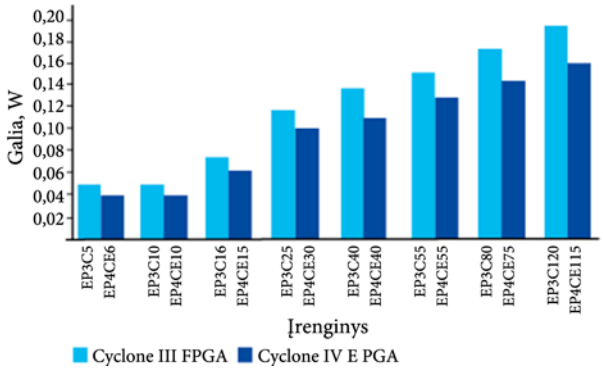
1 lentelė. Pagrindiniai naudojamų programuojamos logikos integrinių grandynų parametrai
Table 1. Main used programmable logic integrated circuit parameters

	Cyclone III	*Cyclone IV*	*Cyclone V*
Gamybos pradžios metai	2007	2009	2011
Modelis	EP3C16	EP4CE115	5CSEMA5F31
Loginių elementų skaičius	15408	114480	85000
Gamybos technologija	65 nm	60 nm	28 nm
Greičio kategorija	6	7	6
Statinė suvartojama galia	70 mW	150 mW	90 mW

1 lentelėje grandyno greičio kategorija apibūdinama indeksu: kuo indekso skaičiaus vertė yra mažesnė, tuo grandyno greičio kategorija yra aukštesnė. *Cyclone III*, greičiausi integriniai grandynai, turi indeksą 6, *Cyclone IV* yra mažesnio greičio kategorijos. *Cyclone III* ir *Cyclone V* programuojamos logikos grandynai yra maksimaliai greiti. Taip pat 1 lentelėje pateikta statinė suvartojama galia, tai yra, minimali galia, kai grandynas nevykdo jokių užduočių. Minimaliam energijos suvartojimui įtakos turi loginių elementų skaičius ir gamybos technologija, dėl šių priežasčių *Cyclone IV* energijos suvartojimas yra didžiausias. Tačiau *Cyclone IV* gali turėti daugiausia SHA-256 IP blokų.

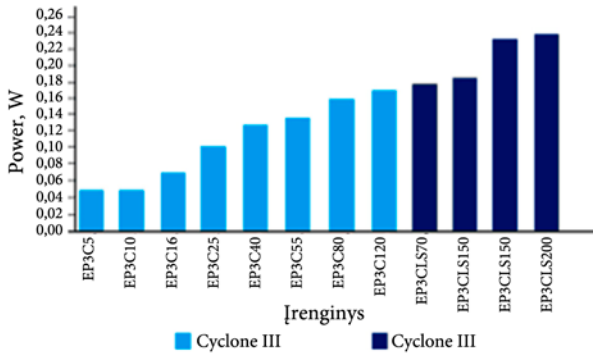
1 pav. pateiktas visų *Cyclone III* šeimos narių statinės suvartojimo galios grafikas. Suvartojamos galios lygis priklauso nuo programuojamos logikos grandyno turimų loginių elementų skaičiaus. Eksperimentuose naudotas EP3C16 programuojamos logikos grandynas turi 15 408 loginius elementus. Tai vienas mažiausių šios šeimos programuojamų loginių grandynų. Jo statinė suvartojama galia lygi 70 mW (Altera Corporation 2015a).

2 pav. pateiktas *Cyclone III* ir *Cyclone IV* šeimų statinės suvartojimo galios grafikas. *Cyclone IV* energijos suvartojimas 25% mažesnis lyginant su *Cyclone III*. Energijos suvartojimas sumažintas panaudojant mažesnių matmenų gamybos technologiją. *Cyclone IV* gamybai panaudota 60 nm technologija.



1 pav. *Cyclone III* statinės suvartojimo galios grafikas (Altera Corporation 2015a)

Fig. 1. *Cyclone III* static power consumption graph (Altera Corporation 2015a)

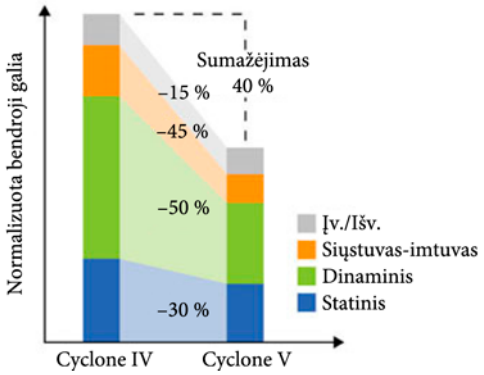


2 pav. *Cyclone III* ir *Cyclone IV* statinės suvartojimo galios grafikas (Altera Corporation 2015b, c)

Fig. 2. *Cyclone III and Cyclone IV* static power consumption graph (Altera Corporation 2015b, c)

Eksperimentuose naudotas EP4CE115 programuojamos logikos grandynas daugiausiai suvartoja statinės energijos, bet turi daugiau loginių elementų. Didelis kiekis loginių elementų leidžia sintezuoti daugiau SHA-256 IP blokų. Naudotame EP3C16 galima susintezuoti tik 11 IP blokų, o EP4CE115 – 80 IP blokų. Taigi skaičiavimų spartą galime padidinti 8 kartus (Altera Corporation 2015a, b, c).

3 pav. pateiktas grafikas, kuriame matome, kiek procentų sumažėjo energijos suvartojimas *Cyclone V* lyginant su *Cyclone IV*. Statinis energijos suvartojimas sumažėjo 30 %, o dinaminis suvartojimas sumažėjo net iki 50 %. Bendras energijos suvartojimas sumažėjo 40 %. Taigi *Cyclone V* yra efektyviausias iš naudotų programuojamos logikos grandynų. Energijos sumažinimui įtakos turi pasirinkta 28 nm gamybos technologija ir pakeista loginių elementų architektūra (Altera Corporation 2015b).



3 pav. *Cyclone IV* ir *Cyclone V* energijos suvartojimo palyginimo grafikas (Altera Corporation 2015b, c)

Fig. 3. *Cyclone IV* and *Cyclone V* static power consumption graph (Altera Corporation 2015b, c)

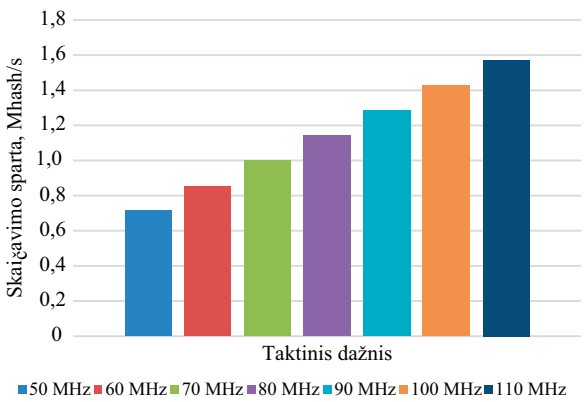
Tyrimo rezultatai

Pirmojo eksperimento metu matuotas maksimalus taktinis dažnis. Matavimų rezultatai pateikti 4–6 pav.

Iš 4 pav. matyti, kad maksimalus taktinis dažnis yra 110 MHz. Maksimali skaičiavimo sparta yra 1,571555 milijonų santraukų per sekundę. Atlikus 10 matavimų, esant maksimaliam taktiniam dažniui, apskaičiuotasis vidutinis nuokrypis lygus 0,000197043.

Apskaičiavus vidutinį nuokrypį visoms trims tirtoms sistemoms ir juos tarpusavyje palyginus, atsiranda galimybė nustatyti stabiliausiai veikiančią sistemą.

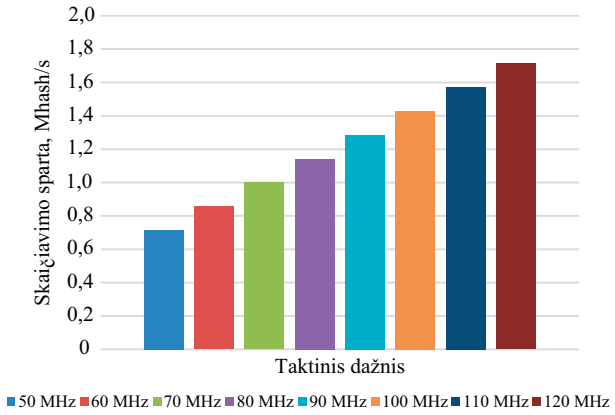
Iš 5 pav. matyti, kad maksimalus taktinis dažnis yra 120 MHz. Pasiekta maksimali skaičiavimo sparta yra 1,714310 milijonų santraukų per sekundę. Atlikus 10 matavimų, esant maksimaliam taktiniam dažniui, iš išmatuotų duomenų apskaičiuota vidutinio nuokrypio vertė lygi 0,0000229804.



4 pav. *Cyclone III* vienos gijos sistemos su skirtingais taktiniais dažniais matavimo rezultatai

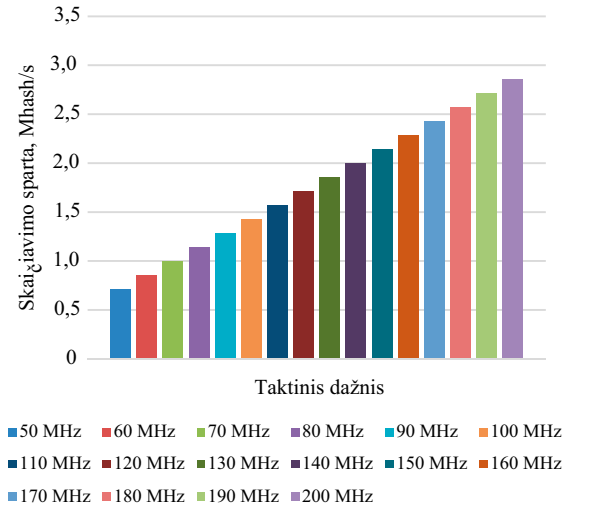
Fig. 4. *Cyclone III* one thread system with different clock frequencies measurement results

Iš 6 pav. matyti, kad pasiektas maksimalus taktinis dažnis yra 200 MHz. Taigi maksimalus dažnis yra 80 MHz didesnis už EP4CE115 programuojamos logikos integrinio grandyno maksimalųjį dažnį. Taip pat vienos gijos sistemoje yra pasiekta didžiausia skaičiavimų sparta. 5CSEMA5F31 programuojamos logikos integriniame grandyne pasiekta 2,857551 milijonų santraukų per sekundę skaičiavimo sparta. Esant maksimaliam dažniui atlikus 10 matavimų ir iš gautų matavimo rezultatų apskaičiavus vidutinio nuokrypio reikšmę gautas rezultatas lygus 0,000819061. Iš atliktų eksperimentų ir apskaičiuotų rezultatų galime daryti išvadą, kad suprojektuota sistema stabiliausiai veikia EP4CE115 programuojamos logikos integriniuose grandynuose. Šio programuojamos logikos integrinio grandyno vidutinis nuokrypis yra mažiausias, vadinasi, jo vertės arčiausiai pasiskirsčiusios ties vidutine matavimų verte.



5 pav. *Cyclone IV* vienos gijos sistemos matavimo rezultatai, esant skirtingiems taktiniams dažniams

Fig. 5. *Cyclone IV* one thread system with different clock frequencies measurement results



6 pav. *Cyclone V* vienos gijos sistemos matavimo rezultatai, esant skirtingiems taktiniams dažniams

Fig. 6. *Cyclone V* one thread system with different clock frequencies measurement results

Antras pagal stabilumą yra EP3C16 programuojamos logikos integrinis grandynas, trečias – 5CSEMA5F31. Šiame grandyne pasiekiamas didžiausias taktinis dažnis, bet jis yra nestabiliausias.

5CSEMA5F31 programuojamos logikos integrinis grandynas yra greičiausias ir mažiausiai energijos suvartojantis. Jis 40 % efektyvesnis už EP4CE115. Eksperimentų metu valdymo dalies programinis kodas buvo modifikuotas – pakeista perkrovimo trukmė. Pirminiame variante perkrovimas truko du taktus, po modifikacijos perkrovimas vyksta vieno takto metu. Tai 2,3 % padidino spartą. Sparta matuota sistemoje įdiegtoje 5CSEMA5F31 programuojamos logikos integriniame grandyne. Sistemos taktinis dažnis 200 MHz.

Iš 4–6 pav. pateiktų rezultatų matyti, kad didinant dažnį tiesiškai didėja ir skaičiavimo sparta. Visuose programuojamos logikos integrinuose grandynuose kitimas vienodas. Taigi, norint padidinti vienos gijos skaičiavimo spartą, reikia didinti taktinį dažnį. Didesnės spartos tirtuose programuojamos logikos integriniuose grandynuose pasiekti nepavyko. Norint pasiekti didesnę spartą reikia naudoti aukštesnės klasės programuojamą loginį grandyną arba gaminti specializuotą integrinį grandyną.

Skaičiavimų spartą įtakoja sintezuotų SHA-2 IP blokų kiekis kiekviename tirtame programuojamos logikos integriniame grandyne. Kiekvienas sintezuotas blokas yra lygiagretaus skaičiavimo šaka. Taigi, kuo daugiau turėsime SHA-2 IP blokų, tuo daugiau santraukų suskaičiuosime per sekundę.

Trečio eksperimento metu buvo tiriama sistema, turinti maksimalų skaičių SHA-2 IP blokų esant maksimaliam taktiniam dažniui. Sistemoje, kuriai panaudotas EP3C16 programuojamos logikos integrinis grandynas, pasiekta 17,304780 milijonų santraukų per sekundę skaičiavimo sparta. Šiame programuojamos logikos integriniame grandyne sintezuoti 11 SHA-2 IP blokų.

Sistemoje, kuriai panaudotas EP4CE115 programuojamos logikos integrinis grandynas, pasiekta apie 5 milijonų santraukų per sekundę skaičiavimo sparta. Teoriškai skaičiavimo sparta turėjo būti 137,1448 milijonų santraukų per sekundę. Išmatuotas rezultatas yra 27 kartus mažesnis už apskaičiuotą. Problemos priežastis slypi valdymo dalyje. Sintezuojant programinį kodą, blokai išdėstomi visame programuojamos logikos integrinio grandyno plote. Taigi kiekvieno bloko signalų keliai skiriasi, dėl tos priežasties sistema veikia nekorektiškai. Iš gauto rezultato galime daryti išvadą, kad iš 80 SHA-256 IP blokų veikia tik 3.

Sistemoje, kuriai panaudotas 5CSEMA5F31 programuojamos logikos integrinis grandynas, pavyko pasiekti 83,420229 milijonų santraukų per sekundę skaičiavimo spartą. Tačiau sistema visiškai nestabili, skaičiavimų spartos diapazonas nuo 22 iki 83 milijonų santraukų per sekundę. Iš gautų matavimo rezultatų matyti, kad valdymo dalis veikia labai nestabiliai. Išmatuoti spartos rezultatus pavyko, tik kai taktinis dažnis buvo lygus 150 MHz, aukštesniame taktiniame dažnyje skaičiavimai nevyko. Dažnis buvo sumažintas iki 120 MHz, tačiau stabilumo pasiekti nepavyko.

Kodo sintezavimas EP4CE115 programuojamos logikos integriniam grandynui trunka nuo 4 iki 7 parų, todėl šiam grandynui buvo sintezuotos dvi sistemos. 5CSEMA5F31 programuojamos logikos integriniam grandynui buvo sintezuojami tik 40 SHA-2 IP blokų, tačiau sintezavimas truko apie parą. Taigi šiam programuojamos logikos integriniam grandynui buvo sintezuotos sistemos, kurių taktinis dažnis nuo 120 MHz iki 200 MHz.

Norint pasiekti kuo didesnę skaičiavimo spartą galima keisti du parametrus: taktinį dažnį ir SHA-2 IP blokų skaičių. Abu parametrai skaičiavimo spartą keičia tiesiškai: jei padvigubinsime dažnį ir SHA-2 IP blokų skaičių, skaičiavimų sparta padidės keturis kartus.

Maksimalią skaičiavimo spartą pavyko pasiekti tik EP3C16 programuojamos logikos integriniame grandyne. Tai pavyko padaryti, nes šis programuojamos logikos integrinis grandynas turi mažiausiai loginių elementų. Dėl to atstumai tarp blokų yra mažiausi ir mažiausia vėlinimo trukmė. Sintezuota sistema veikia tik 100 MHz taktiniu dažniu.

Išvados

1. Didžiausia skaičiavimo sparta pasiekta sistemoje sintezuotoje EP3C16 programuojamos logikos 28 nm KMOP technologijos integriniame grandyne. Ji lygi 17,304780 milijonų santraukų per sekundę.
2. Skaičiavimo sparta tiesiškai priklauso nuo dažnio ir SHA-256 blokų skaičiaus. Norint padidinti skaičiavimo spartą, reikia didinti sistemos taktinį dažnį ir didinti lygiagrečiai skaičiuojančių SHA-256 kriptografinės maišos blokų skaičių.
3. Programuojamos logikos grandynų maksimalus pasiekiamas dažnis priklauso nuo gamybos technologijos – kuo mažesni matmenys, tuo didesnis taktinis dažnis.
4. Suprojektuota vienos gijos sistema veikia stabiliai 200 MHz dažniu.
5. Suprojektuota sistema neveikia stabiliai, kai naudojama daugiau skaičiavimo gijų ir padidinamas taktinis skaičiavimo dažnis. Daugelio gijų sistemos veikia stabiliai iki 150 MHz.
6. Norint, kad daugumoje atvejų gijų sistemos veiktų stabiliai, reikia pakeisti valdymo bloką.
7. Daugelio gijų sistemoje problemos kyla dėl blokų sinchronizavimo. Valdymo blokas neįvertina vėlinimo trukmių ir, esant aukštesniems dažniams, valdymo blokas veikia nekorektiškai. Problemos priežastis – visi blokai turi vienu metu generuoti atsakymą, kitaip blokas atmeta visus rezultatus. Taigi, norint gauti geresnius rezultatus, reiktų, kad valdymo blokas valdytų kiekvieną SHA-2 IP bloką atskirai.

Literatūra

Altera Corporation. 2015a. *Cyclone III FPGAs: optimized for low power* [interaktyvus], [žiūrėta 2014 m. balandžio 30 d.]. Prieiga per internetą: https://www.altera.com/products/fpga/cyclone-series/cyclone-iii/features/cy3-power.html#cyclone_power

Altera Corporation. 2015b. *Cyclone V FPGAs & SOCS* [interaktyvus], [žiūrėta 2014 m. balandžio 30 d.]. Prieiga per internetą: https://www.altera.com/products/fpga/cyclone-series/cyclone-v/overview.html

Altera Corporation. 2015c. *Cyclone IV FPGAs: optimized for lowest power* [interaktyvus], [žiūrėta 2014 m. balandžio 30 d.]. Prieiga per internetą: https://www.altera.com/products/fpga/cyclone-series/cyclone-iv/features/cyiv-power.html

Gauravaram, P. 2012. *Security analysis of salt-password hashes* [interaktyvus], [žiūrėta 2015 m. balandžio 26 d.]. Prieiga per internetą: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6516321

Kavaliūnas, A. 2008. *Kriptografijos maišos algoritmų lyginimas*, Vilnius: Technika [interaktyvus], [žiūrėta 2015 m. gegužės 24 d.]. Prieiga per internetą: http://leidykla.vgtu.lt/conferences/jmk_grafika_2008/files/pdf/kavaliunas_31-37.pdf

Stakėnas, V. 2006. *Kodai ir šifrai* [interaktyvus], [žiūrėta 2014 m. gegužės 18 d.]. Prieiga per internetą: http://www.mif.vu.lt/lmd/kodai_sifrai.pdf

Panaer, W.; Werhoven, T. 2007. *On the secure hash algorithm family* [interaktyvus], [žiūrėta 2015 m. balandžio 24 d.]. Prieiga per internetą: http://www.staff.science.uu.nl/~werkh108/docs/study/Y5_07_08/infocry/project/Cryp08.pdf

Tilborg, H. 2011. *Encyclopedia of cryptography and security* Belgium: Springer US [interaktyvus], [žiūrėta 2015 m. balandžio 20 d.]. Prieiga per internetą: http://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_615

ANALYSIS AND IMPLEMENTATION OF CRYPTOGRAPHIC HASH FUNCTIONS IN PROGRAMMABLE LOGIC DEVICES

T. Brukštus

Abstract

In todays world, data protection is more and more focused on. For data protection cryptographic science is used. In order to have the safe storage of passwords cryptographic hash function is used. In this article the SHA-256 cryptographic hash function

has been selected to implement and explore, based on fact that it is now popular and safe. SHA-256 cryptographic function did not find any theoretical gaps or conflict situations. Also SHA-256 cryptographic hash function used cryptographic currencies. Currently cryptographic currency is popular and its value is high. For the measurements programmable logic integrated circuits were chosen as they are less efficient then ASIC. We chose Altera Corporation produced programmable logic integrated circuits. Counting speed was investigated by three programmable logic integrated circuits. We used programmable logic integrated circuits which belong to the same family, but to the different generations. Each programmable logic integrated circuit was made using different dimension technology. Choosing these programmable logic integrated circuits: EP3C16, EP4CE115 and 5CSEMA5F31. To compare calculations performances parameters are shown in tables and graphs. Research shows the calculation speed and stability of different programmable logic circuits.

Keywords: cryptographic hash function, cryptographic hash functions digest, programmable logic integrated circuits.