Mathematical Problems of Computer Science 37, 75--82, 2012.

A New Approach to Receipt-Free E-Voting

A. Jivanyan

Russian-Armenian(Slavonic) University
e-mail: jivanyan@gmail.com

Abstract

In this paper we introduce a new electronic voting protocol with provable security properties. The generic method of voting presented here allows choosing different approaches for ballot casting to provide the most user-friendly interface.

References

[1] T. El-Gamal, "A public key cryptosystem and a signature scheme based on discrete Logarithms", *Advances in Cryptology - CRYPTO '84, LNCS 196, pp 10-18, 1984*

[2] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", *Advances in Cryptology-CRYPTO '86, vol. 263 of LNCS*

[3] D. Chaum and T. Pedersen, "Wallet databases with observers". *In Proc. of Crypto'92, Springer-Verlag*, pp. 89-105, 1993.LNCS 740.

[4] D. Chaum, "Secret Ballot Receipts and Transparent Integrity Better and less-costly electronic voting at polling places"*, http://vreceipt.com/article.pdf, 2004.*

[5] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *In Communications of the ACM,* 24(2), pp. 84-88, 1981.

[6] A. Shamir,"How to share a secret", *Communications of the ACM,* 22(11), pp. 612-613, 1979.

[7] D. Boneh, P. Golle, "Almost Entirely Correct Mixing With Application to Voting."

[8] A. Neff. "A verifiable secret shuffle and its application to E-Voting", *In Proc. of ACM CCS'01,ACM Press,* pp. 116-125. 2001.

[9] J. Furukawa and K. Sako, "An efficient scheme for proving a shuffle", *Proc. ofCrypto '01,Springer-Verlag, LNCS 2139,* 2001.

[10] P. Golle, S. Zhong, D. Boneh, M. Jakobsson, A. Juels, "Optimsitic mixing for exit-polls", *Advances in Cryptology (Asiacrypt 2002)', Vol. 2501 ofLNCS, Springer-Verlag, 2002.*

[11] M. Jakobsson, A. Juels and R. Rivest. "Making mix nets robust for electronic voting by randomized partial checking", *In Proc. Of USENIX'02.*

[12] D. Wikstrom. "Four practical attacks for "optimistic mixing for exit-polls"", *Technical Report T2003-04, Swedish Institute of Computer Science, 2003.*

[13] C. Park, K. Itoh and K. Kurosawa. "Efficient anonymous channel and all/nothingelectionScheme."*In Proc. of Eurocrypt 93, Springer-Verlag, LNCS765,* pp. 248-259, 1993.

[14] W. Ogata, K. Kurosawa, K. Sako and K. Takatani. "Fault tolerant anonymousChannel". *In Proc. of ICICS 97,* LNCS 1334, pp. 440-444, 1997.

[15] K. Sako and J. Kilian."Receipt-free mix-type voting scheme".*In Proc. of Eurocrypt95.Springer-Verlag, LNCS 921, 1995.*

[16] M. Abe. “Universally verifiable mix-net with verification work independent of thenumber of mix-servers”, *In Proc. of Eurocrypt 98, Springer-Verlag,* pp. 437-447, 1998.
[17] T. Moran, M. Naor. “Receipt-free universally-verifiable voting with everlasting privacy.”*In Advances in Cryptology CRYPTO 2006.*
[18] B. Adida and C. A. Neff.“Efficient receipt-free ballot casting resistant to covertchannels.”*In EVT/WOTE, 2009.*
[19] M. Stadler “Publicly verifiable secret sharing”. *Proc. Eurocrypt '96,* pp. 190-199. 1996.
[20] M. Naor and A. Shamir.“Visual cryptography”.*In EUROCRYPT,* pp 112,1994.

Գաղտնիություն ապահովող էլեկտրոնային քվեարկության նոր մոտեցում

Ա. Ջիվանյան

Ամփոփում

Մենք ներկայացնում ենք էլեկտրոնային քվեարկության նոր համակարգ՝ անվտանգության ձևական ապացուցվող հատկություններով: Առաջարկված է քվեարկության ընդհանուր մոտեցում, որը թույլ է տալիս ընտրել վերջնական քվեարկության տարբեր մեթոդներ, ինչը հնարավորություն է տալիս ընտրել օգտագործողի տեսակետից ամենահարմար ինտերֆեյսը:

Новый подход к обеспечению секретного электронного голосования

А. Дживанян

Аннотация

Мы представляем новую систему электронного голосования с формально доказуемыми свойствами безопасности. Предложен общий подход, позволяющий использовать различные конечные методы, что дает пользователям свободу выбора наиболее подходящего для них интерфейса.