SUMMARIES

A. Riškus, G. Liutkus. An Improved Algorithm for the Approximation of a Cubic Bezier Curve and its Application for Approximating Quadratic Bezier Curve. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 303–308.

In this paper an improved version of an earlier proposed algorithm for approximating cubic Bezier curve by a set of circular arcs is presented. It is investigated how the improved algorithm fits for approximation of quadratic Bezier curves. These issues occur in CAD/CAM systems during data exchange into data formats which do not support Bezier curves. Experimental results on examples, widely used in the sources enlisted in references, are presented. Two typographical errors, made in the previous article, are corrected.

J.-L. Tsai, N.-W. Lo, T.-C. Wu. Efficient Proxy Signature Scheme for Mobile Devices Using Bilinear Pairings. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 309–314.

A proxy signature scheme is useful and convenient because it allows a proxy signer to sign a message on behalf of an entity. This study proposes a novel efficient proxy signature scheme for mobile devices using bilinear pairings. The computational cost of the proposed signature scheme is extremely low, and the length of the proposed signature is limited. In addition, our scheme does not require a special hash function, namely the Map-To-Point hash function. We also show that the proposed scheme is secure against adaptive chosen message attacks under a random oracle.

J.-H. Yang, Y.-F. Chang, Y.-H. Chen. An efficient authenticated encryption scheme based on ECC and its application for electronic payment. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 315–324.

In this paper, we propose an efficient authenticated encryption scheme based on elliptic curve cryptography. The proposed scheme does not need to construct any digital signature, so the computation costs can be greatly reduced. In addition, we also use the proposed authenticated encryption scheme to design a secure electronic payment system. The proposed electronic payment system provides the security requirements of confidentiality, authenticity, integrity, privacy protection, and double-spending prevention. According to the results of this paper, the proposed authenticated encryption scheme can be easily implemented in mobile payment environments. Besides, it can be also applied to electronic auction, online meeting, and electronic voting.

I. Ivanovienė, J. Rimas. The use of the Lambert Function Method for Analysis of a Control System with Delays. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 325-332.

The mathematical model of the mutual synchronization system with complete graph structure, composed of n ($n \in N$) oscillators, is investigated. This mathematical model is defined by the matrix differential equation with delayed argument. The solution of the matrix differential equation with delayed argument is obtained by applying the Lambert W function method. On the base of this solution, the step responses matrix of the synchronization system is defined and the transients in the system are investigated. The results of calculations, received by the Lambert function method, the dde23 method in Matlab and the exact method of consequent integration, are compared.

M. S. Farash, M. A. Attari. An Enhanced Authenticated Key Agreement for Session Initiation Protocol. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 333-342.

In 2012, Xie proposed an authentication scheme based on Elliptic Curve Cryptography (ECC) for Session Initiation Protocol (SIP). However, this paper demonstrates that the Xie's scheme is vulnerable to impersonation at-tack by which an active adversary can easily forge the server's identity. Based on this attack, we also show that the Xie's scheme is also defenceless to off-line password guessing attack. Therefore, we propose a more secure and efficient scheme, which does not only cover all the security flaws and weaknesses of related previous protocols, but also provides more functionalities. We also evaluate the proposed protocol by AVISPA (Automated Validation of Internet Security Protocols and Applications) tools and confirm its security attributes.

J. C. Galan-Hernandez, V. Alarcon-Aquino, J. M. Ramirez-Cortes, O. Starostenko. Region-of-Interest Coding based on Fovea and Hierarchical Trees. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 343-352.

Image and video compression exploits the redundancy of data to create a smaller representation. Lossy compression can be considered to be a type of transform coding where the raw data is transformed to a domain. Such a transform coding stores most of image energy into very few coefficients. In this paper we propose a compression algorithm based on Set Partitioning In Hierarchical Trees (SPIHT) that exploits the Human Visual System (HVS) and its fovea. In order to increase the image quality of the reconstructed image, regions of interest (ROI) are defined around a given point of gaze. The use of a fovea combined with ROI for image compression can help to improve the quality of the perception of the image and preserve different levels of detail around the ROI. In the proposed approach, the image is compressed using the Lifting Wavelet Transform and then quantized at

multiple compression ratios around the point of fixation of an observer, taking advantage of the natural aliasing of the HVS around the fovea. Such a compression delivers better image or frame reconstruction when a fixation point of an observer is given.

O. Kurasova, T. Petkus, E. Filatovas. Visualization of Pareto Front Points when Solving Multi-objective Optimization Problems. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 353–361.

In this paper, a new strategy of visualizing Pareto front points is proposed when solving multi-objective optimization problems. A problem of graphical representation of the Pareto front points arises when the number of objectives is larger than 2 or 3, because, in this case, the Pareto front points are multidimensional. We face the problem of multidimensional data visualization. The visualization strategy proposed is based on a combination of clustering and dimensionality reduction. Moreover, in the obtained projection of the Pareto front points onto a plane, the points are marked according to the Euclidean distance of multidimensional points, corresponding to the points visualized, from the ideal point. In the experimental investigation of the paper, neural gas is used for data clustering, and multidimensional scaling is applied to dimensionality reduction, as well as to visualizing multidimensional data. The strategy can be implemented in a decision support system and it would be useful for a decision maker, who needs to review and evaluate many points of the Pareto fronts, for example, obtained by genetic algorithms.

V. Jusas, T. Neverdauskas. Combining Software and Hardware Test Generation Methods to Verify VHDL Models. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 362–368.

Verification is an important part of the chip design process. Design is usually represented in hardware description language (HDL). Contemporary HDLs have constructs that are characteristic to software programs. Therefore, the methods to automatically generate test for software programs can be applied to generate test for HDL models. One of such methods is symbolic execution. We present a framework to generate test benches for HDL models. The framework combines the methods of symbolic execution and control flow graph, which are usually used in the context of software programs, with finite state machine that is characteristic for HDL models. The framework is implemented in Python programming language. We experimented with ITC'99 benchmark suite and compared the performance of our framework with similar research. Our obtained results outperformed the results taken from similar research.

C.-L. Chen, W.-C. Tsai, Y.-Y. Chen, W.-J. Tsaur. Using a Stored-Value Card to Provide an Added-Value Service of Payment Protocol in VANET. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 369-379.

With the rapid development of the Internet applications, added-value service is widely used in the Internet. The added-value service provides different kind of services for users. In this paper, we propose a stored-value card to provide an added-value service of payment protocol in VANET. When user wants to enjoy the added-value service, the service provider verifies the request and sends it to the payment gateway. Then the payment gateway forwards the transaction message to the Issuer and Acquirer to process it. In our scheme, we use symmetric cryptography and digital signature to solve the security problem of payment scheme in VANET. Our scheme achieves protection against double-spending, unforgeability, non-repudiation, anonymity and the recovery issue.

N. Nedić, G. Švenda. Workflow Management System for DMS. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 4, 380–392.

Dramatic enrichment of high speed communication technology at affordable costs enabled the resolution of problems related to the limitations of power supply. Therefore, introduction of Smart Grid for managing highly controllable power grids has become indispensable. It's very important part is Distribution Management System (DMS). These sophisticated systems execute a large number of workflows with very high resource requirements. In this paper dynamic, centralized scheduling strategies for allocating DMS workflows are presented and compared. Also, a distributed scheduling algorithm for DMS calculation engine is developed. It is argued that minor investment in the resources and introduction of a hybrid scheduling algorithm leads to the significant boost of the system performance. The hybrid scheduling algorithm is the result of combining centralized and distributed scheduling strategies. Experimental study shows that considerable improvement of overall system performance is achieved by using developed algorithms for designing effective schedulers when make-span and workload are optimized.

SANTRAUKOS

A. Riškus, G. Liutkus. Pagerintas kubinės Bezjė kreivės aproksimacijos algoritmas ir jo taikymas kvadratinės Bezjė kreivės aproksimacijai. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 303-308.

Straipsnyje pateikiamas pagerintas kubinės Bezjė kreivės aproksimacijos apskritimo lankais algoritmas. Išnagrinėtas ir praktiškai patikrintas šio algoritmo taikymas kvadratinės Bezjė kreivės aproksimacijai. Šie uždaviniai vykdomi keičiantis duomenims tarp skirtingų topologijos projektavimo sistemų, nes dauguma standartinių duomenų formatų nenaudoja Bezjė kreivių. Pateikti eksperimentinio tyrimo, palyginto su kitų autorių naudojamais testiniais pavyzdžiais rezultatai. Ištaisytos dvi ankstesnės publikacijos spausdinimo klaidos.

J.-L. Tsai, N.-W. Lo, T.-C. Wu. Efektyvi įgaliotojo asmens parašo schema iš dvitiesinių porų mobiliesiems įrenginiams. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 309-314.

Įgaliotojo asmens parašo schema yra naudinga ir patogi, nes ja remiantis įgaliotasis asmuo gali parašyti pranešimą subjekto vardu. Straipsnyje pateikiama nauja efektyvi įgaliotojo asmens parašo schema mobiliesiems įrenginiams, naudojant dvitiesines poras. Siūlomos parašo schemos skaičiuojamoji kaina yra itin maža, o pateiktas parašas yra riboto ilgio. Be to, mūsų schemai nereikia specialios maišos, atvaizdo-taško maišos, funkcijos. Straipsnyje taip pat pateikta, kad siūloma schema yra apsaugota nuo prisitaikančių atakų prieš pasirinktus pranešimus pagal atsitiktinius spėjimus.

J.-H. Yang, Y.-F. Chang, Y.-H. Chen. Efektyvi autentifikuota užšifravimo schema, pagrįsta ECC, ir jos taikymas elektroniniuose mokėjimuose. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 315–324.

Šiame straipsnyje pateikiama efektyvi autentifikuota užšifravimo schema, grindžiama elipsinės kreivės kriptografija. Naudojant siūlomą schemą, nereikia sukonstruoti skaitmeninio parašo, taigi skaičiuojamosios sąnaudos gali būti gerokai sumažintos. Taip pat autentifikuota užšifravimo schema naudojamatam, kad būtų sukurta saugi elektroninių mokėjimų sistema. Pristatoma elektroninių mokėjimų sistema nustato konfidencialumo, autentiškumo, vientisumo, privatumo apsaugos ir dvigubų išlaidų prevencijos saugumo reikalavimus. Remiantis straipsnyje pateiktais rezultatais, ši schema gali būti lengvai pritaikoma mobiliųjų mokėjimų aplinkoje. Be to, ji gali būti panaudota elektroniniuose aukcionuose, tiesioginiuose internetiniuose posėdžiuose ir elektroniniame balsavime.

I. Ivanovienė, J. Rimas. Valdymo sistemų su vėlavimais tyrimas taikant Lamberto funkcijų metodą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 325–332.

Tiriamas tarpusavio sinchronizacijos sistemos, sudarytos iš n ($n \in N$) generatorių, kurios struktūra yra visas grafas, matematinis modelis. Sistemos matematinis modelis yra matricinė diferencialinė lygtis su vėluojančiu argumentu. Matricinės diferencialinės lygties su vėluojančiu argumentu sprendinys yra gaunamas taikant Lamberto funkcijų metodą. Naudojant gautą sprendinį tiriami sistemos pereinamieji procesai. Rezultatai, gauti taikant Lamberto funkcijų metodą, lyginami su rezultatais, gautais taikant *dde23* metodą, aprašytą *Matlab* pakete, ir taikant „žingsniu“ metodą (nuoseklaus integravimo metodu).

M. S. Farash, M. A. Attari. Autentifikuotas raktinio sesijos inicijavimo protokolo susitarimo išplėtimas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 333–342.

2012 m. Xie pateikė autentifikavimo schemą, pagrįstą elipsinės kreivės kriptografija (ECC) ir skirtą sesijos inicijavimo protokolui. Nepaisant to, šis straipsnis rodo, kad Xie schema yra pažeidžiama apsimetimo kitu asmeniu atakomis, kurios leidžia aktyviam priešininkui lengvai suklastoti serverio tapatybę. Taigi Xie schema nepajėgi apsisaugoti nuo tiesioginių atakų, kuriomis siekiama atspėti slaptažodį. Taigi mes siūlome saugesnę ir efektyvesnę schemą, kuri ne tik ištaiso visas saugumo spragas ir ankstesnių saugumo protokolų trūkumus, bet taip pat yra daug funkcionalesnė. Mes taip pat įvertiname pristatomą protokolą, naudodami AVISPA (automatizuotas interneto saugumo protokolų ir taikomųjų programų patvirtinimas) priemones, ir patvirtiname jo saugumo savybes.

J. C. Galan-Hernandez, V. Alarcon-Aquino, J. M. Ramirez-Cortes, O. Starostenko. Regos lauko duomenų kodavimas, grindžiamas skridininės duobės ir hierarchinių medžių savybėmis. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 343–352.

Glaudinant vaizdą naudojamas duomenų perteklius, kad būtų sukurtas prastesnis vaizdas. Glaudinimas su nuostoliais yra viena iš transformacinio kodavimo rūšių, kai neapdoroti duomenys transformuojami į domeną. Toks transformacinis kodavimas įrašo didžiąją vaizdo energijos dalį labai mažais koeficientais. Šiame straipsnyje siūlomas glaudinimo algoritmas pagrįstas aibės padalijimu hierarchiniuose medžiuose (SPIHT), kuris naudoja žmogaus regos sistemą ir jos skridininę duobę. Norint pagerinti pakeisto paveikslo vaizdo kokybę, regos lauko duomenų kodavimas yra nustatytas pagal nurodytą žvilgsnio tašką. Skridininė duobė kartu su regos lauko duomenų kodavimu vaizdui suglaudinti gali padėti pagerinti vaizdo suvokimo kokybę ir išlaiko skirtingus elementų, išsidėsčiusių aplink regos lauką, lygius. Taikant siūlomą metodą vaizdas yra suglaudinamas, naudojant kėlimu grįstą bangelių transformaciją, o tuomet kvantuojama įvairiais glaudinimo koeficientais stebėtojo fiksavimo taške.

Tariama, kad žmogaus regos sistema geba vaizduoti dantytai iš skridininės duobės srities. Taip glaudinant pateikiamas geresnis vaizdas ar rekonstruojamas kadras, kai stebėtojo fiksavimo taškas yra nurodytas.

O. Kurasova, T. Petkus, E. Filatovas. Pareto aibės taškų vizualizavimas sprendžiant daugiakriterius optimizavimo uždavinius. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 353–361.

Straipsnyje pasiūlyta nauja Pareto aibės taškų vizualizavimo strategija, sprendžiant daugiakriterius optimizavimo uždavinius. Pareto aibės taškų grafinio atvaizdavimo problema kyla tada, kai kriterijų yra daugiau nei du ar trys, nes tuo atveju Pareto aibės taškai yra daugiamačiai. Tuomet susiduriama su daugiamačių duomenų vizualizavimo problema. Pasiūlyta vizualizavimo strategija pagrįsta klasterizavimo ir dimensijos mažinimo junginiu. Vizualizuojant Pareto aibės taškus, jie nuspalvinami atsižvelgiant į juos atitinkančių daugiamačių taškų euklidinius atstumus nuo idealaus taško. Eksperimentiniuose tyrimuose duomenims klasterizuoti taikomi neuroninių dujų, o dimensijai mažinti ir taškams vizualizuoti – daugiamačių skalių metodai. Pasiūlyta strategija gali būti įgyvendinta sprendimų paramos sistemoje. Strategija būtų naudinga sprendimų priėmėjui, norint peržiūrėti ir įvertinti daug Pareto aibės taškų, pavyzdžiui, gautų genetiniais algoritmais.

V. Jusas, T. Neverdauskas. Programinės ir aparatinės įrangos testų generavimo metodų sujungimas, testuojant VHDL modelius. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 362–368.

Verifikacija yra svarbi lustų kūrimo ir projektavimo proceso dalis. Projektas beveik visada užrašomas aparatinės įrangos aprašymo kalba. Palyginti su programinės įrangos kūrimo kalbomis, aparatinės kalbos turi panašias charakteristikas, todėl įmanoma pritaikyti programinės įrangos testavimo metodus ir aparatinėms kalboms. Vienas iš tokių metodų yra simbolinis vykdymas. Šiame straipsnyje aptariamas ir pristatomas programinis karkasas, skirtas testams generuoti. Karkasas tarpusavyje jungia simbolinį vykdymą ir vykdymo tėkmės grafą, kurie dažnai naudojami programinės įrangos kontekste, ir baigtinius automatus, kurie būdingi aparatūrai. Karkasas sukurtas Python programavimo kalba. Atlikti eksperimentai su ITC'99 schemų rinkiniu, palygintos karkaso generuojamų testų kokybinės charakteristikos su panašiais šios srities tyrimais.

C.-L. Chen, W.-C. Tsai, Y.-Y. Chen, W.-J. Tsaur. Dvejetaine sistema užkoduotų duomenų saugojimo kortelės taikymas, norint suteikti mokėjimų protokolo pridėtinės vertės paslaugas automobilių komunikacijos belaidžiam tinklui (VANET). *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 369–379.

Vis sparčiau plėtojantis interneto taikomosioms programoms, internete plačiai paplitusios pridėtinę vertę turinčios paslaugos. Pridėtinę vertę turinti programa teikia vartotojams įvairias paslaugas. Šiame straipsnyje siūloma teikti mokėjimo protokolo pridėtinės vertės paslaugas automobilių komunikacijos belaidžiu tinklu naudojant duomenų saugojimo kortelę. Kai vartotojas nori pasinaudoti pridėtinės vertės paslauga, paslaugos tiekėjas patvirtina prašymą ir nusiunčia jį į mokėjimo šliuzus. Tuomet kad būtų apdorotas, iš mokėjimo šliuzų pranešimas apie sandorį perduodamas siuntėjui ir gavėjui. Schemoje, kad būtų išspręsta apmokėjimo schemos saugumo problema VANET tinkle, naudojama simetrinė kriptografija ir skaitmeninis parašas. Mūsų schema yra apsaugota nuo dvigubų išlaidų, klastojimo, nepripažinimo, anonimiškumo ir išieškojimo.

N. Nedić, G. Švenda. Darbo eigos valdymo sistema paskirstymo valdymo sistemai. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 4, 380–392.

Sparčiai augant didelės spartos ryšių technologijoms prieinamomis kainomis, buvo išspręstos problemos susijusios su energijos tiekimo apribojimais. Taigi pažangiojo tinklelio sukūrimas, siekiant valdyti ypatingai kontroliuojamus energijos tinklelius, tapo neatskiriama dalimi. Tai itin svarbi paskirstymo valdymo sistemos (DMS) dalis. Šios ištobulintos sistemos tvarko darbo jėgos srautus, pasižyminčius dideliu išteklių poreikiu. Šiame straipsnyje yra pristatomos ir palyginamos dinamiškos centralizuotos planavimo strategijos, skirtos DMS darbo eigai paskirstyti. Taip pat plėtojamas paskirstymo planavimo algoritmas varikliui DMS apskaičiuoti. Teigiama, kad mažiausiai investuojant į išteklius ir hibridinio planavimo algoritmo įdiegimą sistemos efektyvumas gerokai padidėja. Hibridinis planavimo algoritmas atsiranda sujungus centralizuotas ir paskirstymo planavimo strategijas. Eksperimentiniai tyrimai rodo, kad visos sistemos efektyvumas itin gerėja, kai naudojami išplėtoti algoritmai, skirti efektyviems planuokliams, gerinant jų gamybos trukmę ir darbo krūvį, kurti.