An ID-based Blind Signature Scheme from Bilinear Pairings

B.Umaprasada Rao buprasad@yahoo.co.in
Research scholar
Dept. of Engineering Mathematics
A.U. College of Engineering
Andhra University
Visakhapatnam. A.P, INDIA

K.A.Ajmath
Research scholar kaajmath@yahoo.com
Dept.of Mathematics
Sri Venkateswara University
Tirupati. A.P, INDIA

Dr.P.Vasudeva Reddy vasucrypto@yahoo.com
Associate Professor
Dept. of Engineering Mathematics
A.U. College of Engineering
Andhra University
Visakhapatnam, A.P, INDIA

T.Gowri gowri3478@yahoo.com
Associate Professor
Dept. of Electronics and Communication Engineering
Audisankara College of Engineering & technology
Gudur, Nellore Dist. A.P. INDIA.

Abstract

Blind signatures, introduced by Chaum, allow a user to obtain a signature on a message without revealing any thing about the message to the signer. Blind signatures play an important role in plenty of applications such as e-voting, e-cash system where anonymity is of great concern. Identity based(ID-based) public key cryptography can be a good alternative for certificate based public key setting, especially when efficient key management and moderate security are required. In this paper, we propose an ID-based blind signature scheme from bilinear pairings. The proposed scheme is based on the Hess ID- based digital signature scheme. Also we analyze security and efficiency of the proposed scheme.

Keywords: Public key cryptography, Blind signature scheme, Hess ID based digital signature scheme, Bilinear pairing, CDH problem.

1. INTRODUCTION

Digital signature is a cryptographic tool to authenticate electronic communications. Digital signature scheme allows a user with a public key and a corresponding private key to sign a document in such a way that anyone can verify the signature on the document (using her/his public key), but no one can forge the signature on any other document. This self-authentication is required for some applications of digital signatures such as certification by some authority.

Blind signature is a variant of digital signature scheme. Blind signatures play a central role in digital cash schemes. A user can obtain from a bank a digital coin using a blind signature protocol. The coin is essentially a token properly signed by the bank. The blind signature protocols enable a user to obtain a signature from a signer so that the signer does not learn any information about the message it signed and so that the user can not obtain more than one valid signature after one interaction with the signer. The concept of blind signatures provides anonymity of users in applications such as electronic voting, electronic payment systems etc.

The concept of a blind signature scheme was introduced by Chaum[1], since then many blind signature schemes have been presented in the literature[2,3,4,5].Blind signature scheme allows a user to acquire a signature from the signer without revealing message content for personal privacy. The basic idea is as follows. The user chooses some random factors and embeds them into the message to be signed, while the signer cannot recover the message. Using the blind signature scheme, the user gets the blinded signature and removes the random factors. Then the user outputs a valid signature. This property is very important for implementing e-voting, e-commerce, and e-payment systems, etc.

In public key cryptosystem, each user has two keys, a private key and a public key. The binding between the public key(PK) and the identity(ID) of a user is obtained via a digital certificate. However, in certificate-based system before using the public-key of a user, the participant must first verify the certificate of the user. As a consequence, this system requires a large amount of computing time and storage when the number of users increases rapidly.

In 1984, Shamir [6] introduced the concept of ID-based cryptography to simplify key management procedures in public key infrastructures. Following Joux's [7] discovery on how to utilize bilinear pairings in public key cryptosystems, Boneh and Franklin [8] proposed the first practical ID-based encryption scheme in Crypto 2001. Since then, many ID-based encryption and signature schemes have been proposed that use bilinear pairings. ID-based cryptography helps us to simplify the key management process in traditional public key infrastructures. In ID-based cryptography any public information such as e-mail address, name, etc., can be used as a public key. Since public keys are derived from publicly known information, their authenticity is established inherently and there is no need for certificates in ID-based cryptography. The private key for a given public key is generated by a trusted authority and is sent to the user over a secure channel.

In this paper, a blind signature scheme in the identity-based setting is presented. The scheme is based on the Hess ID-based signature scheme. The proposed signature scheme is validated and its security is proven under the assumption that the hardness of the Computational Diffie-Hellman problem.

The rest of the paper is organized as follows. Section 2 briefly explains the bilinear pairings and some computational problems, on which of our scheme is based .The syntax and security model of ID-based Blind signature Scheme is given in Section3. We then present our ID-based Blind Signature Scheme from bilinear pairings in Section 4. The correctness and security analysis of the proposed scheme is given in Section 5. Section 6 concludes this paper

2. PRELIMANARIES

In this section, we will briefly review the basic concepts on bilinear pairings and some related mathematical problems, and then we present ID-based public key setting from pairings.

2.1 Bilinear Pairings

Let G_1 be a additive cyclic group generated by P whose order is a prime q and G_2 be a multiplicative cyclic group of the same order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

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

2.2 Computational problems

Now, we give some computational problems, which will form the basis of security for our scheme.

-Discrete Logarithm Problem (DLP): Given two group elements P and Q, find an integer n such that $Q = nP$ whenever such an integer exists.

-Decisional Diffie-Hellman Problem (DDHP): For $a, b, c \in_R Z_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \bmod q$.

-Computational Diffie-Hellman Problem (CDHP): For $a, b, c \in_R Z_q^*$, given P, aP, bP, Compute abP.

We assume through this paper that CDHP and DLP are intractable. When the DDHP is easy but the CDHP is hard on the group G, we call G a Gap Diffe-Hellman (GDH) group. Such groups can be found on super singular elliptic curves or hyper elliptic curves over finite field and the bilinear pairings can be derived from the Weil or Tate pairing.

2.3 ID- based public key setting using pairings

In ID-based public key cryptosystems (IDPKC), everyone's public key is predetermined by information that uniquely identifies them, such as name, social security number, email address, etc., rather than an arbitrary string. This concept was first proposed by Shamir [6]. Since then, many researchers devote their effort on ID-based cryptographic schemes.

ID-based public key setting involves a Key Generation Centre (KGC) and users. The basic operations consists of Setup and Private Key extraction (simply Extract). When we use bilinear pairings to construct IDPKC, **Setup** and **Extract** can be implemented as follows:

Let P be a generator of G_1. Remember that G_1 is an additive group of prime order q and the bilinear pairing is given by $e: G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $H_1: \{0,1\}^* \to G_1^*$, $h: \{0,1\}^* \times G_2 \to Z_q^*$.

-Setup: KGC chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$. The center publishes system parameters $params < G_1, G_2, e, P, P_{pub}, H_1, h >$ and keeps $< s >$ as the master-key, which is known only by itself.

-Extract: A user submits his/her identity information ID to KGC. KGC computes the user's public key as $Q_{ID} = H_1(ID)$, and returns $d_{ID} = sQ_{ID}$ to the user as his/her public key.

2.4 Review of Hess-ID- based signature scheme

To prepare for the proposed scheme, we first give a review of the Hess ID-based signature scheme [9].

-Setup: The Private Key Generator (PKG) chooses $s \in_R Z_q^*$ as his master secret key and computes the global public key $P_{pub} = sP$. The PKG also selects a map-to-point hash function $H_1 : \{0,1\}^* \to G_1^*$ and another cryptographic hash function $h : \{0,1\}^* \times G_2 \to Z_q^*$. PKG publishes system parameters $params < G_1, G_2, e, P, P_{pub}, H_1, h >$ and the master key $< s >$ is kept secret.

-Extract: Given the public identity information on ID, compute the secret key for the identity ID as $d_{ID} = sQ_{ID}$. The component $Q_{ID} = H_1(ID)$ plays the role of the corresponding public-key.

-Signature: To sign a message $M \in \{0,1\}^*$, using the secret key d_{ID}, the signer chooses an arbitrary $P_1 \in G_1^*$ and picks a random integer $k \in z_q^*$.

Then signer computes

$$R = e(P_1, P)^k,$$
$$V = h(M, R),$$
$$U = Vd_{ID} + kP_1.$$

The signature on message M is $\sigma = (U,V) \in G_1 \times Z_q^*$.

-Verification: To verify the signature $\sigma = (U,V)$ of an identity ID on a message M, the verifier computes $R = e(U, P)e(Q_{ID}, -P_{pub})^V$. He accepts the signature if and only if $V = h(M, R)$.

3. SYNTAX AND STRUCTURE OF BLIND SIGNATURE SCHEME

The formal definition of a blind signature is presented below.

Blind Signatures: A blind signature scheme consists of three algorithms and two parties (the user and the signer). The details are as follows.

-System Key Generation: This is a probabilistic polynomial time algorithm (PPT algorithm). It takes a security parameter *k* as its input and outputs a pair of public key and private key *{y, x}* for the blind signature scheme, where *x* is preserved secretly by the signer.

-Generation of Blind Signatures: This is an interactive and probabilistic polynomial time algorithm protocol, which is operated by the user and the signer. The user first blinds the message *m* and obtains a new version m' of *m*, and then sends it to the signer. The latter utilizes his/her private key to sign on m' and obtains S', and then sends it to the user. The user unblinds it to obtain S which is a blind signature on *m*.

-Verification of Blind Signatures: This is a deterministic polynomial time algorithm. Given a message *m* and its alleged blind signature S, anyone who knows the public key *can* verify the validity of S. If it is valid, then the algorithm outputs '1'; otherwise outputs '0'.

The blindness property of a signature scheme may be formally defined as follows: A blind signature scheme possesses the blindness property, if the signer's view (m', S') and the message-signature pair (m, S) are statistically independent.

A secure blind signature scheme must satisfy the following three requirements:

-Correctness: If the user and the signer both comply with the algorithm of blind signature generation, then the blind signature S will be always accepted.

-Unforgeability of Valid Blind Signatures: It is with respect to the user especially, i.e. the user is not able to forge blind signatures which are accepted by the algorithm of Verification of Blind Signatures.

-Blindness: While correctly operating one instance of the blind signature scheme, let the output be (*m, S*) (i.e. message-signature pair), and the view of the protocol V. At a later time, the signer is not able to link V to (*m, S*).

4. PROPOSED ID-BASED BLIND SIGNATURE SCHEME:

In this section, we present an ID-based blind signature scheme from the bilinear pairings.

Setup: The PKG chooses $s \in Z_q^*$ as his master key and computes the global public key P_{pub} as sP. The PKG also selects a map-to-point hash function $H_1 : \{0,1\}^* \to G_1^*$ and another cryptographic hash function $h : \{0,1\}^* \times G_2 \to Z_q^*$. PKG publishes system parameters $params < G_1, G_2, e, P, P_{pub}, H_1, h >$ and keeps the master key $< s >$ as secret.

Extract: Given signer's public identity $ID \in \{0,1\}^*$, compute the public key $Q_{ID} = H_1(ID)$ and the corresponding private key $d_{ID} = sQ_{ID}$.

Initialization: The signer randomly chooses $k \in Z_q^*$, compute $R = e(P, P)^k$ and sends R to the user as a commitment.

Blinding: The user randomly chooses $a, b \in Z_q^*$ as blinding factors, compute $R' = e(bQ_{IDs} + aP, \mathrm{P_{pub}}).R$, $V = h(m, \mathrm{R'}) + \mathrm{b}$ and sends V to the signer.

Signing: The signer computes $S = Vd_{IDs} + kP$, and send S to the user

Unblinding: The user compute $S' = S + aP_{pub}$, $V' = V - b$ and outputs (m, S', V'), then (S', V') is the blind signature of the message m.

Verification: Accept the signature if and only if $V' = h(m, e(S', P).e(Q_{IDs}, P_{pub})^{-V'})$.

5. Analysis of the proposed scheme

5.1 Correctness

The following equations give the correctness of the proposed scheme.

$$
\begin{aligned}
& h(m, e(S', P).e(Q_{IDs}, P_{pub})^{-V'}) \\
& = h(m, e(S + aP_{pub}, P).e(Q_{IDs}, P_{pub})^{-V'}) \\
& = h\left(m, e(S, P).e(aP_{pub}, P).e(Q_{IDs}, P_{pub})^{-V'}\right) \\
& = h\left(m, e(Vd_{IDs} + kP, P).e(aP_{pub}, P).e(Q_{IDs}, P_{pub})^{-V'}\right) \\
& = h\left(m, e(Vd_{IDs}, P).e(kP, P).e(aP_{pub}, P).e(Q_{IDs}, P_{pub})^{-V+b}\right)
\end{aligned}
$$

$$= h\left(m, e(d_{IDs}, P)^{V}.e(P,P)^{k}.e\left(aP, P_{pub}\right).e\left(Q_{IDs}, P_{pub}\right)^{-V}.e\left(Q_{IDs}, P_{pub}\right)^{b}\right)$$

$$= h\left(m, e\left(Q_{IDs}, P_{pub}\right)^{V}.e\left(P,P\right)^{k}.e\left(aP, P_{pub}\right).e\left(Q_{IDs}, P_{pub}\right)^{-V}.e\left(Q_{IDs}, P_{pub}\right)^{b}\right)$$

$$= h\left(m, e\left(P,P\right)^{k}.e\left(aP + bQ_{IDs}, P_{pub}\right)\right)$$

$$= h\left(m, R'\right)$$

$$= V - b$$

$$= V'.$$

5.2 Security

In the following, we will show that our ID-based Blind signature scheme satisfies all the requirements stated in Section 3.

Blindness property: To prove the blindness we show that given a valid signature $\left(m, S', V'\right)$ and any view $\left(R, V, S\right)$, there always exists a unique pair of blinding factors $a, b \in Z_q^*$. Since the blinding factors $a, b \in Z_q^*$ are chosen randomly, the blindness of the signature scheme naturally satisfies. We can find more formal definition about the blindness [10, 11, 12, 13].

Given a valid signature $\left(m, S', V'\right)$ and any view $\left(R, V, S\right)$, then the following equations must hold for $a, b \in Z_q^*$:

$$R' = e\left(bQ_{IDs} + aP, P_{pub}\right).R \qquad (1)$$

$$\mathrm{V}=\mathrm{h}\left(\mathrm{m},\mathrm{R}'\right)+b \qquad (2)$$

$$\mathrm{S}' = S + aP_{pub} \qquad (3)$$

$$\mathrm{b}=\mathrm{V}-\mathrm{h}\left(\mathrm{m},\mathrm{R}'\right) \text{ and } \mathrm{aP}_{\mathrm{pub}}=\mathrm{S}'-\mathrm{S}$$

It is obvious that $a, b \in Z_q^*$ is existed uniquely from (2) and (3). Next we show that such $a, b \in Z_q^*$ satisfy the first equation too. Obviously, due to the non-degenerate of the bilinear pairings we have $R' = e\left(bQ_{IDs} + aP, P_{pub}\right).R \Leftrightarrow e(R', P_{pub}) = e\left(e\left(bQ_{IDs} + aP, P_{pub}\right), P_{pub}\right)$. So we only need to show that such a and b satisfy $e(R', P_{pub}) = e\left(e\left(bQ_{IDs} + aP, P_{pub}\right), P_{pub}\right)$.

We have

$$e\left(e\left(bQ_{IDs} + aP, P_{pub}\right).R, P_{pub}\right) =$$

$$=\mathrm{e}\left(\mathrm{e}\left(\mathrm{bd}_{\mathrm{IDs}} + aP_{pub}, P\right).R, P_{pub}\right)$$

$$=\mathrm{e}\left(\mathrm{e}\left(\left(\mathrm{V}-\mathrm{h}\left(\mathrm{m},\mathrm{R}'\right)\right)d_{IDs}, P\right).e\left(aP_{pub}, P\right).R, P_{pub}\right)$$

$$=\mathrm{e}\left(\mathrm{e}\left(\left(\mathrm{V}-\mathrm{h}\left(\mathrm{m},\mathrm{R}'\right)\right)d_{IDs}, P\right)e\left(S' - S, P\right).R, P_{pub}\right)$$

$$=\mathrm{e}\left(\mathrm{e}\left(\mathrm{Vd}_{\mathrm{IDs}}, P\right)e\left(-h\left(m, R'\right)d_{IDs}, P_{pub}\right)e\left(S', P\right)e\left(S, P\right)^{-1}.R, P_{pub}\right)$$

$$=\mathrm{e}\left(\mathrm{e}\left(\mathrm{S}-\mathrm{kP},\mathrm{P}\right)e\left(-h\left(m, R'\right)d_{IDs}, P\right)e\left(S', P\right)e\left(S, P\right)^{-1}.R, P_{pub}\right)$$

$$=\mathrm{e}\left(e\left(-h\left(m, R'\right)d_{IDs}, P\right)R'e\left(Q_{IDs}, P_{pub}\right)^{V_i}, P_{pub}\right)$$

$$=\mathrm{e}\left(\mathrm{e}\left(-\mathrm{h}\left(\mathrm{m},\mathrm{R}'\right)Q_{IDs}, P_{pub}\right)R'e\left(h\left(m, R'\right)Q_{IDs}, P_{pub}\right), P_{pub}\right)$$

$$=\mathrm{e}\left(\mathrm{R}', P_{pub}\right)$$

Thus the blinding factors always exist which lead to the same relation defined in the signature issuing protocol.

Unforgeability: Assume that ***A*** is the adversary (he/she can be a user or any third party) holding the system parameters $params < G_1, G_2, e, P, P_{pub}, H_1, h >$ and the identity public key Q_{IDs} of the signer IDs . ***A*** tries to forge a valid message-signature of the signer.

First, we assume that ***A*** performs the ID attack, i.e. ***A*** queries **Extract** qE (qE>0) times with (PARAMS, $ID_i \neq ID$) for i=1….qE. **Extract** returns to ***A*** the qE corresponding secret key d_{IDs_i} . We assume that qE is limited by a polynomial in k. If ***A*** can get a $\left(ID_{s_i}^{'}, d_{IDs_i}^{'} \right)$ such that $H_1\left(ID_{s_i}^{'} \right) = H_1\left(IDs \right) = Q_{IDs}$, then he/she can forge a valid blind signature of the signer ID. But since H_1 is random oracle, **Extract** generates random numbers with uniform distributions. This means that ***A*** learns nothing from query results.

Next we assume that ***A*** had interacted with the signer ID, and let $\left(R, V, S \right)$ be the view in the blind signature issuing phase. Since $S = Vd_{IDs} + kP$ and ***A*** knows S,V, from S to get d_{IDs} , ***A*** must know k, but k is chosen randomly by signer. ***A*** Knows $R = e\left(P, P \right)^k$, but from R to get k, this is CDHP in G_1 . We assume that CDHP in G_1 in intractable, so ***A*** cannot get the private information of the signer at the blind signature issuing phase.

On the other hand, the signature and the verifying equation are same as Hess ID- based signature scheme. For any message m, if ***A*** can construct $S^{'} and\ V^{'}$ such that $V^{'} = h\left(m, e\left(S^{'}, P \right) e\left(Q_{IDs}, P_{pub} \right)^{-V^{'}} \right)$, then ***A*** can forge a valid signature of Hess ID-based signature scheme on the message m. Due to Hess proof on their ID-based signature scheme (i.e., Hess ID-based signature scheme is proven to be secure against existential forgery on adaptive chosen message and ID attacks, under the hardness assumption of CDHP and the random oracle model), we claim that this attack is impossible.

Efficiency: We compare our blind signature scheme with the Zhang- Kim ID-based blind signature scheme [11] from computation overhead and summarize the result in Table1. We denote p_a the pairing operation, p_m the point scalar multiplication on G_1, ***Ad*** the point addition on G_1, ***Mu*** the multiplication in Z_q^*, and ***Mu*** G_2 the multiplication in G_2, ***Me*** exponentiation in G_2.

Schemes	Blind signature issuing	Verification
Proposed scheme	User : 1***Pa***+3***Pm***+1***Mu***+3***Ad*** Signer: 1***Pa***+1***Me***+2***Mu***+1***Ad***	2***Pa***+1***Me***
The scheme [11]	User : 1***Pa***+3***Pm***+3***Ad*** Signer: 3***Pm***+1***Ad***	2***Pa***+1***Pm***+1***Mu*** G_2

Table 1. Comparision of our scheme with Zhang-Kim scheme

The efficiency of the system of paramount importance when the number of verifications is considerably large (e.g., when a bank issues a large number of electronic coins and the customer wishes to verify the correctness of the coins). Assuming that $\left(S_1^{'}, V_1^{'} \right), \left(S_2^{'} V_2^{'} \right), - - -, \left(S_n^{'}, V_n^{'} \right)$ are ID-based blind signatures on messages $m_1, m_2, - - -, m_n$ respectively, which are issued by the signer with identity ID. The verification of each signature is as follows:

$V_i^{'} = h\left(m_i, e\left(S_i^{'}, P \right) e\left(Q_{IDs}, -P_{pub} \right)^{V_i^{'}} \right)$, *for* i=1,2,...,n .

To verify these signatures individually, our scheme requires only (n+1) pairing operations, where as the Zhang-Kim scheme requires 2n pairing operations. So, with the proposed scheme we can save (n-1) pairing operations. In particular, here, we consider only computations of pairing operation (Pa), we need not consider the remaining operations as they are cheaper than the computation of pairings. We note that the computation of pairing is the most time consuming. Although there has been many papers discuss the complexity of pairings and how to speedup the pairing computation [14, 15], the computation of pairing is still time consuming.

6. CONCLUSIONS

In this paper, we proposed an ID-based blind signature scheme from bilinear pairings. The proposed scheme is based on Hess ID-based signature scheme with the assumption CDH Problem is hard. We have discussed the correctness and security analysis of the proposed scheme. The proposed scheme is efficient when the number of blind signature verifications is considerably large.

REFERENCES

[1] D. Chaum, “Blind signatures for untraceable payments”, In Proc. CRYPTO 82, pp.199-203, NY, Plenum, 1983.

[2] T.Okamoto, “Provable, Secure and Practical Identification Schemes and Corresponding signature schemes”, In Advances in Cryptology-CRYPTO 1984, Springer-Verlag, LNCS 740, pp.31-53,1992.

[3] D.Pointcheval and J.Stern, “Provably Secure Blind signature Schemes”, In Advances in Cryptology – ASIACRYPT 1992, Springer-Verlag, LNCS 1163, pp.252-26,1992.

[4] D.Pointcheval and J.Stern, “New Blind Signature Signatures Equilent to Factorization”, In proceedings of the 4th ACM Conference on Computer and Communications Security, pp.92-99, Zurich, Switzerland, 1997.

[5] C.P. Schnorr, “Efficient Identification and Signatures for Smart cards”, In G.Brassard(ed), In proceedings of CRYPTO 1989, Springer-Verlag,LNCS 435,pp.239-252,1990.

[6] A,Shamir, “Identity-based cryptosystems and signature schemes”, In Proc. of CRYPTO’84, LNCS 196, pp. 47-53 Springer-verlag, 1984.

[7] A.Joux, “A one round protocol for tripartite diffie-Hellman” In proc.of ANTS-IV, LNCS 1838, pp.385-394, Springer-Verlag, 2000.

[8] D.Boneh and M.Franklin, “Identity-based encryption from the Weil pairing”, In Proc.of CRYPTO’01, LNCS 2139, pp.213-229, Springer-verlag, 2001.

[9] F. Hess, “Efficient identity based signature schemes based on pairings”, SAC 2002, LNCS2595, pp.310-324, Springer-Verlag, 2002.

[10] A. Juels, M. Luby and R. Ostrovsky, “Security of blind digital signatures”, Advances in Cryptology-Crypto 97, LNCS 1294, pp.150-164, Springer-Verlag, 1997.

[11] F. Zhang and K. Kim, “ID-based blind signature and ring signature from pairings”, Proc. of Asiacrpt 2002, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.

[12] F. Zhang and K. Kim, “*Efficient ID-based blind signature and proxy signature from bilinear pairings”*, ACISP 03, LNCS 2727, pp. 312-323, Springer-Verlag, 2003.

[13] D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind Signatures”, Journal of Cryptology, Vol.13, No.3, pp.361-396, 2000.

[14] P.S.L.M.Barreto, H.Y.Kim, B.Lynn and M.Scott, “Efficient algorithms for pairing- based cryptosystems”, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.

[15] S.D.Galbraith, K. Harrison, and D.Soldera, “Implementing the Tate pairing”, ANTS 2002, LNCS 2369, pp.324-337, Springer-Verlag, 2002.