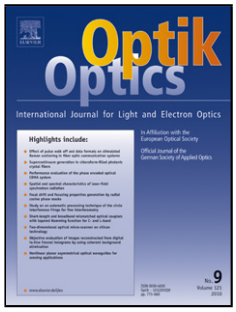

Title: Demonstration and a practical scheme of the optical asymmetric cryptosystem

Authors: Tieyu Zhao, Yushan Jiang, Chao Liu

PII: S0030-4026(17)30272-3
DOI: http://dx.doi.org/doi:10.1016/j.ijleo.2017.03.013
Reference: IJLEO 58936

To appear in:

Received date: 4-6-2014
Revised date: 28-10-2016
Accepted date: 4-3-2017

Please cite this article as: Tieyu Zhao, Yushan Jiang, Chao Liu, Demonstration and a practical scheme of the optical asymmetric cryptosystem, Optik - International Journal for Light and Electron Optics http://dx.doi.org/10.1016/j.ijleo.2017.03.013

Demonstration and a practical scheme of the optical asymmetric cryptosystem

Tieyu Zhao,[1]* Yushan Jiang,[1] Chao Liu[1]

[1]*Information Science Teaching and Research Section，Northeastern University at Qinhuangdao, Qinhuangdao, 064000, China.*

**Corresponding author: zty03y3213@163.com*

Abstract

In recent years, researchers have been focused on the optical asymmetric cryptosystem (OACS). The encryption key and decryption key are independent, the fact of which overcomes the linearity defect of optical encryption system. So the OACS has attracted more and more researchers' attention. We have deeply studied the existing OACS, and found that the cryptosystem is unable to realize communication in practice. In this paper, we demonstrate the shortcomings of the present OACS and propose a practical scheme. The analysis shows that this scheme meets the communication protocol of asymmetric cryptography (ACS).

Keywords: Image encryption; asymmetric cryptosystem; optical asymmetric cryptosystem.

1. Introduction

Since Diffie and Hellman first proposed the idea of public key cryptography in 1976 [1], various public key algorithm (PKA) have been proposed. However most algorithms were proved to be unsafe or difficult realize due to their complexity. The RSA algorithm is one of the most mature PKA [2] at present. Until 2010, only short key of RSA can be cracked by brute force attack [3]. As long as RSA key was long enough, RSA encryption algorithm is quite safe in practical application. However, in the latest research report of Lenstra with his colleagues, they indicated that the RSA-PKA was flawed [4]. They collected the public key from the network and found that two thousandths of RSA algorithm was unsafe. So far, the questionable public key has been deleted from the public access database. In optical information security, Peng et al proposed an asymmetric cryptography based on wavefront sensing (ACWS) in 2006 [5], in which the public key may be derived from optical parameters (such as