JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 24-25 (2015) 1–12

Available online at www.sciencedirect.com

ScienceDirect

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

Fully secure anonymous spatial encryption under affine space delegation functionality revisited

Y. Sreenivasa Rao *, Ratna Dutta

Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721302, India

ARTICLE INFO

Article history:
Available online 21 October 2015

Keywords:
Spatial encryption
Composite order bilinear group
Recipient anonymity
Full security
Affine space delegation

ABSTRACT

Recently, in Information Sciences, Zhang et al. (2014) claimed that they proposed the first anonymous spatial encryption under affine space delegation functionality with full security, which solves the open problems of *full security* proposed in Boneh and Hamburg (2008) and *anonymity* left in Boneh and Hamburg (2008) and Moriyama and Doi (2011). In this paper, we show their construction cannot achieve recipient anonymity as the ciphertext terms leak information about the encryption vector. Hence realizing anonymous spatial encryption with full security is still an open problem. We propose a new fully secure anonymous spatial encryption under an affine space delegation mechanism that addresses the open problem positively. Our construction utilizes composite order bilinear groups where the group order is a product of four primes and achieves the same efficiency as that of the Zhang et al. (2014) construction. Under some well-established cryptographic assumptions, the proposed construction is proven to be fully semantically secure with anonymity in the standard model within the dual encryption system framework.

1. Introduction

Identity Based Encryption (IBE) is central to public key encryption that overcomes the issues inherited from public key infrastructure based systems. In such a primitive, the public key is some known attribute of the intended recipient of the ciphertext and only the user owned a secret key related to the matching attribute can be successful in decryption. The one-to-one communication nature of IBE has greatly made its applications limited in practice. Boneh and Hamburg (2008) generalized the notion of identities and developed a framework called Generalized IBE (GIBE), in which a message is encrypted under a certain *policy* and users hold secret keys corresponding to *roles*. A secret key related to a role ρ can decrypt a ciphertext associated with a policy π only when role ρ satisfies policy π. The set of all allowed roles is organized in a partially-ordered set, a set equipped with reflexive, antisymmetric and transitive relation $\succeq$, to realize delegation functionality, i.e., one can derive a secret key for role ρ' from the secret key of role ρ if $\rho \succeq \rho'$. Many subclasses of public key encryption systems can be embedded in GIBE, such as IBE and broadcast IBE (Boneh and Franklin, 2001; Delerable, 2007; Shamir, 1985), hierarchical IBE (Gentry and Silverberg, 2002; Lewko and Waters, 2010), attribute based encryption (Bethencourt et al., 2007; Goyal et al., 2006), predicate encryption (Katz et al., 2013) and forward secure systems (Canetti et al., 2003).

Boneh and Hamburg (2008) devised a specific instance of GIBE called *spatial encryption* in which encryption policies are vectors $\vec{x}$ in $\mathbb{Z}_p^n$, for some integer n and prime p, and secret

Preprint submitted to Journal of Information Security and Applications April 1, 2015.
* *Corresponding author.* Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721302, India. Tel.: +91 9494776866.
E-mail address: y.sreenivasarao@yahoo.co.in (Y.S. Rao).
http://dx.doi.org/10.1016/j.jisa.2015.08.002
2214-2126/

key roles are affine subspaces V of $\mathbb{Z}_p^n$. The delegation relation $\succeq$ in this case is defined by subspace inclusion, i.e., $\rho \succeq \rho'$ if and only if $V_\rho \supseteq V_{\rho'}$, where V_ρ and $V_{\rho'}$ are affine subspaces corresponding to the roles ρ and ρ', respectively. A role ρ can decrypt every ciphertext created under a vector $\vec{x} \in V_\rho$. Many important instances of GIBE can be constructed from spatial encryption that includes hierarchical IBE, broadcast hierarchical IBE, forward-secure IBE, short identity based ring signatures, multiple authorities IBE and many more. An appealing property of spatial encryption is that the *size of ciphertext is constant*, i.e., independent of the space dimension. This makes the systems generated from spatial encryption more efficient than the existing systems of similar kind.

The proof of security of the first spatial encryption scheme (Boneh and Hamburg, 2008) is relied on the decisional q-Bilinear Diffie–Hellman Exponent (q-BDHE) assumption in a *selective* security model in which the adversary is forced to specify his challenge before the simulation is set up. Zhou and Cao (2009) proposed a spatial encryption construction that is proven to be selectively secure under the standard decisional BDH assumption. Unlike Boneh and Hamburg (2008), the size of ciphertext in this scheme is proportional to the space dimension. Chen et al. (2014) proposed novel property-preserving transformation techniques that enable generic construction of a spatial encryption scheme from a hierarchical inner product encryption scheme, and vice versa. Later, Chen et al. (2013) studied the relation between ciphertext policy inner product encryption and spatial encryption.

By adapting the dual system encryption mechanism introduced by Waters (2009), Attrapadung and Libert (2011), and Moriyama and Doi (2011) independently made the scheme of Boneh and Hamburg (2008) *fully* secure based on composite order (product of three primes) bilinear groups. Their security proofs used a hybrid argument over a sequence of games and relied on simple static assumptions, where the assumptions are independent of the number of adversary's secret key queries.

Recently, Zhang et al. (2014) added recipient (or vector) *anonymity* to the spatial encryption (Boneh and Hamburg, 2008), called anonymous spatial encryption, inspired by De Caro et al. (2010) by means of composite order (product of four distinct primes) bilinear groups. The authors claimed that their construction is an affirmative answer for the open problems of full security in Boneh and Hamburg (2008) and anonymity in Boneh and Hamburg (2008) and Moriyama and Doi (2011). Anonymity here refers to the property that the adversary must be unable to decide whether a ciphertext was encrypted for a chosen vector, or for a random vector. Specifically, no adversary can identify which specific affine vector has originally been used to generate the given ciphertext from a set of known affine vectors. Hence the receiver (or vector) information is anonymous from the adversary's point of view. The scheme features full security in the standard model and constant-size ciphertext. The security proof relies on the dual system encryption framework.

Hamburg (2011) suggested a variant of spatial encryption, called doubly spatial encryption in which encryption policies are also affine subspaces and a secret key can decrypt a ciphertext if its affine space intersects the affine space of the ciphertext.

1.1. *Our contribution*

We first show that the recently proposed anonymous spatial encryption by Zhang et al. (2014) *cannot* realize recipient anonymity. We show in Section 3 that the construction is vulnerable to the Decision Diffie–Hellman (DDH)-test attacks (Abdalla et al., 2008) on the challenged ciphertext, enabling one to distinguish the encryption of a message for a first chosen vector from the encryption of the same message for a second chosen vector of the same length. The DDH-test is a powerful tool for validating the ciphertext components in pairing based constructions. In Abdalla et al. (2008), several existing pairing based primitives are proved not recipient anonymous employing DDH-test attacks.

Due to our attack on the Zhang et al. (2014) construction, the problem of designing anonymous spatial encryption with full security still remained open. We present an anonymous spatial encryption scheme with delegation mechanism that achieves full security under simple static assumptions over composite order bilinear groups whose order is a product of four primes, which settles the open problem positively. The security captures both message confidentiality and recipient (or vector) anonymity against adaptive affine vector attacks by means of dual system proof techniques (Waters, 2009). We transform the non-anonymous spatial encryption scheme of Boneh and Hamburg (2008) into anonymous construction by blinding the actual public parameters and ciphertext terms with another subgroup elements. As a result, every outcome of the DDH-test on the public parameters and the ciphertext components is randomized by some pairings on the blinded elements and thus the test fails always unconditionally. Consequently, no one can draw the conclusions based on these equally distributed outcomes. This prevents the DDH-test attacks and attains recipient anonymity. The blinding terms, however, are removed in the decryption process due to the orthogonal property of subgroups of the composite order group. The new scheme achieves the same efficiency as that of Zhang et al.'s (2014) scheme during encryption and decryption.

Since the actual public parameters are made blinded and so no longer available, the secret key holders cannot delegate their secret keys. To ensure delegation mechanism, the public parameters needed for it are distributed with proper randomness as a part of the secret key. This doubles the size of the secret key in our anonymous construction. It is not easy to simulate the security reduction when combining ciphertext indistinguishability with recipient anonymity in non-selective (full) security model. To this end, we define five suitable complexity assumptions over bilinear groups of order product of four primes following (Lai et al., 2012). These assumptions can be shown to hold in the generic group model under the hardness of factorization problem as described in Lewko et al. (2010).

Table 1 presents the property comparison of our scheme against the previous spatial encryption schemes (Attrapadung and Libert, 2011; Boneh and Hamburg, 2008; Chen et al., 2013; Moriyama and Doi, 2011; Zhang et al., 2014; Zhou and Cao, 2009).

1.2. *Paper organization*

The rest of the paper is organized as follows. The necessary background is reviewed in Section 2. In Section 3, we discuss