Recent advances of information and communication technologies are making societies highly efficient and convenient. When the Internet and credit card systems are combined, people can buy various things without going out from their homes or offices, and if their buying articles are home appliances or manufacturing machines for example, monitoring systems can remotely trace these appliances or machines and monitor their operational states to provide their users with suggestions so that they can be operated in more efficient, safe, and environmentally friendly ways. However, currently these systems are available only on an exchange with privacy disclosure risks of individuals. For example, because all kinds of purchase records of individuals are stored in databases of credit card companies, all privacies of individuals will be revealed if the card companies are not operated adequately. These risks exist also in organizations, e.g. companies must disclose sensitive information including their top secrets to fully utilize latest e-business systems. Threats of these privacy or secret disclosures are becoming more and more serious as people are extending their activities while being supported by the advancing information and communication technologies.

Here, among information about individuals and organizations, identities of entities are one of the most sensitive data on the one hand, i.e. as many books about security refer the phrase “spy agencies acquire more information from the traffic of messages than the messages themselves (Wright, 1987),” sometimes identities of owners and/or users of the information are more sensitive than the information itself. On the other hand, things people can conceal are only their identities in many applications. For example, people cannot conceal messages themselves when they want to inform others of them, also when people buy articles, they cannot conceal articles or their prices from stores. Therefore, establishments of technologies that enable secure handlings of identities of individuals and organizations are one of the keys to make our societies further convenient, efficient, safe, and environmentally friendly. Namely, technologies to conceal owners or users of data and objects reduce risks of privacy and secret disclosures, and as a consequence, encourage many people to reap benefits from advancing information and communication technologies.

Anonymous systems and anonymous security technologies are concerned with information systems and mechanisms that conceal identities of entities at the minimum cost. Here, it is not so difficult to develop anonymous systems when absolutely trustworthy entities can be assumed. For example, if a credit card company is ensured absolutely not to disclose purchase records of its customers to others, cardholders can easily conceal their individual purchases from others. However the costs for maintaining these trustworthy entities become extremely high, because no entity is absolutely trustworthy in the real world, credit card companies must maintain highly educated staffs, and they must protect their main-
taining information from every kind of threats regardless they are intentional or accidental. By making use of anonymous security technologies, it becomes possible to exclude these absolutely trustworthy entities from information systems as much as possible so that people can receive services from them securely at less cost.

Since the pioneering works of Chaum (1985), many researchers and practitioners had been continually making progresses in developing anonymous security technologies, and currently, at least theoretically, it is possible to develop communication systems, in which people can securely exchange information without disclosing their identities to others including senders or receivers of their messages and managers of communication systems. Also cardholders of credit card systems can make purchases without disclosing their identities to any other entities while enabling credit card companies to correctly calculate total expenditures of individual cardholders, and maintenance companies can monitor running states of home appliances while preserving privacies of the users.

This book discusses requirements for anonymous systems in various application fields, and based on currently available technologies, develops anonymous systems so that anonymous security technologies are applied more extensively and people are encouraged to develop more efficient and effective anonymous security technologies that exclude trustworthy entities as much as possible. The book consists of 3 sections: “Introduction,” “Data and Communication Security in Anonymous Systems,” and “Developing Secure Anonymous Systems.” All sections are for every kind of readers who have interests in anonymous systems from non-experts to experts. Only fundamental mathematical knowledge is assumed.

The 1st section introduces requirements for anonymous security technologies in various applications together with fundamental security components such as encryption functions and digital signatures, and the 2nd section discusses schemes for protecting data owned by anonymous entities from their illegitimate modifications, deletions, additions, etc. Schemes for exchanging messages without disclosing identities of senders and/or receivers to others, and calculating aggregate values of data without knowing their individual values are also discussed. Then finally in the 3rd section, anonymous authentication systems, and as applications of anonymous security technologies, electronic payment (e-payment), electronic procurement (e-procurement) and electronic governance (e-governance) systems are developed. In detail, e-payment systems include credit card and electronic cash (e-cash) systems, and e-procurement systems include auction, object delivery and object monitoring systems. Regarding e-governance systems, an electronic voting (e-voting) system is developed as a typical example.

However, it must be noted that although several application systems can be developed without assuming any trustworthy entity (i.e. for an entity in them entities that it can trust is only itself), as far as for currently available technologies, there are still many important applications in which trustworthy entities cannot be excluded completely. Therefore, in these cases, trusts are distributed into multiple independent authorities, and entities can believe that their identities are concealed from others unless all authorities conspire, in other words, when at least one of authorities is honest.

Topics of individual chapters are shown below.
SECTION 1

This section consists of 4 chapters. The first chapter discusses requirements for anonymous security technologies while introducing typical applications. Namely, to preserve privacies of individuals and to protect secrets of organizations, communication systems must enable entities to send or receive messages without disclosing their identities even to managers of communication systems and receivers or senders of messages, and credit card systems must enable cardholders to make their purchases without disclosing their identities to others while ensuring that card companies can collect exact expenditure amounts from cardholders. Also, service providers in cloud computing must be able to calculate various functions of data owned by clients without knowing values of individual data. Moreover, to protect voters from coercers who are forcing the voters to choose their supporting candidates, e-voting systems must conceal correspondences between voters and their votes even from voters themselves. Secure anonymous system technologies must cope with these requirements.

The 2nd chapter defines encryptions and decryptions as the most fundamental security components for developing security enhanced systems. Also, homomorphic (additive or multiplicative), probabilistic, commutative and verifiable features are highlighted as the desirable ones of encryption algorithms for developing secure anonymous systems, and typical encryption algorithms are evaluated in terms of these features. Then, the 3rd chapter, about schemes for protecting data from their illegitimate modifications and forgeries, follows, i.e. hash functions, MACs (Message Authentication Codes) and digital signatures are introduced. Hash functions, MACs, and digital signatures protect data by detecting illegitimate modifications while attaching redundant values to the data, namely, when an entity illegitimately modifies the data, the modified results become inconsistent with the attached values, and among them, digital signatures enable anyone including third parties to convince others that its owning data with signatures are legitimate ones.

In the last chapter of the section, linear equation based encryption functions and re-encryption and threshold encryption schemes are discussed as ones that play important roles in anonymous systems. Linear equation based encryption functions enable entities to calculate sums of data owned by others without knowing individual values, and by using probabilistic, commutative and verifiable re-encryption schemes, entities can encrypt data while concealing the correspondences between encrypted data and their decrypted forms from anyone including the owners of the data. Threshold ElGamal encryption functions disable entities to decrypt encrypted data without the cooperation among t out of n authorities (t ≤ n), while ensuring correct decryptions when at least t-authorities are honest. All encryption schemes will be extensively used in the following sections of this book, e.g. for developing anonymous communication systems, anonymous authentication systems, anonymous payment systems, and e-voting systems.

SECTION 2

This section also consists of 4 chapters. After discussing approaches to implementing secure anonymous systems, discussions about schemes for maintaining integrities of data in anonymous environments and exchanging messages with anonymous entities follow. Schemes for anonymous statistics calculation that enable entities to calculate aggregate values of data without knowing their individual values are also discussed.
The 1st chapter summarizes how homomorphic and commutative features of encryption functions solve various problems appear in satisfying requirements of anonymous systems. Commutative encryption functions can be used to detect illegitimate modifications and forgeries of data without knowing data themselves, and homomorphic encryption functions can be used to calculate functions of data without knowing their individual values, to detect dishonest deletions of data maintained by other entities and to identify dishonest entities without knowing any secret of honest entities. Here, frequently entities can maintain their encryption keys as their secrets in anonymous systems, therefore there are opportunities not only for modern public key based encryption schemes but also for secret key based ones, and legacy encryption algorithms such as linear equation based ones play important roles.

The 2nd chapter relates to schemes for detecting illegitimate modifications and forgeries of data without knowing data themselves. Blind signature schemes enable entity P to obtain the signature of other entity on its data $M$ without disclosing $M$, therefore later on P can prove the authenticity of $M$ without disclosing its identity. Unlinkable signatures on data ensure that signers had honestly signed on only and all eligible data while disabling anyone including data owners and signers to know correspondences between the data and their signed forms, and implicit transaction links (ITLs) can be used to detect deletions of data maintained by other entities without knowing the data themselves. They also enable the developments of anonymous tokens and homomorphic anonymous tokens by which entities can prove their eligibilities while maintaining their anonymities. As another approach to enabling anonymous entities to prove their eligibilities, anonymous tag-based credentials are also discussed, where anonymous tags are attached to physical or logical objects so that entities can identify their objects while disabling others to identify them. Anonymous tokens, homomorphic anonymous tokens, and anonymous credentials can be used also to identify dishonest entities while preserving privacies of honest entities. In addition to tokens and credentials, as schemes to convince others that an entity is honest (knows secrets) without disclosing its secrets, well known cut and choose protocols and zero knowledge proofs (ZKPs) are also discussed.

Schemes of anonymous communication that enable entities to send and/or receive messages without disclosing their identities to others are discussed in the 3rd chapter. Here, anonymous communications are bases for almost all kinds of anonymous application systems because current computer supported services are implemented as networks of service providing servers and clients, and without anonymous communications identities of entities are easily revealed from their network addresses. Among various existing schemes this chapter introduces Crowds, DC net, Mix-net, ESEBM (Enhanced Symmetric key Encryption Based Mix-Net), and Onion Routing. Mechanisms to protect anonymous communication systems from malicious entities are also discussed. However, different from many other schemes in this section that completely exclude trusted entities, current technologies cannot exclude trusted entities completely from anonymous communications, i.e. all of the above mechanisms consist of multiple independent message transferring servers, and senders and/or receivers are ensured to be anonymous only when at least one of multiple servers is honest.

Finally, the last chapter of this section discusses schemes for anonymous statistics calculations, in which entities calculate various functions of data owned by anonymous or non-anonymous entities without knowing their individual values. Employees of a company do not mind even if their average salary is disclosed, but they do not want to disclose their individual salaries for example, and mechanisms in this chapter cope with these requirements. Currently, companies are shifting to achieve their tasks while using resources owned and operated by others, but still they must use their own computing resources to process their secret data. Schemes discussed in this chapter play important roles in accelerating these shifts and consequently to reduce total energy and resource consumptions. However, although theoreti-
cally there are schemes to calculate any function of data without knowing their individual values, their implementations are not practical, i.e. too complicated and time consuming. Therefore, this chapter discusses methods based on encryption functions with homomorphic features, they are blind sum/product calculation schemes, partial computation based multi party computation schemes, and re-encryption based multi party computation schemes. Although they are not for general purposes, they enable efficient calculations of averages, variances, auto and mutual correlations, etc. of given data.

**SECTION 3**

This section analyses requirements of various applications of anonymous system technologies and develops systems that satisfy the requirements while using security components discussed in Section 1 and 2. In the 1st chapter, anonymous authentication systems are developed based on various different approaches, then as anonymous payment systems, an anonymous credit card system and an e-cash system are developed in the 2nd chapter based on ITLs and anonymous tags, respectively. Here, both anonymous authentication and payment systems offer the most fundamental services for almost all kinds of anonymous systems as same as anonymous communication schemes do. The 3rd chapter develops anonymous auction, object delivery, and monitoring systems as components of e-procurement systems, and the last chapter concerns e-governance systems, and an e-voting system is developed. The important thing that must be reminded is every system cannot assume absolutely trustworthy neutral entities faithful to all participants. An entity that each participant in many of the above systems can trust is only the participant itself. Unfortunately it is not possible to develop object delivery or e-voting systems while completely excluding neutral and trustworthy entities at least for technologies developed until now. Therefore, the object delivery and voting systems in this section are constructed while assuming multiple mutually independent authorities. Namely, participants can convince themselves that they are anonymous when at least one of the authorities is honest.

Anonymous authentication schemes enable managers of systems to determine whether entities accessing them are authorized ones or not without knowing identities of the entities. An important thing is that schemes must be able to handle entities that lose their eligibilities or forget their secrets (e.g. passwords) without invading privacies of honest entities in addition to simple authenticating functions, e.g. passwords of expelled entities must be invalidated. Also although entities to be authenticated are anonymous, they must identify dishonest entities when dishonest events happen. As schemes that satisfy these requirements, anonymous tokens, ITLs, ID-lists, and anonymous credential based ones are developed in the 1st chapter while completely excluding trusted entities. Anonymous token, ITL, and anonymous credential based systems have advantages in protecting systems from ineligible entities, i.e. different from password based systems in which eligible entities can tell their passwords to others, entities in these systems cannot give their secrets to others without losing their eligibilities (in ITL based systems, an entity cannot use secrets of others even if it steals them). On the other hand, ID list based systems have advantages in handling entities those forget their secrets or those are expelled from systems.

In the 2nd chapter, an anonymous credit card system in which cardholders can make purchases while concealing their identities is developed without assuming any absolutely trustworthy entity. A difficult thing is that the system must enable the card company to correctly calculate total expenditures of individual cardholders at the same time. Therefore, in the developed system, cardholders maintain their purchase records by themselves, and report only their total expenditure amounts to the card company.
Then mechanisms to force cardholders to honestly report their total expenditures are necessary. ITLs successfully implement these mechanisms. As an e-payment system, an e-cash system is also developed based on anonymous tag based credentials, and entities in the developed e-cash system can use also e-cash that had been paid to them by others, and they can receive changes from others in e-cash, under both online and offline environments.

An e-procurement system is one in which people can choose their favorite articles, obtain them, and receive maintenance services through networks without going out from their homes or offices, and preserving privacies of individuals is the one of the most urgent issues to be addressed for making people accept this kind of systems. In the 3rd chapter, anonymous English auction system and an anonymous Vickrey auction system are developed based on ITLs and homomorphic re-encryption schemes respectively, so that people can sell or buy articles without disclosing their identities. In both systems, although sellers and buyers are anonymous, sellers are forced to sell their articles to the auction winners at the prices determined by the auctions, on the other hand, buyers are forced to buy their winning articles. Here, the English auction system assumes no absolutely trustworthy entity, but the Vickrey auction system ensures the anonymity of entities when at least one of multiple authorities is honest.

Participants of the above auctions can receive their winning articles also without disclosing their identities through anonymous object delivery systems, i.e. as same as anonymous communication systems, anonymous object delivery systems enable people to send or receive physical objects without disclosing their identities. But different from electric signals conveyed in anonymous communication systems, long durations are necessary to transport physical objects and it is difficult to re-send them when they disappear in the delivery channel. Therefore, object delivery systems must enable senders or receivers to identify their objects in the delivery channel and liable entities when accidents happen on them of course while concealing correspondences between the objects and their senders or receivers. Anonymous tags successfully satisfy these requirements.

Anonymous object monitoring systems are ones that monitor states of objects owned by anonymous entities so that they can use them efficiently, safely and environmentally friendlily, and in this chapter, they are developed based on anonymous memories, anonymous statistics calculation schemes, and ITLs. Here, an anonymous memory is a set of memory sections that are assigned to entities, and owners of the sections can maintain their data securely and efficiently without disclosing their identities. Also anonymous statistics calculation schemes and ITLs enable monitoring stations to calculate statistics of operational states of the objects without knowing their individual values and to identify dishonest users without invading privacies of honest users when dishonest events happen on the objects. By these mechanisms, it is expected that more people will accept various kinds of remote software services, e.g. companies will ask service providers to execute even tasks that require their top secrets.

E-voting system is a typical example of e-governance systems, and e-voting is one of the most promising applications of anonymous security technologies. While being supported by computers and networks e-voting systems make elections more convenient, efficient, and accurate. Actually, e-voting systems are widely used already in the real world. However, current e-voting systems cannot preserve privacies of voters successfully enough. For example, it is not trivial to convince voters that election authorities never know votes of individual voters because all information is computerized and the way computer programs are processing votes cannot be seen from the outside. To make e-voting systems be accepted more widely, in the last chapter, an e-voting system is developed so that the following requirements are satisfied: no one except voters can know votes of voters, anyone can verify that all and only eligible votes are counted, no one can know partial tally before ends of elections, no one coerce voters, and no
one can disrupt elections. Then together with a fact that the system does not require much computations all major requirements of e-voting systems can be successfully satisfied in a practical way. However, it must be noted that these requirements are satisfied under the assumption that at least one of multiple authorities is honest.

As mentioned already, although advances in information and communication technologies had been making human activities efficient and convenient, privacy issues still make many people reluctant to reap benefits from them. Anonymous security technologies solve various problems about privacies, and it is expected that application systems enhanced by these technologies encourage more people to make full use of information and communication technologies aiming at the establishment of more secure, convenient, efficient, and environmentally friendly societies. However, although theoretically it is possible to make anonymous security technologies satisfy various kinds of requirements, there are big arguments about the practicality of anonymous systems. For example, it is difficult to convince people that these anonymous systems are reliable enough. Anonymities may easily make people behave dishonestly, also various unforeseen events may happen in the real world, but in anonymous systems it is difficult to limit damages of individuals and authorities even if liable entities can be identified. Effective and unavoidable things to make anonymous systems practical are gathering and systematization of knowledge that is proven through various experiences in real applications. Only these experiences, beginning from ones in simple and small systems used by closed communities, enable enhancements of anonymous security technologies so that anonymous systems for larger and more complicated and important applications can be accepted.

Shinsuke Tamura
University of Fukui, Japan

REFERENCES
