Perspectives in Science (2016) 7, 81—86

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/pisc

A brief review of revocable ID-based public key cryptosystem☆

Tsu-Yang Wu[a,b,*], Jerry Chun-Wei Lin[a,b], Chien-Ming Chen[a,b], Yuh-Min Tseng[c], Jaroslav Frnda[d], Lukas Sevcik[d], Miroslav Voznak[d]

[a] *Shenzhen Graduate School, Harbin Institute of Technology, China*
[b] *Shenzhen Key Laboratory of Internet Information Collaboration, Shenzhen, China*
[c] *Department of Mathematics, National Changhua University of Education, Taiwan, ROC*
[d] *Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. listopadu 15, Ostrava-Poruba 708 00 Czech Republic*

Received 26 October 2015; accepted 11 November 2015
Available online 10 December 2015

KEYWORDS
Identity-based;
Revocable;
Encryption;
Bilinear pairings

Summary The design of ID-based cryptography has received much attention from researchers. However, how to revoke the misbehaviour/compromised user in ID-based public key cryptosystem becomes an important research issue. Recently, Tseng and Tsai proposed a novel public key cryptosystem called revocable ID-based public key cryptosystem (RIBE) to solve the revocation problem. Later on, numerous research papers based on the Tseng-Tsai key RIBE were proposed. In this paper, we brief review Tseng and Tsai's RIBE. We hope this review can help the readers to understand the Tseng and Tsai's revocable ID-based public key cryptosystem.

Introduction

In the traditional public key cryptosystems (Diffie and Hellman, 1976; ElGamal, 1985; Rivest et al., 1978), certificates play important roles to make publicly available the mapping between identities and public keys. Certificate is a signature generated by a trusted certificate authority (CA) which usually include the identity of a user, its associated public key, the issuing date and the expiration date. When user's public key is used, the associated certificate must be checked to ensure its validity (revoked or non-revoked). In general, Certificate Revocation List (CRL) (Housley et al., 2002) is used to revoke the user's public key. Anyone can check these revoked users' public keys by querying the CRL.

In order to solve the management of users' certificates, Shamir (1984) first proposed the concept of ID-based public key cryptosystem (ID-PKS). In his system, each user's

☆ This article is part of a special issue entitled ''Proceedings of the 1st Czech-China Scientific Conference 2015''.

* Corresponding author at: Shenzhen Graduate School, Harbin Institute of Technology, China.
URL: https://www.linkedin.com/in/tsu-yang-wu-4a6b029a/en (T.-Y. Wu).

http://dx.doi.org/10.1016/j.pisc.2015.11.014

identity (e.g. e-mail address or social security number) can be viewed as public key and the user's private key is generated by a trusted private key generation center (PKG). However, Shamir' ID-PKS was not easy in practice because the underlying mathematical methods are not suitable. In 2001, Boneh and Franklin, (2001) followed Shamir's concept to propose a practical ID-based encryption scheme (IBE) from the Weil pairing. Later on, the design of ID-based cryptographic schemes and protocols using bilinear pairings has received much attention from researchers.

For the revocation problem in the ID-PKS system, Boneh and Franklin, (2001) have suggested a solution in which the PKG can periodically renew the private keys for non-revoked users. In other words, when the PKG wants to revoke a specific user, it only stops to issue the new private key. However, this solution has following drawbacks: (1) the workload of generating new private keys of non-revoked users is too heavy for the PKG; (2) secure channels are needed between the PKG and the non-revoked users to transmit the new private keys for each time period.

Boldyreva et al. (2008) proposed a revocable ID-based encryption scheme (RIBE) by using binary tree to reduce the PKG's workload in the Boneh—Franklin IBE. Unfortunately, their scheme is based on the relaxed selective-ID model (Canetti et al., 2003), a weak security model. In the next year, Libert and Vergnaud (2009) based on the Boldyreva et al.'s RIBE to propose a more secure RIBE scheme under an adaptive-ID model, a strong security model. Seo and Emura (2013a) demonstrated Boldyreva et al.'s RIBE (Boldyreva et al., 2008) is vulnerable to the decryption key exposure. They also proposed a provably secure tree-based revocable ID-based encryption scheme. Subsequently, Seo and Emura (2013b) presented a hierarchical revocable ID-based encryption scheme which solved the open problem mentioned in the Libert—Vergnaud RIBE.

Tseng and Tsai (2012) proposed a practical RIBE scheme over a public channel. The key construction their scheme is different from the previous schemes (Boldyreva et al., 2008; Libert and Vergnaud, 2009; Seo and Emura, 2013a,b). In the Tseng-Tsai RIBE, each user's private key consists of a fixed initial private key and an updating time key, where the updating time key is renewed along with the current period. For an honest (non-revoked) user, the PKG periodically issues new time key and sends it to the user via a public channel. Upon receiving the new time key, the user can renew her/his private key by herself/himself. To revoke a malicious/misbehaviour user, the PKG only stops issuing the new time key in current period. In other words, the malicious/misbehaviour user cannot compute the newest private. She/he cannot execute any cryptographic behaviours in later periods. Later on, several revocable ID-based cryptographic schemes and protocols based on the key construction of the Tseng-Tsai RIBE were proposed such as encryption (Tsai et al., 2012, 2014), signature (Hung et al., 2014; Tsai et al., 2013; Wu et al., 2012a), signcryption (Wu et al., 2012b), and authenticated group key exchange (Wu et al., 2012, 2014).

In this paper, we brief review Tseng and Tsai's RIBE scheme which contains the underlying mathematical problems and assumptions, the framework of RIBE, a concrete RIBE scheme, the security notion of RIBE, the security analysis of RIBE (sketched), and a full RIBE scheme. We hope this review can help the readers to understand the Tseng and Tsai's revocable ID-based public key cryptosystem.

Underlying mathematical problems and assumptions

Bilinear pairings

Bilinear pairings defined on elliptic curves over finite fields have been used to establish many ID-based cryptographic mechanisms. Let G_1 be an additive cyclic group of large prime order q and G_2 be a multiplicative cyclic group of the same order q. Specifically, particular, G_1 is a subgroup of the group of points on an elliptic curve over a finite field and G_2 is a subgroup of the multiplicative group over a finite field. A bilinear pairing is a map e: $G_1 \times G_1 \rightarrow G_2$ and satisfies the following three properties:

(1) Bilinear. $e(aP, bQ) = e(P, Q)^{ab}$, for all $P, Q \in G_1$ and $a, b \in Z_q^*$.
(2) Non-degenerate. There exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
(3) Computable. For all $P, Q \in G_1$, there is an efficient algorithm to compute $e(P, Q)$.

A bilinear map that satisfies the above three properties is called an admissible bilinear map. Such non-degenerate admissible bilinear maps can be obtained from the Weil, Tate, or Ate pairings over supersingular elliptic curves or abelian varieties (Boneh and Franklin, 2001; Chen et al., 2007). Some research results (Galbraith et al., 2008; Wu and Tseng, 2010) for the relationship between security levels and speed of pairing computations on microprocessors were presented.

Bilinear Diffie—Hellman (BDH) assumption

The BDH assumption is often used in the security proof of ID-based encryption scheme. The BDH problem is described as follows. Given $P, aP, bP, cP \in G_1$ for some $a, b, c \in Z_q^*$, this problem is to compute the value $e(P, P)^{abc} \in G_2$. The BDH assumption is stated as follows.

Definition 1 *(BDH assumption)*. Given an additive cyclic group G_1 and $P, aP, bP, cP \in G_1$ for unknown $a, b, c \in Z_q^*$, no probabilistic polynomial time (PPT) algorithm A with non-negligible probability which can compute $e(P, P)^{abc} \in G_2$. The successful probability (advantage) of A is presented as

$$\mathrm{Adv}_A = Pr[P \in G_1, a, b, c \in Z_q^* | A(P, aP, bP, cP) = e(P, P)abc \in G_2],$$

where the probability is over the random choice consumed by A.

Framework of the Tseng-Tsai RIBE

The Tseng-Tsai RIBE consists of two roles: a trusted PKG and users. Without loss of generality, the whole lifetime of the system is divided into distinct time periods 1, 2, ..., z. For