SCIENCE CHINA
Information Sciences

• LETTER •

November 2017, Vol. 60 119104:1–119104:3
doi: 10.1007/s11432-016-9204-6

Direct constructions and proofs for CCA secure (LR)IBE with dual system encryption

Yi ZHAO[1,2] & Bo YANG[1,2*]

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

Received November 10, 2016; accepted July 19, 2017; published online September 21, 2017

Citation Zhao Y, Yang B. Direct constructions and proofs for CCA secure (LR)IBE with dual system encryption. Sci China Inf Sci, 2017, 60(11): 119104, doi: 10.1007/s11432-016-9204-6

Dear editor,

In the past decade, the development of identity-based cryptography has been highly motivated. Owing to its superiority in the task of key distribution as well as its expressive ability, many related techniques have been made industrial standards. Boneh and Boyen [1] developed the first secure construction (BB1) in the standard model under a weakened adaptive notion called selective-ID security. Since then, ongoing research has contributed to enhancing the performance of IBE schemes in the standard model.

To reach tight security from simple static assumptions, researchers often make use of a powerful technique called dual system encryption (DSE) which was refined in [2]. Using this technique, selective secure schemes such as BB1 can be upgraded to full security "smoothly" by placing the original scheme in the first subgroup and masking it with random elements from another subgroup.

DSE methodology is not only able to improve the adaptivity and tightness of IBE schemes, but is also able to incorporate other properties, such as leakage resilience. After Ref. [3] demonstrated the use of hash proof system (HPS) [4] to obtain leakage resilience in public key encryption (PKE), Chow et al. [5] combined IB-HPS with DSE to design more adaptive identity-based hash proof system (IB-HPS) schemes. Lewko et al. [6] observed that leakage resilience can be obtained from DSE without IB-HPS. Li et al. [7] extended this result to a post-challenge setting.

For security against chosen ciphertext attack (CCA), there are several techniques which work in a PKE setting while only parts of them also work in IBE. Kiltz et al. [8] constructed a directly CCA secure IBE scheme following a hybrid paradigm. Alwen et al. [9] utilized the property of IB-HPS to extend this result to incorporate leakage resilience.

Obstacles for CCA proofs through DSE techniques. In the years since DSE techniques were first proposed, no direct CCA proof has been found in the literature. One explanation may be the existence of generic transformations such as CHK. However, if leakage is taken into consideration, we must rethink the necessity of proving CCA security directly through DSE techniques. In addition, Kiltz et al. [8] showed that prioritizing direct constructions over ones from CHK transformation are more efficient. There are two main obstacles to prove CCA security in a dual system environment. One is that when the challenge ciphertext is replaced with a semi-functional one, the existing verification structure will become inconsistent. For example, adding semi-functional elements will change the hashed value of the ci-

* Corresponding author (email: byang@snnu.edu.cn)

The authors declare that they have no conflict of interest.

phertext, which will cause the simulation to fail. The second problem is when we generate semi-functional keys for the adversary, it may construct a valid semi-functional ciphertext to issue a decryption query. The simulation will also fail when decryption fails. When leakage is also taken into consideration, more issues become apparent.

Our contribution. We have worked to overcome the problems mentioned above. The inspiration behind solving the first problem comes from a natural thought in mathematics: finding invariance from variance. We associate every ciphertext with a value, called the characteristic value, which is invariant in the change from normal to semi-functional type. The security definition is slightly modified such that the adversary is not allowed to query a ciphertext with the same characteristic value as the challenge one. We can thus maintain the consistency of ciphertexts in the proof.

Based on the observations above, we presents two schemes. The 1st is a CCA secure IBE scheme with DSE methodology based on Kiltz's scheme [8], which we use to show the validity of our modified security notion. The 2nd scheme presents our efforts to incorporate leakage resilience. We start from the DSE-based IB-HPS proposed in [5] and apply Cramer and Shoup's technique as reported in [9]. The adaptivity of this scheme is the same as the 3rd scheme demonstrated in [5]. However, the leakage resilience and CCA security can be obtained simultaneously using simple existing techniques. We refer interested readers to the full version for the details of the proofs.

Essentially, we present an approach to transform LR-CCA IBE schemes based on non-static assumptions to ones based on static assumptions with only a small relaxation of CCA security.

Modified security notion for CCA. We adopt a slightly modified security definition for IBE schemes against chosen ciphertext attack. Our modification is equivalent to normal procedures in a real setting sense. Furthermore, the relation we adopt can be efficiently computed and verified.

The CCA security for an (LR)IBE scheme is defined by the game below, in which a challenger interacts with an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$:

$\mathrm{Game}^{\mathrm{mCCA}}_{\mathrm{(LR)IBE},\mathcal{A}}(\lambda)$:

$(\mathrm{ID}^*, m_0, m_1) \leftarrow_R \mathcal{A}_1^{\mathrm{Keygen}(\cdot),\mathrm{Dec}(\cdot,\cdot),(\mathrm{Leak}(\cdot))}(\mathrm{mpk})$;

$b \leftarrow_R \{0,1\}$; $(C^*, t^*) \leftarrow \mathrm{Enc}(\mathrm{mpk}, \mathrm{ID}^*, m_b)$;

$b' \leftarrow_R \mathcal{A}_2^{\mathrm{Keygen}(\cdot),\mathrm{Dec}(\cdot,\cdot)}(C^*)$;

If $b = b'$ output 1, otherwise 0.

$\mathrm{Leak}(\cdot)$ is the additional leakage query oracle for LR-IBE. Here we associate every ciphertext C with a characteristic value t, such that there is a negligible probability that there exists any different characteristic value associated with the same ciphertext. The restriction of decryption queries in the 2nd stage is that $t \neq t^* \wedge \mathrm{ID} \neq \mathrm{ID}^*$ for any queried (C, ID). It remains to ensure that extract queries for ID^* are forbidden in the 2nd stage.

The advantage of $\mathcal{A}$ is defined as

$$\mathrm{Adv}^{\mathrm{mCCA}}_{\mathrm{(LR)IBE},\mathcal{A}}(\lambda) = \left|\Pr\left[\mathrm{Game}^{\mathrm{mCCA}}_{\mathrm{(LR)IBE},\mathcal{A}}(\lambda) = 1\right] - 1/2\right|.$$

Definition 1. An (l-LR)IBE scheme is mCCA secure if for any (l leakage) adversary $\mathcal{A}$, $\mathrm{Adv}^{\mathrm{mCCA}}_{(l\text{-LR})\mathrm{IBE},\mathcal{A}}(\lambda)$ is negligible.

Construction of IBE.

Setup: Let $\mathrm{AE} = (E, D)$ be a description of a one-time authenticated encryption scheme (AE-OT) scheme. H is a target collision resistant hash function. The algorithm generates a bilinear group system $\mathbb{G} = (N = p_1p_2p_3, G, G_T, e)$ where $p_i, i = 1, 2, 3$ are distinct primes. Let g be a generator of G_{p_1}. Then the algorithm chooses $u_1, u_2, h \leftarrow_R G_{p_1}$, $\alpha \leftarrow_R \mathbb{Z}_N$. mpk is set to be $(\mathbb{G}, H, \mathrm{AE}, u_1, u_2, h, e(g,g)^\alpha)$. msk is set to be α and a generator of G_{p_3}.

Keygen: Given an identity ID, the algorithm picks $r \leftarrow_R \mathbb{Z}_N, R_1, R_2, R_3 \leftarrow G_{p_3}$ and computes $\mathrm{sk}_{\mathrm{ID}} = (g^\alpha(u_1^{\mathrm{ID}}h)^r R_1, g^{-r}R_2, u_2^r R_3)$.

Enc: Given (m, ID), the algorithm picks $s \leftarrow_R \mathbb{Z}_N$ and computes $c_1 = g^s$, $t = H(e(g, c_1))$, $c_2 = (u_1^{\mathrm{ID}}u_2^t h)^s$, $K = e(g,g)^{\alpha s}$, $c_3 = E_K(m)$. The ciphertext is $C = (c_1, c_2, c_3)$. Note that t is the associated characteristic value of c_1. We use $e(g, c_1)$ as the value to be hashed, whereas existing schemes use c_1 itself.

Dec: Given ID with its secret key $\mathrm{sk}_{\mathrm{ID}}$ and a ciphertext C, the algorithm parses $\mathrm{sk}_{\mathrm{ID}}$ as (d_1, d_2, d_3) and C as (c_1, c_2, c_3). Then it computes $t = H(e(g,g)^s)$, $K = e(c_1, d_1 d_3^t)e(c_2, d_2)$ and returns $m = D_K(c_3)$.

Security. Correctness.

$$\begin{aligned}
&K = e(c_1, d_1 d_3^t)e(c_2, d_2)\\
&= e(g^s, g^\alpha (u_1^{\mathrm{ID}}h)^r R_1 \cdot (u_2^r R_3)^t)e((u_1^{\mathrm{ID}}u_2^t h)^s, g^{-r}R_2)\\
&= e(g^s, g^\alpha)e(g^s, (u_1^{\mathrm{ID}}h)^r R_1\\
&\quad \cdot (u_2^r R_3)^t)e((u_1^{\mathrm{ID}}u_2^t h)^s, g^{-r})\\
&= e(g,g)^{\alpha s}e((u_1^{\mathrm{ID}}u_2^t h), g)^{sr}e((u_1^{\mathrm{ID}}u_2^t h), g)^{-sr}\\
&= e(g,g)^{\alpha s}.
\end{aligned}$$

We present the theorem below to indicate the provable security of the construction.

Theorem 1. The construction above is mCCA secure assuming that the subgroup decisional problems are hard and that the AE-OT scheme is secure.

A weakly adaptive construction of the CCA LR-IBE scheme. Here, we demonstrate another application of the characteristic value. A CCA se-

cure LR construction from the 3rd IB-HPS scheme in [5] is given below.

Construction.

Setup: Let H be a target collision resistant hash function. The algorithm generates a bilinear group system $(N = p_1p_2p_3, G, G_T, e)$ where $p_i, i = 1, 2, 3$ are distinct primes. Let g be a generator of G_{p_1}. Then it chooses $u, h \leftarrow_R G_{p_1}$, $\alpha_1, \alpha_2, \alpha_3, \beta \leftarrow_R \mathbb{Z}_N$. mpk is set to be $(N, G, G_T, e, H, u, h, e(g,g)^{\alpha_1}, e(g,g)^{\alpha_2}, e(g,g)^{\alpha_3}, e(g,g)^{\beta})$. msk is set to be $(g^{\alpha_1}, g^{\alpha_2}, g^{\alpha_3}, g^{\beta}, X_3)$ where $X_3 \leftarrow_R G_{p_3}$.

Keygen: Given an identity ID, for $i \in \{1, 2, 3\}$, the algorithm picks $r_i, L_i, w_1, w_2 \leftarrow_R \mathbb{Z}_N$ and computes $\mathrm{sk}_{\mathrm{ID},i} = (d_{i,1}, d_{i,2}, d_{i,3}) = (g^{\alpha_i} g^{-\beta L_i} (u^{\mathrm{ID}} h)^r X_3^{w_1}, g^{-r} X_3^{w_2}, L_i)$. $\mathrm{sk}_{\mathrm{ID}} = \{\mathrm{sk}_{\mathrm{ID},1}, \mathrm{sk}_{\mathrm{ID},2}, \mathrm{sk}_{\mathrm{ID},3}\}$.

Enc: Given (m, ID), the algorithm picks $u \leftarrow_R \mathbb{Z}_N$ and computes $c_1 = g^u$, $c_2 = (u^{\mathrm{ID}} h)^u$, $c_3 = e(g,g)^{\beta u}$, $c_4 = \mathrm{Ext}(e(g,g)^{\alpha_1 u}, s) \oplus m$, $t = H(e(g, c_1)||e(g, c_2)||c_3||c_4||s)$, and $c_5 = e(g,g)^{\alpha_2 u} e(g, g)^{\alpha_3 u t}$. The ciphertext is $C = (c_1, c_2, c_3, c_4, c_5, s)$. Here t is the associated characteristic value, and s is the seed for the extractor.

Dec: Given an identity ID with secret key $\mathrm{sk}_{\mathrm{ID}}$ and ciphertext C, the algorithm first computes $t = H(e(g, c_1)||e(g, c_2)||c_3||c_4||s)$, and checks whether $c_5 = e(c_1, d_{2,1} d_{3,1}^t) e(c_2, d_{2,2} d_{3,2}^t) c_3^{d_{2,3} + d_{3,3} t}$ holds. If the check passes the algorithm returns $m = c_4 \oplus e(c_1, d_{1,1}) e(c_2, d_{1,2}) c_3^{d_{1,3}}$. Otherwise it returns $\perp$.

The correctness of the construction above directly follows from the correctness of Chow's IB-HPS.

Security. The provable security of the construction above is provided by the next theorem.

Theorem 2. Given a (μ, ϵ) extractor $\mathrm{Ext} : \mathcal{K} \to \{0,1\}^{\nu}$, let κ be the length of secret key, the construction above is an mCCA secure $(\kappa - \mu)$-LR-IBE under subgroup decisional assumptions.

Conclusion and future direction. Our work incorporates CCA proofs into DSE methodology, which may result in a wider range of applications. There are, however, some remaining problems. The 1st is to determine whether further properties can be incorporated through our technique. The 2nd is to find more techniques to handle leakage resilience and enhance CPA secure LR-IBE to CCA level in stronger model. An interesting challenge in this line of enquiry is how to achieve LR-CCA security through CHK transformation in a fully leakage model, which allows leakage on the randomness. We eagerly anticipate answers to these questions.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61572303, 61772326), National Key Research and Development Program of China (Grant Nos. 2017YFB0802003, 2017YFB0802004), National Cryptography Development Fund during the 13th Five-Year Plan Period (Grant No. MMJJ20170216), Foundation of State Key Laboratory of Information Security (Grant No. 2017-MS-03), and Fundamental Research Funds for the Central Universities (Grant No. GK201702004).

References

1 Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004. 223–238
2 Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Proceedings of the 7th International Conference on Theory of Cryptography, Zurich, 2010. 455–479
3 Naor M, Segev G. Public-key cryptosystems resilient to key leakage. In: Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, 2009. 18–35
4 Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Berlin: Springer, 2002. 45–64
5 Chow S, Dodis Y, Rouselakis Y, et al. Practical leakage-resilient identity-based encryption from simple assumptions. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, 2010. 152–161
6 Lewko A, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption. In: Proceedings of the 8th Conference on Theory of Cryptography, Providence, 2011. 70–88
7 Li J, Guo Y, Yu Q, et al. Provably secure identity-based encryption resilient to post-challenge continuous auxiliary inputs leakage. Secur Commun Netw, 2016, 9: 1016–1024
8 Kiltz E, Vahlis Y. CCA2 secure IBE: standard model efficiency through authenticated symmetric encryption. In: Proceedings of the Cryptopgraphers' Track at the RSA Conference on Topics in Cryptology, San Francisco, 2008. 221–238
9 Alwen J, Dodis Y, Naor M, et al. Public-Key encryption in the bounded-retrieval model. In: Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques, French Riviera, 2010. 113–134