


## Article

# Quantum Hacking on an Integrated Continuous-Variable Quantum Key Distribution System via Power Analysis

Yi Zheng <sup>\*</sup> , Haobin Shi, Wei Pan, Quantao Wang and Jiahui Mao

School of Computer Science, Northwestern Polytechnical University, Xi'an 710129, China; shihaobin@nwpu.edu.cn (H.S.); panweihh@163.com (W.P.); wqt@nwpu.mail.edu.cn (Q.W.); maojiahui@nwpu.mail.edu.cn (J.M.)

\* Correspondence: yizheng@nwpu.edu.cn; Tel.: +86-029-8843-1517

**Abstract:** In quantum key distribution (QKD), there are some security loopholes opened by the gaps between the theoretical model and the practical system, and they may be exploited by eavesdroppers (Eve) to obtain secret key information without being detected. This is an effective quantum hacking strategy that seriously threatens the security of practical QKD systems. In this paper, we propose a new quantum hacking attack on an integrated silicon photonic continuous-variable quantum key distribution (CVQKD) system, which is known as a power analysis attack. This attack can be implemented by analyzing the power originating from the integrated electrical control circuit in state preparation with the help of machine learning, where the state preparation is assumed to be perfect in initial security proofs. Specifically, we describe a possible power model and show a complete attack based on a support vector regression (SVR) algorithm. The simulation results show that the secret key information decreases with the increase of the accuracy of the attack, especially in a situation with less excess noise. In particular, Eve does not have to intrude into the transmitter chip (Alice), and may perform a similar attack in practical chip-based discrete-variable quantum key distribution (DVQKD) systems. To resist this attack, the electrical control circuit should be improved to randomize the corresponding power. In addition, the power can be reduced by utilizing the dynamic voltage and frequency scaling (DVFS) technology.

**Keywords:** integrated continuous-variable quantum key distribution; quantum hacking; practical security



**Citation:** Zheng, Y.; Shi, H.; Pan, W.; Wang, Q.; Mao, J. Quantum Hacking on an Integrated Continuous-Variable Quantum Key Distribution System via Power Analysis. *Entropy* **2021**, *23*, 176. <https://doi.org/10.3390/e23020176>

Academic Editors: Antonino Messina and Agostino Migliore

Received: 3 December 2020

Accepted: 28 January 2021

Published: 30 January 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Quantum key distribution is an unconditionally secure quantum communication technology that promises that the authorized sender (Alice) and receiver (Bob) can share common keys through an insecure quantum channel in the presence of a potential eavesdropper (Eve) [1,2]. At present, discrete-variable quantum key distribution (DVQKD) and continuous-variable quantum key distribution (CVQKD) are two main categories of QKD systems that have been proved to be secure against general attacks (e.g., photon number splitting attacks on DVQKD and collective attacks on CVQKD) based on some basic assumptions [2–5]. Moreover, fiber-based QKD has been implemented by many research groups in laboratories and in field environments [6–10], and free-space QKD has been also studied experimentally. To further establish quantum communication networks, it is essential to explore high-performance and cost-effective QKD systems. Therefore, the implemented optical components of QKD systems were integrated on a silicon photonic chip by researchers in order to realize stable, miniaturized, and low-cost systems [11–16]. In particular, CVQKD with Gaussian-modulated coherent states (GMCS) is a widely studied protocol that has been integrated and realized [16]. Here, we focus on the exploration of chip-based GMCS CVQKD systems.

In the initial security proofs of QKD systems, the involved devices are modeled as secure and perfect. However, there are some imperfections in real-world QKD implemen-

tations that might open security loopholes for Eves to successfully steal secret key information [17,18]. These kinds of attacks are an effective quantum hacking strategy. For example, in practical DVQKD systems, an Eve may exploit some vulnerabilities in the single photon detector to launch a time-shift attack [19], an after-gate attack [20], a blinding attack [21], etc. Similarly, there are some quantum hacking attacks in practical CVQKD systems, such as the local oscillator (LO) fluctuation attack [22], LO calibration attack [23], wavelength attack [24,25], and saturation attack [26]. In addition, laser damage attacks and laser seeding attacks on the senders of QKD systems have been proposed [27–30]. It is important to note that these proposed quantum hacking attacks have corresponding countermeasures. The research on quantum attack and defense has effectively promoted commercial applications of QKD.

There is no doubt that chip-based QKD systems are also assumed to be perfect in security proofs. However, there are some new imperfections in practical chip-based QKD systems. For example, it is inevitable that the integrated electrical control circuit of a transmitter chip in a state preparation produces power associated with key information [31], which may open a new security loophole for Eves. In this work, we mainly investigate a possible quantum hacking attack exploited by this loophole in a chip-based GMCS CVQKD system. Based on the state preparation process in the transmitter of the system, we first modeled the power. The potential relation between the power and key information can be found by using some classical machine learning algorithms. Then, we exploited a support vector regression (SVR) algorithm to show the attack [32], which was composed of on-line and off-line stages. In the off-line stage, the same system was utilized by the Eve to collect power data in different periods. By using the SVR model to train these data, the aforementioned correlation could be obtained by the Eve, and could be exploited to analyze key information in a real-time chip-based GMCS CVQKD system. These analyses show a complete quantum hacking attack, which is named a power analysis attack. The simulation results indicate that the attack seriously destroys the practical security of the system. In particular, in low-noise environments, this impact is more obvious. Of course, a similar power analysis attack may be launched in practical chip-based DVQKD systems. Importantly, the power can be randomized by improving the electrical control circuit to effectively resist this attack. The dynamic voltage and frequency scaling (DVFS) technology can also be adopted to reduce the power to resist this attack. This study is of significance in promoting the establishment of quantum communication networks.

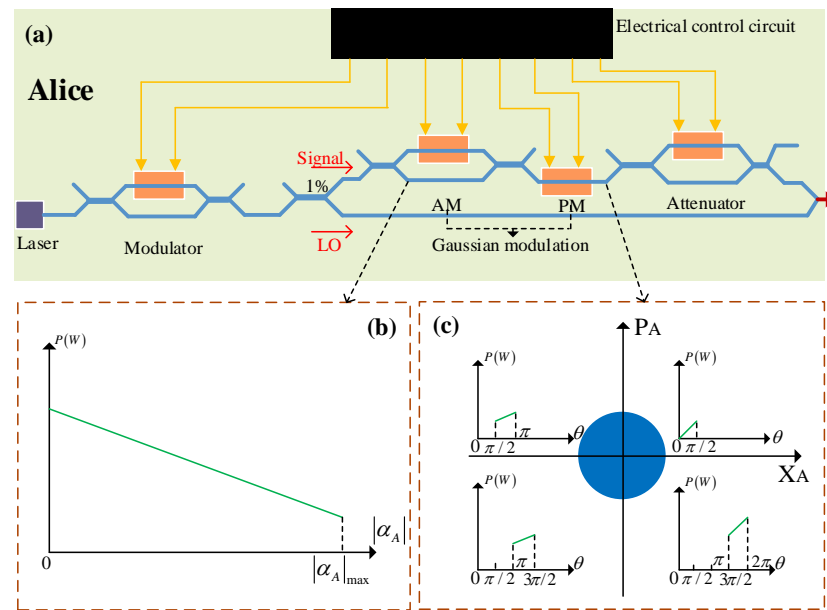
This paper is organized as follows: In Section 2, the power analysis attack is described and modeled. Then, we analyze the secret key rates of chip-based GMCS CVQKD systems under the effects of this attack in Section 3. To close the loophole opened by the power, some countermeasures are discussed in Section 4. Finally, conclusions are presented in Section 5.

## 2. Description of the Power Analysis Attack

Figure 1a shows the transmitter (Alice) of an integrated silicon photonic CVQKD system, where the involved optical components (except the laser source) are integrated on a silicon photonic chip [16]. In the chip, the first and last modulators serve attenuators to adjust the intensity of the optical signal. The other modulators (an amplitude modulator and a phase modulator) are exploited by Alice to generate a series of Gaussian-modulated coherent states  $|\alpha_A\rangle_u$  ( $u = 1, 2, \dots, N$ ) loaded with key information, where  $N$  is the total number of the generated states [7,16]. Based on the phase space,  $|\alpha_A\rangle_u$  can be represented as

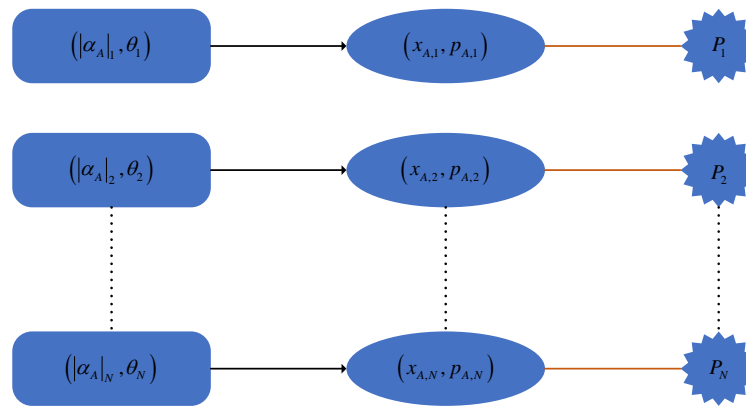
$$\begin{aligned} |\alpha_A\rangle_u &= |\alpha_A|_u e^{i\theta_u} = x_{A,u} + ip_{A,u}, \\ x_{A,u} &= |\alpha_A|_u \cos \theta_u, p_{A,u} = |\alpha_A|_u \sin \theta_u, \end{aligned} \quad (1)$$

where  $|\alpha_A\rangle_u$  and  $\theta_u$  are the amplitudes and phases of these Gaussian-modulated states, respectively. In particular,  $x_{A,u}$  and  $p_{A,u}$  are random numbers that obey a Gaussian distribution  $N(0, V_A N_0 + N_0)$ . Here,  $N_0$  is the variance of shot noise.



**Figure 1.** A possible power model of an integrated electrical control circuit in a Gaussian modulation of an integrated silicon photonic continuous-variable quantum key distribution (CVQKD) system, for which a similar relation in a classical chip has clearly been obtained [31]. Part (a) describes the transmitter of the chip-based CVQKD system. Part (b) shows the possible power in the amplitude modulation. Part (c) depicts the possible power in the phase modulation. AM, amplitude modulator; PM, phase modulator; LO, local oscillator.

In security proofs, the above state preparation is assumed to be perfect. However, it is inevitable that the integrated electrical control circuit of the transmitter chip generates power in the Gaussian modulation of practical chip-based CVQKD systems [31]. Here, the power produced by the integrated electrical circuit includes dynamic power  $P_{dy}$  and static power  $P_{st}$ , where the dynamic power can be further divided into two parts: switching power  $P_{sw}$  and short-circuit power  $P_{sh}$ . Moreover,  $P_{sw} = C_L V_{dd}^2 H_t f_c$ ,  $P_{sh} = L(V_{dd} - 2V_T)^3 \tau f_c H_t$ ,  $P_{st} = V_{dd} I_{leakage}$ , where  $C_L$  is the load capacitance,  $V_{dd}$  is the supply voltage,  $H_t$  is a trns factor,  $f_c$  is the clock frequency,  $L$  is a technical parameter,  $V_T$  is the threshold voltage,  $\tau$  is the rise and fall time of the input signal, and  $I_{leakage}$  is the leakage current [33]. In particular, the leakage current mainly includes the gate-induced drain leakage current, gate leakage current, reverse bias junction leakage current, and sub-threshold leakage current. These formulas for power indicate that the power is different when the operation statuses of the integrated control circuit are different. For the encoding of different key information, the required modulation voltages are different. Therefore, the power generated by the integrated electrical control circuit in the preparation process of these transmitted states should be different. Figure 1b depicts a possible power model during intensity modulation, where the power may decrease with the increase of the amplitude of the Gaussian-modulated coherent states. Figure 1c reveals a possible power model for phase modulation, where the power may be enhanced with the increase in the phase of the Gaussian-modulated states. According to Equation (1), the total power  $P_u$  originating from the integrated electrical control circuit during Gaussian modulation should be hidden with a relation with random numbers  $x_{A_u}$  or  $p_{A_u}$ , which is revealed in Figure 2. In particular, this relation is ambiguous in practical systems, and may be found by Eve through a classical machine learning algorithm. Therefore, the power originating from the integrated electrical control circuit of the transmitter of the practical chip-based CVQKD system may open a security loophole for Eve to successfully obtain key information, which seriously destroys the practical security of the system.



**Figure 2.** The correlation between the power and the key information in the state preparation.

Figure 3 clearly introduces a complete power analysis attack, which includes two steps. The first step is off-line analysis. The purpose of this step is to explore the potential relationship between the key information and the power produced by the integrated electrical control circuit in state preparation. Specifically, Eve first utilizes an identical chip and a power meter to collect a series of power data originating from the integrated electrical control circuit in the preparation processes of different Gaussian-modulated coherent states, where Eve does not need to use some means to enter the transmitter chip. Then, some classical machine learning algorithms may be exploited by Eve to analyze the acquired data and get

$$\begin{aligned}
 P &= f(x_A), \\
 P &= g(p_A),
 \end{aligned}
 \tag{2}$$

where  $P$  is the power variable and  $x_A$  and  $p_A$  are two quadrature variables of the Gaussian-modulated optical signal. The above correlation may be nonlinear. Therefore, a support vector regression (SVR) algorithm may be exploited by Eve to analyze data, which can be modeled as [32]

$$f(x_A) = \mathbf{W}^T \Phi(x_A) + b,
 \tag{3}$$

where  $\Phi(\cdot)$  is a function that maps the input data into a higher dimensional space,  $\mathbf{W}$  is the weight vector, and  $b$  is the bias. In order to achieve the optimal parameters  $\mathbf{W}$  and  $b$ , the SVR model can be simplified as

$$\min \frac{1}{2} \|\mathbf{W}\|^2 + C \sum_{u=1}^N (\xi_u + \xi_u^*), C > 0,
 \tag{4}$$

subject to

$$\begin{aligned}
 f(x_{A,u}) - P_u &\leq \epsilon + \xi_u, \\
 P_u - f(x_{A,u}) &\leq \epsilon + \xi_u^*, \\
 \xi_u &\geq 0, \xi_u^* \geq 0, \epsilon > 0,
 \end{aligned}
 \tag{5}$$

where  $C$  is a regularization parameter, and  $\xi_u$  and  $\xi_u^*$  respectively represent the upper and lower constraints in the outputs. In particular,  $\epsilon$  is the permissible error. Then,  $\mathbf{W}$  can be calculated as

$$\mathbf{W} = \sum_{u=1}^N (\lambda_u - \lambda_u^*) \Phi(x_{A,u}).
 \tag{6}$$

Here,  $\lambda_u$  is the Lagrange multiplier. In addition, parameter  $b$  can also be calculated after  $\mathbf{W}$  is obtained. According to Equations (3) and (6), the SVR model can be expressed by

$$\begin{aligned}
 f(x_A) &= \sum_{u=1}^N (\lambda_u - \lambda_u^*) \Phi^T(x_{A,u}) \Phi(x_A) + b \\
 &= \sum_{u=1}^N (\lambda_u - \lambda_u^*) k(x_{A,u}, x_A) + b,
 \end{aligned}
 \tag{7}$$

where  $k(\cdot, \cdot)$  is a kernel function that includes three basic kernels: a polynomial kernel, linear kernel, and radial basis function (RBF). In general, the RBF kernel is a reasonable choice, as it has low complexity and can solve the nonlinear relation. Here, the corresponding kernel function in Equation (7) should also be the RBF kernel, which is as follows:

$$k(x_{A,u}, x_A) = \exp\{-\gamma|x_A - x_{A,u}|^2\}.
 \tag{8}$$

Here,  $\gamma$  indicates the scale parameter of the RBF kernel and determines model performance. In particular, the data collected by Eve in other time periods can serve as the test data. Based on the test data, the mean squared error (MSE) can be calculated as

$$MSE = \frac{1}{n_t} \sum_{i=1}^{n_t} [f(x_{t,i}) - P_{t,i}]^2,
 \tag{9}$$

where  $n_t$  is the amount of the test data, and  $x_{t,i}$  and  $P_{t,i}$  are the values in test data. Here, MSE reflects the performance of the SVR algorithm. The smaller the value of the MSE, the better the performance of the algorithm. It is important to note that the potential relation between  $p_A$  and the power  $P$  can also be explored by using the SVR model presented by Equations (3)–(8). When Equation (2) is acquired by Eve, she can further get

$$\begin{aligned}
 x_A &= f^{-1}(P), \\
 p_A &= g^{-1}(P).
 \end{aligned}
 \tag{10}$$

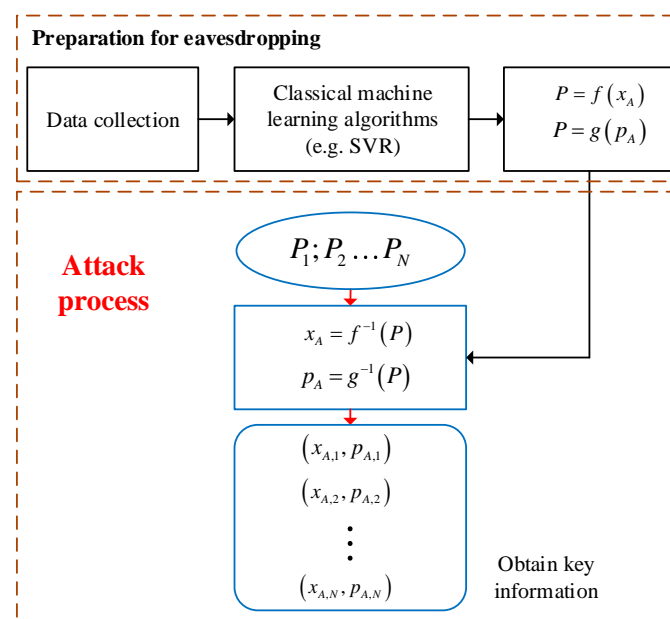


Figure 3. The process of the power analysis attack. SVR, support vector regression.

In a practical chip-based CVQKD system, Eve can exploit the acquired Equation (10) to steal key information by analyzing the power originating from the integrated electrical

control circuit in state preparation, which is on-line analysis. This step is the core of the power analysis attack. Here, we define  $P_a = 1 - MSE (0 \leq MSE < 1)$  as the accuracy of the power analysis attack that reflects the attack strength. In addition, when  $MSE \geq 1$ , the performance of the algorithm is poor, which indicates that the attack is ineffective. In particular, a similar attack can also be implemented in practical chip-based DVQKD systems.

### 3. Security Analysis

The performance of a chip-based CVQKD system can be measured by the secret key rate and the maximal transmission distance of the system. Given the parameters  $V_A, T, \epsilon, \eta$ , and  $\nu_{el}$ , the information shared by Alice and Bob can be calculated, as well as the maximal bound on the information available to the eavesdropper. Here,  $T$  and  $\epsilon$  respectively represent the transmittance and excess noise of the quantum channel, which can be evaluated through parameter estimation. In addition,  $\eta$  and  $\nu_{el}$  are the detector's fixed parameters, which respectively indicate the working efficiency and electronic noise. The secret key rate  $K$  with  $n$  received pulses used for key establishment against collective attacks is expressed as [18,22,27,34]

$$K = \frac{n}{N} [\beta I_{AB} - S_{BE}^{\epsilon_{PE}} - \Delta(n)], \tag{11}$$

where reverse reconciliation and a finite-size effect are considered,  $n = N - m$ ,  $N$  is the total number of the received pulses,  $m$  gives the values used for parameter estimation,  $\beta \in (0, 1)$  is the reconciliation efficiency,  $S_{BE}^{\epsilon_{PE}}$  represents the maximal value of the Holevo information compatible with the statistics except for probability  $\epsilon_{PE}$ , and  $I_{AB}$  represents the Shannon mutual information between Alice and Bob. Moreover,  $\Delta(n)$  is a linear function of  $n$  that is related to the security of the privacy amplification. It can be given by [18,34]

$$\Delta(n) = 7 \sqrt{\frac{\log_2(1/\bar{\epsilon})}{n}} + \frac{2}{n} \log_2 \frac{1}{\epsilon_{PA}}, \tag{12}$$

where  $\bar{\epsilon}$  and  $\epsilon_{PA}$ , which are virtual parameters and can be optimized in the computation, denote the smoothing parameter and the failure probability of the privacy amplification, respectively. In addition,  $\bar{\epsilon}$  and  $\epsilon_{PA}$  are usually set to be equal to  $\epsilon_{PE}$  because the value of  $\Delta(n)$  mainly depends on  $n$ . It is important to note that the power analysis attack does not affect the transmitted states and the measurement of the received states. Therefore, the attack does not affect the parameter estimation, which indicates that Equations (11) and (12) cannot be destroyed by the attack.

According to the above analysis, the secret key rate of a system under a power analysis attack should be given by

$$K_P = (1 - P_a) \frac{n}{N} [\beta I_{AB} - S_{BE}^{\epsilon_{PE}} - \Delta(n)]. \tag{13}$$

Here,  $I_{AB}$  can be derived from Bob's measured variance  $V_B$  and the conditional variance  $V_{B|A}$  as

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2} \log_2 \frac{V_A + 1 + \chi_{tot}}{1 + \chi_{tot}}, \tag{14}$$

where  $\chi_{tot} = \chi_{line} + \chi_{hom}/T$  represents the total noise referred to the channel input,  $\chi_{line} = 1/T - 1 + \epsilon$ , and  $\chi_{hom} = [(1 - \eta) + \nu_{el}]/\eta$ . In particular,  $S_{BE}^{\epsilon_{PE}}$  is determined by the following covariance matrix between Alice and Bob with a finite-size effect:

$$\Gamma_{AB} = \begin{bmatrix} (V_A + 1)\mathbb{I} & \sqrt{T_{\min}(V_A^2 + 2V_A)}\sigma_z \\ \sqrt{T_{\min}(V_A^2 + 2V_A)}\sigma_z & [T_{\min}(V_A + \epsilon_{\max}) + 1]\mathbb{I} \end{bmatrix}, \tag{15}$$

where matrices  $\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  and  $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ . Here,  $T_{\min}$  and  $\varepsilon_{\max}$  respectively correspond to the lower bound of  $T$  and the upper bound of  $\varepsilon$ , which are defined as

$$\begin{aligned} T_{\min} &= (t_{\min})^2, \\ \varepsilon_{\max} &= \frac{\sigma_{\max}^2 - 1}{T}. \end{aligned} \tag{16}$$

According to Refs. [18,34], when  $m$  is large enough (e.g.,  $m > 10^6$ ),  $t_{\min}$  and  $\sigma_{\max}^2$  can be calculated as

$$\begin{aligned} t_{\min} &\approx \sqrt{T} - z_{\varepsilon_{\text{PE}}/2} \sqrt{\frac{1 + T\varepsilon}{mV_A}}, \\ \sigma_{\max}^2 &\approx 1 + T\varepsilon + z_{\varepsilon_{\text{PE}}/2} \frac{(1 + T\varepsilon)\sqrt{2}}{\sqrt{m}}, \end{aligned} \tag{17}$$

where  $z_{\varepsilon_{\text{PE}}/2}$  follows  $1 - \frac{1}{2}\text{erf}(z_{\varepsilon_{\text{PE}}/2}/\sqrt{2}) = \frac{1}{2}\varepsilon_{\text{PE}}$ , and  $\text{erf}(\cdot)$  is the error function defined as  $\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ . Then,  $S_{\text{BE}}^{\varepsilon_{\text{PE}}}$  can be acquired by

$$S_{\text{BE}}^{\varepsilon_{\text{PE}}} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \tag{18}$$

where  $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ ,  $\lambda_i \geq 1$  are symplectic eigenvalues derived from covariance matrices, which can be written as

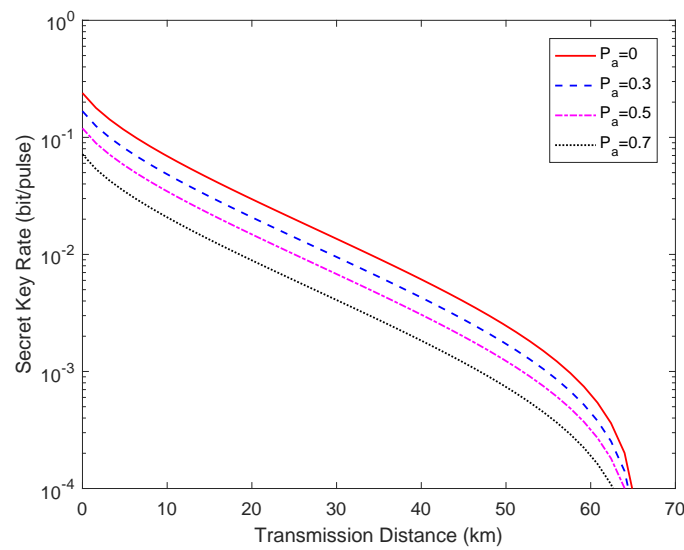
$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \\ \lambda_{3,4}^2 &= \frac{1}{2}(C \pm \sqrt{C^2 - 4D}), \\ \lambda_5 &= 1, \end{aligned} \tag{19}$$

where

$$\begin{aligned} A &= (V_A + 1)^2 - 2T_{\min}(V_A^2 + 2V_A) \\ &\quad + [T_{\min}(V_A + \varepsilon_{\max}) + 1]^2, \\ B &= [(T_{\min}\varepsilon_{\max} + 1)(V_A + 1) - T_{\min}V_A]^2, \\ C &= \frac{A\chi_{\text{hom}} + (V_A + 1)\sqrt{B} + T_{\min}(V_A + \varepsilon_{\max}) + 1}{\eta T_{\min}(V_A + \varepsilon_{\max}) + 1 + \nu_{\text{el}}}, \\ D &= \frac{\sqrt{B}(V_A + 1) + B\chi_{\text{hom}}}{\eta T_{\min}(V_A + \varepsilon_{\max}) + 1 + \nu_{\text{el}}}. \end{aligned} \tag{20}$$

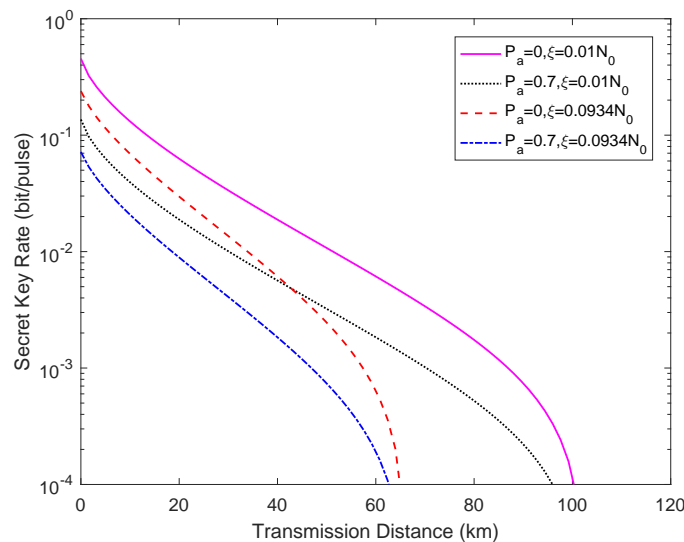
Eventually, based on Equations (12)–(20), one can evaluate the secret key rate of a system under a power analysis attack.

Figure 4 depicts the relationship between the secret key rate and the transmission distance for a practical chip-based CVQKD system under the effects of a power analysis attack when  $P_a = 0, 0.3, 0.5, 0.7$ . In particular,  $P_a = 0$  indicates that the attack was not carried out, i.e., the ideal case. The fixed parameters for the simulation are set as [16]:  $V_A = 7.07$  (in shot-noise units),  $\eta = 0.498$ ,  $\nu_{\text{el}} = 0.0691$  (in shot-noise units),  $\beta = 98\%$ ,  $\varepsilon = 0.0934$  (in shot-noise units), and  $\epsilon = 10^{-10}$ ,  $m = 0.5 \times N$ , respectively. It is obvious that the secret key rate  $K_P$  evaluated by Alice and Bob under the effects of the power analysis attack are reduced compared with the ideal value. The difference between the attacked secret key rate and the ideal value indicates the key information obtained by Eve.



**Figure 4.** Secret key rate vs. transmission distance for different attack situations, where  $P_a = 0$  represents the ideal case without an attack. The fiber loss is 0.2 dB/km.

Figure 5 describes the secret key rate versus the transmission distance under different excess noise levels (i.e.,  $\epsilon = 0.0934, 0.01$ ) when  $P_a = 0.7$ . The other simulation parameters remain unchanged. We find that Eve can acquire more secret key information in the case of less excess noise under the same attack strength.



**Figure 5.** Secret key rate vs. transmission distance for different excess noise situations when  $P_a = 0.7$ , where  $P_a = 0$  represents the ideal case without an attack.

More importantly, defending against power analysis attacks is a key task for establishing a quantum communication network, which is discussed in the next section.

#### 4. Countermeasures

A complete power analysis attack is shown in the above analysis. The potential relation between key information and the power produced by the integrated electrical control circuit in state preparation is a security loophole exploited by Eve in the attack. Therefore, the electrical control circuit can be improved by randomizing the power to close this loophole, thus effectively resisting this attack. In addition, the pipeline structure and parallel structure can be adopted to optimize the electrical control circuit to reduce the power.



Apart from the above countermeasures, dynamic voltage and frequency scaling (DVFS) technology can be applied to reduce the dynamic power. The workflow of DVFS is as follows [35]:

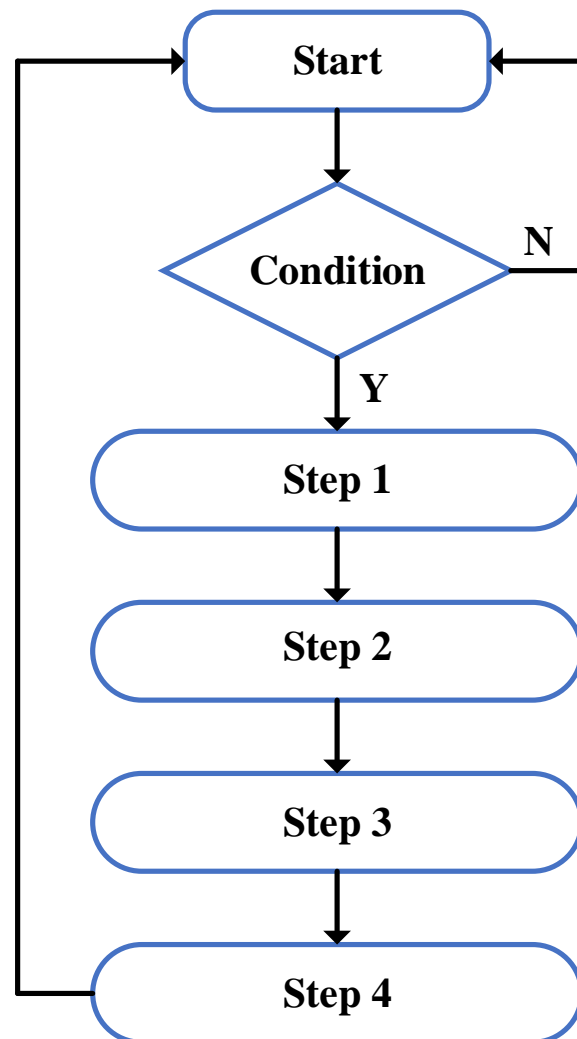
Step 1: The signal related to system load is collected to calculate the current system load for the integrated electrical control circuit;

Step 2: Based on the current system load, the required performance is predicted for the control circuit system;

Step 3: The prediction performance is converted into the required frequency to adjust the clock setting of the integrated control circuit;

Step 4: According to the acquired frequency, the corresponding voltage can be obtained. Then, based on the acquired voltage, the central processing unit (CPU) voltage can be adjusted.

Figure 6 shows a flowchart of a fast DVFS algorithm, where the judged condition is that the integrated control circuit sends data. As shown above, steps 1 to 4 have been described. In particular, the principle of the power produced by the integrated electrical control circuit in chip-based DVQKD systems is similar to that of integrated CVQKD systems. Therefore, these countermeasures can also be applied to resist similar attacks in chip-based DVQKD systems.



**Figure 6.** The flow of the dynamic voltage and frequency scaling (DVFS) algorithm. N, not; Y, yes.

## 5. Conclusions

We have proposed a quantum hacking attack—namely, the power analysis attack—on an integrated silicon photonic CVQKD system. We first modeled the possible power originating from the integrated electrical control circuit in state preparation in the transmitter of the system, which clearly shows the correlation between the key information and the power. This correlation can be explored by Eve through some classical machine learning algorithms to steal key information, which indicates that the power produced by the electrical control circuit in state preparation can open a security loophole. Then, based on the SVR model, we showed a complete power analysis, which included off-line analysis and on-line real-time stealing. We found that Eve can acquire more key information in an environment with less excess noise through numerical analysis. In particular, a similar security loophole may also exist in chip-based DVQKD systems. Finally, electrical control circuits can be improved to effectively resist power analysis attacks. In addition, DVFS technology can also be applied to weaken the power. These countermeasures promote the application of QKD and the establishment of quantum communication networks.

**Author Contributions:** Y.Z. designed the conception of the study, accomplished the formula derivation and numerical simulations, and drafted the article. H.S. gave the general idea of the study, checked the draft, and provided feasible suggestions and a critical revision of the manuscript. W.P. reviewed relevant studies and the literature, conceived of and designed the study, and performed a critical revision of the manuscript. Q.W. conceived of the study and reviewed relevant studies. J.M. gave feasible advice and helped with the calculation. All authors have read and approved the final manuscript.

**Funding:** This research was funded by the National Natural Science Foundation of China (Grants No. 61976178, 62076202).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [[CrossRef](#)]
2. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [[CrossRef](#)]
3. Lo, H.K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056. [[CrossRef](#)]
4. Scarani, V.; Acín, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [[CrossRef](#)]
5. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502. [[CrossRef](#)]
6. Takesue, H.; Nam, S.W.; Zhang, Q.; Hadfield, R.H.; Honjo, T.; Tamaki, K.; Yamamoto, Y. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics* **2007**, *1*, 343–348. [[CrossRef](#)]
7. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [[CrossRef](#)]
8. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323. [[CrossRef](#)]
9. Fossier, S.; Diamanti, E.; Debuisschert, T.; Villing, A.; Tualle-Brouri, R.; Grangier, P. Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.* **2009**, *11*, 045023. [[CrossRef](#)]
10. Zhang, Y.; Chen, Z.; Pirandola, S.; Wang, X.; Zhou, C.; Chu, B.; Zhao, Y.; Xu, B.; Yu, S.; Guo, H. Long-distance continuous-variable quantum key distribution over 202.81 km fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [[CrossRef](#)]
11. Sibson, P.; Erven, C.; Godfrey, M.; Miki, S.; Yamashita, T.; Fujiwara, M.; Sasaki, M.; Terai, H.; Tanner, M.G.; Natarajan, C.M.; et al. Chip-based quantum key distribution. *Nat. Commun.* **2017**, *8*, 1–6. [[CrossRef](#)] [[PubMed](#)]
12. Semenenko, H.; Sibson, P.; Hart, A.; Thompson, M.G.; Rarity, J.G.; Erven, C. Chip-based measurement-device-independent quantum key distribution. *Optica* **2020**, *7*, 238–242. [[CrossRef](#)]
13. Wei, K.; Li, W.; Tan, H.; Li, Y.; Min, H.; Zhang, W.J.; Li, H.; You, L.; Wang, Z.; Jiang, X.; et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **2020**, *10*, 031030.
14. Bunandar, D.; Lentine, A.; Lee, C.; Cai, H.; Long, C.M.; Boynton, N.; Martinez, N.; DeRose, C.; Chen, C.; Grein, M.; et al. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X* **2018**, *8*, 021009. [[CrossRef](#)]

15. Cao, L.; Luo, W.; Wang, Y.X.; Zou, J.; Yan, R.D.; Cai, H.; Zhang, Y.; Hu, X.L.; Jiang, C.; Fan, W.J.; et al. Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems. *Phys. Rev. Appl.* **2020**, *14*, 011001. [[CrossRef](#)]
16. Zhang, G.; Haw, J.Y.; Cai, H.; Xu, F.; Assad, S.M.; Fitzsimons, J.F.; Zhou, X.; Zhang, Y.; Yu, S.; Wu, J.; et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photonics* **2019**, *13*, 839–842. [[CrossRef](#)]
17. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [[CrossRef](#)]
18. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 032309. [[CrossRef](#)]
19. Qi, B.; Fung, C.H.F.; Lo, H.K.; Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **2007**, *7*, 73–82.
20. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New J. Phys.* **2011**, *13*, 013043. [[CrossRef](#)]
21. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [[CrossRef](#)]
22. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [[CrossRef](#)]
23. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [[CrossRef](#)]
24. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [[CrossRef](#)]
25. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [[CrossRef](#)]
26. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [[CrossRef](#)]
27. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Practical security of continuous-variable quantum key distribution with reduced optical attenuation. *Phys. Rev. A* **2019**, *100*, 012313. [[CrossRef](#)]
28. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack. *Opt. Express* **2019**, *27*, 27369–27384. [[CrossRef](#)]
29. Huang, A.; Navarrete, Á.; Sun, S.H.; Chaiwongkhot, P.; Curty, M.; Makarov, V. Laser-seeding attack in quantum key distribution. *Phys. Rev. Appl.* **2019**, *12*, 064043. [[CrossRef](#)]
30. Huang, A.; Li, R.; Egorov, V.; Tchouragoulov, S.; Kumar, K.; Makarov, V. Laser-damage attack against optical attenuators in quantum key distribution. *Phys. Rev. Appl.* **2020**, *13*, 034017. [[CrossRef](#)]
31. Ratanpal, G.B.; Williams, R.D.; Blalock, T.N. An on-chip signal suppression countermeasure to power analysis attacks. *IEEE Trans. Depend. Secur. Comput.* **2004**, *1*, 179–189. [[CrossRef](#)]
32. Chang, C.C.; Lin, C.J. LIBSVM: A library for support vector machines. *ACM Trans. Intell. Syst. Technol.* **2011**, *2*, 1–27. [[CrossRef](#)]
33. Enz, C.C.; Vittoz, E.A. CMOS low-power analog circuit design. In Proceedings of the Emerging Technologies: Designing Low Power Digital Systems, Israel, 15 May 1996; pp. 79–133. [[CrossRef](#)]
34. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [[CrossRef](#)]
35. Wonyoung, K.; Gupta, M.S.; Wei, G.; Brooks, D. System level analysis of fast, per-core DVFS using on-chip switching regulators. In Proceedings of the 2008 IEEE 14th International Symposium on High Performance Computer Architecture, Salt Lake City, UT, USA, 16–20 February 2008; pp. 123–134. [[CrossRef](#)]