doi:10.3969/j.issn.1000-436x.2014.07.004

可证安全的高效可托管公钥加密方案

刘文浩[1]，王圣宝[1]，曹珍富[2]，韩立东[1]
(1. 杭州师范大学 信息科学与工程学院，浙江 杭州 310012；2. 上海交通大学 计算机科学与工程系，上海 200240)

摘 要：可托管公钥加密方案中 1 个公钥对应于 2 个解密私钥，它可大大减少公钥基础设施 PKI 中公钥证书的数目，从而降低其公钥证书管理的负荷。同时对于用户端来说，它也能减小所需私钥存储空间，减轻用户的私钥管理负担。提出 2 个新的可托管公钥加密方案，其中第 2 个方案是文献中所有现存同类方案中最为高效的。它也是第 1 个可证安全的此类方案，其安全性基于标准的双线性 Diffie-Hellman 假设。

关键词：密码算法；加密方案；可托管公钥加密；可证安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)07-0033-05

Provably secure and efficient escrowable public key encryption schemes

LIU Wen-hao[1],WANG Sheng-bao[1], CAO Zhen-fu[2], HAN Li-dong[1]
(1. School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310012, China;
2. Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: In an escrowable public key encryption (E-PKE) scheme, there are two keys associated with one public key. It can reduce the total number of certificates in the public key infrastructure (PKI) to a large extent, thus degrade the complexity of certificate management. Moreover, an E-PKE scheme can also reduce the key storage for end users. Two such schemes were proposed, with the second one being the most efficient one among all existing E-PKE schemes. It is also the first provably secure E-PKE scheme, whose security is based on the standard bilinear Diffie-Hellman (BDH) assumption.

Key words: cryptographic algorithm; encryption scheme; escrowable public key encryption; provable security

1 引言

$N=1$公钥密码学在网络信息安全中的作用越来越受到人们重视，它能够同时为用户提供保密性和抗抵赖（数字签名）服务[1]。然而，利用唯一一个公钥/私钥元组来同时提供这 2 种服务的做法存在严重问题。首先，为了防止由于用户私钥的丢失而造成对先前密文的不可解密，或者出于法律监管的需要，往往要求用户将解密私钥托管到可信任的托管中心(EA, escrow agency)。其次，对于数字签名服务而言，出于满足真正意义上的不可抵赖性的目的，又要求签名私钥应该只能为签名人所掌握，即托管中心不能够获得用户的(签名)私钥。所以，当使用传统公钥加密方案(例如 RSA) 时，由于解密私钥与签名私钥相同，用户的唯一私钥是否被托管就是一个矛盾。

现行公钥基础设施(PKI, public key infrastructure)为了调和这个矛盾，一般采用“双证书模式”[2]，

收稿日期：2014-06-02；修回日期：2014-06-25
基金项目：国家自然科学基金资助项目（61103209, 61170227）；浙江省自然科学基金资助项目（LZ12F02005）；浙江省教育厅科学基金资助项目（Y201222977）；网络与交换技术国家重点实验室开放基金资助项目（SKLNST-2009-1-13）
Foundation Items: The National Natural Science Foundation of China (61103209, 61170227); The Natural Science Foundation of Zhejiang Province (LZ12F02005); Education Department Foundation of Zhejiang Province (Y201222977); The Open Foundationa of State Key Laboratory of Networking and Switching Technology of China (SKLNST-2009-1-13)

即让每个用户使用 2 对公/私钥。2 个公钥分别被 2 份公钥证书所证实。然而，这种做法的最大问题在于它使得 PKI 所颁发的证书数目加倍，极大增加了其证书管理负荷。并且，这种模式也增加了用户端自身负担：每个用户必须存储和管理 2 个私钥，即解密私钥和签名私钥。

2001 年，Verheul[3]提出的可托管公钥加密(E-PKE, escrowable public-key encryption)方案成功解决了上述难题。它的基本思想是，解密权能够在不牺牲数字签名服务的前提下被托管。在这种全新加密方案中，用户的唯一公钥对应于 2 个解密私钥：自己掌握的主解密私钥(primary decryption key)，记为 K_P；可交给托管中心的托管解密私钥(escrow decryption key)，记为 K_E。其中，主解密私钥不能够被托管中心利用托管解密私钥计算出来。此时，用户利用其主解密私钥 K_P 进行的数字签名就满足法律意义上的不可抵赖性。这种方案被分成如下 2 类。

1) 主动方案：用户能自主决定是否将托管解密私钥 K_E 托管。显然，如选择托管，用户需要通过安全信道首先将托管解密私钥 K_E 交付给托管中心。例如，Verheul[3]提出的第 1 个此类方案就是主动式方案。

2) 被动方案：也称为全局托管方案。用户不能自主选择是否将解密权托管。托管中心能依靠其唯一托管解密私钥（也即系统主私钥），解密系统中所有用户的密文。Boneh 和 Franklin[4,5]提出的 E-PKE 方案就属于被动式方案。

2 相关数学基础知识

本文所讨论的全部方案都基于双线性映射(bilinear pairing)。因此，这里有必要首先回顾相关难题假设，然后给出双线性映射的定义。

定义 1 (离散对数难题(DLP, discrete logarithm problem))。假设$(G, \cdot)$表示一个阶为 q 的群，g 是它的生成元。离散对数难题是：给定随机元素 $y\in_R G$，找到一个数 $x\in Z_q$，使得 $y=g^x$。

定义 2 (计算性 Diffie-Hellman 难题(CDHP, computational Diffie-Hellman problem))。假设$(G, \cdot)$表示一个阶为 q 的群，g 表示它的生成元。计算性 Diffie-Hellman 难题是：给定一个随机三元组 (g,g^a,g^b)，其中，元素 $a,b\in Z_q^*$，计算 g^{ab}。

定义 3 (判定性 Diffie-Hellman 难题(DDHP, decisional Diffie-Hellman problem))。假设$(G, \cdot)$是一个阶为 q 的群，g 为其生成元。判定性 Diffie-Hellman 难题是：给定三元组 (g^a,g^b,g^c)，其中，随机元素 $a,b,c\in Z_q^*$，判断 $g^c=g^{ab}$ 成立与否。

概略地说，离散对数(DL)、计算性 Diffie-Hellman (CDH) 以及判定性 Diffie-Hellman (DDH) 假设指的是：不存在概率多项式时间算法能够以不可忽略的优势解决 DLP、CDHP 或 DDHP 难题。

假设 G_1 是由生成元 P 生成的循环群，其阶为素数 q，令 G_2 代表另一个阶也是 q 的循环群。令群 G_1 与 G_2 上的离散对数难题假设成立。

定义 4 (双线性映射(Pairing))。双线性映射 e 是双线性函数 $e:G_1\times G_1\to G_2$，它符合以下性质。

1) 双线性：如果 $P,Q\in G_1$ 并且 $a,b\in Z_q^*$，那么 $e(aP,bQ)=e(P,Q)^{ab}$。

2) 非退化：满足 $e(P,P)=1$。

3) 可计算：如果 $P,Q\in G_1$，则 $e(P,Q)\in G_2$ 是可在多项式时间内计算的。

3 提出的新方案

这里给出本文新提出的 2 个可托管公钥加密方案。值得特别指出的是，为了节省篇幅，省略了对可托管公钥加密方案的形式化定义。相关定义与其他类别的公钥加密方案极其类似，例如 Boneh 和 Franklin[4,5]所给出的关于基于身份的加密方案的形式化定义。不同之处仅在于，可托管公钥加密方案中用户的私钥有 2 个，相应地，解密算法也有 2 个。

3.1 第 1 个新方案

本文第 1 个新方案来源于 Boneh-Frankin[1,2]被动式方案。不同之处在于将它转化为主动式方案。

系统初始化(Setup)：给定安全参数 k，进行以下步骤计算。

1) 输出 2 个阶为素数 q 的循环群 G_1 与 G_2、群 G_1 的生成元 P，以及双线性映射 $e:G_1\times G_1\to G_2$。

2) 选择杂凑函数 $H:G\to\{0,1\}^n$，其中，n 是整数。

此方案的明文空间是 $M=\{0,1\}^n$，密文空间是 $C=G_1^*\times\{0,1\}^n$。系统公共参数 *params* 为 (q,G_1,G_2,e,n,P,H)。

私钥生成(Key-Gen)：每个用户可按如下算法生成自己的公/私钥元组。

1) 随机选择 2 个随机数 $x_1,x_2\in Z_q$，并把其中任意一个设置为主解密私钥，这里假定主解密私钥

$K_P = x_1$。

2) 托管解密私钥：$K_E = x_2$。

3) 用户公钥为 $P_1 = x_1 P$ 及 $P_2 = x_2 P \in G_1$

加密算法(Encryption)：为了加密消息 $m \in M$，加密方首先选择 $r \in Z_q$，把密文设为 $C = (rP, m \oplus H(g^r))$，其中 $g = e(P_1, P_2) \in G_2^*$。

解密算法(Decryption)：密文 $C = (U, V)$，利用自己的主解密私钥 x_1 计算 $m = V \oplus H(e(U, x_1 P_2))$。

托管解密(Escrow-Decrypt)：对于密文 $C = (U, V)$，托管中心利用托管解密私钥 K_E 计算 $m = V \oplus H(e(U, K_E P_1))$。

方案正确性：这个方案的加解密正确性基于如下事实，解密者和托管中心双方都能正确地由密文 C 的前半部分 U 计算获得加密方用于对明文 m 进行加密的会话密钥，即 $e(U, x_1 P_2) = g^r$。同样，$e(U, K_E P_1) = g^r$。

不同于一般意义上的可托管公钥加密方案，这里用户的唯一公钥(由 P_1 和 P_2 双元组组成)还对应于另外 1 个解密私钥——第 3 个解密私钥 $x_1 x_2 P$。用户也可以把私钥 $x_1 x_2 P$ 作为托管解密私钥交付给托管中心。如果这样，用户握有的两对公/私钥元组 (x_1, P_1) 和 (x_2, P_2) 都可以作为签名私钥/验证公钥元组，用来提供抗抵赖服务。

3.2　第 2 个新方案

本文提出的第 2 个方案是主动式的可托管公钥加密方案。它的基本过程描述如下。

系统初始化(Setup): 给定一个安全参数 k，执行下面的步骤。

1) 输出 2 个阶为素数 q 的循环群 G_1 与 G_2、群 G_1 的生成元 P，以及双线性映射 $e: G_1 \times G_1 \to G_2$。

2) 计算 $g_2 = e(P, P)$。

3) 选择杂凑函数 $H: G_2 \to \{0,1\}^n$，其中 n 是整数。

此方案的明文空间是 $M = \{0,1\}^n$，密文空间是 $C = G_1^* \times \{0,1\}^n$。系统公共参数 *params* 为 $(q, G_1, G_2, e, n, P, g_2, H)$。

私钥生成(Key-Gen)：这是用户的（双）私钥生成算法。每个用户生成自己的公钥及其对应的 2 个解密私钥。

1) 首先，随机选择一个随机数 $x \in Z_q$，并将其设置为主解密私钥，即 $K_P = x$。

2) 将托管解密私钥设为 $K_E = x^{-1} P$。

3) 将公钥设为 $P_{\text{Pub}} = xP \in G_1$。

加密算法(Encryption)：对消息 $m \in M$ 进行加密，加密方首先选择 $r \in Z_q$，接着计算得到密文：$C = (rP_{\text{Pub}}, m \oplus H(g_2^r))$。

解密算法(Decryption)：收到密文 $C = (U, V)$，解密方利用 K_P 进行如下计算获得明文：$m = V \oplus H_2(e(U, K_P^{-1} P))$。

托管解密算法(Escrow-Decrypt)：托管中心得到密文 $C = (U, V)$ 后，使用 K_E 进行如下计算获得明文：$m = V \oplus H_2(e(U, K_E))$。

4)方案的正确性：此方案的正确性源自于这一事实，无论是用户自己（解密方）还是托管中心，都能够通过密文 C 的前半部分 U 计算获得加密方用于加密明文 m 的会话密钥，即 $e(U, K_P^{-1} P) = e(U, K_E) = g_2^r$。

方案满足主私钥安全性：托管中心获得的托管解密私钥为 $K_E = x^{-1} P$，而由用户唯一掌握的主解密私钥为 $K_P = x$，因此，从托管解密私钥计算获得主解密私钥，等价于群 G_1 上的离散对数难题。

提供不可抵赖服务的签名私钥/验证公钥密钥元组为(x, g_2^r)。因此，传统的安全性基于离散对数难题假设的数字签名方案，例如 ElGamal 签名[6]、DSA 方案，都可以被用户采用以提供不可抵赖服务。

3.3　效率和实用性

通过表 1 来说明本文所提出方案的高计算效率和强实用性。

表 1　　E-PKE 方案间的比较

方案/比较项目	用户公钥	预先加密	在线双线性映射运算	可证安全
文献[4]中方案	xP	×	1	×
方案 1	$(x_1 P, x_2 P)$	×	1	×
文献[3]中方案	$e(P,P)^x$	×	0	×
方案 2	xP	√	0	√

首先来分析加密方的计算效率。在本文所提出的第 2 个方案的加密过程中，加密方不需要计算任何双线性映射，也即加密方无论是在线还是离线阶段都无需进行双线性映射函数的计算。在现有的总共 4 个方案中，只有 Verheul 方案[3]也满足这样的高计算效率，而其他 2 个方案中的加密方都需要在线地（也即获得了解密方的公钥，或公钥证书之后）

计算一个双线性映射。进一步，第 2 个方案比 Verheul 的方案更加实用，这是因为本文的方案中，加密方在以某种方式获得解密方的公钥之前，就能够首先利用系统公共参数计算得到用于加密明文消息的会话密钥 g_2^r，其中 r 为加密方选择的一个随机整数（可离线选定并存储备用）。这意味着明文可以被预先加密。换句话说，密文 C 的后半部分 V 可在离线阶段提前得到计算。这大大提高了加密效率。而在 Verheul 方案中，要求加密方在获得解密方的公钥 P_{Pub} 之后，方能进行会话密钥 P_{Pub}^r 的计算。其中，r 也是加密方选择的一个随机整数（也可离线选定并存储备用）。

而在其他方案方面，在 Boneh-Frankin 方案和本文所提出的第 1 个方案中，加密方在加密时必须在线地（即获得解密方的公钥之后）完成双线性映射的运算。

其次，来看密钥的长度。本文所提出的第 2 个方案中的用户主解密私钥的长度达到了最优，即为 Z_q 中一个整数的长度。而在公钥的长度方面，Verheul 方案是群 G_2 中的单个元素，相比而言，本文所提出的第 2 个方案中，其值为群 G_1 中的单个元素。一般来说，后者的长度要短于前者。

3.4 第 2 个方案的可证明安全性

众所周知，利用由日本学者 Fujisaki 和 Okamoto 所提出的通用转化方法[7]，能够很方便地把达到选择明文安全性的公钥加密方案，增强为达到选择密文安全性的方案。因此，这里只给出了方案的选择明文安全性证明。由于本文所提出的第 2 个方案是全部现有同类方案中最为高效和实用的。因此，这里只给出对它的安全性证明。类似地，也能够给出其他方案的安全性证明。

为了节约篇幅，省略了对可托管公钥加密方案的形式化安全模型的描述。这一安全模型与传统公钥加密方案的形式化安全模型并无特殊差异。这主要是因为：首先，解密私钥的增加并不会降低方案的安全性，换句话说，所有解密私钥的总体可被看作传统公钥加密方案中的唯一私钥，都是需要被严格保密的；其次，由于托管中心获得了被托管的托管解密私钥，因此它具有同等的解密能力。它不能被看作可能的敌手。

接下来，给出该方案选择明文安全性所基于的难题假设：逆 BDH (iBDH) 难题假设。

定义 5 逆 Diffie-Hellman (iBDH) 问题)。令群 G_1、G_2、生成元 P 以及 e 与前文所定义的同名参数相同。(G_1,G_2,e) 上的 *iBDH* 问题为：假设有 (P,aP,bP)，其中，随机的元素 $a,b\in Z_q^*$，计算 $e(P,P)^{a^{-1}b}\in G_2$。

非严格地说，逆 BDH (iBDH) 难题假设即逆 BDH (iBDH) 难题是难解的，即不存在多项式时间算法能计算这一问题。值得指出的是，Zhang 等人[8]给出了 iBDH 难题假设与标准双线性 Diffie-Hellman (BDH) 难题假设相互等价的证明。以下定理给出了第 2 个方案的选择明文安全性。

定理 1 假设存在一个优势为 ε 的敌手 A，它是针对该方案的选择明文攻击敌手，假设它最多进行 q_2 次 H 询问，则可构造出一个算法 B，它能以不小于 $2\varepsilon/q_2$ 的优势成功破解 iBDH 难题。

证明 假设敌手 A 针对 H2 最多定下 q_2 次询问，其成功优势是 ε。下面，详细构造算法 B，它借助运行敌手 A 并与之进行交互来成功解决 iBDH 难题。

假设 B 的初始输入值为 (q,G_1,G_2,e) 和 (P,aP,bP)。用 $D=e(P,P)^{a^{-1}b}\varepsilon G_2$ 来代表对应于该难题输入的 iBDH 难题的解。

初始化：B 将公钥设定成 $(q,G_1,G_2,e,P_{Pub},n,P,H)$，其中，$P_{\text{Pub}}=aP$。敌手 A 首先获得公钥。这里，未知的解密私钥是 $a^{-1}P$。后续证明过程中，H 为 B 所完全掌握的随机 Oracle。

H-查询：为了模拟敌手 A 对随机 Oracle H 的询问，算法 B 维护一个列表(称为 $H-$表)，其格式为 (X_j,H_j)。面对询问 X，算法 B 首先检查它是否已经存在于 $H-$表之上。若存在，则算法 B 返回相应记录中的 H 值。否则，从 $\{0,1\}^n$ 中随机选择一个 H 值返送到敌手 A，并把条目 (X,H) 添入 $H-$表。

挑战：当上述第一阶段结束后，敌手 A 输出 2 个明文消息 M_0、M_1，它们的长度相同。算法 B 随机选择 $t\in\{0,1\}$ 和串 $S\in\{0,1\}^n$，接着，把针对明文消息 M_t 的加密 C^* 设定为 $C^*=(U,V)$，其中，$U=bP$，$V=M_t\oplus S$。算法 B 将挑战密文 C^* 传递给敌手 A。

如前所述，$a^{-1}P$ 是任何一方都未知的解密私钥，D 是算法 B 所面临的 iBDH 问题的解。注意，对密文 C^* 进行解密，得到的结果为 $V\oplus H(e(a^{-1}P,bP))=V\oplus H(D)$。

猜测：敌手 A 在获得密文 C^* 后，仍然可以发起 $H-$ 询问。过后，敌手 A 输出关于比特值 t 的猜测 $t\in\{0,1\}$。

输出：最后，算法 B 随机地从 H-表上摘下一个条目 (X_j,H_j) 并输出其中的 X_j 作为它的 iBDH 难题解。

显然，算法 B 的上述模拟过程对于敌手来说是完美和不可区分的。因此，得出结论：敌手 A 的成功优势为 ε。将 H 表示为如下事件：在算法 B 的模拟过程中，敌手 A 以 D 作为输入，询问随机 Oracle H。

由于 $H(D)$ 的值是敌手 A 无法预测的，所以，如果它在没有针对 H 询问 D，则它也无法预测挑战密文 C^* 的解密输出。因此有如下结论：在攻击模拟游戏中 $P_r[t=t'|-H]-1/2$。

依据关于敌手 A 的定义，在真正的攻击中(以及在针对它的模拟中)，$|P_r[t=t'|-H]-1/2|\geqslant\varepsilon$。关于 $P_t[t=t']$，可得到以下界值

$$\begin{aligned}P_t[t=t']&=P_r[t=t'|-H]P_r[-H]+P_r[t=t'|H]P_r[H]\\&\leqslant P_r[t=t'|-H]P_r[-H]+P_r[H]\\&=1/2P_r[-H]+P_r[H]\\&=1/2+P_r[H]/2\end{aligned}$$

$$\begin{aligned}P_r[t=t']&\geqslant P_r[t=t'|-H]P_r[-H]\\&=P_r[-H]/2\\&=(1-P_r[H])/2\\&=1/2-P_r[H]/2\end{aligned}$$

因此有：$|P_r[t=t']-1/2|\leqslant P_r[H]/2$。又由于 $|P_r[t=t']-1/2|\geqslant\varepsilon$，因此有：$P_r[H]\geqslant 2\varepsilon$。依据 H 的定义可推出 D 出现在 H-表中的概率不小于 2ε。进一步，算法 B 求得正确的 iBDH 难题实例解的概率不小于 $2\varepsilon/q_2$，这与假设 iBDH 问题是难解的假设矛盾。

4　结束语

可托管公钥加密方案是一种具有很好应用前景的新型加密方案。特别是随着同样利用双线性映射所构造的基于身份的加密方案被逐步应用[9]，可托管公钥加密有望成为解决现行公钥基础设施中证书管理负担过重问题的一种有效解决方案。本文提出了 2 个新的此类方案。其中，第二个方案的加密过程最为高效，并且它允许加密方能够以离线方式提前加密明文。最后，详细给出了它的安全性证明。本文所给出的方案是在随机预言模型中安全的，是否存在标准模型下安全的此类方案，值得进一步研究。

参考文献：

[1] ZIMMERMANN P. Pretty Good Privacy—Public Key Encryption for the Masses, PGP User's Guide[M]. Cambridge, MA: MIT Press, 1995.

[2] SANTESSON S, POLK W, BARZIN P, *et al*. Internet X.509 Public Key Infrastructure, Qualified Certificates Profile, RFC 3039, IETF[S]. 2001.

[3] VERHEUL E R. Evidence that XTR is more secure than supersingular elliptic curve crypto systems[A]. Proc of Eurocrypt'01[C]. Springer, 2001.195-210.

[4] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[A]. Proc of CRYPTO'01[C]. Springer, 2001.213-229.

[5] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[J]. SIAM J Computing, 2003, 32(3):586-615.

[6] ELGAMAL T. A public key cryptosystem and signature scheme based on discrete logarithms[J]. IEEE Trans Inf Theory, 1985, 31(4):469-472,

[7] FUJISAKI E, OKAMOTO T. How to enhance the security of public-key encryption at minimum cost[J]. IEICE Trans Fundamentals, 2000, 9(1): 24-32.

[8] ZHANG F, SAFAVI-NAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[A]. Proc of PKC'04[C]. Springer, 2004.277-290.

[9] LYNN B. On the Implementation of Pairing-Based Cryptography[D]. Stanford University, 2006.

作者简介：

刘文浩（1974-），男，湖北孝感人，博士，杭州师范大学讲师，主要研究方向为信息安全与无线网络安全。

王圣宝[通信作者]（1978-），男，江西鄱阳人，博士，杭州师范大学副教授，主要研究方向为应用密码学与网络信息安全。E-mail: shengbaowang@hznu.com。

曹珍富（1962-），男，江苏滨海人，上海交通大学教授、博士生导师，主要研究方向为密码学、信息安全及计算数论等。

韩立东（1982-），男，山东济南人，博士后，杭州师范大学讲师，主要研究方向为应用密码学与云计算安全。