Information Sciences 412–413 (2017) 223–241

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Insight of the protection for data security under selective opening attacks☆

Zhengan Huang[a], Shengli Liu[b,f], Xianping Mao[c], Kefei Chen[d,e,f], Jin Li[a,*]

[a] School of Computer Science, Guangzhou University, Guangzhou 510006, China
[b] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[c] Shanghai Koal Software Co., Ltd, Shanghai 200436, China
[d] School of Science, Hangzhou Normal University, Hangzhou 310036, China
[e] State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214000, China
[f] Westone Cryptologic Research Center, Beijing 100070, China

ARTICLE INFO

Article history:
Received 16 January 2017
Revised 15 February 2017
Accepted 20 May 2017
Available online 22 May 2017

Keywords:
Data security
Public-key encryption
Non-malleability
Selective opening attack

ABSTRACT

Data security and privacy protection issues are the primary restraints for adoption of cloud computing. Selective opening security (SOA security) focuses on such a scenario of cloud computing: Multiple senders encrypt their own data with the public key of a single receiver. Given the ciphertexts, the adversary is allowed to corrupt some of the senders, seeing not only their plaintexts but also the random coins used during the encryption. The security requirement of SOA security is that the privacy of the unopened data is preserved.

On the other hand, non-malleability is also a very important security notion for data security in cloud computing and public-key cryptography. The security requirement of non-malleability is that given a challenge ciphertext, it should be infeasible to generate a ciphertext vector whose decryption is “meaningfully related” to the corresponding challenge plaintext. However, as far as we know, the relations between non-malleability and SOA security are still undiscovered, and the security notion of non-malleability under selective opening attacks has not yet been formally defined or researched.

In this paper, we formalize the security notion of non-malleability under selective opening attacks (NM-SO security), and explore the relations between NM-SO security and the standard SOA security, the relations between NM-SO security and the standard non-malleability, and the relations among NM-SO security notions.

1. Introduction

1.1. Background and related works

Nowadays, more and more consumers (esp., enterprises and organizations) realize the benefits of cloud computing. However, data security and privacy protection issues are still the primary restraints for adoption of cloud computing. In

☆ An extended abstract of this paper was published in the proceedings of the 13th International Conference on Applied Cryptography and Network Security (ACNS 2015). This is the full version.

[*] Corresponding author.

E-mail addresses: zhahuang.sjtu@gmail.com (Z. Huang), slliu@sjtu.edu.cn (S. Liu), xpmoore@gmail.com (X. Mao), kfchen@hznu.edu.cn (K. Chen), lijin@gzhu.edu.cn, jinli71@gmail.com (J. Li).

http://dx.doi.org/10.1016/j.ins.2017.05.031
0020-0255/© 2017 Elsevier Inc. All rights reserved.

order to meet these special security requirements, lots of cryptographic schemes with some particular properties were put forth, such as attribute-based signatures [23], attribute-based encryption schemes [22], deduplication schemes [21], location-sharing systems [24], multi-keyword ranked search scheme [28], etc. with some particular properties. Because of the special scenarios, security notions of the cryptographic schemes applied in cloud computing should be considered very carefully. In this paper, we focus on the security notions of the encryption schemes applied in cloud storage.

Non-malleability. The basic goal of public-key encryption (PKE) is to protect users' privacy. The notion of semantic security [12], which requires that given a challenge ciphertext, it should be infeasible to learn any partial information about the plaintext of the challenge ciphertext, is a universally accepted formalization of this goal. However, for some application in cloud computing (e.g., bidding), non-malleability is necessary. The notion of non-malleability (NM security) was first introduced by Dolev, Dwork and Naor [9] in 1991. Non-malleability requires that given a challenge ciphertext y, the decryption of which is x, it should be infeasible to generate a ciphertext vector whose decryption is "meaningfully related" to x. Nowadays, there are mainly two kinds of formalizations of non-malleability: simulation-based non-malleability (SIM-NM) [9] and indistinguishability-based non-malleability (IND-NM) [5]. (Actually, there is another formalization of non-malleability, comparison-based non-malleability [1,5], which is seldom used.) Both of these formalizations consider the following standard attacks: chosen-plaintext attacks (CPA), non-adaptive chosen-ciphertext attacks (CCA1) [25] and adaptive chosen-ciphertext attacks (CCA2) [9,10,13,27]. Therefore, the combination of SIM/IND-NM and CPA/CCA1/CCA2 gives six specific security notions (e.g., SIM-NM-CPA security). The relations among the six security notions have been investigated in [5,26].

Selective opening security. This security notion focuses on multi-user scenarios of cloud computing. Consider a set of clients connecting to a server. Each client encrypts its own message with the servers public key and sends the generated ciphertext to the server. Observing all the ciphertexts, the adversary is also able to corrupt some of the clients, by opening their ciphertexts, i.e., obtaining those clients messages and the random coins used during the encryption. This type of attacks is called selective opening attack (for sender corruptions). Security against selective opening attacks (SOA security) requires that the unopened ciphertexts remain secure. The notion of SOA security (for sender corruptions) was formalized by Bellare et al. [4] in Eurocrypt 2009. (Actually, there is another kind of SOA security, SOA security for receiver corruptions [4,18], which we will not discuss in this paper.) They proposed two notions of SOA security in [4], the simulation-based one (SIM-SO) and the indistinguishability-based one (IND-SO), both of which are defined under chosen-plaintext attacks. Later, the notions of IND-SO-CCA1/CCA2 security and SIM-SO-CCA1/CCA2 security were introduced by Hemenway et al. [[15]] in Asiacrypt 2011. Over the years, some SOA secure PKE schemes were proposed [[11,14–16]], and the relations among SOA security notions have also been investigated. Bohl et al. [3] clarified the relations between IND-SO-CPA security and SIM-SO-CPA security. Bellare et al. [2] separated IND-CPA/CCA1/CCA2 security and SIM-SO-CPA security. In TCC 2014, Hofheinz and Rupp [19] proposed a PKE construction which is IND-CCA2 secure but IND-SO-CCA2 insecure, and showed a partial equivalence between IND-CPA security and IND-SO-CPA security. In TCC 2016-B, Hofheinz, Rao and Wichs [20] proposed a construction which is IND-CCA2 secure but IND-SO-CPA insecure, separating IND-CCA2 security and IND-SO-CPA security.

To the best of our knowledge, the security notion of non-malleability under selective opening attacks has not yet been formally defined. Hofheinz and Rupp referred to "NM-SO-CPA security" in [19] without presenting any formal definition, and left it for future work.

1.2. Our contributions

We formally define the security notions of non-malleability under selective opening attacks. More specifically, we formalize the security notion of simulation-based non-malleability under selective opening attacks (SIM-NM-SO), and the security notion of indistinguishability-based non-malleability under selective opening attacks (IND-NM-SO). Then, we investigate the relations among the notions of NM-SO security (i.e., SIM/IND-NM-SO-CPA/CCA1/CCA2 security), the notions of SOA security (i.e., SIM/IND-SO-CPA/CCA1/CCA2 security), and the notions of NM security (i.e., SIM/IND-NM-CPA/CCA1/CCA2 security). Our conclusions are as follows (see Fig. 1). Below, for any two security notions SecNo1 and SecNo2, let SecNo1 $\Rightarrow$ SecNo2 indicate that any PKE scheme possessing SecNo1 also achieves SecNo2, and SecNo1 $\nRightarrow$ SecNo2 indicate that there exists some PKE scheme possessing SecNo1 but not SecNo2.

1. *NM-SO security vs. SOA security*:
   (a) *Simulation-based* (Section 4):
      (1) "SIM-NM-SO-ATK $\underset{\nLeftarrow}{\Rightarrow}$ SIM-SO-ATK", for any ATK $\in$ {CPA, CCA1, CCA2}. In fact, we have a stronger conclusion: "SIM-SO-CCA2 $\nRightarrow$ SIM-NM-SO-CCA1".
      (2) For PKE schemes having an invertible decryption algorithm (Definition 8), if the range of its decryption algorithm is recognizable, "SIM-SO-CCA2 $\Leftrightarrow$ SIM-NM-SO-CCA2".
   (b) *Indistinguishability-based* (Section 5):
      (1) "IND-NM-SO-CPA $\underset{\nRightarrow}{\nLeftarrow}$ IND-SO-CCA1".
      (2) "IND-NM-SO-CCA1/CPA $\underset{\nLeftarrow}{\Rightarrow}$ IND-SO-CCA1/CPA", but "IND-NM-SO-CCA2 $\Leftrightarrow$ IND-SO-CCA2".
2. *NM-SO security vs. NM security*:
   (a) *Simulation-based* (Section 6):
      (1) "SIM-NM-SO-ATK $\underset{\nLeftarrow}{\Rightarrow}$ SIM-NM-ATK", for any ATK $\in$ {CPA, CCA1, CCA2}. In fact, we have a stronger conclusion: "SIM-NM-ATK$'$ $\nRightarrow$ SIM-NM-SO-ATK$''$", for any ATK$'$, ATK$''$ $\in$ {CPA, CCA1, CCA2}.