密码学理论与技术

混合加密方案

*Boneh-Franklin IBE*加密方案

$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

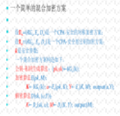
$$M = Y^d \bmod N$$

混合加密方案(1)

- 为什么需要混合方案
  - 公钥加密方案的特点：
  - 使用灵活（无须共享密钥）；
  - 计算效率相对不高，不适于加密长明文。
  - 对称加密方案的特点：
  - 使用相对不灵活（须共享密钥）；
  - 计算效率极高，适于加密长明文。
  - 两者恰具有互补的特性。

混合加密方案(2)

- 一个简单的混合加密方案
-
- 设$\boldsymbol{\Pi_s}=(KG_s, E_s, D_s)$是一个CPA-安全的对称加密方案；
- 设$\boldsymbol{\Pi_a}=(KG_a, E_a, D_a)$是一个CPA-安全的公钥加密方案；
- $\boldsymbol{k}$是安全参数；
- 一个混合加密方案构造如下。
- 公钥-私钥生成算法：$(pk,sk)\leftarrow KG_a(k)$;
- 加密算法$E(pk, M)$：
- $K\leftarrow \mathrm{KG}_s(k)$; $u\leftarrow E_a(pk, K)$; $Y\leftarrow E_s(K, M)$; $\mathrm{output}(u,Y)$;
- 解密算法$D(sk, (u,Y))$：
- $K\leftarrow D_a(sk, u)$; $M\leftarrow D_s(K, Y)$; $\mathrm{output}(M)$;



混合加密方案

安全性质：

如果Π_s和Π_a分别为CPA-安全的加密方案，则$\Pi_{F\text{-}O}$是具有CCA-安全的公钥加密方案。

- *Fujisaki-Okamato*混合

- 设$\Pi_s=(KG_s, E_s, D_s)$是一个CPA-安全的对称加密方案；
- 设$\Pi_a=(KG_a, E_a, D_a)$是一个CPA-安全的公钥加密方案；
- k是安全参数；H、G：随机*Oracle* /*参考OAEP/RSA方案*/
- 公钥-私钥生成算法$KG=KG_a$: $(pk,sk)\leftarrow KG_a(k)$;
- 加密算法$E(pk,M)$：
- 生成随机数σ; /*$H(\sigma\|M)$用作加密算法E_a中的随机数*/
- $Y_1 \leftarrow E_a(pk,\sigma; H(\sigma\|M))$；$Y_2 \leftarrow E_s(G(\sigma),M)$
- output(Y_1, Y_2);
- 解密算法$D(sk,Y)$, $Y=(Y_1, Y_2)$：
- $\sigma \leftarrow D_a(sk,Y_1)$；$M \leftarrow D_s(G(\sigma), Y_2)$；
- *if* $(Y_1 = E_a(pk,\sigma; H(\sigma\|M))$
- *then* output(M)；
- else output(“错误”)；

混合加密方案

安全性质：

如果Π_s和Π_a分别为*CPA*-安全的加密方案，则Π_{REACT}是具有*CCA*-安全的公钥加密方案。

- ***REACT***混合方案Π_{REAC}

- 设Π_s和Π_a分别是CPA-安全的对称和公钥加密方案；
- k是安全参数；H、G：随机*Oracle*；
- 公钥-私钥生成算法$KG=KG_a$: $(pk,sk) \leftarrow KG_a(k)$;
- 加密算法$E(pk,M)$：
- 生成随机数R; $Y_1 \leftarrow E_a(pk,R)$；$Y_2 \leftarrow E_s(G(R),M)$;
- $h \leftarrow H(R||M||Y_1||Y_2)$;
- output(Y_1, Y_2, h);
- 解密算法$D(sk,Y)$, $Y=(Y_1,Y_2,h)$：
- $R \leftarrow D_a(sk,Y_1)$；$M \leftarrow D_s(G(R), Y_2)$；
- $if\ (h = H(R||M||Y_1||Y_2))\ then$ output(M) else output(“错误”)；

- 注：*REACT*方案对密文完整性的验证仅须计算散列函数，因此速度
- 高于Fujisaki-Okamato方案。

混合加密方案(

- ***GEM***混合方案Π_{GEM}(20

安全性质：

如果$\boldsymbol{\Pi_s}$和$\boldsymbol{\Pi_a}$分别为*CPA*-安全的加密方案，则Π_{GEM}是具有*CCA*-安全的公钥加密方案。

例 8-8(*GEM*混合加密方案,2002)F、G和H是随机散列函数，GEM方案Π=(KG, E, D, F, G, H) 由公钥加密方案Π^a=(KG^a, E^a, D^a)和对称加密方案Π^s=(KG^s, E^s, D^s)按以下方式复合而成：

KG=KG^a；加密算法E(pk,M; r||u)=y_1||y_2，其中r是随机数、u是加密算法E^a的随机数，s=F(M||r)、W=s||(r ⊕ H(s))、K=G(W||y_1)、y_1=E^a(pk,W;u)、y_2=E^s(K,M)；解密算法D(sk,y)如下：

parse y as y_1||y_2;

W←D^a(sk,y_1);

K←G(W||y_1);

M←D^s(K,y_2);

Parse W as s||t;

r←t ⊕ H(s);

if s=F(M||r) then output(M) else output("错误");

小　结：

以上所有混合方案实际上都是通用的结构框架，以任何公钥方案和对称方案代入，就能得到各种实例。

在计算效率方面，以上三个方案中以*GEM*方案为最高。

IBE加密方案(1)

- *IBE*加密方案(Identity based Encryption)：通用框架

- 一个IBE方案Π_{IBE}=(Setup, UKG, E, D)是一组算法，其中：
- (1) Setup是全局密钥生成算法，输出全局公钥-私钥偶 (mpk, msk)；
- (2)UKG是用户私钥生成算法，以全局私钥msk、用户身份标识a为输入，
- 输出a的私钥$usk(a)$；
- (3)E是加密算法，以全局公钥mpk、用户身份标识a和消息M为输入并
- 输出密文y；
- (4)D是解密算法，以全局公钥mpk、用户私钥usk(a)和密文y为输入并
- 输出明文M。

【课件修订版说明】
本页语音中所提到阅读的论文和大作业，请忽略之。本课程期末考试将采用笔试。
其他页面涉及的原始论和大作业的信息，均忽略之。

IBE加密方案(2)

- *IBE*加密方案：基本要求

- (1)所有以上算法须满足一致性关系：对任何k、a和M，若
- P[(mpk,msk)←Setup(k);
- usk(a)←UKG(msk,a);
- y←E(mpk, a, M);
- 则 D(mpk, usk(a), y)=M]=1恒成立
- (2)由于*IBE*方案的特殊结构，在刻画其保密性质时需要考虑所谓**合谋**
- **攻击**，这时攻击者可能(通过非法入侵或合谋)持有某些合法用户
- $a^1,\ldots,a^n$的私钥usk(a^1),...usk(a^n).
- **IBE方案的保密性要求**：如果攻击者不持有私钥usk(a)，无论事先能获
- 得多少usk(a^1),...usk(a^n)($a^1,\ldots,a^n \neq a$)都无法从密文E(mpk, a, M)有效获取
- 关于明文M的信息。

IBE加密方案(3)

- *Boneh-Franklin IBE*加密方案：预备知识

- (1) 椭圆曲线$\boldsymbol{E}_{A,B}=\{(x,y)\in F_p\times F_p: y^2=x^3+Ax+B\}$上的*Weil-Pairing*是双线性映射
- $$e(\boldsymbol{u},v): \boldsymbol{E}_{A,B}\times \boldsymbol{E}_{A,B}\to F_p^*$$
- 对任何整数m和n、椭圆曲线$\boldsymbol{E}_{A,B}$上的点$\boldsymbol{u}$和$\boldsymbol{v}$，恒具有性质
- $$e(m\boldsymbol{u},nv)=e(\boldsymbol{u},\boldsymbol{v})^{mn}$$
- (2)双线性群偶$\chi=(q, \mathrm{P}, \mathrm{G}, \mathrm{G}_\mathrm{T}, e:\mathrm{G}\times\mathrm{G}\to\mathrm{G}_\mathrm{T})$上的计算性双线性*Diffie-Hellman*
- 问题(简称*CBDHP*)是这样一类问题：
- 任给G上的元素$U=a\mathrm{P}$、$V=b\mathrm{P}$、$W=c\mathrm{P}$(a、b、c未知)，求$e(\mathrm{P},\mathrm{P})^{abc}$。
- (3) k=素数q的位数，χ上的*CBDH*问题难解是指：对任何P.P.T.算法A，概率
- $\mathrm{P}[a,b,c\xleftarrow{\$}F_q; U\leftarrow a\mathrm{P}; V\leftarrow b\mathrm{P}; W\leftarrow c\mathrm{P}; z\leftarrow \mathrm{A}(\chi,U,V,W): z=e(\mathrm{P},\mathrm{P})^{abc}]=O(2^{-ck})$。
- (4) 典型实例：
- G=椭圆曲线加法群$(\boldsymbol{E}_{A,B},+)$、$\mathrm{G}_\mathrm{T}=F_p^*$的情形。

IBE加密方案(4)

- *Boneh-Franklin IBE*加密方案(2001)：算 法
- e: $G_1 \times G_1 \to G_2$
  $|G_1| = p$
  $P \in G_1$

设(q,P,G₁,G₂, *e*)是双线性群偶，*k*是复杂性参数，H_1: $\{0,1\}^* \to G_1$、H_2: $G_2 \to \{0,1\}^n$ 是两个随机散列函数，n是明文消息的字长。*Boneh-Franklin*方案的组成算法如下。

全局密钥生成算法 Setup(k):

$s \xleftarrow{\$} Z^*_q$; mpk←sP; msk←s; return(mpk, msk);

用户私钥生成算法UKG(msk,*a*), $a \in \{0,1\}^+$是身份标识, msk=s:

usk←$sH_1(a)$; return(usk);

加密算法 E(mpk,*a*,M):

$r \xleftarrow{\$} Z^*_q$; $T \leftarrow M \oplus H_2(e(H_1(a), mpk)^r)$; $y \leftarrow rP||T$; return(y);

解密算法D(mpk,usk,y_0||T):

$M \leftarrow T \oplus H_2(e(usk, y_0))$; return(M);

不难验证以上方案满足一致性条件，事实上有 *e* 的双线性性质有

$e(usk, y_0)=e(sH_1(a), rP)= e(H_1(a), P)^{sr}= e(H_1(a), sP)^r=e(H_1(a), mpk)^r$

注意*Boneh-Franklin*方案具有随机oracle范型。

IBE加密方案(5)

- *Boneh-Franklin IBE*加密方案：安全性质

- (1) 若χ=(q, P, G, G_T, e:G×G→G_T)上的计算性双线性*Diffie-Hellman*问题
- 难解，则χ上的Boneh-Franklin方案具有对用户私钥*sk*的抗合谋攻
- 击能力、以及密文的CPA-安全性。

- (2) 对素域上的椭圆曲线，相应的*Boneh-Franklin*方案具有以上安全特性。

- (3) 通过结合任何一种CPA-安全的对称加密方案，借助前述任何一种混合
- 加密变换，例如*Fujisaki-Okamato*变换，就得到具有用户私钥抗合谋
- 攻击能力和密文CCA-安全性的*IBE*加密方案。

- (4) 注意*Boneh-Franklin*方案具有*random-oracle*范型。
-

IBE加密方案(6)

- *Waters IBE*加密方案(2005)：

8-27 (*Waters* IBE方案,2005) 设(p, P, G_1,G_2, *e*)是双线性群偶，p是*k*位素数，*Waters* IBE方案组成算法如下：

全局公钥/私钥生成算法 Setup(k):

$Q \xleftarrow{\$} G_1$; $\alpha \xleftarrow{\$} Z_p$; $P_1 \leftarrow \alpha P$; $Q_1 \leftarrow \alpha Q$;

$U[0..n] \xleftarrow{\$} G_1^{n+1}$; $E \leftarrow e(P, Q)$;

mpk←(G_1,G_2,p,*e*,P, P_1,U,E);

msk←(mpk,Q_1);

return(mpk, msk);

加密算法E(mpk,*a*,M), mpk=((G_1,G_2,p,*e*,P, P_1,U,E), Q_1), M∈G_2:

$V \leftarrow U[0] + \sum_{i=1}^{n} a(i)U[i]$;

$t \xleftarrow{\$} Z_p$; $T \leftarrow E^t$;

y←(TM, tP, tV);

return(y);

用户私钥生成算法UKG(msk,*a*), *a*=*a*(1)…*a*(n) ∈ $\{0,1\}^n$, msk=((G_1,G_2,p,*e*,P, P_1,U,E), Q_1):

$r \xleftarrow{\$} Z_p$; $V \leftarrow U[0] + \sum_{i=1}^{n} a(i)U[i]$;

usk(*a*)←(Q_1+rV, rP);

return(usk(*a*));

解密算法D(mpk,usk(*a*),y), usk(*a*)=(s_1, s_2), y=(y_1, y_2, y_3):

$T \leftarrow e(s_1, y_2)e(s_2, y_3)^{-1}$;

return($y_1 T^{-1}$);

习题（两题选做之一）

- 1、基于*Fujisaki-Okamato*混合方案为框架，具体采用
- DES为对称加密方案、*ElGamal*为公钥加密方案，
- 给出相应的一个具体实现。

- 2、基于GEM混合方案为框架，具体采用AES为对称
- 加密方案、*Boneh-Franklin*方案为公钥加密方案，
- 给出相应的一个（无须公钥证书的）具体实现。