SUMMARIES

W.-C. Kuo, B.-L. Chen, L.-C. Wuu. Secure Indefinite-Index RFID Authentication Scheme with Challenge-Response Strategy. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 105–112.

In 2011, Chen, Tsai, and Jan proposed a radio frequency identification (RFID) access control protocol for a low-cost RFID system (CTJ-scheme for short). They claimed that their scheme not only guarantees mutual authentication and location privacy but also resists man-in-the-middle, spoofed reader, and spoofed tag attacks. However, in late 2011, Chen et al. pointed out that CTJ-scheme is vulnerable to a spoofed reader attack and did not provide any protection against denial-of-service (DoS) attacks. In addition, our research also found that under Chen et al.'s spoofed reader attack, tag contents can be surreptitiously altered by replaying message. In this paper, we analyze the weaknesses of CTJ-scheme and propose an enhanced scheme. According to our analyses, the proposed scheme is secure against the aforementioned DoS, spoofed reader, and modification attacks, while maintaining the merits of the original scheme.

H. Sun, Q. Wen, H. Zhang, Z. Jin. A Strongly Secure Pairing-free Certificateless Authenticated Key Agreement Protocol for Low-Power Devices. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 113–123.

Certificateless authenticated key agreement (CL-AKA) protocols neither suffer from a heavy certificate management burden nor have the key escrow problem. Recently, many CL-AKA protocols have been proposed. However, many of them need expensive bilinear pairings, which cannot be suitable for low-power devices such as sensors or mobile devices. To be implemented in practice, some pairing-free CL-AKA protocols have been built, however, very few of these pairing-free CL-AKA protocols can be secure in the eCK model. In this paper, we present a pairing-free CL-AKA protocol and provide a full proof of its security in the eCK model. Compared with the existing CL-AKA protocols, our protocol is more secure, practical and suitable for low-power devices.

C.-Y. Yeh, K.-L. Chen, S.-H. Hwang. Consistency Analysis of the Duration Parameter Within a Syllable for Mandarin Speech. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 124–130.

This work presents a study of Mandarin speech focusing on consistency analysis of the duration parameter within syllables. Identified as a result of inspection of the human pronunciation process, this consistency can be interpreted as a high correlation between the warping curves of the spectrum and the prosody intra a syllable. Through three steps in the procedure of the consistency analysis, the HMM algorithm is used firstly to decode HMM-state sequences within a syllable at the same time as to divide them into three segments. Secondly, based on a designated syllable, the vector quantization (VQ) with the Linde-Buzo-Gray algorithm is employed to train the VQ codebooks of each segment. Thirdly, the duration vector of each segment is encoded as an index by VQ codebooks, and then the probability of each possible path is evaluated as a prerequisite to analyze the consistency. It is demonstrated experimentally that a consistency is definitely acquired in case the syllable is located exactly in the same word. These results offer a research direction that the time warping process intra a syllable must be considered in a TTS system to improve the synthesized speech quality.

S. Mišković, Z. Stanimirović. A Memetic Algorithm for Solving Two Variants of the Two-Stage Uncapacitated Facility Location Problem. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 131–149.

This paper deals with a Two-Stage Uncapacitated Facility Location Problem (TSUFLP), which has important applications in designing telecommunication systems. Given a set of demand points and a set of possible locations for the first and second level concentrators (switches, multiplexors), the goal of the TSUFLP is to define the structure of two-level concentrator access network, such that the total cost of establishing such a network is minimized. We consider two variants of the TSUFLP from the literature and propose an efficient memetic algorithm (MA), based on hybridization of an evolutionary approach and two local-search heuristics. A greedy heuristic is incorporated in the MA frame for efficient calculation of the fitness function, which additionally decreases the overall MA running time. The described MA approach is benchmarked on test instances of medium and large dimensions from the literature, which are adapted for the TSUFLP and involve from 50 to 500 user nodes. On these instances, the proposed MA method quickly reaches all known optimal solutions, previously obtained by a linear programming method from the literature or CPLEX solver. In order to test effectiveness of the MA, we further modify some largescale instances from the literature involving 1000 and 2000 demand points, which can not be solved to optimality. Exhaustive computational experiments show that the MA provides solutions for the newly generated data set in relatively short CPU times. Regarding both solution quality and running times, we conclude that the proposed MA represents a powerful metaheuristic method for solving the TSUFLP and other similar network design problems.

Q. Jiang, J. Ma, G. Li, Z. Ma. An Improved Password-Based Remote User Authentication Protocol without Smart Cards. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 150–158.

Authentication is one of the fundamental mechanisms to enable a legitimate user to log into a remote server in an insecure environment. Many authentication protocols have been proposed in the literature for preventing unauthorized parties from access

resources. Recently, Chen et al. proposed a password-based remote user authentication and key agreement scheme using common storage devices, such as USB sticks. They claimed that the scheme can withstand off-line dictionary attacks even if the authentication information stored in the device is obtained by the adversary. However, we observe that Chen et al.'s scheme is insecure against off-line dictionary attacks in this case. To remedy this security flaw, we propose an improved authentication protocol without using smart cards. Compared with the previous schemes, our scheme not only provides more security guarantees, but also is more efficient both in computation and communication cost.

T.-T. Tsai, Y.-M. Tseng, T.-Y. Wu. Efficient Revocable Multi-Receiver ID-Based Encryption. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 159–169.

Quite recently, Tseng and Tsai proposed a revocable identity (ID)-based encryption (RIBE) with a public channel, in which the private key generator (PKG) can efficiently revoke misbehaving/compromised users by using a public channel. Considering the problem where a sender would like to encrypt an identical message for *n* receivers, the sender must re-encrypt the message *n* times using Tseng and Tsai's RIBE scheme. In such a case, *n* expensive pairing operations are required for the re-encrypting procedure. In this paper, for reducing the pairing operations, we extend Tseng and Tsai's RIBE to propose an efficient revocable multi-receiver ID-based encryption (RMIBE) scheme. Our scheme only needs one pairing operation to encrypt an identical message for n receivers while remaining the merit of user revocability in Tseng and Tsai's RIBE scheme. We demonstrate that the RMIBE scheme is semantically secure against adaptive chosen ciphertext attacks (CCA) in the random oracle model.

D. He, D. Wang, S. Wu. Cryptanalysis and Improvement of a Password-Based Remote User Authentication Scheme without Smart Cards. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 170–177.

Recently, Chen et al. [B. Chen, W. Kuo, L. Wuu, A secure password-based remote user authentication scheme without smart cards, Information Technology and Control 41(1) (2012) 53-59] proposed a secure password-based remote user authentication scheme without smart cards and claimed that their scheme could withstand various attacks. Although Chen et al.'s scheme has many benefits, we find that it is vulnerable to the device stolen attack and the privileged insider attack. We also find that their scheme does not support perfect forward secrecy and no key control. Therefore, we propose an improved scheme to overcome weaknesses and maintain the benefits of the original scheme.

T. Skersys, R. Butleris, K. Kapocius, T. Vileiniskis. An Approach for Extracting Business Vocabularies from Business Process Models. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 178–190.

Being a part of business process management (BPM) life cycle, business process modeling has found its place in information systems development (ISD) practices as well. At the same time, concepts of business vocabularies and rules are also the hot topics among BPM and ISD practitioners and academics. Nevertheless, in ISD, the integration of business process models with business vocabularies and rules is still not standardized and remains quite empiric. In this paper, basic aspects of the approach for business vocabularies' extraction from business process models are presented. The approach is based on novel business level OMG standards "Business Process Model and Notation" (BPMN) and "Semantics for Business Vocabularies and Business Rules" (SBVR), thus contributing to OMG's vision about Model-Driven Architecture (MDA) and to model-driven development in general.

Š. Packevičius, G. Krivickaitė, E. Guogis, D. Barisas, R. Jasaitis, T. Blažauskas. Test Data Generation for Complex Data Types Using Imprecise Model Constraints and Constraint Solving Techniques. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 2, 191–204.

Number of software applications is growing rapidly, as well as their importance and complexity. The need of quality assurance of these applications is increasing. Testing is one of the key processes to ensure the quality of software and object-oriented applications in particular. In order to test large and complex systems, test automation methods are needed, which evaluate whether the software is working properly. The main goal is to improve effectiveness of object-oriented applications testing by creating an automated test data generation method for complex data structures.

This paper presents a test data generation method by adhering to software under test static model and its model constraints. The method provides an algorithm that allows generating test data for complex data structures, by analysing software under test model, its constraints and using constraint solving techniques for building corresponding test data objects and their hierarchies. The presented method is exemplified by simple case studies as well as a large I++ protocol implementing web service project.

SANTRAUKOS

W.-C. Kuo, B.-L. Chen, L.-C. Wuu. Saugaus neapibrėžto indekso RFID autentifikavimo nustatymo sistema su *iššūkis* ir *atsakas* strategija. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 105-112.

2011 m. Chen, Tsai ir Jan pasiūlė radijo dažnio identifikavimo (RFID) prieigos kontrolės protokolą pigiai RFID sistemai (trumpiau – CTJ schema). Jie teigė, kad jų sistema ne tik užtikrina abipusį autentiškumo nustatymą ir vietos privatumą, bet ir priešinasi žmogui-tarpininkui, apsimestiniam skaitytojui ir netikrų gairių išpuoliams. Tačiau 2011 m. pabaigoje Chen ir kt. nurodė, kad CTJ schemą pažeidžia apsimestinio skaitytojo išpuoliai, ir nepateikė jokių veiksmų, kaip apsaugoti nuo paslaugos paneigimo (DoS) išpuolių. Be to, Chen ir kt. tyrimai taip pat nustatė, kad pagal apsimestinio skaitytojo išpuolį turinys gali būti slapta pakeistas atsakomuoju pranešimu. Šiame straipsnyje analizuoti CTJ sistemos trūkumai ir pasiūlyta patobulinta schema. Pagal atliktą analizę, siūloma sistema yra apsaugota nuo minėtų DOS, apsimestinio skaitytojo ir modifikacijų išpuolių, išlaikant pradinės schemos pranašumus.

H. Sun, Q. Wen, H. Zhang, Z. Jin. Saugus sertifikato nereikalaujantis autentifikavimo protokolas mažos galios prietaisams. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 113−123.

Pagal autentišką pagrindinio susitarimo (CL-AKA) protokolą nei reikia tvarkyti daug sertifikatų, nei reikia sąlygiškai įsipareigoti. Pastaruoju metu buvo pasiūlyta nemažai CL-AKA protokolų. Tačiau daugeliui iš jų reikia brangaus dvitiesio sujungimo, kuris negali tikti mažos galios prietaisams: jutikliams ar judriojo ryšio prietaisams. Kad būtų įgyvendinti praktiškai, buvo sudaryta keletas nesujungtų CL-AKA protokolų, tačiau mažai šių CL-AKA protokolų gali būti saugūs pagal ECK modelį. Šiame straipsnyje pristatomas nesujungtas CL-AKA protokolas ir pateikiamas ECK modelio saugumo įrodymas. Palyginti su galiojančiais CL-AKA protokolais, šis protokolas yra saugesnis, praktiškesnis ir tinka mažos galios prietaisams.

C.-Y. Yeh, K.-L. Chen, S.-H. Hwang. Mandarino kalbos trukmės parametro skiemens viduje pastovumo analizė. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 124–130.

Straipsnyje pristatomas mandarinų kalbos tyrimas, kuriame daugiausia dėmesio skiriama skiemenų trukmės parametro pastovumo analizei tirti. Šis pastovumas, nustatytas kaip žmogaus tarimo proceso tyrimo rezultatas, gali būti interpretuojamas kaip turintis labai stiprią sąsają tarp deformavimo kreivių spektro ir prozodijos vidinio skiemens. Per tris pastovumo analizės žingsnius, pirma, HMM algoritmas naudojamas HMM-būsena sekoms skiemens viduje iššifruoti tam, kad jos būtų suskirstytos į tris segmentus. Antra, remiantis pažymėtu skiemeniu, naudojamas vektoriaus kvantavimas (VQ) su „Linde-Buzo-Gray“ algoritmu siekiant pateikti kiekvieno segmento VQ *codebooks*. Trečia, kiekvieno segmento vektoriaus trukmė yra VQ *codebooks* užkoduota kaip indeksas, tada kiekvieno galimo kelio tikimybė yra vertinama kaip būtina sąlyga siekiant išanalizuoti pastovumą. Eksperimentiškai parodyta, kad pastovumas įgyjamas tuo atveju, jei skiemuo yra tiksliai tame pačiame žodyje. Aptarus šiuos rezultatus siūloma mokslinių tyrimų kryptis, kad siekiant pagerinti sintetintos kalbos kokybę laiko deformavimo procesas skiemens viduje turi būti TTS sistemoje.

S. Mišković, Z. Stanimirović. *Memetic* algoritmas, skirtas dviejų variantų dviejų etapų paslaugų vietos nustatymo problemai spręsti. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 131–149.

Straipsnyje nagrinėjama dviejų etapų paslaugų vietos problema (TSUFLP), kuri turi svarbių telekomunikacijų sistemų projektavimo programų. Atsižvelgiant į reikalavimus ir galimų vietų pirmojo ir antrojo lygmens koncentratorius (perjungiklius, tankintuvus), TSUFLP tikslas - apibrėžti dviejų lygmenų koncentratorių prieigos tinklo struktūrą taip, kad tinklui įrengti išleista bendra išlaidų suma būtų kuo mažesnė. Remiantis literatūra, apžvelgti du TSUFLP variantai ir pasiūlytas veiksmingas *memetic* algoritmas (MA), remiantis evoliucinio požiūrio ir dviejų vietinės paieškos euristikos mišrinimu. Godi euristika yra įtraukta į MA sistemą siekiant veiksmingai apskaičiuoti treniruoklių funkciją, kuri papildomai sumažina bendrą MA darbo laiką. Aprašytas MA metodas taikomas kaip etalonas vidutinių ir didelių matmenų, remiantis literatūra, pavyzdžiais, kurie yra pritaikyti TSUFLP ir apima 50−500 vartotojų mazgų. Taikant šiuos atvejus, siūlomas MA metodas greitai pasiekia visus žinomus optimalius sprendimus, anksčiau gautus taikant tiesinio programavimo metodą remiantis literatūra arba CPLEX sprendėju. Siekiant patikrinti MA efektyvumą, pakeisti kai kurie didelio masto literatūriniai pavyzdžiai, apimantys 1000 ir 2000 m paklausos taškus, kurie negali būti išspręsti optimaliai. Išsamūs skaičiuojamieji eksperimentai rodo, kad MA pateikia sprendimus naujai sugeneruotam duomenų rinkiniui per palyginti trumpą centrinio procesoriaus darbo laiką. Dėl tiek sprendimo kokybės, tiek ir veikimo laiko daroma išvada, kad siūlomas MA pateikia galingą metaeuristinį metodą TSUFLP ir kitų panašių tinklų projektavimo problemoms spręsti.

Q. Jiang, J. Ma, G. Li, Z. Ma. Tobulesnis slaptažodžiu paremtas nutolusio vartotojo autentifikavimo protokolas nenaudojant lustinės kortelės. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 150–158.

Autentifikavimas yra vienas iš svarbiausių priemonių, kad teisėtas vartotojas galėtų prisijungti prie nutolusio serverio nesaugioje aplinkoje. Literatūroje pateikta daugybė autentifikavimo protokolų, kurie neleistų neįgaliotoms šalims pasiekti

išteklius. Neseniai Chen ir kt. pasiūlė slaptažodžiu paremtą nuotolinio vartotojo autentifikavimo ir pagrindinio susitarimo schemą naudojant bendrus atminties įrenginius–USB atmintinės. Tvirtinta, kad schema gali atlaikyti netinklines žodyno išpuolius, net jei įrenginyje saugojama autentifikavimo informacija pasiekiama priešininkui. Tačiau pastebėta, kad Chen ir kt. schema šiuo atveju nėra saugi nuo netinklinių žodyno išpuolių. Siekiant ištaisyti šią saugumo spragą, siūlomas tobulesnis autentifikavimo protokolas nenaudojant lustinių kortelių. Palyginti su ankstesnėmis schemomis, siūloma schema ne tik suteikia daugiau saugumo garantijų, bet ir yra produktyvesnė atsižvelgiant tiek į skaičiavimą, tiek į ryšių išlaidas.

T.-T. Tsai, Y.-M. Tseng, T.-Y. Wu. Efektyvus atšaukiamas kelių-imtuvas ID grįstas šifravimas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 159–169.

Visai neseniai Tseng ir Tsai pasiūlė atšaukiama tapatybe (ID) pagrįstą šifravimą (RIBE) su viešuoju kanalu, kuriame privatus pagrindinis generatorius (PKG) gali efektyviai panaikinti netinkamai besielgiančius ar susikompromitavusius vartotojus, besinaudojančius viešuoju kanalu. Atsižvelgiant į problemą, kai siuntėjas norėtų užšifruoti identišką *n* gavėjų žinią, siuntėjas privalo pakartotinai užšifruoti pranešimą *n* kartų naudodamas Tseng ir Tsai RIBE schemą. Tuomet brangios *n* sujungimo operacijos peršifravimo procedūrai yra reikalingos. Siekiant sumažinti sujungimo operacijas išplėtus Tseng ir Tsai RIBE šifravimą siūloma veiksminga atšaukiama kelių imtuvų ID grindžiama šifravimo (RMIBE) schema. Šiai schemai reikia tik vienos sujungimo operacijos, kad užšifruotų identišką žinią *n* imtuvams, nors išlaikomas vartotojo atšaukiamumo pranašumas, esantis Tseng ir Tsai yra Ribe schemoje. Pateigta, jog RMIBE schema yra semantiškai apsaugota nuo adaptacinių parinktų užšifruotų tekstų išpuolių (CCA) atsitiktiniame *oracle* modelyje.

D. He, D. Wang, S. Wu. Slaptažodžiu pagrįsto nutolusio vartotojo tapatybės nustatymo schemos be lustinės kortelės kriptoanalizė ir tobulinimas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 170–177.

Chen ir kt. [B. Chen W. Kuo L. Wuu, Saugi slaptažodžiu pagrįsta nutolusio vartotojo tapatybės nustatymo schema be išmaniųjų kortelių, Informacinės Technologijos ir Valdymas, Vol. 41, No. 1 (2012), p. 53–59] pasiūlė saugią slaptažodžiu pagrįstą nutolusio vartotojo tapatybės nustatymo schemą be išmaniosios kortelės ir teigė, kad jų sistema galėtų atlaikyti įvairius išpuolius. Nors Chen ir kt. schema turi daug pranašumų, pastebėta, kad ji yra neapsaugota nuo prietaiso pavogtų išpuolių ir privilegijuoto nario išpuolių. Taip pat nustatyta, kad jų schema nepalaiko idealaus persiuntimo slaptumo ir pagrindinės kontrolės. Todėl siūloma patobulinta schema, kaip įveikti trūkumus ir išlaikyti pradinės schemos naudą.

T. Skersys, R. Butleris, K. Kapocius, T. Vileiniskis. Veiklos žodynų išgavimo iš veiklos procesų modelių metodas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 178–190.

Tradiciškai veiklos procesų modeliavimas yra veiklos procesų valdymo (VPV) gyvavimo ciklo dalis, tačiau pastaruoju metu ši disciplina vis plačiau taikoma ir informacinių sistemų (IS) kūrimo praktikoje. Veiklos žodyno ir veiklos taisyklių konceptai taip pat įgyja vis didesnį populiarumą tiek VPV, tiek ir IS kūrėjų bendruomenėse. Nepaisant to, IS kūrimo procese veiklos procesų modelių integracija su veiklos žodynais ir taisyklėmis vis dar išlieka empirinio pobūdžio. Šiame straipsnyje yra aptariami pagrindiniai veiklos žodynų išgavimo iš veiklos procesų modelių metodo aspektai. Metodas yra grindžiamas naujausiais OMG grupės sukurtais veiklos modeliavimo standartais „Business Process Model and Notation“ (BPMN) ir „Semantics for Business Vocabularies and Business Rules“ (SBVR). Taip prisidedama prie OMG grupės vizijos apie modeliais grindžiamą sistemų kūrimą.

Š. Packevičius, G. Krivickaitė, E. Guogis, D. Barisas, R. Jasaitis, T. Blažauskas. Sudėtingų duomenų tipų testinių duomenų generavimas, naudojantis apribojimų sprendimo technikas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 2, 191–204.

Programinė įranga tampa vis svarbesnė ir sudėtingesnė, ji vis labiau pritaikoma. Reikia vis labiau užtikrinti šių programų kokybę. Siekiant patikrinti didelių ir sudėtingų sistemų veikimą, reikalingi testavimo automatizavimo metodai, padedantys įvertinti, ar programa veikia tinkamai ir atitinka specifikaciją. Pagrindinis tikslas – sukurti efektyvų automatizuotą testinių duomenų generavimo metodą naudojant sudėtingas duomenų struktūras.

Straipsnyje pateikiamas testinių duomenų generavimo metodas sudėtingoms duomenų struktūroms, atsižvelgiant į testuojamos programinės įrangos modelį, klasių ryšius ir pateiktus apribojimus, - pritaikomi apribojimų sprendimo metodai ir jais konstruojami atitinkami testinių duomenų objektai ir jų hierarchijos. Pateiktas metodas iliustruojamas paprasto ir didelio projekto, realizuojančio I++ protokolo saityną, pavyzdžiais.