An Efficient New IBE scheme in the model selective ID

Ch.Ramesh [1] K Venu Gopal Rao [2] D.Vasumathi [3]

1,2 G Narayanamma Institute of Technology and Science, Hyderabad, Telangana,India
3 Jawaharla Nehru Technological University, Hyderabad, Telangana,India

Abstract: A Public-Key System secure against simulation studies, taking into account the purpose of the attacker and the model used. Among the goals there are indistinguished IND and semantic goal. The study considered as strong and concretizing for ideal security is IND-CCA, for the IBE we talk about IND-ID-CCA also: semantics-ID-CPA, semantics-ID-CCA, IND-ID-CPA .This IND-ID-CCA (as well as the others) belongs to a full domain whose identity to attack is declared in the challenge.. It is proved that the transition from selective ID to a complete domain requires a multiplication by N. The first is a HIBE based on the problem and under the Commutative Blinding approach it is known by BB1. While the second is an IBE Under the Exponent-Inversion approach named BB2, it is based on Dq-BDHIP. By combining the idea of the inverse used in BB2 and remaining in the Commutative Blinding approach, In this paper we will propose our New IBE scheme which will be efficient than BB1 and BB2.

keywords: Identity Based Encryption (IBE),Decisional of Diffie and Hellman Problem (DBDHP), Decisional q- Invertible of Bilinear Diffie and Hellman Problem (Dq- BDHIP),CCA,CPA,IND-ID-CPA,IND-ID-CCA .

1 Introduction

1.1 Selective Identification (selective-ID) for IBE / HIBE

The operation of selective-ID is according to the algorithms declared below, here we give the CPA version, without using the extraction of the requests of the decryption in Phase 1. We give the definition in the case of an IBE and it is easy to generalize it for an HIBE.

Init: An opponent A takes up the challenge: the identity ID.
Setup : The challenger derives the Setup algorithm. It gives the opponent the system of parametres resulting in the params and it keeps the master key.
Phase 1 : The adversary resulting from the requests $q_1, q_2, q_3, ...q_m$ with q_i is:
Request the private key for an$< ID_i >$ such as:$ID_i \neq ID*$ And, ID_i is not The prefix of $ID*$. The challenger responds with the KeyGen algorithm (or Extract see Chapter 1) to generate the private key *di* corresponding to the public key of $< ID_i >$. He sends *di* the opponent.

Challenge : Once the opponent decides to finish Phase 1, he takes out two plaintexts $m_0, m_1 \in M$ of the same length. The challenger selects an arbitrary bit b $\in \{0, 1\}$, and it Calculates the ciphertext $c = Encrypt(params, ID*, mb)$. Then he sends it as a challenge to the opponent.
Phase 2 : As Phase 1

Guess : Finally, the opponent makes a guess (*estimation*) $b0 \in \{0, 1\}$. He wins if $b = b_0$

We refer A as an IND-sID-CPA, its advantage to attack a scheme is
$Adv_{\xi,A} =| pr\ [b = b0] - 1$ | it is a probability of a win bit constructed arbitrarily between the challenger and the opponent.

We say that an IBE (for the HIBE of level k, the $ID*$ refers to: $ID1*, ID2*, ...ID_k*$) of a system E is (t, q_{ID}, ε) selective-identity and adaptively secures, if , For each IND-sIDCPA Opponent A which takes place in a time t, which makes at least *qID* requests of private keys that it chooses, one has:
$Adv_{\xi,A} =| pr\ [b = b_0] - ½ |< \varepsilon$ ———— (1)

1.2 Estimation of some bilinear problems of Diffie Hell- man

Setting the parameters G_1, G_2 and G_T ; As well as $\hat{e}$, such as:
G_1, G_2 and G_T of the first order cyclic groups p. g is a generator of G_1 or G_2
$\hat{e} : G_i \times G_i \rightarrow G_T$ or i $\varepsilon\{1, 2\}$,A bilinear application in pairing form.

Definition 1 :

Decisional Bilinear Diffie-Hellman Problem (DBDHP)

Let g be a generator of G1. The DBDHP in < G_1, G_T , $\hat{e}$ > is then:
Given < g, g^a, g^b, g^c, Z > for a,b,c ∈ Zq and $T \in GT$. We say that an algorithm A advantage ∈ to solve the BDHP decision in GT if:

$| \; pr\,[g, g^x, g^{x^2}, ...g^{x^k} \; pr \; [g, g^a, g^b, g^c, \hat{e}(g, g)^{abc}] - | \; pr \; [g, g^a, g^b, g^c, T] > \varepsilon$

This probability is after an arbitrary choice of: a generator g in G_1, (a;b;c) ∈ Z_q X Z_q X Z_q , T ∈ G_T an arbitrary bit chosen by A. The distribution on the right is referenced by P_{BDHP} while that on the left is refreshed by R_{BDHP}.

Definition 2 :

Decisional k-Bilinear Diffie Hellman Inversion Problem (Dk-BDHIP) Is $g \in G2*$ (or in $G1*$). Can we achieve the following inequality :

$| \; pr\,[g, g^x, g^{x^2}, ...g^{x^k} \; \hat{e} \; (g, g)^{\frac{1}{x}}] - | \; pr\,[g, g^x, g^{x^2}, ...g^{x^k} T] > \varepsilon$

For a $g, g^x, g^{x^2}, ...g^{x^k}$ and T given (Where T is in G_T)

2 Proposed New IBE Schema

As we have pointed out, the selective ID model is a weak option. The reader can refer to [7] for a larger idea of the weight of this model. It is also usual that the scheme BB1 traced under this model is more complex, which loses the efficiency for this scheme. In the work [5], we have thought of a reduced scheme under selective ID, to do so we have combined the inverse principle used in the extract Of the BB2 and the approach of the commutative blinding of where it is built BB1.

First scheme: new IBE scheme
Setup : Setting a security parameter t. Let (G1;GT) be two bilinear groups
Choose a generator g ∈ G_1 and let $P_{pub1} = g^l \in G_1*$
Calculate:e(g,g)=x and $e(g,g)^a = x^a = y$ (Where e represents the pairing)

The public parameters are: $M_{pk} = \{G_1, G_T, P_{pub_1}, x, y\}$.

The master key is $M_{sk} = \{l, a\}$.

The message space is: $\{0,1\}^n$.

The ciphertext space is: $G_1^* \times \{0,1\}^n$.

Extract : Given an identity $ID_A \in \{0,1\}^n$ of an Entity M_{pk} and M_{sk}

Select one $r_{ID_A} \in Z_q$ then return $g^{\frac{a+ID_A}{r_{ID_A t}}} = g^{\frac{\frac{a}{r_{ID_A}} + r'_{ID_A} ID_A}{t}} = g^{\frac{a' + r'_{ID_A} ID_A}{t}}$

Then: $d_{ID_A} = (r_{ID_A}, g^{\frac{a+ID_A}{r_{ID_A t}}}) = (r_{ID_A}, d_A)$

Encrypt : Given m ∈ M and M_{p^k} , follow the steps:

1. Choose an arbitrary s in Z_q

2. Calculate: $e(g, g)^{s(ID_A + a)} = (x^{ID_A} y)^s$.

The ciphertext is: $C = (g^{ls} = P_{pub_1}{}^s, m.e(g, g)^{s(ID_A + a)}) = (u, v)$

Decrypt : Given the ciphertext C= (u,v), ID_A, d_A and M_{pk}.

The decryption of C is given by:

Calculate $e(u^{rID_A}, e(u^{rID_A}, g^{\frac{a+ID_A}{rID_A}})$ then output the m= $\frac{v}{e(u^{rID_A}, g^{\frac{a+ID_A}{rID_A}})}$

Note 1: The safety parameter t must satisfy the recommendations of NIST, ECRYPT or others. Filling the desired level requires attention to the largest parameter which constructs the factorization of the order of the curve adapted to the calculation of the pairing e.

Accuracy Since : $e(u^{rID_A}, g^{\frac{a+ID_A}{rID_A}}) = e(g^{lsrID_A}, g^{\frac{a+ID_A}{rID_A}}) = e(g,g)^{s(ID_A+a)}$

The new IBE scheme is then correct.

3 Proof of security under the selective ID model of the new IBE Scheme

Before demonstrating the security of the new IBE scheme, we note that Dk-BDHIP means that, in the sense of Definition 1.2, any k > 0 is used, the latter parameter is not related to the number of users as with Dk-BDHIP (2), it is rather of our choice. It is possible to choose 2 or any number, whereas Dk-BDHIP requires at least 250 from (8) for a security level equal to 80-bits (security level in the case of Symmetric Cryptography).
The security of the new IBE scheme is based on the rigidity of Dk-BDHI, from:

Theorem 1: Suppose that $(t, \overline{k}, \varepsilon)$ -Decision BDHI is rigid in a cyclic group G_1 of length $p(G_1 = p)$.

Then the new IBE scheme is (t, k_s, ε) -selective identity, it is chosen plaintext (IND-sID-CPA) secured, with an advantage:

$$adv^{nouveauIBEscheme}(t) > adv^{\overline{Dk}-DBDHIP}(t - O(\top \overline{k})).$$

for each $k_s(< \overline{k})$ where $\top$ is the time required to calculate the exponentiation in the following study:

Proof:

Suppose an opponent A has a Z advantage to attack the new IBE scheme. We construct an algorithm B that uses A to solve the Decision problem k-BDHI in G1. The algorithm B receives as inputs: arbitrary $(\overline{k}+2)$ -parameters $(g, g^{\propto}, g^{\propto^2}, \ldots g^{\propto^{\overline{k}}}, T)$ $\epsilon G_1^{\overline{k}+1} \times G_T$ which are extracted from P_{BDHI} (with $T = e(g,g)^{a/\alpha}$) or R_{BDHI} (with T is uniform and independent in G_T : group of arrival of the pairings). The purpose of the algorithm B is to output 1 if $T = e(g,g)^{a/\alpha}$ and 0 otherwise. The algorithm B works in collaboration with A to obtain a gain under the selective-ID model as follows:

Setup :

To generate the parameter system, algorithm B does the following:

At the beginning, the algorithm A gives B the identity I = a1 where it wants to attack. The gain of the selective identity begins, but the algorithm B needs the following preparation step:

Preparation step:

In the preparation step, the algorithm B chooses an arbitrary x, then it calculates $b_1 x$. Afterwards, he calculates implicitly:

$$f(\propto) = \sum_{i=1}^{\overline{k}} c_i \propto^i \quad \text{------------ (2)}$$

It arbitrarily chooses r_0 , it also implicitly calculates

$$r_1 = r_0 \sum_{i=1}^{\overline{k}} c_i \propto^{i-1} \quad \text{------------ (3)}$$

Finally, it calculates $h = g^{f(\propto)}$, it publishes this h .

Phase 1 :

Issuing at most k_s private key request, with $k_S < \overline{k}$. Consider the i th request for a private key corresponding to the key ID_i such that:

$(I_i =)ID_i \neq ID^*(= I^*)$. We need private key replies in the form $(r, h^{\frac{a+r(I_t-I^*)}{\propto}})$.

The I_i represents a general identity that has been fixed and I^* represents the identity to be attacked (identity in defie form). r is uniformly distributed in Z_p .

Algorithm B responds to requests as follows:

First, it is possible that the private key in the new IBE scheme can have a syntax in the form: $g^{\frac{a+rID_A}{l}}$ instead of $g^{\frac{a+rID_A}{r^l}}$, since:

$$g^{\frac{a+rID_A}{r^l}} = g^{\frac{a}{r^l}+\frac{r^l ID_A}{l}} = g^{\frac{a^1+r^1 ID_A}{l}} \quad \text{-----------(4)}$$

We need it to simplify the evidence.

B poses $R = \frac{x}{r_0} + r_1$, it calculates implicitly:

$$R = \frac{f(\propto)}{f(\propto)}\left(\frac{x}{r_0} + \frac{r_1}{I_i - I^*} I_i - I^*\right)$$

$$\frac{f(\propto)}{\propto \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}}\left(\frac{x}{r_0} + \frac{r_1}{I_i - I^*}(I_i - I^*)\right)$$

$$= \frac{f(\propto)}{\propto}\left(\frac{x}{r_0 \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}} + \frac{r_1}{\sum_{i=1}^{\bar{k}} c_i \propto^{i-1} (I_i - I^*)}(I_i - I^*)\right)$$

$$= \frac{f(\propto)}{\propto}\left(\frac{x}{r_0 \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}} + \frac{r_0 \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}}{\sum_{i=1}^{\bar{k}} c_i \propto^{i-1} (I_i - I^*)}(I_i - I^*)\right)$$

$$= \frac{f(\propto)}{\propto}\left(\frac{x}{r_0 \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}} + \frac{r_0}{I_i - I^*}(I_i - I^*)\right)$$

$$= \frac{f(\propto)}{\propto}(a' + r'(I_i - I^*)).$$

With $r' = \frac{r_0}{I_i - I^*}$ which can be easily computed by B.

The $a' = \left(\frac{x}{r_0 \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}}\right)$ is the master key, which is not known by B, is like $\propto$.

Note 2: A can publish Q in a system of parameters. To avoid the Computation of a, B can choose its x in such a way that: $g^{a'} = g^{\frac{x}{r_0 \sum_{i=1}^{\bar{k}} c_i \propto^{i-1}}}$ is calculable (it suffices that $X = \sum_{i=1}^{\bar{k}} c_i \alpha^{i-1}$). Next, B looks for a σ such that:

$$g^a g^\sigma = g^{a'}.$$

Then B can easily compute g^R as he knows $g^{\frac{x}{r_0}}$ and g^{r_1} .

However,

$$g^R = g^{\frac{f(a)}{a}}(a'+r'(I_i-I^*)) = h^{\frac{a'+r'(I_i-I^*)}{\alpha}} \text{ ------------(5)}$$

Which is a valid private key, and then B can give A the private key $(r', h^{\frac{a'+r'(I_i-I^*)}{\alpha}})$. With, B does not have the advantage of calculating a private key for I^* .

Challenge :

Outputs two messages $M_0, M_1 \in G_1$. The algorithm B selects an arbitrary bit b$\in \{0,1\}$ and an arbitrary $r \in (Z_p)^*$. It responds with a ciphertext prepared as follows:

We have: $h^s = h^{\frac{s}{a}.\propto} = h^{l'\propto} = c_1$, with $I = \frac{s}{\propto}$

And $c_2 = MT_h^{\frac{s(xb_1+a_1)}{b_1}} = T_h^s(x+I^*)$ or rather

$$c_2 = MT_h^{\frac{s(ab_1+a_1)}{b_1}} = T_h^s(a+I^*)$$

Then if $T_h = e(h,h)^{\frac{1}{\propto}}$ we have

$$e(h,h)^{\frac{s}{\propto}(x+I^*)} = c_2 = e(h,h)^{l'(x+I^*)} \text{. ------------(6)}$$

The combination CT=(c_1, c_2) = $(h^{l'\propto}, e(h,h)^{l'(x+I^*)})$ is valid ciphertext under ID^* if T_h is uniform in G_1 then CT is independent of bit b.

	BB1(version IBE)
Params	$2Exp_{ff_{iG_1/z_q}} + 1coup + 1Exp_{ff_{iG_T/z_q}}$
Extract	$2Mul_{ff_{iz_q/z_q}} + 2Exp_{ff_{iG_1/z_q}}$
Encrypt	$1Mul_{ff_{iz_q/z_q}} + 3Exp_{G_1/z_q} + 1Exp_{ff_{iG_r/z_q}}$
Decrypt	$2coup + 1Div_{ff_{iG_T/G_T}}$
Somme	$3coup + 1Div_{ff_{iG_T/G_T}} + 3Mul_{ff_{iG_1/G_1}} + 7Exp_{ff_{iG_1/z_q}} + 2Exp_{ff_{iG_T/z_q}}$

Table 1. Complexity of BB1

Phase 2 : A has generated more requests for private keys, with a total of at most $k_s < \bar{k}$. The algorithm B responds as before (ie in phase 1).

Guess : Finally, A outputs a guess (estimate) $b' \in \{0,1\}$. If b = b' then B outputs 1 which means that T= $e(g,g)^{\frac{1}{\propto}}$. Otherwise, it outputs 0 which means that $T \neq e(g,g)^{\frac{1}{\propto}}$.

When the input of type $\bar{k}+2$ is computed from P_{BDHIP} (where $T = e(g,g)^{\frac{1}{\propto}}$) then the opinion of A is identical to its opinion in the real attack and hence A must satisfy : $pr[b=b'] - 1/2 > \varepsilon$. On the other hand, when the input of type $\bar{k}+2$ is computed from R_{BDHIP} (or T is uniform in G_T), which gives $pr[b=b'] - 1/2$. Then with g is uniform in G_1 and T is uniform in G_T, then we have:

$$| Pr\left[g, g^{\propto}, g^{\propto^2}, ...g^{\propto^{\bar{k}}}, \hat{e}(g,g)^{\frac{1}{\propto}} \right] - Pr\left[g, g^{\propto}, g^{\propto^2}, ...g^{\propto^{\bar{k}}}, T \right] \; | \geq | (\frac{1}{2} \pm \varepsilon) - \frac{1}{2} = \varepsilon \; .| \text{ ----------(7)}$$

Efficiency of Proposed new IBE Scheme

Complexity calculation for BB1, BB2 and the new IBE scheme The notations used in Tables 1, 2 and3 mean:

$Exp_{ff_{iG}}$: Multiplication Scalar;

Exp_{ff_i} : Exponentiation in a finite field;

Inv_{ff_i} : Inversion into a finite field;

Mul_{ff_i} : Multiplication in a finite field; Coup: Pairing;

In addition, we have: $Exp_{ffi_{*/**}}$, for example (The same will be said for other operations) means the Exponentiation of a finite field grouped in * / **, the * is the basis of the exponentiation, while ** represents the base of the exponent.

Efficiency Testing

Complexity (BB1-IBE version) -Complexity (New IBE scheme)

$= 3coup + 1Div_{ff_{iG_T/G_T}} + 3Mul_{ff_{iG_1/G_1}} + 7Exp_{ff_{iG_1/z_q}} + 2Exp_{ff_{iG_T/z_q}}$ -

$2coup + 1Div_{ff_{iG_T/G_T}} + 2Mul_{ff_{iz_q/z_q}} + 1Mul_{ff_{iG_T/G_T}} + 3Exp_{ff_{iG_1/z_q}} + 3Exp_{ff_{iG_T/z_q}} + 1Inv_{ff_{iz_q/z_q}} =$

$1coup + 4Exp_{ff_{iG_1/z_q}} + 3Mul_{ff_{iG_1/G_1}} - 1Inv_{ff_{iz_q/z_q}} - 2Mul_{ff_{iz_q/z_q}} - 1Mul_{ff_{iG_T/G_T}} - 1Exp_{ff_{iG_T/z_q}} \gg 0$

	BB2
Params	$2Exp_{ff_{iG_1/z_q}} + 1coup$
Extract	$1Mul_{ff_{iz_q/z_q}} + 1Inv_{ff_{iz_q/z_q}} + 1Exp_{ff_{iG_1/z_q}}$
Encrypt	$1Mul_{ff_{iz_q/z_q}} + 3Exp_{ff_{iG_1/z_q}} + 1Exp_{ff_{iG_r/z_q}} + 1Mul_{ff_{iG_1/G_1}}$
Decrypt	$1coup + 1Div_{ff_{iG_T/G_T}} + 1Mul_{ff_{iG_1/G_1}} + 1Exp_{ff_{iG_1/z_q}}$
Sum	$2coup + 1Div_{ff_{iG_T/G_T}} + 2Mul_{ff_{iG_1/G_1}} + 7Exp_{ff_{iG_1/z_q}} + 1Inv_{ff_{iz_q/z_q}} + 2Mul_{ff_{iG_1/z_q}}$

Table 2 Complexity of BB2

	New IBE Schema
Params	$1Exp_{ff_{iG_1/z_q}} + 1coup + 1Exp_{ff_{iG_T/z_q}}$
Extract	$1Exp_{ff_{iG_1/z_q}} + 2Mul_{ff_{iz_q/z_q}} + 1Inv_{ff_{iz_q/z_q}}$
Encrypt	$1Mul_{ff_{iG_T/G_T}} + 2Exp_{G_T/z_q} + 1Exp_{ff_{iG_1/z_q}}$
Decrypt	$1coup + 1Div_{ff_{iG_T/G_T}} + 1Exp_{ff_{iG_1/z_q}}$
Sum	$2coup + 1Div_{ff_{iG_T/G_T}} + 2Mul_{ff_{iz_q/z_q}} + 1Mul_{ff_{iG_T/G_T}} + 3Exp_{ff_{iG_1/z_q}} + 3Exp_{ff_{iG_T/z_q}} + 1Inv_{ff_{iz_q/z_q}}$

Table 3. Complexity of the new IBE scheme

And :

Complexity (BB2) - Complexity (New IBE scheme)

$$= 2coup + 1Div_{ff_{iG_T/G_T}} + 2Mul_{ff_{iG_1/G_1}} + 7Exp_{ff_{iG_1/z_q}} + 1Inv_{ff_{iz_q/z_q}} + 2Mul_{ff_{iG_1/z_q}} -$$

$$2coup + 1Div_{ff_{iG_T/G_T}} + 2Mul_{ff_{iz_q/z_q}} + 1Mul_{ff_{iG_T/G_T}} + 3Exp_{ff_{iG_1/z_q}} + 3Exp_{ff_{iG_T/z_q}} + 1Inv_{ff_{iz_q/z_q}} =$$

$$4Exp_{ff_{iG_1/z_q}} + 1Mul_{ff_{iG_1/G_1}} + 2Mul_{ff_{iG_1/z_q}} - 2Mul_{ff_{iz_q/z_q}} - 2Exp_{ff_{iG_T/z_q}} \gg 0$$

6 References

[1] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology - Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 196 (1985), 4753.

[2] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology CRYPTO 2001, Lecture Notes in Computer Science, 2139 (2001), 213229. Full version: SIAM Journal on Computing, 32 (2003), 586615.

[3] K. Paterson and G. Price, A comparison between traditional public key infrastructures and identity-based cryptography, Information Security Technical Report, 8(3) (2003), 5772.

[4] W. Mao. Modern Cryptography theory and practice. Prentice Hall, 2004.

[5] A. Joux. A one round protocol for tripartite Diffie- Hellman. In W. Bosma, editor, Algorithmic Number Theory, IV-Symposium (ANTS IV), LNCS 1838, pages 385394. Springer-Verlag,2000.

[6] A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to a finite field. In IEEE Trans. Info. Theory, number 39, pages 16361646, 1983.

[7] L. Adleman and M. Huang, Function field sieve methods for discrete logarithms over finite fields, Information and Computation, 151 (1999), 516.

[8] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystem based on pairing. In Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000.

[9] O. Ahmadi, D. Hankerson and A. Menezes, Soft- ware implementation of arithmetic in F3m, International Workshop on Arithmetic of Finite Fields (WAIFI 2007), Lecture Notes in Computer Science 4547 (2007), 85102.

[10] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, 1999.

[11] A. Atkin and F. Morain, Elliptic curves and primality proving, Mathematics of Computation, 61 (1993), 2968.

[12] R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has sub exponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, Journal of Cryptology, 11 (1998) 141145.

[13] P. Barreto, S. Galbraith, C. O hEigeartaigh, and M. Scott, Efficient pairing computation on super singular abelian varieties, Designs, Codes and Cryptography, 42 (2007), 239271.

[14] P. Barreto, H. Kim, B. Lynn and M. Scott, Efficient algorithms for pairing-based cryptosystems, Advances in Cryptology CRYPTO 2002, Lecture Notes in Computer Science, 2442 (2002), 354368.

[15] P. Barreto, B. Lynn and M. Scott, Efficient implementation of pairing-based cryptosystems, Journal of Cryptology, 17 (2004), 321334.

[16] P. Barreto and M. Naehrig, Pairing-friendly elliptic curves of prime order, Selected Areas in Cryptography SAC 2005, Lecture Notes in Computer Science, 3897 (2006), 319331.

[17] B. den Boer, Diffie-Hellman is as strong as discrete log for certain primes, Advances in Cryptology CRYPTO 88, Lecture Notes in Computer Science, 403 (1996), 530539.

[18] A. Boldyreva, Efficient threshold signatures, multi signatures and blind signatures based on the gap-Diffie- Hellman-group signature scheme, Public Key Cryptography PKC 2003, Lecture Notes in Computer Science, 2567 (2003), 3146.

[19] D. Boneh, X. Boyen and H. Shacham, Short group signatures, Advances in Cryptology CRYPTO 2004, Lecture Notes in Computer Science, 3152 (2004), 4155.

[20] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, Public key encryption with keyword search, Advances in Cryptology EUROCRYPT 2004, Lecture Notes in Computer Science, 3027 (2004), 506522.

[21] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology CRYPTO 2001, Lecture Notes in Computer Science, 2139 (2001), 213229. Full version: SIAM Journal on Computing, 32 (2003), 586615.

[22] D. Boneh, C. Gentry, H. Shacham and B. Lynn, Aggregate and verifiably encrypted signatures from bi- linear maps, Advances in Cryptology EUROCRYPT 2004, Lecture Notes in Computer Science, 2656 (2003), 416432.

[23] D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing, Advances in Cryptology ASI- ACRYPT 2001, Lecture Notes in Computer Science, 2248 (2001), 514532. Full version: Journal of Cryptology, 17 (2004), 297319.

[24] M. Young, The Technical Writers Handbook. Mill Val- ley, CA: University Science, 1989.