An Anonymous ID-based Encryption Revisited

Zhengjun Cao
Département d'informatique, Université Libre de Bruxelles, Belgium
zhencao@ulb.ac.be, caoamss@gmail.com

Abstract In 2006, Boyen and Waters proposed an anonymous ID-based encryption. It is impressive that in the scheme the system secret key is a tuple of five numbers. The user's secret key is also a tuple of five elements. The authors did not explain why it should introduce so many parameters. In this paper, we simulate a general attempt to attack the scheme. It shows us which parameters are essential to the scheme and which parameters can be reasonably discarded. Based on the analysis we present a simplified version and an efficient version of the Boyen-Waters scheme. The analyzing technique developed in this paper is helpful to better other cryptographic protocols.

Keywords Anonymous ID-based encryption, Smooth Transition

1 Introduction

The primitive of ID-based encryption allows a sender to encrypt a message for a receiver using only the receiver's identity as the user's public key (of course, some system public parameters are required). An anonymous ID-based encryption ensures the ciphertext does not leak the identity of the recipient. In 2006, Boyen and Waters [6] proposed an ID-based encryption (BW06 for short) that features fully anonymous ciphertexts and hierarchical key delegation.

It is impressive that in the BW06 scheme the system secret key is a tuple of five numbers $(\omega, t_1, t_2, t_3, t_4)$. The user's secret key is also a tuple of five elements $(K_0, K_1, K_2, K_3, K_4)$. One might ask why it should introduce so many parameters. The authors did not explain it. In this paper, we simulate a general attempt to attack the scheme. It shows us which parameters are essential to the scheme and which parameters can be reasonably discarded. Based on the analysis we present a simplified version and an efficient version of the BW06 scheme. The analyzing technique developed in this paper, we think, is helpful to better other cryptographic protocols.

2 Preliminary

G and G_1 are two (multiplicative) cyclic groups of prime order p. g is a generator of G. A bilinear map $\hat{e} : G \times G \to G_1$ is of the following properties:

1) Bilinearity. For all $U, V \in G$ and $a, b \in Z$, $\hat{e}(U^a, V^b) = \hat{e}(U, V)^{ab}$.

2) Non-degeneracy. $\hat{e}(g, g) \neq 1$.

We refer to [1-10] for more details about the constructions and usages of bilinear maps.

3 The Boyen-Waters anonymous ID-based encryption

The BW06 scheme requires that: *Confidentiality* no non-trivial information about the message can be feasibly gleaned from the ciphertext; *Anonymity* the adversary must be unable to decide whether a ciphertext was encrypted for a chosen identity, or for a random identity.

Assume that the identity information $\mathcal{U}$ is an element in $\mathbb{Z}_p^*$, and the message M to be encrypted is an element in G_1. For convenience, in an ID-based scenario we classify the involved parameters as: system public key (spk), system secret key (ssk), user's public key (upk), user's secret key (usk). By the way, there is always a system manager who is responsible for generating spk, ssk, usk. The system secret key is usually called master-key.

3.1 Review

We now describe the BW06 scheme as follows.

Setup Pick random generators $g, g_0, g_1 \in G$, $\omega, t_1, t_2, t_3, t_4 \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ and set

$$\begin{aligned} spk: &\quad \{G, G_1, p, g, g_0, g_1, \hat{e}, \Omega = \hat{e}(g,g)^{t_1 t_2 \omega}, V_1 = g^{t_1}, V_2 = g^{t_2}, V_3 = g^{t_3}, V_4 = g^{t_4}\} \\ ssk: &\quad \{\omega, t_1, t_2, t_3, t_4\} \end{aligned}$$

Extract For the identity $\mathcal{U}$, the key extraction authority picks $r_1, r_2 \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ and sets usk : $\{K_0, K_1, K_2, K_3, K_4\}$, where

$$\begin{aligned} &K_0 = g^{r_1 t_1 t_2 + r_2 t_3 t_4}, K_1 = g^{-\omega t_2}(g_0 g_1^{\mathcal{U}})^{-r_1 t_2}, K_2 = g^{-\omega t_1}(g_0 g_1^{\mathcal{U}})^{-r_1 t_1} \\ &K_3 = (g_0 g_1^{\mathcal{U}})^{-r_2 t_4}, K_4 = (g_0 g_1^{\mathcal{U}})^{-r_2 t_3} \end{aligned}$$

Encrypt For a message M and the identity $\mathcal{U}$, pick $s, s_1, s_2 \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ and create the ciphertext:

$$\begin{aligned} &C' = \Omega^s M, C_0 = (g_0 g_1^{\mathcal{U}})^s, C_1 = V_1^{s-s_1} \\ &C_2 = V_2^{s_1}, C_3 = V_3^{s-s_2}, C_4 = V_4^{s_2} \end{aligned}$$

Decrypt To decrypt a ciphertext $\{C', C_0, C_1, C_2, C_3, C_4\}$, compute:

$$M = C' \hat{e}(C_0, K_0)\hat{e}(C_1, K_1)\hat{e}(C_2, K_2)\hat{e}(C_3, K_3)\hat{e}(C_4, K_4)$$

3.2 Basic observations

In the BW06 model, one should make certain that: 1) the message must be blinded; 2) the identity of the designated recipient must be blinded; 3) without the help of the system manager, who is responsible for generating spk, ssk, usk, nobody can derive out a proper secret key.

In the scheme, the system secret key is a tuple of five numbers $(\omega, t_1, t_2, t_3, t_4)$. Correspondingly, the user's secret key is also a tuple of five elements $(K_0, K_1, K_2, K_3, K_4)$. The authors did not explain why it should introduce so many parameters. As usual, the story behind designing the structure has not been unveiled.

By the ciphertext $(C', C_0, C_1, C_2, C_3, C_4)$, we see:

To blind the message M, it sets $C' = \Omega^s M$, where s is a randomly chosen exponent, $\Omega = \hat{e}(g,g)^{t_1 t_2 \omega}$ is a public system parameter.

To blind a certain user's information, $\mathcal{U}$, it sets $C_0 = (g_0 g_1^{\mathcal{U}})^s$, where g_0, g_1 are two public system parameters.

The remainders C_1, C_2, C_3, C_4 are independent of M and $\mathcal{U}$. They are used to recover M.

In view of these observations, one might ask: a) why it sets so many helpers C_1, C_2, C_3, C_4; b) why the designers blind M and $\mathcal{U}$ separately. We will investigate the two problems and present two different variations of the BW06 scheme.

3.3 Which parameters are not essential to the BW06 scheme

The original consistency argument of the BW06 scheme does not explicitly show us which parameters are essential. To see which parameters are not essential in the scheme, we now simulate a general attempt to attack it.

Given the public parameters

$$G, G_1, p, g, g_0, g_1, \hat{e}, \Omega = \hat{e}(g,g)^{t_1 t_2 \omega}, V_1 = g^{t_1}, V_2 = g^{t_2}, V_3 = g^{t_3}, V_4 = g^{t_4}$$

and a ciphertext relating to a certain identity $\mathcal{U}$

$$C' = M\Omega^s, C_0 = (g_0 g_1^{\mathcal{U}})^s, C_1 = V_1^{s-s_1}, C_2 = V_2^{s_1}, C_3 = V_3^{s-s_2}, C_4 = V_4^{s_2}$$

by the Decryption, we have

$$\begin{aligned} & C'\hat{e}(C_0, K_0)\hat{e}(C_1, K_1)\hat{e}(C_2, K_2) \\ = \; & M\Omega^s \hat{e}\left((g_0 g_1^{\mathcal{U}})^s, K_0\right)\hat{e}(V_1^{s-s_1}, K_1)\hat{e}(V_2^{s_1}, K_2)\hat{e}(V_3^{s-s_2}, K_3)\hat{e}(V_4^{s_2}, K_4) \end{aligned}$$

Now, the adversary tries to recover M from the above equation. (For convenience, we rewrite $g_0 g_1^{\mathcal{U}} = h$ later).

Without loss of generality, suppose that the adversary picks a random identity $\mathcal{U}$, and sets

$$K_0 = g^{\xi_0} h^{\rho_0}, K_1 = g^{\xi_1} h^{\rho_1}, K_2 = g^{\xi_2} h^{\rho_2}, K_3 = g^{\xi_3} h^{\rho_3}, K_4 = g^{\xi_4} h^{\rho_4}$$

where

$$g^{\xi_0}, g^{\xi_1}, g^{\xi_2}, g^{\xi_3}, g^{\xi_4}, h^{\rho_0}, h^{\rho_1}, h^{\rho_2}, h^{\rho_3}, h^{\rho_4}$$

are to be determined. Hence, we have

$$\begin{aligned} & M\Omega^s\hat{e}(h^s, K_0)\hat{e}(V_1^{s-s_1}, K_1)\hat{e}(V_2^{s_1}, K_2)\hat{e}(V_3^{s-s_2}, K_3)\hat{e}(V_4^{s_2}, K_4) \\ = \; & M\hat{e}(g,g)^{t_1 t_2 \omega s}\hat{e}(h^s, g^{\xi_0}h^{\rho_0})\hat{e}(g^{t_1(s-s_1)}, g^{\xi_1}h^{\rho_1})\hat{e}(g^{t_2 s_1}, g^{\xi_2}h^{\rho_2})\hat{e}(g^{t_3(s-s_2)}, g^{\xi_3}h^{\rho_3})\hat{e}(g^{t_4 s_2}, g^{\xi_4}h^{\rho_4}) \\ = \; & M\hat{e}(g,g)^{(t_1 t_2 \omega + t_1\xi_1 + t_3\xi_3)s + (t_2\xi_2 - t_1\xi_1)s_1 + (t_4\xi_4 - t_3\xi_3)s_2}\hat{e}(h,h)^{s\rho_0} \\ & \cdot\hat{e}(h,g)^{(\xi_0 + t_1\rho_1 + t_3\rho_3)s + (t_2\rho_2 - t_1\rho_1)s_1 + (t_4\rho_4 - t_3\rho_3)s_2} \end{aligned}$$

Since s, s_1, s_2 are randomly chosen by the sender, the message m is definitely independent of s, s_1, s_2. In view of that $\log_g h, \log_{\hat{e}(g,g)} \hat{e}(h,g), \log_{\hat{e}(g,g)} \hat{e}(h,h)$ are assumed to be intractable, we have

$$\begin{cases} (t_1 t_2 \omega + t_1\xi_1 + t_3\xi_3)s + (t_2\xi_2 - t_1\xi_1)s_1 + (t_4\xi_4 - t_3\xi_3)s_2 \text{ is independent of } s, s_1, s_2; \\ s\rho_0 \text{ is independent of } s, s_1, s_2; \\ (\xi_0 + t_1\rho_1 + t_3\rho_3)s + (t_2\rho_2 - t_1\rho_1)s_1 + (t_4\rho_4 - t_3\rho_3)s_2 \text{ is independent of } s, s_1, s_2. \end{cases}$$

Thus,

$$\begin{cases} t_1t_2\omega + t_1\xi_1 + t_3\xi_3 = 0 \\ t_2\xi_2 - t_1\xi_1 = 0 \\ t_4\xi_4 - t_3\xi_3 = 0 \\ \rho_0 = 0 \\ \xi_0 + t_1\rho_1 + t_3\rho_3 = 0 \\ t_2\rho_2 - t_1\rho_1 = 0 \\ t_4\rho_4 - t_3\rho_3 = 0 \end{cases}$$

The adversary can take

$$\rho_0 = \rho_1 = \rho_2 = \rho_3 = \rho_4 = \xi_0 = 0$$

Then he has to determine $\xi_1, \xi_2, \xi_3, \xi_4$ such that

$$\begin{cases} t_1t_2\omega + t_1\xi_1 + t_3\xi_3 = 0 \\ t_2\xi_2 - t_1\xi_1 = 0 \\ t_4\xi_4 - t_3\xi_3 = 0 \end{cases}$$

Now the adversary can take

$$\xi_3 = \xi_4 = 0$$

Correspondingly, *both t_3, t_4 are not essential to the security of the scheme.* Hence, the adversary has to determine ξ_1, ξ_2, or g^{ξ_1}, g^{ξ_2}, such that

$$\begin{cases} t_2\omega + \xi_1 = 0 \\ t_2\xi_2 - t_1\xi_1 = 0 \end{cases}$$

or

$$\begin{cases} g^{\xi_1} = g^{-t_2\omega} = V_2^{-\omega} \\ g^{\xi_2} = g^{-t_1\omega} = V_1^{-\omega} \end{cases}$$

Since t_1, t_2, ω are inaccessible to the adversary, it only needs to prevent the adversary from obtaining $V_2^{-\omega}, V_1^{-\omega}$.

Suppose that the adversary could collaborate with another n users with identities $\mathcal{U}_0, \mathcal{U}_1, \cdots, \mathcal{U}_n$ and corresponding keys

$$K_1^{(i)} = (V_2^{-\omega})(g_0 g_1^{\mathcal{U}_i})^{-r_1^{(i)}t_2}, K_2^{(i)} = (V_1^{-\omega})(g_0 g_1^{\mathcal{U}_i})^{-r_1^{(i)}t_1}, \quad i = 0, 1, \cdots, n$$

In view of the given public parameters are $g, \hat{e}, V_1, V_2, \Omega = \hat{e}(g,g)^{\omega t_1 t_2}$, it is easy to find the adversary can not extract out the factor $V_2^{-\omega}$ because $r_1^{(i)}, i = 0, \cdots, n$, are randomly chosen by the system manager and they are only known to the manager. To see this, denote $(g_0 g_1^{\mathcal{U}_i})^{-r_1^{(i)}t_2}$ by $Y^{(i)}$. Apparently, $Y^{(i)}$ is random and only known to the manager. Hence, the adversary can not derive out the common $V_2^{-\omega}$ from $K_1^{(i)} = V_2^{-\omega}Y^{(i)}, i = 0, \cdots, n$.

By the above analysis, we know the secret parameter ω is very important to the security of the BW06 scheme. Whereas, t_3, t_4 can be reasonably discarded. The observation leads us to a simplified version of the BW06 scheme. For convenience, we call it Scheme-1.

3.4 A simplification of the BW06 scheme

See the Table 1 for the simplified version of the BW06 scheme and the differences between the original and the new.

Table 1

	The BW06 scheme	Scheme-1
Setup	spk: Pick $\omega, t_1, t_2, t_3, t_4 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and set $G, G_1, p, g, g_0, g_1, \hat{e}, \Omega = \hat{e}(g,g)^{t_1 t_2 \omega}$, $V_1 = g^{t_1}, V_2 = g^{t_2}, V_3 = g^{t_3}, V_4 = g^{t_4}$ $ssk : \{\omega, t_1, t_2, t_3, t_4\}$	spk: Pick $\omega, t_1, t_2 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and set $G, G_1, p, g, g_0, g_1, \hat{e}, \Omega = \hat{e}(g,g)^{t_1 t_2 \omega}$, $V_1 = g^{t_1}, V_2 = g^{t_2}$ $ssk : \{\omega, t_1, t_2\}$
Extract	$upk : \mathcal{U}$ usk: Pick $r_1, r_2 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $K_0 = g^{r_1 t_1 t_2 + r_2 t_3 t_4}$, $K_1 = g^{-\omega t_2}(g_0 g_1^{\mathcal{U}})^{-r_1 t_2}$ $K_2 = g^{-\omega t_1}(g_0 g_1^{\mathcal{U}})^{-r_1 t_1}$ $K_3 = (g_0 g_1^{\mathcal{U}})^{-r_2 t_4}, K_4 = (g_0 g_1^{\mathcal{U}})^{-r_2 t_3}$	$upk : \mathcal{U}$ usk: Pick $r_1 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $K_0 = g^{r_1 t_1 t_2}$, $K_1 = g^{-\omega t_2}(g_0 g_1^{\mathcal{U}})^{-r_1 t_2}$ $K_2 = g^{-\omega t_1}(g_0 g_1^{\mathcal{U}})^{-r_1 t_1}$
Encrypt	Pick $s, s_1, s_2 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $C' = M\Omega^s, C_0 = (g_0 g_1^{\mathcal{U}})^s, C_1 = V_1^{s-s_1}$, $C_2 = V_2^{s_1}, C_3 = V_3^{s-s_2}, C_4 = V_4^{s_2}$ Output $(C', C_0, C_1, C_2, C_3, C_4)$	Pick $s, s_1 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $C' = M\Omega^s, C_0 = (g_0 g_1^{\mathcal{U}})^s, C_1 = V_1^{s-s_1}$, $C_2 = V_2^{s_1}$, Output (C', C_0, C_1, C_2)
Decrypt	$M = C'\hat{e}(C_0, K_0)\hat{e}(C_1, K_1)$ $\cdot\hat{e}(C_2, K_2)\hat{e}(C_3, K_3)\hat{e}(C_4, K_4)$	$M = C'\hat{e}(C_0, K_0)\hat{e}(C_1, K_1)$ $\cdot\hat{e}(C_2, K_2)$

Consistency argument As for the anonymity of the Scheme-1, it only needs to observe that both C_3, C_4 are not used to blind the message M or the identity $\mathcal{U}$. For the confidentiality, it can be derived from the above analysis, which really differs from the common argument. It is more helpful to explain why a protocol should like this, not like that.

3.5 An explicit analysis of the BW06 scheme

In the original scheme, the authors block the transition of the identity $\mathcal{U}$ and the secret parameters $\omega, t_1, t_2, t_3, t_4, r_1, r_2$ by setting $(g_0 g_1^{\mathcal{U}})$ and the generator g, separately, where $\log_{g_0} g_1, \log_g g_0$, and $\log_g g_1$ are not known to anybody. This leads them to introduce more parameters. But we know the merit of a bilinear map is that it is of Smooth Transition:

$$\hat{e}(g^a, h^b) = \hat{e}(g^b, h^a) = \hat{e}(g^{ab}, h) = \hat{e}(g, h^{ab}) = \hat{e}(g, h)^{ab}$$

We now take advantage of this merit to improve the BW06 scheme. To blind M and $\mathcal{U}$ *simultaneously*, we set

$$C = \Omega^{s\mathcal{U}} M$$

where Ω is a system public parameter to be specified, s is a random number chosen by the encryptor. The new scheme, called Scheme-2, can be described as follows (see the Table 2).

Table 2

	The BW06 scheme	Scheme-2
Setup	*spk*: Pick $\omega, t_1, t_2, t_3, t_4 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and set $G, G_1, p, g, g_0, g_1, \hat{e}, \Omega = \hat{e}(g,g)^{t_1 t_2 \omega}$, $V_1 = g^{t_1}, V_2 = g^{t_2}, V_3 = g^{t_3}, V_4 = g^{t_4}$ $ssk : \{\omega, t_1, t_2, t_3, t_4\}$	*spk*: Pick $\omega, t \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and set $G, G_1, p, g, \hat{e}, \Omega = \hat{e}(g,g)^{\omega t}$, $V = g^t$ $ssk : \{\omega, t\}$
Extract	*upk*: $\mathcal{U}$ *usk*: Pick $r_1, r_2 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $K_0 = g^{r_1 t_1 t_2 + r_2 t_3 t_4}$, $K_1 = g^{-\omega t_2}(g_0 g_1^{\mathcal{U}})^{-r_1 t_2}$ $K_2 = g^{-\omega t_1}(g_0 g_1^{\mathcal{U}})^{-r_1 t_1}$ $K_3 = (g_0 g_1^{\mathcal{U}})^{-r_2 t_4}, K_4 = (g_0 g_1^{\mathcal{U}})^{-r_2 t_3}$	*upk*: $\mathcal{U}$ *usk*: Pick $r \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $K_0 = g^{\omega t(r-\mathcal{U})}$, $K_1 = g^{-\omega r}$
Encrypt	Pick $s, s_1, s_2 \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $C' = M\Omega^s, C_0 = (g_0 g_1^{\mathcal{U}})^s, C_1 = V_1^{s-s_1}$, $C_2 = V_2^{s_1}, C_3 = V_3^{s-s_2}, C_4 = V_4^{s_2}$ Output $(C', C_0, C_1, C_2, C_3, C_4)$	Pick $s \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and compute $A = g^s, B = V^s$, $C = \Omega^{s\mathcal{U}} M$ Output (A, B, C)
Decrypt	$M = C'\hat{e}(C_0, K_0)\hat{e}(C_1, K_1)$ $\cdot\hat{e}(C_2, K_2)\hat{e}(C_3, K_3)\hat{e}(C_4, K_4)$	$M = \hat{e}(A, K_0)\hat{e}(B, K_1)C$

Correctness

$$\begin{aligned}
\hat{e}(A, K_0)\hat{e}(B, K_1)C &= \hat{e}\left(g^s, g^{\omega t(r-\mathcal{U})}\right) \cdot \hat{e}(V^s, g^{-\omega r})\Omega^{s\mathcal{U}} M \\
&= \hat{e}(g,g)^{s\omega t(r-\mathcal{U})} \cdot \hat{e}(g,g)^{-\omega r t s} \cdot \hat{e}(g,g)^{\omega t s \mathcal{U}} M \\
&= M
\end{aligned}$$

Security Without loss of generality, given a ciphertext $(g^s, V^s, \Omega^{s\mathcal{U}} M)$, suppose that the adversary sets

$$K_0 = g^{\lambda_0}, K_1 = g^{\lambda_1}$$

where λ_0, λ_1 are to be determined. By the Decryption, we have

$$\hat{e}(A, K_0)\hat{e}(B, K_1)C = \hat{e}(g^s, g^{\lambda_0})\hat{e}(g^{ts}, g^{\lambda_1})\hat{e}(g,g)^{\omega t s \mathcal{U}} M = \hat{e}(g,g)^{s(\lambda_0 + t\lambda_1 + \omega t \mathcal{U})} M$$

Since the resulting plaintext M is independent of the random number s, the adversary has to determine λ_0, λ_1, or $g^{\lambda_0}, g^{\lambda_1}$, such that

$$\lambda_0 + t\lambda_1 + \omega t \mathcal{U} = 0 \quad \text{or} \quad g^{\lambda_0 + t\lambda_1 + \omega t \mathcal{U}} = 1$$

To generate the proper λ_0, λ_1, or $g^{\lambda_0}, g^{\lambda_1}$, the best choice for the adversary is to set $\lambda_0 = 0$ or $\lambda_1 = 0$.

If $\lambda_0 = 0$, he has to determine λ_1 such that

$$\lambda_1 + \omega \mathcal{U} = 0 \quad \text{or} \quad K_1 g^{\omega \mathcal{U}} = 1$$

In view of ω is only known to the system manager, the adversary has to determine $g^{\omega\mathcal{U}}$. Even suppose the adversary knows the ciphertext is for the identity $\mathcal{U}$, he has to generate g^{ω}.

If $\lambda_1 = 0$, he has to determine λ_0 such that

$$\lambda_0 + \omega t\mathcal{U} = 0 \quad \text{or} \quad K_0 g^{\omega t\mathcal{U}} = 1$$

In view of ω, t are only known to the system manager, the adversary has to determine $g^{\omega t\mathcal{U}}$. Even suppose the adversary knows the ciphertext is for the identity $\mathcal{U}$, he has to generate $g^{\omega t}$.

In sum, the adversary has at least to generate g^{ω} or $g^{\omega t}$, given the public parameters $\Omega = \hat{e}(g,g)^{\omega t}, V = g^t$, and another n users' secret keys

$$K_0^{(i)} = g^{\omega t(r_i - \mathcal{U}_i)} = (g^{\omega t})^{(r_i - \mathcal{U}_i)}, \quad K_1^{(i)} = g^{-\omega r_i} = (g^{\omega})^{-r_i}, \quad i = 1, \cdots, n$$

In view of these $r_i, i = 1, \cdots, n$, are randomly chosen by the system manager and only known to the manager, we see the adversary can not derive out g^{ω} or $g^{\omega t}$ from them.

Remark One could censure our consistency argument does differ from a common argument. But we should stress the argument is more helpful to unveil the psychologic activities during the investigation. It seems that a common argument for a cryptographic protocol is easier to distract the readers' attentions. Sometimes, it also distracts its inventors' attentions.

4 Conclusion

In the past years, the only principle for designing cryptographic protocols is Security. The general instruction for designing a new scheme is to build the new on some preliminary schemes. Consequently, the method to introduce more parameters in a new scheme is broadly adopted. To achieve different purposes, different parameters are separately introduced. As a result, the whole scheme becomes gross. In this paper, by a general attempt to attack the BW06 scheme, we obtain a very efficient version of it. The technique developed in the paper will be helpful to better other protocols.

Acknowledgements We acknowledge the Cryptasc Project (Institute for the Encouragement of Scientific Research and Innovation of Brussels).

References

[1] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In Advances in Cryptology-CRYPTO 2004, LNCS 3152, pp. 443-459. Springer, 2004

[2] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In Advances in CryptologyEUROCRYPT 2004, LNCS 3027, pp. 223-238. Springer, 2004

[3] D. Boneh, X. Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Advances in Cryptology-EUROCRYPT 2005, LNCS 3494, pp. 440-56. Springer, 2005

[4] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. SIAM Journal of Computing, 32(3):586C615, 2003. Extended abstract in Advances in Cryptology-CRYPTO 2001

[5] M. Bellare, T. Ristenpart. Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters'IBE Scheme. In Advances in Cryptology-EUROCRYPT 2009, LNCS 5479, pp. 407-424. Springer, 2006

[6] X. Boyen, B. Waters. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In Advances in Cryptology-CRYPTO 2006, LNCS 4117, pp. 290-307. Springer, 2006

[7] C. Gentry. Practical identity-based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2006, LNCS 4004, pp. 445-464. Springer, 2006

[8] T. Icart. How to Hash into Elliptic Curves, In Advances in Cryptology-CRYPTO 2009, LNCS 5677, pp. 303-316. Springer, 2009

[9] V. Miller. The Weil pairing, and its efficient calculation. Journal of Cryptology, 17(4), pp. 235-261. Springer, 2004

[10] B. Waters. Efficient identity-based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2005, LNCS 3494, pp. 114-127. Springer, 2005