目录

公钥密码体制

基于身份的公钥密码体制

双线性对

计算困难问题

可证明安全性

公钥密码体制

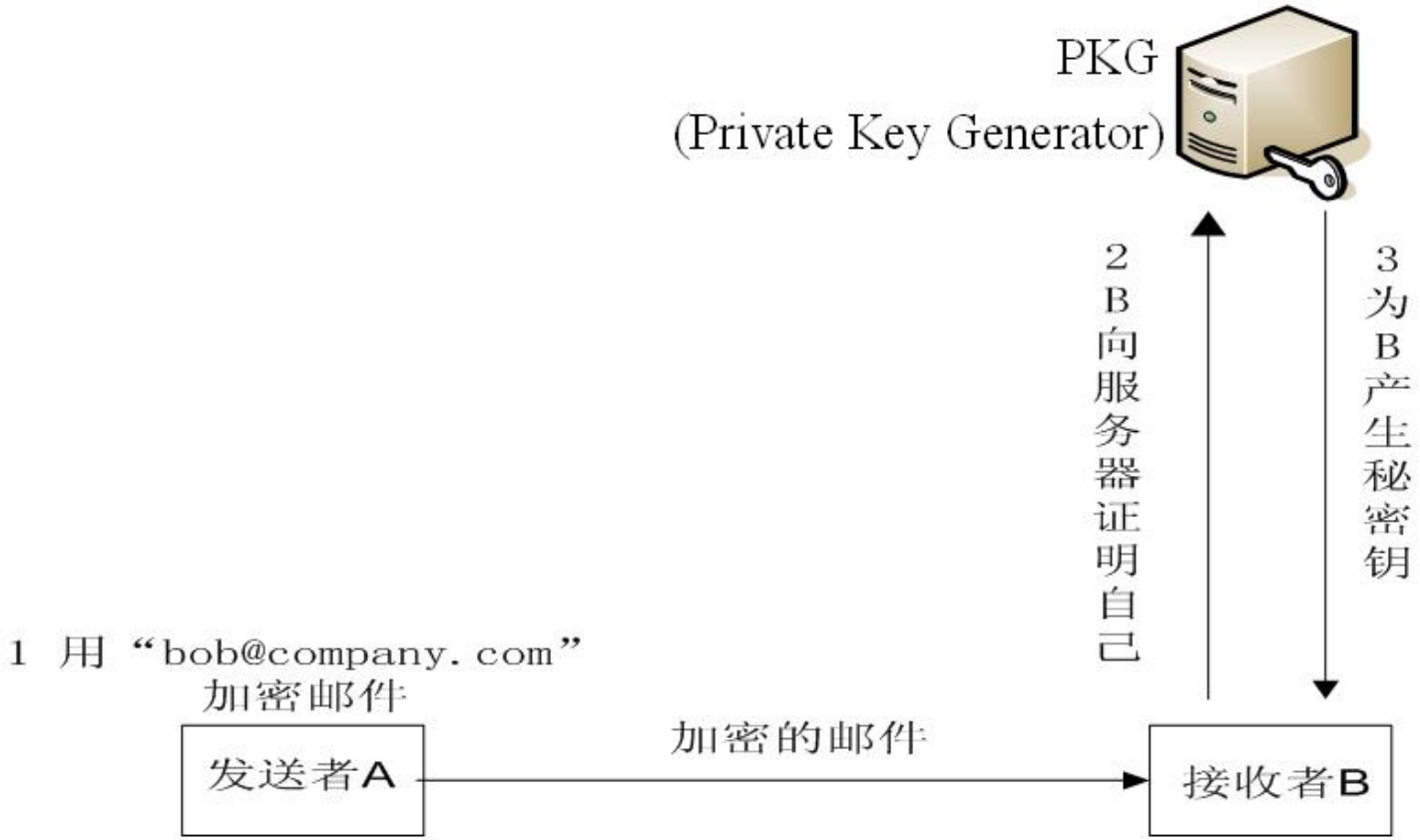
- 公钥密码体制
- CA（Certificate Authority），负责用户公钥证书生命周期的每一个环节：生成、签发、存贮、维护、更新、撤销等
- CA有可能成为系统的瓶颈。

基于身份的公钥密码体制

- 基于身份的公钥密码体制，从根本上改变传统CA公钥体制架构中证书的管理和运作
- 基于身份的公钥体制的思想最早由Shamir于1984年提出，方案中不使用任何证书，直接将用户的身份作为公钥，以此来简化公钥基础设施PKI（Public Key Infrastructure）中基于证书的密钥管理过程

基于身份的加密算法如何工作？

图3: 基于身份的加密方案示例



Identity-Based Encryption

一个基于身份的加密体制(E)由以下四个算法组成：

- 建立（Setup）：由安全参数k生成系统参数*params*和主密钥master-key.
- 提取（Extract）: 由给定公钥（身份）生成秘密钥,即由*params*,master-keys和任意$ID \in \{0,1\}^*$,返回一个秘密钥d.
- 加密（Encrypt）：由输入params, ID, M, 返回密文C.
- 解密（Decrypt）：由输入params, C，d, 返回明文M.

双线性映射

设q是一个大素数，$\mathbb{G}_1$和$\mathbb{G}_2$是两个阶为q的群，$\mathbb{G}_1$到$\mathbb{G}_2$的双线性映射：$\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$，满足如下性质：

1、双线性：如果对任意$P,Q,R\in\mathbb{G}_1$和$a,b\in\mathbb{Z}_q$，$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$或$\hat{e}(P+Q,R)=\hat{e}(P,R)\cdot\hat{e}(Q,R)$成立。

2、非退化性: 映射不把$\mathbb{G}_1\times\mathbb{G}_1$所有的元素对映射到$\mathbb{G}_2$的单位元。由于$\mathbb{G}_1$和$\mathbb{G}_2$都是素数阶的群，即，如果$P$是$\mathbb{G}_1$的单位元，那么$\hat{e}(P,P)$是$\mathbb{G}_2$的单位元。

3、可计算性：任意$P,Q\in\mathbb{G}_1$，存在一个有效算法计算$\hat{e}(P,Q)$。

IBE方案所基于的困难问题之DDH问题

设$\mathbb{G}_1$是一个阶为q的群，$\mathbb{G}_1$中的判定性Diffie-Hellman问题，简称DDH(Decision Diffie-Hellman)问题是指已知P, aP, bP, cP，判定$c = ab \bmod q$ 是否成立，其中P是$\mathbb{G}_1^*$中的随机元素，a, b, c是$\mathbb{Z}_q^*$中的随机数。

由双线性映射的性质可知：

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

因此，可将判定$c = ab \bmod q$是否成立转变为判定$\hat{e}(P, cP) = \hat{e}(aP, bP)$是否成立，所以$\mathbb{G}_1$中的DDH问题是简单的。

IBE方案所基于的困难问题之CDH问题

$\mathbb{G}_1$中的计算性Diffie-Hellman问题，简称CDH问题(Computational Diffie-Hellman)是指已知P, aP, bP，求abP，其中P是$\mathbb{G}_1^*$中的随机元素，a, b是$\mathbb{Z}_q^*$中的随机数。

与$\mathbb{G}_1$中的DDH问题不同，$\mathbb{G}_1$中的CDH问题不因引入双线性映射而解决,因此它仍是困难问题。

MOV规约

$\mathbb{G}_1$中的离散对数问题: 已知$P, Q \in \mathbb{G}_1$,求$a \in \mathbb{Z}_q$,使得$Q = aP$。已知这是一个困难问题。

然而如果记$g = \hat{e}(P, P), h = \hat{e}(P, Q)$，则由$\hat{e}$的双线性可知$h = g^a$，因此，可以将$\mathbb{G}_1$中的离散对数问题归结为$\mathbb{G}_2$ 中的离散对数问题。若$\mathbb{G}_2$中的离散对数问题可解，则$\mathbb{G}_1$中的离散对数问题可解。

MOV规约(也称MOV攻击)是指将攻击$\mathbb{G}_1$中的离散对数问题转化为攻击$\mathbb{G}_2$中的离散对数问题。所以要使$\mathbb{G}_1$中的离散对数问题为困难问题，就必须选择适当参数使$\mathbb{G}_2$中的离散对数问题为困难问题。

Random oracle model

- HASH函数的一个性质：对任一输入，其输出的概率分布与均匀分布在计算上不可区分。
- 改为：对任一输入，其输出是均匀分布的。
- 把HASH函数看作这样一个理想的函数，就称其为Random Oracle。

IBE方案所基于的困难问题之BDH问题和BDH假设

由于$\mathbb{G}_1$中的DDH问题简单，那么就不能用它来构造$\mathbb{G}_1$中的密码体制。IBE体制的安全性是基于CDH问题的一个变形，称之为双线性DH假设。

双线性DH问题，简称BDH(Bilinear Diffie-Hellman)问题，是指给定$(P, aP, bP, cP)(a, b, c \in \mathcal{Z}_q^*)$，计算

$$w = \hat{e}(P, P)^{abc} \in \mathbb{G}_2$$

其中$\hat{e}$是一个双线性映射，P是$\mathbb{G}_1$的生成元，$\mathbb{G}_1, \mathbb{G}_2$是阶为素数$q$的两个群。

IBE方案所基于的困难问题之BDH问题和BDH假设

设算法A用来解决BDH问题，其优势定义为τ，如果

$$Pr \mid A(P, aP, bP, cP) = \hat{e}(P, P)^{abc} \mid \geq \tau$$

目前还没有有效的算法解决BDH问题. 因此，可假设BDH问题是一个困难问题，这就是BDH假设。

选择明文安全的IBE方案

要定义基于身份的密码体制的语义安全，应允许敌手根据自己的选择进行秘密钥询问，即敌手可根据自己的选择询问公钥对应的秘密钥，以此来加强标准定义。

IND游戏（称为IND-ID-CPA游戏）如下：

- 初始化：挑战者输入安全参数k，产生公开的系统参数$params$ 和保密的主密钥.
- 阶段1(训练)：敌手A发出对$ID_1 ... ID_m$的秘密钥产生询问。挑战者运行秘密钥产生算法，产生与公钥ID_i 对应的秘密钥$d_i(i = 1, \ldots, m)$，并把它发送给敌手.

选择明文安全的IBE方案

- 挑战：敌手输出要挑战的两个等长明文m_0,m_1和一个意欲挑战的公开钥ID。唯一的限制是ID不在阶段1中的任何秘密钥询问中出现。挑战者随机选取一个比特值$b \in \{0,1\}$，计算$C = Encrypt(Params, ID, m_b)$，并将$C$发送给敌手.
- 阶段2(训练)：敌手发出对$ID_{m+1}...ID_n$的秘密钥产生询问，唯一的限制是$ID_i \neq ID(i = m+1, \ldots, n)$，挑战者以阶段1中的方式进行回应.
- 猜测：敌手输出猜测$b' \in \{0,1\}$，如果$b = b'$,则A成功.

选择明文安全的IBE方案

敌手的优势定义为安全参数k 的函数：

$$Adv_{\mathcal{E},\mathrm{A}}^{ID-CPA}(k) = |Pr[b = b'] - \frac{1}{2}|$$

Definition2-1

如果对任何多项式时间的敌手A，存在一个可忽略的函数$negl(k)$，使得$Adv_{\mathcal{E},\mathrm{A}}^{ID-CPA}(k) \leq negl(k)$，那么就称这个加密算法在适应性选择密文攻击下具有不可区分性，或者称为IND-ID-CPA安全。

BasicIdent

简单的方案：BasicIdent

该方案包括4个算法：Setup,Extract,Encrypt,Decrypt

1、建立（Setup）：给定安全参数$k \in \mathbb{Z}^+$, 运行BDH参数生成器$\mathcal{G}$

(1) 产生素数q，两个q阶群$\mathbb{G}_1$和$\mathbb{G}_2$,一个双线性映射$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. 选择$\mathbb{G}_1$中的生成元$P$;

(2) 选择一个随机数$s \in \mathbb{Z}_q^*$作为主密钥,计算$P_{pub} = sP$作为公开钥;

(3) 选择2个hash函数$H_1 : \{0,1\}^* \to \mathbb{G}_1^*$，$H_2 : \mathbb{G}_2^* \to \{0,1\}^*$.

系统参数$params =< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, H_1, H_2 >$

BasicIdent

2、密钥提取询问（Extract）：给定ID计算

(1)$Q_{ID} = H_1(ID)$;

(2)$d_{ID} = sQ_{ID}$作为ID对应的秘密钥。

3、加密（Encrypt）：给定明文M和ID

(1)计算$Q_{ID} = H_1(ID) \in \mathbb{G}_1^*$;

(2)选择随机数$r \in \mathbb{Z}_q^*$;

(3)$C =< rP, M \oplus H_2(g_{ID}^r) >$，其中$g_{ID} = \hat{e}(Q_{ID}, P_{pub}) \in \mathbb{G}_2^*$.

BasicIdent

4、解密（Decrypt）：设$C =< U, V >$是用ID加密的密文，使用相应的秘密钥d_{ID}解密：

$$V \oplus H_2(\hat{e}(d_{ID}, U)) = M$$

正确性：

$$\hat{e}(d_{ID}, U) = \hat{e}(sQ_{ID}, rP) = \hat{e}(Q_{ID}, P)^{sr} = \hat{e}(Q_{ID}, P_{pub})^r = g_{ID}^r$$

选择明文安全的IBE方案

定理2-1

在BasicIdent中，设Hash函数H_1，H_2是随机谕言机，如果BDH问题在$\mathcal{G}$生成的群上是困难的，那么BasicIdent是IND-ID-CPA安全的。

具体来说，假设存在一个IND-ID-CPA敌手A以$\epsilon(k)$ 的优势攻破BasicIdent方案，A最多进行$q_{H_1} > 0$ 次H_1 询问、$q_{H_2} > 0$次H_2 询问，那么一定存在一个敌手B至少以

$$Adv_{\mathcal{G},\mathcal{B}}(k) \geq \frac{2\epsilon(k)}{e \cdot q_{H_1} \cdot q_{H_2}}$$

的优势解决$\mathcal{G}$生成的群中的BDH问题

选择明文安全的IBE方案

定理2-1是将BasicIdent规约到BDH问题，为了证明这个规约，我们先将BasicIdent规约到一个非基于身份的加密方案BasicPub，再将BasicPub规约到BDH问题，规约的传递性是显然的。

BasicPub加密方案如下定义：

(1)密钥产生：设安全参数$k \in \mathbb{Z}^+$

1. 运行$\mathcal{G}$,生成两个阶为素数q的群$\mathbb{G}_1$,$\mathbb{G}_2$,一个双线性映射$\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. 随机选择$\mathbb{G}_1$中的生成元$P$;
2. 选择一个随机数$s \in \mathbb{Z}_q^*$，计算$P_{pub} = sP$。随机选取$Q_{ID} \in G_1^*$，计算$d_{ID} = sQ_{ID}$作为秘密钥;
3. 选择一个杂凑函数$H_2 : \mathbb{G}_2 \to \{0,1\}^n$;
4. 公开钥：$< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, Q_{ID}, H_2 >$。

选择明文安全的IBE方案

(2)加密：随机选取$r \in \mathbb{Z}_q^*$，计算$C =< rP, M \oplus H_2(g^r) >$，其中$g = \hat{e}(Q_{ID}, P_{pub}) \in \mathbb{G}_2^*$

(3)解密：设$C =< U, V >$，计算$V \oplus H_2(\hat{e}(d_{ID}, U)) = M$

在BasicIdent中，Q_{ID}是根据用户的身份产生的。而在BasicPub中是随机选取的一个固定值，因此它与用户的身份无关。

选择明文安全的IBE方案

首先证明BasicIdent到BasicPub的规约。

引理2-1

设H_1是从$\{0,1\}^*$ 到$\mathbb{G}_1^*$ 的随机预言机，A是IND-ID-CPA以$\epsilon(k)$优势成功攻击BasicIdent的敌手。假设A最多进行$q_{H_1} > 0$次$H_1(\cdot)$ 询问，那么存在一个IND-CPA敌手B以最少$\frac{\epsilon(k)}{eq_{H_1}}$ 的概率成功攻击BasicPub，运行时间是$O(time(A))$。

选择明文安全的IBE方案

引理2-1之证明

证明: 挑战者先建立BasicPub方案，敌手B攻击BasicPub方案时，以A为子程序，过程如图2所示，其中方案1为BasicIdent，方案2为BasicPub。

为了简化，不失一般性，我们假设：（1）A不会对$H_1(\cdot)$发起两次相同的询问；（2）如果A请求身份ID的密钥提取询问，则它之前已经询问过$H_1(ID)$。

具体过程如下：

选择明文安全的IBE方案

引理2-1之证明

(1) 初始化：挑战者运行BasicPub中的密钥产生算法生成公开钥$K_{pub} =< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, Q_{ID}, H_2 >$，保留秘密钥$d_{ID} = sQ_{ID}$。B获得公开钥。

下面（2）∽（6）步，B模拟A的挑战者和A进行IND游戏。

(2) B的初始化：B发送BasicIdent的公开钥$K_{pub} =< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, H_1, H_2 >$给A，且随机选择$j \in \{1, \ldots, q_{H_1}\}$，这里$j$ 是B的一个猜测值：A的这次H_1询问对应着A最终的攻击结果。因BasicPub中的公开钥无H_1，所以B为了承担A的挑战者，需要构造一个H_1列表H_1^{list}，它的元素类型是3元组$< ID_i, Q_i, b_i >$。

选择明文安全的IBE方案

引理2-1之证明

(3)H_1 询问

设A询问ID_i, $\mathcal{B}$ 如下应答:

1. 如果ID_i已经在H_1^{list}, B以$Q_i \in \mathbb{G}_1^*$作为H_1的值应答A;
2. 否则B选择随机数$b_i \in Z_q^*$,
   - 如果$i = j$，计算$Q_i = b_i Q_{ID} \in \mathbb{G}_1^*$；
   - 否则，计算$Q_i = b_i P \in \mathbb{G}_1^*$；

B将$< ID_i, Q_i, b_i >$加入H_1^{list}，并以$H_1(ID_i) = Q_i$ 回应A。

选择明文安全的IBE方案

引理2-1之证明

(4) 密钥提取询问-阶段1：设ID_i 是A向B发出的密钥提取询问，

1. 如果$i = j$，B报错并退出(此时，B原打算利用A对BasicIdent的攻击来攻击BasicPub，B无法利用A，所以对BasicPub的攻击失败)；
2. 否则B从H_1^{list} 取出$Q_i = b_i P$，求$d_i = b_i P_{Pub}$，并将d_i 作为ID_i 对应的BasicIdent的秘密钥给A。

这是因为$d_i = sQ_i = s(b_i P) = b_i(sP) = b_i P_{Pub}$。

注意：$d_{ID} = sQ_{ID}$是BasicPub中的秘密钥；$d_i = sQ_i = b_i P_{Pub}$是BasicIdent中的秘密钥。

选择明文安全的IBE方案

引理2-1之证明

(5) A发出挑战：设A的挑战是ID_{ch}, m_0, m_1，满足$ID_i = ID_{ch}$，

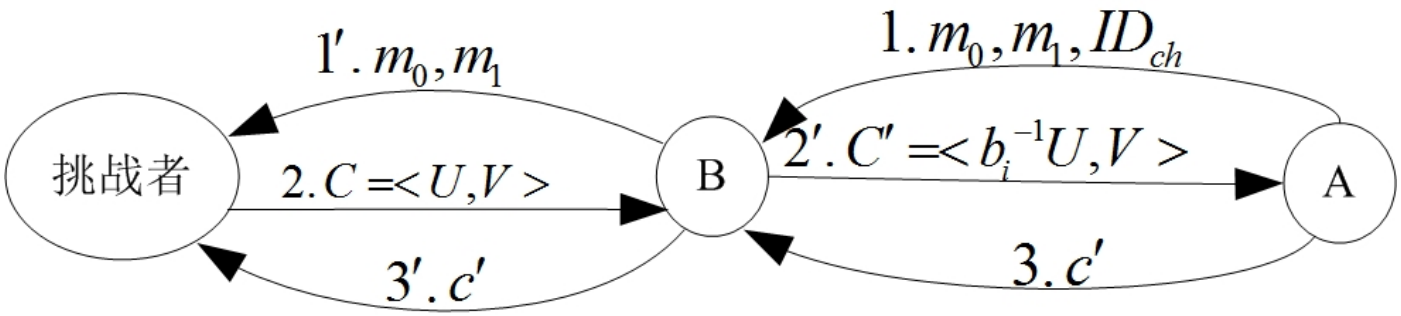
1. 如果$i \neq j$，B报错并退出；
2. 否则(此时$Q_i = b_i Q_{ID}$)，B将m_0, m_1给自己的挑战者，挑战者随机选$c \in \{0, 1\}$，以BasicPub方案加密m_c得$C =< U, V >$ (BasicPub密文)作为对B的应答。B则以$C' =< b_i^{-1} U, V >$ (BasicIdent密文)作为对A的应答。这是因为$d_{ch} = sQ_i = sb_i Q_{ID} = b_i sQ_{ID} = b_i d_{ID}$ (BasicIdent密钥)，
$\hat{e}(d_{ch}, b_i^{-1} U) = \hat{e}(b_i d_{ID}, b_i^{-1} U) = \hat{e}(d_{ID}, U)$

选择明文安全的IBE方案

引理2-1之证明

挑战过程如图4所示。

图4: 挑战过程



(6) 密钥提取询问-阶段2：与密钥提取询问-阶段1相同。

(7) 猜测：A输出猜测c'，B也以c'作为自己的猜测。

选择明文安全的IBE方案

引理2-1之证明

断言2-1

在以上规约过程中，如果B不中断，则B的模拟是完备的。

证明 在以上模拟中，当B猜测正确时，A的视图与其在真实攻击中的视图是同分布的。这是因为

选择明文安全的IBE方案

引理2-1之证明

1. A的q_{H_1} 次H_1 询问中的每一个都是用随机值来回答的：
   - 对ID_j 的询问是用$Q_i = b_i Q_{ID}$ 来应答的；
   - 对ID_i 的询问是用$Q_i = b_i P$来应答的；

   由b_i 的随机性，知Q_i 是随机均匀的。而
   在A对BasicIdent的真实攻击中，A得到的是H_1 的函数值，由于假定H_1 是随机谕言机，所以A得到的函数值是均匀的（这就是假定H_1 是随机谕言机的原因）。
2. 而B对A的密钥提取询问的应答$d_i = b_i P_{pub}$ 等于sQ_i，因而是有效的。

   所以两种视图不可区分。（断言2-1证毕）

选择明文安全的IBE方案

引理2-1之证明

继续引理1.2的证明：由断言2-1知，A在模拟攻击中的优势$Adv_{Sim,\mathrm{A}}^{ID-CPA}(k) = |Pr[b = b'] - \frac{1}{2}|$与真实攻击中的优势$Adv_{\mathcal{E},\mathrm{A}}^{ID-CPA}(k)$ 相等，至少为ϵ

设A进行了q_{H_1} 次H_1 询问，若B的猜测是正确的，且A在第（7）步成功攻击了BasicIdent的不可区分性，则B就成功攻击了BasicPub的不可区分性。

因为B猜测正确的概率为$\frac{1}{q_{H_1}}$，B在第（4）步不中断的概率为$(1 - \frac{1}{q_{H_1}})^{q_{H_1}}$，在第（5）步不中断的概率为$\frac{1}{q_{H_1}}$，因此B不中断的概率为$[1 - \frac{1}{q_{H_1}}]^{q_{H_1}} \frac{1}{q_{H_1}}$，B的优势为

选择明文安全的IBE方案

引理2-1之证明

$$[1-\frac{1}{q_{H_1}}]^{q_{H_1}}\frac{1}{q_{H_1}}Adv_{Sim,A}^{ID-CPA}(k)=\frac{\epsilon(k)}{eq_{H_1}}.$$

运行时间显然。(引理2-1证毕)

选择明文安全的IBE方案

下面证明BasicPub到BDH问题的规约。

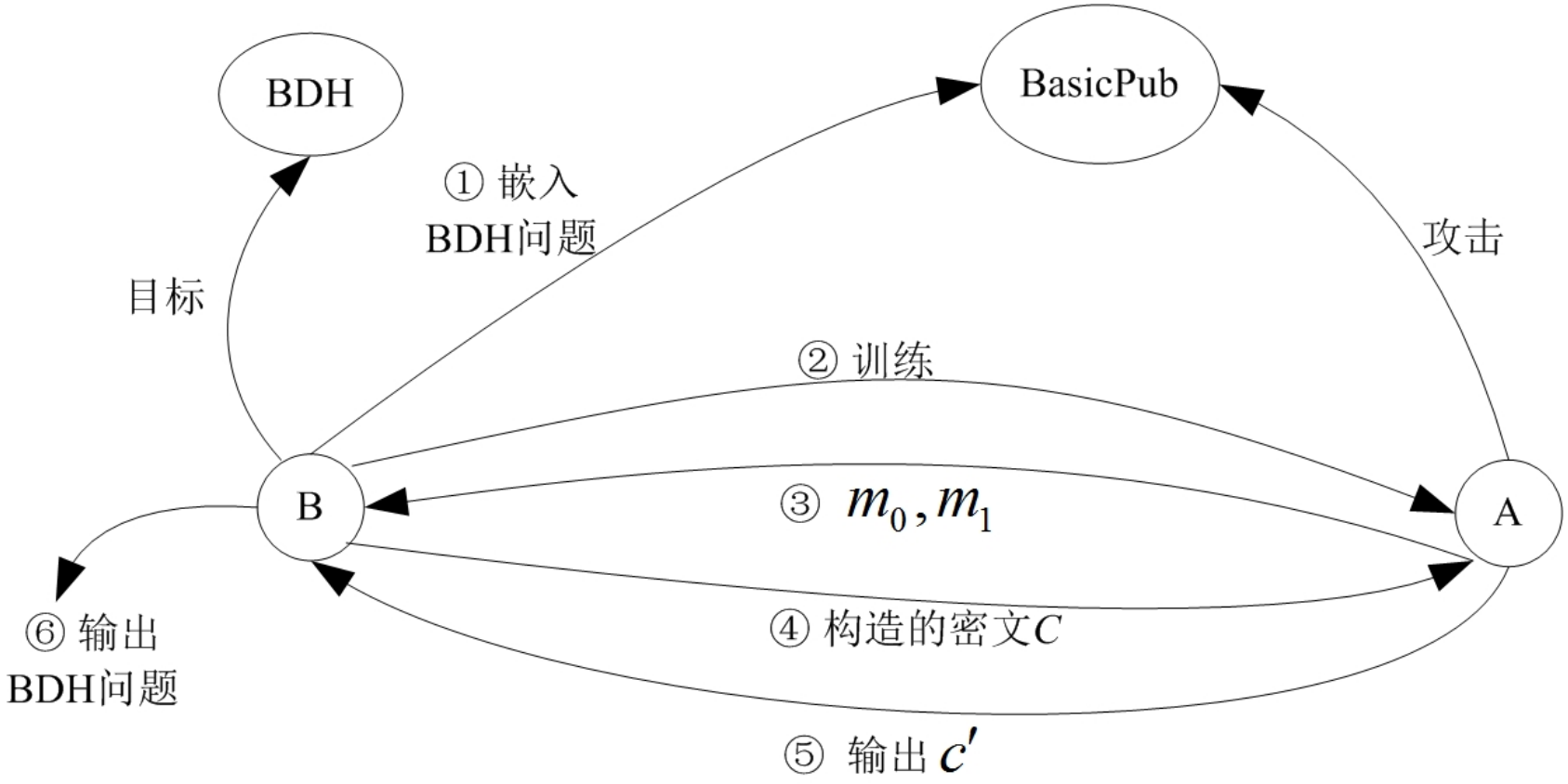
引理2-2

设H_2是从$\mathbb{G}_2$到$\{0,1\}^n$的随机预言机，A是以$\epsilon(k)$的优势攻击BasicPub的IND-CPA敌手, 且A最多向H_2询问$q_{H_2} > 0$次，那么存在一个算法$\mathcal{B}$能以至少$2\epsilon(k)/q_{H_2}$的优势和$O(time(A))$的运行时间解决$\mathcal{G}$上的BDH问题。

证明 为了证明BasicPub到BDH问题的规约，即B已知$< P, aP, bP, cP >=< P, P_1, P_2, P_3 >$，想通过A对BasicPub的攻击，求$D = \hat{e}(P,P)^{abc} \in \mathbb{G}_2$。B在以下思维实验中作为A的挑战者建立BasicPub方案，B设法要把BDH问题嵌入到BasicPub方案。

选择明文安全的IBE方案

图5: BasicPub到BDH问题的规约



选择明文安全的IBE方案

引理2-2之证明

(1) B生成BasicPub的公钥

$$K_{pub} =< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, Q_{ID}, H_2 >$$

其中$P_{pub} = P_1$，$Q_{ID} = P_2$。由于$P_{pub} = sP = P_1 = aP$，所以$s = a, d_{ID} = sQ_{ID} = aQ_{ID} = abP$。

H_2的建立在第（2）步。

选择明文安全的IBE方案

引理2-2之证明

(2) H_2询问：B建立一个H_2^{list} (初始为空)，元素类型为$< X_i, H_i >$，A在任何时候都能发出对H_2^{list} 的询问，B做如下应答：

- 如果X_i已经在H_2^{list}, 以$H_2(X_i) = H_i$应答;
- 否则随机选择$H_i \in \{0,1\}^n$,以$H_2(X_i) = H_i$应答并将$< X_i, H_i >$加入H_2^{list}.

选择明文安全的IBE方案

引理2-2之证明

(3) 挑战：A输出两个要挑战的消息m_0 和m_1 ，B随机选择$R \in \{0,1\}^n$，定义$C =< P_3, R >$，C的解密应为$R \oplus H_2(\hat{e}(P_3, d_{ID})) = R \oplus H_2(D)$，即B已将BDH问题的解$D$埋入$H_2^{list}$。

(4) 猜测：算法A输出猜测$c' \in \{0,1\}$。同时，B从H_2^{list}中随机取$< X_j, H_j >$，把X_j作为BDH的解。

选择明文安全的IBE方案

引理2-2之证明

下面证明B能以至少$2\epsilon(k)/q_{H_2}$ 的概率输出D 。

设$\mathcal{H}$ 表示事件：在模拟中A发出$H_2(D)$ 询问，即$H_2(D)$ 出现在H_2^{list} 中。由B建立的过程知，其中的值是B随机选取的。下面的证明显示，如果H_2^{list} 没有$H_2(D)$ ，即A得不到$H_2(D)$ ，A就不能以ϵ 的优势赢得上述第（4）步的猜测。

选择明文安全的IBE方案

引理2-2之证明

断言2-2

在以上模拟过程中，若$\mathcal{H}$ 不发生，则B的模拟是完备的。

证明 在以上模拟中，若$\mathcal{H}$ 不发生，A的视图与其在真实攻击中的视图是同分布的。这是因为

1. A的q_{H_2} 次H_2 询问中的每一个都是用随机值来回答的，而在A对BasicPub的真实攻击中，A得到的是H_2 的函数值，由于假定H_2 是随机谕言机，所以A得到的H_2 的函数值是均匀的。
2. 若$\mathcal{H}$ 不发生，则$R \oplus H_2(D)$ 对A来说，为$H_2(D)$ 对R 做一次一密加密，A通过$R \oplus H_2(D)$ 得不到m_0 或m_1 的任何信息。所以两种视图不可区分。

选择明文安全的IBE方案

引理2-2之证明

断言2-3

在以上模拟过程中$Pr[\mathcal{H}] \geq 2\epsilon$。

证明 由断言2-2，$Pr[c = c'|\neg\mathcal{H}] = \frac{1}{2}$。又由A在真实攻击中的定义知A的优势为$|Pr[c = c'] - \frac{1}{2}| \geq \epsilon$，得A在模拟攻击中的优势也为$|Pr[c = c'] - \frac{1}{2}| \geq \epsilon$。

$Pr[c = c'] = Pr[c = c'|\neg\mathcal{H}]Pr[\neg\mathcal{H}] + Pr[c = c'|\mathcal{H}]Pr[\mathcal{H}] \leq Pr[c = c'|\neg\mathcal{H}]Pr[\neg\mathcal{H}] + Pr[\mathcal{H}] = \frac{1}{2}Pr[\neg\mathcal{H}] + Pr[\mathcal{H}] = \frac{1}{2} + \frac{1}{2}Pr[\mathcal{H}]$,

$Pr[c = c'] \geq Pr[c = c'|\neg\mathcal{H}]Pr[\neg\mathcal{H}] = \frac{1}{2} - \frac{1}{2}Pr[\mathcal{H}]$

所以$\epsilon \leq |Pr[c = c'] - \frac{1}{2}| \leq \frac{1}{2}Pr[\mathcal{H}]$,

即模拟攻击中$Pr[\mathcal{H}] \geq 2\epsilon$ 。（断言2-3证毕）

选择明文安全的IBE方案

引理2-2之证明

由断言2-3知在模拟结束后, D以至少2ϵ的概率出现在H_2^{list}. 又由引理2-2的假定, A对H_2的询问至少有$q_{H_2} > 0$次，B建立的H_2^{list} 至少有q_{H_2} 项，所以B在H_2^{list} 随机选取一项作为D，概率至少为$2\epsilon(k)/q_{H_2}$。

（引理2-2证毕）

选择明文安全的IBE方案

定理2-1的证明：设存在一个IND-ID-CPA敌手A以$\epsilon(k)$ 的优势攻破BasicIdent方案，A最多进行了q_{H_1} 次H_1 询问，对随机谕言机H_2 至多$q_{H_2} > 0$ 次询问。

由引理2-1，存在IND-CPA敌手B以最少$\epsilon_1 = \frac{\epsilon(k)}{eq_{H_1}}$ 的概率成功攻击BasicPub。由引理2-2，存在另一B能以至少

$$2\epsilon_1/q_{H_2} = \frac{2\epsilon(k)}{eq_{H_1}q_{H_2}}$$

的优势解决$\mathcal{G}$ 生成的群中的BDH问题。

（定理2-1证毕）

选择密文安全的IBE方案

定理2-1已证明BasicIdent是IND-ID-CPA安全的，然而BasicIdent不是IND-ID-CCA安全的。敌手已知密文$C =< C_1, C_2 >$，构造$C' =< C_1, C_2 \oplus m' >$，给解密谕言机，收到解密结果为$m'' = m \oplus m'$，再由$m'' \oplus m'$即获得$C$对应的明文。

选择密文安全的IBE方案

在IBE体制中需加强标准CCA安全的概念，因为在IBE体制中，敌手攻击公钥ID（即获取与之相应的秘密钥）时，他可能已有所选用户$ID_1, \ldots ID_n$的秘密钥，因此选择密文安全应允许敌手获取与其所选身份（除ID外）相应的秘密钥，我们把这一要求看作是对密钥产生算法的询问。

选择密文安全的IBE方案

一个IBE加密方案在适应性选择密文攻击下具有不可区分性，如果不存在多项式时间的敌手，它在下面的攻击过程中有不可忽略的优势。

- 初始化：挑战者输入安全参数k，产生公开的系统参数*params* 和保密的主密钥。

选择密文安全的IBE方案

- 阶段1(训练)：敌手执行$q_1, \ldots, q_m$，这里q_i是下面询问之一：
  - ▷ 对$< ID_i >$的秘密钥产生询问。挑战者运行秘密钥产生算法，产生与公钥ID_i对应的秘密钥d_i，并把它发送给敌手。
  - ▷ 对$< ID_i, C_i >$的解密询问。挑战者运行秘密钥产生算法，产生与ID_i对应的秘密钥d_i，再运行解密算法，用d_i解密C_i，并将所得明文发送给敌手。

选择密文安全的IBE方案

上面的询问可以自适应地进行，是指执行每个q_i 时可以依赖于执行$q_1, \ldots, q_{i-1}$ 时得到的询问结果。

- 挑战：敌手输出两个长度相等的明文m_0,m_1和一个意欲挑战的公开钥ID。唯一的限制是ID 不在阶段1中的任何秘密钥询问中出现。挑战者随机选取一个比特值$b \in \{0, 1\}$，计算$C = Encrypt(params, ID, m_b)$，并将$C$发送给敌手。

选择密文安全的IBE方案

- 阶段2(训练)：敌手产生更多询问$q_{m+1}, \ldots, q_n$，q_i是下面询问之一：
  - ▷ 对$< ID_i >$的秘密钥产生询问（$ID_i \neq ID$）。挑战者以阶段1中的方式进行回应。
  - ▷ 对$< ID_i, C_i >$的解密询问（$< ID_i, C_i > \neq < ID, C >$）。挑战者以阶段1中的方式进行回应。
- 猜测：最后，敌手输出对b的猜测$b' \in \{0, 1\}$，如果$b' = b$, 则成功。

选择密文安全的IBE方案

敌手的优势定义为安全参数k 的函数：

$$Adv_{\varepsilon,A}^{ID-CCA}(k) = |Pr[b = b'] - \frac{1}{2}|$$

Definition 2-2

如果对任何多项式时间的敌手，存在一个可忽略的函数$negl(k)$，使得$Adv_{\varepsilon,A}^{ID-CCA}(k) \leq negl(k)$，那么就称这个加密算法$\varepsilon$ 在选择密文攻击下具有不可区分性，或者称为IND-ID-CCA安全。

选择密文安全的IBE方案

为使上述方案成为IND-ID-CCA安全的，还需对其加以修改。以$\mathcal{E}_{pk}(m,r)$ 表示用随机数r 在公钥pk下加密m的公钥加密算法，Fujisaki-Okamoto指出，如果$\mathcal{E}_{pk}$是单向加密的，则$\mathcal{E}_{pk}^{hy} =< \mathcal{E}_{pk}(\sigma, H_3(\sigma, m)), H_4(\sigma) \oplus m >$ 在随机谕言模型下是IND-CCA安全的，其中σ 是随机产生的比特串，H_3, H_4 是杂凑函数。

$\mathcal{E}_{pk}$取为BasicIdent。

选择密文安全的IBE方案

修改后的加密方案（称为FullIdent方案）如下：

（1）初始化

和BasicIdent相同，此外还需选取两个杂凑函数$H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^*$和$H_4 : \{0,1\}^n \to \{0,1\}^n$，其中$n$是待加密消息的长度。

（2）加密

用公钥ID 加密$m \in \{0,1\}^n$：

- 计算$Q_{ID} = H_1(ID) \in \mathbb{G}_1^*$;
- 选一个随机串$\sigma \in \{0,1\}^n$;
- 计算$r = H_3(\sigma, m)$;
- 确定密文$C =< rP, \sigma \oplus H_2(g_{ID}^r), H_4(\sigma) \oplus m >$,

  这里$g_{ID} = \hat{e}(Q_{ID}, P_{pub}) \in \mathbb{G}_2^*$.

选择密文安全的IBE方案

（3）密钥产生和BasicIdent相同。

（4）解密

令$C =< U, V, W >$是用ID加密所得的密文。如果$U \notin \mathbb{G}_1^*$，拒绝这个密文。否则，用秘密钥$d_{ID} \in \mathbb{G}_1^*$对$C$如下解密：

- 计算$V \oplus H_2(\hat{e}(d_{ID}, U)) = \sigma$；
- 计算$W \oplus H_4(\sigma) = m$;
- 确定$r = H_3(\sigma, m)$. 检验$U = rP$是否成立，如果不成立，则拒绝;
- 把m作为C的明文。

选择密文安全的IBE方案

定理2-2

设Hash函数H_1, H_2, H_3, H_4是随机谕言机，如果BDH问题在$\mathcal{G}$生成的群上是困难的，那么FullIdent是IND-ID-CCA安全的。

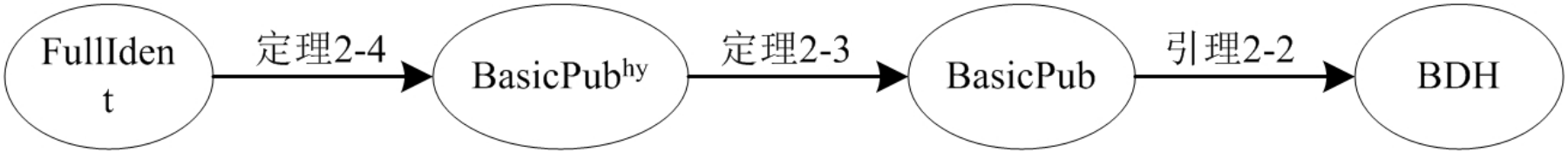
具体来说，假设存在一个IND-ID-CCA敌手A以$\epsilon(k)$的优势攻击FullIdent方案，A 分别对随机谕言机H_1, H_2, H_3, H_4至多$q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}$次询问, 并且假定A的运行时间至多为$t(k)$. 那么存在另一个敌手B至少以$Adv_{\mathcal{G},\mathcal{B}}(k)$的优势和$t_1(k)$的时间解决$\mathcal{G}$生成的群中的BDH问题. 其中

$$Adv_{\mathcal{G},B}(k) \geq 2FO_{adv}(\frac{\epsilon(k)}{eq_{H_1}}, q_{H_2}, q_{H_3}, q_{H_4}), t_1(k) \leq FO_{time}(t(k), q_{H_3}, q_{H_4})$$

选择密文安全的IBE方案

设将$\mathcal{E}^{hy}$作用于BasicPub，得到的方案为BasicPub^{hy}。为了证明FullIdent方案到BDH问题的规约，根据规约的传递性，首先将FullIdent方案规约到BasicPub^{hy}，再将BasicPub^{hy}规约到BasicPub，最后将BasicPub规约到BDH问题，如图6所示。其中BasicPub到BDH问题的规约已由引理2-2证明，BasicPub^{hy}到BasicPub的规约由下面定理2-3给出。FullIdent方案到BasicPub^{hy}的规约由下面定理2-4给出。

图6: FullIdent方案到BDH问题的规约



选择密文安全的IBE方案

定理2-3(Fujisaki-Okamoto): BasicPub^{hy}到BasicPub的规约

假设存在一个IND-CCA敌手A以$\epsilon(k)$的优势攻击BasicPub^{hy}，A分别对随机谕言机H_2, H_3, H_4 至多$q_{H_2}, q_{H_3}, q_{H_4}$次询问, 并且假定A的运行时间至多为$t(k)$. 那么存在一个IND-CPA敌手B至少以$\epsilon_1(k)$的优势和$t_1(k)$的时间攻击BasicPub. 其中

$$\epsilon_1(k) \geq FO_{adv}(\epsilon(k), q_{H_2}, q_{H_3}, q_{H_4}) = \frac{1}{2(q_{H_3}+q_{H_4})}[(\epsilon(k)+1)(1-2/q)^{q_{H_2}} - 1]$$

$$t_1(k) \leq FO_{time}(t(k), q_{H_3}, q_{H_4}) = t(k) + O((q_{H_3} + q_{H_4}) \cdot n)$$

其中q是群的阶，n是消息长度。

选择密文安全的IBE方案

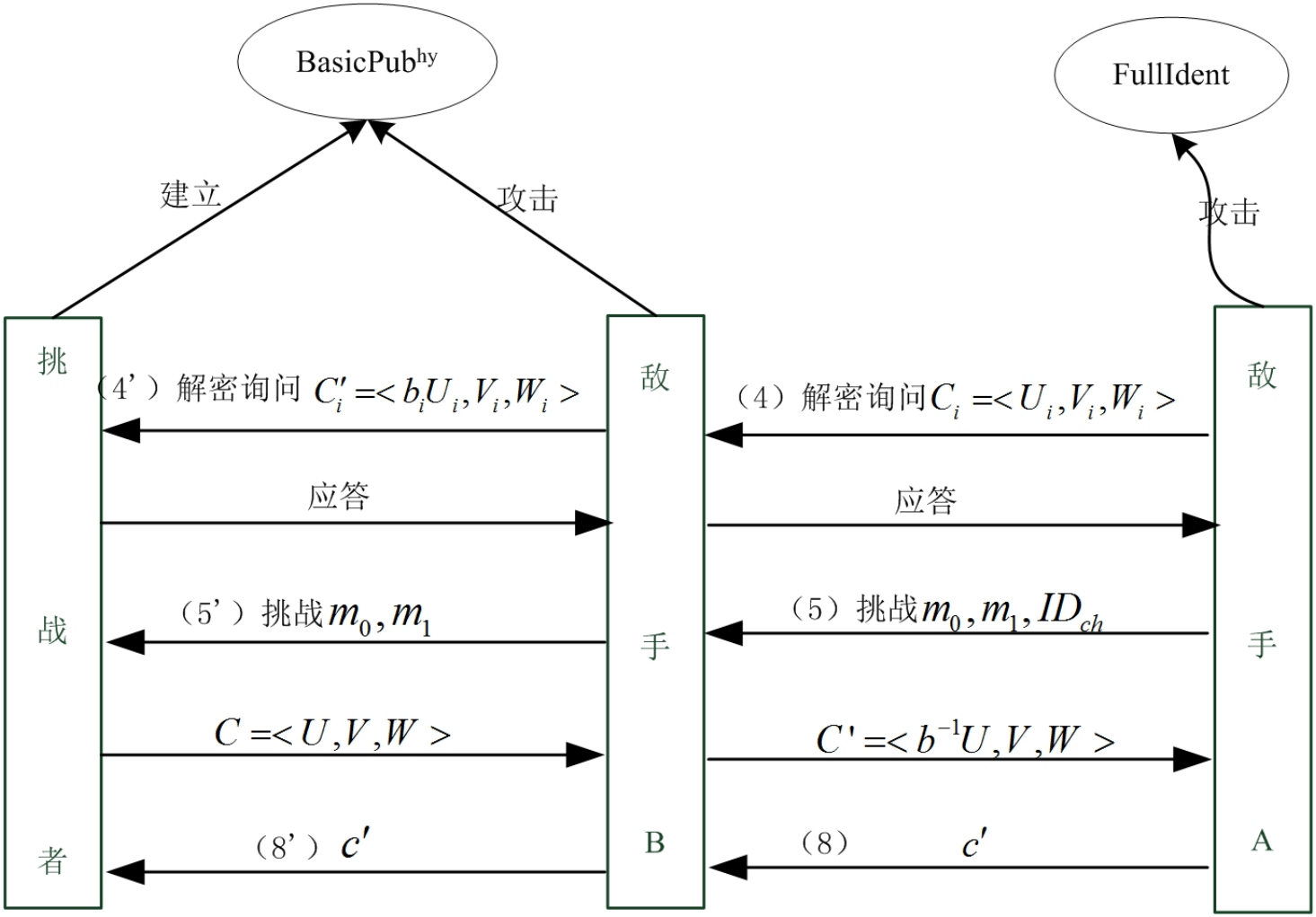
定理2-4: FullIdent方案到BasicPub^{hy}的规约

假设存在一个IND-ID-CCA敌手A以$\epsilon(k)$的优势攻击FullIdent方案，A对随机谕言机H_1 至多做q_{H_1} 次询问。那么存在一个IND-CCA敌手B至少以$\frac{\epsilon(k)}{eq_{H_1}}$ 的优势和$O(time(A))$ 的时间攻击BasicPub^{hy}。

证明：B利用攻击FullIdent的敌手A，如图7所示。为了简化，不失一般性，我们假设：（1）A不会对$H_1(\cdot)$ 发起两次相同的询问；（2）如果A发出解密询问$< ID_i, C_i >$，则它之前已经询问过$H_1(ID_i)$。

选择密文安全的IBE方案

图7: FullIdent方案到BasicPub^{hy}的规约



选择密文安全的IBE方案

(1)初始化：挑战者运行BasicPub^{hy}的密钥产生算法生成公钥$K_{pub} =< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, Q_{ID}, H_2, H_3, H_4 >$给IND-CCA敌手B，并保留秘密钥$d_{ID} = sQ_{ID}$。

下面（2）∽（8）步，B模拟A的挑战者和A进行IND游戏。

(2) B的初始化：

B发送公开钥$K_{pub} =< q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, H_1, H_2, H_3, H_4 >$给A，且随机选择$j \in \{1, \ldots, q_{H_1}\}$，这里$j$ 是B的一个猜测值：A的这次H_1询问对应着A最终的攻击结果。

B为了承担A的挑战者，需要构造一个H_1 列表H_1^{list} ，它的元素类型是3元组$< ID_i, Q_i, b_i >$ 。

选择密文安全的IBE方案

（3）H_1 询问：与引理2-1相同。

（4）密钥提取询问-阶段1：与引理2-1相同。

（5）解密询问-阶段1：设A询问$< ID_i, C_i >$ (注意：FullIdent密文)，其中$C_i =< U_i, V_i, W_i >$ 。B如下应答：

如果$i \neq j$，运行密钥提取询问，获得密钥后做解密询问应答；

如果$i = j$ ，则$Q_i = b_i Q_{ID}$；

- 求$C_i' =< b_i U_i, V_i, W_i >$ (注意：BasicPub^{hy}密文)；
- 向挑战者做$< C_i' >$ 的解密询问，将挑战者的应答转发给A

选择密文安全的IBE方案

（6）A发出挑战：设A的挑战是ID_{ch}, m_0, m_1。设i 满足$ID_{ch} = ID_i$，表示第i 次H_1 询问的询问值。B做以下应答：

•如果$i \neq j$，B报错并退出(B对BasicPubhy的攻击失败)；

•如果$i = j$，将m_0, m_1 给自己的挑战者，挑战者随机选$c \in \{0, 1\}$，以BasicPub^{hy}加密m_c 得$C =< U, V, W >$ 作为对B的应答；B则以$C' =< b_i^{-1}U, V, W >$作为对A的应答。

证明与引理2-1相同。

（7）密钥提取询问-阶段2：与密钥提取询问-阶段1相同。

选择密文安全的IBE方案

（8）解密询问-阶段2：与解密询问-阶段1相同。然而，如果B得到的密文与挑战密文$C_i =< U_i, V_i, W_i >$相同，B报错并退出(B对BasicPub^{hy}的攻击失败)。

（9）猜测：A输出猜测c'，B也以c'作为自己的猜测。

断言2-4

在以上过程中，如果B不中断，则B的模拟是完备的。

证明：在以上模拟中，当B猜测正确时，A的视图与其在真实攻击中的视图是同分布的。这是因为

选择密文安全的IBE方案

1. A的q_{H_1} 次H_1 询问中的每一个都是用随机值来回答的（同断言2-1）；
2. B对A的密钥提取询问的应答是有效的（同断言2-1）；
3. B对A的解密询问的应答是有效的：
   - 如果$i \neq j$，因为密钥提取询问是有效的，B所做的解密是有效的。
   - 如果$i = j$，设$d_i = sQ_i$ 是FullIdent与ID_i 相对应的秘密钥，则在FullIdent中使用d_i 对$C_i =< U_i, V_i, W_i >$的解密与在BasicPub^{hy}中使用d_{ID} 对$C'_i =< b_iU_i, V_i, W_i >$的解密相同，这是因为$\hat{e}(d_{ID}, b_iU_i) = \hat{e}(sQ_{ID}, b_iU_i) = \hat{e}(sb_iQ_{ID}, U_i) = \hat{e}(sQ_i, U_i) = \hat{e}(d_i, U_i)$

所以B所转发的挑战者的解密是有效的。（断言2-4证毕）

选择密文安全的IBE方案

下面考虑在以上过程中B不中断的概率。

引起B中断有3种可能：

(1) 阶段1、2中的密钥提取询问(当$i = j$)；

(2) 挑战时A发出的身份ID_{ch}对应的ID_i，使得$i \neq j$；

(3) 阶段2的解密询问时，A发出的密文与以前的挑战密文相同。

在第（3）种情况中，设A发出的密文$C_i =< U_i, V_i, W_i >$与它的挑战密文$C' =< b_i^{-1}U, V, W >$相同，则$U = b_iU_i, V = V_i, W = W_i$。B将$C_i$转发给挑战者前做变换得$C_i' =< b_iU_i, V_i, W_i >$，得到的结果与B的挑战密文$C =< U, V, W >$相同。这种情况发生当且仅当$i = j$。

选择密文安全的IBE方案

所以整个实验中B不中断的概率为

$$[1-\frac{1}{q_{H_1}}]^{q_{H_1}}\frac{1}{q_{H_1}}[1-\frac{1}{q_{H_1}}]\approx\frac{1}{eq_{H_1}}$$

由断言2-4知，A在模拟攻击中的优势

$$Adv_{Sim,A}^{ID-CCA}(k)=|Pr[c=c']-\frac{1}{2}|$$

与真实攻击中的优势$Adv_{\varepsilon,A}^{ID-CCA}(k)$ 相等，至少为$\epsilon(k)$ 。B的优势为

$$\frac{1}{eq_{H_1}}Adv_{Sim,A}^{ID-CCA}(k)\approx\frac{\epsilon(k)}{eq_{H_1}}.$$

运行时间显然。（定理2-4证毕）

选择密文安全的IBE方案

定理2-2的证明：

参见图6。假定敌手攻击FullIdent的优势为ϵ，则由定理2-4，存在另一攻击BasicPub^{hy} 的敌手，其优势为$\epsilon_1 = \frac{\epsilon}{eq_{H_1}}$ 由定理2-3，存在另一攻击BasicPub的敌手，其优势为

$$\epsilon_2 \geq FO_{adv}(\epsilon_1, q_{H_2}, q_{H_3}, q_{H_4}) = FO_{adv}(\frac{\epsilon}{eq_{H_1}}, q_{H_2}, q_{H_3}, q_{H_4})$$

由引理2-2，存在另一攻击BDH的敌手，其优势为

$$\epsilon_3 \geq \frac{2\epsilon_2}{q_{H_2}} = 2FO_{adv}(\frac{\epsilon}{eq_{H_1}}, q_{H_2}, q_{H_3}, q_{H_4})/q_{H_2}$$

（定理2-2证毕）

以上介绍的CCA和IBE是基于随机谕言机模型的，虽然很有意义和价值，但在这种模型下，不能排除以下可能：攻击者可能不通过攻击它所基于的困难性假定，或者不通过找出hash函数的缺陷而攻击系统。没有随机谕言机的模型称作标准模型。

Thank you!