Design and Construction of Secure Digital Will System

Tzong-Sun Wu, Yih-Sen Chen, and Han-Yu Lin
Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan

Abstract: *The rapid growth of network communications has made applications of electronic commerce the future trend of commercial activities. To ensure the effectiveness of transactions, governments put the electronic signature law into practice. They also proposed guiding or assisting projects to encourage or help enterprises and organizations to construct secure electronic environments. Because of the availability and ease of use of information infrastructure, human's daily life is increasingly digitalized. With the promotion of life education and religious groups, people have gradually accepted the concept of writing down wills before their death, which can reduce conflicts and arguments for inheritance. A legitimate will can be produced with the witness of notaries in the court or the notary public offices. If a testator wishes to modify his will, he must perform again the procedures above. Since, it requires some fees as well as transportation costs for notaries and witnesses, the generation of a traditional will is rather costly. It might also be inefficient for its complicated witnessing procedures. Currently, the electronic Wills Act is under discussions, but not put into practice yet. To date, there are no literatures discussing the issues of digital will. The properties of security, convenience and effectiveness are the most significant reasons why people would like to adopt the digital will mechanism in the future. Based on the mechanisms of public key infrastructure and key escrow systems, we constructed a secure and realistic model for a digital will system which fulfills the above-mentioned properties and is suitable for practical implementation.*

Keywords: *Will system, key escrow, testamentary trust.*

Received February 20, 2014; accepted September 9, 2014; published online October 29, 2015

1. Introduction

One thing that people would not like to think of is the death of beloved persons, especially the unexpected death of dear family. It is often overlooked but should be given serious consideration and well planned. With a will, we can express our wishes or arrange our assets in advance. A valid will can effectively prevent inheriting disputes among beneficiaries. Nevertheless, people often ignore the importance of pre-making a will. It is quite common to see many true stories about family members battling over inheritance, since the deceased did not leave instructions on how his property should be disposed of after he died. A will is a document stating not only who will inherit the assets, but also what the testator's whishes are. The content of a will could include the funeral plan for the deceased as well. With the promotion of life education and the advocacy of religious groups, more and more people have gradually accepted the idea of writing down the will before their death. However, a legitimate will must be notarized by the notary public office or the court and reviewed in a reasonable period. If the testator wants to modify his will, the above procedures must be done again. It might result in expensive fees of notaries and witnesses, not to say the cost and time spent in transportation and waiting. Besides, since the handwritten will is presented in the form of plaintext, the content of will might be read by people with bad intention. If the beneficiary list or the content of the will was known before testator's death, it might cause a dispute among family members.

The testamentary trust supplies another alternative to perform the testator's wish after he passes away. It contains two main elements including a will and a trust. The former takes effect from the time of the death of the testator. The latter refers to the legal relationship in which the consigner transfers or disposes of a right of property and causes the consignee to administer or deal with the trust property according to the stated purpose of the trust for beneficiary benefits or for a specified intention [3, 7, 18]. This kind of trust provides the functions of preserving property, performing will, guarding the young children and taking care of the family of the deceased. These trust affairs must be based on a trusted party which must faithfully execute the contents of the will, especially about the estate, after the testator's death [3, 18]. In the will, the testator must indicate that who he wants to trust and how he would like to dispose his properties. He states the decision of the testamentary trust and designates a conservator who was authorized to dispose his properties and to transfer his estate to a trusted party called will trust banks [7, 18] after he passes away. Then, the consignee follows the content of testamentary trust to manage trust property and allocate trust-benefit to the beneficiary. For the above disposing procedures, the trust party will charge a few additional costs, except the signing cost and the annual fee for the trust relationship. The shortcomings of testamentary trust are that the necessary costs are high. Likewise, the testamentary trust still has the same weaknesses as well as the traditionally handwritten one, i.e., the content of the trust or the will could be read directly. This could not solve the dispute among family members before testator's death.

Nowadays, due to the accessibility of the Internet, more and more documents are exchanged over networks and electronic signatures act is enacted to encourage the use of electronic transactions and ensure the security of electronic transactions. This Act guarantees these transactions with legality on the Internet. In the digital world, providing a secure environment for storage and transactions is essential, in which encryption and digital signature schemes are most widely used technologies to achieve the above security requirements. Encryption mechanisms fulfill the security requirement of confidentiality [19] while digital signature schemes realize those of integrity [17], authenticity [17] and non-repudiation [6, 14, 17]. Therefore, we devoted ourselves to the study of a digital will system in which the will is held in trust with the trust party. We adopt the concept of the testamentary trust and utilize some cryptographic techniques to construct a concrete and feasible will system.

In our system, the testator signs the will with his private key, encrypt the signed will to become a sealed one and then sends it to the will bank for proper conservation. Simultaneously, he delivers the signed beneficiary list to the conservator. Since, the encrypted will includes the signature of the testator; each participant can check the validity of the will by verifying the signature when the encrypted will is decrypted by the bank or court. We assume that the encrypted list and the encrypted will are notarized by the court before sending them to the will bank or the conservator. Therefore, they could be regarded as effective documents. The testator can not only preserve the privacy, but also stand on his wish to construct or maintain the will. Currently, the electronic Wills Act is under discussions, but not put into practice yet. To date, there are no literatures discussing the issues of digital will. Our proposed system is secure against several possible attacks such as impersonation and collusion attacks, and provides a more secure mechanism to meet all security requirements on the Internet.

The rest of this paper is organized as follows: Our proposed digital will system which is presented in section 2. The security of our scheme is analyzed in sections 3. Finally, conclusions are given in section 4.

2. Secure Digital Will System

In this section, we employ some basic cryptographic primitives [4, 5, 6, 11, 12, 13, 15, 16, 17, 19] to construct a feasible digital will system on the Internet. To ensure the security of network applications, we use the public key cryptosystem [5, 6, 13, 14, 15] and the digital signature scheme [14] to fulfill the requirements of confidentiality [1, 17, 19], integrity [11, 17], authenticity [11, 17] and non-repudiation [6, 11, 14, 17]. In an open environment, we suppose that each participant has a private/public key pair and can use a corresponding certificate to verify that a public key belongs to an individual.

2.1. System Model Overview

Our proposed will system allows a testator to create or modify his will in a secure and efficient way with his wish, and then the will is signed, encrypted and kept in the safekeeping bank. Initially, a testator chooses a trusted person as the conservator of his will and signs a contract with a will bank which is authorized to make his will public after he passes away. According to the testator's volition, he generates a will and a beneficiary list. Then, he signs the will with his private key and encrypts the signed one with a secret key called a will secret key. Simultaneously, he uses the conservator's public key to encrypt the beneficiary list signed by him. Then, he sends the will bank both the encrypted will and the encrypted beneficiary list and only the latter is delivered to the conservator. In the upcoming days, he can freely modify his will or the list as he wishes. When the testator passes away, the conservator informs each beneficiary in the beneficiary list and the bank. Both the bank and the conservator compare the list they possess. If the two lists are identical, the bank requests the conservator to decrypt the encrypted list. Upon receiving the notification sent by the conservator, each beneficiary must establish a proof that he is one of the beneficiaries on the list. According to the list, the bank verifies the identities of beneficiaries by checking their certificates [9] and provides the encrypted sub-secret key to the beneficiary individually. Each beneficiary uses his private key to decrypt the corresponding encrypted key separately and then the beneficiary requests the bank to decrypt the encrypted will and make it public. The bank receives all sub-secret keys from the beneficiary, and then the will secret key can be recovered. He uses the secret key to decrypt the encrypted will and hands it over to the conservator.

In case of serious conflicts among beneficiaries or failure to gain all sub-secret keys due to a particular reason, the will secret key would not be recovered. In this situation, the bank submits the encrypted will and the encrypted key to the court according to legal procedures. The court decrypts the encrypted key and will under its authorities and responsibilities. The whole structure of our proposed mechanism is illustrated in Figure 1.

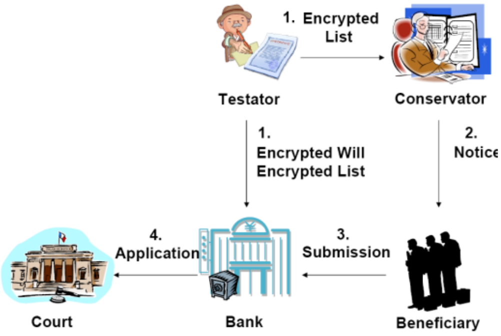

Figure 1. the structure of our system.

As a result of all the efforts, we conclude that our system model does meet the security requirements of X.800 with respect to confidentiality, access control, data integrity, authentication, non-repudiation and availability [10, 17]. Next, we describe involved participants and give a concrete construction.

2.2. Involved Participants

In our mechanism, there are six participants listed as follows: Testator, Conservator, Will Bank, Court and Beneficiary. There is a System Authority (SA) whose tasks are to initialize the system and manage the public directory. We describe the characteristics of participating entities as follows:

1. *Testator*: A testator is a person who writes a testament that is in effect at the time of his death. He must make the will voluntarily, realize the consequences that could possibly result from the will contents he made and designate one person to manage his estate and provide for the transfer of his property at death. In the upcoming days, he can revise his will or the list as he wishes.
2. *Conservator*: A person is appointed as the conservator of the will by a testator. He must faithfully execute the content of the will. In our model, he has to regularly inspect the beneficiaries' public keys from the SA or the public key directory and notify the testator that someone's key has been changed. When the testator passes away, he informs each one of the beneficiary list and the bank. In addition, he is authorized to make the will public and apply to the hospital for the testator's death certificate.
3. *Will Bank*: A will bank is a corporation, may be a commercial bank or organization to perform the fiduciary of trusts and agencies, which specializes in being a trustee of various kinds of trusts and in managing estates. It is primarily responsible for safekeeping the encrypted will, the encrypted beneficiary list and the set of encrypted sub-secret keys. We assume that the will bank is a semi-trust role or an honest-but-curious party who follows the protocol to perform his task and it might attempt to reveal some secrets.
4. *Court*: In both common law and civil law legal systems, courts are the central means for dispute resolution and it is generally understood that all persons have an ability to bring their claims before a court. This role is an arbitrator in our system. On receiving the request from the bank, based on the court's authorities and responsibilities, he decrypts the encrypted will and makes it public.
5. *Beneficiaries*: A beneficiary may be a natural person or other legal entity who receives distributions or other benefits from a will. Upon receiving the notification from the conservator, each beneficiary must prove his identity to the bank that he is one of the beneficiaries. Note that, the beneficiary might not know he is on the beneficiary list until receiving notification from the conservator.

2.3. Concrete Construction of the Proposed Model

Our system consists of five phases: Initiation phase, will generation phase, will preservation phase, will disclosing phase and justification phase. Descriptions of these phases are given below:

1. Initiation Phase: First of all in the system initialization phase, the SA is responsible for generating system parameters, determining a certification system, such as X.509 [9] and defining the following system functions. These functions could be any provably secure signature schemes or cryptosystems, such as Diffie-Hellman [5], ElGamal [6] and RSA [14]. Assume that each participant has a private/public key pair (Pr_i, Pu_i). In the initiation phase, SA can use the certificate to verify the validity of each public key. These functions and system parameters are described as follows:

- $S(x, M)$: Is a signature function which signs a message M with the private key x.
- $V(y, S, M)$: Is a verification function that verifies the signature S on the message M with the public key y.
- $E_K(M)$: Is a symmetric encryption algorithm which encrypts the message M with the secret key K.
- $D_K(C)$: Is a symmetric decryption algorithm which decrypts the ciphertext C with the secret key K.
- $E(K_{pu}, M)$: Is a public encryption algorithm which encrypts the message M with the public key K_{pu}.
- $D(K_{pr}, C)$: Is a public decryption algorithm which decrypts the ciphertext C with the private key K_{pr}.
- $f()$: Is a reconstructing function which recovers the

secret key by obtaining previously shared n sub-secret keys.

2. Will Generation Phase: A testator constructs a will and a beneficiary list and then signs the will W and the list D_{list} with his private key Pr_t. Next, he selects a random integer K as the will secret key and encrypts the secret key with the court's and his public key $\{Pu_{c1}, Pr_t\}$ separately. Simultaneously, he splits the secret key into n sub-secret keys $\{k_1, k_2, \ldots, k_n\}$ for n beneficiaries [4, 16]. After that, he employs each beneficiary's public key to encrypt the sub-secret key individually. The testator performs the following steps:

- *Step* 1: Sign the will W and the beneficiary list $D_{list}= \{u_1, u_2, \ldots, u_n, date\}$ with his private key Pr_t.

$$S_0= S(Pr_t, W) \quad (1)$$

$$S_1= S(Pr_t, D_{list}) \quad (2)$$

Where $u_1, u_2, \ldots, u_n$ are the beneficiaries and "*date*" is the time stamp for the will constructed.

- *Step* 2: Encrypt the beneficiary list D_{list} with the conservator's public key Pu_{c2}

$$C_{list} = E(Pu_{c2}, D_{list} \parallel S_1) \quad (3)$$

Where "||" is a concatenation operator.

- *Step* 3: Select a random integer K as the will secret key and separately encrypt the secret key with the court's and his public key $\{Pu_{c1}, Pr_t\}$ below:

$$Z_{c1}= E(Pu_{c1}, K) \quad (4)$$

$$Z_t= E(Pu_t, K) \quad (5)$$

The encrypted key Z_{c1} is only used later when the will secret key cannot be reconstructed. Once he wants to reuse the will secret key, the above key Z_t will be used.

- *Step* 4: Split the will secret key K into n sub-secret keys $\{k_1, k_2, \ldots, k_n\}$ and individually employ each beneficiary public key to encrypt the corresponding sub-secret key into the encrypted sub-secret key $\{z_1, z_2, \ldots, z_n\}$.

$$k_i = F(K, i, n, Pr_t) \quad (6)$$

$$z_i= E(Pu_i, k_i), \text{ where } i = 1, 2, \ldots, n \quad (7)$$

Where k_i is i^{th} beneficiary's sub-secret key and $F()$ is a secret sharing function [4, 8, 15]. For convenience, let $Z= \{z_1, z_2, \ldots, z_n, Z_{c1}, Z_t\}$ be a set of encrypted keys, where Z_{c1} and Z_t are the previously encrypted keys by the court and the testator.

- *Step* 5: Encrypt the signed will with the secret key K.

$$C_w= E_K(W \parallel S_0) \quad (8)$$

- *Step* 6: Send the will bank the encrypted will C_w, the encrypted beneficiary list C_{list} and the set Z and only the second one is delivered to the conservator.

3. Will Preservation Phase: The bank puts the encrypted will C_w, the encrypted beneficiary list C_{list} and the set Z under their custody. As mentioned in the system model overview, we consider the possible situations where beneficiaries' public keys might be changed or the testator wants to modify the will, the will secret key or the list. The details of these cases are described as follows:

- ***Case* 1**. Beneficiary's Public Key is Changed: Once informed by the conservator, the testator performs the following steps:
  - *Step* 1: The testator decrypts the encrypted key Z_t and reconstructs Equation 6 to obtain the sub-secret key k_i.

$$K= D(Pr_t, Z_t) \quad (9)$$

$k_i= F(K, i, n, Pr_t)$ as Equation 6

  - *Step* 2: Compute the new encrypted sub-secret key z'_i as Equation 7 with the new public key Pu'_i.

$$z'_i = E(Pu'_i, k_i) \quad (10)$$

  - *Step* 3: Send the value z'_i to the bank for replacing z_i.

Note that, the encrypted will and the encrypted list are not updated.

- ***Case* 2**. The Beneficiary List is Changed: The list is different from previous one; the testator must re-make the beneficiary list, re-sign and re-encrypt the list. To make sure the security of the construction, the will secret key must be re-selected. Since, the will secret key is changed, these sub-secret keys muse be obtained by splitting the new one and the will must be re-encrypted with the new will secret key.
  - *Step* 1: Update the list, re-sign the new list $D_{list'}$ with his private key and encrypt the signed list with the conservator's public key.

$$D_{list'}= \{u_1, u_2, \ldots, u'_j, \ldots, u_n, date\}$$
$$S'_1= S(Pr_t, D_{list'}) \quad (11)$$

$$C_{list'}= E(Pu_{c2}, D_{list'} \parallel S'_1) \quad (12)$$

  - *Step* 2: Re-choose a random integer K' as a new will secret key and perform Equations 4 and 7 to obtain the new set Z''.

$$Z'' =\{z'_1, z'_2, \ldots, z'_i, \ldots, z'_n, Z'_c, Z'_t\}$$

  - *Step* 3: Re-encrypt the will with the new secret key $K.'$

$$C'_w= E_{K'}(W \parallel S_0) \quad (13)$$

- *Step* 4: Send encrypted will C'_w, the list $C_{list'}$ and the key set Z'' to the bank. Meanwhile, the list $C_{list'}$ is also, delivered to conservator.

- ***Case* 3**. The Will Content is Changed: A will has the period of validity just like a health certificate. It must be reviewed regularly. When the beneficiary list and the will secret key are kept the same, the testator can re-sign and re-encrypt the will and then send the new encrypted will to the bank if he wants to change the will content.

$$S'_0 = S(Pr_t, W') \qquad (14)$$

$$C_{w'} = E_K(W' \| S'_0) \qquad (15)$$

Note that, the encrypted list and the will secret key are unchanged.

- ***Case* 4**. The will Secret Key is Changed: In general, the will secret key is kept secret by the testator, but it may be unwittingly revealed to others or the testator wants to change it. He must re-select a new will secret key and re-compute the corresponding sub-secret keys. Then, the encrypted will must be re-encrypted with the new key. Finally, the testator sends the encrypted will and the sub-secret key to the bank. The beneficiary list is unnecessary to change.

4. Will Disclosing Phase: After the testator passes away, the conservator informs all of the beneficiaries and the bank. He provides the beneficiary list to the bank. Then, the bank compares the list with the one deposited by the testator. If they are identical, the bank verifies the validity of the signature on the list and checks each beneficiary's identity by verifying their certificates. Then, the bank provides the encrypted sub-secret key to each beneficiary who can therefore use his private key to decrypt the received one and request the bank to make the will public. The bank performs the following procedures:

- *Step* 1: Request the conservator to decrypt the beneficiary list, run the encryption procedure again with the public key of the conservator and then compare the result with his holding one.

$$D_{list} \| S_1 = D(Pr_{c2}, C_{list}) \qquad (16)$$

$$E(Pu_{c2}, D_{list} \| S_1) \overset{?}{=} C_{list} \qquad (17)$$

- *Step* 2: Verify the validity of the signature on the list.

$$V(Pu_t, D_{list} \| S_1) \overset{?}{=} 1 \qquad (18)$$

- *Step* 3: Send each beneficiary u_i on the list the encrypted sub-secret key z_i. Each beneficiary u_i uses his private key to decrypt the received key, respectively.

$$k_i = D(Pr_i, z_i) \qquad (19)$$

- *Step* 4: Combine all of these sub-secret keys to recover the will secret key K, and then use it to decrypt the encrypted will C_w.

$$K = f(k_1, k_2, \ldots, k_n) \qquad (20)$$

Where $f()$ is the reconstructing function.

$$W \| S_0 = D_K(C_w) \qquad (21)$$

- *Step* 5: Verify the validity of the signature with the testator's public key.

$$V(Pu_t, W \| S_0) \overset{?}{=} 1 \qquad (22)$$

5. Justification Phase: If any beneficiary is unwilling or unable to cooperate, the secret key cannot be recovered. In this situation, the bank presents the encrypted secret key Z_c and the encrypted will C_w in the court. Afterwards, the court uses his private key Pr_c to decrypt the will secret key based on his statutory duties and employs the secret key to decrypt the will as Equation 21.

$$K = D(Pr_c, Z_c),\ W \| S_0 = D_K(C_w) \qquad (23)$$

The testator's signature can be verified by Equation 22. Finally, the court announces the will. The justice of the content is not discussed here.

3. Discussion and Analysis

In this section, we analyze the security of our system in terms of efficiency and functionality. Our proposed scheme is secure against various attacks and achieves necessary security requirements.

3.1. Consideration for Implementation

We utilize the digital signature, encryption/ decryption and secret sharing schemes to construct a practical and feasible system. These schemes can be any well-known functions such as RSA signature, ElGamal encryption [6] and Shamir secret sharing scheme [16]. $F(\cdot)$ and $f(\cdot)$ are the existing efficient functions for generating or reconstructing the sharing key. $f(\cdot)$ can recover the share key which used by $F(\cdot)$ to generate sub-secret keys. Here, we give a simple construction for implementing such functions. $F(\cdot)$ first generates n-1 random numbers, $k_1, k_2, \ldots, k_{n-1}$, depending on the input parameters and then computes $k_n = K \oplus k_1 \oplus k_2, \ldots \oplus k_{n-1}$, where "$\oplus$" denotes the XOR operation. Straightforwardly, $f(\cdot)$ is the function of XORing all the sub-secret keys.

3.2. Security Analysis

In this section, a security analysis is performed to examine whether the proposed system is secure or not for practical applications. Since, there are five participants in our system model; we consider how each one may violate different aspects of security. We assume that the court is absolute impartial party which plays the role of an arbitrator and the testator cannot arbitrarily break the rule of model, such as modifying the will or the list, and he does not sent them to the bank or the conservator simultaneously. Therefore, we will not discuss what event could happen in the court or the testator. The analysis aims at focusing on three types of attacks that may have impacts on the system security.

3.2.1. Resistance to Impersonation Attacks

We assume that the attacker might impersonate the conservator, the bank and the beneficiary. The details of each case are described as follows.

- ***Case* 1**. Impersonation of Conservator: If an attacker wants to impersonate the conservator, he might counterfeit the beneficiary list and send it to the bank. The list could be encrypted or un-encrypted. If it is presented in the form of ciphertext, the bank checks whether it is the same as what the testator gave him. If it is a plaintext, the bank verifies the signature on the list with the testator's public key, re-encrypts the list with the public key of conservator and inspects whether it differs from the one his possessed. Obviously, unless the attacker knows the information of list, the timestamp and the testator's private key, it will not the same as the one stored by the bank. Even though the attacker obtains the real encrypted list, both the bank and the attacker still cannot decrypt the list without the decrypting key. Therefore, our proposed system is secure against this attack.
- ***Case* 2**. Impersonation of Bank: In our system, the bank is a semi-trusted party. Any attacker cannot obtain the encrypted will and the encrypted secret key from the bank. Hence, the attacker can only impersonate the bank to request the court for decrypting the encrypted will. When the secret key cannot be restructured, the bank submits the encrypted will and the encrypted key to the court. The requirement must be presented by the bank. Now, the attacker generates a random key as a forged secret key and then uses it to encrypt a forged will. Besides, he encrypted the forged key with court's public key. Finally, he sends the encrypted will and key to the court. Upon receiving the request from the attacker, the court first checks whether the request comes from the bank, then decrypts the encrypted secret key with his secret key. He uses this forged key to decrypt the encrypted will. Obviously, the decrypted will does not have testator's signature and would be regarded as fake. In any situation, the court cannot disclose his secret key to others. So, the attacker cannot gain any benefit from the processes of decrypting the will or the will secret key. Therefore, our proposed scheme can withstand this attack.
- ***Case* 3**. Impersonation of Beneficiary: If an attacker impersonates one or all of the beneficiaries, he needs to obtain the encrypted sub secret key from the bank. Anyone except the real beneficiary cannot decrypt a sub-secret key. Even if the attacker obtains one encrypted key, he still cannot decrypt it without the corresponding private key. Furthermore, we consider that the attacker provides one or more forged sub-secret keys to the bank and the latter cannot exactly recover the will secret key. In this circumstance, the attacker also gains no useful information. In addition, the attacker might attempt to collect all sub secret keys due to the unknown identity of beneficiary on the list. However, since the list has been encrypted, it is not recognizable for him. Therefore, our proposed scheme can prevent this attack.

3.2.2. Resistance to Collusion Attacks

Here, we require the bank should not be able to cheat some participant by colluding with others, since a collusive bank would break this system security trivially. If the bank colludes with the conservator, the latter might want to know the content of the beneficiary list before the testator death. This would be unfair to each beneficiary. We exclude the possibility that both the bank and the conservator collude with each other. If a beneficiary attempts to open the will with the bank early, he will find out that the list is encrypted by the testator with conservator's public key. This kind of collusion is unhelpful to the bank or beneficiary. As a result, the bank plays a semi-trusted party which honestly stores the encrypted will, the encrypted beneficiary list and the set of encrypted sub-secret keys. It is impossible for the bank to collude with the beneficiary. Therefore, we only consider that beneficiary colludes with the conservator. Even if all participants are compromised and colluded, they are still unable to read the content of will before testator's death. The bank examines each beneficiary's identity and checks the authenticity of the death certificate of testator. The death certificate provides an additional security protection.

3.2.3. Forward Secrecy

In our system, if an attacker compromises any subset of old secret keys, he still cannot conclude any subsequent ones. This property means that no one can have the knowledge of the secret key that will be used in later sessions [2]. Once, the new secret key or the new will is established, it implies that previous ones are revoked. Essentially, these keys and the will are independent. No one can conclude a secret key from the previous keys. Therefore, our proposed scheme fulfills the property of forward secrecy.

4. Conclusions

The testamentary trust is a new field in some custody affairs. In the past, the testator writes his will and then conserves it with a trusted person. In recent years, there has been rapid development in the use of electronic documents for communicating over the Internet. These documents maybe contain sensitive information that have to be protected from disclosure. In cryptography, a certificate is able to use a digital signature to bind a public key with an identity. The certificate can be used to verify that a public key belongs to an individual. Those confidential data are encrypted such that only the intended receivers are able to access the content. In the digital world, the legal effects of electronic signature are identical to handwritten ones and guarantee authentication and integrity in the information signed. Thus, a digital will must satisfy the system requirements of the electronic document. We use some preliminary techniques which widely used in cryptosystems, such as the signature and the encryption/decryption techniques, to construct a concrete and feasible digital will system model. By utilizing the notion of the key escrow, a will needs to be encrypted and held in a trusted party so that under certain circumstances an authorized party can decrypt the will. The testator applies the properties of secret sharing schemes and the public key encryption method to generate his encrypted will. After the testator passes away, beneficiaries can employ their individual private keys to resolve the corresponding sub-secret keys and associate those sub-secret keys into the will secret key with the help of bank. Then, the bank decrypts the encrypted will. If beneficiary cannot reconstruct the secret key, the bank submits the encrypted will and encrypted secret key to the court. The latter recovers the will secret key and announces the will. For the effectiveness of the will and the list, the testator generates the encrypted will and the beneficiary list which must be notarized by the court before sending them to the will bank or the conservator. Therefore, these notarized cipher text could be regarded as effective document.

Currently, the electronic Wills Act is under discussions, but not put into practice yet. To date, there are no literatures discussing the issues of digital will. The properties of security, convenience and effectiveness are the most significant reasons why people would like to adopt the digital will mechanism in the future. Our proposed system is a robust mechanism to ensure that the will is generated by the testator, that the will is safely preserved by the bank, that the conservator could not obtain the encrypted will and that each beneficiary could not know the will content in advance. This digital will system not only achieves lots of essential security requirements, but also fulfills the above-mentioned properties, which also provides a practical solution to this subject for related researches in the future. In this paper, we do not discuss the processes of notarized will and the notarized list. Therefore, in our future work, we will pay more attention to the processes of notarizing. In addition, we will also attempt to remove the necessity of the semi-trusted role, i.e., bank involved in our system model.

References

[1] Ali Z. and Ahmed J., "New Computation Technique for Encryption and Decryption based on RSA and ElGamal Cryptosystems," *Journal of Theoretical and Applied Information Technology*, vol. 47, no. 1, pp. 73-79, 2013.

[2] Choi J. and Jung S., "A Handover Authentication using Credentials based on Chameleon Hashing," *IEEE Communications Letters*, vol. 14, no. 1, pp. 54-56, 2010.

[3] Civil Code, Laws and Regulations Database of The Republic of China, available at http://law.moj. gov.tw/Eng/LawClass/LawContent.aspx?pcode= B0000001, last visited 2013.

[4] Damgard I. and Thorbek R., "Linear Integer Secret-Sharing and Distributed Exponentiation," *in Proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography*, New York, pp. 75-90, 2006.

[5] Diffie W. and Hellman M., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[6] Elgamal T., "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[7] Fan R., Chen Y., and Shao J., "The Study of Testamentary Trust Business," available at http://www.trust.org.tw/files/981202.pdf, last visited 2014.

[8] Harn L. and Lin C., "Authenticated Group Key Transfer Protocol based on Secret Sharing," *IEEE Transactions on Computers*, vol. 59, no. 6, pp. 842-846, 2010.

[9] ISO/IEC 9594-8., "Information Technology-Open Systems Interconnection-The Directory: Authentication Framework," available at: https://www.itu.int/rec/T-REC-X.509, last visited 1998.

[10] ISO 7498-2, "Information processing systems-Open Systems Interconnection-Basic Reference Model- Part 2: Security Architecture," available at: www.iso.org/iso/ catalogue_detail.htm? csnumber=14256, last visited 1989.

[11] Lin H., "Toward Secure Strong Designated Verifier Signature Scheme from Identity-based System," *The International Arab Journal of Information Technology*, vol. 11, no. 4, pp.

315-321, 2014.

[12] Lin H., Wu T., and Huang S., "Certificate-Based Secure Three-Party Signcryption Scheme with Low Costs," *Journal of Information Science and Engineering*, vol. 28, no. 4, pp. 739-753, 2012.

[13] Micali S., "Fair Public-Key Cryptosystems," *in Proceedings of the 12th Annual International Cryptology Conference Santa Barbara*, California, pp. 113-138, 1992.

[14] Rivest R., Shamir A., and Adleman L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[15] Rivest R., Shamir A., and Tauman Y., "How to Leak a Secret," *in Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast*, Australia, pp. 552-565, 2001.

[16] Shamir A., "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[17] Stallings W., *Cryptography and Network Security: Principles and Practices*, Prentice Hall, 2010.

[18] Testamentary Trusts Bank., available at https://www.cathaybk.com.tw/cathaybk/trust/trust_2_1_4.asp, last visited 2014.

[19] Wu T., Lin H. and Ting P., "A Publicly Verifiable PCAE Scheme for Confidential Applications with Proxy Delegation," *Transactions on Emerging Telecommunications Technologies*, vol. 23, no. 2, pp. 172-185, 2012.

Tzong-Sun Wu received his BS degree in Electrical Engineering from National Taiwan University, Taiwan in 1990 and his PhD degree in Information Manage-ment from National Taiwan University of Science and Technology, Taiwan in 1998. From August 1998 to July 2001, he has been an Assistant Professor in the Department of Information Management, Huafan University. From August 2001 to January 2007, he has been an Associate Professor in the Department of Informatics, Fo Guang University. Currently, he is with the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include information security, watermarking, digital right management, and e-commerce.

Yih-Sen Chen received his BA degree in Information Manage-ment from Aletheia University, Taiwan in 1997, his MS degree in Informatics from Fo Guang University, Taiwan in 2006, and PhD degrees in Computer Science and Engineering from National Taiwan Ocean University, Taiwan in 2014. He is now an Assistant Engineer in the Department of Rapid Transit Systems, Taipei City Government. His current research interests include cryptography, information theory, security management, and network security.

Han-Yu Lin received his PhD degree in Computer Science and Engineering from the National Chiao Tung University, Taiwan in 2010. He served as a part-time Assistant Professor in both the Department of Information Management, Chang Gung University, Taiwan and the Department of Information Management, Kainan University, Taiwan from 2011. He has been an Engineer in CyberTrust Technology Institute, Institute for Information Industry, Taiwan from January 2012 to July 2012. Since August 2012, he has been an Assistant Professor in the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include cryptology, network security, digital forensics, RFID privacy and application, cloud computing security and e-commerce security.