Short Communications

A secret key distribution technique based on semiconductor superlattice chaos devices

Wei Liu, Zhizhen Yin, Xiaoming Chen, Zhenyun Peng, Helun Song, Peihua Liu, Xinhai Tong, Yaohui Zhang

PII: S2095-9273(18)30302-5
DOI: https://doi.org/10.1016/j.scib.2018.06.017
Reference: SCIB 446

To appear in: *Science Bulletin*

Received Date: 24 May 2018
Revised Date: 13 June 2018
Accepted Date: 20 June 2018

Please cite this article as: W. Liu, Z. Yin, X. Chen, Z. Peng, H. Song, P. Liu, X. Tong, Y. Zhang, A secret key distribution technique based on semiconductor superlattice chaos devices, *Science Bulletin* (2018), doi: https://doi.org/10.1016/j.scib.2018.06.017

A secret key distribution technique based on semiconductor superlattice chaos devices

Wei Liu [1], Zhizhen Yin[1], Xiaoming Chen[2], Zhenyun Peng[1], Helun Song[1], Peihua Liu[1], Xinhai Tong[2], Yaohui Zhang[1*]

[1] *Key Lab of Nanodevices and Applications，Suzhou Institute of Nano-Tech and Nano-Bionics, Chinese Academy of Sciences (CAS), Suzhou 215123, China*

[2] *Beijing Electronic Science and Technology Institute, Beijing 100070, China*

Received: 24-May-2018; Revised: 2018/6/13; Accepted: 20-Jun-2018

* Corresponding author (email: yhzhang2006@sinano.ac.cn)

Key distribution is one of the most important and often also the most difficult parts in cryptography [1]. In symmetric key cryptography, both of the sender and the recipient must share the same secure key for successful communication. Traditionally key distribution is achieved by establishing a separate “secure channel”. The “secure channel” can be a specially-built communication link, or a trusted courier etc., all of which are of high cost and low efficiency. In recent years Public-Key cryptography has been used for key distribution [2], but the high computational cost makes public-key based approaches only available for distributing small amounts of digits. Quantum key distribution which has excellent security properties has also been successfully demonstrated [3, 4, 5], but the key distribution rate is limited and special channels are required.

On the other hand, the one-time pad (OTP) cipher [6] is the only one that has been theoretically proven to be uncrackable [7], providing that the secret keys are truly unpredictable. The absolute security of the one-time pad cipher comes from the fact that every information bit is encrypted with a corresponding key bit. This feature implies that the key size must be larger than the message size. As a result, the one-time pad cipher is seldom used due to the fact that the key distribution cost is too high.

Chaos phenomena are considered useful in cryptography [8] and very recently, chaos in semiconductor superlattices was found to be good entropy sources which were used to generate true random numbers at very high speeds [9]. In 2015, the chaos synchronization in matched semiconductor superlattices was reported [10] and the idea of using matched semiconductor superlattice devices to distribute secure keys was suggested [11]. In 2017, a key distribution scheme based on chaos synchronization was reported [12]. The above works strongly indicate that semiconductor superlattices may be promising for high throughput key distribution. In this paper, we proposed and demonstrated experimentally a new key distribution technique based on chaos synchronization in semiconductor superlattices driven by a synchronizing electrical signal. As each of the sender and the recipient owned a superlattice device that can be synchronized, the same digital key was generated locally for the sender and the recipient respectively, and the sym-