Fully Secure Anonymous HIBE with Short Ciphertexts

Angelo De Caro Vincenzo Iovino*
Giuseppe Persiano

Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84084 Fisciano (SA), Italy.
{decaro,iovino,giuper}@dia.unisa.it

Thursday 27th May, 2010

Abstract

In [LW10], Lewko and Waters presented a fully secure HIBE with short ciphertexts. In this paper we show how to modify their construction to achieve anonymity. We prove the security of our scheme under static (and generically secure) assumptions formulated in composite order groups (of four primes).

1 Introduction

Identity-Based Encryption (IBE) was introduced by [Sha85] to simplify the public-key infrastructure. An IBE is a public-key encryption scheme in which the public-key can be set to any string interpreted as one's identity. A central authority that holds the master secret key can produce a secret key corresponding to a given identity. Anyone can then encrypt messages using the identity, and only the owner of the corresponding secret key can decrypt the messages. First realizations of IBE are due to [BF03] which makes use of bilinear groups and to [Coc01] which uses quadratic residues. Later, [HL02] introduced the more general concept of Hierarchical Identity-Based Encryption (HIBE) issuing a partial solution to it. An HIBE system is an IBE that allows delegation of the keys in a hierarchical structure. To the top of the structure there is the central authority that holds the master secret key, then several sub-authorities (or individual users) that hold delegated keys which can be used to decrypt only the messages addressed to the organization which the sub-authority belongs. Following these works, it followed interest in Anonymous IBE, where the ciphertext does not leak the identity of the recipient. Such systems enjoy a very useful privacy mechanism of privacy and can be used to make search over encrypted data. Interpreting the

*Work done while visiting the Department of Computer Science of The Johns Hopkins University.

identities as keywords, Anonymous IBE allows the encryptor to make the document searchable by keywords, where the capabilities to search on particular keywords are delegated by a central authority. Anonymous IBE can be used to build Public-key Encryption with Keyword Search [BDOP04]. As noticed by [Boy03], the first solution to Anonymous IBE was implicit in the paper of [BF03] though the authors did not state it explicitly. The drawback of the IBE of [BF03] is that its security proof uses the random oracle model. [CHK03] introduced a weaker notion of security called selective-ID, where the attacker choose the identity to attack before it receives the public parameters. In this model [BW06] described an Anonymous Hierarchical Identity-Based Encryption system in the standard model. The first efficient IBE system with full security (non selective-ID) in the standard model was described by [Wat05]. [GH09] described a fully secure HIBE system, although this system is based on a complicated assumption and security proof. [BBG05] constructed an HIBE system with short ciphertexts in the selective-ID model. [Wat09] introduced a proof methodology called Dual System Encryption to prove the full-security of (H)IBE systems. His construction of HIBE is based on simple and established Decision Linear assumption. Recently, [LW10] use the previous methodology to construct the first fully secure HIBE system with short ciphertexts improving the previous result of [BBG05]. The drawback of the latter construction is that it is inherently non anonymous. [SKOS09] build an Anonymous HIBE but their security proof is in the selective-ID model. We show that with an immediate modification to the HIBE of [LW10], we can achieve the first fully secure Anonymous HIBE with short ciphertexts. Recently [LOS$^+$10] built a fully-secure hierarchical predicate encryption system which has as special case Anonymous HIBE, but it has non-constant size ciphertexts and keys are larger than in our construction resulting in a less efficient scheme when instantiated as HIBE. In [CHKP10] the authors constructed the first Anonymous HIBE scheme based on hard lattice problems but the size of a ciphertext depends on the depth of the hierarchy.

2 Model and security notions

2.1 Hierarchical Identity Based Encryption

A Hierarchical Identity Based Encryption scheme (henceforth abbreviated in HIBE) over an alphabet Σ is a tuple of five efficient and probabilistic algorithms: $(\mathsf{Setup}, \mathsf{Encrypt}, \mathsf{KeyGen}, \mathsf{Decrypt}, \mathsf{Delegate})$.

$\mathsf{Setup}(1^\lambda, 1^\ell)$: takes as input security parameter λ and maximum depth of an identity vector ℓ and outputs public parameters Pk and master secret key Msk.

$\mathsf{KeyGen}(\mathsf{Msk}, \mathsf{ID} = (\mathsf{ID}_1, \ldots, \mathsf{ID}_j))$: takes as input master secret key Msk, identity vector $ID \in \Sigma^j$ with $j \leq \ell$ and outputs a private key $\mathsf{Sk}_{\mathsf{ID}}$.

$\mathsf{Delegate}(\mathsf{Pk}, \mathsf{ID}, \mathsf{Sk}_{\mathsf{ID}}, \mathsf{ID}_{j+1})$: takes as input public parameters Pk, secret key for identity vector $\mathsf{ID} = (\mathsf{ID}_1, \ldots, \mathsf{ID}_j)$ of depth $j < \ell$, $\mathsf{ID}_{j+1} \in \Sigma$ and outputs a secret key for the depth $j+1$ identity vector $(\mathsf{ID}_1, \ldots, \mathsf{ID}_j, \mathsf{ID}_{j+1})$.

$\mathsf{Encrypt}(\mathsf{Pk}, M, \mathsf{ID})$: takes as input public parameters Pk, message M and identity vector ID and outputs a ciphertext Ct.

$\mathsf{Decrypt}(\mathsf{Pk}, \mathsf{Ct}, \mathsf{Sk})$: takes as input public parameters Pk, ciphertext Ct and secret key Sk and outputs the message M. We make the following obvious consistency requirement. Suppose ciphertext Ct is obtained by running the $\mathsf{Encrypt}$ algorithm on public parameters Pk, message M and identity ID and that Sk is a secret key identity ID obtained through a sequence of KeyGen and $\mathsf{Delegate}$ calls using the same public parameters Pk. Then $\mathsf{Decrypt}$ returns M except with negligible probability.

2.2 Security definition

We give complete form of the security definition following [SW08]. Our security definition captures semantic security and ciphertext anonymity by means of the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

Setup. The challenger $\mathcal{C}$ runs the Setup algorithm to generate public parameters Pk which it gives to the adversary $\mathcal{A}$. We let S denote the set of private keys that the challenger has created but not yet given to the adversary. At this point, $S = \emptyset$.

Phase 1**.** $\mathcal{A}$ makes Create, Delegate, and Reveal key queries. To make a Create query, $\mathcal{A}$ specifies an identity vector ID of depth j. In response, the $\mathcal{C}$ creates a key for this vector by calling the key generation algorithm, and places this key in the set S. It only gives $\mathcal{A}$ a reference to this key, not the key itself. To make a Delegate query, $\mathcal{A}$ specifies a key $\mathsf{Sk}_{\mathsf{ID}}$ in the set S and $\mathsf{ID}_{j+1} \in \Sigma$. In response, the $\mathcal{C}$ appends ID_{j+1} to ID and makes a key for this new identity by running the delegation algorithm on $\mathsf{ID}, \mathsf{Sk}_{\mathsf{ID}}$ and ID_{j+1}. It adds this key to the set S and again gives $\mathcal{A}$ only a reference to it, not the actual key. To make a Reveal query, $\mathcal{A}$ specifies an element of the set S. $\mathcal{C}$ gives this key to $\mathcal{A}$ and removes it from the set S. We note that $\mathcal{A}$ needs no longer make any delegation queries for this key because it can run delegation algorithm on the revealed key for itself.

Challenge. $\mathcal{A}$ gives to $\mathcal{C}$ two pair message-identity $(M_0, \mathsf{ID}_0^\star)$ and $(M_1, \mathsf{ID}_1^\star)$. The identity vector must satisfy the property that no revealed identity in Phase 1 was a prefix of either $\mathsf{ID}_0^\star$ or $\mathsf{ID}_1^\star$. $\mathcal{A}$ chooses random $\beta \in \{0,1\}$ and encrypts M_β under $\mathsf{ID}_\beta^\star$. $\mathcal{C}$ sends the ciphertext to the adversary.

Phase 2**.** This is the same as Phase 1 with the added restriction that any revealed identity vector must not be a prefix of either $\mathsf{ID}_0^\star$ or $\mathsf{ID}_1^\star$.

Guess. The adversary must output a guess β' for β. The advantage of an adversary $\mathcal{A}$ is defined to be $\mathrm{Prob}[\beta' = \beta] - \frac{1}{2}$.

Definition 2.1 *An Anonymous Hierarchical Identity Based Encryption scheme is secure if all polynomial time adversaries achieve at most a negligible (in λ) advantage in the previous security game.*

References

[BBG05] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 440–456, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany.

[BDOP04] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 506–522, Interlaken, Switzerland, May 2–6, 2004. Springer-Verlag, Berlin, Germany.

[BF03] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[Boy03] Xavier Boyen. Multipurpose identity-based signcryption (a swiss army knife for identity-based cryptography). In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 383–399, Santa Barbara, CA, USA, August 17–21, 2003. Springer-Verlag, Berlin, Germany.

[BW06] Xavier Boyen and Brent Waters. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 290–307, Santa Barbara, CA, USA, August 20–24, 2006. Springer-Verlag, Berlin, Germany.

[CHK03] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 255–271, Warsaw, Poland, May 4–8, 2003. Springer-Verlag, Berlin, Germany.

[CHKP10] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, Nice, France, May 10 –June 3, 2010. Springer-Verlag, Berlin, Germany. To appear.

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363, Cirencester, UK, December 17–19, 2001. Springer-Verlag, Berlin, Germany.

[GH09] Craig Gentry and Shai Halevi. Hierarchical identity based encryption with polynomially many levels. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 437–456, San Francisco, CA, USA, 2009. Springer-Verlag, Berlin, Germany.

[HL02] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481, Amsterdam, The Netherlands, April 28 – May 2, 2002. Springer-Verlag, Berlin, Germany.

[LOS+10] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, 2010. http://eprint.iacr.org/2010/110.pdf, Eurocrypt 2010 to appear.

[LW10] Allison B. Lewko and Brent Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In Daniele Micciancio, editor, *TCC 2010: 7th Theory of Cryptography Conference*, volume 5978 of *Lecture Notes in Computer Science*, pages 455–479, Zurich, Switzerland, February 9–11, 2010. Springer-Verlag, Berlin, Germany.

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53, Santa Barbara, CA, USA, August 19–23, 1985. Springer-Verlag, Berlin, Germany.

[SKOS09] Jae Hong Seo, Tetsutaro Kobayashi, Miyako Ohkubo, and Koutarou Suzuki. Anonymous hierarchical identity-based encryption with constant size ciphertexts. In *Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 215–234. Springer, 2009.

[SW08] Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Automata, Languages and Programming: 35rd International Colloquium*, volume 5126 of *Lecture Notes in Computer Science*, pages 560–578, Reykjavik, Iceland, July 7–11, 2008. Springer-Verlag, Berlin, Germany.

[Wat05] Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany.

[Wat09] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636, Santa Barbara, CA, USA, August 16–20, 2009. Springer-Verlag, Berlin, Germany.