Refereed Journals and Series

   (c) Y. Chen, JS. Chou, Crypto-analyses on "user efficient recoverable offline e-cash scheme with fast anonymity revoking", Cryptology ePrint Archive (2013).

(2) A. Huszti, A Homomorphic Encryption-Based Secure Electronic Voting Scheme, Publicationes Mathematicae Debrecen, **79/3.-4.**, (2011), 479 – 496. (IF 0.358) (sch 6)

(3) A. Huszti, A. Pethő, A Secure Electronic Exam System, Publicationes Mathematicae Debrecen, **77/3.-4.**, (2010), 299–312. (IF 0.568) (sch 26)
   (c) Demirel, Denise, and Jeroen van de Graaf, Universally Verifiable Polling Site Voting Schemes Providing Everlasting Privacy, Diss. TU Darmstadt, (2014).


(o) A. Pavic, F. Skopljanc-Macina, Computer in testing the Fundamentals of electrical engineering at the University of Zagreb Faculty of electrical engineering and computing, Proceedings of the 35th International Convention MIPRO, (2012), 1205–1210.


(a) A. Huszti, A Secure Electronic Voting Scheme, Periodica Polytechnica Electrical Engineering 51/3.-4., (2007), 141–146. (sch 4)


(e) P. Surer, *ε-shift radix systems and radix representations with shifted digit sets*, Publicationes Mathematicae, **74/1.-2.**, (2009), 19–43.


(g) M. G. Madritsch, A. Pethő *Asymptotic normality of additive functions on polynomial sequences in canonical number systems*, Journal of Number Theory, **131/9.**, (2011), 1553–1574.


Refereed Proceedings


(a) Lou, Jia-Ning, Ming-Hour Yang, and Yu-Cheng Ho, **EMV-based mobile payment protocol for offline transaction with the ability of mutual authentication**, International Journal of Science and Engineering, 5/1, (2015), 61–66.


Thesis


Books


Non-refereed Proceedings


