密码学理论与技术

公钥加密方案的安全模型(续)

更多的公钥加密方案

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

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

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

公钥加密方案(5)

- **公钥加密方案普适安全模型: (KG,E,D)的CPA-安全**

P： 解密私钥持有者　　**k**是安全参数　　A： 破译者/P.P.T算法

1. $(pk,sk) \leftarrow \mathrm{KG}(k)$

2. pk

3. $(St,M_0,M_1) \leftarrow \mathrm{A1}(pk)$: $|M_0|=|M_1|$且 $M_0 \neq M_1$

4. M_0,M_1

5. $b \leftarrow^{\$} \{0,1\}$; $\boldsymbol{y}^* \leftarrow E(pk,M_b)$;

6. $\boldsymbol{y}^*$

7. $b^* \leftarrow \mathrm{A}_2(\boldsymbol{y}^*, St)$:

安全的加密算法犹如高明的化妆师，拿手好戏是掩饰。

- 公钥加密方案定义做**CPA-不安全**(*in-Secure Against Chosen Plaintext Attack*)，若存在*P.P.T.*算法A和多项式*poly*$_0(k)$，对$k \rightarrow \infty$满足
- $$|P[b^*= b] - ½| \geq 1/\mathrm{poly}_0(k)$$

【思考】如果加密算法E是确定性算法，以上的过程中A成功的概率是多少？　　答案：P[b*=b]=1！

公钥加密方案(6)

- **公钥加密方案普适安全模型: (KG,E,D)的CCA-安全**

P: 解密私钥持有者	k是安全参数	**A:** 破译者/P.P.T算法
1. $(pk,sk)\leftarrow KG(k)$	2. pk $\rightarrow$	3. $(St_1,\{y_k\}_{k=1\ldots N1})\leftarrow A_1(pk)$: y_k是该方案的一组密文
	4. $\{y_k\}_{k=1\ldots N1}$ $\leftarrow$	
5. $U_k \leftarrow D(sk,y_k)$	6. $\{U_k\}_{k=1\ldots N1}$ $\rightarrow$	7. $(St_2,M_0,M_1)\leftarrow A_2(St_1,\{U_k\})$: $\|M_0\|=\|M_1\|$、$M_0\neq M_1$ 且M_0,M_1不属于$\{U_k\}$
	8. M_0,M_1 $\leftarrow$	
9. $b\leftarrow^{\$}\{0,1\}$; $\mathbf{y}^*\leftarrow E(pk,M_b)$;	10. $\mathbf{y}^*$ $\rightarrow$	11. $(St_3,\{z_k\}_{k=1\ldots N2})\leftarrow A_3(\mathbf{y}^*, St_2)$: z_k是该方案的一组密文
13. $V_k \leftarrow D(sk,z_k)$	12. $\{z_k\}_{k=1\ldots N2}$ $\leftarrow$	
	14. $\{V_k\}_{k=1\ldots N2}$ $\rightarrow$	15. $b^*\leftarrow A_4(\mathbf{y}^*, St_3, \{V_k\})$

- 公钥加密方案定义做**CCA-不安全**(in-*Secure Against Chosen Cyphertext Attack*)，若存在*P.P.T.*算法A和多项式$poly_0(k)$，对$k\rightarrow\infty$满足
- $$|P[b^*= b] - ½| \geq 1/poly_0(k)$$

公钥加密方案(7)

- 公钥加密方案普适安全模型：主要结论
- CPA-安全：语义安全/抗选择明文攻击
- CCA-安全：抗选择密文攻击
- CMA-安全：抗密文可塑性安全
- (1) **CPA-安全 < CCA-安全 = CMA-安全。**
- 原始论文：M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, *Relations among notions of security for public-key encryption schemes*, Lecture Notes in Computer Science, vol. 1462, 1998, pp. 26–45.
- 【注】在学习本课程之后再阅读该论文，是一种很好的认知提高。
- (2) 一个公钥加密方案若是CPA安全的，则加密算法必是随机算法。
- (3) 一个公钥加密方案若是CPA安全的，则任何*P.P.T*算法成功破译任何密文
- 的概率随安全参数$k\to\infty$的渐进上界为O(1/poly(k)), b>0是某个常数。

公钥加密方案(8)

- 公钥加密方案的普适安全模型：小 结
- 任何安全模型均须反映以下要素：
- (1) 安全方案或安全协议的工作特点
- (2) 攻击者的能力：**P.P.T算法**
- (3) 实施攻击时可能获取到的信息
- (4) 攻击者的目标：破译、伪造、身份欺诈....
- (5) 攻击者达成其攻击目标程度的度量：
- 攻击成功的概率随安全参数的渐进下降速率

公钥加密方案(9)

- ***ElGamal***方案：精确的安全性结论
- 记号：$poly(k)$表示k的某个多项式，k是某种安全参数。
- 若群族
- $\{G_{g(k),q(k)}: G_{g(k),q(k)}$是以$g(k)$为生成子的素$q(k)$阶循环群，$k\to\infty\}$
- 上的判定性*Diffie-Hellman*问题难解，即任何*P.P.T*算法(平均时间
- 复杂度是$poly(k)$的随机算法)$\boldsymbol{A}$都有
- $|\ P[A(g(k), u,v,w) = 1 | 1 \leqq x,y \leqq q(k),\ u=g(k)^x,\ v=g(k)^y,\ w=g(k)^{xy}]$
- $-\ P[A(g(k), u,v,w) = 1 | 1 \leqq x,y,w \leqq q(k),\ u=g(k)^x,\ v=g(k)^y,\ w=g(k)^w]\ |$
- $\leqq\ O(2^{-k})$， $k\to\infty$，
- 则*ElGamal*方案具有CPA-安全性。

公钥加密方案(10)

- ***ElGamal***方案的实现

- 实现之一：
- 群族$\{G_{g,q}: G_{g,q}$是F_p^*的q阶循环子群，$q \to \infty\}$；
- 方案的运算是$mod\ p$的整数乘法运算。

- 实现之二：
- 群族$\{G_{g,q}: G_{g,q}$是有限域F_p上的椭圆曲线$E_{A,B}$上的q阶循环子群，
- $q \to \infty\}$；
- $E_{A,B} = \{(x,y): x,y \in F_p,\ y^2 = x^3 + Ax + B\}$
- 方案的运算是$E_{A,B}$上的“加法”运算：

$$x_3 = -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2, \qquad y_3 = -y_1 - \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_3 - x_1)$$

以上ElGamal方案的实现都具有语义安全性。

公钥加密方案

- *ElGamal*方案的安全性证明

- G是素q阶循环群，生成子为g:
- 密钥生成算法KG(q,g):
- $x \leftarrow^{\$} F_q$; $Y \leftarrow g^x$; 公钥$pk=(q,g,Y)$;私钥$sk=(x)$;
- 加密算法E(pk, M), $M \in G$:
- $r \leftarrow^{\$} F_q$; $R \leftarrow g^r$; $T \leftarrow Y^r$; $W \leftarrow TM$; output(R, W);
- 解密算法D(sk, (R,W)):
- $T_1 \leftarrow R^x$; $M \leftarrow WT_1^{-1}$; output(M);

- 证明的思路：
- 利用*ElGamal*方案的破译算法***A***
- 构造求解*DDHP*的算法***B***，*B*仅
- 以多项式复杂度实施计算和调用
- 算法*A*。

ElGamal方案的CPA安全性证明:

DDHP (u_1, u_2, u_3) solver B — A:

$u_1 = g^{x_1} \bmod p$, $u_2 = g^{x_2} \bmod p$;

$u_3 = g^{x_1 x_2} \bmod p$ 或是 F_p^* 上均匀分布的随机数.

$pk \leftarrow u_1$; — pk →

← M_0, M_1

$b \xleftarrow{\$} \{0,1\}$; $y_1 \leftarrow u_2$; $y_2 \leftarrow u_3 \cdot M_b \bmod p$; — $y_1 \| y_2$ →

← $b^* \in \{0,1\}$

if $b^* = b$ output (1): $u_3 = g^{x_1 x_2} \bmod p$

else output (0): u_3是同u_1, u_2无关的随机数.

分析: $P[B(\underbrace{g^{x_1} \bmod p}_{u_1}, \underbrace{g^{x_2} \bmod p}_{u_2}, \underbrace{g^{x_1 x_2} \bmod p}_{u_3})=1] \geq P[A\text{输出}b^*=b]$

$P[B(u_1, u_2;\ u_3\text{是同}u_1,u_2\text{无关的随机数})=1] = \frac{1}{2}$

设 $\left|P[B(g^{x_1} \bmod p, g^{x_2} \bmod p, g^{x_1 x_2} \bmod p)=1] - P[B(g^{x_1} \bmod p, g^{x_2} \bmod p, u_3)=1]\right|$

$\geq \left|P[A\text{输出}b^*=b] - \frac{1}{2}\right| > \tilde{p}(t)^{-1}$, $\tilde{p}(t)$是 $t=|p|$ 的某个多项式

公钥加密方案(11)

- **对称加密方案普适安全模型: (KG,E,D)的CPA-安全**

P： 密钥合法持有者　　**k**是安全参数　　A： 破译者

1. $K \leftarrow KG(k)$

2. $|K|$ (P → A)

3. $(St_1, \{U_k\}_{k=1\ldots N1}) \leftarrow A_1(|K|)$: U_k是该方案的一组明文

4. $\{U_k\}_{k=1\ldots N1}$ (A → P)

5. $y_k \leftarrow E(K, U_k)$

6. $\{y_k\}_{k=1\ldots N1}$ (P → A)

7. $(St_2, M_0, M_1) \leftarrow A_2(St_1, \{y_k\})$: $|M_0|=|M_1|$、$M_0 \neq M_1$ 且M_0, M_1不属于$\{U_k\}$

8. M_0, M_1 (A → P)

9. $b \leftarrow^{\$} \{0,1\}$; $\mathbf{y}^* \leftarrow E(K, M_b)$;

10. $\mathbf{y}^*$ (P → A)

11. $(St_3, \{V_k\}_{k=1\ldots N2}) \leftarrow A_3(\mathbf{y}^*, St_2)$: V_k是该方案的一组明文

12. $\{V_k\}_{k=1\ldots N2}$ (A → P)

13. $z_k \leftarrow E(K, V_k)$

14. $\{z_k\}_{k=1\ldots N2}$ (P → A)

15. $b^* \leftarrow A_4(\mathbf{y}^*, St_3, \{z_k\})$

- 对称加密方案定义做**CPA-不安全**(in-*Secure Against Chosen Plaintext Attacke*)，若存在*P.P.T.*算法A和多项式$poly_0(k)$，对$k \rightarrow \infty$满足
- $$|P[b^* = b] - ½| \geq 1/poly_0(k)$$

公钥加密方案(12)

- **对称加密方案普适安全模型: (KG,E,D)的CCA-安全**

P： 密钥合法持有者　　***k***是安全参数　　A： 破译者

1. $K \leftarrow KG(k)$

2. $|K|$ （P → A）

3. $(St_1, \{y_k\}_{k=1\ldots N1}) \leftarrow A_1(|K|)$: y_k是该方案的一组密文

4. $\{y_k\}_{k=1\ldots N1}$ （A → P）

5. $U_k \leftarrow D(K, y_k)$

6. $\{U_k\}_{k=1\ldots N1}$ （P → A）

7. $(St_2, M_0, M_1) \leftarrow A_2(St_1, \{U_k\})$: $|M_0|=|M_1|$、$M_0 \neq M_1$ 且M_0, M_1不属于$\{U_k\}$

8. M_0, M_1 （A → P）

9. $b \leftarrow^{\$} \{0,1\}$; $\mathbf{y}^* \leftarrow E(K, M_b)$;

10. $\mathbf{y}^*$ （P → A）

11. $(St_3, \{z_k\}_{k=1\ldots N2}) \leftarrow A_3(\mathbf{y}^*, St_2)$: z_k是该方案的一组密文

12. $\{z_k\}_{k=1\ldots N2}$ （A → P）

13. $V_k \leftarrow D(K, z_k)$

14. $\{V_k\}_{k=1\ldots N2}$ （P → A）

15. $b^* \leftarrow A_4(\mathbf{y}^*, St_3, \{V_k\})$

- 对称加密方案定义做**CCA-不安全**(*in-Secure Against Chosen Cyphertext Attacke*)，若存在*P.P.T.*算法A和多项式$poly_0(k)$，对$k \rightarrow \infty$满足

- $$|P[b^* = b] - ½| \geq 1/poly_0(k)$$

公钥加密方案(13)

- *Cramer-Shoup*公钥加密方案(1998)

- (1) *ElGamal*方案密文可塑，*Cramer-Shoup*方案可以看做是该方案的
- 抗密文可塑版(等价地，CCA-安全)。
- (2) 与OAEP/RSA不同，Cramer-Shoup方案不依赖于随机Oracle，
- 即属于Standard-Model。
- (3) Cramer-Shoup方案的公钥依赖于“单向散列函数”***H***。一个函数
- 是**单向**的，是指存在多项式复杂度算法A从自变量*x*计算H(*x*)，但
- 不存在任何*P.P.T*算法以不可忽略的概率从y计算*x*使y=H(*x*)，即
- 对任何*P.P.T*算法***B***成立 $P[B^H(y)=x: H(x)=y] \leqq O(2^{-|x|})$。

- 原始论文：A Practical Public Key Cryptosystem Provably_ Secure against Adaptive Chosen Ciphertext Attack, Lecture Notes in Comput. Sci., 1998。
-
- 【修定版的注一】 本课程期末考试为笔试，语音中凡提到“大作业”的地方均忽略之。
- 【修定版的注二】 凡原始文献，仅作课外参阅材料，不作学习要求。

公钥加密方案(14)

- *Cramer-Shoup*公钥加密方案：算法
-
  - G是素q阶循环群, g_1、g_2是G中的任意两个元素，H是某个单向散列函数.
  - **密钥生成算法*KG***(q,g¹,g²,K)：
  - $x_1,x_2,y_1,y_2,z \xleftarrow{\$} F_q$;
  - $c \leftarrow g_1^{x1}g_2^{x2}$; $d \leftarrow g_1^{y1}g_2^{y2}$; $h \leftarrow g_1^{z}$;
  - $pk \leftarrow (c,d,h)$; $sk \leftarrow (x_1,x_2,y_1,y_2,z)$;

  - **加密算法*E***(pk, M), $M \in G$：
  - $r \xleftarrow{\$} F_q$;
- $u_1 \leftarrow g_1^{r}$; $u_2 \leftarrow g_2^{r}$;
- $e \leftarrow Mh^{r}$;
- $T \leftarrow \boldsymbol{H}(u_1,u_2,e)$;
- $v \leftarrow c^{r}d^{rT}$;
- output(u_1,u_2,e,v);

解密算法 $D(sk,Y)$, $Y=(u_1, u_2, e, v)$：

$T \leftarrow H^{K}(u_1,u_2,e)$;

if $v = u_1^{x1+Ty1}u_2^{x2+Ty2}$

then

$M \leftarrow e(u_1^{z})^{-1}$

else $M \leftarrow$“错误”；

output(M);

- 解密算法的正确性：
- $u_1^{x1+Ty1}u_2^{x2+Ty2} = g_1^{(x1+Ty1)r}g_2^{(x2+Ty2)r} = (g_1^{x1}g_2^{x2})^{r}(g_1^{y1}g_2^{y2})^{rT} = c^{r}d^{rT} = v$;
- $u_1^{z} = (g_1^{r})^{z} = (g_1^{z})^{r} = h^{r}$;

公钥加密方案(15)

- *Cramer-Shoup*公钥加密方案: 安全性

- 若群族$\{G_{g(k),q(k)}: G_{g(k),q(k)}$是素$q(k)$阶循环群，$k\to\infty\}$上的判定性
- *Diffie-Hellman*问题难解，即任何*P.P.T*算法***A***都有
- $|P[A(g(k),u,v,w)=1|1\leqq x,y\leqq q(k), u=g(k)^x, v=g(k)^y, w=g(k)^{xy}]$
- $-P[A(g(k),u,v,w)=1|1\leqq x,y,w\leqq q(k), u=g(k)^x, v=g(k)^y, w=g(k)^w]|$
- $\leqq O(2^{-k})$， $k\to\infty$，
- 则*Cramer-Shoup*方案具有CCA-安全性。

公钥加密方案(16)

- *Cramer-Shoup*公钥加密方案: 安全实现

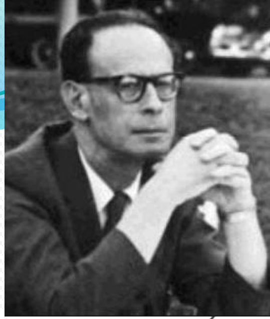
- 实现之一、
- 群族$\{G_{g,q}: G_{g,q}$是F_p^*的q阶循环子群，$q \to \infty\}$；
- 方案的运算是$mod\ p$的整数乘法运算。

- 实现之二、
- 群族$\{G_{g,q}: G_{g,q}$是有限域F_p上的椭圆曲线$E_{A,B}$上的q阶循环子群，$q \to \infty\}$：
- $E_{A,B} = \{(x,y): x,y \in F_p, y^2 = x^3 + Ax + B\}$
- 方案的运算是$E_{A,B}$上的“加法”运算：

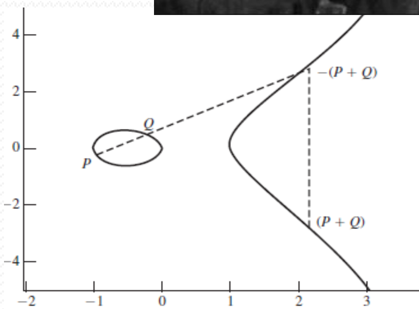
- 单向散列函数H采用当前的业界标准算法，如MD-5和SHA等。

以上*Cramer-Shoup*方案的实现都具有CCA-安全性。

附：椭圆曲线的故事和椭圆曲线密码学简介



- 有限域F_p上的椭圆曲线是由F_p上的两个参数A、B确定的集合
- $$E_{A,B} = \{(x,y): x,y \in F_p,\ y^2 = x^3 + Ax + B\}$$
- 即不定方程$y^2 = x^3 + Ax + B$在F_p上的解(x,y)的集合。



- 一、（连续复变量）椭圆曲线的历史梗概
- 1. 二元双周期函数~椭圆函数~复平面上的半纯函数P(z);
- 2. 椭圆函数P(z)满足非线性微分方程，其中a和b是有周期确定的特殊函数：
- $$(dP/dz)^2=P(z)^3+aP(z)+b$$
- 3. 映射λ：z→(P(z),dP/dz)是一条所谓全纯曲线，称为椭圆曲线。
- 二、有限域上的椭圆曲线$E_{A,B}$是复椭圆曲线的代数类比
- 1. $E_{A,B}$是一个加法群；
- 2. $E_{A,B}$上加法运算相关的离散对数问题难解：
- 不存在具有平均多项式时间复杂度的算法，在任何椭圆曲线上以
- 曲线参数A和B、曲线上的点(x,y)及(x_0,y_0)为输入，算出正整数N，使
- $$(x,y)=(x_0,y_0)+\ldots+(x_0,y_0)=N(x_0,y_0)$$
- 3. $E_{A,B}$上还具有更丰富的代数结构及其相关的难解型问题，例如Weil-pairing
- 用以构造*IBE*方案(2000年~)和同态保密计算协议(2009~)等全新的安全协议

椭圆曲线密码学(ECC)是当前理论创新最活跃、应用最为丰富多彩的信息安全分支之一。