No Title Given

1 Introduction

2 Applications for Identity-Based Encryption

In this section, we show several applications of IBE

2.1 Revocation of Public Keys

Public key certificates are valid, an IBE system key expiration can be done by having Alice encrypt e-mail sent to Bob using the public key: “bob@company.com k current-year”.In this way, Bob can only use his private key within the time limit.This approach makes key revocation very simple. And Alice doesn’t need to communicate with any third-party certificate directories to get Bob’s daily public key.In addition, it can be used to manage user credentials, because Alice allows Bob to read messages within a specified date.

2.2 Delegation of Decryption Keys

Here are two examples to illustrate this function. Among them, Bob plays PKG, and Alice wants Bob to send email.
Delegation to a laptop
Suppose Alice wants Bob to send the message and uses the current date as the encryption key.Bob plans to travel for 7 days. When using IBE system, Bob can simply install seven private keys corresponding to the seven days of travel on his laptop.If the notebook is stolen in this area, only the private key of these seven days will be disclosed. The master key is not compromised.
Delegation of duties
Suppose Alice encrypts mail to Bob using the subject line as the IBE encryption key. Bob can decrypt mail using his master-key.Now, let’s say Bob has several assistants, each responsible for a different task.Bob provides each assistant with a private key according to their duties.Each assistant can then decrypt messages for its subject line within its scope of responsibility, but not for other assistants.So IBE can simplify the management of a large number of public key security system.

3 definition

An identity-based encryption scheme E is specified by four randomized algorithms: Setup, Extract, Encrypt, Decrypt.
Setup:takes a security parameter k and returns params (system parameters) and

master-key.
Extract:takes as input params, master-key, and an arbitrary ID$\in \{0,1\}^*$,and returns a private key d.
Encrypt:takes as input params, ID, and $m \in M$. It returns a ciphertext $c \in C$.
Decrypt:takes as input params, $c \in C$, and a private key d. It return $m \in M$. $\forall m \in M$.: Decrypt(params, C, d) = m where c = Encrypt(params, ID, m).
IBE semantic security
definition 2.1. We say that the IBE system E is semantically secure against an adaptive chosen ciphertext attack if for any polynomial time IND-ID-CCA adversary A the function AdvE,A(k) is negligible.As shorthand, we say that E is IND-ID-CCA secure.
Initialization:Challenger generates system ε, and adversary a obtains the public key of the system.
Training: the enemy makes decryption inquiry to the Challenger (multiple times), that is, takes the ciphertext c to the challenger, the Challenger decrypts the panic, and gives the plaintext to the enemy.
Challenge: the opponent outputs two messages m0 and m1 with the same length, and then receives mb ciphertext from the challenger, where the random value b$\in \{0,1\}$.
Guess: the opponent outputs b', if b' = b, then a succeeds.

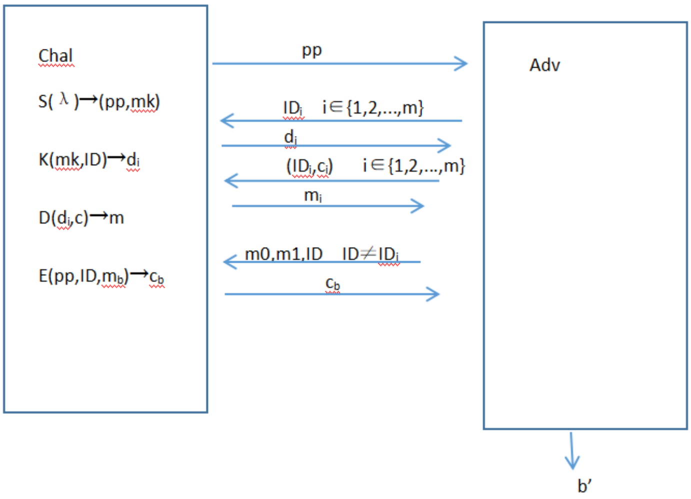

Fig. 1. CCA

Definition 2.2. We say that the IBE system E is semantically secure if for any polynomial time IND-ID-CPA adversary A the function AdvE,A(k) is negligible. As shorthand, we say that E is IND-ID-CPA secure.

Initialization:Challenger generates system ε, and adversary a obtains the public key of the system.
Challenge: the opponent outputs two messages m0 and m1 with the same length, and then receives mb ciphertext from the challenger, where the random value b$\in \{0, 1\}$.
Guess: the opponent outputs b', if b' = b, then a succeeds.

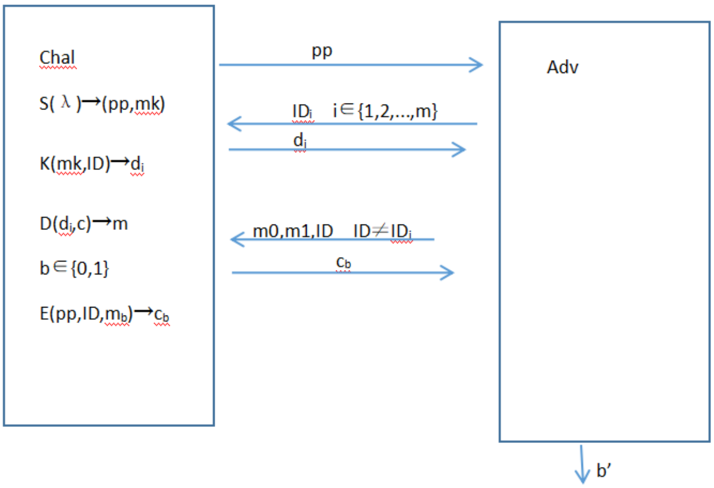

Fig. 2. CPA

4 Bilinear maps and the Bilinear Diffie-Hellman Assumption

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of order q for some large prime q. Our IBE system makes use of a bilinear map$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ between these two groups. The map must satisfy the following properties:
1. Bilinear: We say that a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$is bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all P, Q $\in \mathbb{G}_1$ and all a, b$\in \mathbb{Z}$.
2. Non-degenerate: The map does not send all pairs in $\mathbb{G}_1 X \mathbb{G}_2$ to the identity in$\mathbb{G}_2$. Observe that since $\mathbb{G}_1, \mathbb{G}_2$ are groups of prime order this implies that if P is a generator of $\mathbb{G}_1$ then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.
3. Computable: There is an efficient algorithm to compute$\hat{e}(P, Q)$ for any P, Q $\in \mathbb{G}_1$.
Decision Diffie-Hellman is Easy: The Decision Diffie-Hellman problem (DDH) in $\mathbb{G}_1$ is to distinguish between the distributions $\langle P, aP, bP, abP\rangle$ and $\langle P, aP, bP, cP\rangle$ where a, b, c are random in $\mathbb{Z}_q^*$ and P is random in $\mathbb{G}_1^*$. Joux and Nguyen point out that DDH in $\mathbb{G}_1$ is easy. To see this, observe that given P, aP, bP, cP $\in \mathbb{G}_1^*$ we

have
$c = ab \bmod q \quad \iff \quad \hat{e}(P, cP) = \hat{e}(aP, bP)$

5 IBE

5.1 The Bilinear Diffie-Hellman(BDH) Assumption

The security of Identity-Based Encryption(IBE) is based on the Bilinear Diffie-Hellman(BDH) Problem.

Let $\mathbb{G}_1, \mathbb{G}_2$ be two groups of prime order q. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be an admissible bilinear map and let P be a generator of $\mathbb{G}_1$. The BDH problem in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$ is as follows: Given $\langle P, aP, bP, cP \rangle$ for some $a, b, c \in \mathbb{Z}_q^*$ compute $W = \hat{e}(P, P)^{abc} \in \mathbb{G}_2$. An algorithm A has advantage ϵ in solving BDH in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$ if

$$Pr\left[\mathcal{A}(P, aP, bP, cP) = \hat{e}(P, P)^{abc}\right] \geq \epsilon$$

The BDH hypothesis can be described as:
There is no probabilistic polynomial time algorithm has a nonnegligible advantage in solving BDH problems.

5.2 BasicIdent

BasicIdent is the basic IBE scheme. How it works is shown in the figure below (BasicIdent Model). TA is trust authority and can be viewed as PKG. There are two hashes here, H1 for the hash ID, which is Alice's mailbox number. H2 is the result of a hash bilinear pair. This article uses the RO model, which simulates these two hashes.

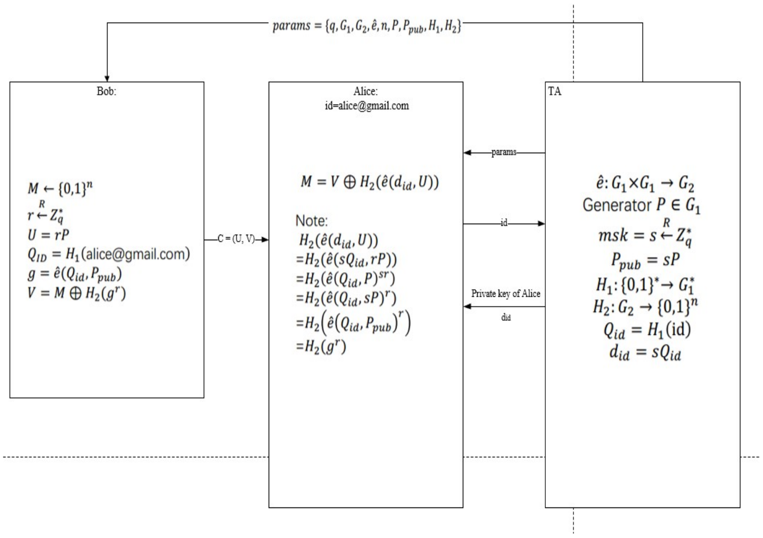
$params = \{q, G_1, G_2, \hat{e}, n, P, P_{pub}, H_1, H_2\}$
Bob:
$M \leftarrow \{0,1\}^n$
$r \overset{R}{\leftarrow} Z_q^*$
$U = rP$
$Q_{ID} = H_1$(alice@gmail.com)
$g = \hat{e}(Q_{id}, P_{pub})$
$V = M \oplus H_2(g^r)$
C = (U, V)
Alice:
id=alice@gmail.com
$M = V \oplus H_2(\hat{e}(d_{id}, U))$
Note:
$H_2(\hat{e}(d_{id}, U))$
$=H_2(\hat{e}(sQ_{id}, rP))$
$=H_2(\hat{e}(Q_{id}, P)^{sr})$
$=H_2(\hat{e}(Q_{id}, sP)^r)$
$=H_2\left(\hat{e}(Q_{id}, P_{pub})^r\right)$
$=H_2(g^r)$
params
id
Private key of Alice
did
TA
$\hat{e}: G_1 \times G_1 \to G_2$
Generator $P \in G_1$
$msk = s \overset{R}{\leftarrow} Z_q^*$
$P_{pub} = sP$
$H_1: \{0,1\}^* \to G_1^*$
$H_2: G_2 \to \{0,1\}^n$
$Q_{id} = H_1$(id)
$d_{id} = sQ_{id}$

Fig. 3. BasicIdent Model

The idea of specification proof is to first convert the above basic ident IBE scheme to a basic pub public key scheme. A relationship between these two advs is negligible. Then, the basicpub public key scheme can be reduced to BDH assumption. The following basicpub is the public key scheme after the specification. There is only one H2. The public key scheme does not need the previous ID, so it is useful to H1.

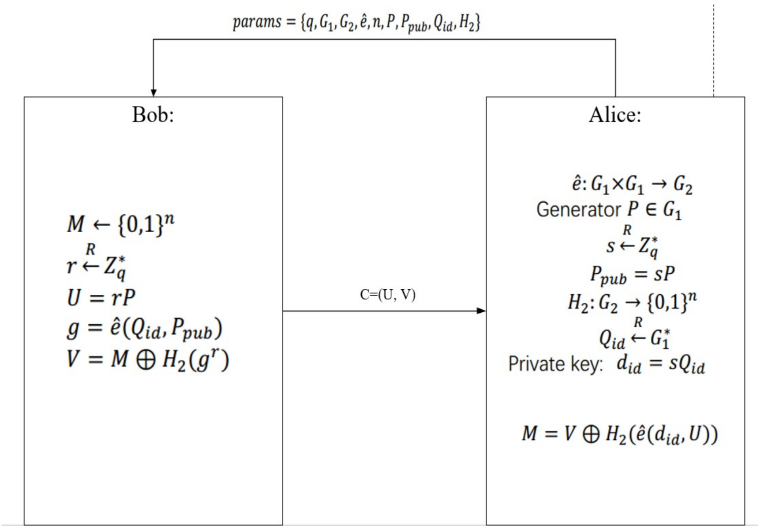
$params = \{q, G_1, G_2, \hat{e}, n, P, P_{pub}, Q_{id}, H_2\}$
Bob:
$M \leftarrow \{0,1\}^n$
$r \overset{R}{\leftarrow} Z_q^*$
$U = rP$
$g = \hat{e}(Q_{id}, P_{pub})$
$V = M \oplus H_2(g^r)$
C=(U, V)
Alice:
$\hat{e}: G_1 \times G_1 \rightarrow G_2$
Generator $P \in G_1$
$s \overset{R}{\leftarrow} Z_q^*$
$P_{pub} = sP$
$H_2: G_2 \rightarrow \{0,1\}^n$
$Q_{id} \overset{R}{\leftarrow} G_1^*$
Private key: $d_{id} = sQ_{id}$
$M = V \oplus H_2(\hat{e}(d_{id}, U))$

Fig. 4. BasicPub Model

5.3 Relaxing the hashing requirements

IBE system uses a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$. Building such hash functions can be difficult. In order to relax the requirement of hashing. So an intermediate set A is introduced. The scheme substitute hashing directly onto $\mathbb{G}_1^*$ into hashing onto $A \subseteq \{0,1\}^*$, and then map A onto $\mathbb{G}_1^*$ through a deterministic encoding function. The encoding function $L : A \rightarrow \mathbb{G}_1^*$ is admissible if it satisfies the following properties:

1. Computable: An efficient deterministic algorithm to compute L(x) for any $x \in A$.
2. l-to-1: $|L^{-1}(y)| = l$ for all $y \in \mathbb{G}_1^*$.
3. Samplable: $\mathcal{L}_S(y)$ is a uniform random element in $L^{-1}(y)$

The modification to FullIdent is to obtain and IND-ID-CCA secure IBE system. The H_1 is replaced by a hash function into some set A. It can be proved that the modified FullIdent is a chosen ciphertext secure IBE.

6 A concrete IBE system using the Weil pairing

The article then use FullIdent to describe IBE system based on the Weil pairing.

The Weil pairing has some properties:

1. Bilinear: For all $P, Q \in \mathbb{G}_1$ and for all $a, b \in \mathbb{Z}$ it satisfy $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-degenerate: If P is a generator of $\mathbb{G}_1$ then $\hat{e}(P, P) \in \mathbb{F}_{p^2}^*$ is a generator of $\mathbb{G}_2^*$
3. Computable: Given $P, Q \in \mathbb{G}_1$ an efficient algorithm to compute $\hat{e}(P, Q) \in \mathbb{G}_2$ exists.

Computational Diffie-Hellman problem (CDH) is hard in the group $\mathbb{G}_1$ and Decisional Diffie-Hellman problem (DDH) is easy in $\mathbb{G}_1$. Later, the author introduced the BDH Parameter Generator into discussion and draw the conclusion that one should not use this BDH parameter generator with primes p that are less than 512-bits long.

6.1 An admissible encoding function: MapToPoint

As the IBE system uses a hash function $H_1 : \{0, 1\}^* \to \mathbb{G}_1^*$. The author presentated an admissible encoding function $MapToPoint$. the MapToPoint work as follows:

1. Compute $x_0 = \left(y_0^2 - 1\right)^{1/3} = \left(y_0^2 - 1\right)^{(2p-1)/3} \in \mathbb{F}_p$
2. Let $Q = (x_0, y_0) \in E(\mathbb{F}_p)$ and set $Q_{\mathrm{lo}} = \ell Q \in \mathbb{G}_1$
3. Output $MapToPoint(y_0) = Q_{ID}$

The admissibility of $MapToPoint$ is proved.

7 Extensions and Observation

The author presented some extensions. The system based on some other curves such as Tate pairings are discussed with the conclusion that encryption and decryption in FullIdent can be made faster by using the Tate pairing on elliptic curves. The application of IBE in an e-mail system storing the CA's private key in PKG is also mentioned. The PKG's master-key can be generated in a distributed fashion. In addition, the performance of the IBE system can be optimized by working in a small subgroup of the curve.

8 Escrow EIGamal encryption

The escrow ability to EIGamal encryption system can be obtained through the Weil pairing. It gives the algorithm under the setup of BDH parameter generator $\mathbb{G}$ and a security parameter $k \in \mathbb{Z}^+$. The system is semantic secure when BDH is hard for groups generated by $\mathcal{G}$.

9 Conclusion

The article introduced the fully functional IBE system. The system is built under in random oracle model with the assumption BDH, which is a natural analogue of the computational Diffie-Hellman problem. The article applied one transformation method from Fujisaki-Okamoto to convert basic BasicIdent scheme into ciphertext secure IBE system in random oracle model as FullIdent. In addition, a concrete IBE system using the Weil pairing and extensions and observations of the scheme are also discussed. To build chosen ciphertext secure identity based systems is currently an open problem.

10 appendix

Wangzhihui Mei has surveyed the basic IBE scheme BasicIdent and the method of relaxing the hashing requirements of FullIdent as well as the example IBE system based on weil pairing. Then Mei watched some extension usage of the introduced IBE system and escrow EIGamal encryption system.