Chapter 17
Theory and Practice of Secure E-Voting Systems

Kun Peng
Institute for Infocomm Research, Singapore

ABSTRACT

Electronic voting is a popular application of cryptographic and network techniques to e-government. Most of the existing e-voting schemes can be classified into two categories: homomorphic voting and shuffling-based voting. In a homomorphic voting, an encryption algorithm with special homomorphic property (e.g. ElGamal encryption or Paillier encryption) is employed to encrypt the votes such that the sum of the votes can be recovered without decrypting any single vote. An advantage of homomorphic voting is efficient tallying. Tallying in homomorphic voting only costs one single decryption operation for each candidate. In this chapter, the existing e-voting solutions in both categories are surveyed and analysed. The key security properties in both categories are presented and then the existing e-voting schemes in each category are checked against the corresponding security properties. Security and efficiency of the schemes are analysed and the strongest security and highest efficiency achievable in each category is estimated. Problems and concerns about the existing solutions including vulnerability to malicious voters and (or) talliers, possible failure of complete correctness, imperfect privacy, dependence on computational assumptions, and exaggerated efficiency are addressed. New approaches will be proposed in both kinds of solutions to overcome the existing drawbacks in them. In homomorphic e-voting, the authors deal with possibly malicious voters and aim at efficient vote validity check to achieve strong and formally provable soundness and privacy. It can be implemented through new zero knowledge proof techniques, which are both efficient and provably secure. In mix-network-based e-voting, the authors deal with possibly deviating operations of both voters and talliers and aim at efficient proof of validity of shuffling, which guarantees the desired security properties and prevent attacks from malicious participants. It can be based on inspiring linear algebra knowledge and the new zero knowledge proof of existence of secret permutation.

DOI: 10.4018/978-1-4666-4030-6.ch017

INTRODUCTION

Election has been playing a very important role in democracy and with the development of human society its form has kept changing. Through the past twenty centuries, different voting platforms have been adopted. The ancient Greeks dropped stones and pot shards into a vase, while the modern democracy developing from West Europe and North America adopts paper ballots, which are dropped in sealed boxes. All these traditional methods heavily depend on human intervention in tallying and so takes time and cannot avoid errors. The 2004 US president election is a typical example to demonstrate this drawback, not to mention the chaos caused by delay in tallying in countries with a large population. Moreover, in the fast-paced modern society, fewer and fewer people are willing to take the troubles to visit voting stations, especially in nations having enjoyed democracy for a long time.

With the rapid development of information technology, automatic voting becomes possible to prevent the drawbacks of traditional elections. The automation should maintain security of the traditional elections including fairness of the election and privacy of the votes. In 1869 Thomas Edison received US patent 90,646 for an "electronic voting device," but failed to sell his invention to the Massachusetts legislative bodies. Mechanical voting booths and punch cards are already employed to replace paper ballots to achieve faster tallying. Absentee ballots was adopted in 1997, when Monterey County, California experimented with the first Voting By Mail (VBM) system. Moreover, Direct Recording Electronic (DRE) systems have been employed in polling stations since the 1970s to store the talliers electromagnetically. As these methods still have drawbacks in convenience and speed, more advanced technologies are desired.

Electronic online voting on the Internet would be much more convenient as it enables voters to vote from anywhere. In the digital era, we have e-mail, e-commerce, e-passport, and many things have been automated by computers. The essential target of world wide Web is to communicate more information in a faster, cheaper and more convenient way. Internet voting enables voters to cast their votes any time anywhere and will result in higher voting rate. Moreover, votes in digital form can be counted fast and absolutely correctly. Fast, error-free and convenient voting and tallying processes could bring a great impact to the contemporary democratic societies. For example, elections can be held more often and in greater scale to make better use of democratic methods to decide more affairs by the citizens.

In 2004, Internet voting system was used in the national referendum in Geneva canton of Switzerland. In that nation, elections or referendums are held four or five times a year, while 580000 Swiss citizens living abroad among its seven million population. So it is important to provide them with a fast and convenient way to vote. Living in a wealthy country, more than half of the Swiss population had Internet access, both at home and at the workplace. Due to all these reasons, the governments, both at local and Federal levels have decided to develop Internet-voting solutions. According to a polling in 2003, about 73% of the Swiss population support online Internet voting. Besides already being applied to referendums, online Internet voting is supported by 80% of the Swiss voters to be employed in elections as well.

Internet voting was adopted in the European Parliamentary elections in the Netherlands in 2004 to help Dutch electors abroad or on trip on the Election Day. There was a registration phase before the elections so that eligible voters can choose the way they hope to use to vote: by post, by proxy holder, by Internet or by telephone. A surprisingly high rate (41%) of the eligible voters preferred the Internet voting system although most of them have access to the other methods. Actually, the rate could be much higher if more voters had receive the voting documents in time.

In the USA, there have been many attempts to employ electronic voting in elections. Among