基于认证的高效公钥加密算法

康 立, 唐小虎, 范 佳
(西南交通大学信息安全与国家计算网格实验室, 四川成都 610031)

摘 要: 2003 年, Gentry 提出基于认证的公钥加密方案. 在基于认证的公钥加密方案中, 第三方对认证申请者的公钥和/或身份进行签名, 并将签名作为认证发送给申请者, 申请者保存该认证作为解密时的部分私钥. 接收方对密文解密需要同时拥有第三方对其公钥和/或身份的认证和接收方公钥对应的私钥, 因此基于认证的加密方案同时具备基于身份加密方案的公钥可认证性和传统公钥方案中的私钥免撤销性. 本文提出一种高效、紧凑的基于认证的公钥混合加密算法, 新算法能在非随机预言机模型下被证明满足选择密文攻击安全.

关键词: 公钥加密; 基于认证加密; 非随机预言机模型
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2008) 10-2055-05

Efficient Certificate-based Public-key Encryption Scheme

KANG Li, TANG Xiao-hu, FAN Jia
(*Information Security and National Grid Computing Laboratory, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*)

Abstract: In 2003, Gentry proposed a certificate-based public-key encryption (CBE) scheme. In CBE scheme, a third part signs a certification on an applicant's public key or identity and sends the certification to the applicant, the applicant saves it and uses it as a partial private key (decryption key). A receiver needs the certification from the third party and his own public-private keys to decrypt a ciphertext, so CBE scheme combines the best aspects of identity-based encryption (implicit certification) and public-key encryption (no key escrow). We present an efficient and tight certificate-based public-key hybrid encryption scheme, which can be proved satisfying adaptive chosen ciphertext attack security without random oracle.

Key words: public-key encryption; certificate-based encryption; without random oracle model

1 引言

在传统基于公钥基础设施的加密方案中, 认证中心对用户公钥的认证是方案的核心, 它包括公钥证书的发放、维护、撤销和更新. 信息发送者要发送加密消息首先需要查看并验证接收方公钥证书.

基于身份密码方案的概念于 1984 年由 Shamir 提出[1], 在基于身份的密码方案中, 信息发送者不需要从用户公钥证书队列中获得用户公钥, 只需使用接收方身份信息来代替公钥. 而接收方要解密密文, 必需向可信任的第三方证明身份并获得身份对应的私钥. 向第三方证明身份的过程可以视为是对其身份(公钥)的认证. 2001 年 Boneh 和 Franklin 给出了第一个安全且高效的基于身份的加密算法[2], 该算法的安全性基于随机预言机模型.

2003 年, Gentry 提出基于认证加密方案的概念[3]. Gentry 提出将用户身份和/或公钥的认证作为一部分私钥, 用户私钥作为另一部分私钥, 只有同时掌握这两部分私钥才能完成密文的解密. 对比基于身份加密方案和传统公钥加密方案, 基于认证的加密方案具有以下特点:

(1) 基于认证的加密方案无需私钥撤销, 因为这里的认证只作为部分私钥, 另一部分私钥由用户自己选择、保存. 由于认证只是部分私钥, 因此分发时用户和第三方之间不需要安全信道, 即暴露部分私钥信息不影响系统安全性, 这样简化了安全要求有利于实际实施、应用;

(2) 基于认证的加密方案对用户认证的撤销变得简单, 只需对认证附加过期时间, 如果新周期中用户需要证书, 他必须再次向第三方申请认证.

(3) 降低了对第三方(认证者)的安全信任要求, 此时第三方只生成部分私钥, 因此无需担心第三方像基于身份密码方案中一样能够解密用户密文、代用户进行签名.

Gentry 利用 Boneh 和 Franklin 基于身份的加密算法[2]在随机预言机模型下实现了基于认证的加密算法[3]. 由于随机预言机要求对任意输入, 预言机的输出是随机独立均匀分布, 这一要求在真实环境中较难实现, 因此在随机预言机模型下证明安全的算法在实际应用时

收稿日期: 2007-08-10; 修回日期: 2008-05-04
基金项目: 西南交通大学博士创新基金; 全国优秀博士学位论文作者专项资金资助项目(No. 200341)

并不能保证安全.

2005 年, Waters 提出了一种基于身份的加密算法[4], 该算法的安全证明不需要随机预言机. 2006 年, Morillo 和 Rafols 利用 Waters 基于身份的加密算法构造了在非随机预言机模型下证明安全的基于认证的加密算法(MR 算法)[5].

本文基于 Waters、Kiltz 等基于身份的加密算法[4,6]给出一种新的基于认证的混合加密算法, 新算法能在非随机预言机模型下直接规约为双线性判定离散对数问题(BDDH), 新算法与 MR 算法相比更为紧凑、高效. 新算法为密钥封装算法和对称加密算法的混合加密算法. 混合加密算法对被加密消息没有长度限制, 更适用于长消息的加密, 而直接加密算法要求被加密消息满足一定长度限制.

2 基于认证的加密方案及其安全要求

2.1 基于认证的加密方案

基于认证的加密方案由下述五个算法组成:

系统建立 Setup: 由第三方生成系统参数< MPK, MSK >, 公布系统公钥 MPK, 保留系统私钥 MSK.

生成公私钥 SetKeyPair: 用户用系统公钥 MPK 生成自己的公私钥对< PK, SK> .

认证 Certify: 用户向第三方申请认证, 提交< ID, PK >, 第三方用用户身份 ID, PK, MPK, MSK 和约定的认证有效期生成用户公钥认证 Cert 并发送给用户.

加密 Enc: 信息发送者用接收方身份 ID, 公钥 PK 和第三方公钥 MPK, 加密消息 M 返回密文 C.

解密 Dec: 密文 C 的接收者用身份 ID, 公私钥对< PK, SK> , 第三方公钥 MPK 和认证信息 Cert, 应用解密算法恢复明文 M.

2.2 安全模型

由下述两个攻击者与挑战者的 Game 定义基于认证的公钥加密方案的安全模型:

基于认证的公钥加密方案可抵抗两类攻击:

Game 1: 未认证用户攻击.

系统建立: 挑战者运行系统建立算法 Setup, 获得系统公钥 MPK 和系统私钥 MSK, 将 MPK 发送给攻击者.

询问阶段 1: 攻击者能够适应性的进行如下两类询问:

(1) 认证询问: 攻击者给出任意< ID, PK, SK> 要求挑战者给出< ID, PK> 对应的认证;

(2) 解密询问: 攻击者给出任意< ID, PK, SK, C> , 要求挑战者返回相应的明文 M .

挑战阶段: 攻击者给出< ID^*, PK^*, SK^*, M_0, M_1> . 挑战者随机选择 β 返回 $\boldsymbol{C}^*$ = Enc< ID^*, PK^*, M_β, MPK > .

询问阶段 2: 除了认证询问< ID^*, PK^*, SK^* > 和解密询问< ID^*, PK^*, SK^*, C^* > 外, 攻击者能够像询问阶段 1 一样适应性的进行询问.

猜测: 攻击者返回对 β 的猜测值 $\beta' \in \{0,1\}$. 攻击者在 $\beta'=\beta$ 时赢得 Game, 我们定义攻击者 A_1 的优势为:

$$Adv_{A_1} = |\Pr[\beta' = \beta] - 1/2| .$$

Game 2: 第三方(认证者)攻击.

系统建立: 挑战者运行系统建立算法 Setup(生成的参数与 Game1 中独立), 获得系统公钥 MPK 和系统私钥 MSK, 挑战者生成随机的用户公私钥对< PK^*, SK^* > , 将< MPK, MSK, PK^* > 发送给攻击者.

询问阶段 1: 攻击者能够适应性的进行解密询问: 攻击者给出任意< ID, PK^*, C> , 要求挑战者返回相应的明文 M.

挑战阶段: 攻击者给出< ID^*, PK^*, M_0, M_1> . 挑战者随机选择 β 返回 $\boldsymbol{C}^*$ = Enc< ID^*, PK^*, M_β, MPK> .

询问阶段 2: 除了解密询问< ID^*, PK^*, $\boldsymbol{C}^*$ > 外, 攻击者能够像询问阶段 1 一样适应性的进行询问.

猜测: 攻击者返回对 β 的猜测值 $\beta' \in \{0,1\}$. 攻击者在 $\beta'=\beta$ 时赢得 Game, 我们定义攻击者 A_2 的优势为:

$$Adv_{A_2} = |\Pr[\beta' = \beta] - 1/2| .$$

定义 1 如果攻击者 A_1 和 A_2 在上述 Game 1 或 Game 2 中不能取得多项式时间下不可忽略的优势, 那么基于认证的加密算法是适应性选择密文攻击安全的(IND-CBE-CCA).

2.3 Pairing 运算

G, G_1 为阶为素数 p 的群, 有双线性 Pairing 映射 $e: G \times G \rightarrow G_1$ 满足:

(1) 双线性: $e(g_1^a, g_1^b) = e(g_1, g_1)^{ab}$;

(2) 非退化性: 对任意 $g \in G$ 有 $e(g,g) \neq 1$;

(3) 可计算性: 存在高效的算法对任意 $g^a, g^b \in G$ 计算 $e(g^a, g^b)$.

2.4 困难问题

群中变化(modified)双线性判定 Diffie-Hellman(mBDDH)难题.

给定阶为素数 p 的群 G, 生成元 g 和 $g^a, g^{a^2}, g^b, g^c \in G$; a, b, c 在 Z_p 中均匀随机选择, T 在 G_1 中随机选择, 挑战者随机选择 β, 如果 β= 1 挑战者给出< $g^a, g^{a^2}, g^b, g^c, g, Z = e(g,g)^{abc}$> , 如果 β= 0 挑战者给出< $g^a, g^{a^2}, g^b, g^c, g, Z = T$> . 攻击者猜测 β', 攻击者在 $\beta'=\beta$ 时赢得 Game, 定义攻击者 A 的优势为:

$$Adv_A = |\Pr[\beta' = \beta] - 1/2|$$

定义 2 如果没有攻击者在多项式时间内能以不可忽略的优势判定群中 mBDDH 问题, 则 mBDDH 难题在群

G 中成立.

当已知参数中去掉 g^{a^2}, 则上述困难问题变为群中的双线性判定 Diffie-Hellman(BDDH) 难题. 在文献[6]中 Kiltz 证明了 mBDDH 问题的强度界于 BDDH 问题和 2-BDDHI 问题之间.

定义 **3**　如果没有攻击者在多项式时间内能以不可忽略的优势判定群中 BDDH 问题, 则 BDDH 难题在群 G 中成立.

2.5　算法定义

对称加密算法: 加密算法 E 和解密算法 D 满足对任意密钥 k 和消息 M, 有 $M = D_k(E_k(M))$. 假设对随机选择的 k, M_0 和 M_1, $E_k(M_0)$ 和 $E_k(M_1)$ 对攻击者是不可区分的.

消息认证码 MAC: 输入消息 C 和密钥 k, 输出 $t = MAC_k(C)$. 假设攻击者给出 C^*, 挑战者给出(每一个 C^* 每次对应随机的 k^*) $< t^* = MAC_{k^*}(C^*), C^* >$, 攻击者不能给出 $< t = MAC_k^*(C), C >$ 且满足 $C \neq C^*$.

密钥分割算法 KDF: 对任意密钥 k, $KDF(k) = (k_1, k_2)$, k_1 用于对称加密算法, k_2 用于消息认证码. 假设随机的 $KDF(k)$ 和 (k_1, k_2) 对攻击者是不能区分的.

3　基于认证的加密算法

系统建立 Setup: 设 G 和 G_1 为阶为素数 p 的群, g 为 G 上生成元, 双线性 Pairing 映射 $e: G \times G \rightarrow G_1$ 是可以高效计算的. 抗碰撞的 Hash 函数 $H_1: \{0,1\}^* \rightarrow \{0,1\}^n$, $H_2: G \rightarrow Z_p$.

在 Z_p 中随机选择 a, 在 G 中随机选择 g_2, u', u_i, $i = \{1, \cdots, n\}$, h. 计算: $g_1 = g^a$. 系统主私钥 MSK 为 (a); 主公钥 MPK 为 $(g, g_1, g_2, u', u_1, u_2, \cdots u_n, h, H_1, H_2)$.

生成公私钥 SetKeyPair: 用户利用系统公钥并随机选择 $x \in Z_p$ 生成自己的公私钥对 $< PK, SK > = (g_1^x, x)$.

认证 Certify: 用户给出 $< ID, PK >$, 认证者计算 $v = H_1(ID, PK)$, v 是长为 n 的比特串, 设 v_i 为 v 的第 i 个比特值, 认证者在 Z_p 中随机选择 r, 给出用户 $< ID, PK >$ 的认证信息 $Cert_{ID,PK} = (Cert_1, Cert_2, Cert_3)$:

$$Cert_{ID,PK} = (Cert_1, Cert_2, Cert_3) = \left(g_2^a \left(u' \prod_{i \in \{i \mid v_i = 1\}} u_i\right)^r, g^r, h^r\right)$$

加密 Enc: 信息发送者计算 $v = H_1(ID, PK)$, 在 Z_p 中随机选择 t, 利用认证者的 MPK 计算:

(1) $k = e(g_1^x, g_2)^t$.

(2) $C_0 = g^t$, $\tau = H_2(C_0)$

(3) $C_1 = \{(u' \prod_{i \in \{i \mid v_i = 1\}} u_i)(h^\tau)\}^t$

(4) $(k_1, k_2) = KDF(k)$

(5) $C_2 = E_{k_1}(M)$

(6) $C_3 = MAC_{k_2}(C_0, C_1, C_2)$

将 $C = (C_0, C_1, C_2, C_3)$ 发送给接收者.

解密 Dec: 密文接收者利用私钥 x、认证信息 $Cert_{ID,PK}$, 先计算 $\tau = H_2(C_0)$, 对密文进行解密:

$$k = \left(\frac{e(Cert_1 Cert_3^\tau, C_0)}{e(Cert_2, C_1)}\right)^x$$

$$(1) \quad = \left(\frac{e(g_2^a (u' \prod_{i \in \{i \mid v_i = 1\}} u_i)^r h^\tau, g^t)}{e(g^r, (u' \prod_{i \in \{i \mid v_i = 1\}} u_i)^t h^\tau)}\right)^x$$

$$= e(g_2^a, g^t)^x = e(g_1^x, g_2)^t$$

(2) $(k_1, k_2) = KDF(k)$

(3) $M = D_{k_1}(C_2)$

验证 $C_3 = MAC_{k_2}(C_0, C_1, C_2)$, 如果成立接受此消息, 否则拒绝.

4　效率及安全性分析

4.1　效率分析

新算法中, 加密和解密一共需要 3 次 pairing 运算, 而 MR 算法中需要 5 次. 新算法使用了混合加密方法, 减少了 MR 方法中对加密消息长度的限制. 就通信量而言, 每次加密 MR 需要 $(5p + 128)$ bits, p 是 G 的阶, 128 为 MAC 码的输出长度; 而新方案只需 $(3p + 128)$ bits. 对比两个方案, 无论在计算量上, 还是通信量上, 新方案都有显著的提高.

新算法在公钥参数、密文通信量和计算效率与 Kiltz 基于身份的混合加密算法[6]相当的条件下实现了基于认证的加密算法. 对比文献[6]算法, 新算法不仅能抵抗未认证用户对系统的攻击, 还能抵抗第三方(认证者)对系统的攻击, 后一性质是文献[6]所不具备的.

表 **1**　方案比较

方案	第三方公钥(p)	用户公钥(p)	通信量(bits)	Pairing 计算量
新 CBE 方案	$n+5$	1	$3p+128$	3
MR CBE 方案	$n+6$	2	$5p+128$	5

说明: 用户公钥和第三方公钥数目为素数 p 阶群中元素个数. Pairing 运算是方案中最费时的运算, 这里比较三个方案中 pairing 运算次数.

4.2　安全性证明

这里给出新算法抵抗适应性选择密文攻击的启发式证明.

定理 **1**　假设在 2.5 算法定义中给出的对称加密算法 $< E, D >$、消息认证码 MAC 算法和密钥分割算法 KDF 是安全的, mBDDH 困难问题和 BDDH 困难问题在群 G 中成立, 那么上述基于认证的公钥加密算法是适应性选择密文攻击安全的.

我们将在 Game1 和 Game2 中分别证明上述定理成立.

证明 1: 如果有攻击者 A_1 能在 Game1 中攻破上述基于认证的公钥加密算法, 那么存在攻击者 B_1 能攻破 mBDDH 问题.

给定阶为素数 p 的群 G, 生成元 g 和 $g^a, g^{a^2}, g^b, g^c \in G$; a, b, c 在 Z_p 中均匀随机选择, T 在 G_1 中随机选择, 挑战者随机选择 β, 如果 $\beta=1$ 挑战者给出 $<g^a, g^{a^2}, g^b, g^c, g, e(g,g)^{abc}>$, 如果 $\beta=0$ 挑战者给出 $<g^a, g^{a^2}, g^b, g^c, g, T>$. 攻击者猜测 β', 在 $\beta'=\beta$ 时赢得 Game. B_1 将利用 A_1 来猜测 β', B_1 作为挑战者给 A_1 提供 Game1 的仿真环境, 具体执行如下.

系统建立: B_1 在 0 到 n 之间选择 l, n 维向量 $(\boldsymbol{x}_i)$ 和 $\boldsymbol{x}'$ 属于 0 到 $w-1$ ($w=2(q_a+q_d)$), q_a 和 q_d 分别为认证提问次数和解密询问次数. n 维向量 $(\boldsymbol{y}_i)$ 和 $\boldsymbol{y}'$ 属于 Z_p. 抗碰撞的 Hash 函数 $H_1: \{0,1\}^* \to \{0,1\}^n$, $H_2: G \to Z_p$. 令 $g_1=g^a$ 和 $g_2=g^b$, 定义 $F(v)$ 和 $J(v)$:

$$F(v)=\boldsymbol{x}'+\sum_{i\in\{i\mid v_i=1\}}\boldsymbol{x}_i-lw \bmod p$$

$$J(v)=\boldsymbol{y}'+\sum_{i\in\{i\mid v_i=1\}}\boldsymbol{y}_i \bmod p$$

令 $\tau^*=H_2(g^c)$, 相应的定义 $u'=g_2^{x'-lw}g^{y'}g_1^{-\tau^*}$, $u_i=g_2^{x_i}g^{y_i}$ 和 $h=g_1$. 系统公钥为: $(g, g_1, g_2, u', u_1, \cdots u_n, h, H_1, H_2)$, 系统私钥为: (a) (未知). 可以看出, 在分布上仿真参数设置与真实环境相同. B_1 将系统公钥发送给攻击者 A_1.

认证询问: 攻击者 A_1 给出任意 $<ID, PK, SK>$, B_1 计算 $v=H_1(ID, PK)$ 和 $F(v)$, 如果 $F(v)$ 等于零终止仿真. 否则在 Z_p 中随机选择 r 计算:

$$Cert_{ID,PK}=(Cert_1, Cert_2, Cert_3)$$
$$=\left(g_1^{-J(v)/F(v)}\left(u'\prod_{i\in\{i\mid v_i=1\}}u_i\right)^r\left(g^{a^2(-\tau^*)}\right)^{-1/F(v)},\ g_1^{-1/F(v)}g^r, g^{-a^2/F(v)}g_1^r\right)$$

这里 v 可以视为 Waters 基于身份加密算法[4]中的身份, 根据 Waters[4] 和 Kiltz[6] 证明中用户私钥生成的推导, 上式为关于 $v=H_1(ID, PK)$ 的有效认证.

这里约定, 如果攻击者已经询问过某公钥 $<ID, PK>$ 的认证, 将不再对 $<ID, PK, SK, C>$ 进行解密询问.

解密询问: 攻击者给出任意 $<ID, PK, SK, C>$, B_1 计算 $v=H_1(ID, PK)$ 和 $F(v)$, 如果 $F(v)$ 不等于零, B_1 按照认证询问中方法生成认证 $Cert_{ID,PK}$, 计算:

$$k=\left(\frac{e(Cert_1 Cert_3^{\tau}, C_0)}{e(Cert_2, C_1)}\right)^x$$

完成解密. 如果 $F(v)$ 等于零那么

$$C_1=\{(u'\prod_{i\in\{i\mid v_i=1\}}u_i)(g_1^{\tau})\}^t=(g_2^{F(v)}g^{J(v)}g_1^{\tau-\tau^*})^t$$
$$=(g^{J(v)}g_1^{\tau-\tau^*})^t,$$

由于已知 g^t, $J(v)$, 我们可以得到 g_1^t ($\tau=\tau^*$ 情况可以忽略), 从而有 $k=e(g_1^x, g_2)^t=e(g_1^t, g_2)^x$, 得到了会话私钥, 完成解密.

挑战阶段: 攻击者 A_1 给出 $<ID^*, PK^*, SK^*, M_0, M_1>$. B_1 计算 $v^*=H_1(ID^*, PK^*)$ 和 $F(v^*)$, 如果 $F(v^*)$ 不等于零终止仿真, 否则 B_1 随机选择 β 给出挑战密文:

(1) $k^*=Z^x$

(2) $C_0^*=g^c$, $\tau^*=H_2(C_0^*)$

$$C_1^*=g^{cJ(v^*)}$$

(3)
$$=(g_2^{F(v^*)}g^{J(v^*)}g_1^{\tau^*-\tau^*})^c$$
$$=\{(u'\prod_{i\in\{i\mid v_i=1\}}u_i)(g_1^{\tau^*})\}^c$$

(4) $(k_1^*, k_2^*)=KDF(k^*)$

(5) $C_2^*=E_{k_1^*}(M_\beta)$

(6) $C_3^*=MAC_{k_2^*}(C_0^*, C_1^*, C_2^*)$

将 $C^*=(C_0^*, C_1^*, C_2^*, C_3^*)$ 发送给接收者.

询问阶段 2: 除了认证询问 $<ID^*, PK^*, SK^*>$ 和解密询问 $<ID^*, PK^*, SK^*, C^*>$ 外, 攻击者能够像询问阶段 1 一样适应性的进行询问.

可以看出当 Z 为 $e(g,g)^{abc}$ 时, C^* 是关于 M_β 的正确密文, 当 Z 为 T 时, C^* 是随机的. 攻击者 A_1 最后返回对 β 的猜测值 β', 如果 $\beta'=\beta$, B_1 返回 mBDDH 挑战者 $\beta'=1$, 反之返回 $\beta'=0$. 如果攻击者 A_1 能在 Game1 下攻破上述基于认证的加密方案, 那么 B_1 作为挑战者能攻破 mBDDH 困难问题, 而 mBDDH 是被证明的困难问题, 故基于认证的加密方案在 Game1 下是安全的.

上述证明中要求攻击者给出的 $<ID, PK, SK>$ 应是合法的用户公私钥对.

证明 2: 如果有攻击者 A_2 能在 Game2 中攻破上述基于认证的公钥加密方案, 那么存在攻击者 B_2 能攻破 BDDH 问题

给定阶为素数 p 的群 G, 生成元 g 和 $g^a, g^b, g^c \in G$; a, b, c 在 Z_p 中均匀随机选择, T 是在 G_1 中随机选择, 挑战者随机选择 β, 如果 $\beta=1$ 挑战者给出 $<g^a, g^b, g^c, g, e(g,g)^{abc}>$, 如果 $\beta=0$ 挑战者给出 $<g^a, g^b, g^c, g, T>$. 攻击者来猜测 β', 攻击者在 $\beta'=\beta$ 时赢得 Game. B_2 将利用 A_2 来猜测 β', B_2 作为挑战者给 A_2 提供 Game2 的仿真环境, 具体执行如下.

系统建立: B_2 选择抗碰撞的 Hash 函数 $H_1: \{0,1\}^* \to \{0,1\}^n$, $H_2: G \to Z_p$, 随机选择 $x \in Z_p$, 令 $g_1=g^x$, $g_2=g^b$ 和 $h=g_2$. 选择 l 在 0 到 n 之间, n 维向量 $(\boldsymbol{x}_i)$ 和 $\boldsymbol{x}'$ 属于 0 到 $w-1$ ($w=2(q_d)$), n 维向量 $(\boldsymbol{y}_i)$ 和 $y\boldsymbol{y}'$ 属于 Z_p. 定义 $F(v)$ 和 $J(v)$:

$$F(v) = x' + \sum_{i \in \{i \mid v_i = 1\}} x_i - lw \bmod p$$

$$J(v) = y' + \sum_{i \in \{i \mid v_i = 1\}} y_i \bmod p$$

$\tau^* = H_2(g^c)$, 相应的定义 $u' = g_2^{x' - lw} g^{y'} g_2^{-\tau^*}$ 和 $u_i = g_2^{x_i} g^{y_i}$. 系统公钥为: $(g, g_1, g_2, u', u_1, u_2, \cdots u_n, h, H_1, H_2)$, 系统私钥为: (χ). B_2 选择挑战的用户公私钥对 $< PK^*, SK^* >$ 为 $< g^{a\chi}, a$(未知)$>$. 可以看出, 在分布上仿真参数设置与真实环境相同. B_2 将系统公钥, 私钥和挑战用户公钥 $PK^* = g^{a\chi}$ 发送给攻击者 A_2.

解密询问: 攻击者 A_2 给出任意 $< ID, PK^*, C >$, B_2 计算:

$$C_1 = \{(u' \prod_{i \in \{i \mid v_i = 1\}} u_i)(g_2^{\tau})\}^t = (g_2^{F(v)} g^{J(v)} g_2^{\tau - \tau^*})^t$$

由于已知 g^t, $F(v)$, $J(v)$, 我们可以得到 g_2^t, 有 $k = e(g_1^{\chi}, g_2)^t = e(g_2^t, g_1)^{\chi}$, 得到了会话私钥, 完成解密.

挑战阶段: 攻击者 A_2 给出 $< ID^*, M_0, M_1 >$. B_2 计算 $v^* = H(ID^*, PK^*)$ 和 $F(v^*)$, 如果 $F(v^*)$ 不等于零终止仿真. 否则 B_2 随机选择 β 给出挑战密文, 此部分与 Game1 中"挑战阶段"完全相同, 最后将 $C^* = (C_0^*, C_1^*, C_2^*, C_2^*)$ 发送给攻击者.

询问阶段 2: 除了解密询问 $< ID^*, PK^*, C^* >$ 外, 攻击者能够像询问阶段 1 一样适应性的进行询问.

可以看出当 Z 为 $e(g, g)^{abc}$ 时, C^* 是关于 M_β 的正确密文, 当 Z 为 T 时, C^* 是随机的. 攻击者 A_2 最后返回对 β 的猜测值 β', 如果 $\beta' = \beta$, B_2 返回 BDDH 挑战者 $\beta' = 1$, 反之返回 $\beta' = 0$. 如果攻击者 A_2 能在 Game2 下攻破上述基于认证的加密方案, 那么 B_2 作为挑战者能攻破 BDDH 困难问题, 而 BDDH 是公认的困难问题, 故基于认证的加密方案在 Game2 下是安全的.

在非随机预言机模型下上述基于认证的公钥加密算法被证明在适应性选择密文攻击 Game1 和 Game2 模型中规约为 mBDDH 困难问题和 BDDH 困难问题, 新算法能抵抗选择密文攻击.

5　结论

Gentry 提出了基于认证的公钥加密方案, 并用 Boneh 和 Franklin 的身份加密算法实现了第一个基于认证的公钥加密算法. Morillo 和 Rafols 第一个实现了在非随机预言机模型下证明安全的基于认证的公钥加密算法. MR 的算法基于 Waters 身份加密算法. 本文在 Waters、Kiltz 等基于身份加密算法的基础上给出了一个新的基于认证的加密算法, 新算法在非随机预言机模型下被证明能抵抗适应性选择密文攻击. 新算法在结构上和 Waters 身份加密更为接近, 计算效率和通信量与 MR 算法相比有了较大的提高, 加密和解密一共需要 3 次 Pairing 运算, 而 MR 的方案需要 5 次; 每次加密 MR 需要 $(5p + 128)$ bits 通信量, 而新方案只需 $(3p + 128)$ bits 通信量. 另外, 新算法使用了密钥封装算法和对称加密算法的混合密码体制, 这样减少了对被加密消息长度的要求, 更适应于实际实施、应用.

参考文献:

[1] Shamir A. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology, Crypto' 84, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1985, 196: 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[A]. Advances in Cryptology, Crypto 2001, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 2001, 2139. 213-229.

[3] Gentry C. Certificate-based encryption and the certificate revocation Problem[A]. Advances in Cryptology, EuroCrypt 2003, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 2003, 2656. 272-291.

[4] Waters B. Efficient identity-based encryption without random oracles[A]. Advances in Cryptology, EuroCrypt 2005, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 2005, 3494. 114-127.

[5] P Morillo, C Rafols. Certificate-based encryption without random oracles[EB/OL]. Cryptology ePrint Archive, Report 2006/012, 2006. http://eprint.iacr.org/2006/012.ps.

[6] Kiltz E. Direct chosen-ciphertext secure identity-based encryption in the standard model with short ciphertext[EB/OL]. Cryptology ePrint Archive, Report 2006/122, 2006. http://eprint.iacr.org/2006/122.pdf

作者简介:

康　立　男. 1982 年 1 月生于四川成都. 2004 年在西南交通大学获得工学学士学位. 现为西南交通大学硕博连读研究生, 主要研究方向为信息安全.

E-mail: kangli@mars.swjtu.edu.cn

唐小虎　男. 教授、博士生导师、IEEE 会员. 1972 年 7 月出生于四川遂宁. 主要研究方向为编码理论、信息安全.