Optics Communications 419 (2018) 83–89

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Strong light illumination on gain-switched semiconductor lasers helps the eavesdropper in practical quantum key distribution systems

Yang-yang Fei [a,*], Xiang-dong Meng [a], Ming Gao [a], Yi Yang [a], Hong Wang [a], Zhi Ma [a,b]

[a] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, 450001, China

[b] CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, 230026, China

ARTICLE INFO

Keywords:
Quantum key distribution
Gain-switched semiconductor laser
Rate equation
Strong light illumination

ABSTRACT

The temperature of the semiconductor diode increases under strong light illumination whether thermoelectric cooler is installed or not, which changes the output wavelength of the laser (Lee et al., 2017). However, other characteristics also vary as temperature increases. These variations may help the eavesdropper in practical quantum key distribution systems. We study the effects of temperature increase on gain-switched semiconductor lasers by simulating temperature dependent rate equations. The results show that temperature increase may cause large intensity fluctuation, decrease the output intensity and lead the signal state and decoy state distinguishable. We also propose a modified photon number splitting attack by exploiting the effects of temperature increase. Countermeasures are also proposed.

1. Introduction

Quantum key distribution (QKD) can provide unconditional security to distribute key between two remote parts with perfect devices [1–3]. However, practical devices always deviate from the models in security proofs. These deviations reduce the secure key and many attacks on imperfect devices have been proposed to steal information about the final key [4–21]. Thus, study on the imperfections of practical devices is extremely important to the security of QKD systems.

The sources of practical QKD systems also suffer from some imperfections. Attenuated laser pulses are always used as the "single photon source" in practical QKD systems due to technique limitation. However, the attenuated pulses may contain more than one photons, which can be attacked by photon number splitting (PNS) attack [4]. To against PNS attack on weak coherent source, decoy state method is proposed [22–24]. In the "weak + vacuum" decoy state method [25], a sender (Alice) needs to transmit pluses of three intensities (signal state, decoy state and vacuum state) to a receiver (Bob). Usually, the intensity of signal state is higher than that of the decoy state.

Gain-switched semiconductor laser is widely used in practical QKD systems as the transmitter, because it simplifies the construction of the source and sends phase randomized pulses [26]. The phase randomness of the pulses is assumed in most security proofs. A gain-switched semiconductor laser is driven from the initial carrier density, which is below the threshold, by a strong AC injection current pulse with the level of J_{AC} for each photon pulse generation in QKD systems. The initial carrier density is determined by a DC bias current, J_{DC}. Short pulses are generated by injection of short current pulses into a semiconductor laser. The shape of the output photon pulses are directly defined by J_{AC} and J_{DC}. Actually, the carrier density and photon density vary fast and acutely in the gain-switched operation. A rate equation description is used to efficiently and accurately simulate the performance of gain-switched semiconductor lasers with proper choice of model parameters. The output performance of a semiconductor laser is sensitive to temperature variation [27]. So most semiconductor lasers work with thermoelectric coolers to keep the temperature of semiconductor diode stable.

In Ref. [28], Lee et al. experimentally show that the temperatures of semiconductor diodes can be increased by strong light illumination, even when the lasers are installed with thermoelectric coolers. Due to the limit power of the thermoelectric cooler, the temperature of the diode increases as long as the illumination is strong enough. Temperature increase leads to output wavelength variation which makes pulses from different lasers distinguishable [28]. However, the wavelength variation do not impact the security of QKD systems with only one laser, such as phase encoding systems. Besides, other characteristics of the semiconductor lasers also change with temperature [27,29]. The variations of other characteristics also deviate the behavior of

* Corresponding author.
E-mail address: fei_yy@foxmail.com (Y.-y. Fei).

https://doi.org/10.1016/j.optcom.2018.03.029
Received 19 January 2018; Received in revised form 6 March 2018; Accepted 12 March 2018

semiconductor lasers from ideal models in security proofs. And the eavesdropper may exploit these variations to steal information about the final key. So it is urgently needed to study the effects of temperature increase on important characteristics of gain-switched semiconductor lasers.

In the following, we mainly focus on the effects of temperature increase on gain-switched semiconductor diodes in QKD systems. This article is constructed as follows: we briefly introduce the temperature dependent single mode rate equation of semiconductor lasers and the model parameters for a gain-switched semiconductor laser used in this paper in Section 2. Then numerical simulation of the efficient and accurate single mode temperature dependent rate equation is performed in Section 3. The effects of temperature increase on three characteristics are studied in detail, which include the recovery time of carrier density, the intensity of output pulses and the time interval between signal state and decoy state pulses. In Section 4, we propose a modified PNS attack strategy which exploits the effects of temperature increase. We also give out the hacking strategy using side channels in time dimension. Finally, we conclude the paper and discuss countermeasures in Section 5.

2. Temperature dependent single mode rate equation of semiconductor laser

Temperature variations effect the output characteristics of semiconductor lasers significantly. Recent research shows the eavesdropper can elevate the working temperature of a semiconductor laser diode by strong light illumination even when thermoelectric cooler is installed. So the effects of temperature increase on the output performance of semiconductor lasers should be taken into consideration in practical QKD systems.

The dynamics of semiconductor laser at different temperatures can be described efficiently and accurately with the following single mode rate equations covering temperature [29–31]

$$\frac{dN(t)}{dt} = \frac{J(t)}{qd} - \frac{N(t)}{\tau_n(T)} - g_0(T)[N(t) - N_0(T)]S(t), \tag{1}$$

$$\frac{dS(t)}{dt} = \Gamma g_0(T)[N(t) - N_0(T)]S(t) - \frac{S(t)}{\tau_p} + \frac{\Gamma\beta N(t)}{\tau_n(T)}, \tag{2}$$

where t represents time, T is temperature, q is electrical charge, $N(t)$ is the time-variation carrier density and $S(t)$ represents the time-variation photon density. $J(t)$ is the overall injection current and $J(t) = J_{AC}(t) + J_{DC}$. Others are material parameters of semiconductor lasers, which are explained in detail in Table 1. Note that $N_0(T)$, $\tau_n(T)$ and $g_0(T)$ are three main temperature related parameters and others can be treated as constants, which are temperature independent.

Experiment observations give the following relationship between the threshold current density and the temperature $J_{th}(T) = J_c exp(T/T_0)$ [32], where T_0 is the characteristic temperature of the diode and J_c is the current density constant. Therefore we have

$$J_{th}(T + \Delta T) = J_c exp(\frac{T + \Delta T}{T_0}) = J_{th}(T) exp(\frac{\Delta T}{T_0}). \tag{3}$$

By solving Eqs. (1) and (2), the threshold current density of the diode can also be approximately given out by

$$J_{th}(T) \approx \frac{qd}{\tau_n(T)} N_{th}(T) = \frac{qd}{\tau_n(T)}[-\frac{1}{g_0(T)\Gamma\tau_p} + N_0(T)], \tag{4}$$

where $N_{th}(T)$ is the threshold value of carrier density. Here we use the same models as the ones in Ref. [29] to describe $g_0(T)$ and $N_0(T)$, as shown in Eqs. (5) and (6). The models fit the experiment results very well.

$$g_0(T) = g_{0c} exp(\frac{-T}{T_{0a}}), \tag{5}$$

$$N_0(T) = N_{0c} exp(\frac{T}{T_{0a}}), \tag{6}$$

where g_{0c} is the differential gain coefficient constant, N_{0c} is the transparent carrier density constant and T_{0a} is the characteristic temperature of the active region. So we have $g_0(T + \Delta T) = g_0(T) exp(-\Delta T/T_{0a})$, $N_0(T + \Delta T) = N_0(T) exp(\Delta T/T_{0a})$ and

$$\begin{aligned} J_{th}(T + \Delta T) &\approx \frac{qd}{\tau_n(T + \Delta T)}[\frac{1}{g_0(T + \Delta T)\Gamma\tau_p} + N_0(T + \Delta T)] \\ &= \frac{\tau_n(T)}{\tau_n(T + \Delta T)} J_{th}(T) exp(\frac{\Delta T}{T_{0a}}). \end{aligned} \tag{7}$$

By combining Eqs. (3) and (7), we can get

$$\tau_n(T + \Delta T) = \tau_n(T)\frac{exp(\frac{\Delta T}{T_{0a}})}{exp(\frac{\Delta T}{T_0})}. \tag{8}$$

Until now, all the three temperature dependent parameters can be calculated at different temperatures. And we can perform numeral simulation of the rate equations (Eqs. (1) and (2)) at different temperatures.

3. The effects of temperature increase on several characteristics of semiconductor lasers in decoy state QKD systems

As we stated before, Eve can increase the temperature of the semiconductor lasers by strong light illumination [28]. And the temperature increase will impact the output performance of semiconductor lasers. In QKD systems, any deviations from ideal models in security proofs will reduce the amount of final key. Thus, it is very important to study the effects of temperature increase on several characteristics of semiconductor lasers. Here by performing numerical simulation with the temperature dependent single mode rate equations (Eqs. (1) and (2)), we mainly study the effects of temperature increase on three characteristics which include the recovery time of the carrier density, the intensity of output pulses and the time interval between signal state and decoy state pulses.

3.1. Recovery time of carriers density

First, we briefly describe the variety of carrier density via time in the gain-switched mode. In the beginning, the carrier density $N(t)$ increases when large current is injected. Then when $N(t)$ reaches the temperature dependent transparent carrier density $N_0(T)$, the stimulated radiation process starts. Output laser is generated when $N(t)$ reaches the temperature dependent threshold carrier density $N_{th}(T)$. Then $N(t)$ falls quickly because of the disappearance of injected current and large amount consumptions of stimulated radiation. When $N(t)$ falls under $N_0(T)$, Eq. (1) can be simplified to $dN(t)/dt = N(t)/\tau_n(T)$, which means $N(t)$ follows the exponential decay after that.

Normally, $N(t)$ should return to temperature dependent initial carrier density $N_{DC}(T)$ before the next injection current comes. Otherwise, the initial carrier density of the next pulse is higher than that of the first one, which results a stronger photon pulse. The time needed for $N(t)$ to decay from $N_0(T)$ to $N_{DC}(T)$ is $t_{ed} = \tau_n(T) ln(N_0(T)/N_{DC}(T))$. Note that $N_{DC}(T) = J_{DC}\tau_n(T)/(qd)$ [33] and $N_{DC}(T)$ decreases as the temperature increases. We call the time needed for $N(t)$ to return back to $N_{DC}(T)$ the *recovery time*, denoted as t_{re}. The maximal repetition rate of the output photon pulses is $1/t_{re}$ in practical QKD systems. t_{ed} contributes most of t_{re}. The temperature increase leads to the elevation of $N_0(T)$ and the decrease of $N_{DC}(T)$, which prolongs t_{ed} as well as t_{re}. To reduce the recovery time of carrier density, J_{DC} should be set close to $J_{th}(T)$ [31,34]. However, the spontaneous emission under high J_{DC} causes high dark counts, which definitely increases the quantum bit error rate and decreases the secure key rate [34]. So the value of J_{DC} should be carefully considered in practical QKD systems. Here we set $J_{DC} = 4.8 \times 10^2$ A cm^{-2} as shown in Table 1. The corresponding $N_{DC}(25\,°C) = 0.3N_{th}(25\,°C)$.

To simulate the variation of $N(t)$, we excite the semiconductor diode with a single current pulse. The initial carrier density is set to $N_{DC}(T)$ for different temperatures. The single injection current pulse is rectangular