Identity-Based Decryption

Daniel R. L. Brown*

May 30, 2011

Abstract

Identity-based decryption is an alternative to identity-based encryption, in which Alice encrypts a symmetric key for Bob under a trusted authority's public key. Alice sends Bob the resulting ciphertext, which Bob can send to the trusted authority. The trusted authority provides Bob the symmetric key only upon verifying Bob's identity.

1 Identity-Based Encryption

Shamir introduced [7] the notion of identity-based encryption (IBE). In contrast to public-key encryption (PKE), a user of IBE does not have a distinct public key. Rather, the user's identity serves the role of public key. The user's private key is created by some trusted authority. Boneh and Franklin proposed a practical identity-based encryption scheme [3, 4].

Some of the advantages of identity-based encryption over public-key encryption are:

Less initialization: Alice can encrypt messages to Bob even if Bob does not yet have a private key. So, unlike in PKE, Bob does not have to be initialized into the system, that is, he does not already need to have a public key. This is because, upon receipt of such an IBE ciphertext from Alice, Bob can, if he does not already have the private key needed for decryption, obtain his private key from the trusted authority. Also, with a conventional PKE, Bob has only a future, not an immediate, incentive to set up a public key, but in IBE, Bob's incentive is immediate: to be able read Alice's ciphertext.

Less intercommunication: Bob's public key does not need to be communicated to Alice. Consequently there is less intercommunication: Bob does not need to send his public key to Alice nor does Alice need to look up Bob's public key in a directory, whereas in PKE, Alice would typically obtain Bob's public key by one of these two methods.

More customizability: Alice can select and add auxiliary information to Bob's identity in IBE, such as a date allowed for decryption, or some other condition that Bob must satisfy in order to obtain his private key from the authority.

Potentially Less Computational Overhead in Encryption: When, as is often the case, PKE relies on a public-key infrastructure (PKI) to authenticate public keys, it will be the case that Alice can only be sure that a public key actually belongs to Bob by verifying a certificate.

*Certicom Research

If Alice does not already trust the certification authority (CA) who signed the public key in Bob's certificate, then validation of Bob's certificate may involve further validation of other chaining up to the public key of an anchor CA that Alice trusts. So, it is possible that Alice may need to verify many signatures in a chain of certificates before she can encrypt a message to Bob.[1]

Advantages of PKE over IBE may include that IBE has key escrow whereas PKE does not, at least, does not as much. Key escrow is the capability of the trusted authority to decipher Alice's ciphertexts to Bob. By contrast, in PKE, if Alice can establish trust in Bob's public key, then no key escrow is known. If Alice relies on a certification authority (CA) to trust Bob's public key, then it could be possible for a malicious entity to fake Bob's public key completely, in which case the CA has some limited key escrow power.[2] But if the CA honestly issues the certificate to Bob and the CA becomes malicious later, then it has no known way to learn Bob's private key.

Key escrow can sometimes be viewed as an advantage. If Bob ever loses his private key, then he will be unable to decipher ciphertexts. Effectively, some encrypted data may be lost indefinitely. Key escrow provides a convenient mechanism for backing up encryption keys in case of emergency.

2 Identity-Based Decryption

Identity-based decryption (IBD) is an alternative to identity-based encryption (IBE). An IBD user Alice can encrypt a message m to Bob, even if Bob does not have a private key. To do this, Alice does the following.

1. She chooses a symmetric key k.
2. She computes a symmetric ciphertext $C_1 = E_k(M)$, using some symmetric encryption algorithm, such as the Advanced Encryption Standard (AES) in the Ciphertext Block Chaining (CBC) mode.
3. She computes a public-key ciphertext $C_2 = P_T(k, B)$ where: T is the public key of the trusted authority; B is Bob's identity (perhaps appended with some auxiliary information selected by Alice); and P is a public-key encryption algorithm, such as ECIES or RSA-OAEP.
4. She sends C_1 and C_2 to Bob, possibly with some non-encrypted instructions I.

If Bob receives (I, C_1, C_2) from Alice, then Bob can read the instructions I. Bob then knows to do the following.

1. He forwards C_2 to the trusted authority.
2. He proves his identity to the trusted authority.
3. He receives the value k from the trusted authority .

[1] On the other hand, in IBE, the recipient may not have any pre-existing trust in Alice's chosen trusted authority. In that case, Bob may need to take extra steps to establish trust in Alice's trusted authority. So, effectively IBE transfers some of Alice's PKI workload to Bob.

[2] To address this possibility, Alice may wish to exercise caution in using a certified public key (where caution could take the form of not revealing anything too sensitive) until she can somehow establish more trust that the public key belongs to Bob, such as by some out of band communication from Bob.

4. He uses k to compute $m = D_k(C_1)$.

To ensure that nobody other than Bob or Alice or the trusted authority learns k, Bob should contact the trusted authority using a secure channel, such as that provided by Transport Layer Security (TLS and https), or by Bob public-key encrypting to the trusted authority a second symmetric key which the trusted authority can use to encrypt Alice's symmetric key back to Bob .

The following optional features may be convenient for some users:

- The unencrypted instructions to Bob could include all or part of the identity information B, which may allow Bob to recognize if he has mistakenly received the message, or if any additional credentials are needed to decrypt the ciphertext.

- In subsequent correspondence between Alice and Bob, all messages can be encrypted under k, without further contact with the trusted authority.

- Alice could send C_2 in the form of a clickable link, which takes Bob to the trusted authority's web site, which could be a TLS-secure https link. Based on decrypting the contents of C_2, the web site delivers to Bob an applet. The applet somehow authenticates Bob, perhaps sending some information back to the server to do this. Once Bob is authenticated, the applet will have access to the symmetric key k. Bob then pastes the value of C_1 into the applet, which decrypts and it display m to Bob. (The applet will have to be trusted not to forward m to the server.)

- Ciphertext C_1 could be omitted. Instead of the value k serving as a public key, it could serve as the message itself. In other words, put $C_2 = P_T(m, B)$. In this case, once Bob establishes the secure channel to the trusted authority, he does no cryptographic operations because he receives m back from the trusted authority.

- As Bob authenticates himself to the trusted authority, he can also make a conventional public-key certificate request, or even a request for an IBE private key. Then, future correspondence between Bob and others can be conducted with a conventional PKI, or IBE, rather than IBD.

- Alice may send the encryption of a message m to multiple recipients using the same key k to obtain a ciphertext C_1. The key k is encrypted once for each recipient, obtain one version of C_2 per recipient. Such key wrapping is already allowed in some email encryption standards such as S/MIME.

- Rather than encrypting the identifying information B in C_2, or at least all of B, the value B, or part of the value B, could instead be used as an extra input to the encryption function. For example, ECIES allows other inputs to be included into the key derivation function. The trusted authority would still need to have these values in order to decrypt C_2. The trusted authority may already have such information. Bob may already have these values and would be able to send them to the trusted authority. Or, Alice may send them to Bob, who then forwards them to the trusted authority.

- Alice could also authenticate herself to the trusted authority, and the trusted authority could indicate this to Bob. This would leverage the trusted authority to provide a functionality similar to authenticated encryption.

3 Advantages of Identity-Based Decryption

Identity-based decryption has most of the advantages (and disadvantages) noted in §1 that IBE has over conventional public-key encryption: less initialization, less intercommunication, more customizability, and less computational overhead for the sender (and key escrow).

Some distinctions between identity-based encryption (as Shamir defined and Boneh and Franklin constructed) and identity-based decryption (as defined above) are:

1. In IBE, Bob has a private key, which can be used to decrypt ciphertexts from parties other than Alice. Bob need only contact the trusted authority once for each identity string. This may be viewed as advantage of IBE over IBD.[3]

2. Identity-based decryption seems to be realizable using any secure public-key encryption scheme, such as RSA-OAEP or ECIES, whereas IBE seems to require more specialized techniques, such as pairings. This may be viewed as an advantage of IBD over IBE.

3. In IBD, Bob generally does public-key operations to establish a secure channel to the trusted authority[4], but otherwise only does symmetric key operations; whereas, in IBE, Bob generally does some operations that are essentially equivalent to public-key operations.

4 Previous Work

Boneh, Ding, Tsudik and Wong [2] discuss a system where an authority helps provide decryption. Every user has a different public key, so it is not identity-based. Ding and Tsudik [5] discuss an extension of [2] which is identity-based. Their scheme is specific to RSA.

Baek and Zheng [1] discuss identity-based threshold decryption. Their scheme uses pairings, and may be closer to a variation of IBE than to IBD in the sense of this paper.

Various centralized email systems may provide users with symmetric or public keys with which users can encrypt messages to each other. Many of these systems may be fairly closed in the sense of distributing the keys through an already available out-of-band centralized distribution network. Many of these systems may also employ a centralized directory. It is unknown to the author if any of these systems employ the exact mechanism of IBD, or rather, provide all the security features of identity-based decryption.

After making this work public, the author was informed of very similar work by Khurana and Basney [6], which focussed on the case of RSA.

5 Further Work

A thorough comparison of the benefits of IBE versus IBD may be worthwhile.

A security analysis of IBD may be worthwhile. In particular, if the public-key encryption used in IBD is a secure public-key encryption, and the channel between the ciphertext recipient and the

[3] If Alice wants to select different auxiliary identity information for every message, then Bob will need to contact the IBE trusted authority multiple times, even if he only receives ciphertexts from Alice and nobody else. In this case, the advantage above of IBE over IBD does not apply.

[4] If Bob and the trusted authority have some previous trust relationship, such as a resumable TLS session, then perhaps the public-key operation can be avoided.

trusted authority is secure, then it would appear plausible that the IBD scheme in this paper is at least as secure as would be expected for IBE. Perhaps such an appearance can be formalized and proved using the formal notions of security for PKE such as IND-CCA2 and formal notions of security for IBE.

Acknowledgments

I thank Rob Gallant for practical suggestions, such as the use of an applet, Greg Zaverucha for several of the optional features and editorial comments, Alfred Menezes for technical and editorial comments, and Nevine Ebeid, Koray Karabina and Matt Campagna for editorial comments.

I thank Aniket Kate for informing me of [6].

References

[1] J. Baek and Y. Zheng. Identity-based threshold decryption. In F. Bao, R. Dend, and J. Zhou, editors, *Public Key Cryptography — PKC 2004*, number 2947 in LNCS, pages 262–276. IACR, Springer, Mar. 2004. http://eprint.iacr.org/2003/164.

[2] D. Boneh, X. Ding, G. Tsudik, and M. Wong. A method for fast revocation of public key certificates and security capabilities. In *Proceedings of the 10th USENIX Security Symposium*, pages 297–308, 2001. http://crypto.stanford.edu/~dabo/papers/sem.pdf.

[3] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *Advance in Cryptology — Crytpo 2001*, number 2139 in LNCS, pages 213–229. IACR, Springer, Aug. 2001.

[4] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. of Computing*, 32(3):586–615, 2003.

[5] X. Ding and G. Tsudik. Simple identity-based cryptography with mediated RSA. In M. Joye, editor, *Topics in Cryptology — CR-RSA 2003*, number 2612 in LNCS, pages 193–210. Springer, Apr. 2003.

[6] H. Khurana and J. Basney. On the risks of IBE. In *Fifth International Workshop on Applied PKC (IWAP'06)*, 2006.

[7] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *Advance in Cryptology: Proceedings of CRYTPO 1984*, number 196 in LNCS, pages 47–53. IACR, Springer, Aug. 1984.