基于身份加密机制的光学加密密钥系统

徐宁[1]，杨庚[2]

(1. 南京邮电大学 光电工程学院，江苏 南京 210003；
2. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室，江苏 南京 210003)

摘 要：从非对称的基于身份密钥体系出发，提出了一种适用于光学加密系统密钥管理的方法。首先简要介绍了基于身份密钥体系，特别是 Boneh-Franklin 算法，然后针对光学加密参数安全传输问题，给出了非对称密钥系统的密钥生成、分配、更新等算法，并从方法的复杂性、安全性等方面对算法进行了分析，最后对二维码加密问题进行了仿真，结果表明算法是正确有效和安全的。

关键词：基于身份标识密钥系统；通信安全；光学加密系统；二维码标识

中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2012)04-0121-08

Key establish scheme for optical encryption system based on IBE

XU Ning[1], YANG Geng[2]

(1. College of Opto-Electronic Engineering, Nanjing University of Posts & Telecommunications, Nanjing 210003, China;
2. Key Lab of Broadband Wireless Communication & Sensor Network Technology, Ministry of Education,
Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: Based on asymmetric identity-based encryption, a key management mechanism for optical encryption was proposed. First, the IBE scheme, particularly the Boneh-Franklin algorithm was described. Then, the algorithms for key generating, distributing and updating was presented. And the performance of the algorithms in terms of complexity and security was evaluated. Finally, some simulation results about two-dimensional code under two different encryption systems was given, which demonstrate the efficiency, correctness and security of the proposed mechanism.

Key words: identity-based cryptography; communication security; optical encryption; two-dimensional code identity

1 引言

近几年来，作为信息安全研究的一个分支，一种基于光学原理与技术的非数学密码理论与技术显示出了极大的潜力，已成为当前研究的热点之一[1~8]。可并行实现数据处理是光学系统中所固有的能力，由于光学信息处理技术本身还具有高速度、光的波长短、信息容量大等特点，同时又具有振幅、相位、波长、偏振等多种属性，是一种多维的信息载体，从而也为光学加密系统的密钥空间提供了更为宽广的选择，使其具有更高的安全性。另一方面，近来物联网技术的发展，进一步推动了基于 RFID 和光学标签的应用，如无源二维码，可以将信息编码到二维码中，再对其进行加密。目前，一个二维码

收稿日期：2011-08-22；**修回日期**：2011-11-11

基金项目：国家重点基础研究发展规划（“973”计划）基金资助项目（2011CB302903）；国家自然科学基金资助项目（60873231，60977069）；江苏省自然科学基金资助项目（BK2009426）；江苏省高校自然科学研究重大基金资助项目（11KJA520002）

Foundation Items: The National Basic Research Program of China (973 Program) (2011CB302903); The National Natural Science Foundation of China (60873231, 60977069); The Natural Science Foundation of Jiangsu Province (BK2009426); The Natural Science Foundation for Colleges and Universities of Jiangsu Province (11KJA520002)

的信息容量可达到 1 850 个大写字母，或 500 多个汉字。条码也可以把图片、声音、文字、签字、指纹等可以数字化的信息进行编码，目前即使在二维条码因穿孔、污损等损毁面积达 50%情况下，照样可以恢复信息，获取正确的信息。二维条码可以使用激光或 CCD 阅读器识读。在商品标签、票据等方面已经得到了广泛的应用。特别是火车票上的二维码可含有个人的身份证号等信息，需要进行加密等处理，以达到保护个人隐私的目的。

从密码学观点来看，目前国内外对光学加密方法的研究还局限于对称密钥系统，即在加密解密过程中采用同样的光学参数进行运算。这种密码系统由于密钥的分发、更新、删除、传输等管理问题需要进一步研究解决，使其实际应用受到了影响。而非对称密钥系统采用一对公、私密钥的思路，用户保存自己的私钥，公钥对外公布公开。非对称密钥系统在密钥的管理方面显示了良好的适应性，但与对称密钥系统相比，在加密和解密算法的复杂性方面仍然有差距，加密解密时间长。为此，文献[9]将公开密钥系统的算法应用于双相位随机编码的光学数据加密方案中，解决了加密中对称密钥的传输问题，但在方法的可应用性方面仍需要完善。文献[4]从认证、加密等多角度分析了光学信息安全问题，提出了一种基于公钥密码学的混合密钥加密系统，并加入认证技术构建了一个网络环境下的虚拟光学信息安全系统模型。

与非对称密钥相比，对称密钥的最大优点是计算量小。但是其明显的缺点是必须有一个密钥预分配过程，即要通过一个安全途径将对称密钥传送给用户，并能安全有效地进行密钥的更新，以及用户的增加和离。所以，人们一直在试图寻求非对称密钥系统在虚拟光学密钥系统中的应用。

作为一种非对称密钥系统，基于身份标识的加密(IBE, identity-based encryption)算法于 1984 年首先提出[10]，但直到 2001 年研究人员才设计出一个可实际应用的实现方法[11]。这种加密算法的优点之一是，公钥可以是任何唯一的字符串，如身份证号、E-mail 地址、标签的标枳、IP 地址等。由于通常可以使这个标识具有一定的含义，是可识别的，从而不需要 PKI 系统的证书发放，就省去了对用户的认证过程。另一方面，IBE 算法可以采用椭圆曲线形式实现，在 2001 年可实现算法提出后，引起了人们的高度重视，根据不同的应用方向，相继提出了一些列基于身份标识的加密算法[12~14]。

由于身份标识的加密算法可以是椭圆曲线类型的算法，在安全性和密钥分配等管理方面显示出一些良好的特点。同时诸如光学标签的身份标识性，使探索 IBE 算法在虚拟光学加密系统中的应用显得具有重要的意义和可能性，这也是本文的研究出发点。本文将首先介绍光学加密系统和 IBE 加密机制的基本概念和算法；然后提出一种基于 IBE 的光学加密系统的密钥管理方法，设计相关的算法，包括密钥的分配、更新、删除等算法，以及用户的加入和退出过程中的密钥管理问题，以保证密钥系统的前向和后向安全性，同时从内存需求、算法复杂性和安全等方面分析了方法的性能；最后通过对二维码等实际光学标签的应用，验证方法的正确性和有效性，并讨论了可进一步研究的工作。

2 IBE 算法

本节主要简要介绍 IBE 算法。在 IBE 算法中，公钥是用户的身份标识，密钥的生成与传送需要由可信第三方完成，记可信第三方为 PKG(private key generator)。下面给出文献[11]中的 IBE 算法。

1) 安全假设

IBE 加密算法的数学基础是可计算 Diffie-Hellman 问题的一个变化形式，其安全性是建立在双线性 Diffie-Hellman 困难问题的之上一，即 Bilinear-Diffie-Hellman（BDH）问题。IBE 实现算法的核心是采用了超奇异椭圆曲线上的一个双线性映射（如 Weil pairing）。记 Zq 为 q 阶的加法群，Zq= {0, …, q−1}，q 为素数，Z^+为正整数集合。

设 G_1 和 G_2 为 q 阶的群，则双线性映射 $\hat{e}: G_1 \times G_1 \to G_2$ 满足如下性质：

□ 双线性(bilinear)：$\forall x, y \in G_1$， $a, b \in Z$，有 $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$，则称映射 $\hat{e}$ 为一个双线性映射。

□ 非退化性(non-degenerate)：存在 $P, Q \in G_1$，使得 $\hat{e}(P, Q) \neq 1$。

□ 可计算性(computable)：对于任意 $P, Q \in G_1$，有一个多项式时间算法来计算 $\hat{e}(P, Q)$。

则 BDH 问题可以描述为，设 P 是 G_1 的生成元。已知 (P, aP, bP, cP)，$a, b, c \in Z_p^*$，计算 $\hat{e}(P, P)^{abc} \in G_2$ 称为 $(G_1, G_2, \hat{e})$ 中的 BDH 问题。

2) Boneh-Franklin IBE 算法

算法有 2 种实现形式，一种是包含 4 个散列函数的完全算法，另一个是只包含 2 个散列函数的基本算法，这里主要叙述基本的 Boneh-Franklin IBE 算法，它由 4 个函数：Setup、Extract、Encrypt 和 Decrypt 组成，分别完成 IBE 算法中的参数建立、密钥提取、加密和解密的功能。设消息的明文空间为 $M=\{0,1\}^n$，密文空间为 $C=G_1\times\{0,1\}^n$。

算法 1　基本 Boneh-Franklin (BBF) 算法。

1) Setup 的步骤如下。

步骤 1　给定安全参数 $k\in Z^+$，PKG 选择 $k$bit 长的素数 q，2 个 q 阶群 G_1和 G_2，同时选择一双线性映射 $\hat{e}:G_1\times G_1\to G_2$，随机选择 G_1 的生成元 P。

步骤 2　PKG 随机选择一非零整数 $s\in Z_q^*$，计算 $P_{\text{pub}}=sP$。

步骤 3　PKG 选择散列函数 $H_1:\{0,1\}^*\to G_1^*$，$H_2:G_2\to\{0,1\}^n$。

步骤 4　生成系统参数 $\psi=\langle q,G_1,G_2,\hat{e},n,P,P_{\text{pub}},H_1,H_2\rangle$，主密钥为 $s\in Z_q^*$。

2) Extract: 对给定的身份标识的字符串 $ID\in\{0,1\}^*$，生成密钥。

步骤 1　计算 $Q_{\text{ID}}\in H_1(ID)\in G_1^*$。

步骤 2　计算私钥 $K_{\text{ID}}=sQ_{\text{ID}}$，其中 s 为主密钥。

3) Encrypt: 对原文 $m\in M$ 和公钥 ID，加密步骤如下。

步骤 1　计算 $Q_{\text{ID}}\in H_1(ID)\in G_1^*$。

步骤 2　随机选择数 $r\in Z_q^*$。

步骤 3　随机取 $r\in Z_q^*$，则加密的密文为

$$c=\langle rP,m\oplus H_2(g_{\text{ID}}^r)\rangle$$

其中，$G_{\text{ID}}=\hat{e}(Q_{\text{ID}},P_{\text{pub}})\in G_2^*$。

4) Decrypt: 设密文为 $c=<U,V>$，解密步骤如下。

应用密钥 $K_{\text{ID}}\in E/\text{GF}(p)$，计算原文 $m=V\oplus H_2(\hat{e}(K_{\text{ID}},U))$。

IBE 加密算法的安全性建立在 Diffie-Hellman 问题复杂性基础上。文献[15]的成果表明，BBF 算法是单向身份加密算法(one-way identity-based encryption scheme)，详细的结论参见文献[15]。

3　一种光学加密系统的密钥分配管理方法

作为一种非数学形式的加密系统，基于光学成像技术的光学加密技术近年来引起了人们的极大兴趣，成为现代加密技术的重要研究领域。主要的加密技术有基于菲涅耳变换的加密算法和基于双随机相位编码方法的加密算法等。光学加密系统的密钥空间维数高，可以从振幅、相位、波长、偏振等多种属性入手，使加密信息的安全性更高。但如何在系统中建立密钥管理机制仍是需要解决的问题，包括密钥的产生、分配、更新、删除等过程。本节给出一种可应用于基于光学加密技术的密钥管理方法，其基本思想是应用 IBE 算法进行光学加密参数的交换，再应用该对称密钥进行正常的数据通信。本方法的优点是采用 IBE 的非对称系统进行参数交换，采用对称系统进行通信的数据加密，充分利用了两者的优点；同时不存储多余的密钥，对内存需求小。采用 IBE 算法交换参数，简单安全，不需要认证过程，详细的分析将在后面讨论。为了便于算法的描述，先给出方法的一般形式，然后在定义其具体的计算方法。

1) 系统初始化

初始化过程就是要生成系统的公共参数 ψ 以及各个节点的非对称密钥系统的私钥，以便为后面的光学系统的加密参数提供安全的传输途径。对一个存在类似于服务器或 PKG 的系统，由于 PKG 和用户节点之间可以建立一个安全的会话通道，即生成一个会话密钥实现初始化参数的安全分发。而对光学标签在传感网与物联网中的应用系统，由于网络拓扑结构的不断变化，以及有可能系统就不存在类似于服务器或 PKG，可以在节点系统生成阶段，将有关的参数存入节点，对节点进行初始化。例如可以以传感器网络的具体使用范围进行节点公共参数初始化管理，如物流系统、票务系统等。系统中的节点管理系统完成对节点的公共参数初始化，然后供现场实际使用。系统的主密钥 s 只存在于节点参数的初始化管理系统中，这样使通信密钥系统更为安全。若应用系统中需增加新的节点，就用初始化管理系统根据主密钥计算该节点的密钥，再对新节点进行初始化，这样能很好地解决新增节点和替换节点的问题。初始化算法在具体的应用中只执行一次。下面给出系统初始化算法。

算法 2　系统初始化算法。

输入：密钥空间长度 k，群的阶 q。

输出：公共参数 π，各用户的密钥。

步骤 1　生成公共参数: 根据密钥长度 k 和参数 q，PKG 执行算法 1 中的 Setup 算法，生成公共

参数 $\psi=\{q, p, \hat{e}, n, P, P_{\text{pub}}, H_1, H_2\}$。

步骤 2 用户密钥生成 KeyGen: 根据节点标识 ID 和公共参数 ψ，PKG 执行 IBE 算法中的 Extract 算法，生成用户的通信密钥 K_{ID}。采用上面讨论的 2 种方法将参数 ψ，以及通信密钥分配到相应的节点，完成节点的初始化过程。

2) 光学加密系统密钥参数对的生成

在系统初始化过程后，每个节点都生成了与其节点标识相对应的通信密钥 K_{ID}。为了使通信的双方能够采用光学加密系统进行传输数据的加密，必须要将光学加密参数安全地传送到接收方。基于在初始化过程中建立的非对称密钥对，就可以采用基于 IBE 的加密算法将光学加密参数安全传送给对方。

设数据发送方生成的光学加密参数为 Θ，如对典型的基于 4f 系统的双随机相位编码方法，参数 Θ 包含 2 个相位函数 $N(x,y)$和 $B(\alpha,\beta)$，以及一个透镜的焦距 f；对基于菲涅耳变换的双随机相位编码，参数 Θ 包含 2 个相位随机函数 $R_1(x,y)$和 $R_2(x,y)$，以及 2 个菲涅耳衍射 D_1 和 D_2。光学加密系统可以根据这些加密参数设计对具体的数据的加密，特别是图像的加密。因为在这种情况下，光学加密系统可以并行运行加密、解密过程，密钥空间是多维的，在性能上比传统的加密系统更为优越。图 1 给出了一个二维的基于虚拟成像的多维数据加密系统的理论模型结构。

该系统是一个加入了随机模板的单透镜光学成像系统，其中，d_0 是信息平面（即需要加密的信息)到成像透镜前表面的距离，d_i 是透镜后表面到像平面的距离，像平面就是加密后的信息平面，即密文。设 $U_0(x_0, y_0)$、$U_{L1}(\zeta, \eta)$、$U_{L2}(\zeta, \eta)$和 $U_r(x, y)$分别为信息平面、透镜前表面、透镜后表面以及随机模板的复振幅。根据傅里叶光学原理，光波从信息平面到透镜前表面的传播过程和光波从透镜后表面到像平面的传播过程都可以利用菲涅耳衍射变换来描述。记 $U_{d0}(k,l)$为信息平面 $U_0(x_0, y_0)$在衍射距离 d_0 下的菲涅耳衍射，$U_{rd}(k, l)$为随机模板 $U_r(x,y)$在衍射距离 d 下的菲涅耳衍射。

为了能采用计算机仿真手段实现虚拟光学加密系统，需要对所有连续函数进行离散。设对正方形的信息平面进行等距离划分，步长分别为 Δx 和 Δy，划分数为 N。首先对信息平面 $U_0(x_0, y_0)$进行 $N\times N$ 的离散采样，得到菲涅耳变换的离散表达形式，记为离散菲涅耳变换（DFD, discrete Fresnel diffraction)，则信息平面 $U_0(x_0, y_0)$的 DFD 如式(1)所示，即

$$\begin{aligned} DU_{d0}(m,n) &= DFD\left[U_{d0}(k,l);\lambda,d_0\right] \\ &= \frac{1}{\mathrm{j}\lambda d_0}\exp\left[\mathrm{j}\frac{\pi}{\lambda d_0}\left(m^2\Delta\xi^2+n^2\Delta\eta^2\right)\right]\cdot \\ &\quad \sum_{k=0}^{N-1}\sum_{l=0}^{N-1}U_{d0}(k,l)\exp\left[\mathrm{j}\frac{2\pi}{N}(km+ln)\right]\cdot \\ &\quad \exp\left[\mathrm{j}\frac{\pi}{\lambda d_0}\left(k^2\Delta x_0^{\,2}+l^2\Delta y_0^{\,2}\right)\right] \end{aligned} \tag{1}$$

其中，λ 为波长，k, l, m, n=0, 1, …, N−1。

采用同样的离散处理方法对透镜的复振幅透过率函数进行离散计算，得到其离散形式：

$$\chi(m,n;f)=\exp\left[-\mathrm{j}\frac{K}{2f}\left(m^2\Delta\xi^2+n^2\Delta\eta^2\right)\right] \tag{2}$$

其中，f 为透镜焦距，波数 $K=2\pi/\lambda$。

在加密过程中，可以用 DFD 分别计算信息平面到透镜前表面的衍射和随机模板到透镜前表面

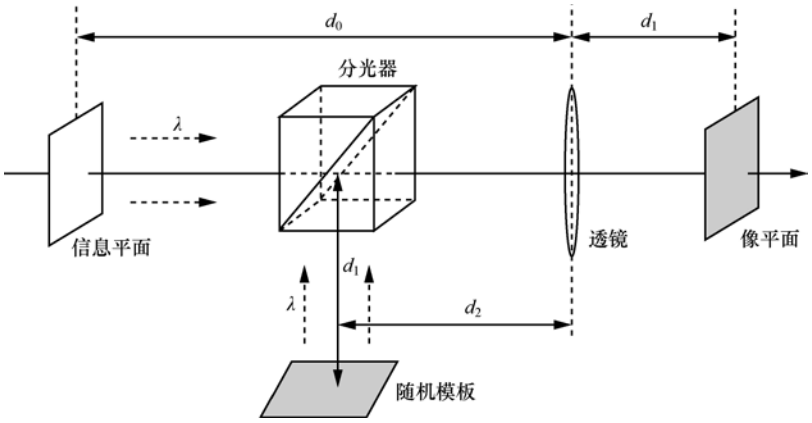

图 1 虚拟光学加密系统的理论模型结构

的衍射，衍射距离分别为 d_0 和 d，其中，$d=d_1+d_2$。它们在透镜前表面就产生了有干涉的菲涅耳衍射图，干涉图又经透镜的复振幅透过率函数的转换到达透镜的后表面。而密文就是成像透镜后表面的复振幅分布 U_{L2}，加密过程可以简单地用式(3)描述。

$$U_{L2}(m,n)=\{DFD[U_{d0}(k,l);\lambda,d_0]+DFD[U_{rd}(k,l);\lambda,d]\}\chi(m,n;f) \tag{3}$$

解密过程为上述加密过程的逆运算过程，事实上，有：

$$DFD[U_{d0}(k,l);\lambda,d_0]=U_{L2}(m,n)/\chi(m,n;f)-DFD[U_{rd}(k,l);\lambda,d] \tag{4}$$

则有：

$$U_0(x_0,y_0)=IDFD[U(k,l);\lambda,d_o] \tag{5}$$

其中，*IDFD* 为逆菲涅耳变换。

从解密过程可以看出，要想完全解密出原信息，除了随机模板外，还需要知道 4 个参数，即 d_0、d、f、λ，这些密钥参数需要从发送端安全传送到接收端。下面的算法给出了这些参数具体的传输过程。

算法 3　加密/解密参数传输算法。

输入：发送端选择的光学加密参数 Θ，接收端标识 ID_r

输出：接收端获取光学加密参数 Θ。

步骤 1　加密光学参数：根据接收端的标识 ID_r，执行算法 1 中的 Encrypt 算法，其输入为光学加密参数 Θ 和接收端标识 ID_r，生成加密密文 c，并发送给接收端。

步骤 2　获取光学参数：接收端获取密文 c，执行算法 1 中的 Decrypt 算法，解密得到光学加密参数 Θ。

3) 新加入用户的密钥生成

一个完整的密钥管理系统应该包含对新用户加入的密钥生成算法，以实现系统的可扩展性。设新用户的标识为 ID_n，基于 IBE 算法，算法 4 为新用户生成非对称密钥系统的私钥，使新用户在该密钥的基础上获取光学加密参数，或其他机密信息。具体算法如下。

算法 4　新用户密钥分配算法。

输入：新用户标识 ID_n。

输出：新用户的密钥。

步骤 1 新用户向 PKG 发送加入请求，并发送标识 ID_n。

步骤 2　PKG 执行算法 2 中密钥生成算法 KeyGen，新用户 ID_n 获得非对称密钥系统的私钥，将用于光学参数的传输等。

4) 密钥更新

为了系统的安全，密钥管理系统有时需要对系统的密钥进行更新，算法 5 给出了系统密钥更新过程。

算法 5　系统密钥更新算法。

输入：密钥空间长度 k，群的阶 q。

输出：公共参数 π，各用户的密钥。

情况 1　采用已有的公共参数。

步骤 1　PKG 取 $\psi=\{q, p, \hat{e}, n, P, P_{\text{pub}}, H_1, H_2\}$，及新的主密钥 s'，根据节点标识 ID 和公共参数 ψ，PKG 执行 IBE 算法中的 Extract 算法，生成用户的新密钥 $K_{\text{ID}'}$。

步骤 2　PKG 取新密钥 $K_{\text{ID}'}$为明文，用旧密钥 K_{ID} 执行 IBE 算法中的 Encrypt 算法，得到密文 c。

步骤 3　PKG 将密文 c 发送用户 ID，该用户根据自己的私钥执行 IBE 算法中的 Decrypt 算法，得到新的密钥 $K_{\text{ID}'}$，并更新密钥。

情况 2　采用新的公共参数。

步骤 1 根据密钥长度 k 和参数 q，PKG 执行 IBE 算法中的 Setup 算法，生成新的公共参数 $\psi'=\{q, p, \hat{e}, n, P, P_{\text{pub}}, H_1, H_2\}$和选取新的主密钥 s'。

步骤 2　根据节点标识 ID 和新公共参数 ψ'，PKG 执行算法 1 中的 Extract 算法，生成用户的新密钥 $K_{\text{ID}'}$。

步骤 3　PKG 取新密钥 $K_{\text{ID}'}$为明文，用旧密钥 K_{ID} 执行算法 1 中的 Encrypt 算法，得到密文 c。

步骤 4　PKG 将密文 c 发送用户 ID，该用户根据自己的私钥执行算法 1 中的 Decrypt 算法，得到新的密钥 $K_{\text{ID}'}$，并更新密钥。

在密钥的更新过程中，一般情况下采用已有的公共参数能够满足密钥更新的安全，除非对安全性要求特别严格的系统，可以在每次更新时，重新计算公共参数。因为事实上公共参数是公开的信息，所以对攻击者来说，安全性不依赖于这些公共参数。

4　方法性能分析

本节将分析上节提出的密钥管理方案的效益和安全性，主要讨论方法复杂性和安全性等。

1) 复杂性分析

在本文的方案中，使用 IBE 算法 1 产生非对称密钥对，并利用该密钥对进行光学加密参数的安全

传输。在非对称密钥对中，公钥是用户的标识，所以不需要计算公钥，计算量主要在计算私钥过程中。同时，公共参数 ψ 的计算由 PKG 完成，且主要在系统生产阶段或更新阶段才需计算，所以，可以不讨论计算公共参数的复杂性，而主要考虑基于 IBE 算法的加密解密过程的复杂性。必须指出的是，在一些光学标签的应用中，由于标签节点的资源相对有限，如内存、计算能力、电源等的限制，希望密钥管理系统的计算量相对小。

本文的方法包含了 4 个算法，实现非对称密钥对的生产、对光学加密参数的加密传输、新用户加入后的密钥分配和密钥对的更新等。算法 2 负责生成公共参数，一般在系统初始化时执行一次，同时计算主要为群的乘法和散列函数运算，涉及 IBE 算法中的 Setup 和 Extract 部分，算法 4 主要调用算法 2 中的密钥生成算法 KeyGen，所以与算法 2 具有同等的复杂性；算法 5 是对系统的密钥对进行更新，除涉及 IBE 算法中的 Setup 和 Extract 外，还应用 Encrypt 和 Decrypt 完成新密钥的加密传输；算法 3 主要执行 IBE 算法中的 Encrypt 和 Decrypt 算法。在 IBE 算法中 Encrypt 和 Decrypt 算法的复杂性最高，因为要进行双线性对的计算。所以在本文的方法中，算法 3 和算法 5 的计算复杂性较高。

事实上，Encrypt 和 Decrypt 算法主要需要进行散列函数、 XOR 运算和双线性映射运算等，具体复杂性如表 1 所示。

表 1 计算复杂性

运算	基本 IBE 算法（算法 1）	
	Encrypt 加密过程	Decrypt 解密过程
$\hat{e}$ 运算	1	1
散列运算	2	1
XOR 运算	1	1
乘法运算	1	0
指数运算	1	0

2) 安全性分析

基于身份标识的加密算法是椭圆曲线类型的算法 ECC(elliptic curve cryptography)，文献 [16]就不同的密钥长度分别对椭圆曲线算法和 RAS 算法进行了比较，结果表明，非对称密钥算法在无需硬件加速条件下，也可以在微处理器上实现。同时在安全性能相当的情况下，椭圆曲线算法的密钥长度也只是对称密钥算法密钥长度的一倍。表 2 给出了在同等安全条件下，ECC、RSA 和对称密钥算法密钥长度的比较。

表 2 ECC、RSA 和对称密码算法密钥长度的比较

对称密钥算法	ECC 方案（IBE 算法）	RSA
56	112	512
80	160	1 024
112	224	2 048

从表 2 可以看出，ECC 算法的 160bit 与 RAS 的 1 024bit 处于同一安全水平，但密码长度要短得多。

另一方面，由于采用基于身份标识的密钥机制，其公钥可以是任何唯一的字符串，如 E-mail 地址、身份证号、二维条码标识或其他标枳。它的优点是公钥是可识别的，不需要通常 PKI 系统的证书发放，也就省去了用户的认证过程，使非对称密钥对的分配更为安全可靠，增强了本文方法的安全性，也减低了密钥管理系统的计算复杂性。

3) 与其他方法的分析比较

在基于虚拟成像光学的加密系统中如何实现对称加密参数的分发、更新、删除等管理是系统理论与应用研究的关键问题之一。利用非对称密钥系统进行对称密钥的分配是常用的有效手段，文献[4]对此问题进行了研究，提出了一种分配光学加密参数的方法，与本文的方法比较有以下不同点。一是对初始的非对称密钥系统的形成，文献[4]没有给出具体的方法，这是后继发送光学加密参数的基础，本文给出了如何建立具体的基于身份标识的加密系统进行光学加密参数的分发；二是一般的非对称密钥系统需要可信第三方的认证，包括文献[4]提出了方法。而基于身份标识的加密系统不需要进行身份认证，共钥本身就是接收方的身份标识，使光学加密参数的发送算法可简单化，也是本文的创新点。当然，目前基于身份标识加密系统的实现算法比较单一复杂，有待进一步寻求新的双线性对的计算方法。

5 仿真实验及其结果

为检测基于身份密钥机制的光学加密的密钥管理系统模型的性能，利用 MATLAB 软件对基于虚拟成像的多维数据加密系统系统和基于 4f 系统的双随机相位编码进行数字仿真。设置一个 PKG 负责非对称密钥的生成与管理，IBE 算法的密钥空

间长度 k=112，群的阶 q 为一个 112bit 的素数，光学原信息为二维码。

1) 虚拟光学加密系统

图 2 是基于虚拟成像的密码系统对于二维码的加密和解密的仿真实验结果，所用的图像信息为 132×132 的二维码。图 2(a)是原始二维码，该二维码经系统加密后的结果如图 2(b)所示。用于模拟随机光场的随机模板是在 MATLAB 中用 rand()函数生成的(132×132)二维伪随机阵列，如图 2(c)所示。在解密过程中，如果没有加密时所用的随机模板密钥，解密得到的图像还是可以看到原始图像的大概轮廓，尤其对于二维码而言，这样就会得出隐藏其中的信息，如图 2(d)所示。只有当所有的密钥参数全部正确，又知道随机模板密钥，才可以得到清晰的解密结果，如图 2(e)所示。通过仿真可以看出，如果除了随机模板，其他参数信息（包括信息平面和随机模板到透镜前表面的衍射距离 d_0 和 d，透镜焦距 f，光波波长 λ）一旦泄露，那么加密的信息就有攻破的可能性，图 3 给出了衍射距离 d_0 对信息加密的影响，当 d_0 与其实际值只有 0.000 001cm 偏差时，解密的结果已接近明文。因此，对光学加密参数需要进行安全的传输，才能使其加密的功能得到体现，本文提出的基于 IBE 的加密机制为此提供了一个解决方案。

2) 基于 4f 系统的双随机相位编码加密系统

基于 4f 系统的双随机相位编码的加密过程只涉及傅里叶变换和逆傅里叶变换。图 4 是基于 4f 系统的双随机相位编码对于二维码的加密和解密的仿真实验结果，所用的图像信息为 132×132 的二维码。从图 4 中可以看出，该系统也可以正确还原出原信息。但若解密密钥不正确，就无法还原二维码图像，解密结果如同是随机的白噪声。

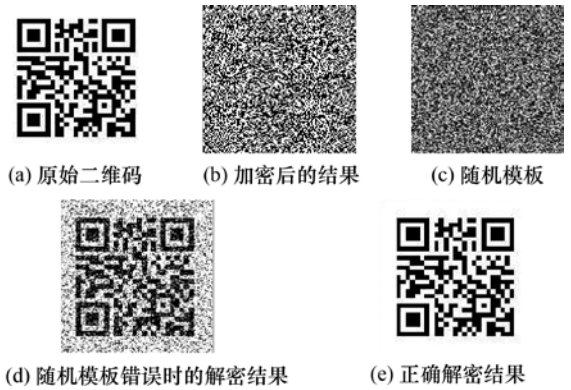

图 2　基于虚拟成像的密码系统的二维码加密和解密实验结果

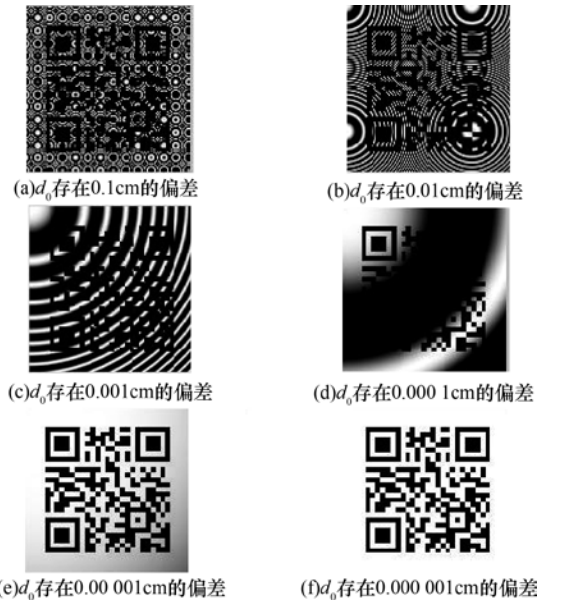

图 3　信息平面到透镜前表面的衍射距离 d_0 对信息加密的影响

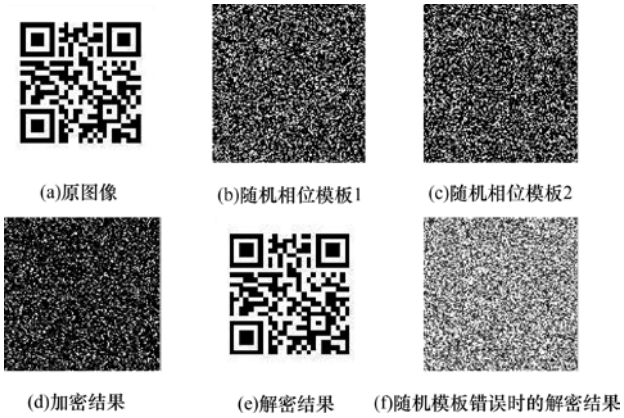

图 4　基于 4f 系统的双随机相位编码对二维码的加密和解密结果

6　结束语

基于光学理论与方法的密码技术近年来引起了人们的高度重视，与传统基于数学的计算机密码学相比，光学密码技术具有多维、大信息量、多自由度、固有的并行数据处理能力等诸多优点，特别是光学二维码等方面的应用，为光学加密技术提出了新的挑战，如光学加密参数的选择、传输、更新等问题。非对称密码技术具有通信双方不必事先建立关系、能有效进行数据完整性检验、密钥管理容易等优点，特别是基于身份标识的加密机制无需进行认证过程，它是基于椭圆曲线的密钥系统，与传统了非对称密钥系统相比，如 RSA 等，在同等密钥长度情况下，其安全强度高等特点。

本文利用 IBE 的高安全性和身份为公钥的特征，将非对称密钥系统与光线加密系统有效地结合

起来，提出了一个基于 IBE 加密机制的光学加密系统的密钥管理方案，给出了具体的密钥生成、更新、加入等算法，解决了光学加密系统的加密参数的安全传输和管理等问题。理论分析表明，方案能实现通信双方的密钥生成和更新等功能，其安全性建立在 Diffie-Hellman 问题复杂性基础上，为光线加密参数的安全传输提供了手段。针对当前应用日益广泛的二维码加密问题，通过对虚拟光学加密系统和基于 4f 系统的双随机相位编码的加密系统的仿真实验，结果表明了方案的正确性和有效性。实验同时也表明了光学加密参数对原图像信息恢复的影响，由于目前的光学加密系统大多采用对称加密形式实现，因此，用来进行加密的光学参数就必须以一个极其安全的传输渠道发送给对方，以保证加密信息的安全，而本文基于 IBE 密钥管理系统的高安全性能够很好地解决这一问题。另外寻求该方法在实际中的应用，特别是在物联网中的应用将是很有意义的工作。

参考文献：

[1] 张鹏, 彭翔, 牛憨笨. 一种虚拟光学数据加密的系统实现[J].电子学报,2004,32(10):1585-1588.
ZHANG P, PENG X, LIU H B. An implementation scheme of virtual optics based data encryption system[J]. Chinese Journal of Electronics, 2004,32(10):1585-1588.

[2] 高丽娟,杨晓苹,李智磊等.一种单通道彩色图像加密方法[J].物理学报，2009,58(2):1053-1056.
GAO X L, YANG X P, LI Z R, *et al*. A encryption algorithm for single channel color picture[J]. Acta Physica Sinica, 2009,58(2):1053-1056.

[3] 袁建国，梁天宇，李柚等.基于双密钥分割合成滤波的相位编码的密钥恢复算法[J]. 光电子·激光,2011,22(4):607-611.
YUAN J G, LIANG T Y, LI Y, *et al*. A key retriveal algorithm for the phase-coding based on segmented composite filtering[J]. Journal of Optoelectronicos·Laser, 2011,22(4):607-611.

[4] 张鹏，彭翔. 基于公钥的虚拟光学信息安全系统[J].系统仿真学报,2006,18(1):176-180.
ZHANG P, PENG X. Information security system based on public key and virtual-optics encryption[J]. Journal of System Simulation, 2006,18(1):176-180.

[5] 吴克难,胡家升,乌旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展,2008,45(7):30-38.
WU K N, HU J S, WU X. Optical encryption in information security[J]. Laser & Optoelectronics Progress, 2008,45(7):30-38.

[6] CHEN W, CHEN X D. Space-based optical image encryption[J]. Optics Express, 2010, 18(26): 27095-27104.

[7] HAN Y J, ZHANG Y H. Optical image encryption based on two beams' interference[J]. Optics Communications, 2010,283(9): 1690-1692.

[8] ISLAM M M, KARIM M A. Optical encryption system employing orthogonal code and multiple reference-based joint transform correlation[A]. Computer and Information Technology (ICCIT), 13th International Conference[C]. 2010. 470-475.

[9] LIN G S, CHANG H T, LIE W N, *et al*. Public-key-based optical image cryptosystem based on data embedding techniques[J]. SPIE Digital Library, 2003, 42(8): 2331-2339.

[10] SHAMIR A. Identity-based cryptography and signature schemes[A]. CRYPTO'84, Lecture Notes in Computer Science[C]. Berlin, Springer-Verlag, 1985. 47-53.

[11] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[A]. CRYPTO 2001, Lecture Notes in Computer Science[C]. Berlin, Springer-Verlag, 2001. 213-229.

[12] ANIKET K, IAN G. Distributed private-key generators for identity-based cryptography[A]. Security and Cryptography for Networks[C]. 2010.436-453.

[13] ABDALLA M, BIRKETT J, CATALANO D, *et al*. Wildcarded identity-based encryption[J]. Journal of Cryptology, 2011, 24(1): 42-82.

[14] 杨庚，陈伟，曹晓梅.无线传感器网络安全[M]. 北京: 科学出版社，2010.
YANG G, CHEN W, CAO X M. Security in Wireless Sensor Network[M]. Beijing: Science Press, 2010.

[15] BOYEN X. Multipurpose identity-based signcryption, a Swiss army knife for identity-based cryptography[A]. Lecture Notes in Computer Science[C]. Berlin, Springer-Verlag, 2003. 383-399.

[16] GURA N, PATEL A, WANDER A, *et al*. Comparing elliptic curve cryptography and RSA on 8-bit CPU[A]. Proceedings of the Workshop on Cryptography Hardware and Embedded Systems (CHES 2004)[C]. Boston, 2004. 11-13.

作者简介：

徐宁（1960-），女，江苏南京人，硕士，南京邮电大学副教授，南京邮电大学光电工程学院副院长，主要研究方向为光通信理论与技术和光学信息安全。

杨庚（1961-），男，江苏建湖人，南京邮电大学教授、博士生导师，主要研究方向为计算机通信与网络、网络安全、分布与并行计算等。