Theoretical Computer Science 581 (2015) 9–25

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Anonymous protocols: Notions and equivalence ☆

Paolo D'Arco *, Alfredo De Santis

Dipartimento di Informatica, Via Giovanni Paolo II, 132, I-84084, Fisciano (SA), University of Salerno, Italy

ARTICLE INFO

Article history:
Received 25 October 2013
Received in revised form 31 July 2014
Accepted 14 February 2015
Available online 2 March 2015
Communicated by J. Camenisch

Keywords:
Anonymous protocols
Key privacy
Secret sets
Anonymous broadcast encryption

ABSTRACT

Privacy protection has become a major issue in modern societies. Many efforts have been provided in the last years to catch properly the requirements that cryptographic primitives and low-level protocols should meet in order to be useful for building privacy-preserving applications. In particular, anonymity is an important property to achieve, and the notion of *key privacy* in public-key encryption, which guarantees that an adversary is unable to tell with which public key a certain ciphertext has been produced, plays a key-role in the design of anonymous protocols.

Secret sets and *anonymous broadcast encryption* are two examples of useful anonymous protocols. A secret set is a representation of a subset of users of a given universe satisfying some basic membership privacy properties, and anonymous broadcast encryption is a mechanism to encrypt a broadcast message that only authorized users, whose identities are kept secret, can decrypt.

In this paper we show that, even if apparently the key privacy property of an encryption scheme seems to be unrelated to the security of the encrypted content, and it looks like just an additional property the encryption scheme can enjoy, for a *robust* encryption scheme key privacy under chosen ciphertext attack *implies* non-malleability and, hence, security under chosen ciphertext attacks. This result helps to simplify the set of requirements that public key encryption schemes need to satisfy when stating and proving theorems regarding anonymous protocols in which the encryption schemes are used.

Then, we provide a formal model for both secret sets and anonymous broadcast encryption and we prove that they are *equivalent* with respect to non-adaptive adversaries: the former can be used to design the latter and vice versa.

Finally, we revisit some previous constructions for secret sets, and we analyze the security properties they enjoy within our adversarial model.

1. Introduction

A challenging world. In all its forms privacy has become a major issue in information technology. Several events of the last couple of years, in which secret and classified information has been disclosed, e.g., *Wikileaks* [20] or the *Snowden affair* [19], have shown that authorities have access to phone calls, e-mails and other communications far beyond constitutional bounds. Many nations, including those expressing the strongest protests in the name of user rights, collect intelligence on each

☆ A preliminary version of this paper appeared with the title *Key Privacy and Anonymous Protocols* in the Proc. of the IEEE 11th International Conference on Privacy, Security and Trust (PST2013), July 10–12, 2013.

* Corresponding author.
E-mail addresses: paodar@dia.unisa.it (P. D'Arco), ads@dia.unisa.it (A. De Santis).

http://dx.doi.org/10.1016/j.tcs.2015.02.042
0304-3975/

other. Adversarial entities, for plenty of reasons, might trace or build a profile of movements, interests and, more generally, of user behaviors. Attacks of these types are a strong threat to the user freedom. People should be protected against these attacks made possible by the current methods of communication and of information processing. At the same time "political springs", as they have been called, in the middle east area and in other parts of the world, have shown that social networks and new communication media in general are a powerful tool for young generations to discuss, exchange ideas, plan and organize actions, which might also lead to social changes.[1] It is therefore becoming compelling to put forward methods for guaranteeing user privacy and protocols for anonymous computation and communication.

However, general notions and efficient methods for building privacy-preserving applications have been proposed in the past. Among them, the notion of *key-privacy* in public-key encryption [2] is an important feature a public-key encryption scheme may exhibit, which is helpful in building applications providing user anonymity, through which an adversary is unable to tell *which* public key has been used to compute a given ciphertext. Moreover, many privacy-preserving low-level cryptographic protocols, like secret sets and anonymous broadcast encryption, have been introduced.

Secret sets. Fifteen years ago, Molva and Tsudik [16] put forward the notion of *secret set* as a method to enhance user privacy. Loosely speaking, a secret set is a *representation* of a subset of users of a given universe such that *any* user of the universe can check whether he is or is not a member of the subset, *no one* can check if another user of the universe is or is not a member, and *no one* can determine the size of the subset. The last two properties should hold also against coalitions of users. The authors proposed some constructions and showed how secret sets can be useful to protect receivers' privacy in multicast communications, and against traffic analysis of mobile devices. Later on, De Santis and Masucci [9] provided a formal treatment of the notion. They defined unconditionally secure secret sets by using the language of information theory, showed lower bounds in terms of needed number of bits on user storage, on representation length of a secret set, and on the randomness needed to set up a scheme, and proved the bounds are tight. Moreover, they defined computationally secure secret sets in terms of *indistinguishability* of representations associated to different sets, and showed that such schemes exists if and only if semantically secure symmetric encryption exists. Micali et al. in [15] put forward the notion of *zero-knowledge set*, which is somehow related. A zero-knowledge set is a method through which a prover can construct a representation of a set of strings S of a given universe $\mathcal{U}$ such that, for any string $x \in \mathcal{U}$, he is able to prove non-interactively and in zero-knowledge whether $x \in S$ or $x \notin S$. In particular, the representation of S does not leak any other information about S, e.g., the size of S. The authors showed that zero-knowledge sets exist if the discrete logarithm problem is hard. Several papers have further focused on Micali et al.'s work, e.g., see [5–7,17].

Anonymous broadcast encryption. Broadcast Encryption schemes enable a center to deliver encrypted data to a large set of users, in such a way that only a privileged subset of them can decrypt the data. Applications for these schemes range from pay-tv to systems for delivering sensitive information stored on media like a CD/DVD. Broadcast encryption works as follows: during a set-up phase, every user receives a set of predefined keys. Then, at the beginning of each data transmission, the center sends a broadcast message enabling privileged users to compute a session key, by means of which, the encrypted data, that will be delivered later on, can be decrypted. In many content distribution systems it is important to both restrict access to content to authorized users and to protect *their identities*. Unfortunately, a broadcast encryption scheme *does not* guarantee any form of privacy for the set of recipients. Actually, in almost all existing constructions, the broadcast message contains an *explicit description* of the set of recipients, which is used by each recipient to identify the part of the broadcast message he/she is able to decrypt with the predefined keys received during the set-up phase, in order to retrieve the session key. In [4] the authors introduced *private broadcast encryption*. A private broadcast encryption scheme is exactly a mechanism to encrypt a broadcast message such that only authorized users can decrypt the message and read the content and, at the same time, the identities of the recipients are kept secret, even from each other. Such a notion has been further studied in [14], under the name of *anonymous broadcast encryption*.

Motivations and goals. In this paper, by using the currently available knowledge and tools, developed during the last years, we take a further look at the key-privacy notion, at secret sets, focusing our attention on constructions in the public-key setting, and at anonymous broadcast encryption. Indeed, several issues are still open: key privacy was introduced as an additional property a secure encryption scheme might exhibit, but it was not clarified what kind of relation this notion has with security. With respect to secret sets, the authors of [16] proposed some constructions based on encryption schemes and the Chinese Remainder Theorem and suggested two important applications, but the treatment they provided was quite informal. Security reductions within a formal adversarial model were not provided. On the other hand, De Santis and Masucci [9] provided a formal treatment, but in the computational case the authors looked mainly at the symmetric setting. Moreover, in both papers, no efficient construction hides the size of the set S, which is disclosed to the users. Regarding anonymous broadcast encryption, the authors of [4] gave a look at the current practice, by discussing a PGP implementation which supports private broadcast encryption and is secure against a *passive* adversary, proposed two new constructions which are secure against an *active* adversary, and discussed a useful application, i.e., how to realize encrypted file systems preserving user privacy. Later on, [14] revised the notion of private broadcast encryption, which was referred to as *anonymous broadcast*

[1] To get an idea of the consideration some governments have of the new media, the words of the Turkish prime minister in May 2013, reported by many newspapers everywhere in the world, e.g., [18], are a clear example: *There is now a menace which is called Twitter*, Erdogan said. *The best examples of lies can be found there. To me, social media is the worst menace to society.*