DOI：10.19789/j.1004-9398.2025.05.005
文献引用：陈奕彤，杨哲，孙东云，等.基于时域鬼成像的保密通信发展[J].首都师范大学学报（自然科学版），2025，46（5）：28-38+46. CHEN Y T，YANG Z，SUN D Y，et al. Development of secure communications based on temporal ghost imaging [J]. Journal of Capital Normal University（Natural Science Edition），2025，46（5）：28-38+46.

基于时域鬼成像的保密通信发展*

陈奕彤，杨　哲**，孙东云，程雅涛，张存林**
（首都师范大学物理系，太赫兹光电子教育部重点实验室，北京　100048）

摘要：时域鬼成像（TGI）可以使用低速探测器探测高速时域信号。基于TGI技术的保密通信系统能够传输超出系统带宽限制的高频光波形，且具有高保密性和安全性。近年来，许多基于TGI技术的保密通信系统相继被提出。本文主要介绍了基于TGI的对称加密和非对称加密通信系统的原理、实验装置的发展历史，以及几种评估保密通信系统品质的方法。

关键词：保密通信；时域鬼成像；非对称加密；光学加密
中图分类号：TN92；O434　　**文献标志码**：A

Development of secure communications based on temporal ghost imaging*

CHEN Yitong，YANG Zhe**，SUN Dongyun，CHENG Yatao，ZHANG Cunlin**
（Department of Physics，Capital Normal University，Key Laboratory of Terahertz Optoelectronics，Ministry of Education，Beijing　100048）

Abstract：Temporal ghost imaging（TGI）enables the detection of high-speed temporal signals using low-speed detectors. Communication systems based on TGI technology can transmit high-frequency optical waveforms that exceed the bandwidth limitations of the system，while also providing high confidentiality and security. In recent years，numerous communication systems utilizing TGI technology have been proposed. This paper primarily discusses the principles and historical development of experimental setups for symmetric and asymmetric encryption communication systems based on TGI，as well as several methods for evaluating the quality of secure communication systems.

Keywords：secure communications；temporal ghost imaging；asymmetric encryption；optical encryption
CLC：TN92；O434　　**DC**：A

0　引　言

1995年，Pittman等[1]首次使用纠缠光子对实现了鬼成像（ghost imaging，GI）。GI通过探测光和参考光之间的关联特性来重构物体的图像。在探测光路中，入射光与物体发生相互作用，产生的透射光或反射光被无空间分辨能力的桶探测器接收，并记录光强；在参考光路中，参考光不与物体发生相

收稿日期：2024-09-04
*国家自然科学基金项目（12104251）；北京市教委科技一般项目（KM202410028020）；国家自然科学基金面上项目（61875140）
**通信作者：yangzhe7010@cnu.edu.cn；cunlin_zhang@cnu.edu.cn

互作用,由具有空间分辨能力的探测器接收,记录含有空间分布的光强信息[2-5],对信号光和参考光信息进行关联计算后能实现对物体图像的重构。

GI技术的实现不仅展示了光学成像的新方法,也为光学信息处理领域带来了新的思考。特别是,随着光学元器件和技术的发展,光学成像与加密技术的结合逐渐成为信息安全领域的一个重要研究方向。光学加密技术作为信息安全重要的手段之一,引起了人们的广泛关注。例如,1995年,Refregier和Javidi[6]提出了基于光学4f系统的双随机相位编码的光学加密方案(光学4f系统是一种在光学和图像处理领域广泛应用的系统,是由物平面、2个焦距为f的透镜和像平面组成,2个透镜间距为2f,中间平面为傅里叶平面)。该方案在4f相干光学系统的空间平面和傅立叶平面中引入2个随机相位掩模,通过这2个独立的随机相位掩模将原始图像转换为平稳白噪声,从而实现了对图片信息的加密。光学元器件和光学系统的不断发展及其日益提高的技术性能也促使光学加密在信息安全应用方面发挥着更大的作用,进而发展出基于分数傅里叶变换、菲涅耳变换和数字全息等技术的不同光学加密技术[7-9]。

2010年,Clemente等[10]首次提出基于GI的光学加密方案。该方案中,随机光场重复照射在图像上获得密文,密文通过信道传输,接收方使用桶探测器获得密文后通过将密文与随机光场相关联来重构明文图像。基于压缩感知(compressive sensing,CS)技术的发展,该方案将图像加密为一个简单的强度向量,能够在相同或更少的实现次数下获得更高品质的解密图像,从而显著提升了加密传输的效率和安全性。基于光学加密的GI可灵活操控一对“信号”和“闲频”光束的位置相关性来加密图像[11],并且桶探测器信号数据量低,这个领域取得了快速发展[12-13]。

2016年,Ryczkowski等[14]利用光在空间和时间上传播的对偶性,提出了时域鬼成像(temporal ghost imaging,TGI),并实现了皮秒级别的时间分辨率。基于TGI的光通信系统可以重构超出系统带宽限制的高速光波形[15-19]。TGI为超快信号检测和光通信提供了新思路。2021年,孙宝清和王玉鹏[20]对TGI领域进行了综述。

TGI的技术原理和实验装置与保密通信具有较高相似性和关联性。TGI技术可以为通信系统提供新的加密手段。基于TGI的保密通信系统具有安全性高、抗噪声能力强和硬件要求低等独特优势。具体而言,基于TGI的通信系统可以传输超过系统光源或探测器带宽限制的信号,低带宽探测器的探测面积大、灵敏度更高及成本较低,有利于提升系统在大衰减环境(如雾霾大气、水下信道)中的适应性;TGI系统天然具有的强抗干扰能力也提升了其用作保密通信系统的抗干扰能力。所以,将TGI的原理运用到保密通信领域发展迅速。2017年,Pan和Zhang[21]将混沌激光TGI技术应用于光学加密;2020年,Wang等[22]使用微型发光二极管(micro-light-emitting diode,Micro-LED)作为发射器实现了基于TGI原理的对称加密光通信系统;2021年,Kang等[23]提出了一种基于TGI的光学混合加密方案,在该方案中实现了对称和非对称的双重加密过程;2022年,Chen等[24]使用Micro-LED作为探测器,实现了基于TGI的可见光对称加密系统。

文章首先介绍了TGI的基本原理及实验装置,基于TGI的一般加密过程以及几种评估通信系统品质的方法,从对称加密和非对称加密2个方面回顾了基于TGI的发展历史,并进行总结与展望。

1 基本原理

1.1 TGI实验装置与理论分析

TGI实验装置见图1,利用激光二极管发射具有强度涨落特性的光,并由光纤分束器分成探测光和参考光。在探测光的路径中使用超快电光调制器(electro-optic modulator,EOM)对入射光的时间强度进行调制,这个调制信号为时间物体,由慢探测器(即桶探测器)接收,并记录该时域调制信号在一段时间内的总光强。慢速探测器的测量带宽远低于时域波形,所以无法直接恢复时域波形。参考光由快探测器接收并记录光强随时间变化的信息。通过多次测量,对接收到的2路光信号进行关联计算后,可以实现对该时间物体的重构。

1.2 基于TGI一般加密过程

基于计算TGI的光学加密通信(图2(a))中,明文($m(t)$)通常由一串二进制序列信号组成(t为时间),密钥($K_i(t)$(i=1,2,…,N))由随机矩阵或Hadamard矩阵($\boldsymbol{H}_i$)组成,其中i为序列号,N为设定的密钥序列总数。

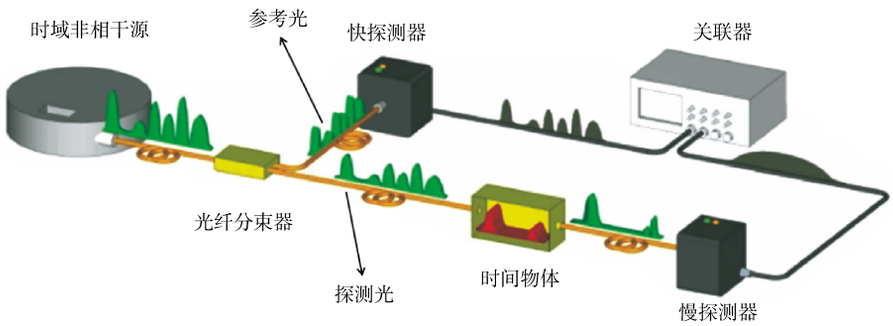


图1　时域鬼成像(TGI)实验装置[14]

加密过程中,将明文和密钥直接相乘并积分从而获得密文(S_i)为

$$S_i = \int K_i(t) \cdot m(t)\mathrm{d}t。 \tag{1}$$

发送方发出的S_i经过信道后变成S_i'。值得注意的是,直接传输未积分信号$S_i(t) = K_i(t) \cdot m(t)$,在接收端完成积分过程也是可行的。

解密过程中,根据TGI理论,使用二阶关联计算对接收密文S_i'进行解密以重建明文。解密算法为

$$m'(t) = \left\langle (S_i' - \langle S \rangle)(K_i(t) - K(t)) \right\rangle, \tag{2}$$

式中:$m'(t)$是解密后的明文;〈 〉是统计平均值。

需要说明的是,明文、密钥、密文和解密后的明文是基于TGI的通信加密中的4个重要概念,在不同的文献中可能用不同的符号表示,如$m(t)$还可以用$O(t)$、$X(t)$和$C(t)$等来表示;$K_i(t)$还可以用$I_n(t)$、$M_i(t)$和$B_i(t)$等来表示;S_i还可以用y_n和D_i来表示;解密后的$m'(t)$还可以用$\tilde{O}(t)$、$\tilde{X}(t)$和$\tilde{C}(t)$等来表示。

实验实现示意如图2(b)所示,代表$m(t)$和$K_i(t)$的电信号都可由信号发生器产生,相乘获得密文,强度调制器对光源产生的光信号进行调制,得到了加载在光信号上的$S_i(t)$。加载了密文的光信号在信道中进行传输,可以由发送方完成积分获得S_i后传输,也可以在接收方完成积分获得S_i'。接收方通过A/D转换器(analog to digital converter,A/D)将S_i'转化为电信号。最后通过计算单元处理,将接收到的信号S_i'进行解密得到明文$m'(t)$。

1.3　评估方法

$m'(t)$与$m(t)$的相似度越高,说明保密通信系统的通信品质越好,相似度评估方法有以下几种:

(1)均方根误差(root mean squared error,RMSE)是一种常用的衡量预测值与实际测量值之间差异的指标,计算公式为

$$E_{\mathrm{RMS}} = \sqrt{\frac{\sum_{t=1}^{n}(m'(t) - m(t))^2}{n}}, \tag{3}$$

式中E_{RMS}表示RMSE,取值为0~1,值越小表明$m'(t)$与$m(t)$相似度越高。

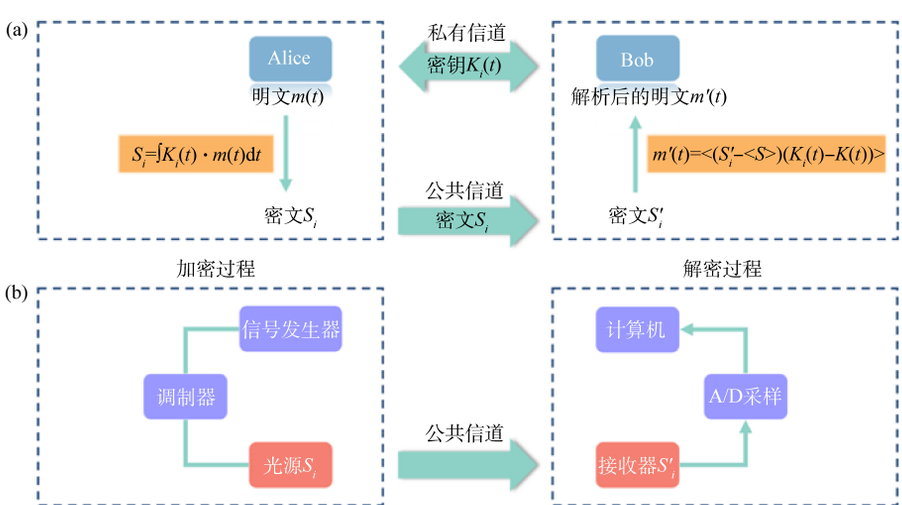


图2　基于TGI的对称加密原理

(a)模型示意;(b)仪器示意

(2)相关系数(correlation coefficient,CC)是一种反映变量之间相关关系密切程度的统计指标,计算公式为

$$C_{\mathrm{C}}=\frac{\left\langle\left(m(t)-\left\langle m(t)\right\rangle\right)\left(m'(t)-\left\langle m'(t)\right\rangle\right)\right\rangle}{\sqrt{\left\langle\left(m(t)-\left\langle m(t)\right\rangle\right)^{2}\right\rangle}\sqrt{\left\langle\left(m'(t)-\left\langle m'(t)\right\rangle\right)^{2}\right\rangle}},\tag{4}$$

式中C_{C}表示CC,取值为-1~1,值越大表明$m'(t)$与$m(t)$相似性越好。

(3)归一化相关性(normalized correlation,NC)是一种用来量化预测值和实际测量值线性相关程度的指标,计算公式为

$$C_{\mathrm{N}}=\frac{\sum_{t=1}^{n}\left(m'(t)-\left\langle m'(t)\right\rangle\right)\left(m(t)-\left\langle m(t)\right\rangle\right)}{\sqrt{\sum_{t=1}^{n}\left(m'(t)-\left\langle m'(t)\right\rangle\right)^{2}}\sqrt{\sum_{t=1}^{n}\left(m(t)-\left\langle m(t)\right\rangle\right)^{2}}},\tag{5}$$

式中C_{N}表示NC,取值为0~1,值越大表明$m'(t)$与$m(t)$相似度越高。

(4)皮尔逊相关系数(Pearson correlation coefficient,PCC)是一种用来衡量2个变量相关性的指标,计算公式为

$$C_{\mathrm{PC}}=\frac{\sum_{t=1}^{n}\left(m'(t)-\left\langle m'(t)\right\rangle\right)\left(m(t)-\left\langle m(t)\right\rangle\right)}{\sqrt{\sum_{t=1}^{n}\left(m'(t)-\left\langle m'(t)\right\rangle\right)^{2}}\sqrt{\sum_{t=1}^{n}\left(m(t)-\left\langle m(t)\right\rangle\right)^{2}}},\tag{6}$$

式中C_{PC}表示PCC,取值为-1~1,其中1表示完全正相关,-1表示完全负相关,0表示无线性相关关系。C_{PC}值越接近1,$m'(t)$与$m(t)$越相似。

(5)峰值信噪比(peak signal-to-noise ratio,PSNR)是一种评价图像的客观标准,其值越大表明$m'(t)$与$m(t)$相似度越高,计算公式为

$$R_{\mathrm{PSN}}=10\lg\left(\frac{E_{\max}^{2}}{\frac{1}{n}\left(\sum_{t=1}^{n}\left[m'(t)-m(t)\right]\right)^{2}}\right),\tag{7}$$

式中:R_{PSN}表示PSNR;$E_{\max}$是图像可能的最大值,一般为255,归一化后为1。

(6)误比特率(bit error ratio,BER)也叫比特误码率、误信率,是指在一定时间内收到的错误信号比特数与收到信号的总比特数之比,计算公式为

$$R_{\mathrm{BE}}=\frac{X_{\mathrm{e}}}{X},\tag{8}$$

式中:R_{BE}表示BER;X_{e}为错误信号比特数;X为信号总比特数。

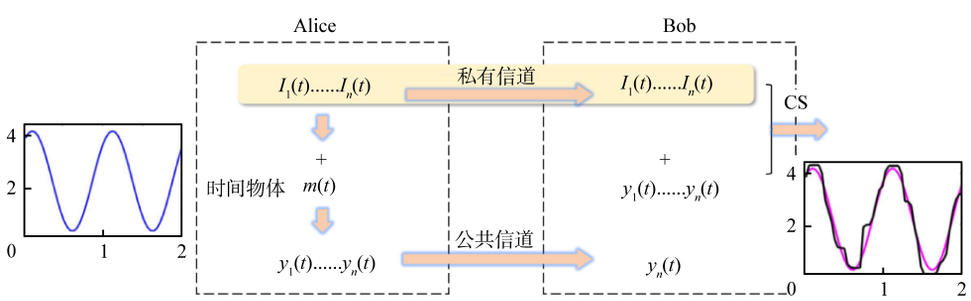
2　发展历史

2.1　对称加密

2.1.1　基于TGI对称加密的相关工作

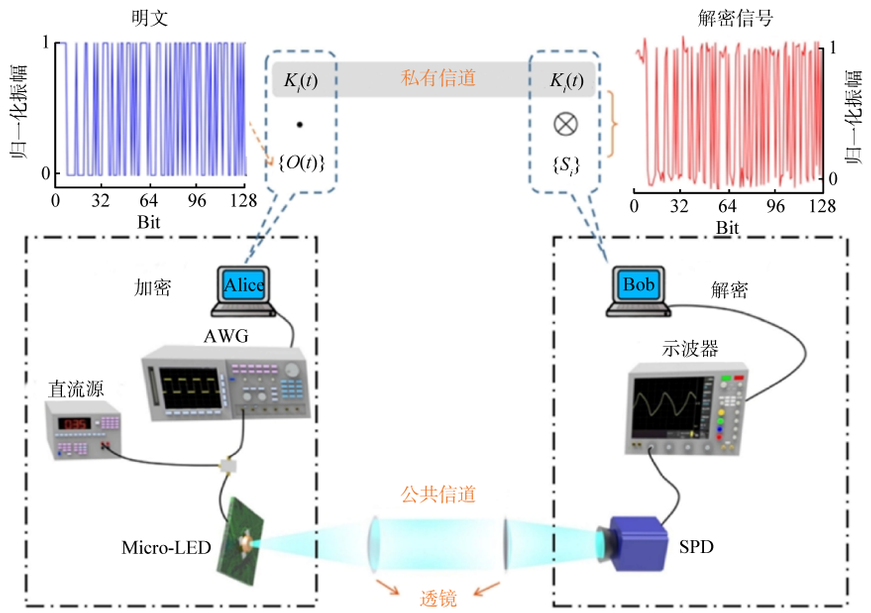
2017年,上海理工大学Pan和Zhang[21]采用CS技术在混沌激光TGI的基础上提高了重建信号的品质,并进一步将该技术应用于光学加密。基于混沌激光压缩TGI方案如图3所示,在加密过程中,Alice是信号的加密方,Bob是接收方,密钥($I_i(t)$)通过私有信道进行传输。Alice将密钥$I_i(t)$加载到明文$m(t)$上形成密文$y_n(t)$,密文$y_n(t)$通过公共信道进行传输。在解密过程中,Bob接收到密文$y_n(t)$后结合密钥$I_i(t)$采用CS作为解密算法来重构明文内容。

2020年,Wang等[22]基于计算TGI的光学加密工作如图4所示。计算TGI使用调制器代替原始TGI中的快速探测器来简化光路。在加密过程中,明文$O(t)$与计算机中的密钥$K_i(t)$通过式(1)得到加密后的密文$S_i(t)$,使用任意波形发生器驱动Micro-LED得到密文S_i。实验中Micro-LED的带宽为160 MHz,驱动速度为4 Gbps,这超出了其运行速度的极限,因此发出的信号变得随机且完全无法识别,可以



注:CS表示压缩感知。

图3　基于混沌激光压缩TGI方案[21]



注:AWG为任意波形发生器;Micro-LED为微型发光二极管;SPD为单像素探测器。

图4　基于微型发光二极管(Micro-LED)TGI的可见光通信加密方案[22]

利用传输失真提供额外的加密,本质是利用低通滤波代替积分过程获得密文。在公共信道无线传输0.8 m后,Micro-LED发出的携带密文的光信号由单像素探测器(single-pixel detector,SPD)接收,其带宽为100 MHz。在解密过程中,光信号通过SPD转换为电信号,并用示波器记录接收到的密文S_i',并通过式(2)进行解析,最终得到解析后的明文$O'(t)$。

利用遮挡攻击对该加密系统鲁棒性的测试结果如图5所示。在传输过程中,对密文分别进行20%、30%、40%和50%的遮挡,得到的部分解密后的明文$O'(t)$与明文$O(t)$的比较分别如图5(a~d)所示,随着遮挡密文的比例增加,解密后的明文$O'(t)$的C_{PC}和E_{RMS}如图5(e、f)所示。虽然解密后的明文$O'(t)$的品质随着遮挡率的增加而下降,但当遮挡率为40%且密文仅保留60%时,明文仍能较好重建。可见该实验算法和器件的双重加密为可见光通信提供了潜在的应用前景。

2022年,复旦大学Chen等[24]把Micro-LED用作探测器的可见光加密通信系统示意如图6所示。其加密和解密过程与2017年[21]、2020年[22]这2项工作类似。不同的是该实验使用的是405 nm紫色激光二极管,且该激光二极管发出的光信号经1.5 m的无线传输后,由基于Micro-LED的探测器接收并转换为电信号,最后使用数字信号示波器(digital signal oscilloscope,OSC)接收,通过式(2)进行解析。

为了展示该通信系统中解析后的明文$S'(t)$与

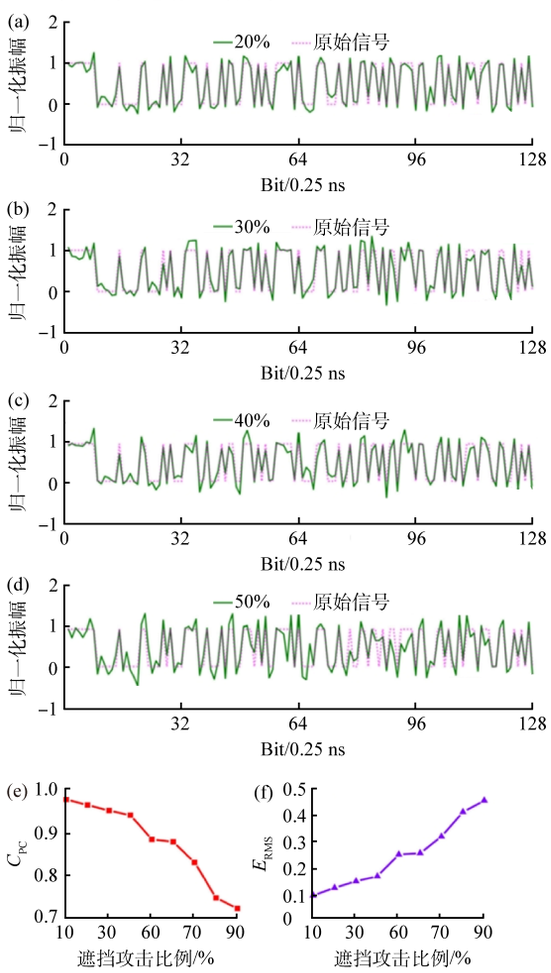
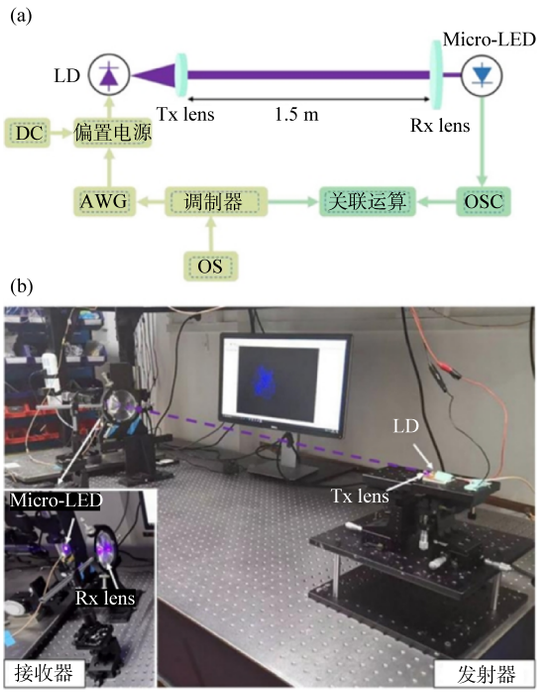


图5　加密系统抵抗遮挡攻击的测试结果[22]

(a~d)分别表示对密文进行20%、30%、40%和50%遮挡;(e)皮尔逊相关系数(C_{PC})计算结果;(f)均方根误差(E_{RMS})计算结果



注:LD 为半导体激光器;DC 为耦合直流电源;OS 为原始信号;OSC 为数字信号示波器;Tx/Rx lens 为激光透镜。

图 6　基于 Micro-LED 用作探测器的 TGI 可见光通信系统示意[24]
(a)实验原理;(b)实验装置

4 GHz 发射频率下直接传输明文之间的差异,将二者与明文 $S(t)$ 进行了比较(图 7)。由于明文 $S(t)$ 是由 0 和 1 组成的信号,因此对二者进行了归一化处理。由图 7 可知,与直接传输明文相比(光源带宽不足导致直接探测到的是密文),解析后的明文 $S'(t)$ 与原始明文 $S(t)$ 相似度更高。

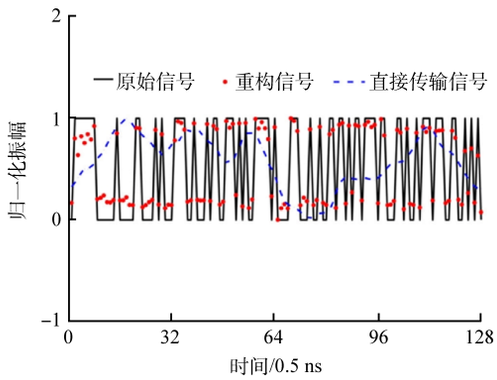
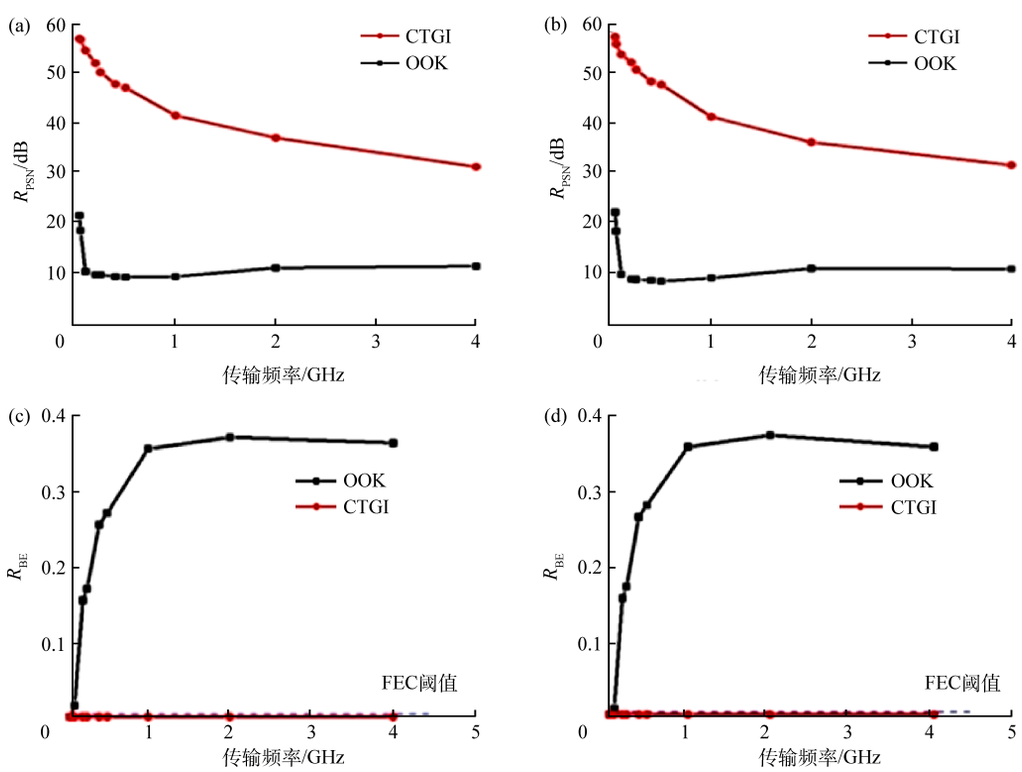


图 7　原始明文 $S(t)$、解析后的明文 $S'(t)$ 和 4 GHz 发射频率下直接传输明文的比较[24]

系统在 0 和 −5 V 偏置电压、不同发射频率下 TGI 和二进制振幅键控(on-off keying,OOK)的测试结果如图 8 所示。实验结果表明,在 1.5 m 的自由空间距离下,该方案可以在 4 GHz 发射频率下实现无



注:OOK 为二进制振幅键控;CTGI 为计算时域鬼成像;FEC 为前向纠错;R_{PSN} 为峰值信噪比;R_{BE} 为误比特率。

图 8　不同偏置电压下 TGI 和 OOK 发射频率的测试结果[24]
(a)0 时 R_{PSN};(b)−5 V 时 R_{PSN};(c)0 时 R_{BE};(d)−5 V 时 R_{BE}

误码传输,并且R_{PSN}远高于OOK。这证明TGI技术在一定程度上缓解了Micro-LED作为探测器的低带宽限制问题。同时,作为探测器,Micro-LED可以在0偏置电压下工作,具有自供电器件的潜力,可以有效节省能源。

2.1.2　基于TGI的水下对称加密方案

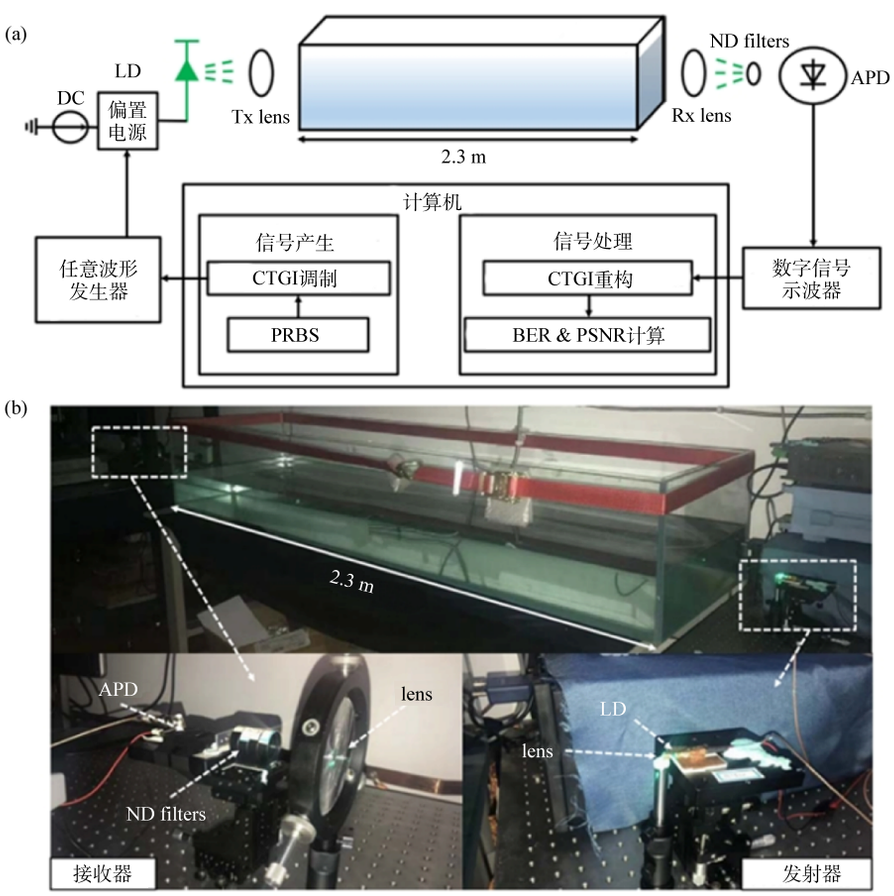
以上介绍了在大气环境无线传输情况下对称加密的几项相关工作。2021年,复旦大学Chen等[25]首次提出了基于计算TGI的水下无线光保密通信(underwater wireless optical communication,UWOC)系统(图9)。520 nm绿色激光二极管发出的光信号在水下无线传输了2.3 m后由雪崩光电二极管(avalanche photodiode,APD)接收。该方案拓展了GI加密系统的应用,为水下无线通信的进一步发展提供了重要参考。

2.1.3　基于TGI的一对多对称加密方案

上述加密方案都属于一对一传输方案。这不仅限制了传输信息的容量,而且降低了传输效率。2019年,上海理工大学Kang等[26]提出了一种基于TGI和码分多址(code division multiple access,CDMA)技术的一对多信息加密传输方案。该方案利用CDMA中的码片序列和TGI中的随机时间模式作为密钥来实现双重加密,实现了同一信道上同时一对多的信息加密传输。

如图10所示,在加密过程中,利用CDMA技术结合了多组明文,每组明文D_n对应的码片序列l_n作为第一密钥K_1。发送方将传输信息M加载到一系列TGI的时间随机模式l_n上并通过光纤将其传输到接收器。其中,这一系列时间随机模式I_n作为第二密钥K_2。这里的第二密钥K_2与一般TGI加密方案中的密钥地位相同。在解密过程中,每个接收器都可以获得相同的密文B_n,并使用第二密钥K_2来获取相应的传输信息M'(也称为重构信息)。最后,每个接收器使用第一密钥K_1得到解析后的明文D'_n(即重构明文)。

基于TGI和CDMA的一对多光信息加密传输



注:ND filters为中性密度滤光片;APD为雪崩光电二极管;PRBS为伪随机二进制序列;BER为误比特率;PSNR为峰值信噪比。

图9　基于计算TGI的水下无线光通信系统[25]

(a)加密解密示意;(b)实验装置

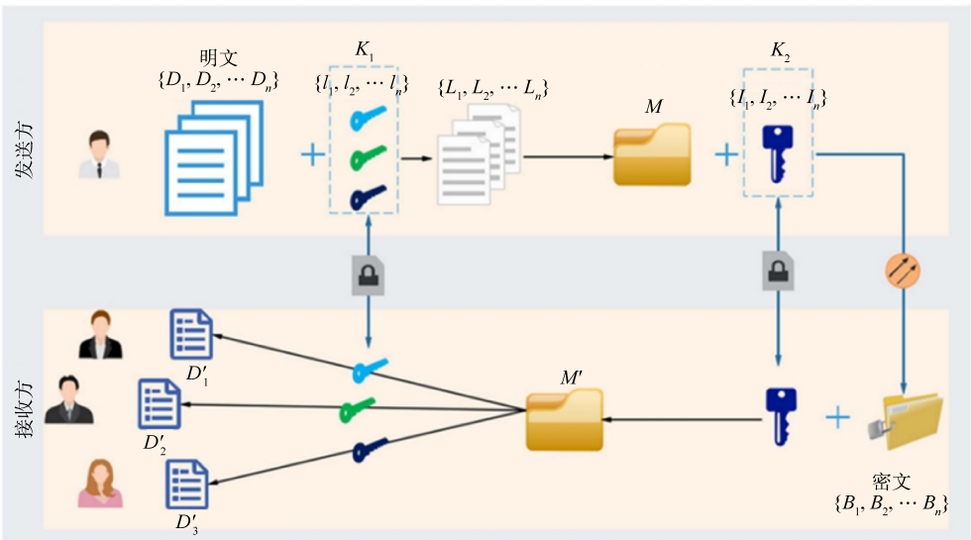
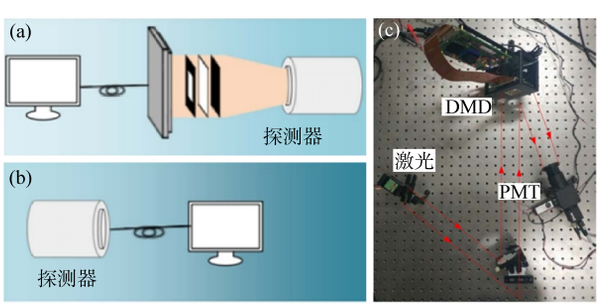


图10　基于TGI和码分多址(CDMA)的一对多光信息加密传输方案[26]

方案的光学实验装置如图11所示。首先,在计算机中完成2次加密过程,并将加密后的密文B_n加载到数字微镜器件(digtial micromirror devices, DMD)上。DMD作为光源传输密文B_n,其传输的密文B_n由光电倍增管(photo multiplier tube, PMT)接收并传输到计算机的采集卡上,最后由计算机进行解密得到重构明文D'_n。



注:DMD为数字微镜器件;PMT为光电倍增管。

图11　基于TGI和CDMA的一对多光信息加密传输实验示意[26]
(a)加密过程;(b)解密过程;(c)光学实验装置

在该实验中,2组不同的信息组成了传输信息M,实验数据如图12所示。图12(a)展示了使用正确的第二密钥K_2进行解密时,对应的传输信息M'。尽管此时的重构信息M'与原始信息(即密文B_n)之间存在一些误差,但大多数信息是一致的。然后利用正确的第一密钥K_1对重构信息M'进行解密,并判断阈值。如图12(b)所示,解析后的明文D'_n与原始明文D_n是相同的,这说明使用该方案即使传输信息M'出现错误也能正确获得明文D'_n,系统具有很强的鲁棒性。如图12(c)所示,当使用错误的第二密钥K_2进行解密时,得到的传输信息M'与原始信息B_n有很大差异。图12(d)展示了即使此时使用正确的第一密钥K_1进行解密,解析后的明文D'_n也是错误的,这说明该系统具有很强的安全性。

2.2　非对称加密

2.2.1　非对称加密的一般方法

加密方法可以分为对称加密和非对称加密2类。上文提到的几个工作都属于对称加密方法,其特点是加密和解密时密钥是相同的,信息的发送方和接收方共享同一个密钥。然而,对称加密存在密钥分发安全性难以保障的问题,容易因密钥泄露导致信息无法安全传输。

1976年,美国斯坦福大学Diffie和Hellman[27]为了解决信息公开传送和密钥管理问题,提出了非对称加密算法。与对称加密不同,非对称加密需要2组不同密钥,分别为公钥和私钥,并由信息的接收方生成。公钥通过私有信道从信息的接收方传输到信息的发送方,参与信息的加密过程。而私钥不被传输,泄露的风险低,参与信息的解密过程。即使公钥发生泄露,也难以从密文中解析出正确的明文信息,所以与对称加密相比,非对称加密系统的安全性较高。

1977年,美国麻省理工学院Rivest等[28]首次提出Rivest-Shamir-Adleman(RSA)算法,该算法由作者3人姓氏首字母命名,并于1978年正式发表。RSA算法是非对称加密领域中最有代表性的工作之一。相较于使用共同密钥的对称加密系统,基于RSA算

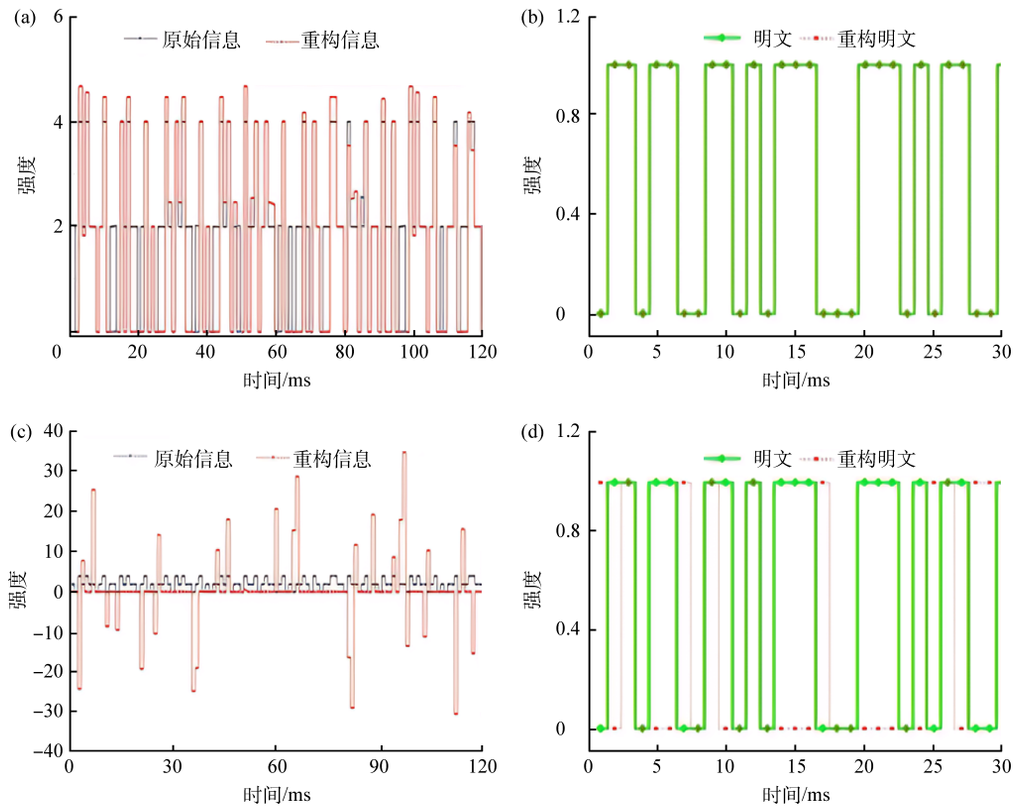


图12　基于TGI和CDMA的一对多光信息加密传输实验结果[26]

(a)使用第二密钥K_2实验组重构信息M';(b)使用第一密钥K_1实验组重构明文D'_n;
(c)使用错误的第二密钥K_2对照组重构信息M';(d)使用第一密钥K_1对照组重构明文D'_n

法的非对称加密系统,因其更高的安全性而受到了学者的广泛关注和研究[29-30],并针对如何解决RSA算法计算复杂度高、加密速度慢,以及如何进一步提高加密效率和加密系统安全性等问题,提出了一系列的解决方案[31-32]。

基于RSA算法的非对称加密流程如图13所示。以RSA算法为例,非对称加密的具体流程为[23]:(1)Bob使用RSA算法生成1对密钥(K_{pub},K_{prv})。私钥K_{prv}由Bob保存,公钥K_{pub}发送给Alice;(2)Alice使用K_{pub}加密明文X,得到密文Y;(3)Bob使用K_{prv}解密从Alice收到的密文Y,得到明文X。

2.2.2　基于TGI非对称加密的相关工作

2021年,上海理工大学Kang等[23]提出了一种压缩感知TGI的光学混合加密方案。如图14所示,在加密过程中,首先Bob使用RSA公钥算法生成1对密钥(K_{pub},K_{prv}),将公钥K_{pub}通过私有信道传输给Alice。Alice使用伪随机数生成器生成混沌参数P并生成混沌激光$I(t)$。混沌激光通过时间物体$T(t)$(相当于明文)后被桶探测器记录,经过多次采样得到密文C_1。Alice使用公钥K_{pub}对混沌参数P进行加密,得到密文C_2。最后将密文C_1和密文C_2组合起来,得到完整的密文。

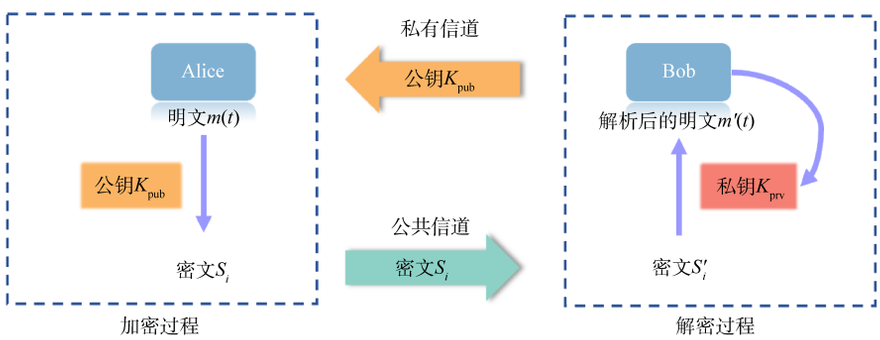
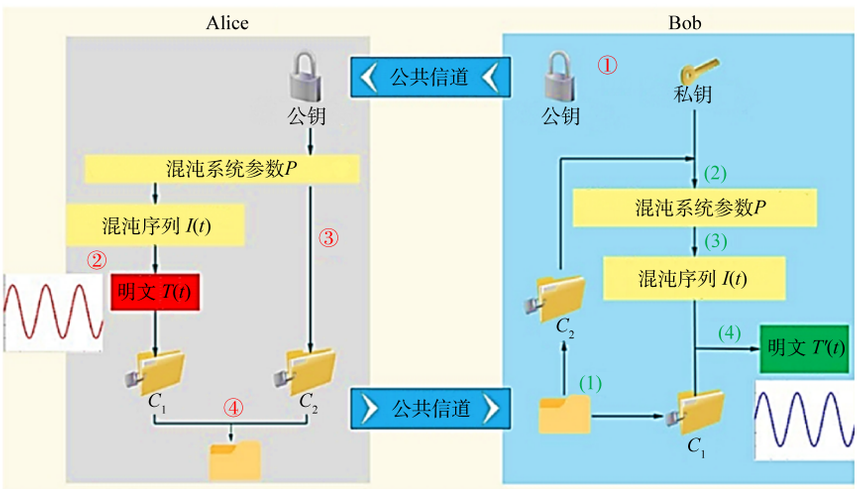


图13　基于RSA算法的非对称加密流程[23]

在解密过程中,首先Bob将收到Alice的密文分解为密文C_1和密文C_2;Bob利用私钥K_{prv}解密C_2,得到混沌参数P;再利用解密得到的混沌参数P生成混沌激光$I(t)$并将其记录下来;最后对密文C_1和依次存储的混沌序列$I(t)$进行关联计算,得到的结果就是解密后的明文$T'(t)$。可以看出,此方案的核心是使用对称加密方法加密明文,使用非对称加密方法加密混沌参数,从而实现密钥的安全分发。该方案一定程度解决了基于GI原理的加密系统的密钥安全分发问题,降低了建立安全通道的额外成本。该方案可应用于加密和数据存储,具有高安全性、高鲁棒性和低成本的优点,为高效的信息传输带来便利和安全。

选择明文攻击和已知明文攻击的结果如图15所示。从仿真的结果可知使用传统的TGI加密方案,无论是选择明文攻击还是已知明文攻击都可以在一定程度上破解密文。但是压缩感知TGI加密方案则不易被破解,一定程度上可以抵抗选择明文攻击和已知明文攻击,系统的安全性较高。



注:C为密文。

图14　基于TGI的光学混合加密方案[23]

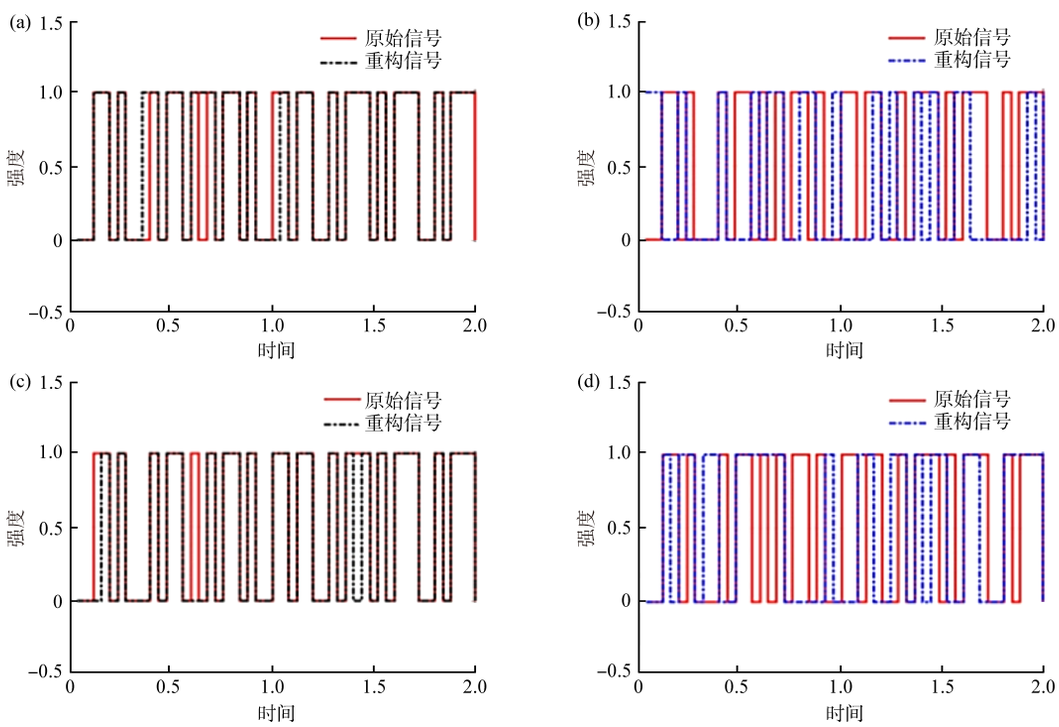
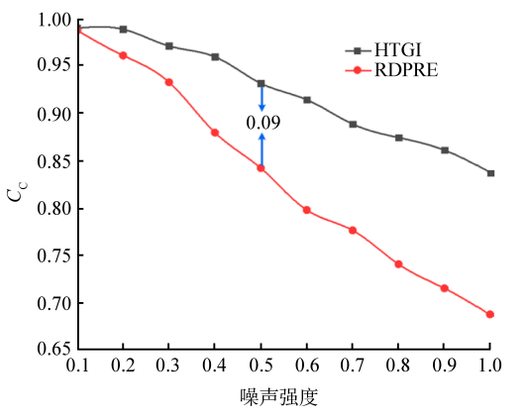


图15　选择明文攻击和已知明文攻击的结果[23]

(a)TGI方案被选择明文攻击的结果;(b)压缩感知TGI方案被选择明文攻击的结果;(c)TGI方案被已知明文攻击的结果;(d)压缩感知TGI方案被已知明文攻击的结果

将该方案与基于RSA算法的双随机相位编码加密方案进行比较。由图16可知,随着噪声强度的增加,2种方案的C_C曲线都呈下降趋势。但在相同强度下,该方案优于双随机相位编码的加密方案。当噪声强度为0.5时,该方案的性能提高10%。而且,随着噪声强度的增加,该方案的优越性将越来越明显。当噪声强度为1时,该方案解密后的信息与原始信息仍然具有很强的相关性,说明系统的鲁棒性高。



注:C_C为相关系数;RDPRE为双随机相位编码。

图16 噪声强度和相关系数[23]

3 总结与展望

基于TGI的光学加密系统可以使用远低于信号带宽的探测器来接收加密信息,弥补了因光源或探测系统带宽不足导致的数据传输速率受限等问题,为未来高速无线光通信系统提供安全保障。本文综述了基于TGI加密系统的基本原理、实验装置和发展历史。主要介绍了基于TGI技术的光学对称加密系统和非对称加密系统。其中,对称加密系统能够恢复出高品质的信号,能有效抵抗噪声攻击,且系统装置简单、成本低、速度快。相较于对称加密系统,非对称加密系统的优势是能够解决密钥安全分发问题,降低建立安全通道的成本,为高效的信息传输带来安全性和便利性,并且可以实现高品质、高安全性、高鲁棒性加密。

尽管基于TGI的光学加密系统已取得了一系列进展,目前仍处于初步探索和发展阶段,面临着诸多亟需克服的问题与挑战。这一现状也凸显了其蕴含的巨大研究价值。我们有理由相信,随着硬件设备的不断升级和加密算法的持续优化,必将促进TGI保密通信技术在安全和高速通信相关领域的发展和应用。

参 考 文 献

[1] PITTMAN T B, SHIH Y H, STREKALOV D V, et al. Optical imaging by means of two-photon quantum entanglement[J]. Physical Review A, 1995, 52(5): R3429-R3432.

[2] BENNINK R S, BENTLEY S J, BOYD R W. "Two-photon" coincidence imaging with a classical source[J]. Physical Review Letters, 2002, 89(11): 113601.

[3] SHAPIRO J H. Computational ghost imaging[J]. Physical Review A, 2008, 78(6): 061802.

[4] YANG Z, BAI Y M, HUANG K X, et al. Single-pixel full-field simultaneous spatial and velocity imaging[J]. Optics and Lasers in Engineering, 2023, 169: 107691.

[5] YANG Z, HUANG K X, ZHANG M C, et al. Derivative ghost imaging[J]. Chinese Optics Letters, 2022, 20(1): 011101.

[6] REFREGIER P, JAVIDI B. Optical image encryption using input plane and Fourier plane random encoding[J]. International Society for Optics and Photonics, 1995, 2565: 62-68.

[7] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics Letters, 2000, 25(12): 887-889.

[8] SITU G H, ZHANG J J. Double random-phase encoding in the Fresnel domain[J]. Optics Letters, 2004, 29(14): 1584-1586.

[9] POON T C, KIM T, DOH K. Optical scanning cryptography for secure wireless transmission[J]. Applied Optics, 2003, 42(32): 6496-6503.

[10] CLEMENTE P, DURÁN V, TAJAHUERCE E, et al. Optical encryption based on computational ghost imaging[J]. Optics Letters, 2010, 35(14): 2391-2393.

[11] KONG L J, LI Y, QIAN S X, et al. Encryption of ghost imaging[J]. Physical Review A, 2013, 88(1): 013852.

[12] CHEN W, CHEN X D. Marked ghost imaging[J]. Applied Physics Letters, 2014, 104(25): 251109.

[13] WU J J, XIE Z W, LIU Z J, et al. Multiple-image encryption based on computational ghost imaging[J]. Optics Communications, 2016, 359: 38-43.

[14] RYCZKOWSKI P, BARBIER M, FRIBERG A T, et al. Ghost imaging in the time domain[J]. Nature Photonics, 2016, 10(3): 167-170.

[15] RYCZKOWSKI P, BARBIER M, FRIBERG A T, et al. Magnified time-domain ghost imaging[J]. APL Photonics, 2017, 2(4): 046102.

(下转第46页)

[22] DUQUE C A, MORALES A, PORRASMONTENEGRO N, et al. Effects of applied electric fields on the infrared transitions between hydrogenic states in GaAs low-dimensional systems[J]. Physical Review B, 1997, 55(16): 10721-10728.

[23] CAMPOS T, FARIA-JUNIOR P E, GMITRA M, et al. Spin-orbit coupling effects in zinc-blende InSb and wurtzite InAs nanowires: realistic calculations with multiband $k\cdot p$ method[J]. Physical Review B, 2018, 97(24): 245402.

[24] VURGAFTMAN I, MEYER J A, RAM-MOHAN L R. Band parameters for III-V compound semiconductors and their alloys[J]. Journal of Applied Physics, 2001, 89(11): 5815-5875.

[25] TEDESCHI D, DE-LUCA M, GRANADOS-DEL-AGUILA A, et al. Value and anisotropy of the electron and hole mass in pure wurtzite InP nanowires[J]. Nano Letters, 2016, 16(10): 6213-6221.

[26] ZHANG J, SHI L, YAN Z W. Conversion efficiency of strained wurtzite $In_xGa_{1-x}N/ZnSnN_2$ core/shell quantum dot solar cells under external electric field [J]. Optoelectronics Letters, 2023, 19(3): 144-150.

[27] SHI L, YAN Z W. Conversion efficiency of strained core/shell quantum dot solar cell: converting from type-I to type-II structures [J]. Journal of Applied Physics, 2019, 125(17): 174302.

[28] SAHIN M. Effect of the shell material and confinement type on the conversion efficiency of core/shell quantum dot nanocrystal solar cells [J]. Journal of Physics (Condensed Matter), 2018, 30(20): 205301.

(责任编辑:兰丽丽)

(上接第38页)

[16] DEVAUX F, MOREAU P A, DENIS S, et al. Computational temporal ghost imaging [J]. Optica, 2016, 3(7): 698-701.

[17] JIANG W J, LI X Y, JIANG S, et al. Increase the frame rate of a camera via temporal ghost imaging[J]. Optics and Lasers in Engineering, 2019, 122: 164-169.

[18] TIAN Y, GE H, ZHANG X J, et al. Acoustic ghost imaging in the time domain [J]. Physical Review Applied, 2020, 13(6): 064044.

[19] XU Y K, SUN S H, LIU W T, et al. Detecting fast signals beyond bandwidth of detectors based on computational temporal ghost imaging [J]. Optics Express, 2018, 26(1): 99-107.

[20] 孙宝清,王玉鹏.时域鬼成像及其应用[J].中国激光, 2021, 48(12): 343-360.

[21] PAN Z L, ZHANG L H. Optical cryptography-based temporal ghost imaging with chaotic laser [J]. IEEE Photonics Technology Letters, 2017, 29(16): 1289-1292.

[22] WANG Y P, CHEN H L, JIANG W J, et al. Optical encryption for visible light communication based on temporal ghost imaging with a Micro-LED [J]. Optics and Lasers in Engineering, 2020, 134: 106290.

[23] KANG Y, ZHANG L H, YE H L, et al. Hybrid encryption scheme based on temporal ghost imaging[J]. Applied Physics B, 2021, 127(8): 124.

[24] CHEN X W, JIN M Y, LIN R Z, et al. Visible light communication based on computational temporal ghost imaging and Micro-LED-based detector[J]. Optics and Lasers in Engineering, 2022, 152: 106956.

[25] CHEN X W, JIN M Y, CHEN H L, et al. Computational temporal ghost imaging for long-distance underwater wireless optical communication [J]. Optics Letters, 2021, 46(8): 1938-1941.

[26] KANG Y, ZHANG L H, YE H L, et al. One-to-many optical information encryption transmission method based on temporal ghost imaging and code division multiple access[J]. Photonics Research, 2019, 7(12): 1370-1380.

[27] DIFFIE W, HELLMAN M E. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[28] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.

[29] ZHANG C N. Integrated approach for fault tolerance and digital signature in RSA [J]. IEE Proceedings-Computers and Digital Techniques, 1999, 146(3): 151-159.

[30] HUANG Y L, LEU F Y, YOU I, et al. A secure wireless communication system integrating RSA, Diffie-Hellman PKDS, intelligent protection-key chains and a data connection core in a 4G environment[J]. The Journal of Supercomputing, 2014, 67: 635-652.

[31] VANSTONE S A, ZUCCHERATO R J. Short RSA keys and their generation[J]. Journal of Cryptology, 1995, 8: 101-114.

[32] BHASKAR R, HEGDE G, VAYA P R. An efficient hardware model for RSA encryption system using Vedic mathematics[J]. Procedia Engineering, 2012, 30: 124-128.

(责任编辑:兰丽丽)