# SUMMARIES

**L. Sekanina, R. Ruzicka, Z. Vasicek, V. Simek, P. Hanacek.** Implementing a Unique Chip ID on a Reconfigurable Polymorphic Circuit. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 7–14.

The need for secure physical implementations of cryptography functions has become urgent in the recent years. In particular, a unique unclonable chip ID has been implemented using various techniques. In this paper, we investigate the use of polymorphic gates as a new mechanism for implementing a unique chip ID in systems already containing some polymorphic gates. The proposed solution exploits the fact that switching time of polymorphic gates (controlled by $V_{dd}$) is slightly different even for neighboring gates on the same die because of fabrication variations. We applied a partial reconfiguration in order to generate 48-bit IDs on the reconfigurable polymorphic REPOMO32 chip that we have developed in our previous research. In some application scenarios, we achieved 94.44% stable bits which is reasonably close to existing approaches

**D. Levišauskas, T. Tekorius.** An Approach to Identification of Dynamic Model for Optimization of Fed-Batch Fermentation Processes. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 15–20.

An approach to mathematical model identification of fed-batch fermentation process is presented, which is based on using a versatile structure dynamic model and the formalized identification procedure of the nonlinear model parameters, which includes preliminary estimation of the parameter values. The proposed identification procedure is tested by model identification of fed-batch culture *E. coli*. The identified model is applied for calculation the optimal feed-rate time-profile maximizing the total biomass of cells' at the end of cultivation cycle.

**Z. Tan.** An Enhanced ID-based Authenticated Multiple Key Agreement Protocol. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 21–29.

Authenticated multiple key agreement protocols provide secure communication between the participants via multiple session keys within one run of the protocol in an authentic way. Recently, Dehkordi and Alimoradi proposed an identity-based authenticated multiple key agreement protocol. Subsequently, Cheng presented ephemeral key compromise attack and impersonation attack against Dehkordi and Alimoradi's protocol. In order to overcome their security flaws, Cheng proposed an improvement on Dehkordi and Alimoradi's identity-based authenticated multiple key agreement protocol. In this paper, we demonstrate that Cheng's protocol is also insecure. Then we propose an identity-based multiple key agreement protocol which removes their weaknesses of the two protocols. A detailed analysis demonstrates that the proposed protocol can satisfy the strong security requirements.

**R. Liutkevičius, A. Davidsonas.** Surface Reconstruction from Partially Structured Noisy Cloud Of Points Using B-Splines. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 30–37.

This paper presents a new approach how to reconstruct a parametric surface from a partially structured and noisy cloud of points representing surface that has a centre-line, such that all perpendicular rays to that line intersects with a surface not more than once. Presented algorithm analyses partially structured cloud of points, generated by point based 3D scanner and calculates parameters to build a non-uniform B-spline 3D mesh.

**U. Kač, F. Novak.** Reconfiguration Schemes of SC Biquad Filters for Oscillation Based Test. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 38–47.

Transformation rules for oscillation based test for different types of switched-capacitor (SC) biquad filter stages based on Fleischer-Laker biquad SC structure are proposed. In our earlier work presented at the 9th European Test Symposium, a solution for all-pass SC biquads has been reported. In this paper we generalize the approach to other classes of SC filter biquads. Theoretical background of the proposed approach is described and a set of practical design-for-test rules for each of the addressed SC structure is provided. Proposed oscillation based test structures can be included into a built-in self-test design with minimum hardware overhead.

**S. Pavalkis, L. Nemuraitė, R. Butkienė.** Derived Properties: a User Friendly Approach to Improving Model Traceability. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 48–60.

The paper presents a new approach to improving vertical traceability of UML models by defining derived properties that are calculated by a modeling tool on the fly. The proposed traceability metamodel and framework is implemented in UML CASE tool MagicDraw. The exploratory case study of applying the approach to a particular development process has shown that the approach allows validating completeness of the project, analyzing impact of changes, and, by doing this, avoids typical traceability issues. In contrast to other existing solutions, this approach does not burden users with additional complexity for defining and maintaining traceability in their projects. The approach gives a possibility for UML CASE tool developers to adapt their tools for traceability analysis not overloading them with traceability information, flexibly introducing required derived properties, dynamically calculating them, and analyzing via dedicated and already existing tool-specific means.

**C.-C. Yang, T.-Y. Chan, M.-S. Hwang.** A New Group Signature Scheme Based on RSA Assumption. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 61–66.

In this paper, we present a new group signature scheme based on RSA assumption. It not only achieves the same objective as the Lee-Chang scheme but also reduces the amount of computing time as compared to the Lee-Chang scheme and the Lee-Chang-Hwang scheme.

**A. Fatehi, B. Sadeghpour, B. Labibi.** Nonlinear System Identification in Frequent and Infrequent Operating Points for Nonlinear Model Predictive Control. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 67–76.

This paper studies identification of a process in both frequent and infrequent operating points to design a nonlinear model predictive controller. Although, many of industrial processes normally work around an operating point, however they should seldom work in some infrequent points as well. In this case, due to low ratio of data points, identification of the processes based on all data set results in poor identification of the infrequent operating points. To resolve this problem, in this paper, at the first step, a data clustering strategy is used to group the data in different operating points. Since the ratio of infrequent to frequent data points is extremely low, the strategy used is the fuzzy Gath-Geva clustering methodology. Then, at the second step, a new approach has been proposed to compromise performance of identification of the nonlinear model for frequent and infrequent operating points. It is shown that if the ratio of data associated with frequent operating point to data of infrequent operating point is appropriately selected, the performance of the model remains satisfactory in the frequent operating point while the performance in the infrequent operating point is significantly improved as well. The proposed method gives an interval for appropriate ratio of data set in the highly nonlinear pH neutralization process.

**I. Jr. Fister, T. Kosar, I. Fister, M. Mernik.** EasyTime++: A case study of incremental domain-specific language development. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 77–85.

EasyTime is a domain-specific language (DSL) for measuring time during sports competitions. A distinguishing feature of DSLs is that they are much more amenable to change, and EasyTime is no exception in this regard. This paper introduces two new EasyTime features: classifications of competitors into categories, and the inclusion of competitions where the number of laps must be dynamically determined. It shows how such extensions can be incrementally added into the base-language reusing most of the language specifications. Two case studies are presented showing the suitability of this approach.

**P. J. García-Laencina.** Improving Predictions Using Linear Combination of Multiple Extreme Learning Machines. *Information Technology and Control, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 86–93.

This work presents several effective approaches for linear combination of multiple artificial neural networks based on the extreme learning machine (ELM) algorithm. Given a learning task, a large set of neural networks are firstly trained by ELM. Then, these trained machines are efficiently ranked and the useless models are effectively discarded in order to provide an ensemble system with better generalization performance. The ensemble system is constructed using an automatic and fast forward model selection by minimizing the leave-one-out error, without user intervention. Experiments on an artificial regression dataset and three real-world engineering problems are discussed. According to the obtained results, the weighted linear combination of ELMs improves predictions by exploiting model diversity in the ensemble system with fast learning speed.

# SANTRAUKOS

**L. Sekanina, R. Ruzicka, Z. Vasicek, V. Simek, P. Hanacek.** Unikalaus lustinio identifikatoriaus įdiegimas į perkonfigūruojamą polimorfinę schemą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 7–14.

Saugių fizinių kriptografijos funkcijų realizacija tapo neatidėliotina pastaraisiais metais. Visų pirma, unikalus neklonuojamas lustinis identifikatorius buvo įgyvendintas taikant įvairius metodus. Šiame straipsnyje aptariami polimorfiniai vartai, kurie kaip naujas mechanizmas gali būti naudojami diegiant unikalius lustinius identifikatorius sistemose, jau turinčiose tam tikrus polimorfinius vartus. Sprendimas siūlomas pasinaudojus faktu, kad polimorfinių vartų perjungimo trukmė (kontroliuoja $V_{dd}$) yra šiek tiek kitokia nei gretutinių vartų ant tos pačios plokštės dėl gamybos paklaidų. Siekiant sukurti 48bitų identifikatorius perkonfigūruojamiems autorių anksčiau sukurtiems polimorfiniams REPOMO32 lustams, šie buvo iš dalies pertvarkyti. Kai kurie taikymo scenarijai pasiekėme 94,44 % stabilių bitų. Šis rezultatas yra artimas esamais metodais gautiems rezultatams.

**D. Levišauskas, T. Tekorius.** Būdas identifikuoti dinaminį modelį periodiniams su pamaitinimu fermentacijos procesams optimizuoti. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 15–20.

Pateikiamas periodinio su pamaitinimu fermentacijos proceso matematinio modelio identifikavimo būdas, kuris remiasi universalios struktūros dinaminio modelio panaudojimu ir formalizuota netiesinio modelio parametrų identifikavimo procedūra, naudojančia preliminarius parametrų verčių įverčius. Pasiūlytoji identifikavimo procedūra yra ištirta identifikuojant periodinės su pamaitinimu kultūros E. coli modelį. Identifikuotasis modelis yra panaudotas optimaliam pamaitinimo greičio laiko profiliui, maksimizuojančiam ląstelių biomasės kiekį kultivavimo ciklo pabaigoje, apskaičiuoti.

**Z. Tan.** Išplėstas identifikatoriumi pagrįstas autentifikuotas daugialypio rakto susitarimo protokolas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 21–28.

Autentifikuotieji daugialypio rakto susitarimo protokolai užtikrina saugų ryšį tarp dalyvių per daugialypių sesijų raktus vienu autentifikuotu protokolo paleidimu. Dehkordi ir Alimoradi neseniai pasiūlė tapatumu pagrįstą autentifikuotą daugialypio rakto susitarimo protokolą. Vėliau Chengas pristatė efemerišką rakto kompromitavimo ataką ir mėgdžiojimo ataką prieš Dehkordi ir Alimoradi protokolą. Siekdamas įveikti jų saugumo spragas, Chengas pasiūlė, kaip patobulinti Dehkordi ir Alimoradi tapatumu pagrįsto autentifikuoto daugialypio rakto susitarimo protokolą. Šiame darbe parodoma, kad Chengo protokolas taip pat yra nesaugus. Pasiūlytasis tapatumu grindžiamas daugialypio rakto susitarimo protokolas pašalina minėtų dviejų protokolų trūkumus. Išsami analizė parodė, kad jis gali atitikti didelio saugumo reikalavimus.

**R. Liutkevičius, A. Davidsonas.** *B-spline* paviršiaus modelio sudarymas iš dalinai sustruktūrinto ir triukšmais paveikto taškų debesies. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 29–37.

Pateikiamas naujas metodas, kaip iš dalinai sustruktūrinto ir triukšmais paveikto taškų debesies sudaryti parametrinį *B-spline* paviršiaus modelį su sąlyga, kad modeliuojamasis paviršius turėtų centrinę ašį tokią, kad iš jos išeinantys ir jai statmeni spinduliai paviršių kirstų ne daugiau kaip vieną kartą. Pateiktasis algoritmas analizuoja iš 3D skaitytuvo gautą paviršių aprašantį taškų debesį ir apskaičiuoja modeliuojamąjį paviršių aproksimuojančio netolydaus *B-spline* paviršiaus parametrus.

**U. Kač, F. Novak.** Perjungtų kondensatorių kvadratinių filtrų perkonfigūravimo schemos virpesiais grindžiamiems testams. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 38–47.

Siūlomos skirtingų tipų perjungtų kondensatorių (SC) kvadratinio filtro stadijų transformacijos, remiantis Fleischerio ir Lakerio kvadratinio SC struktūra, taisyklės svyravimu grindžiamam testui atlikti. Ankstesniame autorių darbe, kuris buvo pristatytas 9-ajame Europos testų simpoziume, buvo pasiūlytas visiško perdavimo SC kvadratinių filtrų sprendinys. Šiame darbe apibendrinamas kitų klasių SC filtro kvadratams taikytinas metodas. Aprašomas teorinis pasiūlytojo metodo pagrindas ir pateikiamas praktinių testo sudarymo taisyklių kiekvienai nagrinėtai SC struktūrai rinkinys. Pasiūlytosios svyravimais grindžiamo testo struktūros gali būti įtrauktos į įterptinį savikontrolės testo projektavimą minimaliomis aparatinės įrangos pridėtinėmis išlaidomis.

**S. Pavalkis, L. Nemuraitė, R. Butkienė.** Išvestinės savybės: vartotojui draugiškas požiūris į modelių trasavimo pagerinimą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 48–60.

Pateikiamas naujas požiūris, leidžiantis pagerinti vertikalų *UML* modelių trasavimą – išvestines savybes, automatiškai skaičiuojamas modeliavimo metu. Sukurtas trasavimo metamodelis ir sistema realizuota *UML CASE* įrankyje *MagicDraw*. Patvirtinta, kad šis požiūris leidžia tikrinti projekto išbaigtumą, analizuoti pokyčių poveikį ir išvengti būdingų trasavimo problemų. Skirtingai nuo kitų esamų trasavimo sprendimų, išvestinių savybių taikymas neapsunkina vartotojų dideliu sudėtingumu. *UML CASE* įrankių kūrėjai gali pritaikyti savo įrankius trasavimui, neapkraudami jų trasavimo informacija; šis požiūris leidžia lanksčiai apibrėžti norimas išvestines savybes, sparčiai jas skaičiuoti ir analizuoti ir sukurti specialias ar pritaikyti esamas įrankių galimybes.

**C.-C. Yang, T.-Y. Chan, M.-S. Hwang.** Nauja grupinio parašo schema pagrįsta RSA prielaida. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 61–66.

Pristatoma nauja grupinio parašo schema pagrįsta RSA prielaida. Ji ne tik pasiekia tą patį tikslą kaip Lee ir Chang schema, bet ir sumažina skaičiavimo laiką, palyginti su Lee ir Chang, taip pat Lee, Chang ir Hwang schemomis.

**A. Fatehi, B. Sadeghpour, B. Labibi.** Netiesinis sistemos identifikavimas dažnai ir nedažnai veikiančiuose taškuose nuspėjamai netiesinei modelinei kontrolei atlikti. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 67–76.

Nagrinėjamas proceso identifikavimas tiek dažnai, tiek nedažnai veikiančiuose taškuose siekiant sukurti nuspėjamą netiesinio modelio valdiklį. Nors daugelis pramoninių procesų paprastai vyksta aplink veikiantį tašką, tačiau kai kada jie turėtų vykti ir kai kuriuose nedažnai veikiančiuose taškuose. Šiuo atveju dėl mažo duomenų taškų santykio procesų, pagrįstų visų duomenų rinkiniu, identifikavimas baigiasi prastu nedažnai veikiančių taškų identifikavimu. Siekiant išspręsti šią problemą, pirmajame etape duomenims grupuoti skirtingai veikiančiuose taškuose naudojama klasterių formavimo strategija. Kadangi nedažnų ir dažnų duomenų taškų santykis yra ypač mažas, naudojama neapibrėžta *Gath Geva* klasterių formavimo metodika. Tuomet antrajame etape buvo pasiūlytas naujas metodas dažnai ir nedažnai veikiantiems taškams skirtų netiesinių modelių identifikavimui pažeisti. Parodyta, kad jei duomenų, asocijuojamų su dažnai veikiančiu tašku, ir nedažnai veikiančiu tašku, santykis parenkamas tinkamas, modelio vykdymas dažnai veikiančiame taške išlieka patenkinamas, o nedažnai veikiančiame taške labai pagerėja. Pasiūlytuoju metodu nurodomas intervalas tinkamam duomenų rinkinio santykiui gauti itin netiesiniuose pH neutralizavimo procesuose.

**I. Jr. Fister, T. Kosar, I. Fister, M. Mernik.** *EasyTime*++: laipsniško konkrečios srities kalbos vystymosi atvejų tyrimai. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 77–85.

*EasyTime* yra konkrečios srities kalba (DSL) laikui sporto varžybų metu matuoti. Skiriamasis DSL bruožas yra didesnis polinkis keistis; *EasyTime* taip pat nėra išimtis. Pristatomos dvi naujos *EasyTime* funkcijos: konkurentų klasifikavimas į kategorijas, ir lenktynių, kuriose ratų skaičius turi būti greitai nustatomas, įtraukimas. Tai parodo, kaip tokie plėtiniai gali būti palaipsniui pridedami prie bazinės kalbos pakartotinai naudojant daugumą kalbinių specifikacijų. Pateikiami dviejų atvejų tyrimai, iš kurių matyti, jog šis metodas tinka.

**P. J. García-Laencina.** Prognozių gerinimas naudojant tiesines daugialypių ekstremumų mokymosi mašinų kombinacijas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 1, 86–93.

Pristatomi keli veiksmingi metodai daugialypių dirbtinių neuronų tinklų, pagrįstų ekstremalaus mokymosi mašinos (EMM) algoritmu, tiesinei kombinacijai atlikti. Atsižvelgiant į mokomąją užduotį, didelis neuronų tinklų rinkinys pirmiausia apmokomas EMM. Tada šios apmokytos mašinos yra veiksmingai įvertinamos ir nenaudingi modeliai išmetami siekiant gauti labiau apibendrintą sistemą. Bendroji sistema yra sukurta naudojant automatinį ir spartų modelio parinkimą sumažinant galimybę palikti vieną klaidą, be vartotojo įsikišimo. Aptariami eksperimentai su dirbtinės regresijos duomenų rinkiniu ir trimis realaus pasaulio inžinerijos problemomis. Gautieji rezultatai parodė, kad svertinė tiesinė EMM kombinacija pagerina prognozes, kai jos gaunamos naudojant modelio įvairovę bendroje spartaus mokymosi sistemoje.