Chapter 12

Electronic Governance Systems

ABSTRACT

As one of applications in electronic governance, this chapter develops an electronic voting (e-voting) system. After discussing requirements for e-voting systems and reviewing existing approaches, an e-voting system is developed based on confirmation numbers and signature pairs. Here, e-voting systems must satisfy requirements intrinsically contradicting each other, e.g. they must convince anyone that votes from only and all eligible voters had been counted, but at the same time to protect voters from a coercer that forces voters to choose its supporting candidate, correspondences between voters and their votes must be concealed from anyone including election authorities and voters themselves. The developed e-voting system successfully satisfies these requirements. However, it must be noted that these requirement are satisfied under the assumption that at least one of mutually independent multiple authorities is honest.

INTRODUCTION

Electronic governance (e-governance) systems are governmental systems supported by information and communication technologies, and because of features of information included, as same as e-payment systems they are most privacy sensitive systems. Among various mechanisms about e-governance systems, this chapter develops mechanisms for electronic voting (e-voting) systems, as ones, in which anonymous features are essential (e.g. if correspondences between voters and their votes are identified, an entity can easily force other entities to choose a candidate that the entity is supporting), while exploiting several schemes discussed in Part I and II. Anonymous features are also essential in electronic poll (e-poll) systems that enable government offices to collect opinions from citizens quickly, accurately and environmentally friendlily, but requirements for e-poll systems are almost the same as e-voting systems. Therefore, this chapter does not discuss them; they can be developed in the same way as e-voting systems.

Here, it must be noted that although many individual governmental tasks are intrinsically non-anonymous, i.e. they cannot be accomplished without knowing identities of individuals, there are many opportunities for anonymous security
technologies also in these systems. For example, although people inevitably must disclose their identities to register their cars and estates, they may not want that their cars and estates are linked by others.

In the following, after discussing requirements for e-voting systems and existing approaches for satisfying them, the e-voting system is developed and performances of the system are evaluated. In the developed e-voting system, the election administrator consists of multiple independent authorities, and it works under the assumption that at least one of the authorities is honest, i.e. nothing can make the system unreliable if at least one of the authorities is honest.

**REQUIREMENTS FOR E-VOTING SYSTEMS**

E-voting is one of anonymous security applications that attract most researchers because of its difficult challenges, i.e. to develop e-voting systems various requirements that intrinsically contradict each other must be satisfied. In practical aspect, e-voting systems are also one of most important applications. Namely in e-voting systems, voters cast their votes as electronic signals and votes are tallied by computers, therefore voting and tallying processes become efficient and accurate. In addition because ballot papers are replaced by electronic signals, physical resources required for voting can be reduced substantially, and moreover, supported by computer networks voters in remote places can participate in elections more easily. However, different from paper based voting systems where physically sealed ballot boxes and publicly disclosed tallying processes ensure the legitimate voting, in e-voting systems, everything is processed by computer programs that cannot be seen physically, and as a consequence, people cannot convince themselves that voting is legitimate, e.g. even when the computer program replaces some votes with different ones no one except the computer can notice that. Therefore simple mechanisms ruin all the above benefits of e-voting systems.

Here, ideal e-voting systems must preserve privacies of individual voters, must be able to convince people that the voting is accurate and fair, must disable any entity to coerce voters to choose a candidate it is supporting, and must be able to resolve disputes between voters and election administrators. Also, they must be robust against various intentional or accidental troubles, must be applicable to large-scale elections, and must be supported by practical assumptions. However, some of these requirements completely contradict each other, e.g. individual votes must be linked to their voters to convince people that all votes are legitimate, but these links reveal privacies of voters, also they enable an entity to coerce voters to choose its supporting candidate more reliably. To protect a voter from being coerced by other entities, any link between a voter and its vote must be concealed even from the voter itself.

Requirements for e-voting systems are summarized as follows.

1. **Privacy**

   Choices of voters must be concealed from others including election authorities. Here, it must be noted that the choice of a voter includes the abstention from the voting. A solution in paper based voting systems is easy when abstentions are not considered, i.e. sealed ballot boxes of which insides are not visible from the outside satisfy the requirement. At a time when a ballot box is opened, anyone (even voters themselves) cannot identify correspondences between voters and their votes, because votes in the box are shuffled. However, in e-voting systems, it is not trivial to convince voters that computer programs had actually shuffled votes in the way that no one including election authorities can know the shuf-