ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2013, Vol. 42, No. 3

A Novel Designated Verifier Signature Scheme Based on Bilinear Pairing

Cheng-Chi Lee[1], Yan-Ming Lai[2], Chin-Ling Chen[3], Lung Albert Chen[4*]

[1] *Department of Library and Information Science*
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang Dist.,
New Taipei City 24205, Taiwan, R.O.C.
e-mail: cclee@mail.fju.edu.tw

[2] *Graduate Institute of Networking and Multimedia*
National Taiwan University
#1 Roosevelt Rd. Sec. 4,
Taipei 106, Taiwan, R.O.C.

[3] *Department of Computer Science and Information Engineering*
Chaoyang University of Technology
No. 168, Jifong E. Rd., Wufong Shiang,
Taichung, Taiwan, R.O.C.

[4] *Department of Multimedia Information Science and Applications*
Asia University
No. 500, Lioufeng Road, Wufeng Shiang,
Taichung, Taiwan, R.O.C.

crossref http://dx.doi.org/10.5755/j01.itc.42.3.2549

Abstract. A designated verifier scheme can protect information from uncertainty. Only the designated verifier can verify the signature and make sure that the information is correct. In addition, a strong designated verifier scheme allows the verifier to maintain a transcript signature of the verifier's secret key. Recently, Yoon proposed an identity-based strong designated verifier signature scheme to solve the problems of some previously proposed schemes. Unfortunately, Yoon's scheme still has some weaknesses, such as inefficiency in the verifying phase and being vulnerable to replay-attack. To overcome these, we propose a novel designated verifier signature scheme in this paper.

Keywords: bilinear pairing; designated verifier; ID-based cryptography; signature.

1. Introduction

Digital document has been widely used since the development of network. However, digital document from the network is not considered always dependable. Malicious digital document may come from malicious user or be modified by an attacker. To guarantee the integrity and originality of a piece of information, digital signature is proven to be a proper solution. Whitfield Diffie and Martin Hellman proposed the first description about digital signature in 1976 [2]; and the first operation based on the RSA algorithm was proposed in 1978 [11]. Since the digital signature scheme, people can trust the information originality in Internet. Nowadays, digital signature is used even more widely, such as in e-voting, e-commerce, and e-taxation. Digital signature not only guarantees the integrity of information, but also achieves non-repudiation, that is, everyone must be responsible for his/her behavior on Internet [7].

However, a typical digital signature scheme allows anyone to verify the validity of a given signature with the signer's public key. In some scenarios, signer wants to keep his/her privacy and only allows the designated verifier to verify the validity of the signature, such as in e-voting [1, 17]. In e-voting, a

* Corresponding E-mail: achen@asia.edu.tw

voter must be responsible for his/her vote, and the voting center has to verify the validity of the received votes. For this reason, digital signature is necessary in e-voting. If e-voting uses the typical digital signature scheme, then anyone can verify the signature, such as the candidates, and by doing so they can figure out the original of the signature. Therefore, the typical digital signature scheme is not suitable for every scenario.

To solve this problem, Jakobsson, Sako, and Impagliazzo introduced the concept of designated verifier signature (DVS) in 1996 [4]. DVS does not allow the signature to be transferred to a third party from the designated verifier. In the case of e-voting, the candidate is considered a third party that is not trustworthy, and only the voting center is the designated verifier. Jakobsson et al. also introduced a stronger vision to forbid the third party to verify the signature. In 2003, Saeednia et al. [12] formalized the strong DVS (SDVS) notation and proposed an efficient scheme. The SDVS allows the signer to embed the designated verifier's private parameters in the signature, and only the designated verifier can verify the validity of the signature. This ensures that any third party cannot verity the integrity and originality of the signed contents, and the signer is no longer responsible for undesignated verifier.

Following that, many variants of the designated verifier signature schemes were proposed [6, 10, 14, 15]. In 2008, Zhang and Mao [17] proposed a novel ID-based strong designated verifier signature scheme and they claimed their scheme achieved source hiding. However, Huang et al. [3] pointed out Zhang and Mao's scheme fails in source hiding. In the same year, Kang et al. [5] showed that Zhang-Mao's scheme cannot satisfy the strong designated verifier signature, either. To overcome the problem of Zhang's scheme, Kang et al. proposed an efficient ID-based designated verifier signature scheme in the same paper and claimed their scheme is strong and unforgeable.

Nevertheless, Yoon pointed out that the Kang et al.'s scheme still cannot survive the forgery attacks, in 2011 [16]. Furthermore, the Kang et al.'s is also vulnerable to the replay attack because the receiver cannot judge whether the received signature is fresh or not. To improve the designated verifier signature scheme, Yoon proposed an efficient and secure scheme. Unfortunately, Yoon's scheme is inefficient in the verify phase and is vulnerable to the replay attack. The details of Yoon's scheme's weaknesses are described in section 4. To overcome these weaknesses, we propose a novel designated verifier signature in this paper.

The paper is organized as follows. Section 2 describes the background concepts of bilinear pairings, and their security properties. We review the Yoon's scheme in Section 3 and then show its weaknesses in Section 4. Section 5 presents the proposed novel ID-based designated verifier signature and Section 6 analyzes its security and efficiency. Finally, Section 7 is our conclusion of this paper.

2. Preliminaries

2.1. Bilinear Pairing

Bilinear pairing is adopted in both, Yoon's scheme and ours. We briefly describe the characters and some related mathematical elements in this section [13]. Let G be a cyclic additive group, and G_T be a cyclic multiplicative group, where G and G_T have the same prime order q, which means $|G|=|G_T|$. After that, we define $\hat{e}:G\times G\rightarrow G_T$ as a bilinear map. Bilinear map has some mathematical characters as follows:

1. **Bilinearity:** Let $\{a, b\}\in Z_q$ and $\{P, Q\}\in G$, $\hat{e}(aP, bQ)$ satisfies $\hat{e}(aP, bQ)= \hat{e}(P, Q)^{ab}$.
2. **Non-degenerate:** There exist $\{P, Q\} \in G$ such that $\hat{e}(P, Q)\neq 1$.
3. **Computability:** There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $\{P, Q\} \in G$.

The security of cryptographic algorithm is always based on the hardness of some mathematical problems, and that there is no powerful enough algorithm to solve those problems in a reasonable period of time. Bilinear pairing is also based on the hard problems, which are described as follows [8]:

1. **The discrete logarithm problem (DLP):** Given $\{P, Q\} \in G$. It is hard to find an integer $a \in Z_q^*$ such that $Q = aP$.
2. **The computational Diffie–Hellman problem (CDHP):** Given $\{a, b, c\} \in Z_q$ and $\{P, aP, bP\} \in G$. It is hard to compute abP.
3. **The bilinear Diffie–Hellman problem (BDHP):** Given $\{a, b, c\} \in Z_q$ and $\{P, aP, bP, cP\} \in G$. It is hard to compute $\hat{e}(P, P)^{abc}$.

2.2. Security properties

To be more feasible, the designated verifier signature scheme should also satisfy the following security properties [16, 17].

1. Correctness: To guarantee the information correctness is the prime design goal of the digital signature, regardless of which digital signature class.
2. Strength: To ensure only the designated verifier can verify the signature, the secret key of the designated verifier should be involved in the signature.
3. Unforgeability: Forgery attack will cause the signature scheme to lose its reliability, and non-repudiation. For this reason, a secure digital signature scheme should be unforgeable.
4. Source hiding: If a designated verifier signature's original is revealed, it defeats the purpose of the primary design goal. Because of that, a designated verifier signature scheme should hide the source of signature, and ensure no one can find the original from the body of the information and its signature.

5. Non-transferability: To ensure the signature will not be disclosed and transferred, a designated verifier scheme should avoid the designated verifier from revealing the validity of a signature to any third party.

3. A review of Yoon's scheme

Yoon's scheme is composed of five phases [16]: *Setup phase*, *Key-Extract phase*, *Sign phase*, *Verify phase*, and *Transcript simulation phase*. To explain this scenario in an example, we assume there are two users, the signer Alice and the designated verifier Bob, where Alice owns the *IDA* and Bob owns the *IDB*. The details are described as following.

1. Setup phase

In *Setup phase*, the PKG (private key generation center) has to define the system parameters, such as master secret key and public key. PKG defines the bilinear map as $\hat{e}: G \times G \rightarrow G_T$, where G is a cyclic additive group, and G_T is a cyclic multiplicative group, and $\{G, G_T\}$ have the same prime order q. PKG then chooses an arbitrary value $P \in G$, and selects a random number $s \in Z_q^*$ as the master key of system and computes the public key $P_{pub} = sP$. In addition, PKG selects two one-way hash functions $H_1()$ and $H_2()$, where $H_1(): \{0, 1\}^* \rightarrow G$ and $H_2(): \{0, 1\}^* \times G \rightarrow G_T$. Finally, PKG publishes the system public parameters $\{\hat{e}, G, G_T, P, P_{pub}, q, H_1(), H_2()\}$, and keeps master keys secret.

2. Key-Extract phase

In *Key-Extract phase*, PKG generates the privacy key $S_{ID} = sH_1(ID)$ for each *ID*, and sends it to the user. The pubic key of each *ID* is $Q_{ID} = H_1(ID)$. ID-based design allows the user to compute the other user's public key without relying on the third party.

3. Sign phase

When Alice wants to sign the message M and send it to Bob, Alice has to compute $Q_{IDB} = H_1(IDB)$ first. Next, Alice selects a random number $r \in Z_q^*$, and computes signatures σ:

$\sigma = H_2(M, \hat{e}(rQ_{IDB}, S_{IDA}))$.

Finally, Alice sends $\{M, r, \sigma\}$ to Bob.

4. Verify phase

Upon receiving the information, Bob must compute Q_{IDA} before verifying the signature. After that, Bob checks σ as follows:

$\sigma = ?H_2(M, \hat{e}(S_{IDB}, rQ_{IDA}))$.

If the equation is correct, Bob accepts the information; otherwise, Bob rejects it. *Sign phase* and *Verify phase* in Yoon's scheme are shown in Figure 1.

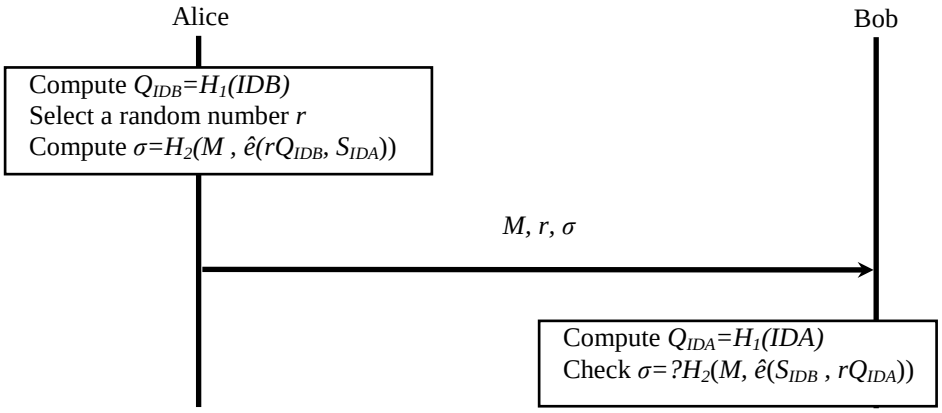

Figure 1. Sign phase and verify phase in Yoon's scheme

5. Transcript simulation phase

When Bob accepts the message and signature from Alice, he can produce the transcripts. First, Bob selects a random number $r' \in Z_q^*$, which is different than r, and computes $\sigma' = H_2(M, \hat{e}(S_{IDB}, r'Q_{IDA}))$. Finally, Bob stores $\{r', \sigma'\}$.

4. Cryptanalysis of Yoon's scheme

Yoon proposed a simple scheme for designated verifier signature. Unfortunately, the proposed scheme has two weaknesses--inefficiency in verification phase and being vulnerable to the replay attack. The detail is described as following.

4.1. Ineffective in verify phase

According to the security properties (refer to subsection 2.2), "Source hiding" is one of the security requirements. For this reason, Bob doesn't know the source of the message. However, Bob has to compute rQ_{IDA} to verify σ sent form Alice, and he must try each user's *QID* to find the correct one. In addition, an adversary can send a fake signature to Bob to exhaust his resource, such as the battery power or memory space. Because the verify phase is so ineffective, user cannot find out the fake signature effectively.

4.2. Vulnerable to replay attack

The other weakness of Yoon's scheme is that it is vulnerable to replay attack. An adversary can intercept Alice's information and signature $\{M, r, \sigma\}$ and replay them to Bob after some time. Because the signature doesn't include the date information and Bob does not know the signature's original, Bob will accept the replayed signature. Replay attack has a great impact on some scenario, such as e-vote or e-business. In addition, Alice can send the same signature to Bob at a different time, and negate the signature by claiming the signature is replayed by an adversary. For this reason, Yoon's scheme is not secure.

5. The proposed scheme

To solve the problems in the previous literature, we propose a new scheme in this section. In next section, we will analyze the proposed scheme to prove our scheme is more secure and effective than the original scheme. The proposed scheme is also composed of five phases: *Setup phase*, *Key-Extract phase*, *Sign phase*, *Verify phase*, and *Transcript simulation phase*. As in the previous example, we also assume there are two users in the scenario, the signer Alice and the designated verifier Bob, where Alice owns the *IDA* and Bob owns the *IDB*.

1. Setup phase

In *Setup phase*, the PKG (private key generation center) has to define the system parameters, such as master secret key and public key. PKG defines the bilinear map as $\hat{e} : G \times G \rightarrow G_T$, where G is a cyclic additive group, and G_T is a cyclic multiplicative group, and $\{G, G_T\}$ have the same prime order q. After that, PKG selects a random number $s \in Z_q^*$ as the master key of system. Then, PKG selects three one-way hash functions $H_1()$ and $H_2()$, where $H_1(): \{0, 1\}^* \rightarrow G$ and $H_2(): \{0, 1\}^* \rightarrow Z_q^*$. Finally, PKG publishes the system public parameters $\{\hat{e}, G, G_T, q, H_1(), H_2()\}$, and keeps master key s secret. In our scheme, there is no unneeded value as the public key of PKG.

2. Key-Extract phase

In *Key-Extract phase*, PKG generates the privacy key $S_{ID} = sH_1(ID)$ for each *ID*, and sends it to the user. The public key of each *ID* is $Q_{ID} = H_1(ID)$. ID-based design allows the user to compute the other user's public key without relying on the third party.

3. Sign phase

When Alice wants to sign the message M and send it to Bob, Alice has to compute $Q_{IDB} = H_1(IDB)$ first. Next, Alice computes $r = H_2(T)$, where T is a correct timestamp. After, Alice computes $\delta = xQ_{IDA}$, where x is a random number selected by Alice. Then, Alice computes the signature σ:

$\sigma = H_2(M, \hat{e}(xQ_{IDB}, rS_{IDA}))$.

Finally, Alice sends $\{M, T, \sigma, \delta\}$ to Bob.

4. Verify phase

Upon receiving the information, Bob must check the timestamp T first. If T is not recent enough, Bob needs to reject the information. Otherwise, Bob computes $r = H_2(T)$ before verifying the signature. After that, Bob checks σ as follows:

$\sigma = ?H_2(M, \hat{e}(rS_{IDB}, \delta))$.

If the equation is correct, Bob accepts the information; otherwise, Bob rejects it. *Sign phase* and *Verify phase* in the proposed scheme are shown in Figure 2.

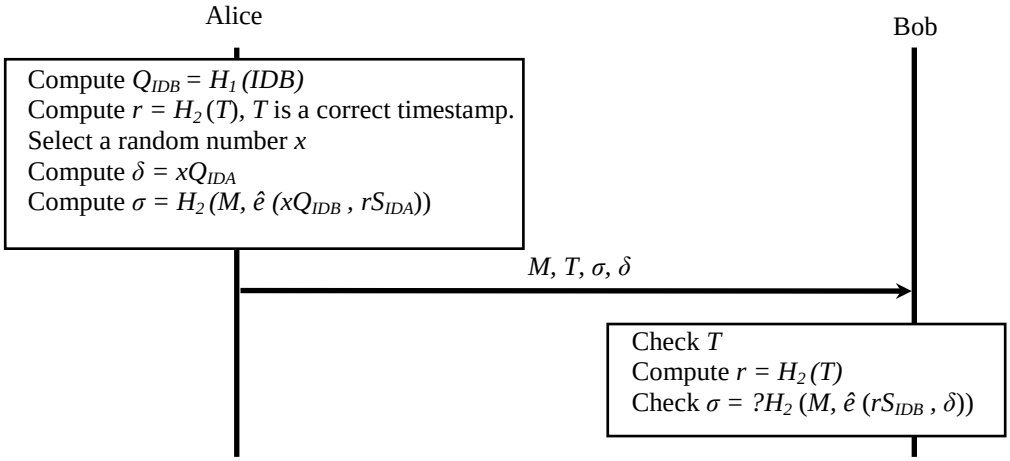

Figure 2. Sign phase and verify phase in the proposed scheme

5. Transcript simulation phase

When Bob accepts the message and signature from Alice, he can produce the transcripts. First, Bob selects a random number $r' \in Z_q^*$, which is different than r, and computes $\sigma' = H_2(M, \hat{e}(r'S_{IDB}, \delta))$. Finally, Bob stores $\{r', \sigma', \delta\}$.

6. Analysis of the proposed scheme

In this section, we will analyze the security of the proposed scheme and compare the efficiency with the previous scheme.

6.1. Security analysis

According to the subsection 2.2 in this paper, there are five necessary security properties for building a feasible designated verifier signature scheme: *Correctness*, *Strongness*, *Unforgeability*, *Non-Transferability*, *Source hiding*. In this subsection, we will describe how the proposed scheme satisfies those properties and overcomes the weaknesses of Yoon's scheme individually as following.

1. Correctness:

A correct scheme should be operated correctly. In the proposed scheme, the signature $\sigma = H_2(M, \hat{e}(xQ_{IDB}, rS_{IDA}))$ generated by Alice can be verified correctly by Bob as the following equation:

$\sigma = H_2(M, \hat{e}(xQ_{IDB}, rS_{IDA}))$
$= H_2(M, \hat{e}(xQ_{IDB}, rsQ_{IDA}))$
$= H_2(M, \hat{e}(rsQ_{IDB}, xQ_{IDA}))$
$= H_2(M, \hat{e}(rS_{IDB}, \delta))$.

Obviously, the designated verifier can accept the signature correctly.

2. Strength:

To ensure the strong property of the designated verifier signature scheme, only the designated verifier can verify the signature; and the signature should involve the public information of the designated verifier. In our scheme, we let the signature include the public information Q_{IDB} of the designated verifier Bob, and Bob can use his privacy information S_{IDB} to verify the signature. Because anyone except Bob does not have the necessary value S_{IDB} for computing $\hat{e}(rS_{IDB}, \delta)$, he/she can't verify the signature σ.

3. Unforgeability:

Some previous schemes are vulnerable to forgery attack, such as Kang et al.'s scheme [16]. The weakness allows an attacker to forge a signature and make it look like it is from a valid user, by using the public information sP of PKG, where s is the secret value of PKG and $P \in G$. To withstand the weakness, we don't allow the PKG to publish the information about secret value s. In our scheme, only the registered user has the secret value $S_{ID} = sH_1(ID)$, that means only the registered user can generate the valid signature. In addition, the verifier also needs to use his/her secret value $S_{ID} = sH_1(ID)$ to verify the signature. If an attacker intercepts $\{M, T, \sigma, \delta\}$ which was sent from Alice, he/she wants to forge a signature by altering δ. Then, the σ is still protected by the $H_2()$. Therefore, our proposed signature is unforgeable.

4. Source hiding:

To ensure no one can derive the origins from the information and signature, we have the identity information of Alice hiden in $\delta = xQ_{IDA} = xH_1(IDA)$. Because value x is a random number, and it is changed each time, no one, including Bob, can find the correlation between two different δ. For this reason, our scheme achieves source hiding.

5. Non-transferability:

As described for *Strongness* and *Source hiding*, only the owner of S_{IDB}, that is, Bob, can verify the signature involved in Q_{IDB} and the verifier can't claim the originality of the signature. In addition, because the δ is computed by a random x, the real original will be protected, even if all private keys are revealed.

6. Resisting replay attack

Yoon's scheme is vulnerable to replay attack. In this paper, we overcome the weakness by computing $r = H_2(T)$, where T is a correct timestamp. When Bob receives the signature from Alice, he can be sure the signature is fresh by checking T. In addition, T is involved in σ, and the σ can be modified. If an attacker intercepts $\{M, T, \sigma, \delta\}$ which was sent from Alice, and he/she wants to replay the signature by altering T, he/she will fail.

6.2. Efficiency analysis

This subsection gives a performance comparison between the proposed scheme and the related ID-based designated verifier signature schemes. The different calculations in our scheme include one point multiplication over an elliptic curve, denoted T_{mul}, MapToPoint hash operation, denoted T_{mtp}, and pairing operation, denoted T_{par}. Table 1 shows the comparison results of the computational costs of the proposed scheme and of various ID-based designated verifier signature schemes.

Table 1. The comparison results of the computational cost

	Signing cost	**Verifying cost**
The proposed scheme	$3T_{mul} + 1T_{mtp} + 1T_{par}$	$1T_{mul} + 1T_{par}$
Kang et al.'s scheme [5]	$2T_{mul} + 2T_{mtp} + 1T_{par}$	$1T_{mtp} + 1T_{par}$
Yoon's scheme [16]	$1T_{mul} + 2T_{mtp} + 1T_{par}$	$1T_{mul} + 2T_{mtp} + 1T_{par}$

We adopt the MNT curve [9, 18], which embeds a degree k = 6 and 160-bit q, running on an Intel

Pentium IV 3.0 GHZ machine. The following results are obtained: T_{mul} is 0.6 *ms*, T_{par} is 4.5 *ms*, and T_{mtp} is 0.6 *ms*. From Table 1, the signing and verifying's sum of the proposed scheme is $4T_{mul} + 1T_{mtp} + 2T_{par}$, that means the need of once signing and verifying is 12 *ms*. The sum of the Kang et al.'s scheme is $2T_{mul} + 3T_{mtp} + 2T_{par}$, that also means 12 *ms* once signing and verifying, and the sum of Yoon's scheme is $2T_{mul} + 4T_{mtp} + 2T_{par}$, that means 12.6 *ms* once signing and verifying. Although the proposed scheme has to transfer the timestemp T when Alice sends a signature to Bob, it ensures the freshness of proposed scheme. On the other hand, the proposed scheme has another advantage over the Yoon's scheme. The proposed scheme allows Bob to verify the signature from Alice immediately, but the Yoon's scheme doesn't provide this mechanism. Hence, Bob has to compare each user to find the matched one. Bob perhaps has to compare all the registered users in the worst situation, and therefore it is inefficient. For the above reasons, the proposed scheme is the most adaptive scheme for designated verifier signature.

7. Conclusions

This paper points out the weaknesses of Yoon's ID-based strong designated verifier signature scheme, i.e. being valuable to replay attack and the high cost of verify phase. We propose some improvements to overcome these problems. The result is a more efficient and secured ID-based strong designated verifier signature scheme.

Acknowledgement

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC101-2221-E-030-018.

References

[1] **F. Cao, Z. Cao**. An identity based universal designated verifier signature scheme secure in the standard model. *The Journal of Systems and Software*, 2009, Vol. 82, No. 4, 643-649.

[2] **W. Diffie, M. Hellman.** New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, Vol. 22, No. 6, 644-654.

[3] **X. Huang, W. Susilo, Y. Mu, F. Zhang.** Short designated verifier signature scheme and its identity-based variant. *International Journal of Network Security*, 2008, Vol. 6, No. 1, 82-93.

[4] **M. Jakobsson, K. Sako, R. Impagliazzo**. Designated verifier proofs and their applications. *Lecture Notes in Computer Science*, 1996, Vol. 1070/1996, pp. 143-154.

[5] **B. Kang, C. Boyd, E. Dawson.** Identity-based strong designated verifier signature schemes: attacks and new construction. *Computers and Electrical Engineering*, 2009, Vol. 35, No. 1, 49-53.

[6] **F. Laguillaumie, D. Vergnaud**. Multi-designated verifiers signatures: anonymity without encryption. In: *Information Processing Letters*, 2007, Vol. 102, No. 2-3, pp. 127-132.

[7] **C.-C. Lee, T.-C. Lin, S.-F. Tzeng, M.-S. Hwang**. Generalization of proxy signature based on Factorization. *International Journal of Innovative Computing, Information and Control*, 2011, Vol. 7, No. 3, 1039-1054.

[8] **X. Lin, X. Sun, P.-H. Ho, X. Shen.** GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 2007, Vol. 56, No. 6, 3442-3456.

[9] **A. Miyaji, M. Nakabayashi, S. Takano.** New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transaction on Fundamentals of Electronics*, 2001, Vol. E84-A, No. 5, 1234-1243.

[10] **C. Y. Ny, W. Susilo, Y. Mu.** Universal designated multi-verifiers signature schemes. In: *Proceedings of ICPADS'05*, 2005, pp. 305-309.

[11] **R. L. Rivest, A. Shamir, L. M. Adleman.** Cryptographic communications system and method. *Communications of the ACM*, 1978, Vol. 21, No. 2, 120-126.

[12] **S. Saeednia, S. Kremer, O. Markowitch.** An efficient strong designated verifier signature scheme. In: *Lecture Notes in Computer Science*, 2004, Vol. 2971/2004, 40-54.

[13] **M. Scott.** Efficient implementation of cryptographic pairings [Online]. Available: ftp://ftp.disi.unige.it/pub/person/MoraF/CRYPTO/PARING/mscott-samos07.pdf, accessed: 2012/4/21.

[14] **G. Shailaja, K. P. Kumar, A. Saxenh**. Universal designated multi-verifier signature without random oracles. In*: Proceedings of ICIT'06*, 2006, pp. 168-171.

[15] **Y. Ming, Y. Wang.** Universal designated multi-verifier's signature scheme without random oracles. *Wuhan University Journal Of Natural Sciences*, 2008, Vol. 13, No. 6, 685-691.

[16] **E.-J. Yoon**. An efficient and secure identity-based strong designated verifier signature scheme. *Information Technology and Control*, 2011, Vol. 40, No. 4, 323-329.

[17] **J. Zhang, J. Mao.** A novel ID-based designated verifier signature scheme. *Information Sciences*, 2008, Vol. 178, No. 3, 766-773.

[18] **C. Zhang, P.-H. Ho, J. Tapolcai.** On batch verification with group testing for vehicular communications. *Wireless Networks*, 2011, Vol. 17, No. 8, 1851-1865.

Received October 2012.