SUMMARIES

G. Korvel, V. Šimonytė, V. Slivinskas. A Phoneme Harmonic Generator. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 7–12.

In the paper we present a new speech harmonic generator that retains the mutual harmonic amplitude ratio. This ratio is important for retaining the speaker timbre in the synthesized signal. The fourth order quasipolynomial model is chosen as the harmonic model in time domain. A novel algorithm for determining the amplitude and phase of harmonic is derived and its stepwise form is presented. A harmonic generator is excited by dynamic pseudo-periodic input sequences. An example of the synthesized harmonic of the vowel "a" and its comparison with the true sound signal harmonic is given.

C.-X. Zhou. Identity Based Generalized Proxy Signcryption Scheme. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 13–26.

Generalized signcryption can work as an encryption scheme, a signature scheme or a signcryption scheme with only one key pair and one algorithm. We extend it to the proxy system setting by considering sharing the same key pair and algorithm between the proxy signature and proxy signcryption, and we call it generalized proxy signcryption (GPSC). We give a formal definition and security model of GPSC in the identity-based setting by considering the whole abilities of an attacker, and propose a concrete scheme in the standard model. Our scheme is publicly verifiable, with strong security by considering insider attack, resisting proxy key exposure attack and with short system public parameters. Our scheme can be proved semantically secure against adaptively chosen ciphertext, chosen id and chosen warrant attack (IND-IB-GPSC-CCA for short) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption, and existentially unforgeable against adaptively chosen message, chosen id and chosen warrant attack (EUF-IB-GPSC-CMA for short) under the Computational Diffie-Hellman (CDH) assumption. The performance evaluation shows it to be of high efficiency. Moreover, we give a general construction of identity-based GPSC scheme from an identity-based combined signature and encryption scheme.

A. Šukys, L. Ablonskis, L. Nemuraitė, B. Paradauskas. A Grammar for ADVANCED SBVR Editor. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 27–41.

Semantics of Business Vocabulary and Business Rules (SBVR) is the richest knowledge model allowing to create specifications that are understandable for business people and also interpretable by computers. Existing SBVR editors still lack capabilities that could allow generating formal SBVR models, adapting SBVR to several languages or making SBVR extensions for various purposes (e.g., implementing transformations to software modelling languages) without changing the original SBVR metamodel. The goal of the paper is to present a grammar for SBVR structured language and a prototype of SBVR editor, created on the base of this grammar. An experiment conducted with the prototype has shown that it allows defining business vocabularies, business rules and questions in SBVR structured English and Lithuanian languages; producing formal SBVR models; using concepts from several vocabularies, and extending SBVR without changing its metamodel.

K. Błaszkiewicz, R. Piotrowski, K. Duzinkiewicz. Analysis the Parameters of the Adaptive Controller for Quality Control of Dissolved Oxygen Concentration. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 42–51.

The wastewater treatment plant can be considered as a dynamic large scale complex system, in which the most important control parameter is the dissolved oxygen concentration in the aerobic zone. The air is supplied to this zone by the aeration system. In the paper, both the sequencing batch reactor and the aeration system are modelled and used as plant of control performed by the cascade nonlinear adaptive control system extended by the anti-windup filter. The effect of certain parameters of the adaptive controller on the quality of control is analysed. Simulation results based on real data recorded in the case study plant are included.

D. Brodić, Z. N. Milivojević. Text Line Segmentation with Parametric Water Flow Algorithm. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 52–61.

The paper proposes an extension to the original water flow algorithm used for the text line segmentation in a document image. This extension is called a parametric water flow algorithm. The original algorithm assumes that the hypothetical water flows to the barrier representing objects. After that barrier, the hypothetical water creates different pathways under few specified angles creating labeled wetted and unwetted regions. The direction of the hypothetical water is from left to right side and vice versa. Hence, the final labeled wetted and unwetted image regions are created as their unions. The unwetted regions are used to segment text lines in a document image. The extension of the original water flow algorithm establishes the so-called water flow function, which is responsible for the unwetted region's creation. The proposed linear water flow function is exchanged with its parametric function counterpart. The basic, linear and parametric water flow algorithms are tested and evaluated under different synthetic and handwritten text samples. The experiments show promising results in the area of text line segmentation.

F. Wei, J. Ma, Q. Jiang, J. Shen, C. Ma. Cryptanalysis and Improvement of an Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 62–70.

In order to address the scenario in which the user wants to access the real-time data directly from the sensor node in wireless sensor networks (WSNs), Das proposed a two-factor authentication scheme. In 2010, Khan et al. pointed out that Das's scheme has some security flaws and proposed an improved scheme. Recently, Yuan demonstrated that Khan et al.'s improvement is still insure against several attacks. Yuan also proposed an enhanced two-factor user authentication scheme using user's biometrics to fix the security flaws in Khan et al.'s scheme. In this paper, we show that Yuan's scheme still suffers from the stolen smart card attack and the GW-node impersonation attack. Moreover, biometric keys are misused in Yuan's scheme such that even the valid user cannot pass the biometric verification. To remedy these problems, we propose an improved two-factor authenticated key distribution scheme based on fuzzy extractors. Security and performance analysis demonstrates that our scheme is more secure and efficient than previous schemes.

H.-Y. Lin. Secure Certificateless Two-Party Key Agreement with Short Message. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 71–76.

Two-party key agreement protocol allows two communication parties to share a common key for secure communication. Constructed from the certificateless public key cryptography (CL-PKC), a certificateless key agreement (CL-KA) protocol can not only solve the key escrow problem inherited from identity-based systems, but also avoid the troublesome issue of certificate management. Although the topic of two-party CL-KA has been extensively studied during past few years, it is unknown whether such a protocol can be achieved with only one exchanged message. In this paper, we put this idea into practice and propose a new one-round CL-KA for two-party. Specifically, each party of the proposed protocol only has to transmit one group element for sharing a session key and still maintains low computational costs. Moreover, we analyze the security of our scheme in the extended Canetti-Krawzcyk (eCK) security model.

D. Komosny, M. Voznak, S. Bezzateev, K. Ganeshan. The Use of European Internet Communication Properties for IP Geolocation. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 77–85.

IP Geolocation is a term used for finding the geographical location of an IP node. In this paper, we study the Internet communication properties and their use for client-independent Geolocation - finding the location without assistance of the node being located. We present and discuss the communication properties dependence on geographical aspects such as the geographical distance, differences between the source and destination country, and country population density and country ICT development index. For the study, we used a large set of data captured between the nodes geographically distributed across Europe. Based on the results, we propose an algorithm for a final location estimation within the delimited geographical area. The proposed algorithm improves the location accuracy when compared with the current techniques.

D. C. Gandolfo, L. R. Salinas, A. Brandão, J. M. Toibero. Path Following for Unmanned Helicopter: An Approach on Energy Autonomy Improvement. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 86–98.

In the last decades, the research efforts related to Unmanned Aerial Vehicles (UAV) has grown substantially in terms of control stabilization and navigation strategies. However, the energy available on board is finite and this is a limiting factor that prevents engineers from coming up with the best aerial solution in many situations. In this paper the path following control of a helicopter UAV based on the kinematic model is proposed, using a feedback linearization technique. The helicopter speed is adjusted according to direction changes of the desired path. Thus, the aircraft should holds its own weight in the air for the shortest possible time, aiming to save energy without neglecting the position control errors which can accumulate when its velocity increases and path direction changes. The proposed controller output is coupled to a dynamic model of a helicopter in order to evaluate the dynamic effects and to adjust the controller parameters. The stability of the controller is demonstrated in the sense of Lyapunov theory and validated by simulation results.

J. Čeponis, A. Venčkauskas, L. Čeponienė, A. Zonys. Extending Rule Set for Static Code Analysis in .NET Platform. *Information Technology and Control, Kaunas, Technologija*, 2016, Vol. 45, No. 1, 99–108.

This paper focuses on static code analysis tools for .NET platform. Static code analysis tools typically use a certain set of rules. In this paper, we propose to implement four rules, which we consider important from our practical experience of software development. We analyze the existing popular static analysis tools for .NET platform in order to determine whether they have the rules equivalent to our new rules. We select an open-source tool *Gendarme* for the implementation of these rules. We also investigate existing *Gendarme* rules and discover that some of them could be improved. Therefore, we propose and implement improvements for four existing *Gendarme* rules. In order to evaluate the improvements made in *Gendarme* rule set in a real-life environment, the source code of five open-source programs from sourceforge.net is tested using new and improved rules. Results indicate that new and improved *Gendarme* rules enable detection of more errors and can increase the quality of source code.

SANTRAUKOS

G. Korvel, V. Šimonytė, V. Slivinskas. Fonemų harmonikų generatorius. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 7–12.

Straipsnyje pristatomas naujas kalbos harmonikų generatorius, kuris išlaiko harmonikų amplitudžių tarpusavio santykį. Šis santykis yra svarbus siekiant išlaikyti diktoriaus tembrą sintezuotame signale. Laiko srityje harmonika aprašoma ketvirtos eilės kvazipolinominiu modeliu. Sukurtas naujas harmonikų amplitudžių ir fazių skaičiavimo algoritmas, kurio žingsniai ir pateikti straipsnyje. Harmonikų generatorius yra žadinamas dinamine pseudoperiodinių impulsų seka. Eksperimentinėje straipsnio dalyje pateikiamas balsio „a“ sintezuotos ir tikros harmonikos palyginimas.

C.-X. Zhou. Tapatumu grįsta apibendrinta įgaliotojo kodavimo su parašu schema. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 13–26.

Apibendrintas kodavimas su parašu gali veikti kaip užšifravimo schema, parašo schema ar kodavimo su parašu schema, kurią sudaro viena raktų pora ir vienas algoritmas. Ji išplečiama iki tarpinio serverio sistemos, nutarus, kad tarpinio serverio paraša ir kodavimas su parašu naudos tą pačią raktų porą ir algoritmą. Tai vadinama apibendrintu įgaliotojo serverio kodavimu su parašu (angl. generalized proxy signcryption – GPSC). Straipsnyje pateikiamas oficialus apibrėžimas ir GPSC saugumo modelis tapatumu grįstoje aplinkoje, nagrinėjamos visos galimybės, kurias turi puolantysis, standartiniame modelyje siūloma konkreti schema. Ši schema viešai patikrinama, gerai apsaugota žvelgiant iš vidinės atakos galimybės perspektyvos, galinti pasipriešinti tarpinio serverio atskleidimo atakai esant sumažintos sistemos viešiesiems parametrams. Schema gali būti įrodyta esanti semantiškai apsaugota nuo adaptyviai parinkto šifruoto teksto, ID ir įgaliotosios atakos (kitaip – IND-IB-GPSC-CCA), remiantis sprendimų priėmimo dvitiese Diffie'o ir Helmano (DBDH) prielaida, taip pat nepaneigiama prieš adaptyviai parinktą pranešimą, pasirinktą ID ir įgaliotąją ataką (kitaip – EUF-IB-GPSC-CMA). Veikimo savybių tyrimas parodė ją esant itin efektyvią. Taip pat pateikiama apibendrinta tapatumu grįsta GPSC schema, kurią sudaro tapatumu grįsta parašo ir šifravimo schema.

A. Šukys, L. Ablonskis, L. Nemuraitė, B. Paradauskas. Perspektyvaus *SBVR* Redaktoriaus Gramatika. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 27–41.

Veiklos žodyno ir veiklos taisyklių semantika (angl. *Semantics of Business Vocabulary and Business Rules* (*SBVR*)) yra išsamiausias šiuolaikinis žinių modelis, leidžiantis kurti dalykinės srities aprašus, kuriuos supranta veiklos dalyviai ir gali interpretuoti kompiuteriai. Esami *SBVR* redaktoriai dar nėra tiek ištobulinti, kad leistų generuoti formalius *SBVR* modelius, juos pritaikyti *SBVR* kelioms kalboms ar plėsti *SBVR* įvairiems tikslams (pvz., transformuoti į kitas modeliavimo kalbas) nekeičiant *SBVR* metamodelio. Straipsnio tikslas – pateikti *SBVR* struktūrizuotos kalbos gramatiką ir jos pagrindu realizuotą *SBVR* redaktoriaus prototipą, kuris įvykdytų minėtus reikalavimus. Eksperimentas, atliktas su prototipu, parodė, kad sukurtas *SBVR* redaktorius leidžia redaguoti veiklos žodynus, veiklos taisykles ir klausimus struktūrizuota anglų ir lietuvių kalba, generuoti formalius *SBVR* modelius, naudoti konceptus iš kelių žodynų ir plėsti *SBVR* nekeičiant jo metamodelio.

K. Błaszkiewicz, R. Piotrowski, K. Duzinkiewicz. Adaptyviojo valdiklio parametrų analizė ištirpusio deguonies koncentracijos kokybei kontroliuoti. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 42–51.

Nuotekų valymo įrenginys gali būti laikoma dinamine didelės apimties sudėtinga sistema, kurioje pagrindinis valdymo parametras yra ištirpusio deguonies koncentracija aerobinėje zonoje. Vėdinimo sistema perduoda orą į šią sritį. Straipsnyje yra modeliuojama ir vėdinimo sistema, ir nuoseklusis paketinis reaktorius, laikomi valdymo įrenginiu, kai kontrolė užtikrinama naudojant pakopinę netiesinę adaptyvią valdymo sistemą, papildytą neribojančiu filtru. Analizuojama atitinkamų adaptyviojo valdiklio parametrų įtaka valdymo kokybei. Įtraukiami simuliaciniai rezultatai, pagrįsti realiais duomenimis, įrašytais atvejo tyrimo įrenginyje.

D. Brodić, Z. N. Milivojević. Teksto eilutės segmentavimas, taikant parametrinį vandens tekėjimo algoritmą. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 52–61.

Straipsnyje siūloma, kaip išplėsti pradinį vandens srauto algoritmą, naudojamą teksto eilutei segmentuoti dokumento paveikslėlyje. Šis išplėtimas suvokiamas kaip parametrinis vandens tekėjimo algoritmas. Pradiniu algoritmu daroma prielaida, kad hipotetinis vanduo teka iki kliūties žyminčių objektų. Aplenkęs šią kliūtį, hipotetinis vanduo sukuria skirtingus kelius pagal kelis nurodytus kampus, sudarydamas sudrėkintas ir nesudrėkintas sritis. Hipotetinis vanduo teka iš kairės į dešinę ir atvirkščiai. Taigi galutinės pažymėtos sudrėkintos ir nesudrėkintos paveikslėlio sritys sudaromos kaip sąjungos. Sudrėkintos sritys yra naudojamos teksto eilutėms dokumento paveikslėlyje segmentuoti. Pirminiu vandens tekėjimo algoritmo plėtiniu nustatoma vadinamoji vandens tekėjimo funkcija, kuri atsakinga už nesudrėkintos srities sukūrimą. Siūloma tiesinė vandens tekėjimo funkcija pakeičiama jos parametrinės funkcijos atitikmeniu. Bazinis, tiesinis ir parametrinis vandens tekėjimo algoritmai yra testuojami ir vertinami pagal skirtingus dirbtinius ir ranka rašytus tekto pavyzdžius. Eksperimentai rodo daug žadančius rezultatus testo eilutės segmentavimo srityje.

F. Wei, J. Ma, Q. Jiang, J. Shen, C. Ma. Kriptoanalizė ir išplėstos dviejų veiksnių vartotojo autentifikavimo schemos pagerinimas belaidžiuose jutiklių tinkluose. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 62–70.

Siekdamas išspręsti scenarijų, pagal kurį vartotojas siekia prieiti prie realaus laiko duomenų tiesiogiai iš jutiklio mazgo belaidžiuose jutiklių tinkluose, Das pasiūlė dviejų veiksnių autentifikavimo schemą. 2010 m. Khan ir kt. atkreipė dėmesį, kad Das schema turi kelias saugumo spragas ir pasiūlė patobulintą schemą. Neseniai Yuan įrodė, kad Khan ir kt. patobulinimas neužtikrina, kad bus apsiginta nuo atakų. Yuan taip pat pasiūlė išplėstą dviejų veiksnių vartotojo autentifikavimo schemą, naudojant vartotojo biometrinius duomenis saugumo spragoms Khan ir kt. schemoje sutvarkyti. Straipsnyje parodoma, kad Yuan schema taip pat nepajėgi apsisaugoti nuo pavogtos lustinės kortelės atakos ir jutiklio mazgo apsimetimo atakos. Be to, biometriniai raktai Yuan schemoje yra naudojami neteisingai – net teisingas vartotojas negali pereiti biometrinio patikrinimo. Siekiant išspręsti šias problemas, siūloma išplėsta dviejų veiksnių vartotojo autentifikavimo schema, grindžiama apytiksliais ekstraktoriais. Saugumo ir veikimo analizė rodo, kad ši schema yra saugesnė ir veiksmingesnė nei ankstesnės.

H.-Y. Lin. Saugus be sertifikatų dvišalis susitarimas dėl raktų trumpa žinute. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 71–76.

Dvišalis susitarimo dėl raktų protokolas suteikia galimybę dviem bendravimo šalims naudoti bendrą raktą saugiai komunikacijai užtikrinti. Sudarius iš be sertifikatų viešojo rakto kriptografijos (angl. *certificateless public key cryptography – CL-PKC*), susitarimo dėl raktų be sertifikatų protokolą (angl. *certificateless key agreement – CL-KA*), galima ne tik išspręsti tapatumu grįstų sistemų sukeltą rakto sąlyginio deponavimo problemą, bet ir išvengti varginančio sertifikatų valdymo klausimo. Nors pastaruosius kelerius metus *CL-KA* tema intensyviai nagrinėjama, nėra žinoma, ar tokį protokolą gali užtikrinti tik viena apsikeista žinutė. Straipsnyje idėja įgyvendinama praktiškai, pasiūlomas naujas vieno apsikeitimo *CL-KA* abiem šalims. Svarbu pabrėžti, kad norėdama pasidalyti sesijos raktu kiekviena siūlomo protokolo šalis turi perduoti vieną grupės elementą, ir kompiuterinių duomenų apdorojimo sąnaudos vis dar išlieka menkos. Taip pat straipsnyje analizuojamas straipsnio autoriaus schemos saugumas išplėstiniame Canetti'o ir Krawzcyko saugumo modelyje.

D. Komosny, M. Voznak, S. Bezzateev, K. Ganeshan. Europos interneto ryšio savybių pritaikymas IP geolokacijai. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 77–85.

IP geolokacijos terminu apibrėžtas IP mazgo geografinės padėties nustatymas. Straipsnyje analizuojamos interneto ryšio savybės ir jų panaudojimas nuo kliento nepriklausančiai geolokacijai – tai vietos nustatymas, nenaudojant esančio mazgo. Pristatoma ir aptariama ryšių savybių priklausomybė nuo geografinių aspektų: geografinio nuotolio, skirtumų tarp pradinės ir paskirties šalies, šalies gyventojų tankumo ir IKT plėtros indekso. Straipsnyje atliekant tyrimą naudojama daug duomenų, surinktų tarp mazgų, geografiškai pasklidusių Europoje. Remiantis tyrimo rezultatais, siūlomas algoritmas dėl galutinės padėties nustatymo apibrėžtame geografiniame plote. Palyginti su dabartiniais metodais, siūlomas algoritmas pagerina vietovės nustatymo tikslumą.

D. C. Gandolfo, L. R. Salinas, A. Brandão, J. M. Toibero. Bepiločių straigtasparnių sekimo trajektorija: energetinės autonomijos pagerinimo metodas. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 86–98.

Pastaraisiais dešimtmečiais, kalbant apie valdymo stabilizavimą ir navigacijos strategijas, mokslinių tyrimų pastangos, susijusios su nepilotuojamais orlaiviais (UAV), padidėjo. Nepaisant to, energijos kiekis, prieinamas laive, yra baigtinis. Jis yra veiksnys, neleidžiantis inžinieriams daugelyje situacijų rasti geriausio aviacinio sprendimo. Straipsnyje siūloma bepiločių orlaivių kontrolės trajektorija, grindžiama kinematiniu modeliu. Tam taikomas grįžtamojo ryšio linearizacijos metodas. Drono greitis pritaikomas atsižvelgus į siekiamos trajektorijos krypties pokyčius. Taigi orlaivis pats turi išsilaikyti ore trumpiausią įmanomą laiką, kad sutaupytų energijos. Reikia nepamiršti ir pozicijos kontrolės klaidų, kurių gali padaugėti padidėjus greičiui ir pasikeitus trajektorijos krypčiai. Siūlomo valdiklio išeiga siejama su dinaminiu orlaivio modeliu, kad būtų įvertinti dinaminiai rezultatai ir pakoreguoti valdiklio parametrai. Valdiklio stabilumas įrodomas Liapunovo teorija ir patvirtinamas modeliavimo rezultatais.

J. Čeponis, A. Venčkauskas, L. Čeponienė, A. Zonys. Statinės kodo analizės taisyklių rinkinio papildymas .NET platformai. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2016, T. 45, Nr. 1, 99–108.

Straipsnyje analizuojami statinės kodo analizės įrankiai, skirti .NET platformai. Statinės kodo analizės įrankiai dažniausiai naudoja tam tikrą taisyklių rinkinį. Straipsnyje siūloma įgyvendinti keturias naujas taisykles, papildančias šį rinkinį, kurios galėtų būti naudingos ir reikalingos statinei kodo analizei. Analizuojami populiarūs statinės kodo analizės įrankiai .NET platformai, siekiant nustatyti, ar jų turimų taisyklių rinkiniuose yra straipsnyje siūlomų naujų taisyklių atitikmenų. Pasiūlytoms taisyklėms įgyvendinti pasirinktas *Gendarme* įrankis. Analizuojant *Gendarme*, taip pat pastebėta, kad kai kurios *Gendarme* taisyklės gali būti patobulintos. Taigi straipsnyje aptariama ne tik naujų taisyklių įgyvendinimas, bet ir keturių egzistuojančių *Gendarme* taisyklių patobulinimas. *Gendarme* taisyklių rinkinio patobulinimas eksperimentiškai įvertintas atliekant statinę kodo analizę penkioms atviro kodo programoms iš programų portalo iš *sourceforge.net*. Eksperimento rezultatai rodo, kad naujos ir pataisytos *Gendarme* taisyklės padeda rasti daugiau klaidų ir gali pagerinti programos kodo kokybę.