标准模型下选择密文安全的基于身份加密方案

刘振华[1,2] 胡予濮[1] 张襄松[2]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[1]
(西安电子科技大学应用数学系 西安 710071)[2]

摘 要 Waters在欧密2005上提出的基于身份加密方案是选择明文安全的,这就使得该方案很难应用于一些安全性要求较高的环境中。针对这一问题,设计了一个标准模型下选择密文安全的基于身份的加密扩展方案。该扩展方案基于Waters的方案,其密文中增加一个附加信息,而扩展方案是选择密文安全的,所以解决了Waters方案仅达到选择明文安全的问题。在标准模型下,扩展方案的安全性归约为判定性双线性Diffie-Hellman困难假设。安全性分析表明,扩展方案抵抗自适应选择密文攻击是不可区分的。

关键词 公钥密码,基于身份加密,选择密文安全,双线性对,标准模型
中图法分类号 TP309 **文献标识码** A

Chosen Ciphertext Secure Identity-based Encryption in the Standard Model

LIU Zhen-hua[1,2] HU Yu-pu[1] ZHANG Xiang-song[2]
(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)[1]
(Department of Applied Mathematics, Xidian University, Xi'an 710071, China)[2]

Abstract In Eurocrypt 2005, Waters' identity-based encryption scheme suffers from a drawback that the scheme only guarantees chosen plaintext security, which hampers its applications in higher security level environments. A chosen ciphertext secure identity-based encryption scheme was proposed to remedy this drawback. The proposed encryption scheme was regarded as the extended version of Waters' scheme with only one additional element in the ciphertext, and guaranteed chosen ciphertext security. The extended scheme's indistinguishability against adaptive chosen ciphertext attacks was proven in the standard model and rested on the hardness of the decisional bilinear Diffie-Hellman intractability assumption.

Keywords Public key cryptography, Identity-based encryption, Chosen ciphertext security, Bilinear maps, Standard model

为了简化公钥证书管理,Shamir[1]在1984年提出了基于身份的公钥密码系统。在这个公钥密码系统中,用户的公钥可以由用户的身份(姓名、身份证号、电话号码、Email地址等)公开计算得到,而与用户身份相匹配的私钥则是由可信的密钥生成中心KGC(Key Generator Center),利用系统主密钥和用户的身份信息计算得到。但是多年以来,高效实用的基于身份加密方案一直是一个公开问题。直到2001年,才由Boneh和Franklin[2]基于椭圆曲线上的双线性对提出了第一个高效且实用的基于身份加密方案,该方案在随机预言机模型下可证明是安全的。随后,许多基于身份的加密、签名和密钥协商方案被提出。虽然随机预言机模型[3]在密码方案安全性证明中起到了关键作用,但是有学者指出在该模型下的安全性证明实际上是一种启发式的证明,在实际应用中并不安全[4,5]。从而在随机预言机模型下安全的基于身份的加密方案[2]不一定实际安全。因此在标准模型(即不借助于随机预言机模型)下设计加密方案是十分有意义的[6-8]。

Waters[7]在欧密2005上提出了第一个标准模型下的完全安全的基于身份加密方案,但是该方案仅能达到选择明文安全(IND-CPA),很难应用于一些安全性要求较高的环境。在公钥密码中,加密方案的安全性目标可以分为3种:单向性、不可区分性和非延展性;敌手的攻击模型也可以分为3种:选择明文攻击、非适应性选择密文攻击和适应性选择密文攻击。组合安全性目标和攻击模型,可以获得不同级别的安全性,其中强度最大、最重要的是适应性选择密文攻击的不可辨识性(IND-CCA2)和适应性选择密文攻击的非延展性(NM-CCA2),而二者被证明是等价的[9]。因此在标准模型下设计选择密文安全的基于身份的加密方案具有现实意义。

本文在Waters方案和Cramer-Shoup方案[10]的基础上,提出了一个基于身份的加密扩展方案,在密文中增加了一个附加信息,使扩展方案达到了选择密文安全。在标准模型下

到稿日期:2009-02-20 返修日期:2009-04-27 本文受973国家基础研究发展规划基金项目(2007CB311201),国家自然科学基金(60673072,60803149)资助。

刘振华(1978-),男,博士研究生,讲师,主要研究方向为密码学与信息安全,E-mail:zh_liu@mail.xidian.edu.cn;胡予濮(1955-),男,教授,博士生导师,主要研究方向为密码学与信息安全;张襄松(1981-),女,博士研究生,主要研究方向为最优化算法和密码算法。

扩展方案的选择密文安全性归约为判定性双线性 Diffie-Hellman 困难假设。

1 预备知识

1.1 双线性映射

定义 1 令 G 和 G_T 为素数 p 阶循环乘法群，g 是 G 的生成员。假设 G 和 G_T 群中的离散对数问题都是困难问题。双线性对是指满足下列性质的一个映射 $e:G\times G\to G_T$：

1) 双线性性。$e(g^a,h^b)=e(g,h)^{ab}$，a,b 是 Z_p^* 中的元素，g,h 是 G 中的元素。

2) 非退化性。存在的元素的 g,h，使得 $e(g,h)\neq 1$。

3) 可计算性。对 G 中所有的元素 g,h，存在有效的算法计算 $e(g,h)$。

1.2 DBDH 问题

定义 2 设 G 和 G_T 为素数 p 阶循环乘法群，g 是 G 的生成员。对于任意 $a,b,c\in Z_p^*$ 和二进制比特 $\beta\in\{0,1\}$，如果 $\beta=1$，输出五元组 $(g,g^a,g^b,g^c,e(g,g)^{abc})$，否则输出五元组 (g,g^a,g^b,g^c,Z)，其中 $Z\in G_T$，则 (G,G_T,e) 上的 Decisional Bilinear Diffie-Hellman(DBDH)问题是输出 β 的值。

如果存在算法 $\mathscr{C}$，使 $|\Pr[\mathscr{C}(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-\Pr[\mathscr{C}(g,g^a,g^b,g^c,Z)=1]|\geqslant 2\varepsilon$ 成立，则称算法 $\mathscr{C}$ 解决 DBDH 问题的优势是 ε。如果没有以至少 ε 的优势在时间 t 内解决 DBDH 问题的算法 $\mathscr{C}$，则称 (ε,t)-DBDH 困难假设成立。

1.3 基于身份的加密方案及其安全性

1.3.1 基于身份的加密方案

一个基于身份的加密方案由以下 4 个算法组成。

Setup：由 KGC 完成，输入安全参数 k，输出主密钥 msk 和系统参数 $params$。KGC 保密 msk，公开 $params$。

Extract：输入一个用户的身份 u，KGC 计算用户私钥 d_u 并通过安全方式发送给这个用户。

Encrypt：输入系统参数 $params$，接收者身份 u，消息 M，输出密文 $\sigma=Encrypt(M,u)$。

Decrypt：输入系统参数 $params$，密文 σ，接收者 u 的私钥 d_u，输出明文消息 M 或符号“⊥”表示解密失败。

1.3.2 形式化安全模型

基于身份的加密方案的安全模型[2]。在敌手 $\mathscr{A}$ 和挑战者 $\mathscr{C}$ 之间进行下面的游戏。

Initial：挑战者 $\mathscr{C}$ 输入安全参数 k，运行 Setup 算法，将系统参数 $params$ 发送给敌手 $\mathscr{A}$。

Phase 1：敌手 $\mathscr{A}$ 执行多项式次数的适应性询问，即每次询问可以依赖于以前询问的结果，这些询问包括：

Extract 询问：$\mathscr{A}$ 选择一个身份 u，$\mathscr{C}$ 计算相应身份的私钥 $d_u=Extract(u)$，并将结果发送给 $\mathscr{A}$。

Decrypt 询问：$\mathscr{A}$ 选择一个身份 u 和一个密文 σ。$\mathscr{C}$ 首先计算 $d_u=Extract(u)$，然后计算 $Decrypt(\sigma,d_u)$，最后返回明文 M 或符号“⊥”表示解密失败。

Challenge 阶段：$\mathscr{A}$ 决定结束第一阶段的询问，生成两个相同长度的明文 M_0,M_1 和希望挑战的身份 u^*，其中 u^* 不能是已经执行过 Extract 询问的身份。$\mathscr{C}$ 随机选择 $\gamma\in\{0,1\}$，计算 $\sigma^*=Encrypt(M_\gamma,u^*)$，并将结果 σ 发送给 $\mathscr{A}$。

Phase 2：$\mathscr{A}$ 像在 Phase 1 那样执行多项式有界次询问，但是不能对 u^* 执行 Extract 询问，也不能对密文 σ^* 执行 Decrypt 询问。

Guess：$\mathscr{A}$ 输出一个值 γ' 作为对 γ 的猜测。如果 $\gamma'=\gamma$，则 $\mathscr{A}$ 赢得游戏。

$\mathscr{A}$ 的优势定义为 $Adv(\mathscr{A})=|2\Pr[\gamma'=\gamma]-1|$。

定义 3(IND-IBE-CCA2) 如果敌手在时间 t 内做至多 q_e 次私钥提取询问和 q_d 次解密询问，它攻破一个基于身份的加密方案的优势至多是 ε，则称该加密方案是 (ε,t,q_e,q_d) 语义安全的。

2 基于身份的加密方案

下面给出扩展的基于身份的加密方案，由以下 4 个算法组成。

Setup：令群 (G,G_T)，g 是 G 的生成元，双线性映射 $e:G\times G\to G_T$，见第 1 节定义。无碰撞 Hash 函数 $H_m:\{0,1\}^*\to\{0,1\}^m$。KGC 随机选取主私钥 $\alpha\in Z_p$，计算 $g_1=g^\alpha$，随机选择 $g_2,u',v'\in G$ 和向量 $U=(u_i)_n$，$V=(v_j)_m$，其中 u_i,v_j $(i=1,\cdots,n;j=1,\cdots,m)$ 从群 G 中随机选取。系统公共参数 $params=(g,g_1,g_2,u',v',U,V,H_m)$，系统主私钥是 g_2^α。

Extract：令 $u\in\{0,1\}^n$，表示某个用户的身份，$u[i]$ 表示 u 的第 i 个比特。随机选择 $r_u\in Z_p$，生成相应的私钥 $d_u=(d_{u,1},d_{u,2})=(g_2^\alpha)(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_u},g^{r_u})$。

Encrypt：为了发送消息 $M\in G_T$ 给用户 u，随机选取 $r_m\in Z_p$，计算 $\sigma_1=Me(g_1,g_2)^{r_m}$，$\sigma_2=g^{r_m}$，$\sigma_3=(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_m})$，然后计算 $m=H_m(\sigma_1,\sigma_2,\sigma_3,u)\in\{0,1\}^m$，其中 $m[j]$ 表示 m 的第 j 比特，最后计算 $\sigma_4=(v'\prod_{j=1}^{m}v_j^{m[j]})^{r_m})$。则密文是 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$。

Decrypt：收到密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 后，检查密文是否满足下式：

$$e(\sigma_2,u'\prod_{i=1}^{n}u_i^{u[i]}\cdot v'\prod_{j=1}^{n}v_j^{[j]})=e(g,\sigma_3\sigma_4)$$

其中，$m=H_m(\sigma_1,\sigma_2,\sigma_3,u)\in\{0,1\}^m$，$m[j]$ 表示 m 的第 j 比特。如果不满足，则拒绝 σ；否则返回 $M\leftarrow\sigma_1 e(d_{u,2},\sigma_3)e(d_{u,2}^{-1},\sigma_2)$。

正确性：假设 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 是关于用户 u 的合法密文，方案的正确性可由下式直接得到：

$$\begin{aligned}\sigma_1\frac{e(d_{u,2},\sigma_3)}{e(d_{u,1},\sigma_2)}&=Me(g_1,g_2)^{r_m}\frac{e(g^{r_u},(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_m})}{e(g_2^\alpha(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_u},g^{r_m})}\\&=Me(g_1,g_2)^{r_m}\frac{e(g^{r_u},(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_m})}{e(g_2^\alpha,g^{r_m})((u'\prod_{i=1}^{n}u_i^{u[i]})^{r_u},g^{r_m})}\\&=M\end{aligned}$$

效率分析：扩展方案中，加密算法不需要双线性对运算，其中 $e(g_1,g_2)$ 可以预运算；解密算法中先验证密文是否有效，合法后返回解密明文，需要 4 个双线性对运算，一个群 G 上元素的逆运算和至多 $n+m+1$ 次乘法运算。与文献[7]相比，扩展方案密文增加一个群 G 上的元素，在密文验证中增加两个双线性对运算，但是在第 3 节将证明扩展方案能达到最高安全级别——IND-CCA2。与文献[11](其安全性基于很强的困难问题假设——Truncated Decision q-Augmented Bilinear Diffie-Hellman Exponent(q-ABDHE)问题)相比，该

方案的安全性基于更一般的困难问题假设——判定性双线性 Diffie-Hellman(DBDH)问题。

3 基于身份的加密方案的安全证明

扩展方案的保密性由下面的定理 1 给出。

定理 1 在标准模型下，如果(ε',t')-DBDH 困难假设成立，则改进方案是(ε,t,q_e,q_d)-语义安全的，其中 $\varepsilon'=\varepsilon/(32q_d(q_e+q_d)(n+1)(m+1))$，$t'=t+\mathcal{O}((q_e+q_d)t_e+(nq_e+(n+m)q_d)t_m+q_dt_p)$，且 t_e，t_m 和 t_p 分别表示群 G 上计算一次乘法，一次指数和进行一次对运算所需要的时间。

证明：假设存在(ε,t,q_e,q_d)-敌手 $\mathcal{A}$ 能够攻击扩展的加密方案，则可以构造一个算法 C 至少以 ε' 的优势在至多时间 t' 内解决 DBDH 问题，与(ε',t')-DBDH 困难假设成立矛盾。

$\mathcal{C}$ 收到一个随机的 DBDH 问题实例$(g,A=g^a,B=g^b,C=g^c,Z\in G_T)$，其任务是输出 β 的一个猜测 β'，作为判断 $Z=e(g,g)^{abc}$ 是否成立。$\mathcal{C}$ 把敌手 $\mathcal{A}$ 作为子程序，并扮演游戏中的挑战者回答敌手的询问。

Setup：C 设置 $l_1=2(q_e+q_d)$ 和 $l_2=2q_d$，随机选择整数 k_1,k_2,x',y',z',w'，其中 $0\leqslant k_1\leqslant n$，$0\leqslant k_2\leqslant m$，$x'\in Z_{l_1}$，$z'\in Z_{l_2}$，$y',w'\in Z_p$；再随机选择向量 $X=(x_i)_n$，$Y=(y_i)_n$，$Z=(z_j)_m$ 和 $W=(w_j)_m$，其中 $x_i\in Z_{l_1}$，$z_j\in Z_{l_2}$，$y_i,w_j\in Z_p$。

为简便，对于身份 u 和消息 m，定义函数[12]

$$F(u)=(p-l_1k_1)+x'+\sum_{i=1}^{n}u[i]x_i,J(u)=y'+\sum_{i=1}^{n}u[i]y_i$$

$$K(m)=(p-l_2k_2)+z'+\sum_{i=1}^{m}m[j]z_j,L(m)=w'\sum_{i=1}^{m}m[j]w_j$$

然后，$\mathcal{C}$ 设置公开参数如下：

$$g_1=A,g_2=B,u'=g_2^{p-l_1k_1+x'}g^{y'},v'=g_2^{p-l_2k_2+z'}g^{w'}$$

$$u_i=g_2^{x_i}g^{y_i}(1\leqslant i\leqslant n),v_j=g_2^{z_j}g^{w_j}(1\leqslant j\leqslant m)$$

在这种设置下，主私钥是 $g_2^a=g^{ab}$（$\mathcal{C}$ 不知道），且公开参数与实际的公开参数具有相同的概率分布。对于任意的身份 u 和消息 m，有 $u'\prod_{i=1}^{n}u_i^{u[j]}=g_2^{F(u)}g^{J(u)}$，$v'\prod_{j=1}^{m}v_j^{m[j]}=g_2^{K(m)}g^{L(m)}$。

Extract 询问：考虑询问身份 u 的私钥。虽然 $\mathcal{C}$ 不知道主私钥，假设 $F(u)\neq 0 \bmod p$，$\mathcal{C}$ 仍能模拟出有效私钥

$$d_u=(d_{u,1},d_{u,2})=(g_1^{-J(u)/F(u)}(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_u},g_1^{-1/F(u)}g^{r_u})$$

记 $\tilde{r}_u=r_u-a/F(u)$。当且仅当 $F(u)\neq 0 \bmod l_1$（蕴含 $F(u)\neq 0 \bmod p$）[7,11]，上述模拟的私钥是有效的，由于

$$\begin{aligned}d_{u,1}&=g_1^{-J(u)/F(u)}(u'\prod_{i=1}^{n}u_i^{u[i]})^{r_u}\\&=g_2^{a}(g_2^{F(u)}g^{J(u)})^{-a/F(u)}(g_2^{F(u)}g^{J(u)})^{r_u}\\&=g_2^{a}(g_2^{F(u)}g^{J(u)})^{r_u-a/F(u)}=g_2^{a}(u'\prod_{i=1}^{n}u_i^{u[i]})^{\tilde{r}_u}\end{aligned}$$

和 $d_{u,2}=g^{r_u-a/F(u)}=g^{\tilde{r}_u}$，为简便，这里仅考虑充分条件 $F(u)\neq 0 \bmod p$。如果 $F(u)=0 \bmod p$，则 $\mathcal{C}$ 简单停止并猜测 β 的值 β'。

Decrypt 询问：考虑询问接收者 u 收到密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$。$\mathcal{C}$ 首先执行密文验证：

$$e(\sigma_2,u'\prod_{i=1}^{n}u_i^{u[i]})^{r_u}\cdot v'\prod_{j=1}^{m}v_j^{m[j]})=e(g,\sigma_3\sigma_4)$$

其中，$m=H_m(\sigma_1,\sigma_2,\sigma_3,u)\in\{0,1\}^m$，$m[j]$ 表示 m 的第 j 比特。如果不满足，则拒绝 σ 并返回“$\perp$”；否则，$\mathcal{C}$ 解密如下：

1）$\mathcal{C}$ 对身份 u 执行 Extract 询问，获得 u 的私钥 d_u（假设 $F(u)\neq 0 \bmod p$），然后运行 Decrypt 算法，并返回明文。

2）如果 $F(u)=0 \bmod p$，$\mathcal{C}$ 尽力完成解密。对某 $r_m\in Z_p$，$\sigma_2=g^{r_m}$，$\sigma_4=v'\prod_{j=1}^{m}v_j^{m[j]})^{r_m}$，$m=H_m(\sigma_1,\sigma_2,\sigma_3,u)\in\{0,1\}^m$。假设，$K(m)\neq 0 \bmod l_2$，$\mathcal{C}$ 能提取 $g_2^{r_m}=(\sigma_4/\sigma_2^{L(m)})^{1/K(m)}$，从而计算出 $e(g_1,g_2^{r_m})$ 和 $M=\sigma_1/e(g_1,g_2^{r_m})$。

3）如果 $F(u)=0 \bmod l_1$ 且 $K(m)=0 \bmod l_2$，则 $\mathcal{C}$ 简单停止并猜测 β 的值 β'。

解决 DBDH 问题：经过多项式有界次上述询问后，$\mathcal{A}$ 选择提交挑战身份 u^* 和两个等长的明文 $M_0,M_1\in G_T$。如果 $F(u^*)\neq 0 \bmod p$ 或者已经询问过 u^* 的私钥，$\mathcal{C}$ 停止并猜测 β 的值 β'。否则，$\mathcal{C}$ 随机选择 $\gamma\in\{0,1\}$ 和 $r_u\in Z_p$，模拟明文 M_γ 的密文如下：计算 $\sigma_1^*=M_\gamma\cdot Z,\sigma_2^*=C,\sigma_3^*=C^{J(u^*)}$，计算 $m_\gamma=H_m(\sigma_1^*,\sigma_2^*,\sigma_3^*,u^*)\in\{0,1\}^m$。如果，$K(m_\gamma)\neq 0 \bmod p$，$C$ 简单停止并猜测 β 的值 β'。否则，$\mathcal{C}$ 计算 $\sigma_4=C^{L(m_\gamma)}$，返回密文 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*)$。$\mathcal{A}$ 像在第一阶段一样，继续进行第二阶段的各种询问，除了对 u^* 和 σ^* 的解密询问。在游戏的最后，$\mathcal{A}$ 输出 γ' 作为对 γ 的猜测。如果 $\gamma'=\gamma$，$\mathcal{C}$ 回答 $\beta'=1$，意味着 $Z=e(g,g)^{abc}$；否则，回答 $\beta'=0$，意味着 Z 是 G_T 中的随机元素。

概率估算：先估算 $\mathcal{C}$ 在整个模拟过程中不停止的概率。为了能让整个模拟过程完整地完成，在 Extract 询问中要求对所有的身份 u 有 $F(u)\neq 0 \bmod l_1$，在 Decrypt 询问时要求敌手提交的二元组(σ,u)中有 $F(u)\neq 0 \bmod l_1$ 或者 $K(m)\neq 0 \bmod l_2$，其中 $m=H_m(\sigma_1,\sigma_2,\sigma_3,u)\in\{0,1\}^m$，在挑战密文阶段要求 $F(u^*)=0 \bmod p$ 和 $K(m_\gamma)=0 \bmod p$。令 $u_1,u_2,\cdots,u_{q_I}$ 表示在 Extract 询问，或者 Decrypt 询问中出现过的身份，但不涉及挑战身份；并令 $m_1,m_2,\cdots,m_{q_M}$ 表示在 Decrypt 询问中出现过的消息（Hash 值），但不涉及挑战值 $m_\gamma=H_m(\sigma_1^*,\sigma_2^*,\sigma_3^*,u^*)$。显然有 $q_I\leqslant q_e+q_d$ 和 $q_M\leqslant q_d$。定义事件：

$A^*:F(u^*)=0 \bmod p,A_i:F(u_i)\neq 0 \bmod l_1(1\leqslant i\leqslant q_I)$

$B^*:K(m_\gamma)=0 \bmod p,B_j:K(m_j)\neq 0 \bmod l_2(1\leqslant j\leqslant q_M)$

因此，挑战者 $\mathcal{C}$ 在整个模拟过程中不停止的概率为：

$$\Pr[\neg abort]\geqslant\Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A^*\wedge\bigwedge_{j=1}^{q_M}B_j\wedge B^*]$$

由于函数 F 和 K 是独立选择的，因此事件 $\bigwedge_{i=1}^{q_I}A_i\wedge A^*$ 和事件 $\bigwedge_{j=1}^{q_M}B_j\wedge B^*$ 是独立的。假定 $l_1(n+1)<p$，那么 $0\leqslant l_1k_1\leqslant p$，则 $F(u)=0 \bmod p$ 蕴含 $F(u)=0 \bmod l_1$。如果 $F(u)=0 \bmod l_1$，则存在唯一的 k_1，其中 $0\leqslant k_1\leqslant n$，满足 $F(u)=0 \bmod p$。

由于 k_1,x' 和 X 的随机性，有：

$$\begin{aligned}\Pr[A^*]&=\Pr[F(u^*)=0 \bmod p]=\Pr[F(u^*)=0 \bmod p\\&\wedge F(u^*)=0 \bmod l_1]=\Pr[F(u^*)=0 \bmod p]\\&[\Pr[F(u^*)=0 \bmod p|\wedge F(u^*)=0 \bmod l_1]=\\&1/(l_1(n+1))\end{aligned}$$

同时也有：

$$\Pr[\bigwedge_{i=1}^{q_I}A_i|A^*]=1-\Pr[\bigvee_{i=1}^{q_I}\neg A_i|A^*]\geqslant 1-\sum_{i=1}^{q_I}\Pr[\neg A_i|A^*]$$

对于不同身份 u_1 和 u_2，事件 $F(u_1)=0 \bmod l_1$ 和 $F(u_2)=0 \bmod l_1$ 是独立的。令 $l_1=2(q_e+q_d)$ 和 $l_2=2q_d$。作为一种特殊情形，对任意 i，事件 A_i 和 A^* 是独立的，可得：

$$\Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^*]=\Pr[A^*]\Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*]=\Pr[A^*](1-\Pr[\bigvee_{i=1}^{q_I} \neg A_i \mid A^*])\geqslant \Pr[A^*](1-\sum_{i=1}^{q_I}\Pr[\neg A_i \mid A^*])=\frac{1}{(l_1(n+1))}\cdot(1-\frac{q_I}{l_1})\geqslant \frac{1}{(l_1(n+1))}\cdot(1-\frac{(q_e+q_d)}{l_1})=\frac{1}{(4(q_e+q_d)(n+1))}$$

同理，有：

$$\Pr[\bigwedge_{j=1}^{q_M} B_j \wedge B^*]=\Pr[B^*]\Pr[\bigwedge_{j=1}^{q_M} B_j \mid B^*]\geqslant \frac{1}{(l_2(m+1))}\cdot(1-\frac{q_d}{l_2})=\frac{1}{(4q_d(m+1))}$$

所以有：

$$\Pr[\neg abort]\geqslant \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{j=1}^{q_M} B_j \wedge B^*]=\Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^*]\Pr[\bigwedge_{j=1}^{q_M} B_j \wedge B^*]=\frac{1}{(16q_d(q_e+q_d)(n+1)(m+1))}$$

若 $Z=e(g,g)^{abc}$，则敌手 $\mathcal{A}$ 将以 $\varepsilon+1/2$ 的概率猜对比特 γ；否则，若 Z 是随机的，$\mathcal{A}$ 没有任何优势猜对比特 γ，即它猜对 γ 的概率是 1/2。从而 $\mathcal{C}$ 解决 DBDH 问题的优势至少为 $\varepsilon/(32q_d(q_e+q_d)(n+1)(m+1))$。

时间复杂度分析：对 C 的运行时间的估算主要来自于应答询问需要的指数、乘法和双线性对运算。每次 Extract 询问至多需要 $\mathcal{O}(1)$次指数运算和 $\mathcal{O}(n)$次乘法运算。每次 Decrypt 询问至多需要 $\mathcal{O}(1)$次指数运算，$\mathcal{O}(n+m)$次乘法运算和 $\mathcal{O}(1)$次双线性对运算。所以 $\mathcal{C}$ 的时间复杂度为 $t'=t+\mathcal{O}((q_e+q_d)t_e+(nq_e+(n+m)q_d)t_m+q_dt_p)$。

结束语 针对 Waters 基于身份的基本加密方案仅达到选择明文安全的问题，提出了一个自适应选择密文安全的基于身份的加密扩展方案。与 Waters 加密方案相比，扩展方案增加了 1/3 密文长度，更重要的是提高了安全级别，适合应用于安全性要求较高的环境。在标准模型下，扩展方案的语义安全性归约为判定性双线性 Diffie-Hellman 困难假设。本文的结果为进一步具体的安全实施提供了有力的理论依据。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proc. Crypto 1984. LNCS 196. Berlin: Springer-Verlag, 1984:47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairings[C]// Proc. Crypto 2001. LNCS 2139. Berlin: Springer-Verlag, 2001:213-229

[3] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols[C]// Proc. of the first ACM conference on computer and communications security. New-York: ACM Press, 1993:62-73

[4] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4):557-594

[5] Nishioka M, Komatsu N. A note on the random oracle methodology[J]. IEICE Transaction Fundamentals, 2008, E91-A(2): 650-663

[6] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10):1743-1756

[7] Waters R. Efficient identity based encryption without random oracles[C]// Proc. Eurocrypt 2005. LNCS 3494. Berlin: Springer-Verlag, 2005:114-127

[8] Dent A W, Libert B, Paterson K G. Certificateless encryption schemes strongly secure in the standard model[C]// Proc. of the 11th International Workshop on Practice and Theory in Public Key Cryptography 2008. LNCS 4939. Berlin: Springer-Verlag, 2008:344-359

[9] Bellare M, et al. Relations among notions of security for public-key encryption schemes[C]// Proc. Crypto 1998. LNCS 1462. Berlin: Springer-Verlag, 1998:26-45

[10] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[C]// Proc. Crypto 1998. LNCS 1462. Berlin: Springer-Verlag, 1998: 13-25

[11] Gentry C. Practical Identity - based encryption without random oracles[C]// Proc. Eurocrypt 2006. LNCS 4004. Berlin: Springer-Verlag, 2006:445-464

[12] Paterson K G, Schuldt J C. Efficient identity based signatures secure in the standard model[C]// Proc. of the 11th Australasian Conference Information Security and Privacy 2006. LNCS 4058. Berlin: Springer-Verlag, 2006:207-222

(上接第 58 页)

[3] Siganos G, Faloutsos M, Faloutsos P, et al. Power laws and the AS-level Internet topology[J]. IEEE/ACM Trans. on Networking, 2003, 11(4):514-524

[4] Zhou S, Mondragon R J. The rich-club phenomenon in the Internet topology [J]. IEEE Communication Letters, 2004, 8(3): 180-182

[5] 赵海，徐野，苏威积，等. Internet 网络效能及其物理特征量分析[J]. 东北大学学报：自然科学版，2006，27(11)：1216-1219

[6] 张君，赵海，周艳. Internet 路由级节点的度与核数的关系[J]. 东北大学学报：自然科学版，2008，29(5)：653-656

[7] Gao J B, Rubin I. Statistical properties of multiplicative multifractal processes in modeling telecommunications traffic streams [J]. Electronics Letter, 2000, 36:101-102

[8] 魏进武，邹江兴，陈庶樵. 网络流量的联合多重分形模型及特性分析[J]. 电子学报，2004，32(9)：1459-1463

[9] 罗恒端，吴诗其. 数据分组网中自相似业务模型的研究进展[J]. 通信学报，2002，23(7)：107-115

[10] Yook S H, Jeong H, Barabasi A L. Modeling the Internet's large-scale topology [J]. Applied Physical Sciences, 2002, 99(21):13382-13386

[11] Song C, Havlin S, Makse H A. Self-similarity of complex networks [J]. Nature, 2005, 433:392-395

[12] 肯尼斯·法尔科内. 分形几何[M]. 沈阳：东北大学出版社，2003