Information Processing Letters 130 (2018) 16–24

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Leakage-resilient CCA2-secure certificateless public-key encryption scheme without bilinear pairing

Yanwei Zhou [a,b], Bo Yang [a,b,*]

[a] School of Computer Science, Shaanxi Normal University, Xi'an 710062, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 13 July 2015
Received in revised form 25 April 2017
Accepted 25 September 2017
Available online 28 September 2017
Communicated by X. Wu

Keywords:
Cryptography
Certificateless public-key encryption
Leakage-resilience
Chosen ciphertext attacks

ABSTRACT

In practical applications, an encryption scheme should withstand various leakage attacks (e.g., side-channel attacks, cold-boot attacks, etc.). Thus, in this paper, a new leakage-resilient certificateless public-key encryption (LR-CL-PKE) scheme is presented, and whose security is based on the classic decisional Diffie–Hellman (DDH) assumption. Considering the computational costs, because without bilinear pairing, our construction is more efficient than traditional LR-CL-PKE schemes. Based on the hardness of the DDH assumption, the security of our proposal is proved. Furthermore, in the leakage setting, our construction can keep its claimed security even if the adversary can learn a certain amount of additional information on the secret key through various leakage attacks.

1. Introduction

To simplify the certificate management in traditional public key infrastructure, Shamir [1] introduced the concept of identity-based encryption (IBE) scheme which is a new cryptographic primitive. The public key is user's digital identity (such as telephone number, email address, etc.) which can reduce the managing costs of certificates. However, the IBE scheme requires a trusted third party to generate the secret key for all identities. Therefore, the key escrow problem is integrated in the IBE scheme.

To relieve the key escrow problem of IBE scheme and certificate authorities in traditional public-key encryption (PKE) scheme, a new notion of certificateless public-key encryption (CL-PKE) scheme is presented [2]. In a CL-PKE scheme, it also requires a trusted third party named key generation center (KGC) to generate the partial secret key and the partial public key for all identities. Thus, the user's secret key can be computed from the partial secret key and the secret value, where the secret value is generated by user itself. Therefore, the KGC does not generate the full secret key for the user. Instead, the KGC supplies the user only with a partial secret key which is computed from the user's identity. Thus, the CL-PKE scheme can successfully resolve the key escrow problem while avoiding the use of certificates.

Traditionally, cryptographic infrastructures are researched in an ideal model where participants have an internal secret state that is assumed to be completely inaccessible by the adversary. That is, in this model, an efficient adversary can only see the appointed input and output of a cryptographic scheme but cannot to access the internal secret information (e.g., secret key, etc.). In the real life, an adversary will learn some partial information about the internal secret information through various leakage attacks, such as side-channel attacks, cold-boot attacks, etc. If the adversary can obtain a certain amount of leakage on the secret key, the traditional cryptographic schemes may not be unable to keep their original security. To solve this problem, the leakage-resilient cryptographic primitives are constructed by cryptographic researchers in recently years,

* Corresponding author at: School of Computer Science, Shaanxi Normal University, Xi'an 710062, China.
E-mail addresses: zyw@snnu.edu.cn (Y. Zhou), byang@snnu.edu.cn (B. Yang).

https://doi.org/10.1016/j.ipl.2017.09.012
0020-0190/

such as leakage-resilient public-key encryption (LR-PKE) [3–5], leakage-resilient identity-based encryption (LR-IBE) [6,7], leakage-resilient certificate-based encryption [8,9], leakage-resilient authenticated key exchange [10], etc.

According to the results of [11], [12] and [13], Naor and Segev [5] made a distinction between leakage-resilient chosen-plaintext attacks (LR-CPA) and leakage-resilient chosen-ciphertext attacks (LR-CCA). They suggested that any public-key encryption (PKE) schemes based on the hash proof systems (HPS) [14] can be made secure against LR-CPA with the help of randomness extractors. Two LR-PKE schemes are constructed in [5]. The first scheme is secure resist adaptive prior leakage-resilient chosen-ciphertext attacks (LR-CCA1). The second scheme is secure resist adaptive posteriori leakage-resilient chosen-ciphertext attacks (LR-CCA2). Later, two new variants are designed by Liu et al. [3] and Li et al. [4], these schemes are more efficient than the original LR-PKE scheme [5] in terms of computational costs. Furthermore, the first leakage-resilient certificateless public-key encryption (LR-CL-PKE) scheme is presented in [15], this scheme considers different leakage conditions for Type I (third-party attackers) and Type II (honest-but-curious PKG) attackers, following the classification in traditional CL-PKE scheme. Xiong et al. [15] provided a concrete construction based on the bilinear pairing, and prove its security in the standard model. However, this scheme is only achieve the LR-CPA security and LR-CCA1 security.

2. Preliminaries, assumption and tools

In this section, we first introduce some notations, computational assumption on which the security of our proposal is mainly based. Next, we present the definitions and some properties of statistical distance, minimum entropy, universal hash and average-case strong extractor which are important tools that will be used in our construction and security analysis. Finally, we give the description on the leakage oracle.

2.1. Notations

Let $k \in \mathbb{N}$ denote the security parameter and 1^k denote the string of k ones. For an integer n, we use the notation $[n]$ to denote the set $\{1, 2, \cdots, n\}$. If S is a string, then $|S|$ denotes its length, while if S is a set then $|S|$ denotes its size and $s \leftarrow_R S$ denotes the operation of picking an element s uniformly at random from S. We denote $y \leftarrow \mathcal{A}(x)$ the operation of running $\mathcal{A}$ with input x and assigning y as the result. We use $negl(k)$ to denote the set of all functions which are negligible in security parameter k. An algorithm $\mathcal{A}$ is probabilistic polynomial-time (PPT) if $\mathcal{A}$ is randomized and the computation of $\mathcal{A}$ for any input terminates in at most polynomial steps.

2.2. Target collision resistant

Definition 1 *(Target collision-resistant [13]).* Let $\mathcal{H}_{\mathcal{I}} = \{H_i : \mathcal{X} \to \mathcal{Y}\}_{i \in \mathcal{I}}$ be a set of one-way hash functions, then $\mathcal{H}_{\mathcal{I}}$ is target collision-resistant if any PPT adversary $\mathcal{A}$ has negligible probability $Adv^{TCR}_{\mathcal{H}_{\mathcal{I}}}(k) = \Pr[H_i(x) = H_i(x') \wedge x \neq x']$ for any $i \in \mathcal{I}$, where $x \leftarrow_R \mathcal{X}$ and $x' \leftarrow \mathcal{A}(x, H_i)$.

2.3. Computational assumptions

Let $\mathcal{G}(1^k)$ be a PPT algorithm that outputs a tuple $\mathbb{G} = (q, G, P)$, where q is a big prime, G is a group of order q, and P is a generator of G.

Definition 2 *(Decisional Diffie–Hellman, DDH [13]).* Given two 4-tuple (P, aP, bP, abP) and (g, g^a, g^b, Q_{DDH}) for some unknown elements $a, b \leftarrow_R Z_q^*$ and $Q_{DDH} \leftarrow_R G$, the purpose of DDH problem is decided whether $Q_{DDH} = abP$ or not. The DDH assumption states that for any PPT adversary $\mathcal{A}$, the advantage $Adv^{DDH}(k) = |\Pr[\mathcal{A}(P, aP, bP, abP) = 1] - \Pr[\mathcal{A}(P, aP, bP, Q) = 1]|$ of $\mathcal{A}$ to solve the DDH problem is negligible.

2.4. Randomness extraction

The statistical distance of two random variables X and Y is $SD(X, Y) = \frac{1}{2}\sum_{w \in \Omega} |\Pr[X = w] - \Pr[Y = w]|$, where X and Y are two random variables over a finite domain Ω. The min-entropy of a random variable X is $H_\infty(X) = -\log(\max_x \Pr[X = x])$ [16].

Definition 3 *(Average min-entropy [16]).* The average conditional min-entropy of random variable X conditioned on a variable Z is $\widetilde{H}_\infty(X|Z) = \log(\mathbf{E}_z \max_x \Pr[X = x|Z = z]) = -\log(\mathbf{E}_{z \leftarrow Z}[2^{-H_\infty(X|Z=z)}])$, where $\widetilde{H}_\infty(X|Z)$ denotes the remaining unpredictability of random variable X conditioned on another variable Z. Namely, for any PPT adversary $\mathcal{A}$, we can get $\Pr(\mathcal{A}(Z) = X) = \mathbf{E}_z[\Pr(\mathcal{A}(Z) = X)] \leq \mathbf{E}_z[2^{-H_\infty(X|Z=z)}] = 2^{-\widetilde{H}_\infty(X|Z)}$.

Lemma 1 *([16]). Let X, Y and Z be random variables, if Y has at most 2^λ possible values, then we will have $\widetilde{H}_\infty(X|(Y, Z)) \geq \widetilde{H}_\infty(X|Z) - \lambda$.*

Definition 4 *(Randomness extractor [16]).* An efficient computable function $Ext : \{0,1\}^{l_n} \times \{0,1\}^{l_t} \to \{0,1\}^{l_m}$ is an average-case (k, ε)-strong extractor if for all pairs of random variables (X, Y) such that $X \in \{0,1\}^{l_n}$ and $\widetilde{H}_\infty(X|Y) \geq k$, we have $SD((Ext(X, S), S, Y), (U_m, S, Y)) \leq \varepsilon$, where $S \leftarrow_R \{0,1\}^{l_t}$, $U_m \leftarrow_R \{0,1\}^{l_m}$, and ε is negligible.

Definition 5 *(Universal hash [16]).* A family of functions $\mathcal{H}_{\mathcal{S}} = \{H_S : \mathcal{X} \to \mathcal{Y}\}_{S \in \mathcal{S}}$ is universal if $\Pr_{S \leftarrow \mathcal{S}}[H_S(x_1) = H_S(x_2)] \leq \frac{1}{|\mathcal{Y}|}$ for all distinct $x_1 \neq x_2 \leftarrow_R \mathcal{X}$.

Lemma 2 *(Leftover hash lemma [16]). Let $\mathcal{H}_{\mathcal{S}} = \{H_S : \mathcal{X} \to \mathcal{Y}\}_{S \in \mathcal{S}}$ be a family of universal hash functions. Let U_y is a uniform distribution over the domain $\mathcal{Y}$. For any two random variables $X \leftarrow_R \mathcal{X}$ and C, it holds that*

$$SD((H_S(X), S), (U_y, S)) \leq \frac{1}{2}\sqrt{2^{-H_\infty(X)}|\mathcal{Y}|} \text{ and}$$

$$SD((H_S(X), S, C), (U_y, S, C)) \leq \frac{1}{2}\sqrt{2^{-\widetilde{H}_\infty(X|C)}|\mathcal{Y}|}.$$