Theoretical Computer Science 630 (2016) 95–116

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Constructions of dynamic and non-dynamic threshold public-key encryption schemes with decryption consistency ☆

Yusuke Sakai [a,*,1], Keita Emura [b], Jacob C.N. Schuldt [a], Goichiro Hanaoka [a], Kazuo Ohta [c]

[a] AIST, Japan
[b] NICT, Japan
[c] The University of Electro-Communications, Japan

ARTICLE INFO

Article history:
Received 19 October 2015
Received in revised form 1 February 2016
Accepted 1 April 2016
Available online 11 April 2016
Communicated by X. Deng

Keywords:
Threshold public-key encryption
Public-key encryption with non-interactive opening
Verifiable secret sharing
Decryption consistency

ABSTRACT

Dynamic threshold public-key encryption, proposed by Delerablée and Pointcheval (CRYPTO 2008), is an extension of ordinary threshold encryption which enables decryption servers to join the system even after the setup phase, and to choose the authorized set and the threshold of decryption dynamically. Delerablée and Pointcheval proposed the first dynamic threshold public-key encryption scheme, which they proved secure under a non-standard q-type assumption. However, decryption consistency, which is an important security property that guarantees uniqueness of decryption, even when a sender and decryption servers behave maliciously, is only shown to hold in the random oracle model. In this paper, we propose three threshold public-key encryption schemes. The first and second schemes are both dynamic schemes. The former achieves a relatively weaker variant of decryption consistency, while the latter achieves a strong variant thereof. The former is a generic construction from public-key encryption with non-interactive opening (PKENO), while the latter is a specific construction from a standard number-theoretic assumption. These are the first constructions of dynamic public-key encryption, which achieve decryption consistency without relying on the random oracle model. Furthermore, both schemes can be realized based on standard assumptions. The third construction is a generic construction from PKENO achieving the strong variant of decryption consistency. This construction affirmatively answers the question indirectly posed by Galindo et al. (AFRICACRYPT 2010) of whether a generic construction achieving strong decryption consistency is possible.

☆ An extended abstract of this work appears in The 20th Australasian Conference, ACISP 2015 [1]. This is the full version which includes a third construction as well as full proofs of security of the proposed schemes.

* Corresponding author.
E-mail address: yusuke.sakai@aist.go.jp (Y. Sakai).

[1] The first author is supported by a JSPS Fellowship for Young Scientists.

http://dx.doi.org/10.1016/j.tcs.2016.04.003
0304-3975/

1. Introduction

1.1. Dynamic threshold encryption

In a threshold public-key encryption (TPKE) scheme, the decryption key of the scheme is distributed among several (say n) servers, in order to avoid a single point of failure [2–5], and to decrypt a ciphertext, k (among n) servers needs to cooperate in the decryption. Among such schemes, we consider non-interactive TPKE schemes, in which the decryption process is non-interactive. Namely, when receiving a ciphertext, each decryption server submit a decryption share, and by combining these shares the plaintext can be recovered.

A TPKE scheme is not only required to provide plaintext confidentiality, but also to satisfy *decryption consistency* [6,5], which intuitively requires uniqueness of decryption. More precisely, even if a sender and the decryption servers collude, it should be hard to produce two sets of decryption shares which, when combined, respectively result in two different plaintexts. In other words, decryption consistency prevents a malicious sender from producing an "equivocal" ciphertext, which essentially corresponds to two different plaintexts, and then controlling the decryption result by forcing a specific set of servers to participate in the decryption process.

Most of the TPKE schemes suffer from the limitation that the set of decryption servers and the threshold need to be fixed when the system is set up. This inflexibility potentially limits their applications.

To address this restriction, Delerablée and Pointcheval [7] proposed *dynamic TPKE*. Dynamic TPKE enables new decryption servers to join the system after the system is set up, and also enables a sender to choose the threshold at the time of encryption. Delerablée and Pointcheval also presented a specific instantiation of dynamic TPKE. Unfortunately, this scheme relies on a non-standard q-type assumption named the multi-sequence of exponent Diffie–Hellman (MSE-DDH) assumption. In addition, providing decryption consistency of this scheme requires the random oracle heuristics. In summary, *the only known dynamic TPKE with decryption consistency relies on both a q-type assumption and random oracles.*

1.2. Our contribution

In this paper, we present first dynamic TPKE schemes with decryption consistency, which avoid the use of random oracles and q-type assumptions. In particular, we propose two dynamic TPKE constructions, both of which utilize public-key encryption with non-interactive opening (PKENO) [8]. PKENO is an extension of public-key encryption, which enables the receiver to prove that a given ciphertext is decrypted to a given plaintext without revealing the decryption key. A PKENO scheme can be constructed from the decisional linear assumption and the decisional bilinear Diffie–Hellman assumption [9, 10], and so can for our proposed constructions.

The first construction is a black-box construction from any PKENO scheme. This construction combines a PKENO scheme and a technique from verifiable secret sharing [11,12] to achieve decryption consistency. Unfortunately, this construction achieves only a relatively weak level of decryption consistency, when compared with known (non-dynamic) constructions, for example, the Boneh–Boyen–Halevi scheme [6]. Another weakness of this construction is a large ciphertext overhead. Namely, the ciphertext size is $O(n^2)$, where n is the number of decryption servers which can participate in the decryption process.

To overcome the weakness of our first construction, we propose another construction. The second scheme is not achieved via a black-box construction, but it is constructed from a specific number-theoretic assumption. This scheme achieves a strong definition of decryption consistency, which is similar in strength to that of the Boneh–Boyen–Halevi schemes. Another merit of this scheme is that the ciphertext size is $O(n)$. *This is the first dynamic TPKE scheme with strong decryption consistency which is proven secure under a standard assumption without random oracles.*

Our results suggest effectiveness of using PKENO to construct TPKE schemes, as the two constructions both rely on PKENO, especially to achieve decryption consistency. Note that this effectiveness has been conjectured by Galindo et al. [9], but is not studied in detail. In addition, our results highlight some subtleties regarding this conjecture. Specifically, in both of our constructions a simple combination of secret sharing and PKENO is not sufficient, rather we need to introduce a non-trivial technique to achieve decryption consistency.

Our two constructions further lead to a new question: Is it possible to achieve the strong decryption consistency with a purely black-box construction? That is, the first construction is purely black-box but does not have the strong decryption consistency, while the second construction has the strong decryption consistency, but is not purely black-box. To answer this new question, we propose a third construction, which is a black-box construction while *simultaneously* achieving the strong decryption consistency. A drawback of this third scheme is that it is a static (i.e., non-dynamic) scheme and ciphertext size is large, i.e., proportional to $\binom{n}{k-1}$, in which n is the number of the decryption servers and k is the threshold.

The first two schemes are proven secure under an extension of the Boneh–Boyen–Halevi model for dynamic TPKE [6]. We stress that we considered a security model with static corruption (rather than adaptive), in which the set of corrupted user should be declared in the beginning of the security game. In contrast, the Delerablée–Pointcheval scheme allows adaptive corruption. To construct a dynamic TPKE secure in an adaptive corruption model with decryption consistency still remains an open problem.

Table 1 summarizes the performance and security of these three schemes and some of the existing schemes. The second, third, and fourth columns respectively show the sizes of the public parameter and public keys, the ciphertext, and the