一种可用于光学密码的安全增强工作模式

袁 科[①] 贾春福*[①] 吕述望[②] 黄贻望[③] 高社成[④]
[①](南开大学信息技术科学学院 天津 300071)
[②](中国科学院信息安全国家重点实验室 北京 100083)
[③](武汉大学软件工程国家重点实验室 武汉 430072)
[④](南开大学光学信息技术教育部重点实验室 天津 300071)

摘 要：为满足云计算对高安全、高效率密码方案的需求，该文提出一种安全增强密码工作模式——密码反馈“一组一密”(Cipher FeedBack one Block one Key, CFB-BK)模式，并基于数学密码和光学密码组合实现：光学密码对数据分组进行“一组一密”加解密，数学密码利用光学密码密文生成供光学密码下一组数据加解密使用的密钥。安全性分析表明，攻击者在密码学技术范围内，只能采用穷举密钥攻击方式，攻击复杂度高；效率分析表明，比基于数学密码实现的模式效率更高。

关键词：云计算；光学密码；数学密码；密码反馈一组一密模式；一组一密
中图分类号：TP309.07 **文献标识码**：A **文章编号**：1009-5896(2013)03-0735-07
DOI: 10.3724/SP.J.1146.2012.00930

A Security Enhanced Mode of Operation Can Be Used in Optical Cryptography

Yuan Ke[①] Jia Chun-fu[①] Lü Shu-wang[②] Huang Yi-wang[③] Gao She-cheng[④]
[①](*College of Information Technical Science*, *Nankai University*, *Tianjin* 300071, *China*)
[②](*State Key Laboratory of Information Security*, *Chinese Academy of Sciences*, *Beijing* 100083, *China*)
[③](*State Key Laboratory of Software Engineering*, *Wuhan University*, *Wuhan* 430072, *China*)
[④](*Key Laboratory of Optical Information Science and Technology*, *Ministry of Education*, *Nankai University*, *Tianjin* 300071, *China*)

Abstract: For meeting the high security and high efficiency of cryptography schemes in Cloud Computing, a security enhanced cryptographic mode of operation named Cipher FeedBack one Block one Key (CFB-BK) is proposed, and this mode is implemented based on the combination of mathematical cryptography and optical cryptography. Optical cryptography module encrypts (or decrypts) data blocks in a “one block one key” way. Moreover, it provides its ciphertext as a feedback to the mathematical cryptography module, which uses it to generate keys for the next block encryption (or decryption) of the optical cryptography module. Security analysis shows that the only possible attack in the area of cryptography for the proposed scheme is exhaustive attack, indicating that no adversary could get a significant advantage against the scheme without spending a huge amount of recourses and time. Efficiency analysis shows that the scheme implementing CFB-BK mode works much faster than the existing modes implemented based on mathematical cryptography.

Key words: Cloud computing; Optical cryptography; Mathematical cryptography; Cipher FeedBack one Block one Key (CFB-BK) mode; One block one key

1 引言

密码学是信息安全的核心技术，密码体制可基于数学知识，也可基于物理、生物等学科知识。为表述方便，本文中，我们称基于数学知识的密码体制为数学密码，称基于光学知识的密码体制为光学密码。

数学密码体制，无论是密码算法，还是密码模块，都相对成熟，是目前保障信息安全的主流密码技术。数学密码体制中，对称密码加密速度比非对称密码快。对于分组密码而言密码分组链接(Electronic Code Book, ECB)并行工作模式可提高

2012-07-19收到，2012-10-26改回
国家自然科学基金(60973141, 61272423)，国家重点基础研究发展计划项目(2013CB834204)和高等学校博士学科点专项科研基金(20100031110030)资助课题
*通信作者：贾春福 cfjia@nankai.edu.cn

工作效率，但这种模式不安全，且基本加密单元仍是串行的。密码分组链接(Cipher Block Chaining, CBC)等工作模式可增强安全性，但属于串行工作模式。对于序列密码而言，加密是串行工作方式。总之，数学密码算法相对安全成熟，但基本加密单元是串行工作方式，属串行密码算法，不能从根本上解决高速加密问题。

光学密码体制中，输入端明文模板一经光线照射，输出端可立刻得到密文。具体而言，光学密码单幅(甚至多幅)图像(相当于数学分组密码的单个分组)的所有像素(相当于数学密码加密中的 1 位或多位)的加解密是并行的，并且每一个像素的加解密是即时的。也即，光学密码基本加解密单元是并行的，属并行密码算法。另外，光学密码分组长度非常长。因此，光学密码可以解决海量数据高速加密问题。但已有论文针对部分光学对称密码，成功实施了选择密文攻击(Chosen Ciphertext Attack, CCA)[1]、选择明文攻击(Chosen Plaintext Attack, CPA)[2−4]、已知明文攻击(Known Plaintext Attack, KPA)[2,5−7]，文献[8–12]等提出了光学密码增强方案，文献[13–15]针对文献[8]的方案提出了新的攻击方法；文献[16]针对光学非对称密码提出了攻击方法。其它目前认为是安全的方案，即尚无能对其实施有效攻击的方法，也几乎没有经过在长期实践应用中的安全检验，其安全性是不能令用户放心的。

从国家安全战略考虑，云计算必然会被高度重视。因为云计算拥有庞大的计算资源，可被用以破解密码算法。因此，应设计新型的安全密码算法或新型的密码工作模式，以应对云计算对密码算法构成的威胁。另外，云计算拥有的计算资源可被客户使用，以减少客户成本。从信息安全考虑，客户需要对传输至云服务器的信息进行加密。由于客户，特别是大型公司等，需要加密的数据量庞大，这对高速加密提出了要求。因此，云计算需要既安全，又高效的密码解决方案。

分组密码工作模式是利用分组密码解决实际问题的密码方案。好的工作模式可弥补分组密码的某些缺憾；相反，不好的工作模式可能带来安全隐患[17]。不同的工作模式有不同的适用场景。CBC 模式适用于数据加密，但 CBC 模式存在一些安全问题。文献[18]提出了抗 CPA 的 HCBC 模式，文献[19]提出了抗 CCA 的 HPCBC 模式，文献[20]提出了抗 CCA 的 MHCBC 和 MCBC 模式。上述安全增强工作虽然都提高了 CBC 的安全性，但却降低了 CBC 的工作效率。另外，上述安全增强模式也不便于采用光学密码实现无损二进制数据加解密。原因是上述模式涉及对数据明/密文进行变换操作，光学实现会增加光学密码系统复杂度，并产生更多的系统误差，从而提升误码率。

根据 Shannon 完善保密性，“一次一密”密码体制是具有完善保密性的密码体制。但是，“一次一密”由于需要大量的密钥，带来了严重的密钥管理问题。如何既规避密钥管理问题，又可实现“一次一密”，是一个富有挑战性的问题。文献[21]提出一种基于混沌序列产生“一组一密”密钥供 IDEA 使用的方案。该方案是一种类“一次一密”方案，安全性高，但其加密效率只有 IDEA 的一半。

总之，上述安全增强工作模式，无论是对 CBC 的安全增强，还是基于类“一次一密”提出的安全方案，都不是既高安全，又高效率的模式。

本文提出一种新型“一组一密”工作模式，并将其应用于光学密码，结合数学密码的安全性和光学密码的并行高速性，来增强密码应用的安全性和高效性。第 2 节对论文用到的术语进行说明；第 3 节介绍 CFB-BK 工作模式，并基于数学密码和光学密码实现该模式；第 4 节给出模式的安全性分析；第 5 节给出模式的性能分析和模式特点；最后是结束语。

2 术语说明

为表述方便，论文中多处出现的相关术语定义如下：

加密用户明文数据的光学分组密码算法，记为光学数据加密算法 F_{ode}，其明文分组记为 P^i_{ode}，密钥记为 K^i_{ode}，空域密钥记为 K^i_s，频域密钥记为 K^i_f，密文分组记为 C^i_{ode}，分组长度记为 n_{ode}，密钥长度记为 k_{ode}，加密操作记为 E^{ode}_K，解密操作记为 D^{ode}_K，一组明密文变换时间记为 t_{ode}，数据总分组数记为 l。密钥生成器中采用的数学分组密码算法，记为密钥生成算法 F_{mkg}，其待处理消息分组记为 M^i_{mkg}，明文分组记为 P^i_{mkg}，密钥记为 K_{mkg}，密文分组记为 C^i_{mkg}，分组长度记为 n_{mkg}，密钥长度记为 k_{mkg}，加密操作记为 E^{mkg}_K，解密操作记为 D^{mkg}_K，一组明密文变换时间记为 t_{mkg}。密钥流生成器中，保密初始向量记为 **SIV**，初始向量记为 **IV**；初始化保密参数记为 P_{is}，去相关性保密参数记为 P_{ds}；初始化密钥流生成器操作记为 I_{mkg}，其花费时间记为 t_{imkg}；密钥流生成器数据扩展操作记为 G_{de}，对密文 C^i_{mkg} 进行数据扩展后的数据记为 D^i_e；一组数据扩展时间记为 t_{de}，密钥流生成器生成一组光学密钥的时间记为 t_{okg}。

3 可用于光学密码的 CFB-BK 工作模式

密码反馈模式(Cipher FeedBack, CFB)，由分

组密码加密上一组密文产生提供本组加解密使用的密钥流，实现自同步序列密码功能。类似的，我们定义密码反馈“一组一密”工作模式如下：

定义 1　密码反馈“一组一密”(Cipher Feed Back one Block one Key, CFB-BK)工作模式，数据加解密算法对数据分组进行“一组一密”加解密操作，密钥生成器中的分组密码利用数据加解密算法的密文生成供下一组数据加解密使用的密钥。数学公式描述如下，加密：$C_i = E_{K_i}^{de}(P_i)$，$K_i = F_{cs}(E_K^{kg}\cdot(F_{ps}(C_{i-1})))$；解密：$P_i = D_{K_i}^{de}(C_i)$，$K_i = F_{cs}(E_K^{kg}(F_{ps}\cdot(C_{i-1})))$。其中，$i \in Z^+$，$C_0 = \mathbf{SIV}$；$E_K^{de}$，$D_K^{de}$ 和 E_K^{kg}，分别是数据加密操作、数据解密操作和密钥生成器中的加密操作；F_{ps}，F_{cs} 分别是明文和密文遮蔽操作。

本文采用数学密码与光学密码组合实现 CFB-BK 工作模式，简称 CFB-BK 数光实现模式。数学分组密码产生密钥流供光学分组密码使用，光学密码对数据进行“一组一密”加解密，如图 1 所示。通信双方每次进行保密通信，都要完成下述 3 个步骤：系统初始化、密钥流生成、数据加解密。

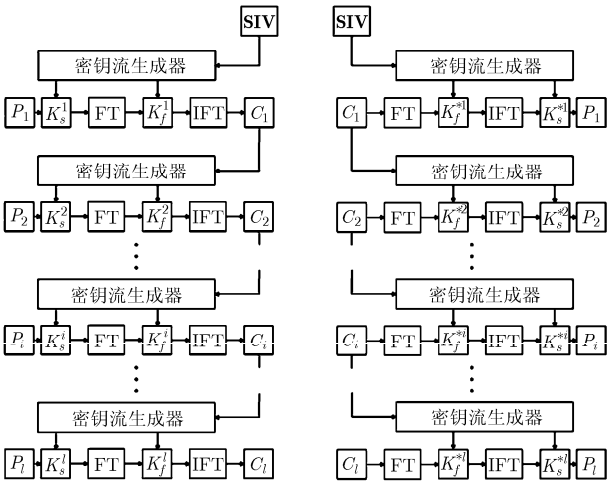

图 1 CFB-BK 数光实现模式抽象示意图

3.1 系统初始化

通信双方每次开始新的保密会话都要首先进行系统初始化。具体初始化算法如下：

(1)如果发送方 A 与接收方 B 之间，之前进行过保密通信，且 K_{mkg}，P_{is}，**SIV** 还在有效期内，则 A 更新 **IV**，转到第(4)步。否则，转到第(2)步。

(2)A 生成 K_{mkg}，P_{is}，**SIV**，**IV**，保密传输 K_{mkg}，P_{is}，**SIV** 至接收方 B。

(3)A,B 分别进行以下计算：①$C_{mkg}^1 = E_{K_{mkg}}(\mathbf{SIV} \oplus P_{is})$。②定义变量 i，$M \leftarrow C_{mkg}^1$，$H \leftarrow \{0,1\}^0$，数组 $H[8] \leftarrow \{0,1\}^0$；对 $i \leftarrow 0,1,\cdots,7$，分别计算 $\{H[i] \leftarrow HASH_{sha-512}(M), H \leftarrow H \parallel H[i], M \leftarrow M \parallel H[i]\}$。③$P_{ds} \leftarrow H$。

(4)A 将 **IV** 传输至 B，系统初始化结束。

3.2 密钥流产生

从安全增强、数学分组密码和光学分组密码分组长度不一致等因素考虑，密钥流生成器工作流程包括明文遮蔽、加密变换、数据扩展和去相关性。光学密码空域密钥生成算法如下：

(1)明文遮蔽　CFB-BK 数光实现模式以第 i 组光学分组密码密文作为密钥流生成器的输入，并引入密钥流生成器加密变换产生的第 i 组密文，生成密钥流生成器中第 $i+1$ 组被遮蔽明文。数学公式表示如下：$P_{mkg}^i = M_{mkg}^i \oplus C_{mkg}^{i-1}$，$i \in [1,l]$。其中，$M_{mkg}^1 = \mathbf{SIV}$，$C_{mkg}^0 = \mathbf{IV}$；$M_{mkg}^i = C_{ode}^{i-1}[1,\cdots,n_{mkg}]$，$i \in [2,l]$（$C_{ode}^i[1,\cdots,n_{mkg}]$表示从第 i 组光学密码密文提取的前 n_{mkg} 位）。

(2)加密变换　对遮蔽后的明文实现加密变换，数学公式表示如下：$C_{mkg}^i = E_{K_{mkg}}(P_{mkg}^i), i \in [1,l]$。

(3)数据扩展　该实现模式采用密钥扩展算法将分组长度为 n_{mkg} 的数学分组密码密文 C_{mkg}^i 扩展成长度为 n_{ode} 的数据 D_e^i。数学公式表示如下：$D_e^i = G_{de}(C_{mkg}^i), i \in [1,l]$。

对于 $n_{mkg} = 128$，$n_{ode} = 4096$，该实现模式采用 SM4 密钥扩展变形算法进行扩展。此变形算法描述如下：(a) K_0, K_1, K_2, K_3 取值同原算法；

(b)对 $i \leftarrow 4, 5,\cdots,131$，分别计算 $\{t \leftarrow K_{i-1}$；若 i 能整除 4，则 $t \leftarrow T'(t \oplus CK_{i/4})$；$K_i \leftarrow K_{i-4} \oplus t\}$；

(c) $D_e^i = K_4 \parallel K_5 \parallel \cdots \parallel K_{131}$。

(4)去相关性　密钥扩展算法产生的分组之间具有相关性。该实现模式使用去相关性保密参数 P_{ds} 去除数据 D_e^i 内部分组数据的相关性(同时实现数学密码密文遮蔽)，产生光学密码空域密钥：$K_s^i = D_e^i \oplus P_{ds}$，$i \in [1,l]$。

光学密码空域密钥生成流程，如图 2 所示。同理，以 $C_{ode}^i[n_{mkg}+1,\cdots,2n_{mkg}]$ 作为输入，重复上述 4 个步骤，产生光学密码频域密钥：$K_f^i = D_e^{'i} \oplus P_{ds}$。这样就得到光学密码密钥：$K_{ode}^i \leftarrow (K_s^i, K_f^i)$。

3.3 数据加解密

为使 CFB-BK 数光实现模式能做到数据解密无差错，则只能采用无差错解密的光学密码算法(目前，多数光学密码算法只适用于能够容忍数据解密有差错场景)。文献[22]提出的基于双随机偏振(Double Random Polarization, DRP)密码算法可满足上述要求。因此，CFB-BK 数光实现模式中，光学密码采用 DRP 算法实现。CFB-BK 数光实现模

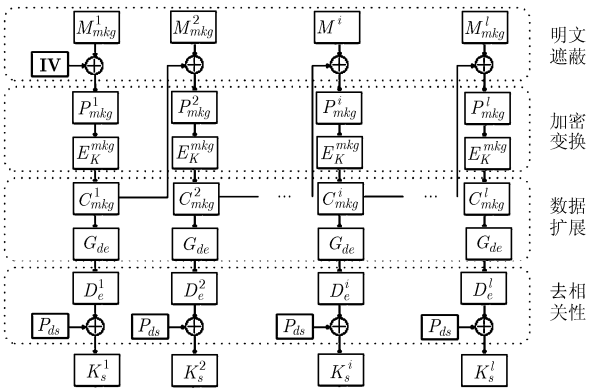

图 2 光学密码空域密钥生成流程

式一组加密过程简化图如图 3 所示，加密过程算法如下：

(1)光学明文分组输入　A 的存储设备上的二进制数据以时长 t_{okg} 为时间间隔，以长度 n_{ode} 为数据分组长度，逐组输入到位于光学输入平面的正交线偏振模板。其中，位‘1’对应竖直方向线偏振，位‘0’对应水平方向线偏振。

(2)光学组密钥导入　密钥流生成器利用上一组密文生成光学密码密钥后，将空域密钥 K_s^i 导入到光学空域偏振调制掩模板，将频域密钥 K_f^i 导入到光学频域偏振调制掩模板。偏振调制掩模板每一像素相位延迟角度 Δ 随机分布于区间 $[0,2\pi]$ 上，偏转角度 θ 随机分布于区间 $[0,\pi/2]$ 上。为使 (Δ,θ) 能够对应二进制位串并增强系统安全性，我们对 Δ 和 θ 进行离散化处理如下：$\Delta_i = 0+(2\pi/15)\times i$，$\theta_j = 0+(\pi/30)\times j$，$i,j = 0,1,\cdots,15$。$(\Delta_i,\theta_j)$ 共有 256 种组合状态，每一状态需要用一个字节来对应。我们设置下列对应关系：$(\Delta_i,\theta_j)\leftrightarrow(16\times i+j)_2$，$i,j=0,1,\cdots,15$。这样偏振调制掩模板每一像素都与一个字节对应。为避免密钥扩张问题，以空域密钥 K_s^i 导入为例，我们令字节 $K_s^i[(i\times 64+j)\bmod n_{ode},(i\times 64+j+1)\bmod n_{ode},\cdots,(i\times 64+j+7)\bmod n_{ode}]$ 对应状态作为像素 $P_{i,j}(i,j=0,1,\cdots,63)$ 的状态。

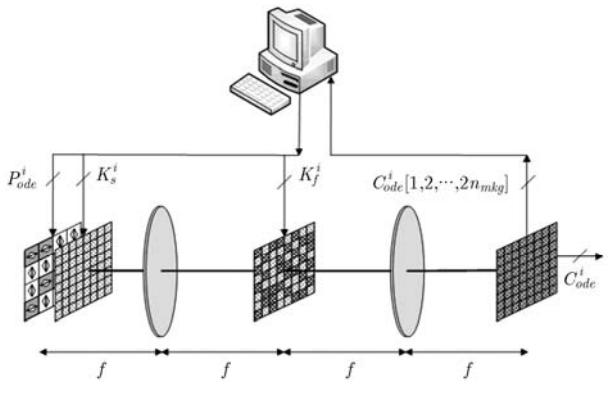

图 3 CFB-BK 数光实现模式一组加密过程简化图

(3)光学加密　明文与密钥导入成功后，按照文献[22]提出的 DRP 加密方案即可完成一组数据加密。

(4)光学密文分组输出　光学密文生成后，经通信链路传输至接收端。同时将密文前 $2n_{mkg}$ (从上至下，从左至右顺序)像素的偏振光偏振方向 α，以 $\alpha\in[0,\pi/2]\cup[3\pi/2,2\pi]\rightarrow$ ‘0’, $\alpha\in(\pi/2,3\pi/2)\rightarrow$ ‘1’方式得到的位串导入密钥流生成器，作为密钥流生成器产生下一组光学密码密钥的新鲜因子。

解密方案是加密方案的逆过程。当矢量相位-共轭光束逆向经过和加密过程在同一位置同一掩模板时，即可恢复明文[22]。

4 安全性分析

假定通信双方能够严格执行安全管理工作，模式的软硬件实现能够采用安全的方法，使得攻击者无法实施边信道攻击等非密码学技术手段。即，我们只限于密码学技术攻击方法范围内的安全性分析。

4.1 定性分析

攻击者首先自然想到攻击密文经由通信链路传输的光学密码。但是 CFB-BK 模式是一种“一组一密”分组密码，且每次新会话都更新 **IV**，攻击者很难得到两组以上使用相同密钥的明密文对。另外，本文基于 DRP 光学密码实现，目前尚无利用一对明密文破解该方案的攻击方法。因此，针对光学密码相对有效的攻击方法 CPA、CCA 无法被实施，攻击者只能采用穷举密钥方式破解。即使破解成功，也得不到其它组密钥，进而无法得到其它组数据明文。

攻击者另一路径是通过破解密钥流生成器，进而利用窃听通信信道等途径获取的密文，得到算法 F_{ode} 所有分组密钥，最终解密数据明文。但这样难度更大。因为，密钥生成器只工作在通信双方本地密码设备中，通信链路中没有算法 F_{mkg} 任何密文信息；另外，虽然密钥流生成器使用算法 F_{ode} 的密文(可通过窃听通信链路获取)作为输入，但并没有将其直接作为算法 F_{mkg} 的明文，而是进行了明文遮蔽操作。因此，攻击者难以通过窃听通信链路获取算法 F_{mkg} 的任何明密文信息，难以针对算法 F_{mkg} 实施诸如 CCA, CPA 等相对有效的攻击手段来破解密钥流生成器。

总之，在密码学技术攻击方法范围内，攻击者针对 CFB-BK 数光实现模式无法实施有效的攻击方

法，以加速破解速度，只能针对上述两条路径之一，采用穷举密钥攻击的方法。

4.2 定量分析

为便于分析两条攻击路径的复杂度，设 $D_m=\{0,1\}^m$ 为问题所有长度为 m 的实例集合，输入实例 $I\in D_m$，其概率记为 $P(I)$，实例 I 所需的基本操作次数记为 $t(I)$；并定义如下概率事件，X，Y，Z，S_1，S_2，S_3。X：攻击者猜中密钥 K_{mkg}，Y：攻击者猜中 **SIV**，Z：攻击者猜中初始化保密参数 P_{is}，S_1：攻击者成功破解一组光学密码密钥 K_{ode}，S_2：攻击者成功破解 K_{mkg} 和 **SIV**，S_3：攻击者成功暴力破解 CFB-BK 数光实现模式。

4.2.1 攻击路径 1　攻击算法包括下述步骤：

(1)攻击者通过某种途径获取 C_{ode}^1，C_{ode}^2，$\cdots$，P_{ode}^{j-1}，C_{ode}^{j-1}，P_{ode}^j，C_{ode}^j，$j\in(1,l]$；对 $i\leftarrow 1,2,\cdots,j-1$，依次计算：$M_{mkg}^{i+1}=C_{ode}^i[1,\cdots,n_{mkg}]$，$M'^{i+1}_{mkg}=C_{ode}^i[n_{mkg}+1,\cdots,2n_{mkg}]$。

(2)攻击者随机猜测 K_{ode}^j。

(3)攻击者计算：$C_{ode}^{'j}=E_{K_{ode}^j}(P_{ode}^j)$。

(4)如果 $C_{ode}^{'j}=C_{ode}^j$，攻击者暴力破解一组光学密钥成功；否则，转到步骤(2)。

(5)攻击者随机猜测一组 K_{mkg}，**SIV**。

(6)攻击者计算：(a)对 $i\leftarrow 1,2,\cdots,j$，依次计算：$\{C_{mkg}^i=E_{K_{mkg}}(M_{mkg}^i\oplus C_{mkg}^{i-1})$，$C'^i_{mkg}=E_{K_{mkg}}(M'^i_{mkg}\oplus C'^{i-1}_{mkg})\}$；其中，$M'^1_{mkg}=M_{mkg}^1=$ **SIV**，$C'^0_{mkg}=C_{mkg}^0=$ **IV**。(b) $D_e^j=G_{de}(C_{mkg}^j)$；$P_{ds}=D_e^j\oplus K_s^j$；$D_e^{j-1}=G_{de}(C_{mkg}^{j-1})$，$D'^{j-1}_e=G_{de}(C'^{j-1}_{mkg})$；$K_s^{j-1}=D_e^{j-1}\oplus P_{ds}$，$K_f^{j-1}=D'^{j-1}_e\oplus P_{ds}$，$K_{ode}^{j-1}\leftarrow(K_s^{j-1},K_f^{j-1})$；$C_{ode}^{'j-1}=E_{K_{ode}^{j-1}}(P_{ode}^{j-1})$。

(7)如果 $C_{ode}^{'j-1}=C_{ode}^{j-1}$，攻击者暴力破解系统成功；否则，转到步骤(5)。

从上述攻击算法可看出，在事件 S_1 发生的前提下，如果事件 S_2 发生，则事件 S_3 发生。由 $P(S_1)=2^{-k_{ode}}$ 可得，暴力破解光学密码密钥这一问题的实例 I 长度 m 为 k_{ode}，又由于各实例等概率，可得事件 S_1 的期望复杂度：$E(S_1)=A(m)=\sum_{I\in D_m}P(I)t(I)=P(I)\sum_{I\in D_m}t(I)=2^{-k_{ode}}\cdot[1+2+\cdots+2^{k_{ode}}]=2^{(k_{ode}-1)}+1/2$。而事件 S_1 的基本操作为一组光学加密，因此，事件 S_1 发生需要耗费的平均时间为

$$[2^{(k_{ode}-1)}+1/2](t_{ode}) \tag{1}$$

由于只有当相互独立事件 X，Y 同时发生，事件 S_2 才能发生，因此，$P(S_2)=P(X)P(Y)=2^{-k_{mkg}}\cdot 2^{-n_{mkg}}=2^{-(k_{mkg}+n_{mkg})}$。可得，暴力破解 K_{mkg} 和 **SIV** 这一问题的实例 I 长度 m 为 $k_{mkg}+n_{mkg}$，又由于各实例等概率，可得事件 S_2 的期望复杂度：$E(S_2)=A(m)=\sum_{I\in D_m}P(I)t(I)=P(I)\sum_{I\in D_m}t(I)=2^{-(k_{mkg}+n_{mkg})}\cdot[1+2+\cdots+2^{(k_{mkg}+n_{mkg})}]=2^{(k_{mkg}+n_{mkg}-1)}+1/2$。而事件 S_2 的基本操作为 $2j$ 次数学密码加密操作，3 次数据扩展操作，1 次光学加密操作，因此，事件 S_2 发生需要耗费的平均时间为

$$[2^{(k_{mkg}+n_{mkg}-1)}+1/2](2jt_{mkg}+3t_{de}+t_{ode}) \tag{2}$$

由式(1)，式(2)可得，该攻击路径下，事件 S_3 发生需要耗费的平均时间为

$$[2^{(k_{ode}-1)}+1/2](t_{ode})+[2^{(k_{mkg}+n_{mkg}-1)}+1/2]\cdot(2jt_{mkg}+3t_{de}+t_{ode}) \tag{3}$$

说明：攻击者首先暴力破解一组光学密码密钥，据此花费很大代价可能能够破解参数 P_{ds}，然后分别随机猜测两组 n_{mkg} 位数据，并使用数据扩展算法扩展至 n_{ode} 位，进行光学密码暴力攻击。但这种方法不仅实施非常困难，且只要采用 $n_{mkg}\geq k_{mkg}$ 的密码算法，都可以使攻击时间复杂度远高于式(3)，我们这里不做论述。

4.2.2 攻击路径 2　攻击算法包括下述步骤：

(1)攻击者通过某种途径获取 C_{ode}^1，C_{ode}^2，$\cdots$，P_{ode}^j，C_{ode}^j，$j\in(1,l]$；对 $i\leftarrow 1,2,\cdots,j-1$，依次计算：$\{M_{mkg}^{i+1}=C_{ode}^i[1,\cdots,n_{mkg}]$，$M'^{i+1}_{mkg}=C_{ode}^i[n_{mkg}+1,\cdots,2n_{mkg}]\}$。

(2)攻击者随机猜测一组 K_{mkg}，**SIV**，P_{is}。

(3)攻击者计算：① $P_{ds}=I_{mkg}(K_{mkg},\mathbf{SIV},P_{is})$；②对 $i\leftarrow 1,2,\cdots,j$，依次计算：$\{C_{mkg}^i=E_{K_{mkg}}(M_{mkg}^i\oplus C_{mkg}^{i-1})$，$C'^i_{mkg}=E_{K_{mkg}}(M'^i_{mkg}\oplus C'^{i-1}_{mkg})\}$；其中，$M'^1_{mkg}=M_{mkg}^1=$ **SIV**，$C'^0_{mkg}=C_{mkg}^0=$ **IV**。③ $D_e^j=G_{de}(C_{mkg}^j)$，$D'^j_e=G_{de}(C'^j_{mkg})$；$K_s^j=D_e^j\oplus P_{ds}$，$K_f^j=D'^j_e\oplus P_{ds}$，$K_{ode}^j\leftarrow(K_s^j,K_f^j)$；$C_{ode}^{'j}=E_{K_{ode}^j}(P_{ode}^j)$。

(4)如果 $C_{ode}^{'j}=C_{ode}^j$，攻击者暴力破解系统成功；否则，转到步骤(2)。

从上述攻击算法可看出，只有当相互独立事件 X，Y，Z 同时发生，事件 S_3 才能发生。由 $P(X)=2^{-k_{mkg}}$，$P(Y)=2^{-n_{mkg}}$ 与 $P(Z)=2^{-n_{mkg}}$ 可得，$P(S_3)=P(X)P(Y)P(Z)=2^{-k_{mkg}}\cdot 2^{-n_{mkg}}\cdot 2^{-n_{mkg}}=2^{-(k_{mkg}+2n_{mkg})}$。因此，该攻击路径下，暴力破解 CFB-BK 数光实现模式这一问题的实例 I 长度 m 为 $k_{mkg}+2n_{mkg}$，又由于各实例等概率，可得期望复杂度：$E(S_3)=A(m)=\sum_{I\in D_m}P(I)t(I)=P(I)\sum_{I\in D_m}t(I)=2^{-(k_{mkg}+2n_{mkg})}\cdot[1+2+\cdots+2^{(k_{mkg}+2n_{mkg})}]=2^{(k_{mkg}+2n_{mkg}-1)}+1/2$。而该攻击路径下，事件 S_3 的基本操作为：1 次系统初始化操作，$2j$ 次数学密码加密操作，2 次数据扩展操作，1 次光学加密操作，因此，事件 S_3 发生需要耗费的平均时间为

$$[2^{(k_{mkg}+2n_{mkg}-1)}+1/2](t_{imkg}+2jt_{mkg}+2t_{de}+t_{ode}) \quad (4)$$

具体地，如果算法 F_{ode} 采用 64×64 像素 DRP 光学密码，算法 F_{mkg} 采用 SM4，则 $k_{mkg}=128$，$n_{mkg}=128$，$k_{ode}=8192$。对于攻击路径 1，由式(3)可得，暴力破解 CFB-BK 数光实现模式需要耗费的平均时间为：$(2^{8191}+1/2)(t_{ode})+(2^{255}+1/2)(2jt_{mkg}+3t_{de}+t_{ode})$。对于攻击路径 2，由式(4)可得，暴力破解 CFB-BK 数光实现模式需要耗费的平均时间为：$(2^{383}+1/2)\,(t_{imkg}+2jt_{mkg}+2t_{de}+t_{ode})$。可见，针对 CFB-BK 数光实现模式，攻击复杂度很高。

5 性能分析与模式特点

5.1 效率分析

CFB-BK 数光实现模式的数据加密采用光学密码算法，加解密速度是光速，但由于“一组一密”密钥由密钥流生成器提供，而密钥流生成器采用数学密码算法进行变换，工作效率的瓶颈在于数学密码的变换速度。因此，我们以一组数学密码加密的耗费时间为基本操作时间，对该工作模式进行效率分析。

CFB-BK 数光实现模式主要耗费时间的操作包括：数学密码一次加密时间 t_{mkg}，密钥流生成器中一组数据扩展时间 t_{de}。密钥流生成器每产生一组光学密钥，都需要两次数学密码加密操作和数据扩展操作，即 $2(t_{mkg}+t_{de})$。如果光学密码采用 64×64 像素明文模板，且每一像素对应 1 位数据，即分组长度为 4096 位，而数学密码采用 SM4，数据扩展算法采用 SM4 密钥扩展变形算法，则 $t_{de}\approx t_{mkg}$。在此情形下，CFB-BK 数光实现模式大约是采用 SM4 实现的 CBC 模式的 8 倍；大约是采用 SM4 实现的 HCBC, HPCBC, MHCBC 和 MCBC 模式的 16 倍；大约是文献[21]所提方案的 16 倍。如果增加光学密码分组长度为上述长度的 n 倍，且并行实现密钥流生成器操作，则可在原基础上再提高至 $2n$ 倍。

5.2 空间需求

CFB-BK 数光实现模式，同 CBC, HCBC 等模式相比，通信双方需要保管的保密数据增加了 $2n_{mkg}$；同 HPCBC 模式相比，通信双方需要保管的保密数据增加了 n_{mkg}。同光学密码相比，保密数据相当于其 $(k_{mkg}+2n_{mkg})/n_{ode}$，极大减少。

5.3 可并行性

CFB-BK 数光实现模式可并行实现。并行实现该模式可视为同时发起的多个新会话且每个会话只执行一组加密操作，由于每组数据加密密钥都不同，可以抵抗分组重放攻击，这是 ECB 模式所不具备的能力。

5.4 模式特点

CFB-BK 数光实现模式灵活性好，既可类似于 ECB 模式并行实现，也可类似于 CFB 模式串行实现，且模式内部密钥流生成器的操作同样即可串行实现，也可并行实现。该模式容错特性是，密文中 1 位错误会影响本组明文分组以及下一组明文分组，同步错误不可恢复。模式实现相对复杂，涉及数学密码实现、光学密码实现、光电-电光转换等操作。

6 结束语

云计算需要高安全、高效率密码方案。而之前的密码增强工作模式能够保障高安全，难以保障高效率；光学密码虽然具备高速并行性，但不能很好地保障安全性。为此，本文提出一种新型的安全增强型密码工作模式——CFB-BK 模式，该模式可用于光学密码，从而可实现数学密码的安全性结合光学密码的高效性，满足云计算对高安全与高效率的需求。

对于 CFB-BK 数光实现模式，攻击者无论是以光学密码为入口，还是以数学密码为入口发起攻击，攻击者都无法对其实施诸如 CCA，CPA 等相对有效攻击方式，在密码学技术攻击方法范围内，只能采用穷举密钥攻击，复杂度很高；同其它基于数学密码实现的安全增强型模式相比，具备高效率。另外，该模式密钥管理负担小，既可串行实现，也可并行实现。不足之处，实现相对复杂。

CFB-BK 模式还可基于数学密码结合数学密码、光学密码结合光学密码、光学密码结合数学密码方式组合实现。每种实现方式都各有其自身特点，适用于不同应用场景，我们将在后续工作中分别予以深入探讨和详细论述。

参 考 文 献

[1] Carnicer A, Usategui M M, Arcos S, *et al*.. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. *Optics Letters*, 2005, 30(13): 1644–1646.

[2] Frauel Y, Castro A, Naughton T J, *et al*.. Resistance of the double random phase encryption against various attacks[J]. *Optics Express*, 2007, 15(16): 10253–10265.

[3] Qin Wan, Peng Xiang, and Meng Xiang-feng. Cryptanalysis of optical encryption schemes based on joint transform correlator architecture[J]. *Optical Engineering*, 2011, 50(2): 028201.

[4] Qin Wan, Peng Xiang, Meng Xiang-feng, *et al*.. Vulnerability to chosen plain-text attack of optoelectronic information encryption with phase-shifting interferometry[J]. *Optical Engineering*, 2011, 50(6): 065601.

[5] Peng Xiang, Zhang Peng, Wei Heng-zheng, *et al*.. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Optics Letters*, 2006, 31(8): 1044–1046.

[6] Gopinathan U, Monaghan D S, Naughton J T, *et al*.. A known-plaintext heuristic attack on the Fourier plane encryption algorithm[J]. *Optics Express*, 2006, 14(8): 3181–3186.

[7] Barrera J F, Vargas C, Tebaldi M, *et al*.. Known-plaintext attack on a joint transform correlator encrypting system[J]. *Optics Letters*, 2010, 35(21): 3553–3555.

[8] Cheng Xue-cai, Cai Lv-zhong, Wang Yu-rong, *et al*.. Security enhancement of double-random phase encryption by amplitude modulation[J]. *Optics Letters*, 2008, 33(14): 1575–1577.

[9] He Ming-zhao, Tan Qiao-feng, Cao Liang-cai, *et al*.. Security enhanced optical encryption system by random phase key and permutation key[J]. *Optics Express*, 2009, 17(25): 22462–22473.

[10] Tashima H, Takeda M, Suzuki H, *et al*.. Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack[J]. *Optics Express*, 2010, 18(13): 13772–13781.

[11] Yuan Sheng, Xin Yan-hui, Tang Ming, *et al*.. An improved method to enhance the security of double random-phase encoding in the Fresnel domain[J]. *Optics and Laser Technology*, 2012, 44(1): 51–56.

[12] Lin Chao and Shen Xue-ju. Analysis and design of impulse attack free generalized joint transform correlator optical encryption scheme[J]. *Optics and Laser Technology*, 2012, 44(7): 2032–2036.

[13] Kumar P, Joseph J, and Kehar S. Known-plaintext attack-free double random phase-amplitude optical encryption: vulnerability to impulse function attack[J]. *Journal of Optics*, 2012, 14(4): 045401.

[14] He Wen-qi, Peng Xiang, and Meng Xiang-feng. A hybrid strategy for cryptanalysis of optical encryption based on double-random phase–amplitude encoding[J]. *Optics and Laser Technology*, 2012, 44(5): 1203–1206.

[15] Kumar P, Kumar A, Joseph J, *et al*..Vulnerability of the security enhanced double random phase-amplitude encryption scheme to point spread function attack[J]. *Optics and Lasers in Engineering*, 2012, 50(9): 1196–1201.

[16] Wang Xiao-gang and Zhao Dao-mu. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Communications*, 2012, 285(6): 1078–1081.

[17] 吴文玲, 冯登国. 分组密码工作模式的研究现状[J]. 计算机学报, 2006, 29(1): 21–36.
Wu Wen-ling and Feng Deng-guo. The state-of-the-art of research on block cipher mode of operation[J]. *Chinese Journal of Computers*, 2006, 29(1): 21–36.

[18] Bellare M, Boldyreva A, Knudsen L, *et al*.. On-line ciphers and the Hash-CBC constructions[C]. Advances in Cryptology -CRYPTO 2001, Springer-Verlag, 2001, LNCS, 2139: 292–309.

[19] Bellare M, Boldyreva A, Knudsen L, *et al*.. On-line ciphers and the Hash-CBC constructions[R]. Cryptology ePrint Archive: report 2007/197, 2007-6-29. Full version of [18].

[20] Nandi M. Two new efficient CCA-secure online ciphers: MHCBC and MCBC[C]. INDOCRYPT 2008, Springer-Vertlag, 2008, LNCS, 5365: 350–362.

[21] 宣蕾, 闫纪宁. 基于混沌的“一组一密”分组密码[J]. 通信学报, 2009, 30(11A): 105–110.
Xuan Lei and Yan Ji-ning. The “one-group-one-cipher” cryptograph of block-cipher based on chaotic[J]. *Journal on Communications*, 2009, 30(11A): 105–110.

[22] Matoba O and Javidi B. Secure holographic memory by double-random polarization encryption[J]. *Applied Optics*, 2004, 43(14): 2915–2919.

袁　科：　男，1982 年生，博士生，研究方向为密码学.

贾春福：　男，1967 年生，教授，博士生导师，研究方向为信息安全、密码学.

吕述望：　男，1941 年生，教授，博士生导师，研究方向为密码学、信息安全.