Security Vulnerability in Identity-Based Public Key Cryptosystems from Pairings

Jyh-Haw Yeh

***Abstract*—Many identity-based public key cryptosystems from bilinear pairings use hash functions to construct their public keys. Most of these schemes only specify the need of applying cryptographic strong or collision free hash functions, without giving any detail of which or what hash functions should be used. Traditional understanding of a cryptographic strong hash function has three security properties, which are pre-image resistance, second pre-image resistance and collision resistance. However, with only these three properties, in this paper we show a potential security vulnerability of identity-based cryptographic cryptosystems if the hash functions used are not correctly constructed. To fix this vulnerability, this paper defines an additional desirable security property for the hash functions in these identity-based cryptosystems.**

***Index Terms*—Public key cryptosystems, identity-based cryptosystems, cryptographic strong hash functions, bilinear pairings.**

I. Introduction

Public key cryptography is used in a variety of security applications such as secure message exchange, secret sharing, digital signatures, digital watermarking, identity authentication, data integrity checking and much more. However, most of current existing public key cryptosystems require communicating parties knowing each other's public key. To ensure the validity of each other's public key, it requires a trusted third party issuing public key certificates [1] for all participating entities in a cryptosystem. Even though inquiring and verifying each other's public key certificate in every communication is not too expensive to do, it is obviously annoying and interruptive.

To take out the requirement of public key certificates, an identity-based cryptosystem, introduced by Shamir [2] in 1984, is a public key cryptosystem, which intended to embed user's identities into the construction of their public keys. As a result, each user can derive another user's public key without the need of public key certificates from a third trusted party.

In 2001, Boneh and Franklin [3] proposed an identity based encryption scheme from Weil pairings. Following their paper, many identity-based cryptographic schemes, based on bilinear pairings from supersingular elliptic curves, were proposed in the literature such as those in [4]–[14]. The public key generation in these schemes is simple and similar, merely the hash value of each user's publicly known identity. Instead of providing any specific hash functions, these schemes only gave a very general statement that the hash functions used must be cryptographic strong. Traditionally, a hash function is said to be cryptographic strong if it satisfies the following four properties: easy forward computation, pre-image resistance, second pre-image resistance and collision resistance. In this paper, we provide a simple hash function satisfying the above four properties, but the resulting identity-based schemes are insecure, where private keys can be easily derived from public keys.

To be secure against this vulnerability, the hash functions used must satisfy an additional property, name it "image ratio resistance" in this paper. A hash function H satisfying this property should generate images such that the ratio between them is hard to compute. In other words, given arbitrary two pre-images m_1 and m_2, it is hard to compute the ratio c such that $H(m_1) = cH(m_2)$ or $H(m_2) = cH(m_1)$. The main contribution of this paper is explicitly pointing out and defining this desired hash property in identity-based cryptosystems.

The rest of this paper is organized as follows: Section II gives the definition of a cryptographic strong hash function, as well as defining the proposed image ratio resistance hashing property. In this section, we also provide some mathematical background of bilinear pairings. Section III describes briefly the common key generation procedure in identity-based cryptosystems based on supersingular elliptic curves and its typical signature and verification scheme using bilinear pairings. Section IV gives a simple cryptographic strong hash function without the image ratio resistance property and then describes the security vulnerability of the resulting identity-based cryptosystems. Hash functions with the image ratio resistance property will also be suggested in this section. Finally, Section V concludes the paper.

II. Mathematical Background

In this section, we give some required mathematical background for identity-based cryptosystems, including cryptographic hash functions and bilinear pairings.

A. Hash Functions

Traditional cryptographically-strong hash functions $H : \{0,1\}^* \to Z_{2^l}^*$, where l is the pre-defined bit length of hash values, should satisfy the following properties:

1) Easy forward computation: Given a pre-image m, it should be computational efficient to derive $H(m)$.
2) Pre-image resistance: Given an image $H(m)$, it should be hard to find the pre-image m.
3) Second pre-image resistance: Given a pre-image m_1, it

Manuscript received April 5, 2013; revised June 24, 2013.

Jyh-Haw Yeh is with the Department of Computer Science, Boise State University, Boise, ID 83725, USA (e-mail: jhyeh@ boisestate.edu).

DOI: 10.7763/IJIET.2013.V3.319

should be hard to find another pre-image m_2, where $m_1 \neq m_2$, such that $H(m_1) = H(m_2)$.

4) Collision resistance: It should be hard to find any pair of pre-images m_1 and m_2, where $m_1 \neq m_2$, such that $H(m_1) = H(m_2)$.

The popular SHS [15] and MD5 [16] hash functions are believed to be cryptographically strong, even though some research showed that they were vulnerable to collision resistant. However, most of security schemes or protocols based on hash functions only rely on their pre-image resistance and/or second pre-image resistance. Thus, these security schemes/protocols are still safe for now.

In this paper, we propose and define another hash function property, image ratio resistance, as below:

Definition: A hash function H is said to be image ratio resistance if it is hard to derive the ratio c such that $H(m_1) = cH(m_2)$ or $H(m_2) = cH(m_1)$, given arbitrary two different pre-image m_1 and m_2.

For the proposed image ratio resistance, the traditional hash functions $H: \{0, 1\}^* \rightarrow Z_{2^l}^*$ is impossible to satisfy this property since the ratio c between two images $H(m_1) \in Z_{2^l}^*$ and $H(m_2) \in Z_{2^l}^*$ is merely the fraction $H(m_1)/H(m_2)$ or $H(m_2)/H(m_1)$.

In the context of identity-based cryptosystems, the hash function used is a mapping $H: \{0, 1\}^* \rightarrow G$, where G is a cyclic additive group of some prime order q with a generator P. In this mapping, it is possible to construct a hash function satisfying the image ratio resistance, in addition to the three original resistances.

Without using image ratio resistance hash functions, identity-based cryptosystems are insecure. Unfortunately, most identity-based papers only specify the need of using cryptographic strong hash functions, which do not include the property of image ratio resistance. In Section IV, we give a simple cryptographic hash function that satisfies the original three resistance properties but fails on the image ratio resistance, and then describe a potential security vulnerability of the resulting identity-based cryptographic schemes.

B. Bilinear Pairings

Given a cyclic additive group $(G_1, +)$ with a generator P and a cyclic multiplicative group $(G_2, \times)$ of the same prime order q, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

- Bilinearity:

$$\begin{aligned} &\forall Q,\ R, S \in G_1, \forall a, b \in F_q^*, \\ &e(Q, R) = e(R, Q) \\ &e(aQ, bR) = e(Q, R)^{ab} = e(bQ, aR) \\ &e(Q, R+S) = e(Q, R)e(Q, S) \end{aligned} \tag{1}$$

- Non-degeneracy:

$$\begin{aligned} &\forall Q \in G_1, \\ &e(Q, R) = 1, \forall R \in G_1 \Leftrightarrow Q = O \end{aligned} \tag{2}$$

- Computability: There is an efficient algorithm to compute

$$e(Q, R) \in G_2, \forall Q, R \in G_1 \tag{3}$$

The security of bilinear maps relies on the hardness assumption of some Diffie-Hellman problems such as

1) Computational Diffie-Hellman Problem (CDHP): Given $Q, aQ, bQ \in G_1$ and $a, b \in F_q^*$, to compute $abQ \in G_1$.
2) Decision Bilinear Diffie-Hellman Problem (DBDHP): Given $Q, aQ, bQ, cQ \in G_1$ and $a, b, c \in F_q^*$, and an element $g \in G_2$, to decide whether $g = e(Q, Q)^{abc}$.

The security of the identity-based signature scheme demonstrated in the next section, as well as most of other identity-based cryptographic schemes, is based on the hardness assumption of CDHP.

III. Common Identity-Based Cryptosystem Key Generation

In this section, we describe briefly the common key generation procedure in most identity-based cryptosystems. Each user U_i in a system has a unique identity $ID_i \in \{0,1\}^*$. There is a trusted private key generator (PKG) responsible for key generation.

A. Setup

PKG chooses a cyclic additive group $(G_1, +)$ and a cyclic multiplicative group $(G_2, \times)$ of the same prime order q, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$, a generator P of the group G_1, a master private key $s \in F_q^*$, a system public key

$$P_{pub} = sP \in G_1 \tag{4}$$

and two cryptographic strong hash functions

$$H_1: \{0, 1\}^* \rightarrow G_1 \tag{5}$$

$$H_2: \{0, 1\}^* \rightarrow F_q^* \tag{6}$$

PKG then publishes the public parameters

$$PARA = < G_1, G_2, e, P, P_{pub}, q, H_1, H_2 > \tag{7}$$

B. Key Generation

Given an ID_i of a user U_i, the PKG computes U_i's public key Q_i and private key D_i by

$$Q_i = H_1(ID_i) \tag{8}$$

$$D_i = sQ_i \tag{9}$$

Both Q_i and D_i are points in the group G_1. The PKG then sends both keys to U_i, in which the private key D_i needs to be sent by a secure channel.

Many proposed identity-based signature, encryption or signcryption schemes in the literature generate their public and private key pair as (8) and (9). Following the key

generation, we give a typical identity-based signature scheme in the following sections for the purpose of completeness and readability, though our proposed security vulnerability only exploits the weakness of the key generation procedure.

C. Signature Generation

To sign a message $m \in \{0,1\}^*$, a user U_i randomly picks a number $r_i \in F_q^*$. U_i computes two points V_i and S_i in G_1 as follows:

$$V_i = r_i P \tag{10}$$

$$S_i = H_2(m, [V_i]_x) D_i + r_i P_{pub} \tag{11}$$

where $[V_i]_x$ is the *x*-coordinate of the point V_i. The signature on the message m is the pair (V_i, S_i).

D. Signature Verification

U_i's signature (V_i, S_i) on the message m can be publicly verified. The verifier compares whether

$$e(P, S_i) = e(P_{pub}, Q_i)^{H_2(m,[V_i]_x)} e(P_{pub}, V_i) \tag{12}$$

The signature (V_i, S_i) is valid if and only if the checking in (12) return true since

$$\begin{aligned}
& e(P, S_i) \\
&= e(P,\ H_2(m,[V_i]_x) D_i + r_i P_{pub}) && by\ Eq.(11) \\
&= e(P, H_2(m,[V_i]_x) sQ_i + r_i sP) && by\ Eq.(4),(9) \\
&= e(sP,\ H_2(m,[V_i]_x) Q_i + r_i P) && by\ Eq.(1) \\
&= e(sP,\ H_2(m,[V_i]_x) Q_i) e(sP, r_i P) && by\ Eq.(1) \\
&= e(P_{pub}, H_2(m,[V_i]_x) Q_i) e(P_{pub}, V_i) && by\ Eq.(4),(10) \\
&= e(P_{pub}, Q_i)^{H_2(m,[V_i]_x)} e(P_{pub}, V_i) && by\ Eq.(1)
\end{aligned}$$

IV. Security Analysis

Before exploiting the potential vulnerability of the common key generation procedure described in the section III.B, we first discuss the hardness assumption of CDHP and its implication to the security of identity-based cryptosystems.

A. Hardness Assumption of CDHP

The security of the identity-based cryptosystem is based on the hardness assumption of CDHP. For the signature scheme presented in the previous section, a malicious user U_i may try to derive secret information $r_j P_{pub}$ inside another user U_j's signature $S_j = H_2(m, [V_j]_x) D_j + r_j P_{pub}$. This derivation is a difficult CDHP since U_i, with known information P, sP (which is P_{pub}) and $r_j P$ (which is V_j), is trying to compute $r_j sP$ (which is $r_j P_{pub}$). Another example of a CDHP in this scheme is trying to maliciously derive someone's private key as follows: A user U_i can access his own keys Q_i and $D_i = sQ_i$, as well as another user U_j's public key Q_j. Since P is a generator in G_1 and both Q_i and Q_j are points in G_1, there exist $a, b \in F_q^*$ such that $Q_i = aP$ and $Q_j = bP$. Thus $c = (b/a) \bmod q$ also exists and $Q_j = cQ_i$. With known information Q_i, cQ_i (which is Q_j) and sQ_i (which is D_i), it is a CDHP if the malicious user U_i tries to derive another user U_j's private key $D_j = sQ_j = scQ_i$.

Therefore, under the hardness assumption of CDHP, deriving other user's private key should be hard if both $s \in F_q^*$ and $c \in F_q^*$ are unknown. However, if either s or c can be inferred by some other means, the private key can be derived easily, or in other words, the identity-based cryptosystems are insecure.

B. The Potential Security Vulnerability

Security vulnerability can be exploited in the common key generation procedure in most of the identity-based cryptographic schemes. The vulnerability described in this section can be applied to all these identity-based schemes. Assume an implementer of an identity-based scheme is misguided by the scheme specification and uses a cryptographic strong hash function satisfying only the original three resistance properties. There is a straightforward way to come up such hash function, $H_1 : \{0,1\}^* \to G_1$, to map a user U_i's identity ID_i to his public key Q_i as below:

$$H_1(ID_i) = H_3(ID_i) P = Q_i \tag{13}$$

where $H_3 : \{0,1\}^* \to F_q^*$ is a regular cryptographic hash function such as those in [15] and [16] with the original three resistance properties, i.e., pre-image resistance, second pre-image resistance and collision resistance. The following three propositions show that the hash function H_1 defined in (13) also satisfies the original three cryptographic resistance properties.

Proposition 1: Given that $H_3 : \{0,1\}^* \to F_q^*$ is a cryptographic strong hash function satisfying the original three resistance properties. The hash function $H_1 : \{0,1\}^* \to G_1$ defined in (13) also satisfies the pre-image resistance property.

Proof: Given that $H_1(ID_i) = H_3(ID_i) P$ and $H_3 : \{0,1\}^* \to F_q^*$ satisfies the pre-image resistance property. Let's assume H_1 does not satisfy the pre-image resistance property. That means ID_i can be recovered from $H_1(ID_i)$. Under this assumption, given $H_3(ID_i)$, ID_i can also be recovered since someone can first compute $H_3(ID_i)P = H_1(ID_i)$ and then recover ID_i from $H_1(ID_i)$. It implies that H_3 does not satisfy the pre-image resistance property. This is a contradiction and thus the assumption we made about H_1 is incorrect. Therefore H_1 should satisfy the pre-image resistance property.

Proposition 2: Given that $H_3 : \{0,1\}^* \to F_q^*$ is a cryptographic strong hash function satisfying the original three resistance properties The hash function $H_1 : \{0,1\}^* \to G_1$ defined in (13) also satisfies the second

pre-image resistance property.

Proof: Given that $H_1(ID_i) = H_3(ID_i)P$ and $H_3 : \{0,1\}^* \rightarrow F_q^*$ satisfies the second pre-image resistance property. Let's assume H_1 does not satisfy the second pre-image resistance property, which means that, given ID_i, it's not hard to find a pre-image $ID_j \neq ID_i$ such that $H_1(ID_j) = H_1(ID_i)$. Under this assumption, given ID_i and the hash function H_3, someone can first compute $H_3(ID_i)P = H_1(ID_i)$ and then find a pre-image $ID_j \neq ID_i$ such that $H_1(ID_j) = H_1(ID_i)$. This ID_j actually is a pre-image such that $H_3(ID_j) = H_3(ID_i)$. It implies that H_3 does not satisfy the second pre-image resistance property. This is a contradiction and thus the assumption we made about H_1 is incorrect. Therefore H_1 should satisfy the second pre-image resistance property.

Proposition 3: Given that $H_3 : \{0,1\}^* \rightarrow F_q^*$ is a cryptographic strong hash function satisfying the original three resistance properties. The hash function $H_1 : \{0,1\}^* \rightarrow G_1$ defined in (13)also satisfies the collision resistance property.

Proof: Given that $H_1(ID_i) = H_3(ID_i)P$ and $H_3 : \{0,1\}^* \rightarrow F_q^*$ satisfies the collision resistance property. Let's assume H_1 does not satisfy the collision resistance property, which means that it's not hard to find a pair of (ID_i, ID_j), where $ID_i \neq ID_j$, such that $H_1(ID_i) = H_1(ID_j)$. Under this assumption, given the hash function H_3, the pair (ID_i, ID_j) satisfies $H_1(ID_i) = H_1(ID_j)$ will also satisfies $H_3(ID_i) = H_3(ID_j)$ since $H_1(ID_i) = H_1(ID_j) \Rightarrow H_3(ID_i)P = H_3(ID_j)P \Rightarrow H_3(ID_i) = H_3(ID_j)$. This implies that H_3 does not satisfy the collision resistance property. This is a contradiction and thus the assumption we made about H_1 is incorrect. Therefore H_1 should satisfy the collision resistance property.

The above three propositions showed that H_1 defined in (13) satisfies the original three resistance properties for a cryptographic strong hash function. However, H_1 fails to have the image ratio resistance we defined in this paper since, given ID_i and ID_j, it is easy to compute the ratio

$$c = (H_3(ID_j) / H_3(ID_i)) \mod q \qquad (14)$$

such that $Q_j = cQ_i$ as shown below.

$$\begin{aligned} cQ_i &= (H_3(ID_j)/H_3(ID_i))\ Q_i && \text{by Eq. (14)} \\ &= (H_3(ID_j)/H_3(ID_i))\ H_3(ID_i)P && \text{by Eq. (13)} \\ &= H_3(ID_j)P \\ &= Q_j \mod q && \text{by Eq. (13)} \end{aligned}$$

A malicious user U_i can take advantage of the computable ratio among public keys to derive another user U_j's private key D_j by the following steps:

- U_i computes the ratio $c = Q_j / Q_i$ by calculating $c = (H_3(ID_j)/H_3(ID_i)) \mod q$.
- U_i computes $cD_i = csQ_i = sQ_j = D_j$.

The derivation of another user U_j's private key is no longer a CDHP (refer to Section IV.A) since the ratio c can be inferred from insecure generation of Q_i and Q_j. This security vulnerability can be fixed by using hash functions with the image ratio resistance. The hash functions based on the map-to-curve or map-to-point algorithms from Weil pairings in [3], [4] are actually such functions, though these algorithms were not designed specifically for the image ratio resistance.

V. Conclusion

The main contribution of this paper is defining an additional desirable cryptographic hashing property, image ratio resistance, to hash functions for identity-based cryptosystems. Without this hashing property, this paper showed the identity-based cryptosystems are potentially insecure. Most of these identity-based cryptosystems only specify the need of using cryptographic strong hash functions for mapping a string to a point in a cyclic additive group. Traditional understanding of cryptographic strong hash functions does not include the property of image ratio resistance. An example of such cryptographic hash functions without the image ratio property is also given in this paper. As a result, readers or implementers of these identity-based cryptosystems may be misguided to develop insecure cryptographic schemes.

References

[1] D. Cooper, S. Santesson, S. Farrell, S.Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," *Request for Comments 5280 (RFC 5280)*, 2008.

[2] A. Shamir, "Identity Based Cryptosystems and Signature Schemes," *CRYPTO'84*, *LNCS*, Springer, 1984, pp. 47-53.

[3] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing," *CRYPTO'01*, *LNCS*, Springer, vol. 2139, 2001, pp. 213-229.

[4] X. Yi, "An Identity-based Signature Scheme from the Weil Pairing," *IEEE Communications Letter*, vol. 7, no. 2, 2002, pp. 76-78.

[5] C. Gentry and A. Silverberg, "Hierarchical ID-based Cryptography," *ASIACRYPT'02*, *LNCS*, Springer, vol. 2501, 2002, pp. 548-566.

[6] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *SAC'02*, *LNCS*, Springer, vol. 2595, 2003, pp. 310-324.

[7] B. Libert and J. J. Quisquater, "A New Identity Based Signcryption Scheme from Pairings," in *Proc. IEEE Information Theory Workshop*, 2003, pp. 155-158.

[8] X. Boyen, "Multipurpose Identity-based Signcryption: A Swiss Army Knife for Identity-based Cryptography," *CRYPTO'03*, *LNCS*, Springer, vol. 2729, 2003, pp. 383-399.

[9] J. C. Cha and J. H. Cheon, "An Identity-based Signature from Gap Diffie-Hellman Groups," *PKC'03*, *LNCS*, Springer, vol. 2567, 2003, pp. 18-30.

[10] D. Boneh and X. Boyen, "Secure Identity Based Encryption without Random Oracles," *CRYPTO'04*, *LNCS*, Springer, vol. 3152, 2004, pp. 443-459.

[11] X. Li and K. Chen, "Identity Based Proxy-Signcryption Scheme from Pairings," in *Proc. the 2004 IEEE International Conference on Service Computing*, 2004, pp. 494-497.

[12] L. Chen and J. Malone-Lee, "Improved Identity-based signcryption," *PKC'05*, *LNCS*, Springer, vol. 3386, 2005, pp. 362-379.

[13] A. Awasthi and S. Lal, "ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings," *International Journal of Network Security*, vol. 4, no. 2, 2007, pp. 187-192.

[14] J. Liu and S. Huang, "Identity-based Threshold Proxy Signature from Bilinear Pairings," *Informatica*, vol. 21, no. 1, 2010, pp. 41-56.
[15] Information Technology Laboratory, National Institute of Standards and Technology, "Secure Hash Standard (SHS)," *Federal Information Processing Standards Publication (FIPS PUB 180-4)*, March 2012.
[16] R. Rivest, "The MD5 Message-Digest Algorithm," *Request for Comments 1321 (RFC 1321)*, 1992.

Jyh-Haw Yeh was born in Taoyuan, Taiwan on May 20, 1966. He received a B.A. degree in applied mathematics from National Chung-Hsing University, Taiwan in 1984, a M.S. degree in computer Information science from Cleveland State University, Cleveland, Ohio in 1993, and a Ph.D degree in computer and information Science and Engineering from University of Florida in 1999. His major research field is in computer security in general.

He is a faculty at Boise State University (BSU), Boise, Idaho. He joined BSU since 2000. He was awarded tenure at 2006. He has published more than 40 conference/journal articles, including IEEE/ACM conferences and Elsevier journals such as Information Processing Letters, Computer Networks and Information Sciences. His current research interests are database security, cryptography, and cloud security.

Dr. Yeh is currently a member of the Association of Computing Machinery. He also serves as an Associate Editor for the International Journal of Handheld Computing Research since 2009; Editorial Board of the Journal of Computer Science and Systems Biology since 2010; Program Committee of the 6th IEEE International Conference on Ubi-Media Computing 2013; International Program Committee of the ACIS International Conference on Software Engineering Research, Management and Applications (SERA 2009 and SERA 2110); Program Committee of 2009 World Congress on Computer Science and Information Engineering (CSIE 2009); 2008 NSF Cyber Trust Panelist; Editorial Review Board of the International Journal of E-Business Research (IJEBR) from 2004 to 2008; Program Committee of the 2004 & 2005 IRMA International Conferences; Outstanding Students Award, University of Florida, 1999.