Efficient Identity-Based Encryption Without Random Oracles

Brent Waters

Group D

Radhika Patwari - 18CS10062
Proteet Paul - 18CS10065
Aayush Prasad - 18CS30002
Aayushi Vidyanta - 18CS30003
Adireddi Chandrika Lavanya - 18CS30004

Outline

- Introduction
- Motivation
- Complexity Assumptions
    - Decisional Bilinear Diffie-Hellman (BDH) Assumption
    - Computational Diffie-Hellman (CDH) Assumption
- Construction
    - Setup
    - Key Generation
    - Encryption
    - Decryption
    - Efficiency
    - Similarity to the Boneh-Boyen IBE Scheme
- Security
- Applications
- Conclusion

Introduction

Identity-Based Encryption (IBE) allows for a party to encrypt a message using the recipient's identity as a public key. The ability to use identities as public keys avoids the need to distribute public key certificates. This can be very useful in applications such as email where the recipient is often offline and unable to present a public-key certificate while the sender encrypts a message.

Brent Waters proposed the first efficient IBE that is fully secure without random oracles. The proof of the scheme makes use of an algebraic method first used by Boneh and Boyen and the security of the scheme reduces to the decisional Bilinear Diffie-Hellman(BDH) assumption.

Motivation

Boneh and Boyen had previously described a scheme that was proved to be fully secure without random oracles; the possibility of such a scheme was to that point an open problem. However, their scheme is too inefficient to be of practical use.

Hence, this paper presents the **first efficient** Identity-Based Encryption scheme that is **fully secure without random oracles**.

Complexity Assumptions

Let G, G_1 be s groups of prime order p and g be a generator of G. We say G_1 has an admissible bilinear map, $e : G \times G \rightarrow G_1$, into G_1 if the following two conditions hold:

- The map is bilinear; for all a, b we have $e(g^a , g^b) = e(g, g)^{ab}$
- The map is non-degenerate; we must have that $e(g, g) \neq 1$.

The two complexity assumptions in this IBE scheme are:

1. Decisional Bilinear Diffie-Hellman (BDH) Assumption
2. Computational Diffie-Hellman (DH) Assumption

Decisional BDH Assumption

The challenger chooses a, b, c, z ∈ Z_p at random and then flips a fair binary coin β.

- If β = 1, it outputs the tuple (g, A = g^a , B = g^b , C = g^c , Z = e(g, g)^{abc}).
- Otherwise, if β = 0, the challenger outputs the tuple (g, A = g^a , B = g^b , C = g^c , Z = e(g, g)^z).

The adversary must then output a guess β’ of β.
An adversary, Ɓ, has at least an ε advantage in solving the decisional BDH problem if

$$\left| \Pr\left[\mathcal{B}\left(g, g^a, g^b, g^c, e(g,g)^{abc}\right) = 1\right] - \Pr\left[\mathcal{B}\left(g, g, g^a, g^b, g^c, e(g,g)^z\right) = 1\right] \right| \geq 2\epsilon$$

where the probability is over the randomly chosen a, b, c, z and the random bits consumed by B.

Definition. The decisional (t,ε)-BDH assumption holds if no t-time adversary has at least ε advantage in solving the above game.

Computational DH Assumption

The challenger chooses a, b $\in Z_p$ at random and outputs (g, $A = g^a$, $B = g^b$). The adversary then attempts to output $g^{ab} \in G$.

An adversary, B, has at least an ε advantage if

$$Pr\left[\mathcal{B}\left(g, g^a, g^b\right) = g^{ab}\right] \geq \epsilon$$

where the probability is over the randomly chosen a, b and the random bits consumed by B.

Definition. The computational (t,ε)-DH assumption holds if no t-time adversary has at least ε advantage in solving the above game.

Construction of IDE Scheme

- Let G be a group of prime order, p, for which there exists an efficiently computable bilinear map into G_1 .
- Additionally, let $e : G \times G \rightarrow G_1$ denote the bilinear map and g be the corresponding generator of G. The size of the group is determined by the security parameter.
- Identities will be represented as bitstrings of length n, a separate parameter unrelated to p.
- The identities are bitstrings of arbitrary length and n is the output length of a collision-resistant hash function,

$$H : \{0, 1\}^* \rightarrow \{0, 1\}^n$$

Steps involved in Construction

The steps involved in the process of construction of this efficient Identity-Based Encryption scheme are :

1. Setup
2. Key Generation
3. Encryption
4. Decryption

1. Setup

The system parameters are generated as follows :

- A secret $\alpha \in Z_p$ is chosen at random.
- We choose a random generator, $g \in G$, and set the value $g_1 = g^\alpha$ and choose g_2 randomly in G.
- Additionally, the authority chooses a random value $u' \in G$ and a random n-length vector $U = (u_i)$, whose elements are chosen at random from G.
- The published public parameters are g, g_1, g_2, u' and U.
- The master secret is $(g_2)^\alpha$.

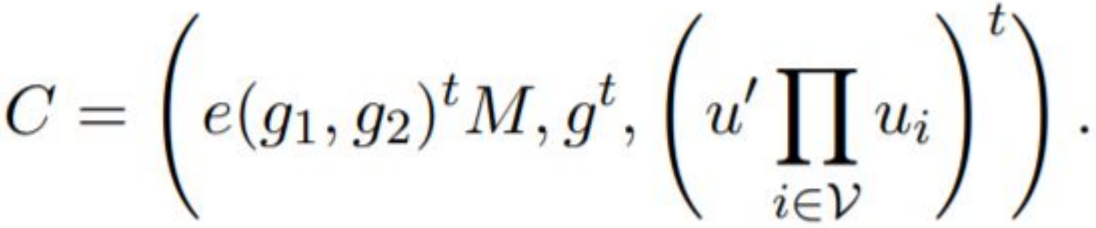
2. Key Generation

- Let v be an n bit string representing an identity such that v_i denote the i^{th} bit of v
- Let V ⊆ {1, . . . , n} be the set of all i for which v_i = 1. (Thus V is the set of indices for which the bitstring v is set to 1)
- A private key for identity v is generated as follows. First, a random r ∈ Z_p is chosen. Then the private key is constructed as:

$$d_v = \left(g_2^{\alpha} \left(u' \prod_{i \in \mathcal{V}} u_i \right)^{r}, g^{r} \right).$$

3. Encryption

- A message M ∈ G_1 is encrypted for an identity v as follows.
- A value t ∈ Z_p is chosen at random.
- The ciphertext is then constructed as



$$C = \left(e(g_1, g_2)^t M, g^t, \left(u' \prod_{i \in \mathcal{V}} u_i \right)^t \right).$$

4. Decryption

- Let ciphertext C = (C_1 , C_2, C_3) be a valid encryption of M under the identity v.
- C can be decrypted by d_v = (d_1 , d_2) as:

$$
\begin{aligned}
C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)} &= \left(e(g_1, g_2)^t M\right) \frac{e\left(g^r, \left(u' \prod_{i \in \mathcal{V}} u_i\right)^t\right)}{e\left(g_2^\alpha \left(u' \prod_{i \in \mathcal{V}} u_i\right)^r, g^t\right)} \\
&= \left(e(g_1, g_2)^t M\right) \frac{e\left(g, \left(u' \prod_{i \in \mathcal{V}} u_i\right)^{rt}\right)}{e(g_1, g_2)^t e\left(\left(u' \prod_{i \in \mathcal{V}} u_i\right)^{rt}, g\right)} = M.
\end{aligned}
$$

Efficiency

Encryption

$$C = \left(e(g_1, g_2)^t M, g^t, \left(u' \prod_{i \in \mathcal{V}} u_i \right)^t \right).$$

Decryption

$$\begin{aligned} C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)} &= \left(e(g_1, g_2)^t M\right) \frac{e\left(g^r, \left(u' \prod_{i \in \mathcal{V}} u_i\right)^t\right)}{e\left(g_2^\alpha \left(u' \prod_{i \in \mathcal{V}} u_i\right)^r, g^t\right)} \\ &= \left(e(g_1, g_2)^t M\right) \frac{e\left(g, \left(u' \prod_{i \in \mathcal{V}} u_i\right)^{rt}\right)}{e(g_1, g_2)^t e\left(\left(u' \prod_{i \in \mathcal{V}} u_i\right)^{rt}, g\right)} = M. \end{aligned}$$

If the value of e(g_1, g_2) is cached, then encryption requires on average n/2 (and at most n) group operations in G, two exponentiations in G, one exponentiation in G_1 and one group operation in G_1

Decryption requires two bilinear map computations, two group operation in G_1 and one inversion in G_1 .

Similarity to Boneh-Boyen’s IBE scheme

This construction is a modification of Boneh-Boyen’s IBE scheme. Here, for an identity v, $u'\Pi_{i\in V}u_i$ is evaluated whereas in their scheme, they evaluate $u'g_1^v$, where v is interpreted as an integer.

Security

The security of this scheme is based on the following theorem

Theorem :

This IBE- scheme is (t, q, ϵ) secure assuming the decisional ($t+O(\epsilon^{-2}\,\ln(\epsilon^{-1})\,\lambda^{-1}\,\ln(\lambda^{-1}))$, $\epsilon/[32(n+1)q]$) BDH assumption holds, where $\lambda = 1/[8(n+1)q]$.

Application 1 - Revocation of Public Keys

- Public key certificates contain a preset expiration date. In an IBE system key expiration can be done by having Alice encrypt an email sent to Bob using the public key: ***bob@hotmail.com*** || ***current-year*** . In doing so Bob can use his private key during the current year only. Once a year, Bob needs to obtain a new private key from the PKG. Hence, we get the effect of annual private key expiration. Note that unlike the existing PKI, Alice does not need to obtain a new certificate from Bob every time Bob refreshes his certificate.
- This approach could potentially be made more granular by encrypting an email for Bob using ***bob@hotmail.com*** || ***current-date*** . This forces Bob to obtain a new private key every day. This might be feasible in a corporate PKI where the PKG is maintained by the corporation.
- With this approach key revocation is quite simple: when Bob leaves the company and his key needs to be revoked, the corporate PKG is instructed to stop issuing private keys for Bob's e-mail address. Alice does not need to communicate with any third party to obtain Bob's daily public key. This approach enables Alice to send messages into the future: Bob will only be able to decrypt the email on the date specified by Alice.

Application 2 - Delegation of Decryption Keys

- Another application for IBE systems is delegation of decryption capabilities.
- We give one example application. In this application, the user Bob plays the role of the private key generator(PKG).
- Bob runs the setup algorithm to generate his own IBE system parameters *params* and his own *master-key*. Here we view *params* as Bob's public key.
- Bob obtains a certificate from a CA for his public key *params*.
- When Alice wishes to send mail to Bob she first obtains Bob's public key *params* from Bob's public key certificate. Note that Bob is the only one who knows his *master-key* and hence there is no key-escrow with this setup.

Example of Delegation : Delegation of a laptop

- Suppose Alice encrypts mail to Bob using the current date as the IBE encryption key (she uses Bob's *params* as the IBE system parameters).
- Since Bob has the *master-key* he can extract the private key corresponding to this IBE encryption key and then decrypt the message.
- Now, suppose Bob goes on a trip for seven days. Normally, Bob would put his private key on his laptop.
- If the laptop is stolen, the private key is compromised.
- When using the IBE system Bob could simply install on his laptop the seven private keys corresponding to the seven days of the trip.
- If the laptop is stolen, only the private keys for those 7 days are compromised.
- The *master-key* is unharmed.

Conclusion

The first efficient and practical Identity based encryption that is secure in the full model without random oracles.

Two interesting open problems remains to be solved:

1. To construct an efficient IBE system that has short public parameters without random oracles.
2. To construct an IBE system with a tight reduction in security.

References

- https://eprint.iacr.org/2004/180.pdf
- https://crypto.stanford.edu/ibe/