

适应性选择密文安全的可公开验证加密方案

杜卫东^{1*}, 杨晓元^{1,2}, 张祥火¹, 王绪安¹

(1. 武警工程大学 网络与信息安全武警部队重点实验室, 西安 710086; 2. 武警工程大学 信息安全研究所, 西安 710086)

(* 通信作者电子邮箱 pepertual@sina.com)

摘要:在密钥托管、电子公平交易、可公开分享和安全多方计算中,对可公开验证加密有广泛的应用需求,但是已有的可公开验证加密方案或者是选择明文安全的,或者是在随机预言机模型下是选择密文安全的,显然不满足诸多复杂应用环境的安全需求。在对已有可公开验证加密方案的分析 and 现实应用需求的基础上,结合 CS 加密方案,利用非交互性零知识证明协议提出了一个新的可公开验证的加密方案,新方案使得除发送方和接收方外的任何第三方都可以验证密文的有效性,且不会泄露消息的其他任何信息。最后,相对于随机预言机模型,在标准模型下证明了新方案是适应性选择密文安全的。

关键词:可公开验证;CS 方案;零知识证明协议;标准模型;适应性选择密文安全

中图分类号:TP391 **文献标志码:**A

Adaptively-chosen ciphertext secure and publicly verifiable encryption scheme

DU Weidong^{1*}, YANG Xiaoyuan^{1,2}, ZHANG Xianghuo¹, WANG Xu'an¹

(1. Key Laboratory of Network and Information Security under Chinese Armed Police Force, Engineering University of Chinese Armed Police Force, Xi'an Shaanxi 710086, China;

2. Institute of Information Security, Engineering University of Chinese Armed Police Force, Xi'an Shaanxi 710086, China)

Abstract: There is a great demand for publicly verifiable encryption in key escrow, optimistic fair exchange, publicly verifiable secret sharing and secure multiparty computation, but the current schemes are either chosen plaintext secure or chosen ciphertext secure in the random oracle model, which obviously are not secure enough to be applied in the complicated circumstances. Based on the analysis of the current schemes and application of the reality, this paper proposed a new publicly verifiable encryption scheme by combining the CS encryption scheme with the non-interactive zero knowledge proof protocol. The new scheme enabled any third party other than the sender and receiver to verify the validity of the ciphertext, but leaked no information about the message. Finally, without using the random oracle, the adaptively chosen ciphertext security of the scheme is proved in the standard model.

Key words: publicly verifiable; CS scheme; zero knowledge proof protocol; standard model; adaptively chosen ciphertext security

0 引言

可公开验证加密系统在现实中有广泛的应用需求:1)在密钥托管^[1-2]中,委托方需将自己的私钥加密后发送给托管方,为了防止欺骗,托管方需要对密文中的私钥的真实性进行验证。2)在可公开验证秘密分享^[3]中,秘密的分发者与 n 个共享者分享一个秘密,为了使除秘密分享者的第三方也能确保秘密被合法地分发,验证者需要对秘密份额的正确性进行验证。3)在电子公平交易^[4-5]中,交易双方需要交换电子数据,必须保证双方都得到对方的数据,或者都得不到对方的数据。为了防止其中一方意外中止交换,双方在交换数据之前,必须使用可信第三方的公钥加密自己的数据,这样对方可以对密文中数据的有效性进行验证。4)在网络中传递敏感信息,需要对消息进行加密,而中间节点为了过滤非法的数据流,减少网络的拥塞,需要对传递的密文的合法性进行验证。在上述的可公开验证的加密系统中都要求验证者除了能够对密文进行验证外,不能获得关于消息的其他任何信息。

Stadler^[3]提出了可公开验证加密的概念,随后 Bellare

等^[6],Young 等^[2]分别提出了面对密钥托管、电子商务等具体应用的可公开验证的加密方案,但是文献[7]指出,这些方案都不是选择密文安全的。文献[8]中虽然提出了选择密文安全的可公开验证加密方案,却只能在随机预言机模型下证明是安全的。Canetti 等^[9]研究证明,在随机预言机模型中可证明安全的方案在用密码学中的哈希函数实现时却是不安全的。所以构造标准模型下可证明安全的加密方案已成为目前的主要趋势。2012 年,Nieto 等^[10]提出了在标准模型下安全的可公开验证加密方案,但是该方案对于验证者却是选择明文安全的,显然不满足诸多复杂应用环境的安全性需求。根据对以上方案不足的分析 and 现实的应用需求,本文提出了一个在标准模型下可证明适应性选择密文安全的可公开验证加密方案。

可公开验证的加密系统可以利用一个三方协议^[11]来实现,其中证明者 P 是一般公钥加密系统中的密文发送方,Receiver 是一般公钥加密系统中的消息接收方。验证者 V 可以是任意第三方,能够验证 P 发送给 Receiver 的密文是否与先前对消息的承诺具有关系 R ,但是 V 并不能从密文中提取消息

收稿日期:2012-10-25;修回日期:2012-12-03。 基金项目:国家自然科学基金资助项目(61272492,61103231,61103230)。

作者简介:杜卫东(1988-),男,河北邯郸人,硕士研究生,主要研究方向:信息安全、密码学; 杨晓元(1959-),男,湖南湘潭人,教授,主要研究方向:信息安全、密码学; 张祥火(1988-),男,江西上饶人,硕士研究生,主要研究方向:信息安全、密码学; 王绪安(1981-),男,湖北公安人,讲师,硕士,主要研究方向:信息安全、密码学。

的任何其他信息。协议中公开的加密算法 E , 对秘密消息 m 的一个公开承诺和一个关系 R 是三方的公共输入。 V 根据 $(x, m) \in R$ 是否成立来验证密文的有效性。协议需要保证一个不合法的密文通过 V 的验证的概率是可忽略的, 而且, 除了密文隐藏的消息是否有效的以外, V 不能进一步获得消息的任何信息, 即该协议是零知识性的。

CS 方案^[12] 是适应性选择密文安全的经典加密方案, 发送方利用接收方的公钥生成对密文的一个验证值 v , 只有接收方可以用自己的私钥验证密文的有效性, 这就保证了该方案的选择密文安全性。但是, 其存在的缺点是, CS 方案不是可公开验证的。这使得其在前面提到的应用中受到了限制。

针对上述具体的应用需求, 本文在原 CS 的基础上提出了一个可公开验证的加密方案, 并且证明了新方案可公开验证性的完备性、有效性和零知识性, 最后, 本文证明了新方案的适应性选择密文安全性。

1 安全定义与组成模块

1.1 加密系统可公开验证性的安全性

下面给出加密系统可公开验证性的安全模型的形式化定义。

定义 1^[8] 设 R 是一个二分关系且 $L_R = \{x \mid \exists m: (x, m) \in R\}$ 。对关系 R 的一个可公开验证加密方案可以表示为一个三方协议 $\{P; V; Receiver\}$ 。其中: P 是证明者, 即密文的发送方; V 是密文的验证者; $Receiver$ 是密文的接收方; $V_p(E, x, l)$ 表示 V 与 P 对输入 (E, x, l) 交互后的输出, E 是一个公开的加密算法, $x \in L_R$, l 是一个安全参数。一个方案的可公开验证性是安全的, 如果满足下列条件:

1) 完备性。如果 P 和 V 诚实地执行协议, 那么对于任意的 $(E, D) \in G(1^l)$ 和任意 $x \in L_R$, $V_p(E, x, l) = \perp$ 的概率是可忽略的, 其中: D 是加密算法 E 对应的解密算法, 1^l 是输入安全参数的 1 元编码, $G(1^l)$ 表示一个概率多项式时间算法, \perp 表示协议因异常而中止。

2) 有效性。对所有的多项式时间 p , 所有的多项式时间算法 $Recover(\cdot)$, 所有充分大的 l , 以及所有的 $(E, D) \in G(1^l)$, 有

$$\Pr[(x, Recover(D, \delta)) \notin R, \delta \neq \perp, \\ \delta = V_p(E, x, l)] < 1/p(l)$$

3) 零知识性。对任意 V' , 存在一个多项式时间模拟器 $S_{V'}$ 以黑盒子的方式访问 V' 满足对任意的区分器 $A(\cdot)$, 所有的 $p(\cdot)$, 所有 $x \in L_R$, 和所有充分大的 l , 有

$$\Pr[A(E, x, \delta_i) = i, \delta_0 = S_{V'}(E, x, l), \delta_1 = V'_p(E, x, l), \\ i \in \{0, 1\}] < 1/2 + p(l)$$

1.2 密文不可区分性

对任一公钥加密方案 (K, E, D) , 如果满足

$$\text{adv}_A = 2 \times \Pr[(k_p, k_s) \leftarrow K(1^k), (m_0, m_1, s) \leftarrow A_1(k_p), \\ c = E(k_p, m_0, r): A_2(m_0, m_1, s, c) = b] - 1$$

是可忽略的, 则称该方案是多项式安全的或密文不可区分的。

密文不可区分性意味着, 如果敌手不能以不可忽略概率猜出 b 的值, 则该加密方案是安全的, 经证明这个结论反过来也成立, 即一个安全的加密方案是密文不可区分的。更进一步, 一个加密方案是适应性选择密文安全的, 则意味着敌手在既可以询问加密预言机, 又可以适应性选择密文来询问解密机器的情况下, 密文是不可区分的^[13]。

1.3 陷门承诺

设 G 是一个高阶循环群, $\langle g \rangle \subseteq \langle h \rangle \subseteq G$, 其中 g 和 h 生成 G 的高阶子群, 在 $\langle g \rangle$ 和 $\langle h \rangle$ 中计算离散对数是一个困难问题。 $\log_g h$ 的值未知。设 Alice 拥有秘密 x , 可以向 Bob 作如下承诺。Alice 随机选取整数 r , 向 Bob 发送 $C = \text{commit}(x, r) = g^x h^r$ 作为对 x 的承诺。因为 Alice 不知道 $\log_g h$, 所以不可能找到 $x_1 \neq x_2$ 满足 $\text{commit}(x_1, r_1) = \text{commit}(x_2, r_2)$ 。而即使 Bob 的计算能力是无限的, 也不可能从承诺 C 中提取关于秘密 x 的任何信息(无条件隐藏性)。如果 Alice 要欺骗 Bob, 则必须知道 $\log_g h$, 而这在计算上是不可行的。这就构成了一个陷门承诺^[14]。

1.4 零知识证明协议

设 $\langle g_1 \rangle \subseteq \langle h_1 \rangle$ 和 $\langle g_2 \rangle \subseteq \langle h_2 \rangle$ 为循环群, 在其中计算离散对数是一个困难问题。Alice 不知道 $\log_{g_i} h_i (i = 1, 2)$ 的值。下面的协议^[15] 允许 Alice 向 Bob 证明她知道满足 $y_1 = g_1^x h_1^r$ 和 $y_2 = g_2^x h_2^r$ 的 x, r_1, r_2 的值, 其中 y_1, y_2 是公开的。Alice 随机选取整数 w, w_1, w_2 , 计算出 $W_1 = g_1^w h_1^{w_1}, W_2 = g_2^w h_2^{w_2}, c = H(W_1 \parallel W_2), D = w - cx, D_1 = w_1 - cr_1, D_2 = w_2 - cr_2$ 。Alice 向 Bob 发送证据 (c, D, D_1, D_2) 。Bob 可以验证是否有 $c = H(g_1^D h_1^{D_1} g_2^{D_2} h_2^{D_2})$ 。记上述协议 $ZPK\{x, r_1, r_2 \mid y_1 = g_1^x h_1^{r_1} \wedge y_2 = g_2^x h_2^{r_2}\}$ 。这是一个完全零知识证明协议 (Zero-knowledge Proof of Knowledge, ZPK), 即使攻击者计算能力是无限的也不能提取 x 的任何信息。

1.5 CS 加密方案

CS 加密方案是少数几个在标准模型下证明适应性选择密文安全的高效加密方案之一。其安全性归约为循环群上的判定性 Diffie-Hellman 问题。其方案细节如下:

1) 密钥生成。 G 是一个阶为素数 q 的循环群。随机选择 $g_1, g_2 \in G$, 和 $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbf{Z}_q$ 。然后计算 $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^{z_1} g_2^{z_2}$ 。最后的公钥为 (g_1, g_2, c, d, h) , 私钥为 $(x_1, x_2, y_1, y_2, z_1, z_2)$ 。

2) 加密。给定一条消息 $m \in G$, 加密算法首先随机选择 $r \in \mathbf{Z}_q$, 然后计算:

$$u_1 = g_1^r, u_2 = g_2^r, e = h^r m, \delta = H(u_1, u_2, e), v = c^r d^{r_0}$$

其中 H 为抗碰撞的哈希函数, 最终的密文为 (u_1, u_2, e, v) 。

3) 解密。收到密文后, 解密算法首先计算 $\delta = H(u_1, u_2, e)$, 然后检验是否 $u_1^{x_1} u_2^{x_2} (u_1^{y_1} u_2^{y_2})^\delta = v$ 。如果等式成立, 则计算 $m = (u_1^{x_1} u_2^{x_2})/e$; 否则, 拒绝解密。

2 可公开验证加密方案

下面结合本文 1.3 节中介绍的完全零知识证明系统和 1.5 节中介绍的 CS 加密方案, 构造可公开验证的加密方案, 具体算法如下:

1) 密钥生成。系统确定一个额外的安全参数 l , 与原 CS 方案密钥生成算法相同, 计算出公钥 (g_1, g_2, c, d, h) , 私钥 $(x_1, x_2, y_1, y_2, z_1, z_2)$ 。

2) 加密。设 g, f 是群 G 的两个不相等的生成元。给定 $m \in G$, 加密算法随机选择 $n, r \in \mathbf{Z}_q$, 然后计算:

$$u_1 = g_1^r, u_2 = g_2^r, e = m^{-1} h^r, \delta = H(u_1, u_2, e), v = c^r d^{r_0}$$

最后发送方利用 $ZPK\{x, r_1, r_2 \mid y_1 = g_1^x h_1^{r_1} \wedge y_2 = g_2^x h_2^{r_2}\}$ 对明文进行承诺, 使得第三方可以验证密文的有效性。具体过程如下:

① 发送方公开对消息 m 的承诺 $M = g^m f^n$ 。

② 对 $i = 0, 1, \dots, l-1$, 其中 l 是安全参数, 发送方随机选取 $w_i \in_R \mathbf{Z}_q, \theta_i \in_R \mathbf{Z}_q$, 计算 $t_i = (g_1 g_2)^{w_i}, s_i = g^{h w_i} f^{\theta_i}, C = H(M \| u_1 \| u_2 \| v \| t_0 \| s_0 \| \dots \| t_{l-1} \| s_{l-1})$ 和 $\eta_i = w_i - c_i r$, $\delta_i = \theta_i - c_i e h \eta_i n$, 其中 c_i 是 C 的第 i bit。最终的密文为 $(u_1, u_2, e, v, M, C, \eta_0, \delta_0, \dots, \eta_{l-1}, \delta_{l-1})$ 。

这样中间接收者可以通过验证是否有 $C = H(M \| u_1 \| u_2 \| v \| (g_1 g_2)^{\eta_0} (u_1 u_2)^{c_0} \| (g^{1-c_0} M^{e_0 e})^{h \eta_0} \| \dots \| (g_1 g_2)^{\eta_{l-1}} (u_1 u_2)^{c_{l-1}} \| (g^{1-c_{l-1}} M^{e_{l-1} e})^{h \eta_{l-1}})$ 来确定密文的有效性。

3) 解密。接收方收到密文后, 解密算法首先计算 $\delta = H(u_1, u_2, e)$, 然后检验是否 $u_1^{x_1} u_2^{x_2} (u_1^{x_1} u_2^{x_2})^\delta = v$ 。如果等式成立, 则计算 $m = (u_1^{x_1} u_2^{x_2})/e$; 否则, 拒绝解密。

3 方案的公开验证性分析

3.1 方案公开验证性的完备性

证明 由定义知完备性保证诚实的证明者和验证者交互后输出异常的概率是可忽略的, 即诚实的证明者和验证者总是能够成功地执行该协议。由上述算法过程知:

$$\begin{aligned} (g_1 g_2)^{\eta_i} (u_1 u_2)^{c_i} &= (g_1 g_2)^{\eta_i} (g_1 g_2)^{c_i r} = \\ &= (g_1 g_2)^{\eta_i + c_i r} = (g_1 g_2)^{w_i} \\ (g^{1-c_i} M^{e_i e})^{h \eta_i} f^{\delta_i} &= (g^{1-c_i} (g^m f^n)^{e_i e})^{h \eta_i} f^{\delta_i} = \\ g^{[1-c_i + c_i m e] h \eta_i} f^{e_i e h \eta_i n + \delta_i} &= g^{[1-c_i + c_i m m^{-1} h] h \eta_i} f^{\delta_i} = \\ \left\{ \begin{array}{l} g^{h \eta_i} f^{\theta_i} \quad c_i = 0 \\ g^{h \eta_i + r} f^{\theta_i} \quad c_i = 1 \end{array} \right\} &= s_i \end{aligned}$$

3.2 方案公开验证性的有效性

证明 由定义知有效性保证恶意的证明者伪造证据 $x \notin L_R$, 并通过验证的概率小于 $1/p(l)$, 其中 p 是任意多项式, l 是安全参数, 即恶意的证明者欺骗诚实的验证者成功的概率是可以忽略的。假设恶意的证明者对明文的承诺为 $M' = g^{m'} f^{n'}$, 且 $M' \neq M$, 若恶意的证明者欺骗成功则有:

$$\begin{aligned} (g^{1-c_i} M'^{e_i e})^{h \eta_i} f^{\delta_i} &= g^{(1-c_i) h \eta_i} M'^{e_i e h \eta_i} f^{\delta_i} = s_i = \\ (g^{1-c_i} M^{e_i e})^{h \eta_i} f^{\delta_i} &= g^{(1-c_i) h \eta_i} M^{e_i e h \eta_i} f^{\delta_i} \end{aligned}$$

当 $c_i = 1$ 时, 由以上两式可得 $M' = M$, 但是 M, M' 是对 m 的陷门承诺, 证明者无法找到满足等式的 M' 。

当 $c_i = 0$ 时对于任意的 M' 都满足等式, 但是要使得最终的验证通过则有对于所有的 $i = 0, 1, \dots, l-1, c_i = 0$, 而其发生的概率为 2^{-l} , 显然 $2^{-l} < 1/p(l)$ 对于任意多项式 p 总是成立。当 l 足够大时, 恶意的证明者成功的概率是可以忽略的。所以该方案是有效的。

3.3 方案公开验证性的零知识性

证明 由定义知零知识性保证验证者与证明者之间的交互都可以用一个多项式时间模拟器来模仿, 即验证者除了接受 $x \in L_R$ 外, 不能获得关于消息的其他任何信息。在本文的方案中, M 是发送方对消息 m 的陷门承诺, 所以即使接收方具有无限的计算能力, 也不可能从 C 中提取任何信息; 又 r, n, w_i 是随机选择的, 所以验证者也无法从 η_i, δ_i 获得加密消息的任何信息。综上, 该可公开验证方案是零知识性的。所以验证者无法从密文元组 $(M, \eta_0, \delta_0, \dots, \eta_{l-1}, \delta_{l-1})$ 中获得关于消息的任何信息。

4 方案的安全性分析

4.1 判定性 Diffie-Hellman 问题

定义 2 设 G 是一个阶为素数 q 的群, 给定四元组 (g_1, g_2, u_1, u_2) , 判断其属于分布 $D = (g_1, g_2, g_1', g_2')$, 还是分布 $R = (g_1, g_2, g_1^0, g_2^1)$, 其中 $g_1, g_2 \in G, r, r_0, r_1 \in \mathbf{Z}_q$ 是随机选择的。

4.2 方案的安全性证明

为了证明方案在标准模型下的适应性选择密文安全性, 首先假设有一个可以攻破该加密系统的敌手, 然后本文证明可以利用该敌手解决判定性 Diffie-Hellman 问题。而判定性 Diffie-Hellman 问题是困难的, 与得出的结论矛盾, 所以不存在可以攻破该加密系统的敌手, 即本加密方案在标准模型下是适应性选择密文安全的。

证明矛盾的大体思路是: 首先构建一个模拟器来模拟加密预言机和解密预言机。如果模拟器使用 D 分布中的四元组来加密消息, 由于敌手可以攻破该加密系统, 则加密预言机输出的密文的分布与敌手的攻击中获得密文的分布相同, 进而敌手可以以不可忽略优势猜对 b 。如果模拟器使用 R 分布中的四元组来加密消息, 加密预言机输出的密文是非法的, 此时敌手猜对 b 的概率是可以忽略的, 即 b 独立于敌手的猜测。这样就可以利用敌手区分出 D 分布和 R 分布, 从而解决了判定性 Diffie-Hellman 问题。下面是证明的过程。

4.2.1 模拟器的构造

模拟器的密钥生成 使用给定的 g_1, g_2 , 模拟器随机选择 $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbf{Z}_q$, 并计算 $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^{z_1} g_2^{z_2}$ 。最后的公钥为 (g_1, g_2, c, d, h) , 私钥为 $(x_1, x_2, y_1, y_2, z_1, z_2)$ 。

加密预言机的模拟 当加密预言机使用 D 分布中的四元组来加密消息时, 模拟器随机选择 $g_1, g_2 \in G, r \in \mathbf{Z}_q$, 此时加密预言机的输入为 (g_1, g_2, g_1', g_2') 。对给定 m_0, m_1 , 加密预言机随机选择 $b \in (0, 1)$, 计算 $e = u_1^{x_1} u_2^{x_2} m_b^{-1}, \delta = H(u_1, u_2, e), v = u_1^{x_1} u_2^{x_2} (u_1^{x_1} u_2^{x_2})^\delta$, 其中: $u_1 = g_1', u_2 = g_2'$ 。

然后, 加密预言机用零知识证明协议对明文 m_b 进行承诺:

- 1) 加密预言机首先对消息 m_b 进行承诺, 计算出 $M = g^{m_b} f^n$ 。
- 2) 然后对 $i = 0, 1, \dots, l-1$, 其中 l 是密钥生成是确定的安全参数, 加密预言机随机选取 $w_i \in_R \mathbf{Z}_q, \theta_i \in_R \mathbf{Z}_q$, 计算 $t_i = (g_1 g_2)^{w_i}, s_i = g^{h w_i} f^{\theta_i}, C = H(M \| u_1 \| u_2 \| v \| t_0 \| s_0 \| \dots \| t_{l-1} \| s_{l-1})$ 和 $\eta_i = w_i - c_i r, \delta_i = \theta_i - c_i e h \eta_i n$, 其中 c_i 是 C 的第 i bit。

最终输出的密文为 $(u_1, u_2, e, v, M, C, \eta_0, \delta_0, \dots, \eta_{l-1}, \delta_{l-1})$ 。

当加密预言机使用 R 分布中的四元组来加密消息时, 模拟器随机选择 $g_1, g_2 \in G, r_0, r_1 \in \mathbf{Z}_q$, 此时加密预言机的输入为 (g_1, g_2, g_1^0, g_2^1) 。对给定 m_0, m_1 , 加密预言机随机选择 $b \in (0, 1)$, 计算 $e = u_1^{x_1} u_2^{x_2} m_b^{-1}, \delta = H(u_1, u_2, e), v = u_1^{x_1} u_2^{x_2} (u_1^{x_1} u_2^{x_2})^\delta$ 。其中: $u_1 = g_1^0, u_2 = g_2^1$ 。

然后对明文 m_b 进行承诺, 方法如下:

- 1) 发送方公开对消息 m 的承诺 $M = g^{m_b} f^n$ 。
- 2) 对 $i = 0, 1, \dots, l-1$, 其中 l 是安全参数, 发送方随机选取 $w_i \in_R \mathbf{Z}_q, \theta_i \in_R \mathbf{Z}_q$, 计算 $t_i = (g_1 g_2)^{w_i}, s_i = g^{h w_i} f^{\theta_i}, C = H(M \| u_1 \| u_2 \| v \| t_0 \| s_0 \| \dots \| t_{l-1} \| s_{l-1})$ 和 $\eta_i = w_i - c_i r_i$, 其

中 $j = i \bmod 2, \delta_i = \theta_i - c_i e h^{n_i} n, c_i$ 是 C 的第 i bit。

最终的密文为 $(u_1, u_2, e, v, M, \eta_0, \delta_0, \dots, \eta_{l-1}, \delta_{l-1})$ 。

因为模拟器拥有私钥 $(x_1, x_2, y_1, y_2, z_1, z_2)$, 所以解密预言机可以正常解密合法密文, 拒绝非法密文。

4.2.2 方案安全性证明的细节

由本文对方案的可公开验证性安全性的证明知密文中元组 $(M, \eta_0, \delta_0, \dots, \eta_{l-1}, \delta_{l-1})$ 不会泄露消息的任何信息, 所以只需考虑密文中元组 (u_1, u_2, e, v) 的安全性。

当模拟器使用 D 分布中的四元组来加密消息时, 密文是合法的。因为敌手可以攻破该加密系统, 所以敌手可以以不可忽略的概率猜对 b 的值。

当模拟器使用 R 分布中的四元组来加密消息时, 密文是非法的, 下面证明此时解密预言机将拒绝解密非法密文, 且 b 是独立于敌手的。

1) 如果敌手不能找到哈希函数的一个碰撞, 则解密预言机将以绝对优势拒绝解密非法密文。

仅仅根据公钥 (c, d, h) 和加密预言机的输出, 敌手可以得到关于私钥 $(x_1, x_2, y_1, y_2) \in \mathbf{Z}_q^4$ 的方程组:

$$x_1 + wx_2 = \log c$$

$$y_1 + wy_2 = \log d$$

$$r_0 x_1 + wr_1 x_2 + (\partial r_0) y_1 + (\partial wr_1) x_2 = \log v$$

其中 $\partial = H(u_1, u_2, e)$ 。因为 $(x_1, x_2, y_1, y_2) \in \mathbf{Z}_q^4$ 可以看成是三个超平面相交的直线上的一个随机的点, 所以敌手无法获得关于 (x_1, x_2, y_1, y_2) 的任何信息。

如果敌手对解密预言机进行询问, 并提交一个非法密文 $(u_1', u_2', e', v') \neq (u_1, u_2, e, v)$, 下面证明预言机将拒绝解密。

当 $(u_1', u_2', e') = (u_1, u_2, e)$ 时, 它们的哈希值是相同的, 但是 $v' \neq v$, 所以解密预言机拒绝解密。

当 $(u_1', u_2', e') \neq (u_1, u_2, e)$ 时, 有 $\partial' = H(u_1', u_2', e')$ 和 $\partial = H(u_1, u_2, e)$ 。因为哈希函数 H 是抗碰撞的, 所以 $\partial' \neq \partial$ 。设 $u_1' = g_1^{r_1'}$, $u_2' = g_2^{r_2'}$, 因为密文是非法的, 所以有 $r_0' \neq r_1'$ 。如果非法密文要通过验证, 则必须有 $v' = v'' = (u_1')^{x_1} (u_2')^{x_2} ((u_1')^{y_1} (u_2')^{y_2})^{\partial'}$, 由公钥 (c, d, h) , 密文 (u_1, u_2, e, v) , 可以得到方程组:

$$\begin{pmatrix} \log c \\ \log d \\ \log v \\ \log v'' \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix}; M = \begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_0 & wr_1 & \partial r_0 & \partial wr_1 \\ r_0' & wr_1' & \partial r_0' & \partial wr_1' \end{pmatrix}$$

因为 $r_0 \neq r_1, r_0' \neq r_1', \partial' \neq \partial$, 所以 $\det(M) = w^2(r_1 - r_0)(r_1' - r_0')(\partial - \partial') \neq 0$ 。

所以矩阵 M 是满秩的。即使敌手知道了 $\log c, \log d, \log v$, 也无法知道 $\log v''$ 的值。敌手猜出 $\log v'$ 的值, 使得 $\log v' = \log v''$ 的概率是可忽略的, 所以解密预言机将以绝对的拒绝解密非法密文。

2) 当解密预言机拒绝解密所有的非法密文时, b 的分布独立于敌手的猜测。

敌手根据公钥可知 $z_1 + wz_2 = \log h$, 如果解密预言机解密一个有效密文 (u_1', u_2', e', v') , 则由 $(u_1')^{x_1} (u_2')^{x_2} = g_1^{r_1'} g_2^{r_2'} = h^{r'}$, 敌手只获得一个线性依赖关系 $r' z_1 + r' w z_2 = r' \log h$, 因此没有泄露私钥 (z_1, z_2) 的信息。

当模拟器使用 R 分布中的四元组来加密消息时, 由加密预言机的输出 (u_1, u_2, e, v) , 敌手可以得到 $\log(em_b) = r_0 z_1 + wr_1 z_2$, 即敌手可以得到方程组:

$$\begin{pmatrix} \log h \\ \log(e/m_b) \end{pmatrix} = \begin{pmatrix} 1 & w \\ r_0 & wr_1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

因为矩阵 $\begin{pmatrix} 1 & w \\ r_0 & wr_1 \end{pmatrix}$ 是满秩的, 所以无论敌手选择 $b = 0$

或者 $b = 1, (z_1, z_2)$ 都有解。所以 b 的分布是独立于敌手的。

至此, 利用敌手区分出了 D 分布和 R 分布, 而这是一个困难性问题, 所以假设的敌手是不存在的, 即新的可公开验证的加密方案在标准模型下是适应性选择密文安全的。

5 结语

本文基于 CS 方案, 提出了一个在标准模型下具有适应性选择密文安全的可公开验证加密方案, 新方案继承了 CS 方案的优点, 其安全性是基于判定性 Diffie-Hellman 问题的困难性。同时该方案的可公开验证性, 满足了现实中的诸多应用需求, 保证了方案的实用性。

参考文献:

- [1] POUPARD G, STERN J. Fair encryption of RSA keys[C]// EUROCRYPT'00, LNCS 1807. Berlin: Springer-Verlag, 2000: 173 - 189.
- [2] YOUNG A, YUNG M. Auto-recoverable auto-certifiable cryptosystems[C]// EUROCRYPT'98, LNCS 1403. Berlin: Springer-Verlag, 1998: 17 - 31.
- [3] STADLER M. Publicly verifiable secret sharing[C]// EURO-CRYPT'96, LNCS 1070. Berlin: Springer-Verlag, 1996: 191 - 199.
- [4] CAMENISCH J, MAURER U, STADLER M. Digital payment systems with passive anonymity revoking trustees[C]// Computer Security - ESORICS'96, LNCS 1146. Berlin: Springer-Verlag, 1996: 33 - 43.
- [5] FRANKEL Y, TSIOUNIS Y, YUNG M. Indirect discourse proofs: achieving efficient fair on-line e-cash[C]// ASIACRYPT'96, LNCS 1163. Berlin: Springer-Verlag, 1996: 68 - 82.
- [6] BELLARE M, GOLDWASSER S. Encapsulated key escrow, TR688[R]. Cambridge: MIT Laboratory for Computer Science, 1996.
- [7] ASOTAN N, SHOUP V, WADNER M. Optimistic fair exchange of digital signatures[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 591 - 610.
- [8] 伍前红, 王继林, 袁素春, 等. 可公开验证的 ElGamal/RSA 加密[J]. 电子与信息学报, 2005, 27(4): 608 - 611.
- [9] CANETTI R, GOLDBREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557 - 594.
- [10] NIETO J M G, MANULIS M, POETTERING B, et al. Publicly verifiable ciphertexts[C]// SCN'12: Proceedings of the 8th International Conference on Security and Cryptography for Networks, LNCS 7485. Berlin: Springer-Verlag, 2012: 393 - 410.
- [11] CAMENISCH J, SHOUP V. Practical verifiable encryption and decryption of discrete logarithms[C]// CRYPTO'03: 23rd Annual International Cryptology Conference, LNCS 2729. Berlin: Springer-Verlag, 2003: 126 - 144.
- [12] CRAMER R, SHOUP V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[C]// CRYPTO'98, LNCS 1462. Berlin: Springer-Verlag, 1998: 13 - 25.
- [13] 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.
- [14] FUJISAKE E, OKAMOTO T. Statistical zero knowledge protocols to prove modular polynomial relations[C]// CRYPTO'97, LNCS 1294. Berlin: Springer-Verlag, 1997: 1294: 16 - 30.
- [15] CHAUM D, WALLET P R. Databases with observers[C]// CRYPTO'92, LNCS 740. Berlin: Springer-Verlag, 1992: 89 - 105.