ICIC Express Letters
Part B: Applications
Volume **7**, Number **10**, October **2016**

ICIC International ©2016 ISSN 2185-2766
pp. **2183–2188**

NEW CONCEPT OF WITNESS ENCRYPTION AND APPLICATION

Ren Guo[1,2], Fuji Chen[2], Xiaogang Cheng[3,*] and Yonghong Chen[3]

[1]College of Business Administration
[3]College of Computer Science and Technology
Huaqiao University
No. 269, Chenghua North Road, Quanzhou 362021, P. R. China
[*]Corresponding author: cxg@hqu.edu.cn

[2]School of Economics and Management
Fuzhou University
No. 2, Xueyuan Road, University Town, Fuzhou 350116, P. R. China

Received April 2016; accepted July 2016

Abstract. *WE (Witness Encryption) is a new kind of encryption scheme without key generation. The original security definition of WE does not consider the scenario where the instance belongs to the NP language L, but the adversary does not know any witness for this fact. This could be a problem in many applications of WE. We strengthen the security definition of WE by considering this scenario, and present a theoretical construction based on the original WE scheme and hard subset membership problem. Demonstrate the advantage of the new concept by constructing an IBE scheme based on WE with simplified construction and security proof.*
Keywords: Witness encryption, Security enhancement, Subset membership problem

1. **Introduction.** WE (Witness Encryption) was introduced by Garg et al. [1] recently as a new kind of encryption scheme without key generation. It encrypts a message with respect to an instance x of a certain NP (Non-deterministic Polynomial) language L. If $x \in L$ and a decryptor holds the NP witness w for this fact, then the decryptor can decrypt the ciphertext and get the message. Otherwise (i.e., $x \notin L$), it is semantically secure (i.e., no one can distinguish between the ciphertexts of two equal length and different messages).

The original construction of WE in [1] is based on multi-linear map [2] and Exact Cover problem, which is NP-Complete [3]. The security is based on Decision Graded Encoding No-Exact-Cover Assumption, which is intimately tied to the particular NP language used (i.e., Exact Cover). It is not known how to base security on a fixed, natural assumption that works for all instances. Recently Gentry et al. presented a WE scheme based on instance independent assumption [4], which is based on another candidate multi-linear map construction over integers [5]. However, the CLT scheme in [5] was shown to be totally insecure recently [6]. So it is still an open problem to construct WE based on an instance independent assumption.

Note that the original WE definition only guarantees the secrecy of encryption when $x \notin L$, and it says nothing about the situation when $x \in L$ but the decryptor has no witness. In this paper, we strengthen the security definition of WE with respect to this kind of situation, i.e., if the decryptor does not have an NP witness, then the ciphertext is also semantically secure to him according to some well-known mathematical assumptions. And we also give a theoretical construction based on the original WE scheme and hard subset membership problem.

This kind of security enhancement is needed. Since in many applications of WE scheme, like IBE (Identity Based Encryption) [1], ABE (Attribute Based Encryption), and reusable

garbled Turing machine [7], the NP language used is something like:

$$L = \{(x, PK) : \exists \delta,\ \mathit{Verify}(x, PK, \delta) = 1\}$$

where PK is the public key of a signature scheme, x is an arbitrary string, e.g., an ID string in IBE, or a circuit in ABE, or a Turing machine, and δ is a signature for x. Apparently for this kind of applications, for any x, then there is a witness (i.e., the signature of x with respect to PK) for $(x, PK) \in L$. So the scenario other than $(x, PK) \notin L$ considered in the original security definition of WE [1] is void, i.e., any adversary knows that $(x, PK) \in L$. However, this scenario is not considered in the original security definition. In [1], the authors also mentioned that this is a tricky issue and can be their future research direction.

In this paper, we strengthen the security definition of WE and give a theoretical construction. The idea is that we use a hard subset membership problem (such as DDH (Decisional Diffie-Hellman), DLIN (Decisional Linear), and subgroup membership) as the NP language L. Then combining this NP language with the original WE construction, we prove that if the adversary has no witness, then his probability of breaking the semantic security of the WE is negligible, even though he knows that $x \in L$.

The shortcoming of our construction is that the NP language used is a hard subset membership problem, which is not an NP-Complete problem usually. This may hinder many applications of the WE scheme. To alleviate this problem, we also construct a refined WE construction. And show that this refined WE scheme can be used for constructing IBE scheme by replacing the original WE scheme, but with significantly simplified construction and security proof.

So our contributions are threefold. Firstly we put forward the new security concept for WE scheme. Secondly we present a theoretical construction for the new concept. Lastly we demonstrate the advantage of the new concept by a simplified IBE construction, and surely the new WE concept can find more applications that lead to simplified construction and/or security proof.

2. **Preliminaries.** In this section, we review the original WE definition and construction.

Definition 2.1. *(The original WE definition) A WE scheme for an NP language L has the following polynomial-time algorithms:*

- $ENC(1^\lambda, x, M)$: This encryption algorithm takes as inputs the security parameters 1^λ, a string x and a message M, and outputs a ciphertext CT.
- $DEC(CT, w)$: This decryption algorithm takes as inputs a ciphertext CT and a string w, and outputs a message M or a special symbol $\perp$.

And the algorithms satisfy the following properties:

- Correctness: If $x \in L$ and w is an NP witness for this fact, then the decryption algorithm always outputs the right message M, i.e.,

$$\Pr[DEC\left(ENC\left(1^\lambda, x, M\right), w\right) = M] = 1$$

- Soundness: If $x \notin L$, for any polynomial adversary A, then two distributions of encryption of two different messages m_0 and m_1 with equal length are the same except with negligible probabilities, i.e.,

$$\left|\Pr\left[A\left(ENC\left(1^\lambda, x, m_0\right)\right) = 1\right] - \Pr\left[A\left(ENC\left(1^\lambda, x, m_1\right)\right) = 1\right]\right| < \mathit{negligible}(\lambda)$$

Note that the original definition says nothing about the situation when the adversary A knows that $x \in L$, but A knows no witness. Our security enhancement is just for this scenario, see Section 3.

Now we briefly review the original construction of WE, which is based on multi-linear map and Exact Cover problem.

The NP language L used in [1] is Exact Cover problem, which is NP-Complete. The Exact Cover problem is the following: Given a set $[n]$ with n distinct elements $1, \ldots, n$, and l subsets of $[n]$, i.e., $T_i \subset [n]$, $1 \leq i \leq l$. The problem is to find an exact cover of $[n]$ from the subsets T_i.

The WE scheme based on Exact Cover is as the following.

- *ENC*: Given an instance x, i.e., T_i and $[n]$, and a message M. Randomly select n numbers $a_1, \ldots, a_n$, and then set $C = M \cdot g_n^{a_1,\ldots,a_n}$. Besides, for each T_i, set $C_i = g_{|T_i|}^{\prod_{i \in T_i} a_i}$. Finally output the ciphertext $CT = (C, C_1, \ldots, C_l)$.
- *DEC*: If $x \in L$ and w is an NP-Witness for this fact, i.e., $w \subset [l] \wedge \bigcup_{i \in w} T_i = [n]$, then we can recover $g_n^{a_1,\ldots,a_n}$ from $(C_1, \ldots, C_l)$ as the following:

$$e\left(C_{i_1}, \ldots, C_{i_{|w|}}\right) = g_n^{a_1,\ldots,a_n},\ i_j \in w$$

With $g_n^{a_1,\ldots,a_n}$, the message M can be easily recovered from C by division.

3. Our Definition and Construction.

Definition 3.1. *Our strengthened WE definition is the same as the original WE definition with an added third property.*

- *Special Soundness: Even if an adversary A knows that $x \in L$, but he has no witness, then the encryption is still semantically secure to him, i.e.:*
  - *The adversary A can select two messages m_0 and m_1 with the same length, and send them to the challenger.*
  - *The challenger then randomly sets $b \leftarrow \{0, 1\}$, and encrypts the message m_b. Send the ciphertext to the adversary A.*
  - *Now the adversary A has to guess if $b = 0$ or $b = 1$. For any polynomial time adversary A, his success probability is 1/2, except with negligible probabilities.*

Now we give a theoretical construction with this added special soundness property by combining the original WE scheme and hard subset membership problem.

Our NP language L is a hard subset membership problem. For simplicity and clarity, we use DDH problem in the following. However, note that any hard subset membership problem (such as DLIN, and subgroup membership) will be equally suitable for our construction. So our construction is essentially a combination of the original WE scheme and a hard subset membership problem.

The DDH problem is to distinguish DDH tuple (g^r, h^r) with $(g^{r_1}, h^{r_2} : r_1 \neq r_2)$. So our NP language is $L = \left\{(G, H) : \log_g G = \log_h H = r\right\}$ with NP witness r. An instance of this language is just two group elements $x = (G, H)$. Then our WE construction is to encrypt a message m with respect to this language.

Theorem 3.1. *The WE scheme constructed above satisfies the original WE securities; besides, it also satisfies the added special soundness property based on the DDH assumption.*

Proof: 1) If $x = (G, H) \in L$ and a decryptor knows the witness r, then he can decrypt the ciphertext according to the original WE scheme.

2) If $x = (G, H) \notin L$, it is clear that the ciphertext is semantically secure according to the original WE scheme.

3) The new scenario is that when $x = (G, H) \in L$, but the decryptor has no witness, we claim that it is also semantically secure to the decryptor.

Suppose there is an adversary A that can break the semantic security. We show how to solve DDH assumption by using this adversary A. The reduction is simple.

Given two group elements (G, H), to judge if it is a DDH tuple. The challenger just uses it as an NP instance x of the language L, to encrypt a message m_b chosen randomly

from two messages m_0, and m_1. Then send the ciphertext to the adversary A. Based on the correctness of the answer from A, the challenger can easily judge if (G, H) is a DDH tuple. I.e. if A's answer is correct, then clearly $x = (G, H) \in L$ and although A has no witness, A still can break the semantic security. If A's answer is not correct, then $x = (G, H) \notin L$, since in this scenario nobody can break the semantic security based on the security of the original WE encryption scheme.

4. **Extension and Application.**

4.1. **Refined WE construction with signature.** Goldwasser et al. use WE to construct reusable garbled Turing machine [7]. The NP language used in their construction is $L = \{(x, PK) : \exists(M, \delta,\ \textit{Tableau of}\ M(x) = 1)\}$, where M is a Turing machine, δ is a valid signature on M with respect to the PK, a tableau of running the Turing machine with input x and the result is 1. It is clear that for any x, such witness exists. So for any x, we always have $(x, PK) \in L$. Hence the security definition of the original WE scheme is void, since the scenario that $(x, PK) \notin L$ never happens. So it is clear that for such kind of applications, we need the stronger security assurance that we put forward in this paper.

However, the problem with the above construction of WE is that usually a hard subset membership problem is not NP-Complete (such as DDH, and DLIN). So it is not known how to reduce an arbitrary NP problem to it even theoretically. This can be a problem in many applications of WE, since this kind of reduction is needed when an arbitrary NP language is used. So we leave open the problem of constructing WE scheme with special soundness with respect to an NP-Complete problem.

Now we present a refined construction that can be used directly in many applications instead of using the original WE scheme. And we show that this leads to simplified construction and/or security proof.

The NP-language used is based on a signature scheme, which is an SPK (Signature of Proof of Knowledge) [8] based on ROM model [9] or Fiat-Shamir heuristic [10], which turns an interactive zero-knowledge into a non-interactive one. The public key is $(G, H) = (g^r, h^r)$, and the signature is $SPK\{r : (G, H) = (g^r, h^r)\}(m)$, which is realized as follows. Given the message to be signed m. Generate $(G', H') = (g^k, h^k)$ for random k. Then set $c = H(G', H', m)$, where H is a hash function modeled as random oracle, and $s = k - cr$. The signature is (G', H', s). To verify the signature, just check if $G' = g^s G^c$ and $H' = h^s H^c$, where $c = H(G', H', m)$.

So the NP-language is $L = \{((G, H, m), \delta) : \textit{Verify}(m, \delta) = 1\}$, where m is an arbitrary message and the NP-Witness is a valid signature on m with respect to the public key (G, H). Note that if (G, H) is not a DDH tuple, then no such witness exists for an adversary with no control of the random oracle.

The proof that this refined WE construction satisfies the added special soundness property is essentially the same as our proof of Theorem 3.1, i.e., we can break the DDH assumption by using the adversary that breaks the special soundness property.

4.2. **Simplified IBE scheme based on WE.** By using this refined WE construction with added special soundness, we construct an IBE scheme. The construction follows the same strategy of [1]. However, with the added special soundness property, the construction and the security proof are both simplified significantly. Our IBE scheme is as the following.

- Setup: Generate the public key of the signature scheme as above, i.e., $(G, H) = (g^r, h^r)$.
- KeyGen: For an arbitrary ID, generate the secret key for ID as the signature on ID, i.e., the secret key for ID is $SPK\{r : (G, H) = (g^r, h^r)\}(ID)$.

- Encrypt: To encrypt a message m with identity ID, use the WE scheme described as above, namely use WE. $ENC((G, H, ID), m)$, where the NP-language is $L = \{(G, H, ID) : \exists\delta \wedge Verify(ID, \delta) = 1\}$.
- Decrypt: With the secret key, this is a witness to the language L. The user with identity ID can decrypt the ciphertext by WE.DEC(CT).

Theorem 4.1. *The IBE scheme above is adaptively secure based on DDH assumption and ROM model.*

Proof: We show how to solve the DDH problem by using a successful adversary against the IBE adaptive security game. Given two group elements (G, H), the problem is to judge it is a DDH tuple or not. The challenger setups the IBE scheme described above by using (G, H) as the public parameters (i.e., the verification key of the signature scheme). Then the challenger interacts with the adversary A as follows.

- Secret Key Query: When A issues a secret key query for identity ID, the challenger just simulates the signature (in the ROM model), i.e., the challenger selects random s and c, and then sets $G' = g^s G^c$ and $H' = h^s H^c$. And program the random oracle to return c on input $H(G', H', m)$. Finally return the signature as (G', H', s). Note that even if (G, H) is not a DDH tuple, this simulated signature is still valid for verification. If (G, H) is a DDH tuple, the distribution of the simulated signature is the same as the real signature.
- Challenge Phase: A presents an identity ID* and two equal length messages m_0 and m_1 to the challenger. The challenger randomly sets $b \Downarrow \{0, 1\}$ and encrypts m_b with the NP instance (G, H, ID^*) and sends the ciphertext CT to A.
- More Secret Key Query: The challenger can still answer secret queries from the adversary by forging signatures as above by programming the random oracle.

Finally the adversary has to guess if $b = 0$ or $b = 1$. Based on the correctness of the adversary's answer, the challenger can know if (G, H) is a DDH tuple or not. If (G, H) is a DDH tuple, then the game described above is perfect, so A's successful probabilities is high. Otherwise (G, H, ID^*) is not in the language L, so A's successful probabilities is negligible according to the WE encryption security definition. Note that for the challenger, he can forge the signature because he can program the random oracle. However, for the adversary, he has no such capability. Therefore, with the help of the adversary, the challenger can find out if (G, H) is a DDH tuple or not.

5. Conclusions.

In this paper, we present a strengthened security definition for WE scheme, which we called "Special Soundness". It is exactly what is left open in the original work of WE in [1]. We also construct a WE scheme satisfying the strengthened security based on the original WE scheme and a hard subset membership problem. And demonstrate its usage by constructing an IBE scheme, which leads to significantly simplified construction and security proof. The shortcoming of our construction is that the NP language used is not an NP-Complete problem. This may hinder many applications of the WE scheme. So the most important problem that is left open in this work is how to construct a WE scheme based on an NP-Complete problem. This kind of WE scheme will certainly find much more applications, since any NP problem can be reduced to an NP-Complete problem theoretically.

Acknowledgment. This work is partially supported by the National Natural Science Foundation of China (Nos. 71271056, 61370007), and the Natural Science Foundation of Fujian Province of China (No. 2016J01336). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] S. Garg, C. Gentry, A. Sahai et al., Witness encryption and its applications, *Proc. of the 45th Annual ACM Symposium on Theory of Computing*, NY, USA, pp.467-476, 2013.

[2] S. Garg, C. Gentry and S. Halevi, Candidate multilinear maps from ideal lattices, in *Advances in Cryptology – EUROCRYPT 2013*, T. Johansson and P. Nguyen (eds.), Springer Berlin Heidelberg, 2013.

[3] M. Garey and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman & Co. Ltd., 1979.

[4] C. Gentry, A. Lewko and B. Waters, Witness encryption from instance independent assumptions, in *Advances in Cryptology – CRYPTO 2014*, J. Garay and R. Gennaro (eds.), Springer Berlin Heidelberg, 2014.

[5] J. Coron, T. Lepoint and M. Tibouchi, Practical multilinear maps over the integers, in *Advances in Cryptology – CRYPTO 2013*, R. Canetti and J. Garay (eds.), Springer Berlin Heidelberg, 2013.

[6] J. Cheon, K. Han, C. Lee et al., Cryptanalysis of the multilinear map over the integers, in *Advances in Cryptology – EUROCRYPT 2015*, E. Oswald and M. Fischlin (eds.), Springer Berlin Heidelberg, 2015.

[7] S. Goldwasser, Y. Kalai, R. Popa et al., How to run Turing machines on encrypted data, in *Advances in Cryptology – CRYPTO 2013*, R. Canetti and J. Garay (eds.), Springer Berlin Heidelberg, 2013.

[8] J. Camenisch and M. Stadler, Efficient group signature schemes for large groups, in *Advances in Cryptology – CRYPTO'97*, B. Kaliski Jr. (edt.), Springer Berlin Heidelberg, 1997.

[9] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, *ACM Conference on Computer & Communication Security*, pp.62-73, 1993.

[10] A. Fiat and A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, in *Advances in Cryptology – CRYPTO' 86*, A. Odlyzko (edt.), Springer Berlin Heidelberg, 1987.