A Note on "Efficient Algorithms for Secure Outsourcing of Bilinear Pairings"

Lihua Liu[1] and Zhengjun Cao[2]
(Corresponding author: Zhengjun Cao)
Department of Mathematics, Shanghai Maritime University[1]
No.1550, Haigang Ave, Pudong New District, Shanghai, China
Department of Mathematics, Shanghai University[2]
No.99, Shangda Road, Shanghai 200444, China
(Email: caozhj@shu.edu.cn)
(Received Mar. 13, 2016; revised and accepted May 20 & June 20, 2016)

Abstract

Recently, Chen et al. have proposed a scheme [Theoretical Computer Science, 562 (2015), 112-121] for secure outsourcing of bilinear pairings. The scheme is motivated by the Chevallier-Mames et al.'s scheme. But the new scheme misses the feature of Chevallier-Mames et al.'s checking mechanism. In this note, we show that the verifying equations in the Chen et al.'s scheme cannot filter out some malformed values returned by the malicious servers, which makes it fragile to such malicious attacks. We also remark that the trick of equipping a low capability chip with two untrusted softwares in the scheme is somewhat artificial because of its heavy communication overhead.

Keywords: Bilinear Pairing; Outsourcing Computation; Semi-honest Server

1 Introduction

In 2000, Joux [19] proposed one round protocol for tripartite Diffie-Hellman key agreement protocol using Weil pairing. This is the first instance to show that pairings can be used for "good". At Crypto'2001, Boneh and Fracklin [6] proposed a fully functional identity-based encryption scheme using Weil Pairing. After that, paring-based cryptography (PBC) has interested many researchers [1, 2, 3, 4, 5, 7, 8, 9] because it has many beautiful and elegant properties.

Suppose that an elliptic curve E is defined over the finite field $\mathbb{F}_q$. Then elliptic curve cryptography (ECC) is working with elements which are defined over the base field $\mathbb{F}_q$ (its parameters have size $O(\log q)$ bits). But PBC is working with the functions and elements defined over the extension field $\mathbb{F}_{q^k}$ (its parameters have size $O(k \log q)$ bits), where k is the *embedding degree*. From the practical point of view, it is annoying for PBC schemes to have to work in extensions of the base fields, even though the inputting parameters are defined over the base field. The security of PBC depends directly on the intractable level of either elliptic curve discrete log problem (ECDLP) in the group $E(\mathbb{F}_q)$ or discrete log problem (DLP) in the group $\mathbb{F}^*_{q^k}$. That means PBC protocols have to work in a running environment with parameters of 1024 bits so as to offer 80 bits security level [16].

The computation of bilinear pairing represents most of the computing cost when dealing with PBC protocols.

In order to mitigate the pairing computation burdens, researchers have put forth various methods. At Asiacrypt'05, Girault and Lefranc [15] introduced the primitive of server-aided verification to speed up the verification task of a signature scheme or an identification scheme. They assumed that the verifier has only small computation capabilities while having access to a more powerful, but untrusted server or, equivalently, to a trusted server via a non authenticated communication link.

At TCC'05, Hohenberger and Lysyanskaya [17] considered that an auxiliary server is made of two untrusted softwares which are assumed not to communicate with each other.

Liao and Hsiao [20] studied the problem of multi-servers aided verification using self-certified public keys for mobile clients. Liu et al. [22] have investigated the problem of identity-based server-aided decryption. Zhang and Sun [23] proposed an ID-based server-aided verification of short signature scheme without key escrow.

In 2013, Canard et al. [11] considered the method for generically transforming a given instance into a secure server-aided version. In 2014, Canard, Devigne and Sanders [10] provided some efficient ways to delegate the computation

of a pairing $e(A, B)$, depending on the status of A and B. Their protocols enable the limited device to verify the value received from the third party by computing one exponentiation.

In 2016, Cao et al. [12] pointed out two kinds of flaws in some server-aided verification schemes. Hsien et al. [18, 21] presented two surveys of public auditing for secure data storage in cloud computing.

Very recently, Chen et al. [13] have put forth a scheme for outsourcing computations of bilinear pairings in two untrusted programs model which was introduced by Hohenberger and Lysyanskaya [17]. In the scheme, a user T can indirectly compute the pairing $e(A, B)$ by outsourcing some expensive work to two untrusted servers U_1 and U_2 such that A, B and $e(A, B)$ are kept secret. Using the returned values from U_1, U_2 and some previously stored values, the user T can recover $e(A, B)$.

The Chen et al.'s scheme is derived from the Chevallier-Mames et al.'s scheme [14] by storing some values in a table in order to save some expensive operations such as point multiplications and exponentiations. Besides, the new scheme introduces two servers U_1 and U_2 rather than the unique server U in the Chevallier-Mames et al.'s scheme. The authors [13] claim that the scheme achieves the security *as long as one of the two servers is honest*.

In other word, a malicious server cannot obtain either A or B. Unfortunately, the assumption cannot ensure that the scheme works well, because a malicious server can return some random values while the user T cannot detect the malicious behavior. As a result, T outputs a false value.

In this note, we show that the verifying equations in the Chen et al.'s scheme [13] cannot filter out some malformed values returned by the malicious servers. To fix this drawback, it has to specify that the servers are semi-honest. We also point out that the two untrusted programs model in the scheme is somewhat artificial and discuss some reasonable scenarios for outsourcing computations.

2 Review of the Scheme

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic additive groups with a large prime order q. Let G_3 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ with the following properties.

1) Bilinear: $e(aR, bQ) = e(R, Q)^{ab}$ for all $R \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, and $a, b \in \mathbb{Z}_q^*$.
2) Non-degenerate: There exist $R \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ such that $e(R, Q) \neq 1$.
3) Computable: There is an efficient algorithm to compute $e(R, Q)$ for all $R \in \mathbb{G}_1, Q \in \mathbb{G}_2$.

The Chen et al.'s scheme [13] uses two untrusted servers U_1, U_2. The outsourcer T queries some pairings to the two servers. The scheme can be described as follows.

Setup.

A trusted server computes a table *Rand* which consists of the elements of random and independent six-tuple

$$(W_1, W_2, w_1W_1, w_2W_1, w_2W_2, e(w_1W_1, w_2W_2)),$$

where $w_1, w_2 \in_R \mathbb{Z}_q^*, W_1 \in_R \mathbb{G}_1$, and $W_2 \in_R \mathbb{G}_2$. The table is then loaded into the memory of T.

Look-up table.

Given $A \in \mathbb{G}_1, B \in \mathbb{G}_2$, where A and B may be secret or protected and $e(A, B)$ is always secret or protected. T looks up *Rand* to create

$$(V_1, V_2, v_1V_1, v_2V_1, v_2V_2, e(v_1V_1, v_2V_2)),$$
$$(X_1, X_2, x_1X_1, x_2X_1, x_2X_2, e(x_1X_1, x_2X_2)),$$
$$(Y_1, Y_2, y_1Y_1, y_2Y_1, y_2Y_2, e(y_1Y_1, y_2Y_2)).$$

Interaction with U_1.

T sends

$$(A + v_1V_1, B + v_2V_2), (v_1V_1 + v_2V_1, V_2), (x_1X_1, x_2X_2), (y_1Y_1, y_2Y_2)$$

to U_1. U_1 returns

$$\begin{aligned} \alpha_1 &= e(A + v_1V_1, B + v_2V_2), \\ \delta &= e(V_1, V_2)^{v_1+v_2}, \\ \beta_1 &= e(x_1X_1, x_2X_2), \\ \beta_2 &= e(y_1Y_1, y_2Y_2). \end{aligned}$$

Interaction with U_2.

T sends

$$(A+V_1, v_2V_2), (v_1V_1, B+V_2), (x_1X_1, x_2X_2), (y_1Y_1, y_2Y_2)$$

to U_2. U_2 returns

$$\begin{aligned} \alpha_2 &= e(A+V_1, v_2V_2), \\ \alpha_3 &= e(v_1V_1, B+V_2), \\ \widehat{\beta_1} &= e(x_1X_1, x_2X_2), \\ \widehat{\beta_2} &= e(y_1Y_1, y_2Y_2). \end{aligned}$$

Verification.

T checks that both U_1 and U_2 produce the correct outputs by verifying that

$$\beta_1 = \widehat{\beta_1} \text{ and } \beta_2 = \widehat{\beta_2}.$$

If not, T outputs "error".

Computation.

T computes

$$e(A,B) = \alpha_1\alpha_2^{-1}\alpha_3^{-1}\delta \cdot e(v_1V_1, v_2V_2)^{-1}.$$

Remark 1. *In the original description of the scheme, the Step 2 (see Section 4.2 in Ref.[13]) has not specified any actions. It only explains that the pairing $e(A,B)$ can be composed by the related values. The authors have confused the explanation with steps of the scheme (it is common that a step of a scheme should specify some actions performed by a participator), which makes the original description somewhat obscure.*

Remark 2. *It should be stressed that the pre-computation table must be very large in order to ensure the randomness of the picked tuples, which makes the proposed table-lookup method uncompetitive. Actually, it is a rare practice in cryptography to pick random numbers by table-lookup method.*

3 The Checking Mechanism in the Scheme is Flawed

In the Chen et al.'s scheme [13], to check whether the returned values α_1, δ, β_1, β_2 and α_2, α_3, $\widehat{\beta_1}$, $\widehat{\beta_2}$ are properly formed, the user T has to check the verifying equations

$$\beta_1 = \widehat{\beta_1} \text{ and } \beta_2 = \widehat{\beta_2}.$$

We now want to stress that the checking mechanism *cannot filter out some malformed values*. The drawback is due to that the protected values A, B are not involved in the equations at all.

For example, upon receiving

$$(A+v_1V_1, B+v_2V_2),\ (v_1V_1+v_2V_1, V_2), (x_1X_1, x_2X_2),\ (y_1Y_1, y_2Y_2),$$

U_1 picks a random $\rho \in \mathbb{Z}_q^*$ and returns

$$\alpha_1 = e(A+v_1V_1, B+v_2V_2),\ \rho, \beta_1 = e(x_1X_1, x_2X_2),\ \beta_2 = e(y_1Y_1, y_2Y_2)$$

to T.

Clearly, $\beta_1 = \widehat{\beta_1}$ and $\beta_2 = \widehat{\beta_2}$ hold still. Thus, the returned values will pase the verification process. But in such case, we have

$$\alpha_1\alpha_2^{-1}\alpha_3^{-1}e(v_1V_1, v_2V_2))^{-1}\rho = e(A,B)e(V_1,V_2)^{-v_1-v_2}\rho.$$

That means T obtains $e(A,B)e(V_1,V_2)^{-v_1-v_2}\rho$ instead of $e(A,B)$.

To fix the above drawback, we have to specify that *both two servers are semi-honest*. The term of semi-honest here means that a server can copy the involved values and always returns the correct outputs, but cannot conspire with the other server.

Under the reasonable assumption, the original scheme can be greatly simplified. We now present a revised version as follows.

Look-up table.

Given $A \in \mathbb{G}_1, B \in \mathbb{G}_2$, where A and B may be secret or protected and $e(A, B)$ is always secret or protected. T looks up *Rand* to create

$$(V_1, V_2, v_1V_1, v_2V_1, v_2V_2, e(v_1V_1, v_2V_2)).$$

Interaction with U_1.

T sends

$$(A + v_1V_1, B + v_2V_2),\ (v_1V_1 + v_2V_1, V_2)$$

to U_1. U_1 returns

$$\alpha_1 = e(A + v_1V_1, B + v_2V_2),\ \delta = e(V_1, V_2)^{v_1+v_2}.$$

Interaction with U_2.

T sends

$$(A + V_1, v_2V_2),\ (v_1V_1, B + V_2)$$

to U_2. U_2 returns

$$\alpha_2 = e(A + V_1, v_2V_2),\ \alpha_3 = e(v_1V_1, B + V_2).$$

Computation.

T computes

$$e(A, B) = \alpha_1\alpha_2^{-1}\alpha_3^{-1}e(v_1V_1, v_2V_2)^{-1}\delta.$$

4 The Chevallier-Mames et al.'s Checking Mechanism

As we mentioned before, the Chen et al.'s scheme [13] is derived from the Chevallier-Mames et al.'s scheme [14]. But the new scheme misses the feature of the checking mechanism in the Chevallier-Mames et al.'s scheme. We think it is helpful for the later practitioners to explain the feature.

In the Chevallier-Mames et al.'s scheme, the outsourcer T wants to compute the pairing $e(A, B)$ with the help of the untrusted server U such that A, B and $e(A, B)$ are kept secret. The scheme can be described as follows (See Table 1).

Table 1: The Chevallier-Mames et al.'s scheme

The outsourcer T $\{P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2, e(P_1, P_2)\}$		The server U
Input: $A \in \mathbb{G}_1, B \in \mathbb{G}_2$ Pick $g_1, g_2, a_1, r_1, a_2, r_2 \in Z_q^*$, compute $A + g_1P_1, B + g_2P_2$		Compute
$a_1A + r_1P_1, a_2B + r_2P_2$	$\xrightarrow{(A+g_1P_1, P_2)}$	$\alpha_1 = e(A + g_1P_1, P_2)$
and query them.	$\xrightarrow{(P_1, B+g_2P_2)}$	$\alpha_2 = e(P_1, B + g_2P_2)$
	$\xrightarrow{(A+g_1P_1, B+g_2P_2)}$	$\alpha_3 = e(A + g_1P_1, B + g_2P_2)$
Compute	$\xrightarrow{(a_1A+r_1P_1, a_2B+r_2P_2)}$	$\alpha_4 = e(a_1A + r_1P_1, a_2B + r_2P_2)$
$e(A, B) = \alpha_1^{-g_2}\alpha_2^{-g_1}\alpha_3 e(P_1, P_2)^{g_1g_2}$	$\xleftarrow{\alpha_1, \alpha_2, \alpha_3, \alpha_4}$	and return them.
Check that $\alpha_4 \stackrel{?}{=} e(A, B)^{a_1a_2}\alpha_1^{a_1r_2}\alpha_2^{a_2r_1}$ $\cdot e(P_1, P_2)^{r_1r_2 - a_1g_1r_2 - a_2g_2r_1}$ If true, output $e(A, B)$.		

Notice that the true verifying equation is

$$\begin{aligned}\alpha_4 &= \left(\alpha_1^{-g_2}\alpha_2^{-g_1}\alpha_3 e(P_1, P_2)^{g_1g_2}\right)^{a_1a_2} \cdot \alpha_1^{a_1r_2}\alpha_2^{a_2r_1} e(P_1, P_2)^{r_1r_2 - a_1g_1r_2 - a_2g_2r_1} \\ &= \alpha_1^{-g_2a_1a_2 + a_1r_2}\alpha_2^{-g_1a_1a_2 + a_2r_1} \cdot \alpha_3^{a_1a_2} e(P_1, P_2)^{g_1g_2a_1a_2 + r_1r_2 - a_1g_1r_2 - a_2g_2r_1}\end{aligned}$$

where $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are generated by the server U, and the session keys $g_1, g_2, a_1, r_1, a_2, r_2$ are randomly picked by the outsourcer T.

Clearly, the server U cannot generate the four-tuple $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ satisfying the above verifying equation because the exponents

$$a_1 r_2 - g_2 a_1 a_2,\ a_2 r_1 - g_1 a_1 a_2,\ a_1 a_2, g_1 g_2 a_1 a_2 + r_1 r_2 - a_1 g_1 r_2 - a_2 g_2 r_1$$

are not known to the server. The intractability of the above equation can be reduced to the following general challenge:

$$\text{Without knowing a secret exponent } \theta, \text{find } X, Y \in Z_q^*,\ X \neq 1, Y \neq 1, \text{such that } X^\theta = Y.$$

5 The Remote and Shared Servers

5.1 On the Client's Communication Overhead

The authors stress that the two servers U_1 and U_2, in the real-world applications, can be viewed as two copies of one advertised software from two different vendors. We would like to remark that the two copies are neither nearby nor private. They must be remote and shared by many outsourcers. Otherwise, the user T equipped with two private copies of one software can be wholly viewed as an *augmented user*. But the situation is rarely considered in practice.

We now consider the situation that the outsourcer T has to communicate with two remote and shared servers. If the data transmitted over channels are not encrypted, then an adversary can obtain $A+v_1V_1, B+v_2V_2$ by tapping the communication between T and U_1, and get v_1V_1, v_2V_2 by tapping the communication between T and U_2. Hence, he can recover A and B. Thus, it is reasonable to assume that all data transmitted over channels are encrypted. From the practical point of view, the communication costs (including that of authentication of the exchanged data, the underlying encryption/decryption, etc.) could be far more than the computational gain in the scheme. The authors have neglected the comparisons between the computational gain and the incurred communication costs. Taking into account this drawback, we think the scheme is somewhat artificial.

5.2 A Nearby and Trusted Server

Girault and Lefranc [15] have described some situations in which a chip has only a small computation capability is connected to a powerful device.

- In a GSM mobile telephone, the more sensitive cryptographic operations are performed in the so-called SIM (Subscriber Identification Module), which is already aided by the handset chip, mainly to decipher the over-the-air enciphered conversation.
- In a payment transaction, a so-called SAM (Secure Access Module) is embedded in a terminal already containing a more powerful chip.
- A smart card is plugged into a personal computer, seeing that many PCs will be equipped with smart card readers in a near future.

We find that in all these situations (a SIM vs. a handset, a SAM vs. a powerful terminal, a smart card vs. a personal computer) the servers are nearby and trusted, not remote and untrusted.

6 Conclusion

The true goal of outsourcing computation in the Chen et al.'s scheme is to compute bilinear pairings. In view of that pairings spread everywhere in pairing-based cryptograph, we do not think that the trick of equipping a low capability chip with two untrusted softwares is feasible because of its heavy communication overhead. In practice, we think, it is better to consider the scenario where a portable chip has access to a nearby and trusted server. Otherwise, the communication costs could overtake the computational gain of the outsourced computations.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.

References

[1] D. Boneh, "Pairing-based cryptography: Past, present, and future," in *Proceedings of Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security*, Beijing, China, December 2012.

[2] D. Boneh and X. Boyen, "Short signatures without random oracles," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[3] D. Boneh and X. Boyen, "Efficient selective identity-based encryption without random oracles," *Journal of Cryptology*, vol. 24, no. 4, pp. 659–693, 2011.

[4] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proceedings of Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 440–456, Aarhus, Denmark, May 2005.

[5] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proceedings of Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference*, pp. 41–55, Santa Barbara, California, USA, August 2004.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference*, pp. 213–229, Santa Barbara, California, USA, August 2001.

[7] D. Boneh, A. Raghunathan, and G. Segev, "Function-private identity-based encryption: Hiding the function in functional encryption," in *Proceedings of Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 255–275, Bengaluru, India, December 2013.

[8] D. Boneh, A. Raghunathan, and G. Segev, "Function-private subspace-membership encryption and its applications," in *Proceedings of Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, pp. 461–478, Santa Barbara, CA, USA, August 2013.

[9] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in *Proceedings of Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 573–592, St. Petersburg, Russia, 2006.

[10] S. Canard, J. Devigne, and O. Sanders, "Delegating a pairing can be both secure and efficient," in *Proceedings of Applied Cryptography and Network Security - ACNS 2014*, pp. 549–565, Lausanne, Switzerland, June 2014.

[11] S. Canard and et al., "Toward generic method for server-aided cryptography," in *Proceedings of Information and Communications Security - ICICS 2013*, pp. 373–392, Beijing, China, November 2013.

[12] Z.J. Cao, L.H. Liu, and O. Markowitch, "On two kinds of flaws in some server-aided verification schemes," *International Journal of Network Security*, vol. 18, no. 6, pp. 1054–1059, 2016.

[13] X.F. Chen and et al., "Efficient algorithms for secure outsourcing of bilinear pairings," *Theoretical Computer Science*, no. 562, pp. 112–121, 2015.

[14] B. Chevallier-Mames and et al., "Secure delegation of elliptic-curve pairing," in *Proceedings of Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference - CARDIS 2010*, pp. 24–35, Passau, Germany, April 2010.

[15] M. Girault and D. Lefranc, "Server-aided verification: Theory and practice," in *Proceedings of Advances in Cryptology - ASIACRYPT 2005*, pp. 605–623, Chennai, India, December 2005.

[16] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. U.S.A: Springer-Verlag, 2004.

[17] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in *Proceedings of Theory of Cryptography - TCC 2005*, pp. 264–282, Cambridge, MA, USA, February 2005.

[18] W.F. Hsien, C.C. Yang, and M.S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[19] A. Joux, "A one round protocol for tripartite diffie-hellman," in *Proceedings of Algorithmic Number Theory, 4th International Symposium, ANTS-IV*, pp. 385–394, Leiden,Netherlands, July 2000.

[20] Y.P. Liao and C.M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, pp. 886–900, 2013.

[21] C.W. Liu, W.F. Hsien, C.C. Yang, and M.S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[22] J. Liu, C.K. Chu, and J.Y. Zhou, "Identity-based server-aided decryption," in *Proceedings of Information Security and Privacy - ACISP 2011*, pp. 337–352, Melbourne, Australia, July 2011.

[23] J.H. Zhang and Z.B. Sun, "An id-based server-aided verification short signature scheme avoid key escrow," *Journal of Information Science and Engineering*, vol. 29, pp. 459–473, 2013.

Biography

Lihua Liu is an associate professor of Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Zhengjun Cao is an associate professor of Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.