# 通过量子背景相关性验证的随机数生成器研究

（申请清华大学工学硕士学位论文）


培 养 单 位 ： 交叉信息研究院

学 科 ： 计算机科学与技术

研 究 生 ： 严 马 可

指 导 教 师 ： 金 奇 奂 副 教 授


二〇一四年五月

通过量子背景相关性验证的随机数生成器研究

严马可

# Research on Random Number Generation Certified by Quantum Contextuality

Thesis Submitted to

**Tsinghua University**

in partial fulfillment of the requirement

for the degree of

**Master of Science**

in

**Computer Science and Technology**

by

**Mark Um**

Thesis Supervisor ： Associate Professor Kihwan Kim

**May, 2014**

# 关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容。

本人保证遵守上述规定。

**（保密的论文在解密后遵守此规定）**

| | | | |
|---|---|---|---|
| 作者签名： | 严马可 | 导师签名： | |
| 日期： | 2014.5.2 | 日期： | |

# 摘　要

量子力学本质上的不可预测性正好可以用来生成真正意义上的随机数。本论文描述的随机数生成器的随机性和安全性通过量子背景相关性得到验证，Kochen-Specker（KS）定理能够将利用量子力学生成的结果与利用经典力学生成的结果区分开来。此项工作用一个囚禁的 $^{171}Yb^{+}$离子的三个内部能级生成随机数。

论文中的实验利用 KS 不等式，更具体地，利用了 Klyachko-Can-Binicioglu-Shumovsky（KCBS）不等式，它表现了量子力学当中测量结果对测量背景的依赖性，这样既保持了严格的随机性，同时也大大简化了实验要求，能够以较快的速度生成随机数。实验生成的随机数据明显破坏了经典力学当中的 KCBS 不等式，验证了其随机性。而不等式的破坏值还能够进一步为生成的随机数字符串提供随机性最小熵的下限。再者，囚禁离子技术的探测效率趋近于完美，由此彻底克服了一般量子光学实验中存在的探测漏洞，充分地保证了随机性。此项实验工作提供了一个实用性的快速、安全的随机数的生成器，会在很多实际应用中发挥重要作用。

此项工作可以通过进一步延伸关闭相容性漏洞，这项扩展需要囚禁一个具有稳定的搁置态的 $^{137}Ba^{+}$ 离子，而这两种离子的混合囚禁可以通过完美的同时测量使随机数生成器更加高效。为此，我们需要控制离子的外部运动态来实现一个完全摆脱漏洞的随机数生成器。本论文的成果还包括在实验中通过拉曼跃迁技术实现了离子-激光的相互作用，还拓展出离子外部运动态中的声子数态$|n\rangle$的加减操作。借助绝热蓝边带跃迁技术的开发，对于 0 到 10 的任何一个声子数 $n$，离子的声子数态得到了+1 或-1 平移，并在实验中观察到了非经典声子态的产生。

**关键词**：随机数；量子力学；量子背景相关性；囚禁离子；声子数态

# Abstract

The intrinsic unpredictability of quantum mechanics can be used to generate genuine randomness. This dissertation demonstrates a random number generator certified by quantum contextuality, where Kochen-Specker(KS) theorem distinguishes the results of classical theories from those of quantum mechanics. In my work, three internal levels in a single trapped $^{171}Yb^{+}$ ion are used to generate random numbers.

We observe a violation of a KS inequality, in particular, the Klyachko-Can-Binicioglu-Shumovsky (KCBS) inequality which shows the measurement result in quantum mechanics rely on the context of the measurement. In this way, we not only guarantee the randomness strictly, but also lower the experimental requirement, thus the speed of random number generation can be reasonably fast. Generated experimental result obvious breaks the inequality and certifies its randomness. Furthermore, the violation value of the inequality provides the bounds for the minimum entropy in the generated string. It can be emphasized that this experiment closes the detection loophole due to the perfect detection fidelity, which secures the random number generation. This experiment provides a practical fast and secure random number generator which will play an important role in various applications.

This work can be extended to close the compatibility loophole by trapping a $^{137}Ba^{+}$ ion which has stable shelving states, and hybrid trapping of these two species of ions in the same trap will further improve the random number generation by implementing perfect sequential measurement. It requires the control of external motional state of the ion to achieve a loophole-free random number generator. This dissertation involves the result in developing ion-light interaction by Raman transition technique and extension of addition and substraction operations to external motional phonon state $|n\rangle$ of the ion. By the development of adiabatic blue sideband transition, we accomplish +1 and -1 shift to phonon number for any *n* from 0 to 10 and observe the production of non-classical state of phonon.

**Key words:** random number; quantum mechanics; quantum contextuality; trapped ion; phonon state

# Contents

Chapter 1 Introduction ..... 1
1.1 Random Numbers ..... 1
1.2 Quantum Contextuality ..... 1
1.3 Trapped Ion System ..... 2
Chapter 2 Random Number Generation and Certification ..... 5
2.1 The KCBS Inequality ..... 5
2.2 Violation of the KCBS inequality ..... 6
2.3 Random Number Generation ..... 10
2.4 Minimum Entropy of Randomness ..... 14
2.5 Experimental Setup ..... 19
2.6 Experimental Result ..... 22
2.7 Extension for Loophole Free Experiment ..... 26
Chapter 3 Phonon Shift Operation ..... 30
3.1 Motional Structure of an Ion ..... 30
3.2 Stimulated Raman Transition ..... 31
3.3 Sideband Cooling ..... 36
3.4 Rapid Adiabatic Transition Process ..... 40
3.5 Experimental Setup ..... 42
3.6 Experimental Result ..... 45
3.7 Related Work ..... 46
Chapter 4 Conclusion ..... 50
4.1 Experimental Conclusion ..... 50
4.2 Outlook ..... 50
Bibliography ..... 51
致 谢 ..... 55
声 明 ..... 56

个人简历、在学期间发表的学术论文与研究成果 .....57

# Chapter 1 Introduction

## 1.1 Random Numbers

Random number generation is important for many applications[1,2]. For cryptographic applications, random numbers should have good unpredictability in order to be secure under attack by the adversaries[3]. Genuine random numbers can never be generated by a classical device because any classical device bears in principle a deterministic description. Quantum mechanics, on the other hand, has intrinsic randomness, and thus can be explored to construct a genuine random number generator. There have been many demonstrations of random number generators based on quantum principles[4-14].

Self-certified random number generation is an advance made recently, where the randomness is guaranteed by violation of certain fundamental inequalities[14-16]. In particular, it was proposed in Refs. 14,15 that through violation of the Clauser-Horn-Shimony-Holt (CHSH) inequality, one can certify the generated random numbers in a device-independent fashion that is secure against the adversaries who have only classical side information[17]. The first proof-of-principle experiment for this scheme has been recently demonstrated[14].

## 1.2 Quantum Contextuality

We consider here a scenario where the provider of the device is assumed to be honest. However, we still need to physically certify that the random numbers are generated due to the intrinsic uncertainty of quantum mechanics instead of some uncontrolled classical noise process in the device. In this case, we can use quantum contextuality manifested through the violation of certain Kochen-Specker (KS) inequality to certify the generated random numbers[18,19]. Quantum contextuality is a basic property of quantum mechanics, where the measurement outcomes depend on the specific context of the measurements[20,21]. Quantum contextuality would be revealed by violations of some KS inequalities, and such violations can be observed even in a single indivisible system without any entanglement[22-27]. Because there is no need of entanglement, a certification

scheme of random numbers based on the KS theorem can significantly simplify the experimental requirement and generate certified random numbers with a much higher speed[18]. A proof-of-principle experimental implementation of this idea has been reported with a photonic system quite recently[18].

## 1.3 Trapped Ion System

Trapped ion system has been in the forefront of quantum optics, quantum information, quantum metrology and quantum thermodynamics, especially one of the strongest candidates for large-scale practical quantum computation as it performed a series of ground-breaking experiments demonstrating universal quantum gates and quantum teleportation over the last decades. It has been shown to be a paramount example for precision and control. The advantage of long coherence time of trapped ion systems and the easy access to long range tunable interactions make it a dominant example for precision and control. Technology of trapping ions has also achieved great advances in gathering the knowledge about the interaction of light with atomic particles as well as implementation of multiple gate operations involving a quantum controlled-NOT gate proposed by Cirac and Zoller[32]. This technique is applicable to a large number of qubits in scalable trap structures.

We perform the test of the experiment with a single trapped Ytterbium ($^{171}Yb^{+}$) ion in a four-rod radio-frequency(RF) trap (shown in Figure 1.2(a)(b)) based on the confining action of static and time-dependent electric fields[26,29].

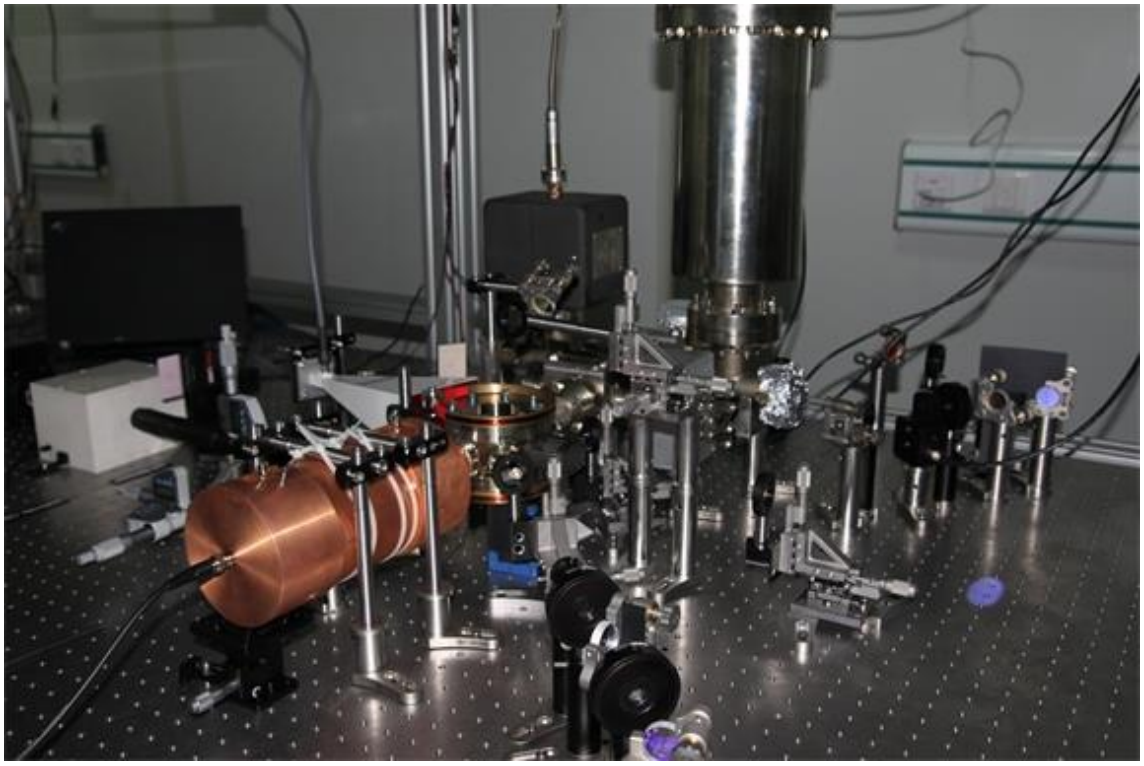


Figure 1.1 Tsinghua ion trap. RF signal is amplified and connected to the trap through a helical resonator. An ion pump and a Ti sublimation pump are connected to the trap to make ultra-high vacuum environment lower than $10^{-11}$ torr.

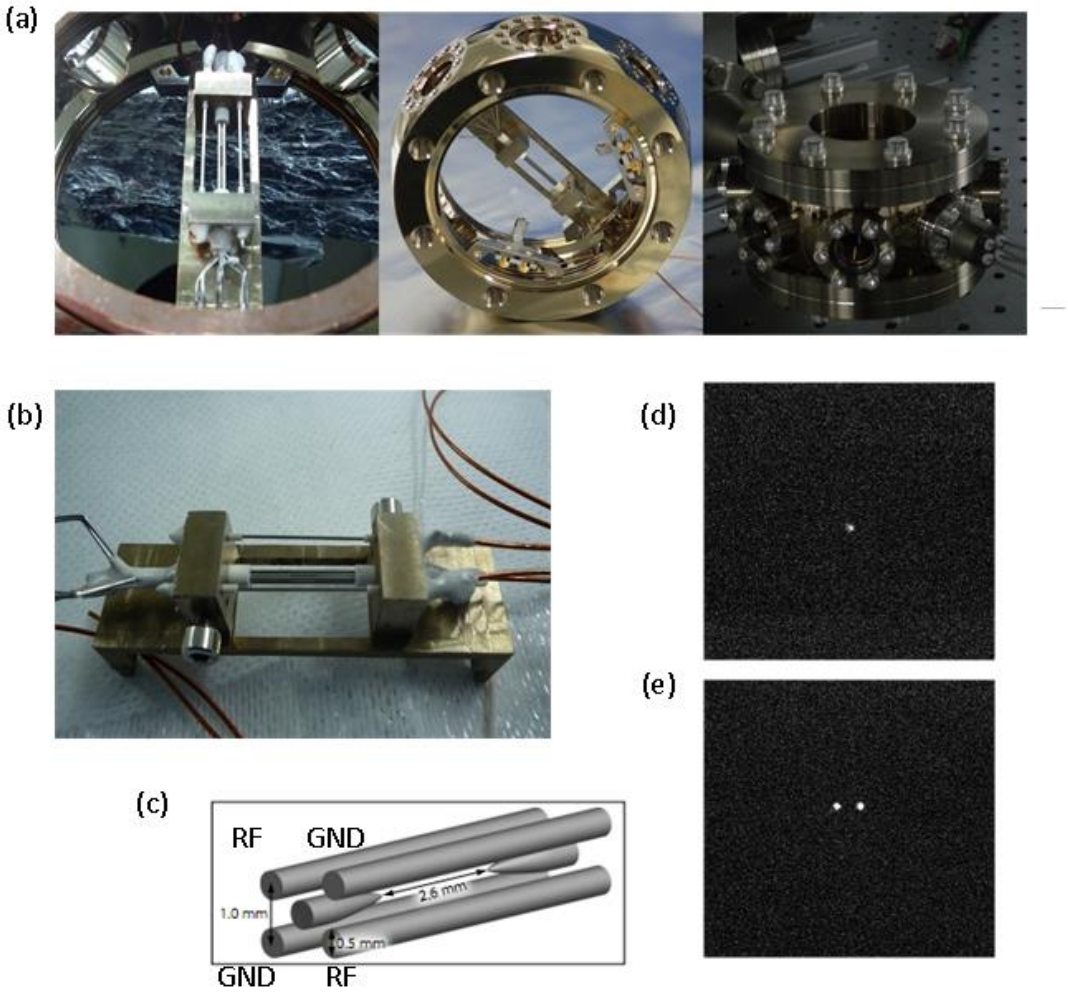



Figure 1.2 Four-rod trap and pictures of $^{171}Yb^{+}$ ion. (a) Connection of the trap and oven of $^{171}Yb^{+}$ ion in an octagon. The lasers shine into the trap through viewports. (b) Assembly of the four-rod trap with two micromotion compensation electrodes on the top. (c) Schematic of the four-rod trap. Among the four rods, two connect to RF while the other two are ground(GND) electrodes. In Chapter 3, the two ground electrodes are given 10.6V DC voltage to differentiate the two transverse modes clearly (380 KHz apart). (d)(e) Pictures of one/two trapped $^{171}Yb^{+}$ ion on the CCD camera.

# Chapter 2 Random Number Generation and Certification

## 2.1 The KCBS Inequality

A particular type of the KS inequality, the Klyachko-Can-Binicioglu-Shumovsky (KCBS) inequality[22], is convenient for certification of random numbers. Violation of the KCBS inequality has been observed before in a single-photonic system[23]. For experimental test of the KCBS inequality, there are two possible loopholes: the detection efficiency loophole if the detectors only register a subset of data due to their inefficiency, and the compatibility loophole, which occurs if additional assumptions are required to guarantee that the observables with simultaneous assignment of values in the KCBS inequality are compatible with each other and remain identical when their measurement contexts change. The test of the KCBS inequality with the photonic system is immune to the compatibility loophole[23], however, it requires the fair-sampling assumption due to the low photon detection efficiency and thus subject to the detection efficiency loophole.

In our scheme, a random number generator certified by quantum contextuality with a single trapped ion allows us to close the detection efficiency loophole for the first time for the KCBS inequality. For the compatibility, we follow basically the same configurations as in Ref. 23, where errors in compatible measurement settings only reduce the amount of the violations. Even with experimental noise and imperfections, we get significant violations of the KCBS inequality, which lead to lower bounds the minimum entropy of the generated random string. Compared to the experimental certification based on the CHSH inequality[14], the generation rate of random numbers is increased by about four orders of magnitudes in our experiment, which is important for practical applications. Report of our experiment is organized as follows. First, we introduce the KCBS inequality and show the experimental violation of this inequality. Then, we introduce the relation between the violation of the KCBS inequality and the minimum entropy of the generated random string for the case of an honest provider, and compare the theoretical prediction with our experimental observation. The generated random bits are tested under uniform or biased choice of measurement settings. We conclude this chapter by summarizing the results and discussing further improvements of our random number generation scheme.

The Kochen-Specker theorem states that the results of quantum mechanics cannot

be fully explained by non-contextual classical theories which assume that the measurement outcomes of a physical system are predetermined and independent of their own and other simultaneous compatible measurements[20,21]. The KCBS inequality illustrates the conflict between quantum mechanics and non-contextual classical theory in the simplest possible system with the Hilbert space dimension $d=3$[22]. The KCBS inequality is connected with the following simple algebraic equation.

$$a_1a_2+a_2a_3+a_3a_4+a_4a_5+a_5a_1\geq -3, \qquad (2.1.1)$$

where the value of $a_i$ is either 1 or $-1$. If the values of the observables are predetermined, the average of the left hand of the above equation should be no less than $-3$, leading to the following inequality:

$$\langle \chi_{KCBS}\rangle=\langle A_1A_2\rangle+\langle A_2A_3\rangle+\langle A_3A_4\rangle+\langle A_4A_5\rangle+\langle A_5A_1\rangle\geq -3. \qquad (2.1.2)$$

## 2.2 Violation of the KCBS inequality

In quantum mechanics, however, the outcomes of $A_i$ do not have predetermined values, which allows violation of the KCBS inequality (2.1.2) for a specific state $|\psi_0\rangle$ in systems with $d\geq 3$. In the case of $d=3$, we denote the bases by $|1\rangle$, $|2\rangle$ and $|3\rangle$ and the observable $A_i$, represented by $A_i=1-2|v_i\rangle\langle v_i|$, is the projector on the axis $|v_i\rangle$. The maximal violation of the KCBS inequality (2.1.2) is achieved for the state along the symmetric axis of the pentagram shown in Figure 2.1(a). Here $|v_1\rangle=|1\rangle$, $|v_2\rangle=|2\rangle$, $|v_3\rangle=R_1(\gamma,0)|v_1\rangle$, $|v_4\rangle=R_2(\gamma,0)|v_2\rangle$, $|v_5\rangle=R_1(\gamma,0)|v_3\rangle$ and $|v_1\rangle=R_2(\gamma,0)|v_4\rangle$, where $\gamma=51.83^\circ$ and $R_{1,2}$ denote the rotation operations between $|1\rangle$ to $|3\rangle$ and between $|2\rangle$ to $|3\rangle$, respectively. Maximal violation the KCBS inequality is achieved under the state to $|\psi_0\rangle=\frac{1}{\sqrt[4]{5}}|1\rangle+\frac{1}{\sqrt[4]{5}}|2\rangle+\sqrt{1-\frac{2}{\sqrt{5}}}|3\rangle$, with the corresponding value $\langle \chi_{KCBS}\rangle=5-4\sqrt{5}\approx -3.944$.

Figure 2.1(b) shows the scheme for preparation of the initial state $|\psi_0\rangle$ starting from the basis state $|3\rangle$, and Figure 2.1(c)–(g) describe the implementation of the measurement configurations along the five axes. To ensure context independence, we emphasize that the measurement configuration of $A_i$ remains the same when it is measured with either $A_{i-1}$ or $A_{i+1}$ (let $A_0 \equiv A_5$, $A_6 \equiv A_1$). For example, the scheme for the measurement $A_2$ is exactly the same in the first [Figure 2.1(c)] and the second stage [Figure 2.1(d)]. To move to the second configuration, we perform a rotation between the states $|1\rangle$ and $|3\rangle$, which does not influence the state $|2\rangle$ that corresponds to the observable $A_2$. Only the observable related to the state $|1\rangle$ is changed from $A_1$ to $A_3$.

The configuration for the measurement of $A_1$ in Figure 2.1(c) is not the same as that in Figure 2.1(g), which is therefore denoted by $A_1'$. If $A_1$ and $A_1'$ are not identical, it is possible to violate the inequality (2.2.1) even in classical theory. To solve this problem, similarly to Ref. 23, we use a new inequality that includes the observable $A_1'$ with the form

$$\begin{aligned}\langle \chi_{KCBS} \rangle = &\langle A_1 A_2 \rangle + \langle A_2 A_3 \rangle + \langle A_3 A_4 \rangle + \langle A_4 A_5 \rangle + \\ &\langle A_5 A_1' \rangle + \left[1 - \langle A_1 A_1' \rangle\right] \geq -3 .\end{aligned} \tag{2.2.1}$$

Note that the inequality (2.2.1) becomes the original KCBS inequality (2.1.2) when $A_1 = A_1'$. Therefore, the difference between two measurements decrease the violation that can be obtained in the experiments[23]. Another possible way out is to introduce an empirical parameter to upper bounds the violation of compatibility, which would be similar in spirit to a recent work where a parameter is introduced to bound violation of the locality loophole for test of the Bell inequalities[28]. Any imperfection in the initial state preparation or final measurements only leads to a reduction of violation of the KCBS inequality, so a significant violation of this inequality guarantees that the randomness comes from the quantum origin instead of a classical noise process.

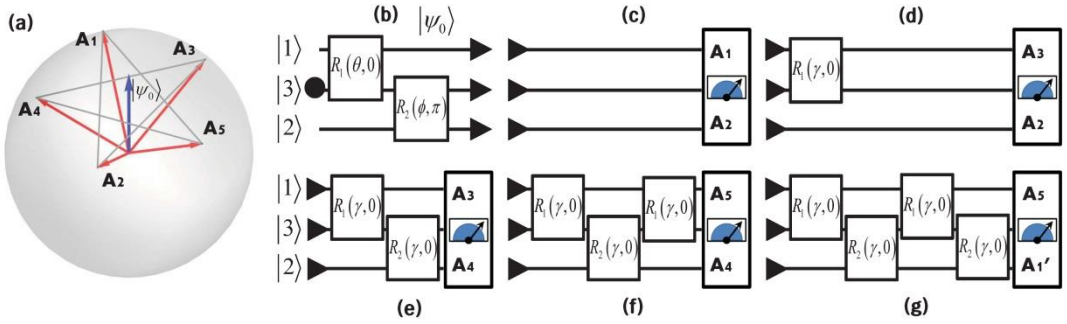



Figure 2.1 The representation in $3d$ space and pulse sequences of a state and measurement configurations for the maximal violation of the KCBS inequality (2.1.2). (a) The five vectors form a regular pentagram, which represent observables $A_1$, $A_2,\ldots,A_5$ that are the projectors on them. The vectors related to observables $A_i, A_{i+1}$ are orthogonal, which makes the neighboring observables compatible. The initial state $|\psi_0\rangle$ for the maximal violation is located at the center axis (blue arrow) of the pentagram. The initial state and measurements of the compatible observables are realized by the pulse sequences shown in (b) and (c)-(g). (b) The pulse sequence to prepare $|\psi_0\rangle=\frac{1}{\sqrt[4]{5}}|1\rangle+\frac{1}{\sqrt[4]{5}}|2\rangle+\sqrt{1-\frac{2}{\sqrt{5}}}|3\rangle$. Here, $R_1$ and $R_2$ represent the coherent rotations between $|1\rangle$ to $|3\rangle$ and between $|2\rangle$ to $|3\rangle$, respectively, where $\theta=$ 41.97。 and $\phi=64.09$。. The sequence starts from $|3\rangle$ state (black filled circle) after optical pumping. (c)–(g) The pulse sequences for the measurement configurations (c) $A_1A_2$, (d) $A_2A_3$, (e) $A_3A_4$, (f) $A_4A_5$, (g) $A_5A_1^{'}$, where $\gamma=$ 51.83。. The important aspect of the configuration is that the measurement scheme for $A_i$ is perfectly unchanged when it is measured with either $A_{i-1}$ or $A_{i+1}$ except $A_1$, similarly to the photon realization[23]. The pulse sequence for the confirmation of the identicalness between $A_1$ and $A_1^{'}$ is shown in Figure 2.2(d). For the random number generation, we choose one of the five configurations (c)–(g) based on software

random numbers.

The violation of the KCBS inequality have been observed with single photons[18,23], however, those experiments are subject to the detection efficiency loophole. Here, we present the experimental violation of the KCBS inequality in a single trapped ion. Because of the high detection efficiency for the trapped ion, we close the detection efficiency loophole for the first time for this inequality.

## 2.3 Random Number Generation

We perform the test of the KCBS inequalities (2.1.2) with a single trapped $^{171}Yb^{+}$ ion in a four-rod radio-frequency trap[26,29]. The qubit states are represented by the two internal levels in the $S_{1/2}$ ground state manifold, with $|F=1, m_F=0\rangle \equiv |\uparrow\rangle$ and $|F=0, m_F=0\rangle \equiv |\downarrow\rangle$.

The initial state preparation and the measurement configurations are shown in Figure 2.1(b)-(g), and they are realized by two microwaves with the frequencies $\omega_1$ and $\omega_2$, which produce Rabi oscillations $R_1(\theta_1,\phi_1)$ and $R_2(\theta_2,\phi_2)$ between $|1\rangle$ to $|2\rangle$ and between $|1\rangle$ to $|3\rangle$, respectively. Here, $\theta_{1,2}$ and $\phi_{1,2}$ are controlled by the duration and phase of the microwaves. $R_1(\theta_1,\phi_1)$ and $R_2(\theta_2,\phi_2)$ have the following explicit forms

$$R_1(\theta_1,\phi_1)=\begin{pmatrix} \cos\frac{\theta_1}{2} & 0 & -ie^{i(\phi_1+\frac{\pi}{2})}\sin\frac{\theta_1}{2} \\ 0 & 1 & 0 \\ -ie^{i(\phi_1+\frac{\pi}{2})}\sin\frac{\theta_1}{2} & 0 & \cos\frac{\theta_1}{2} \end{pmatrix},$$

$$R_2(\theta_2,\phi_2)=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\frac{\theta_2}{2} & -ie^{i(\phi_2+\frac{\pi}{2})}\sin\frac{\theta_2}{2} \\ 0 & -ie^{i(\phi_2+\frac{\pi}{2})}\sin\frac{\theta_2}{2} & \cos\frac{\theta_2}{2} \end{pmatrix}.$$

For experimental convenience, we transform the observable $A_1$ to $V_i=(1-A_i)/2$, which is assigned to value $v_i=0$ when photons are detected or $v_i=1$ when no photons are detected. With $V_i$, the KCBS inequality (2.2.1) is rewritten as

$$\left\langle \chi'_{KCBS} \right\rangle = 5 - 4\sum_{i=1}^{5}\langle V_i \rangle + 4\left( \sum_{i=1}^{4}\langle V_i V_{i+1} \rangle + \left\langle V_5 V_1' \right\rangle \right) + \left[ 4\langle V_1 \rangle - 4\left\langle V_1 V_1' \right\rangle \right] \geq -3 . \quad (2.3.1)$$

We obtain $\langle V_i \rangle$ by mapping the axis $v_i$ to the state $|3\rangle$ and then measuring the probability $P_{|3\rangle}(v_i = 1) = \langle V_i \rangle$ (Figure 2.2(b)). For simplicity, let $P_{|3\rangle} = P$. The correlation terms $\langle V_i V_{i+1} \rangle$ are obtained by sequential measurements depicted in Figure 2.2(c). First, we transfer $V_i$ on the state $|3\rangle$ and apply the standard fluorescence detection scheme. If we detect photons, the state should not be $|3\rangle$ and we assign $v_i = 0$ to the observable $V_i$, where the outcome of the correlation term $V_i V_j$ vanishes and no further measurements are needed. If we detect no photons, we assign $v_i = 1$ to the $V_i$. Then, we apply the swapping microwave $\pi$-pulse that converts $V_j$ to $|3\rangle$ before another round of fluorescence detection. If we observe photons, $v_j = 0$, and if no photons, $v_j = 1$. We assign the value 1 to $V_i V_j$ only when we detect no photons for both rounds of measurements. We obtain the average of the correlation term $\langle V_i V_j \rangle = P(v_i = v_{i+1} = 1)$ by repeating the same experimental sequence many times[26].

The expectation value $\left\langle V_1 V_1' \right\rangle$ is obtained by the scheme shown in Figure 2.2(d). If $V_1 = V_1'$ ideally, the correlation $\left\langle V_1 V_1' \right\rangle$ should be same to $\langle V_1 \rangle$ since $V_1$ is projection operator $V_1^2 = V_1$. The state $|1\rangle$ at the beginning of Figure 2.1(g) corresponds to the observable $V_1$, which is exactly the same configuration as in Figure 2.1(c). Therefore, if photons are detected $(v_1 = 0)$ or not detected $(v_1 = 1)$ at the place where $V_1$ would be measured, photons should be observed $(v_1' = 0)$ or not be observed $(v_1' = 1)$ for the $V_1'$ shown in Figure 2.2(d). After repeating the sequence of Figure 2.2(d), we acquire the probability that no photons are measured $(P(v_1 = v_1' = 1))$, which gives $\left\langle V_1 V_1' \right\rangle$ by definition.

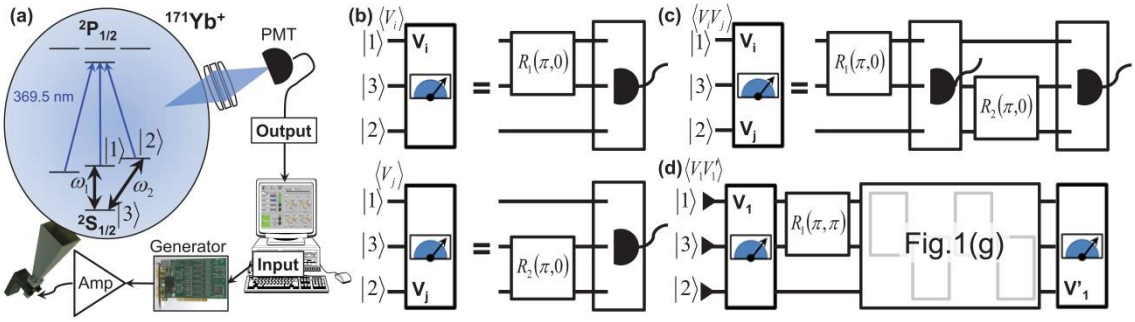



Figure 2.2 The trapped $^{171}Yb^+$ ion system and detection schemes. (a) The schematic diagram of trapped ion $^{171}Yb^+$ experimental setup for observing the violation of the KCBS inequality and for generating random numbers certified by the inequality. The three states $|F=1,m_F=0\rangle, |F=1,m_F=1\rangle$ and $|F=0,m_F=0\rangle$ in the $S_{1/2}$ ground state manifold are mapped onto $|1\rangle, |2\rangle$ and $|3\rangle$, respectively. One of the five measurement configurations in Figure 2.1(c)–(g) is chosen by the software generated random number and the pulse sequence of the chosen setting is transferred to the arbitrary waveform generator(AWG) and is applied to the ion through the amplifier. Depending on the photon counts on the photomultiplier tube(PMT), we assign values on the observables mapped on the state $|3\rangle$. (b) The detection schemes for obtaining results of single observables $V_i$, $V_j$. First, $V_i$ or $V_j$ is mapped to the state $|3\rangle$ and apply the standard fluorescent detection method. If we detect photons (no photons), we assign zero (one) on the observable $V_i$ or $V_j$. After repeating the same pulse sequence and the detection, we obtain the average value of the observable. (c) The sequential measurement scheme for the correlation $V_iV_j$. $V_iV_j$ has a value one when both of $V_i$ and $V_j$ have one, where no photons are detected at each stage. (d) The experimental confirmation of the identicalness of $V_1$ and $V_1^{'}$. Ideally, whenever $V_1$ has a result one (no photons), $V_1^{'}$ should have the same result (no photons). Any imperfection or changes in the system will cause the mismatch of them, which reduces the violation in the extended KCBS inequality (2.2.1).

We randomly choose one of the five configurations (c)–(g) of Figure 2.1 based on computer generated random numbers and perform the sequential measurements. We change the order of sequential measurements ($V_iV_{i+1}$ or $V_{i+1}V_i$) with equal probability. We occasionally check the overlap of $V_1$ and $V_1^{'}$. We repeat the sequences $1 \times 10^5$ times and observe $\langle \chi_{KCBS} \rangle = 3.852(0.030)$, which violates the extended KCBS inequality (2.2.1, 2.3.1) by $31\sigma$. The detailed results of the measurements are summarized in Table 2.1.

Table 2.1 Experimental results for each of five settings and five joint probabilities for the KCBS inequality

| Setting | $P_{\|3\rangle}$ | | | Correlations | | |
|---|---|---|---|---|---|---|
| | Term | Ideal | Result | Term | Ideal | Result |
| Fig 2.1(c) | $\langle V_1 \rangle$ | | 0.452(5) | $\langle V_1V_2 \rangle$ | | 0.014(1) |
| | $\langle V_2 \rangle$ | | 0.446(5) | $\langle V_2V_1 \rangle$ | | 0.015(1) |
| Fig 2.1(d) | $\langle V_2 \rangle$ | | 0.448(5) | $\langle V_2V_3 \rangle$ | | 0.016(1) |
| | $\langle V_3 \rangle$ | | 0.436(5) | $\langle V_3V_2 \rangle$ | | 0.017(1) |
| Fig 2.1(e) | $\langle V_3 \rangle$ | 0.447 | 0.428(5) | $\langle V_3V_4 \rangle$ | 0 | 0.014(1) |
| | $\langle V_4 \rangle$ | | 0.443(5) | $\langle V_4V_3 \rangle$ | | 0.016(1) |
| Fig 2.1(f) | $\langle V_4 \rangle$ | | 0.464(5) | $\langle V_4V_5 \rangle$ | | 0.015(1) |
| | $\langle V_5 \rangle$ | | 0.439(5) | $\langle V_5V_4 \rangle$ | | 0.014(1) |
| Fig 2.1(g) | $\langle V_5 \rangle$ | | 0.443(5) | $\langle V_5V_1 \rangle$ | | 0.017(1) |
| | $\langle V_1^{'} \rangle$ | | 0.431(5) | $\langle V_1^{'}V_2 \rangle$ | | 0.014(1) |
| Fig 2.2(d) | | | | $\langle V_1V_1^{'} \rangle$ | 0.447 | 0.451(5) |
| $\langle \chi_{KCBS}^{'} \rangle (= -\hat{L} = -3.944) = -3.852(30)$ | | | | | | |

We emphasize that our result of the violation cannot be explained by any non-

contextual classical theory which does not exploit the compatibility loophole (the detection loophole is closed in our experiment). In other words, any classical part of the system such as technical noise, imperfections and/or unexpected changes of control parameters cannot produce the violation. Therefore, as long as we observe the violation of the inequality, we can ensure that the outcomes of our measurements originate from quantum mechanics.

## 2.4 Minimum Entropy of Randomness

We establish the relation between violation of the KCBS inequality (2.1.2, 2.3.1) and randomness of the generated string from the experiment, similar to the photonic demonstration[18]. We focus on the scenario with an honest provider of the device[17] rather than the extreme adversary scenario where the device has been produced by a malicious manufacturer. Even though we trust the device provider, we still need to ensure that the randomness of the generated sequence is caused by quantum uncertainty instead of technical noise[17]. For this purpose, we assume: (1) the system can be described by quantum theory; (2) the input at $l$ th trial is chosen from a random process that is independent and uncorrelated from the system and its value is revealed to the system only at step $l$; (3) the outcomes of the corresponding pairs of measurements at step $l$ are compatible (the measurement of one observable does not influence on the marginal distribution of the results of the other observable); (4) the adversary does not have any capability of controlling the inside of the system. The first and the second assumptions here are identical to those made in the certification scheme of Bell's inequality[14]. The third is the contextuality assumption that replaces the role of locality assumption for the Bell inequality. The fourth is an assumption about the honest provider[17].

We consider five sets of measurement configurations $S=\{A_1A_2, A_2A_3, A_3A_4, A_4A_5, A_5A_1\}$, where $A_i$ is the observable with the output $a_i=\pm1$ and compatible with $A_{i-1}$ and $A_{i+1}$. We can rewrite the KCBS inequality (2.1.2) as

$$L\equiv\sum_{i=1}^{5}\sum_{a_i,a_j}\left[P(a_i=a_{i+1}\left|A_iA_{i+1}\right.)-P(a_i\neq a_{i+1}\left|A_iA_{i+1}\right.)\right]\leq 3, \qquad (2.4.1)$$

where $P(a_i=a_{i+1}\left|A_iA_{i+1}\right.)$ or $P(a_i\neq a_{i+1}\left|A_iA_{i+1}\right.)$ is the probability that the output results are the same or different for a chosen measurement setting $A_iA_{i+1}$. Note that we change the sign of the inequality to make the deviation similar to that in Refs. 14,17,30. In our

experiment, since we use the observable $V_i$ (result $v_i = 0,1$) instead of $A_i$ and only distinguish the event of $v_i = v_{i+1} = 1$ from others, the Eq. (2.4.1) is modified as

$$L \equiv 5 - 4\sum_{i=1}^{5} P(v_i = 1|V_i) - \left\{ 4\sum_{i=1}^{5} P(v_i = v_{i+1} = 1|V_i V_{i+1}) \right\} \le 3, \qquad (2.4.2)$$

where $P(v_i = 1|V_i)$ is the probability that the output result $v_i$ is 1 at a measurement setting $V_i$. The result of terms inside $\{\cdots\}$ is ideally zero and non-zero positive value can be occurred by experimental errors or imperfections, which only reduces the amount of violation from the optimal. Therefore, we can conclude that the experimental violations of the inequality (2.4.2) arise from solely quantum mechanical origin not any classical mean.

In our realization, we estimate the violation of the inequality (2.4.2) by repeating the sequences $n$ times and additional runs $n_{cc}$ of the compatibility check, the measurement setting $V_1 V_1^{'}$. The estimation $\hat{L}$ of Eq. (2.4.1), obtained from the experimental data, is written as

$$\begin{aligned} \hat{L} \equiv & 5 - \frac{4}{n}\sum_{i=1}^{5} \frac{N(v_i = 1|V_i)}{P(V_i)} \\ & - \left\{ \frac{4}{n}\sum_{i=1}^{4} \frac{N(v_i = v_{i+1} = 1|V_i V_{i+1})}{P(V_i V_{i+1})} + \frac{N(v_5 = v_1^{'} = 1|V_5 V_1^{'})}{P(V_5 V_1^{'})} \right\}, \\ & - \left[ \frac{4N(v_1 = 1|V_1)}{nP(V_1)} + \frac{4N(v_1 = v_1^{'} = 1|V_1 V_1^{'})}{n_{cc}} \right] \end{aligned} \qquad (2.4.3)$$

where $N(v_i = 1|V_i)$ or $N(v_i = v_{i+1} = 1|V_i V_{i+1})$ is the number of times that the outcome $v_i$ or $v_i$ and $v_{i+1}$ is one under a measurement setting $V_i$ or $V_i$ and $V_{i+1}$, respectively. $P(V_i)$ or $P(V_i V_{i+1})$ is the probability with which a measurement configuration $V_i$ or $V_i$ and $V_{i+1}$ is chosen. Note that positive result of terms inside $\{\cdots\}$ and $[\cdots]$ originates from the experimental flaws, which only reduces the amount of violation.

The randomness of a single generated bit $v_i$ from a measurement setting $V_i$ can be characterized by the min-entropy $H_\infty(v_i|V_i) = -\log_2\left[\max_{v_i} P(v_i|V_i)\right]$, where

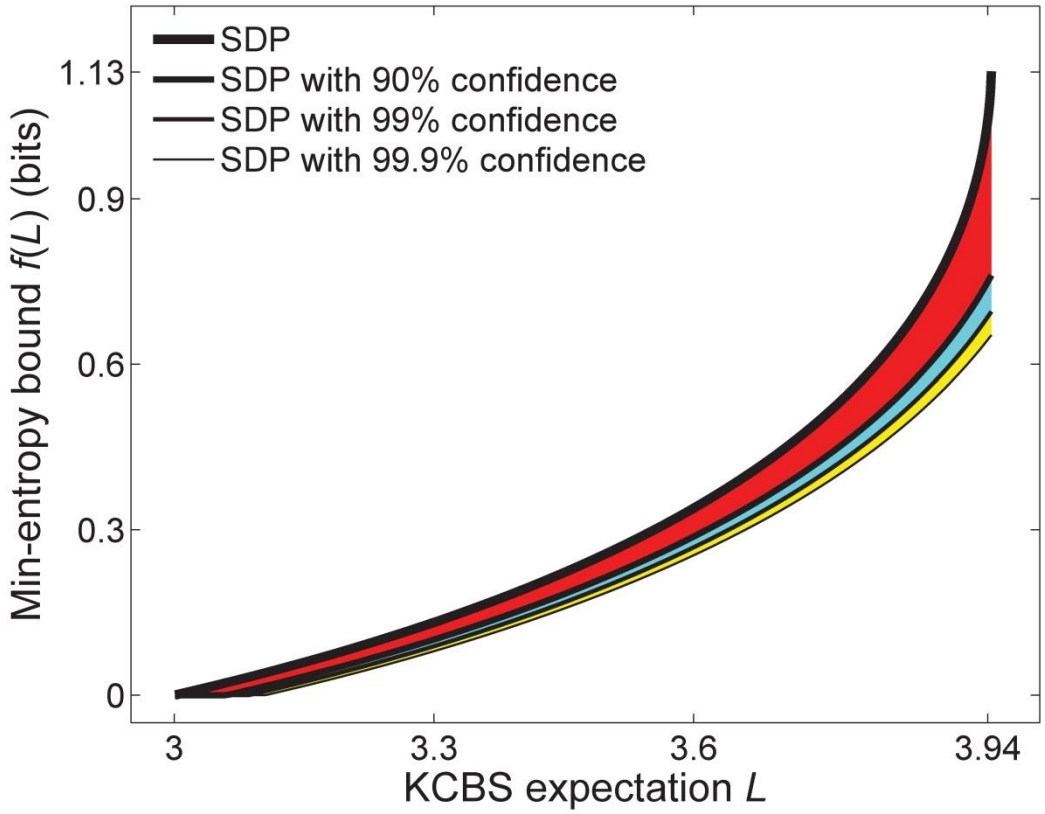



Figure 2.3 The min-entropy vs. the violation. The function $f(L)$ in Eq. (2.4.4) depending on the violation $L$ of the KCBS inequality (2.4.1), which is calculated by semi-definite programming (SDP). The function $f(L-\delta)$ at various confidence levels $(1-\delta')$ such as 90%, 99% and 99.9% are plotted for the uniform choices of measurement configurations, where $?\equiv(\ _{m_{max}}+1/r)\sqrt{-2\ln\delta'/n}$ and $r=\min_i P(A_iA_{i+1})=1/5$. Here we divide interval with the spacing $L_m-L_{m-1}=(L_{m_{max}}-3)/10(=0.0944)$. Given a measured $\hat{L}$ and confidence level, we can estimate the min-entropy of a generated random string as summarized in Eq. (2.4.4). Note that we ignore the term $\log_2\delta$ in Eq. (2.4.4) that does not have dependence on the trial $n$.

$P(v_i|V_i)$ is the conditional probability of obtaining $v_i$ when the input setting $V_i$ and the maximum is taken over all possible values of the output string. The theorem 1 of Ref. 17 shows that the min-entropy of the generated string after $n$ trials is bounded by

$$H_\infty(\mathrm{v}|\mathrm{V},m) \geq nf(\mathrm{L}_m - ?) + \log_2 \delta, \qquad (2.4.4)$$

where $\mathrm{L}_m (m = 0,1,...,m_{max})$ is a series of KCBS violation thresholds with $\mathrm{L}_0 = 3$ the classical bound, and $\mathrm{L}_{m_{max}} = 4\sqrt{5} - 5$ the maximum violation, and $?\equiv(\ _{m_{max}} + 1/r)\sqrt{-2\ln \dot{o}'/n}$ , with $r$ the smallest probability of input choices $\min_i P(V_i)$. The parameter $\epsilon'$ denotes the closeness between the resulting distribution that characterizes $k$ successive uses of the device and another extended distribution that is well defined mathematically. $f$ is found as a lower bound on the min-entropy of the joint probability $P(\mathrm{v}_i\mathrm{v}_j|\mathrm{V}_i\mathrm{V}_j) = \{P(v_i v_j|V_i V_j)\}$ which establishes a relation between quantum contextuality and randomness of the measurement outcomes of our quantum system. According to the discussion in Ref. 14, the joint probability $P(\mathrm{v}_i\mathrm{v}_j|\mathrm{V}_i\mathrm{V}_j)$ is a quantum realization if $P(v_i v_j|V_i V_j) = \mathrm{Tr}(\rho O_{A_i}^{a_i} O_{A_j}^{a_j})$ on a state $\rho$ and observables $O = \{O_{A_i}^{a_i}\}(i = 1,2,3,4,5)$ where $O_{A_i}^{a_i}$ is a projector that projects the state onto an eigenstate of measurement $A_i$ with eigenvalue $a_i$. We want to obtain the lower bound on the min-entropy of the output randomness for a given violation $\hat{L}$:

$$H_\infty(\mathrm{v}_i\mathrm{v}_j|\mathrm{V}_i\mathrm{V}_j) = -\log_2\left[\max_{v_i v_j} P(v_i v_j|V_i V_j)\right] \geq f(\hat{L}), \qquad (2.4.5)$$

which is equivalent to solving the following optimization problem:

$$\begin{aligned} &\max \quad P(v_i v_j|V_i V_j) \\ &\text{subject to} \sum_{(i,j)\in S}\left[P(v_i \neq v_j|V_i V_j) - P(v_i = v_j|V_i V_j)\right] = \hat{L}, \\ &\qquad P(v_i v_j|V_i V_j) = \mathrm{Tr}(\rho O_{A_i}^{a_i} O_{A_j}^{a_j}) \end{aligned} \qquad (2.4.6)$$

where the optimization is carried over all quantum realization $\{\rho, O, P\}$. The solution $P^*(v_i v_j | V_i V_j)$ of the above problem gives the minimal value of entropy $H_\infty(\mathrm{v_i v_j}|\mathrm{V_i V_j}) = -\log_2 P^*(v_i v_j | V_i V_j)$ consistent with the quantum theory and the KCBS violation $\hat{L}$. To obtain a lower bound on the min-entropy as a function of $\hat{L}$ which is independent of the input pair $(V_i V_j)$, it is sufficient to solve (2.4.6) for all input and output pairs $(V_i V_j)$ and $(v_i v_j)$.

Using to the technique introduced in Refs. 56,57, the above optimization problem can be effectively solved by casting it to a semi-definite programs (SDP) problem. For the set of operators $O = \{I, \langle v_1\rangle, \langle v_2\rangle, \langle v_3\rangle, \langle v_4\rangle, \langle v_5\rangle\}$, theoretically from the setting of the pentagram we have $\langle v_1 v_2\rangle = \langle v_2 v_3\rangle = \langle v_3 v_4\rangle = \langle v_4 v_5\rangle = \langle v_1 v_5\rangle = 0$, thus the set of operators changes to $O = \{I, (5-\hat{L})/4 - \langle v_2\rangle - \langle v_3\rangle - \langle v_4\rangle - \langle v_5\rangle, \langle v_2\rangle, \langle v_3\rangle, \langle v_4\rangle, \langle v_5\rangle\}$. Now we only need to solve the SDP problem over all symmetric 6×6 positive semi-definite matrices $\Gamma$ with $c = \{1\ 0\ ...\ 0\}$ and vector $y = \{y_1\ y_2\ ...\ y_9\}^T = \{\langle v_2\rangle\ \langle v_3\rangle\ \langle v_4\rangle\ \langle v_5\rangle\ \langle v_1 v_3\rangle\ \langle v_1 v_4\rangle\ \langle v_2 v_4\rangle\ \langle v_2 v_5\rangle\ \langle v_3 v_5\rangle\}^T$ :

$$\begin{array}{ll} \max & c^T y_1 \\ \text{subject to} & \Gamma\, \mathrm{f} = 0 \end{array}, \qquad (2.4.7)$$

with the form

$$\Gamma = \begin{pmatrix} 1 & (5-\hat{L})/4 - \langle v_2\rangle - \langle v_3\rangle - \langle v_4\rangle - \langle v_5\rangle & \langle v_2\rangle & \langle v_3\rangle & \langle v_4\rangle & \langle v_5\rangle \\ & 1 & 0 & \langle v_1 v_3\rangle & \langle v_1 v_4\rangle & 0 \\ & & 1 & 0 & \langle v_2 v_4\rangle & \langle v_2 v_5\rangle \\ & & & 1 & 0 & \langle v_3 v_5\rangle \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix}. \qquad (2.4.8)$$

Here only the upper triangular part of $\Gamma$ is given since it is symmetric. This SDP problem is solved using the matlab toolbox SeDuMi[58]. $f(\hat{L})$ equals zero at the

classical point $\hat{L}=3$ and increases monotonously as $\hat{L}$ increases. For the maximal violation $\hat{L}=4\sqrt{5}-5$, we get $P^*=0.457$, corresponding to approximately $f(\hat{L})=1.13$ bits. Figure 2.3 presents how the min-entropies are affected by the confidence levels, $1-\epsilon'$ and $1-\delta$. When we set a high confidence level, $1-\epsilon'$, the bound on the min-entropy reduces as expected. Note that the certified min-entropy is only determined by measured value $\hat{L}$ and the choice of $\epsilon'$, independent of experimental details.

## 2.5 Experimental Setup

For a single trapped $^{171}Yb^{+}$ ion in a four-rod radio-frequency trap[26,29], the qubit states are represented by the two internal levels in the $S_{1/2}$ ground state manifold, with $|F=1, m_F=0\rangle \equiv |\uparrow\rangle$ and $|F=0, m_F=0\rangle \equiv |\downarrow\rangle$(shown in blue in Figure 2.4(b)). The transition frequency between $|\uparrow\rangle$ to $|\downarrow\rangle$ is $\omega_{HF}=(2\pi)\,12642.821$ MHz, determined by the hyperfine interaction. These two states form a qutrit with $|F=1, m_F=1\rangle$. In detail, $|F=1, m_F=0\rangle$, $|F=1, m_F=1\rangle$ and $|F=0, m_F=0\rangle$ are mapped onto $|1\rangle$, $|2\rangle$ and $|3\rangle$, the energy levels of qutrit are shown in Figure 2.4(b).

Laser system for a $^{171}Yb^{+}$ ion consists of 369 nm, 399 nm, 638 nm, 935 nm lasers. To load a $^{171}Yb^{+}$ ion, we first heat up the $^{171}Yb$ oven in the trap so that the $^{171}Yb$ atoms pump out. A 399 nm laser beam excites them from $1S_0$ to $1P_1$ then ionized by a strong 369 nm laser beam.

The experimental procedure consists of Doppler cooling, initialization, coherent operations and detection. The frequency stabilized 369 nm laser is split into several beams to be used for Doppler cooling, initialization and detection by applying sidebands of different frequencies.

Doppler cooling happens on $2S_{1/2}-2P_{1/2}$ at wavelength 369.5 nm. $2S_{1/2}$ and $2P_{1/2}$, Both 12.643 GHz and 2.105 GHz are necessary in order to cover all the hyperfine states of $2S_{1/2}$ and $2P_{1/2}$, thus an Electro Optic Modulator (EOM) at 7.37 GHz is used to generate 14.74 GHz modulation by its second order sideband.

Initialization to the $|\downarrow\rangle$ state is realized by optical pumping that excites transition

between $2S_{1/2}\left|F=1,m_F=0\right\rangle \leftrightarrow 2P_{1/2}\left|F=1,m_F=0,1,-1\right\rangle$, where the latter states

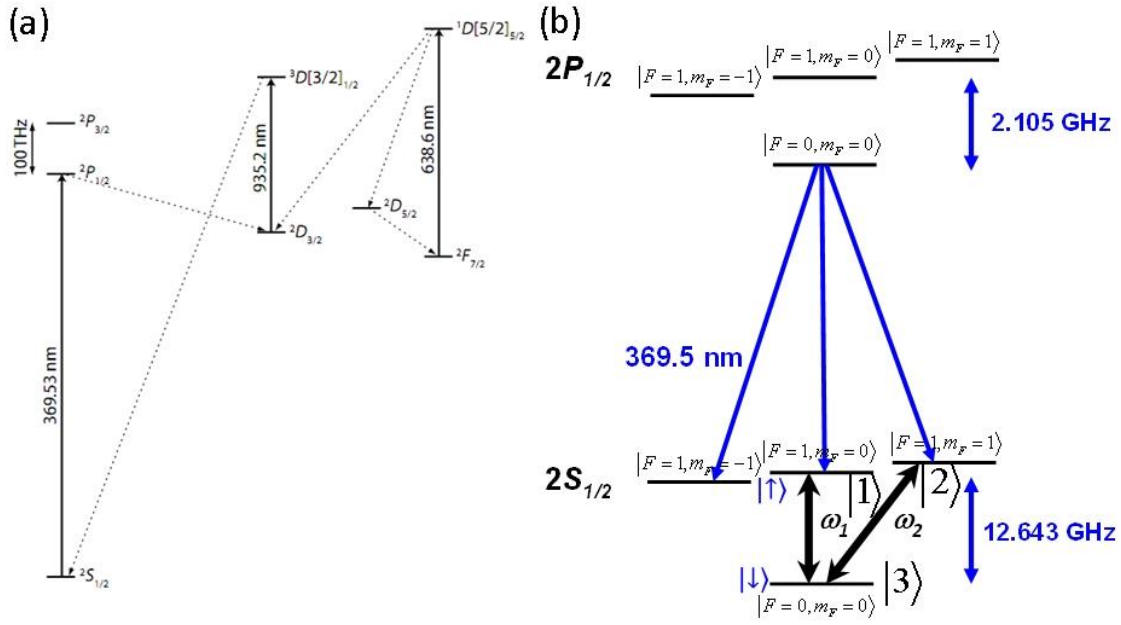



Figure 2.4 Energy state of a $^{171}Yb^{+}$ ion. (a) The usages of 369 nm, 638 nm and 935 nm lasers. (b) Qubit(blue) and qutrit(black) setting of a $^{171}Yb^{+}$ ion. Detection covers $2S_{1/2}\left|F=1,m_F=0\right\rangle \leftrightarrow 2P_{1/2}\left|F=0,m_F=0\right\rangle$ without any modulation because $2P_{1/2}\left|F=0,m_F=0\right\rangle$ decays to the $2S_{1/2}\left|F=1,m_F=0,1,-1\right\rangle$ states as the blue arrows. Doppler cooling covers both 12.643 GHz and 2.105 GHz, optical pumping covers 2.105 GHz. $\omega_1$ and $\omega_2$ are resonant to the transitions between $\left|1\right\rangle$ and $\left|3\right\rangle$, and between $\left|2\right\rangle$ and $\left|3\right\rangle$

decay into the $|\downarrow\rangle$ state from where ion is hard to scatter because of hyperfine splitting. This procedure is implemented by adding 2.105 GHz sideband through another EOM.

Detection beam only need to cover the transition between $2S_{1/2}|F=1,m_F=0\rangle \leftrightarrow 2P_{1/2}|F=0,m_F=0\rangle$ because ion at $2P_{1/2}|F=0,m_F=0\rangle$ state only decays to one of the $2S_{1/2}|F=1,m_F=0,1,-1\rangle$ states and transition to $|\downarrow\rangle$ state is forbidden. Thus, no modulation is required for detection procedure.

The other two lasers of 935 nm and 638 nm bring the ion back to state $2S_{1/2}$ from metastable states $2D_{3/2}$ and $2F_{7/2}$ respectively as Figure 2.4(a) shows.

After 1 ms Doppler cooling, the internal state of the ion is initialized to $|3\rangle$ by 3 $\mu$s standard optical pumping with efficiency 99.1%[26]. The states are coherently manipulated by the microwaves $\omega_1$ and $\omega_2$ that are resonant to the transitions between $|1\rangle$ and $|3\rangle$, and between $|2\rangle$ and $|3\rangle$ (Figure 2.4(b)). The quantum operations of the microwaves $\omega_1$ and $\omega_2$ are described by the rotation matrix $R_1(\theta_1,\phi_1)$ and $R_2(\theta_2,\phi_2)$, respectively. Here $\theta_1,\theta_2$ and $\phi_1,\phi_2$ are controlled by the duration and the phase of the applied microwaves through an amplifying horn as shown in Figure 2.5. The $2\pi$ times for both Rabi oscillations are adjusted to 29.5 $\mu$s, that is $\Omega_{1,2}=(2\pi)$ 33.9 kHz in frequency. The maximum probability of off-resonant excitation $\Omega^2/(\omega_2-\omega_1)^2$ is about $1.6 \times 10^{-5}$, small enough to ensure independence of each Rabi oscillation. The standard fluorescent-detection method enables us to differentiate between one state versus the other two states of a qutrit. We observe on average 10 photons at 369.5 nm for the $|1\rangle$ or the $|2\rangle$ state and detect no photon for the $|3\rangle$ state. The state detection error rates for wrongly registering the state $|3\rangle$ and missing the state $|3\rangle$ are 0.9% and 1.9%, respectively, with the discrimination threshold $n_{ph}=1$. As shown in Figure 2.2(b), we transfer the information of observable

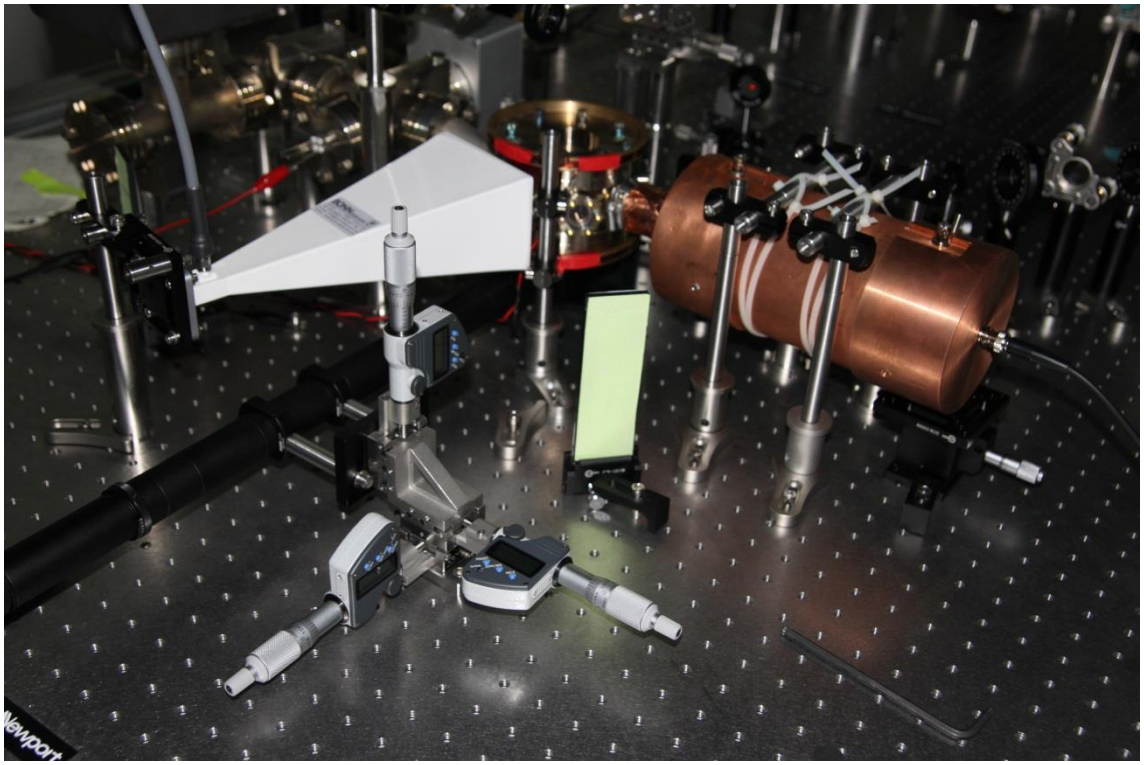


Figure 2.5 Photo of the microwave horn applying to the trap. The microwave horn is almost attached to trap, applying the amplified microwave signal through the viewport and providing operation to the trapped ion.

$A_i(A_j)$ by $\pi$-pulse and apply the measurement sequence. Then we assign the value $a_i = 1$ ($a_j = 1$) on the observable $A_i(A_j)$ when photons detected or $a_i = -1$ ($a_j = -1$) when no photons are detected. After repeating the same experimental procedures, we obtain the $\langle A_i \rangle$ ($\langle A_i \rangle$). Here we emphasize that our setup is not subject to detection loophole and provide a value of the measurement at every trial.

## 2.6 Experimental Result

We perform hundred thousand trials to generate random bits as described in the previous section. At each trial, we choose one of the five measurement configurations shown in Figure 2.1(c)–(g) by computer-generated random numbers, perform the sequence composed of Doppler cooling, state initialization and rotations for the chosen

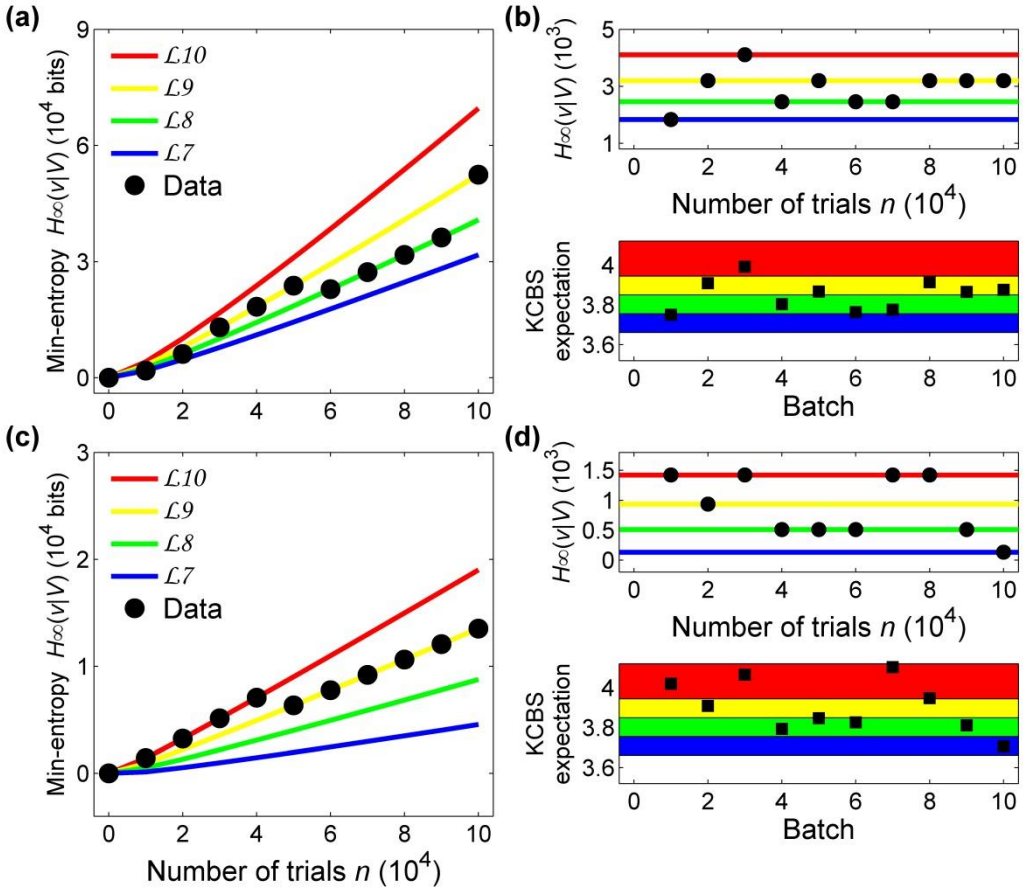



Figure 2.6 Comparison between theory and experimental results. (a)(c)The min-entropy $H_\infty(\mathrm{v}|\mathrm{V})$ (2.4.4) depending on the number of trials for (a) an uniform distribution of measurement settings $P(V_i)=1/5$ and (c) a biased distribution with $P(V_1)=1-4q$, $P(V_2)=P(V_3)=P(V_4)=P(V_5)=q$, and $q=6(100000)^{-1/2}$ with the probability of errors $\epsilon'$=0.01 and $\delta$=0.001. The min-entropies $H_\infty(\mathrm{a}|\mathrm{A})$ are bounded by the relation of the violation $\hat{L}$ of the KCBS inequality (2.4.4), where we set the 10 intervals of $\hat{L}$ between $\mathrm{L}_0$ and $\mathrm{L}_{m_{max}}$. The min-entropies are linearly increasing as the number of trial increases and the slopes are basically dependent on the thresholds of the intervals $\mathrm{L}_7$=3.6610 (blue), $\mathrm{L}_8$=3.7554 (green), $\mathrm{L}_9$=3.8496 (yellow), and $\mathrm{L}_{10}(\mathrm{L}_{m_{max}})$=3.944 (red). The black dots are obtained from the violation

values that were observed at the number of trials. (b)(d) The correlation between the KCBS violations (2.4.4) and the min-entropy (2.4.4) of the strings for (b) the uniform input choices and (d) the biased settings. Here we divide the total $1 \times 10^5$ numbers by 10 division and show the KCBS violations $\hat{L}$ and min-entropies in the division. We can clearly show that the monitor of $\hat{L}$ at each division provides sufficient information to guarantee the min-entropy in the division.

configuration and finally record the existence of fluorescence. As explained, we obtain a random bit, *i.e.*, 1 (or 0) with fluorescence (or no fluorescence) for each trial. The sequence takes about 10 ms, mainly limited by the wave-form loading time to the pulse generator. Note that the random generator based on the CHSH inequality produced a random bit per several minutes.

Figure 2.6 shows the min-entropies of generated strings. We produce a string of length $1\times10^5$ with uniform choices of the measurement settings, $P(V_i)=1/5$. As shown in Table 2.1, we observe the expectation $\hat{L}=3.852\pm0.030$, implying the min-entropy $H_\infty^{uni}(\mathrm{v}|\mathrm{V})>5.24\times10^4$ with 99% confidence. Note that the other confidence level $\delta$ does not have any noticeable influence on the bound of min-entropy. Here we used the thresholds of KCBS violations $\mathrm{L}_9=3.8496\left(=\frac{9}{10}(\mathrm{L}_{m_{max}}-3)\right)$.

Figure 2.6 shows clearly the advantage of our certification scheme, *i.e.*, we can guarantee the min-entropy of the generated random string by only monitoring the violation $\hat{L}$ independent of experimental details. Figure 2.6(a) shows the accumulated behavior of the min-entropy as the number of experimental trials $n$ increases. The solid lines show the theoretical linear increment of the min-entropies and the slopes are determined by only the thresholds $\mathrm{L}_m$. Due to drifts of experimental parameters, the violations $\hat{L}$ are fluctuating from one threshold to another, which accordingly introduces the changes to the min-entropy, accordingly. Figure 2.6(b) shows details of

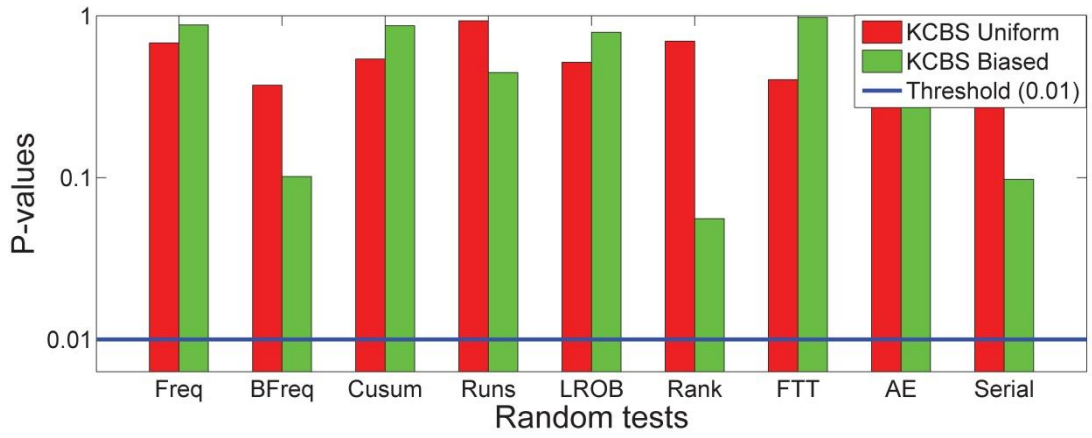



Figure 2.7 The results for random tests. The summary for the results of random tests[31] on our generated random numbers. In the tests, we can consider the sequences as random if *P–values* of the tests are over the threshold that we set, 0.01. All of random numbers pass the listed tests.

the transient behavior of the generated random string. We monitor the violation $\hat{L}$ for each batch of $n = 1\times10^4$ trials and estimate the min-entropy in the batch. Figure 2.6(b) reveals that the min-entropies are correlated to the violations $\hat{L}$ and completely determined by the thresholds $\mathrm{L}_m$ at given confidence level 99%. Here, we do not need massive random tests to ensure the amount actual random number in the generated string. The amount of min-entropy of our random numbers is guaranteed by the measured violation $\hat{L}$, regardless of unexpected changes of experimental parameters.

We also generate random bits with a biased choice of measurement settings, where $P(V_1) = 1-4q$, $P(V_2) = P(V_3) = P(V_4) = P(V_5) = q$, and $q = \alpha n^{-1/2}$ with $\alpha = 6$ and $n = 10^5$. We observe basically the same behavior of the min-entropy for the generated string except for a slightly smaller bound due to the non-uniform setting. We get the min-entropy bound $H_\infty^{bia}(\mathrm{v}|\mathrm{V}) > 1.4\times10^4$ from $1\times10^5$ rounds with violation of $\hat{L} = 3.901$. For the biased choice of measurement settings, the output entropy ($1.35\times10^4$) exceeds the input entropy ($1.14\times10^4$), and we obtain $2.1\times10^3$ net random bits. For the case of uniform

measurement settings, we always need more initial randomness and thus cannot obtain net randomness. This is similar to the random number generation scheme with the CHSH inequality, where to generate net randomness, one always needs to consider non-uniform measurement settings.

Finally, we carry out a series of random tests[31] to examine the quality of our random numbers obtained by collecting the outcomes of the first measurement in each trial. We apply the random tests that are appropriate for the size of our random numbers, which are 'Frequency', 'Block Frequency', Cumulative Sums (Cusums)', 'Runs', 'Longest-Run-of-Ones in a Block (LROB)', 'Rank', 'Discrete Fourier Transform Test (FTT)', 'Approximate Entropy (AE), 'Serial' The *p*-values of all the tests, which are the probabilities that an ideal random number generator would produce less random sequence than the tested one. Therefore, a *p*-value of 0 simply means that the tested sequence appears to be completely non-random, whereas a *p*-value of 1 implies that the sequence in test appears to be perfectly random. The *p*-value lies in the open interval (0,1) and if *p*-value is larger than a significance level $\theta$, we accept the sequence as random for the test. Typically $\theta$ is chosen to be in the range [0.0001, 0.01] and we set $\theta$=0.01. Note that we use Von-Neumann extractor for the output strings to make uniform distributions, which reduces the size of random numbers to one quarter. We also note that the random tests are different from guaranteeing the amount of min-entropy in the generated string. In other words, even the data could not pass the random tests but still have the quoted min-entropy.

Figure 2.7 shows the summary of the test results. Actually the real randomness of our generated strings is already certified by the KCBS inequality, which is a much stronger statement than claiming that the produced numbers pass all the random tests, since no random tests on finite strings should be considered complete.

## 2.7 Extension for Loophole Free Experiment

Our scheme of sequential measurement invented an effective way to distinguish the probability of $\langle V_i V_j \rangle = 1$ with $\langle V_i V_j \rangle = 0$ by defining $v_i = 0$ if we detect the

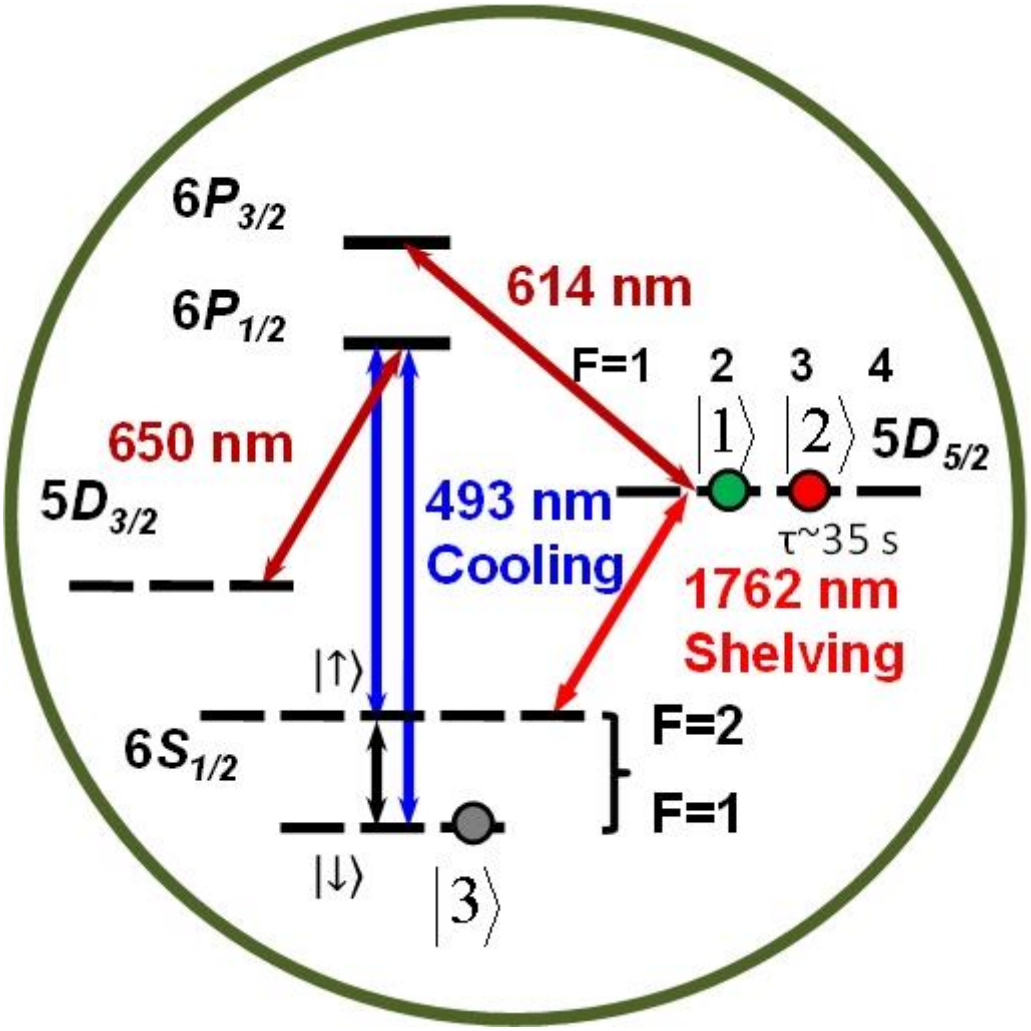



Figure 2.8 Energy state of a $^{137}Ba^{+}$ ion. It has a stable shelving state at $5D_{5/2}$ state with a 1762 nm narrow band laser. When the ion is at this shelving state, it does not fluoresce when illuminated with the cooling lasers of 493 nm thus provide clear detection. Ion can be excited out of the dark shelving state and begin a new run with a 614 nm laser. A repump laser at 650 nm excites the ion out of the $5D_{3/2}$ state. Both hyperfine states and Zeeman sublevels (not shown in the figure) of $5D_{5/2}$ state and $6S_{1/2}$ state can be used as a qutrit. The example shown here uses two hyperfine states of $5D_{3/2}$ state and $6S_{1/2}\left|F=0,m_F=0\right\rangle$ to form a qutrit.

photon and $v_i = 1$ if no photon is detected. However, the detection of the ion breaks the dark state, in this case, second detection of $V_j$ is not meaningful anymore at all, which implies our current system cannot distinguish the results of $\langle V_i = 0, V_j = 0 \rangle$ and $\langle V_i = 0, V_j = 1 \rangle$. Although it is enough for experimentally certifying random numbers, the compatibility loophole still left open in the theory.

A perfect solution as well as the next step of improving our experiment system is trapping a Barium ion. For a $^{137}Ba^{+}$ ion, the hyperfine states of the metastable $5D_{5/2}$ state with 35 s lifetime provide direct shelving from the ground state. This highly efficient and robust shelving process can be accomplished by using a 1762 nm narrow band laser with adiabatic passage technique[48,49]. The detection of this shelving event is reliable since the ion remains dark and does not fluoresce when illuminated with the cooling lasers at this "shelved" state, it is obvious to clarify the "dark" and "bright" state. When we use the hyperfine states and Zeeman levels of the $6S_{1/2}$ state as qutrit similar to a $^{171}Yb^{+}$ ion, the information can be fully transferred and detected in the $5D_{5/2}$ state. Furthermore, multiple hyperfine states and Zeeman levels of the $5D_{5/2}$ state itself are also strong candidates for forming a qutrit with the $6S_{1/2}$ state, like one of the examples shown in Figure 2.8. Both schemes can fully close the compatibility loophole, lead to a totally loophole free random number generator!

After realizing Barium ion trapping, we plan to develop hybrid trapping technique to invent an even stronger random number generator. To accomplish this, we may first realize sub-Doppler cooling to lower temperature than Doppler cooling with independent trapping of Barium ion. By co-trapping two species of ion in the same trap with the scheme in Figure 2.9, we can take advantage of both easy and clear hyperfine structure of $^{171}Yb^{+}$ as well as stable shelving of $^{137}Ba^{+}$ or $^{138}Ba^{+}$ ion. Although two different species of ions are trapped in one trap, they have independent detection setting, which will lead to simultaneous detection of both ions' information at the same time thus implement perfect sequential measurement. In this way, our generated random numbers will be much more secure and effective both theoretically and practically.

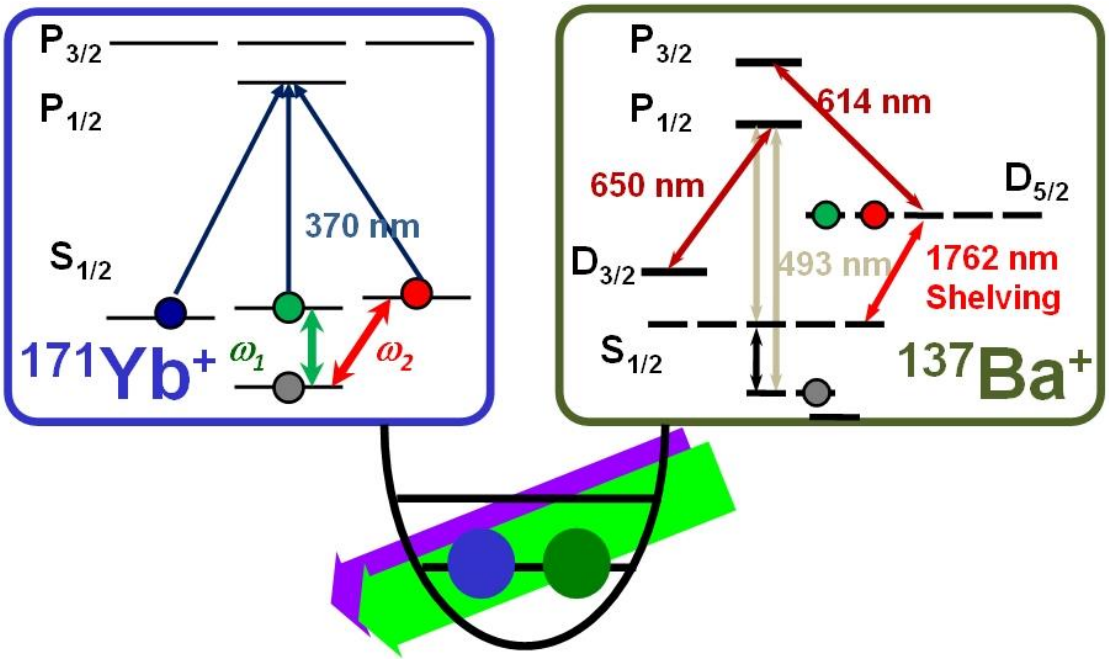



Figure 2.9 Hybrid trapping of a $^{171}Yb^{+}$ ion and a $^{137}Ba^{+}$ ion. These two species of ions can be trapped in the same trap and implement perfect sequential measurement.

# Chapter 3 Phonon Shift Operation

## 3.1 Motional Structure of an Ion

In our system, a single atomic $^{171}Yb^{+}$ ion is confined in a harmonic potential generated by radio frequency in the radial axis and dc-voltage in the axial direction. This harmonic oscillator potential is used as a quantum databus for transferring and processing information between multiple ions. By using an external coherent laser light, the internal electronic levels can be coupled to each other and the external motional degrees of freedom of the ions. Light is able to influence motion of the ion during an emission or absorption because of the momentum transfer between the ion and a photon. Controlling the ion motion becomes available by controlling the atom-photon coupling since the light field can act as a source of energy. In our case, the internal state of the ion, which is simply represented by a two-level subsystem, stores the quantum information. When we tune the laser mode close to the transition of this two-level ion with ground state $|\downarrow\rangle$ and excited state $|\uparrow\rangle$, this accurate interaction between light and the electronic structure of the ion can be transferred to the state of motion, thus the motion of two or more ions in the same potential realizes the "databus" to exchange information.

The motion of the ion can be approximated by a harmonic oscillator

$$\hat{H}^{(m)} = \frac{\hat{P}^2}{2M} + \frac{1}{2} M \omega_X^2 \hat{X}^2, \qquad (3.1.1)$$

where M is the mass of the ion, $\omega_X$ is the trap frequency along the radial direction X-axis which comes from confinement of the transverse mode. The transverse COM modes oscillate the ion at two different motional modes $\omega_X = .(2\pi)$ 2.8 MHz and $\omega_Y = .(2\pi)$ 3.18 MHz. The frequency difference of these two modes is 380 KHz, which is enough for getting rid of mutual effect. We achieved this amount by adding 10.6 V DC voltage to the two ground electrodes of the four rods in Figure 1.2(c). In our experiment, we only care the inner mode $\omega_X$. $\hat{X}$ and $\hat{P}$ are position and momentum operators. The framework of this quantum system is defined by its eigenstates $|n\rangle_M$, $n = 0,1,...$ with

eigenenergies $E_n = \hbar\omega_X (n+1/2)$. The energy quantum of this system is called a phonon for vibrational quanta. The motion of the ion in the harmonic potential is quantized using the creation and annihilation operators

$$\hat{a}^{\dagger} = \sqrt{\frac{M\omega_X}{2\hbar}}\hat{X} + \frac{i}{\sqrt{2M\hbar\omega_X}}\hat{P}, \qquad (3.1.2)$$

$$\hat{a} = \sqrt{\frac{M\omega_X}{2\hbar}}\hat{X} - \frac{i}{\sqrt{2M\hbar\omega_X}}\hat{P}, \qquad (3.1.3)$$

for all $n \geq 0$, we have the usual ladder algebra

$$\hat{a}^{\dagger}|n\rangle_M = \sqrt{n+1}|n+1\rangle_M, \quad \hat{a}|n\rangle_M = \sqrt{n}|n-1\rangle_M, \qquad (3.1.4)$$

but $\hat{a}|0\rangle_M = |0\rangle_M$. The Hamiltonian is then given by

$$\hat{H}^{(m)} = \hbar\omega_X (\hat{a}^{\dagger}\hat{a} + \frac{1}{2}). \qquad (3.1.5)$$

## 3.2 Stimulated Raman Transition

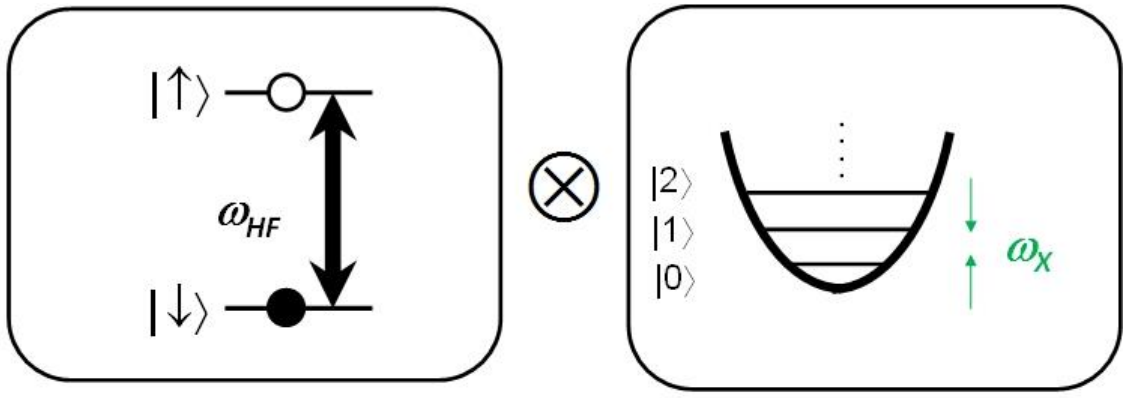
The total Hamiltonian of the system can be written now as[51,52]

$$\hat{H} = \hat{H}^{(e)} + \hat{H}^{(m)} + \hat{H}^{(i)}. \qquad (3.2.1)$$

$H^{(e)}$ characterizes the internal electronic state of the ion, $H^{(i)}$ describes the interaction of ion to the applied light fields. With the denotation $\hat{\sigma}_+ := |\uparrow\rangle\langle\downarrow|$ and $\hat{\sigma}_- := |\downarrow\rangle\langle\uparrow|$, the coupling Hamiltonian has the form[50]

$$\hat{H}^{(i)} = \frac{1}{2}\hbar\Omega(\hat{\sigma}_+ + \hat{\sigma}_-)(e^{i(k\hat{X}-\omega_L t)} + e^{-i(k\hat{X}-\omega_L t)}), \qquad (3.2.2)$$

with rabi frequency $\Omega$ measures the strength of the coupling and $\omega_L$ is the effective frequency of the light field. $k = 2\pi/\lambda$ is the wave number with $\lambda$ being




$$\hat{H}^{(e)} = \frac{\hbar\omega_{HF}}{2}\left(|\downarrow\rangle\langle\downarrow| - |\uparrow\rangle\langle\uparrow|\right) = \frac{\hbar\omega_{HF}}{2}\sigma_z \qquad \hat{H}^{(m)} = \frac{\hat{p}^2}{2M} + \frac{1}{2}M\omega_X^2\hat{X}^2 = \hbar\omega_X\left(a^+a + \frac{1}{2}\right)$$

Figure 3.1 Interaction between internal and external degree of freedom. Ion with two levels of internal electronic states couples to the harmonic oscillator of vibrational motion states with $\hbar\omega_X$ energy difference.

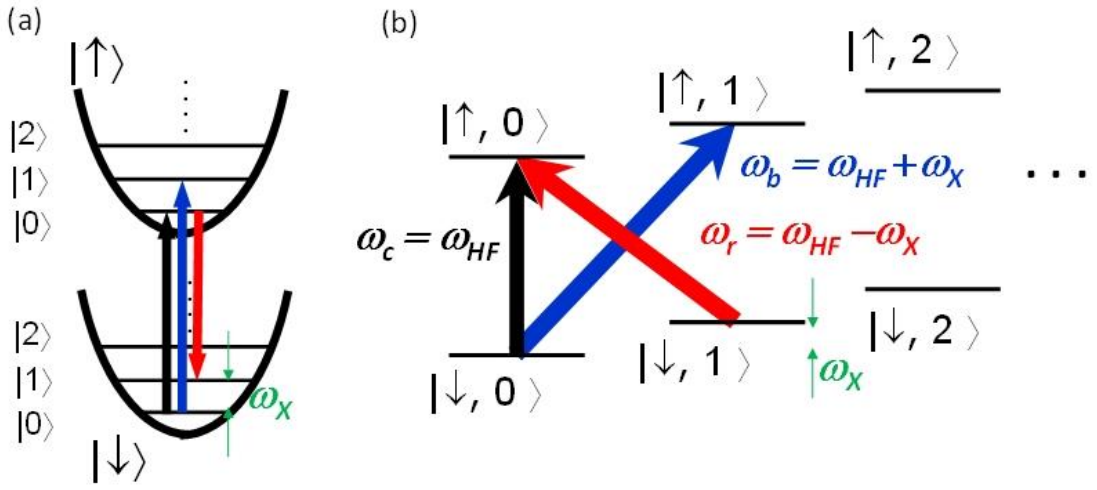



Figure 3.2 Schematic of three typical transitions (carrier, blue sideband and red sideband). They are shown in the view of (a) harmonic oscillation potential, (b) motional state with two levels.

the wavelength of the light field. Introducing the Lamb-Dicke parameter $\eta = k\sqrt{\mathrm{h}/2M\omega_X}$, it describes the interaction strength between the light and the motional modes of the ion in the ground state, thus yielding $k\hat{X} = \eta(\hat{a} + \hat{a}^\dagger)$. Induced by the light field, this Hamiltonian is moved into the interaction with the free Hamiltonian $\hat{H}_0 = \hat{H}^{(e)} + \hat{H}^{(m)} = \mathrm{h}\omega_{HF}\hat{\sigma}_z/2 + \mathrm{h}\omega_X(\hat{a}^\dagger\hat{a} + 1/2)$ (Figure 3.1). When the transformation with the unitary transformation $\hat{U}_0 = \exp[-(i/\mathrm{h})\hat{H}_0 t]$ is applied, the two terms which oscillating rapidly with frequency $\omega_{HF} + \omega_L$ are neglected in the rotating-wave approximation(RWA), while the other two terms oscillate with frequency $\Delta = \omega_L - \omega_{HF} = \omega_{HF}$, resulting the Hamiltonian in the interaction picture

$$\begin{aligned}\hat{H}_{\mathrm{int}} &= \hat{U}_0^{\dagger}\hat{H}^{(i)}\hat{U}_0 \\ &= \frac{1}{2}\mathrm{h}\Omega(\hat{\sigma}_+ e^{-i\Delta t}\exp(i\eta(\hat{a}^\dagger e^{i\omega_L t} + \hat{a}e^{-i\omega_L t})) + h.c.)\end{aligned}. \qquad (3.2.3)$$

If the ion is confined to the Lamb-Dicke regime (defined by the condition $\eta\sqrt{2n+1} = 1$ for all the phonon number $n$), which implies the ion's position spread is small compared to the wavelength[53], we can simplify the model to

$$\hat{H}_{\mathrm{int}} = \frac{1}{2}\mathrm{h}\Omega\hat{\sigma}_+\{1 + i\eta(\hat{a}^\dagger e^{i\omega_L t} + \hat{a}e^{-i\omega_L t})\}e^{-i\Delta t} + h.c. \quad . \qquad (3.2.4)$$

Excitation with the external field coherently couples the vibrational motion of the ion to the internal electronic state. As the ion oscillates in the trap and the detuning of the laser field is set precisely to meet the trap frequency, the laser can couple the state $|\downarrow, n\rangle$ to all phonons. The sidebands of the transition occur in the absorption or emission processes, leads to the transfer of the energy difference $\mathrm{h}\Delta$ in kinetic energy of the ion when changing the phonon number $n$.

From Eq.(3.2.4), it is clear to identify three most commonly used transitions defined as follows considering respective levels

$$\begin{aligned}&\text{Carrier:} && |\downarrow, n\rangle \leftrightarrow |\uparrow, n\rangle \\ &\text{Blue Sideband:} && |\downarrow, n\rangle \leftrightarrow |\uparrow, n+1\rangle \\ &\text{Red Sideband:} && |\downarrow, n\rangle \leftrightarrow |\uparrow, n-1\rangle\end{aligned} \qquad (3.2.5)$$

Neglect the terms proportional to $\eta$, the first resonance, carrier transition, is excited

when the frequency is tuned to $\Delta = 0$. The Hamiltonian reads

$$\hat{H}_{car} = \frac{1}{2}\hbar\Omega\hat{\sigma}_{+}e^{-i\Delta t} = \frac{1}{2}\hbar\Omega_{n,n}\left|\uparrow,n\right\rangle\left\langle\downarrow,n\right|e^{-i\Delta t} \qquad (3.2.6)$$

with coupling strength $\Omega_{n,n} = \Omega_0(1-\eta^2 n)$ for all $n \geq 0$ while $\Omega_0 = \omega_{HF}$. It is actually pure qubit transitions without motional modes of the ion, thus bring no changes to the phonon number distribution.

When the resonance of the laser is blue detuned by one unit of the trap frequency to have $\Delta = \omega_X$, the blue sideband (bsb) transition is excited with the form[53,54]

$$\hat{H}_{blue} = \frac{1}{2}\hbar\Omega\hat{\sigma}_{+}i\eta(\hat{a}^{\dagger}e^{i\omega_L t})e^{-i\Delta t} = \frac{1}{2}\hbar\Omega_{n,n+1}\left|\uparrow,n+1\right\rangle\left\langle\downarrow,n\right|e^{-i\Delta t}, \qquad (3.2.7)$$

corresponding rabi frequency changes to $\Omega_{n,n+1} = \eta\sqrt{n+1}\Omega_0$. It is description of absorption of a photon reducing the phonon number by one, and successfully entangles the motion state with the internal state of the ion.

In the same way, the red sideband (rsb) transition is excited when the laser is red detuned by the trap frequency *s.t.* $\Delta = -\omega_X$

$$\hat{H}_{red} = \frac{1}{2}\hbar\Omega\hat{\sigma}_{+}i\eta(\hat{a}e^{-i\omega_L t})e^{-i\Delta t} = \frac{1}{2}\hbar\Omega_{n,n-1}\left|\uparrow,n-1\right\rangle\left\langle\downarrow,n\right|e^{-i\Delta t} \qquad (3.2.8)$$

$$\text{with } \Omega_{n,n-1} = \eta\sqrt{n}\Omega_0,$$

for $n \geq 1$, but not for the ground state as previously mentioned. This stimulated emission of a phonon leads to increasing of the phonon number.

Stimulated Raman transition is a two photon process involving two qubit levels in the ground state as well as an excited electronic state $\left|e\right\rangle$ [55], it consists of combined stimulate absorption and emission of a photon. This virtual level must be far off the resonances of all real levels, especially the lifetimes of the $\left|\downarrow\right\rangle \leftrightarrow \left|e\right\rangle$ needs to be much shorter than the transitions $\left|\downarrow\right\rangle \leftrightarrow \left|\uparrow\right\rangle$. Thus the frequency difference of the two light fields make $\omega_L$. Raman detuning $\Delta_e$ of this virtual level from the $P_{1/2}$ state is determined by the wavelength of the counter-propagating laser beams. Figure 3.4 shows the Raman transition configuration for $^{171}Yb^{+}$ ion.

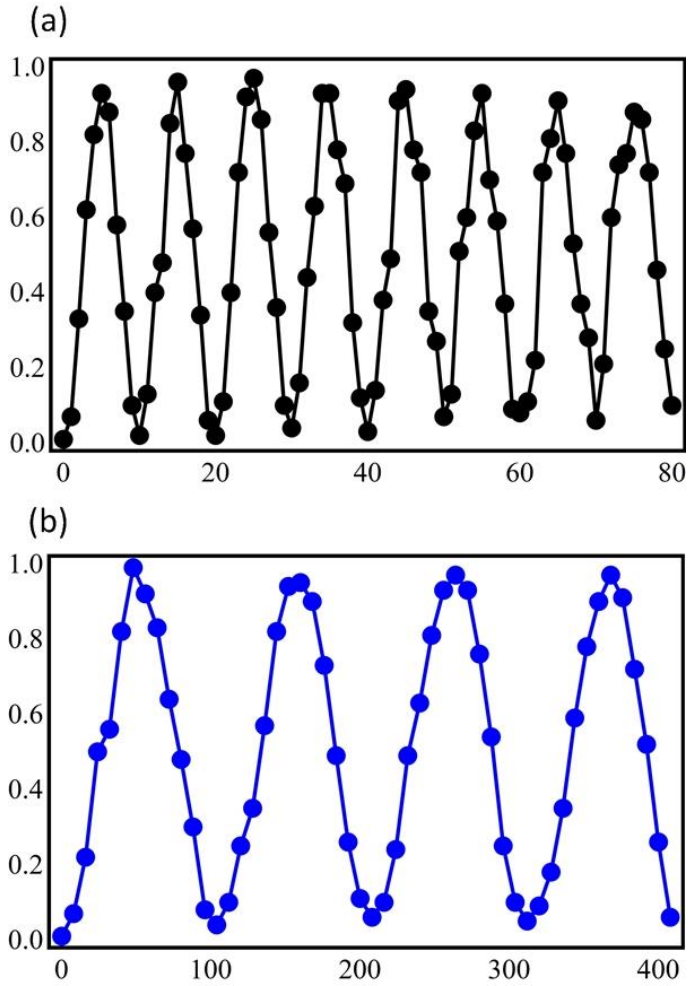



Figure 3.3 Rabi oscillation of carrier and blue sideband transition. (a) Rabi oscillation on the carrier transition in the spin qubit between $|\downarrow,0\rangle$ and $|\uparrow,0\rangle$. (b) Rabi oscillation on the blue transition between $|\downarrow,0\rangle$ and $|\uparrow,1\rangle$. The vertical axis shows the probability of detecting the ion in the bright state, and the horizontal axis shows the interaction time between light field and the ion. Here we get the value $\eta = \Omega_{1,0} / \Omega_0 = 0.098$.

## 3.3 Sideband Cooling

Although the ion is Doppler cooled in the trap, due to the average energy $\langle E \rangle = k_B T = \bar{n}\hbar\omega_X$ that originates from the temperature T of the system, the ion is in a mixture of the vibrational motion states. Sideband cooling is necessary procedure to cool the ion to the ground state[50,54]. The idea of the process that substracting the vibrational quantum number one by one until the ion is cooled to phonon number 0 is implemented by iteration of red sideband transition and optical pumping. A $\pi$-pulse of red sideband, for which the frequency of the laser is tuned to $\omega_{HF} - \omega_X$, excites the ion from $|\downarrow, n\rangle \rightarrow |\uparrow, n-1\rangle$ and then leads to the reduction of phonon number by one when the optical pumping process is followed. In this way, a cooling cycle is established without changing the initial internal state. We repeat this Raman cooling cycle for N=100 iterations until the ion is brought to $|\downarrow, 0\rangle$. To the result, the ground state is a dark state that not affected by the laser light, as the ion cannot make a red sideband transition from $n = 0$ to $n = -1$ since the latter does not exist. Figure 3.5(a) shows the scheme of sideband cooling.

According to the definition of red sideband transition, its $\pi$-pulse time $T_{n,n-1} = \pi / \Omega_{n,n-1} = \pi / \eta\sqrt{n}\Omega_0$ depends on their initial vibrational state. It means that another independent process is needed to calibrate the resonance frequency as well as rabi frequency. By taking a Raman spectrum separately, we first apply frequency scan, then use the fitted resonance frequency to do time scan to obtain $T_{1,0} = \pi / \eta\Omega_0$ between $|\downarrow, 1\rangle \leftrightarrow |\uparrow, 0\rangle$ in experiment, and then calculate exact Raman cooling time for each step. After Doppler cooling and optical pumping procedure which pumps the ion to dark state, we start the first sideband cooling cycle by turning on the Raman beams to excite transition from $|\downarrow, 100\rangle$ to $|\uparrow, 99\rangle$ then again applying optical pumping beam to make ion from $|\uparrow, 99\rangle$ to $|\downarrow, 99\rangle$. We repeat the procedures in the same way only changing the red sideband transition time by $T_{n,n-1} = T_{n,n+1}\sqrt{n} / \sqrt{n+1}$, and ends up with a $\pi$-pulse from $|\downarrow, 1\rangle$ to $|\uparrow, 0\rangle$ and optical pumping. The schematic of all the sequences is depicted in Figure 3.5(b). Effect of sideband cooling is clearly showed in Figure 3.6, complete suppression of the red sideband transition implies the ion is cooled to the ground state.

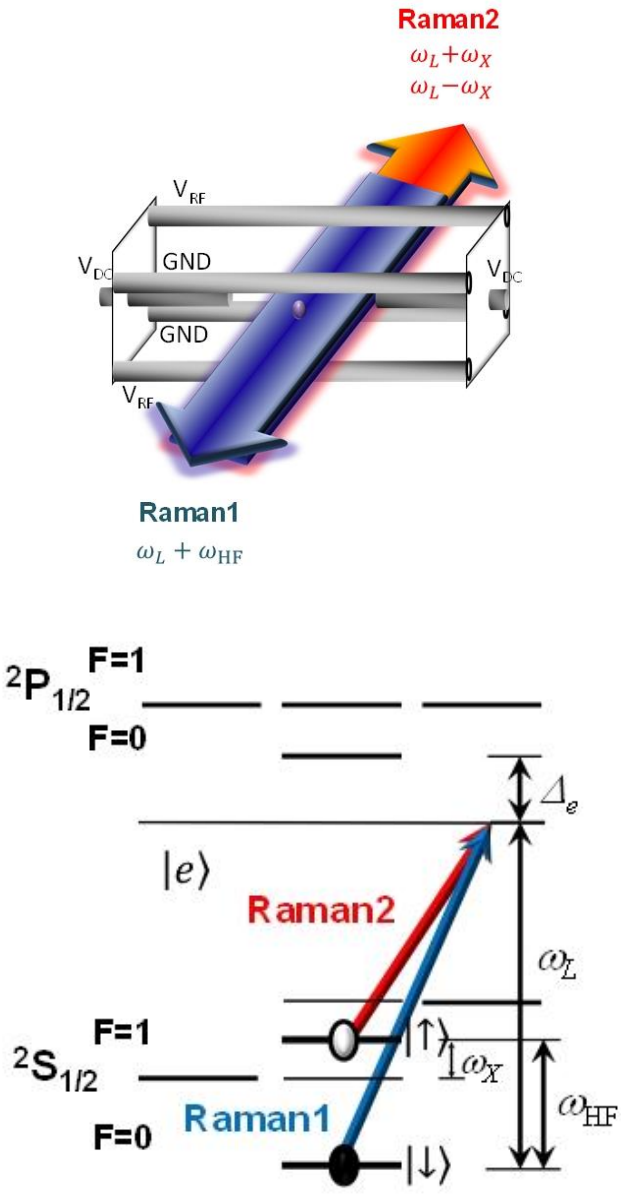



Figure 3.4 Raman transition configuration. (a) Raman beams applied to the trapped ion. (b) Raman transition via an excited state. Light fields couple the qubit levels between $|\downarrow\rangle$ and $|\uparrow\rangle$ at detuning $\Delta = \omega_L - \omega_{HF}$. Blue sideband and red sideband can be realized by blue and red detuning of $\omega_X$ amount from effective laser frequency $\omega_{HF}$.

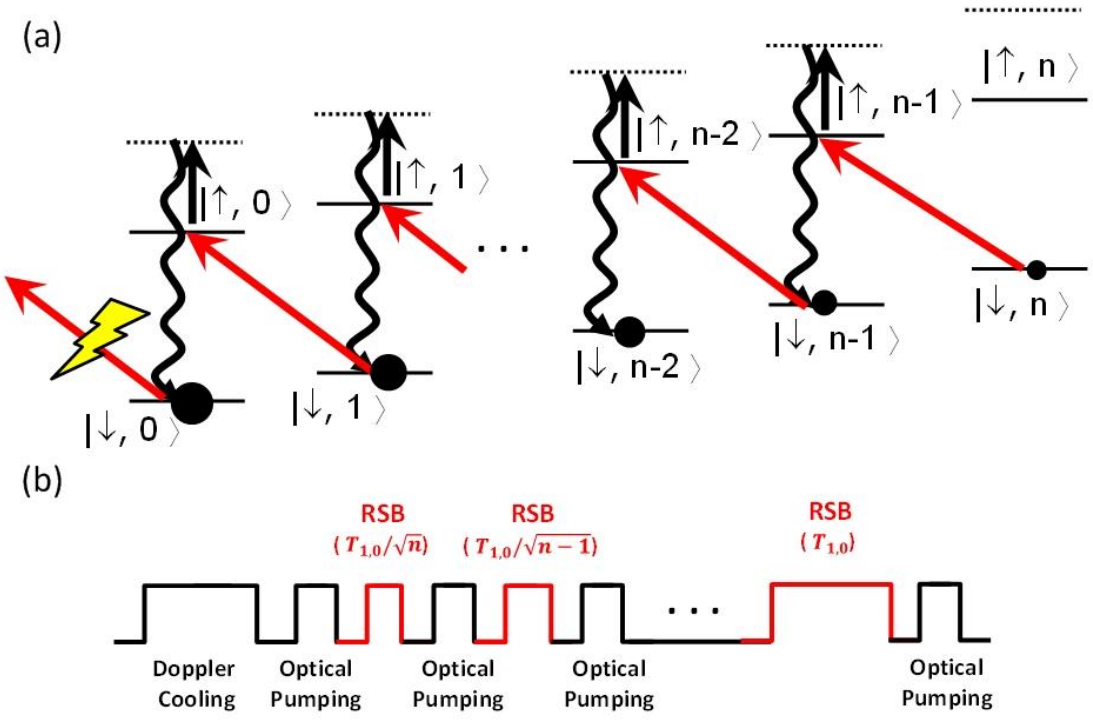



Figure 3.5 Schematic and procedure of Raman sideband cooling. (a) Raman sideband cooling process starts from Doppler cooling and optical pumping, then the ion is supposed to be in $|\downarrow, n\rangle$ state. A $\pi$-pulse of red sideband transition reduces the vibrational motion state by one as the spin is flipped to $|\uparrow\rangle$ state. When followed by optical pumping, the ion is transferred to $|\downarrow, n-1\rangle$ state. This cycle is processed until the ion is in the $|\downarrow, 0\rangle$ where no more red sideband can be excited. (b) Time schematic for sideband cooling. Duration of the pulsed Raman transition at first cycle is $T_{1,0}/\sqrt{n}$, then $\pi$-time of red sideband increases by factor of $\sqrt{n+1}/\sqrt{n}$. Finally, the ion is cooled to the ground state after $n$ cycles.

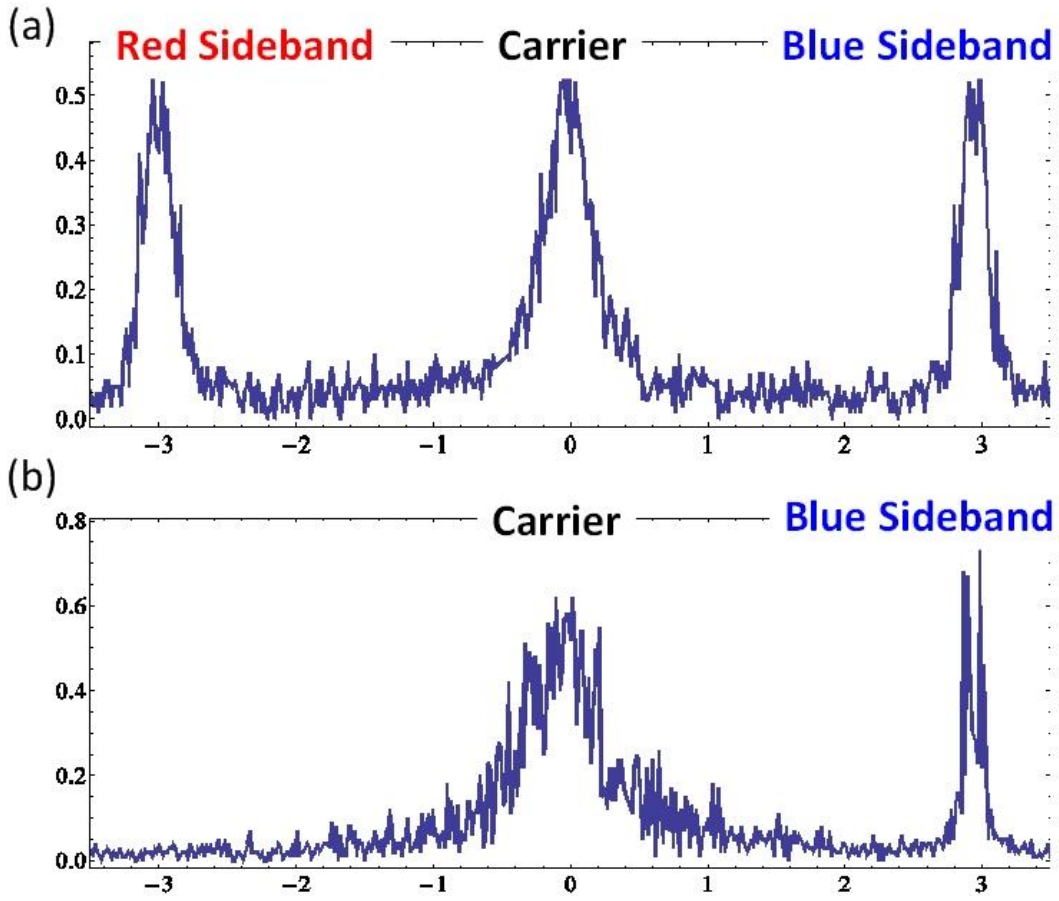



Figure 3.6 Effect of sideband cooling shown by spectrum. (a) Spectrum before sideband cooling. (b) Spectrum after sideband cooling. Red sideband transition is completely suppressed.

## 3.4 Rapid Adiabatic Transition Process

Now it is straightforward to implement the creation operator $\hat{a}^{\dagger}$ as the ion is cooled to the ground state. A $\pi$-pulse of blue sideband transition followed by a $\pi$-pulse of carrier transition will map the ion from $|\downarrow,0\rangle \rightarrow |\uparrow,1\rangle \rightarrow |\downarrow,1\rangle$, thus increases the phonon number by one. This scheme can be applied for any vibrational number state $|\downarrow,n\rangle$, but the $\pi$-pulse period of blue sideband transition changes on the dependency of $n$, which makes it difficult to simultaneously apply exact $\pi$-pulse of blue sideband for every phonon number state if the ion is in a mixture of vibrational motion states. Condition is same for the annihilation operator $\hat{a}$ which consists of first $\pi$-pulse of carrier transition followed then a $\pi$-pulse of blue sideband transition. Furthermore, the creation and annihilation operators $\hat{a}^{\dagger}$ and $\hat{a}$ do not simply add and substract phonons, but also bring modification to the state amplitudes with $\sqrt{n}$ factors. Therefore, pure shift operation independent of phonon number $n$, actually bare addition and substraction of phonons, are required besides the creation $\hat{a}^{\dagger}$ and annihilation $\hat{a}$. Instead of normal blue sideband transition, the adiabatic blue sideband transition $\pi$ operation transfers the ion from $|\downarrow,n\rangle$ to $|\uparrow,n+1\rangle$ for any $n$.

We apply the scheme shown in Ref. 33 to accomplish the adiabatic blue sideband transition by changing intensity and detuning of the Raman beams. Intensity $\Omega$ follows Sine curve to have $\Omega(t) = \Omega_0 \sin(\pi t / T)$, where adiabatic transition duration takes 7 times of $\pi$-pulse time of blue sideband transition with $T = 7 \times T_{1,0} = 91\mu s$ in experiment, which is reasonably fast comparing to the scheme demonstrate in Ref. 34 with linear control of the intensity and Gaussian control of the detuning. Detuning $\Delta$ is realized by adding a time varying detuning phase $\phi(t) = \int_0^t \delta(t)dt$, with $\delta(t) = \delta_0 \cos(\pi t / T)$ and the parameter is set to be $\delta_0 = 1.5\Omega_0$, experimentally takes the value of $(2\pi)$ 55.6 KHz.

However, the geometric phases are acquired during this rapid adiabatic passage (RAP) and they have to be cancelled out. Spin-echo is the solution for eliminating accumulated geometric phases. Experimentally it is realized by inverting the intensity $\Omega$ of the laser beams as depicted in Figure 3.7. This protocol transfers the state from

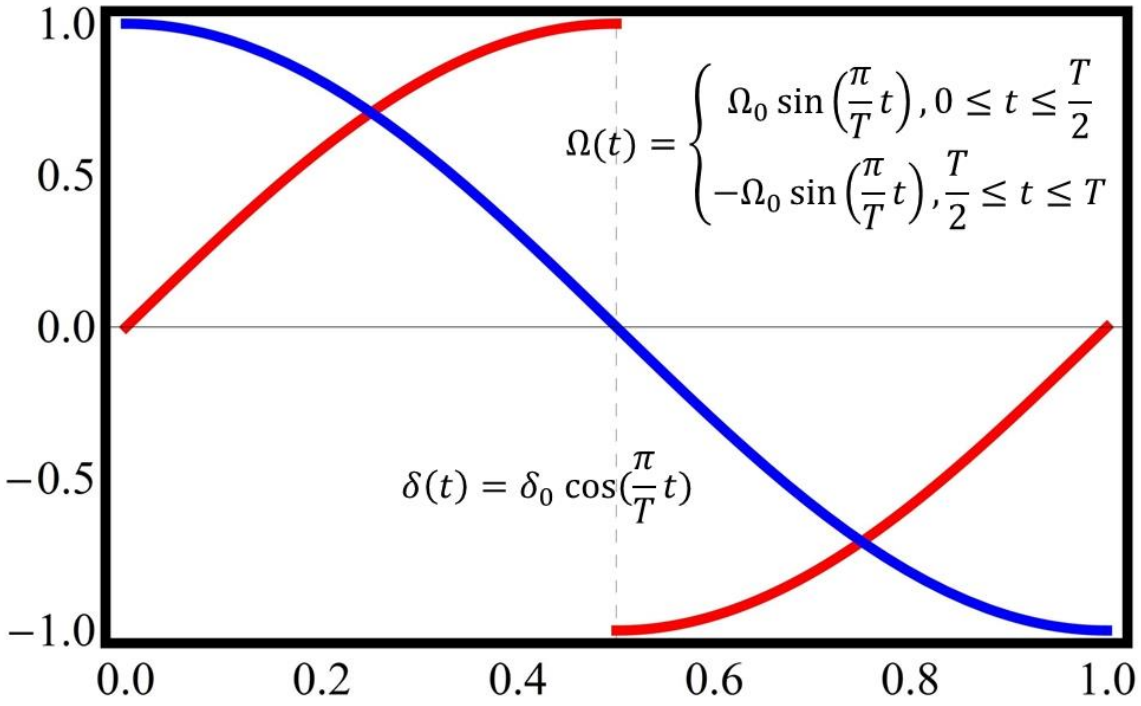



Figure 3.7 Time dependent control of the laser intensity and detuning in rapid adiabatic transition process. The time dependence of the laser intensity $\Omega(t) = \Omega_0 \sin(\pi t/T)$ and the detuning $\delta(t) = \delta_0 \cos(\pi t/T)$. Intensity is inverted in the middle as spin-echo.

$|\downarrow, n\rangle$ to $|\uparrow, n+1\rangle$ regardless of phonon number $n$ between 0 to 6. The observed fidelity of the adiabatic operation is shown in Table 3.1. The error compared to the simulation mainly comes from heating process and imperfection of Fock state preparation which is also mainly due to the heating during the operation.

Table 3.1 The comparison between the simulation and the experimental result of the adiabatic blue-sideband transition

| | $\|\downarrow,0\rangle \rightarrow \|\uparrow,1\rangle$ | $\|\downarrow,1\rangle \rightarrow \|\uparrow,2\rangle$ | $\|\downarrow,2\rangle \rightarrow \|\uparrow,3\rangle$ | $\|\downarrow,3\rangle \rightarrow \|\uparrow,4\rangle$ | $\|\downarrow,4\rangle \rightarrow \|\uparrow,5\rangle$ |
|---|---|---|---|---|---|
| simulation(%) | 99.48 | 99.88 | 99.15 | 99.52 | 98.17 |
| experiment(%) | 98.8 | 96.3 | 96.9 | 96.4 | 92.4 |

Although this pure addition and substraction operations are different from creation and annihilation operators, they produce non-classical state of phonon[35]. For Fock state

and coherent state, Wigner function measurement is done after pure phonon shifting operations either addition or substracting. The observation of a negative probability proves the generation of non-classicality.

## 3.5 Experimental Setup

The laser source of the Raman transition is a Coherent Mira 900 mode-locked Titanium:Sapphire (Ti:S) laser which provides switching between continuous wave (CW), femtosecond and picosecond operations. It is pumped by a Verdi 532 nm green laser and has quite a wide frequency range. This Titanium:Sapphire laser provides 2.2W at 756 nm, we lock the frequency-doubled laser at 378 nm with 200 mW to start optical path to the trap. As the laser's repetition rate is 76.2 MHz, a band pass filter chooses the frequency between $166^{th}$ and $167^{th}$ which is closest to $\omega_{HF}$ .

The 756 nm red laser is used for frequency stabilization. Its frequency that acquired from Photo Diode is mixed with frequency of $\omega_{HF}/2$, then the frequency is doubled after first passing through a low-pass filter to filter out high frequency component from the output of the mixer. The doubled frequency is mixed with the frequency of Raman1 (213 MHz) then feedback again to Raman1 RF source which provide frequency modulation (FM). Finally, the stabilized frequency is applied to the Acousto-Optic Modulator (AOM1 in Figure 3.8) where the laser source divides into two beams. The frequency generated by either another RF source or an Arbitrary Waveform Generator(AWG) board of Raman2 is applied by AOM2 and its first order needs to pass the same distance as Raman1 beam to excite Raman transition. This procedure is accurately controlled by an one-dimensional translation stage covered with two mirrors on the path of Raman1. The signals of RF source and AWG are combined together then output to AOM2 which provide the choice of using either RF source or AWG. For most cases, RF source is first used to process sideband cooling to cool the ion to the ground state, then we use AWG for subsequent operations. The zeroth order of AOM2 is used for stabilizing the intensity which feedback to AOM0.

The laser is first focused at AOM1 position with a 400 mm lens (L1), L2 and L3 with the same focal length collimate Raman1 and Raman2 respectively. A vertical

cylindrical lens V1(f=500 mm) converges the height of Raman2. L4(f=75 mm) and L5(f=300 mm) makes the beam size of Raman2 bigger. By adding these two lenses, the distance of the image of AOM1 to the image of AOM2 in the trap is lowered to guarantee the strength of the transitions as well as convergence of the laser alignment at various frequencies.

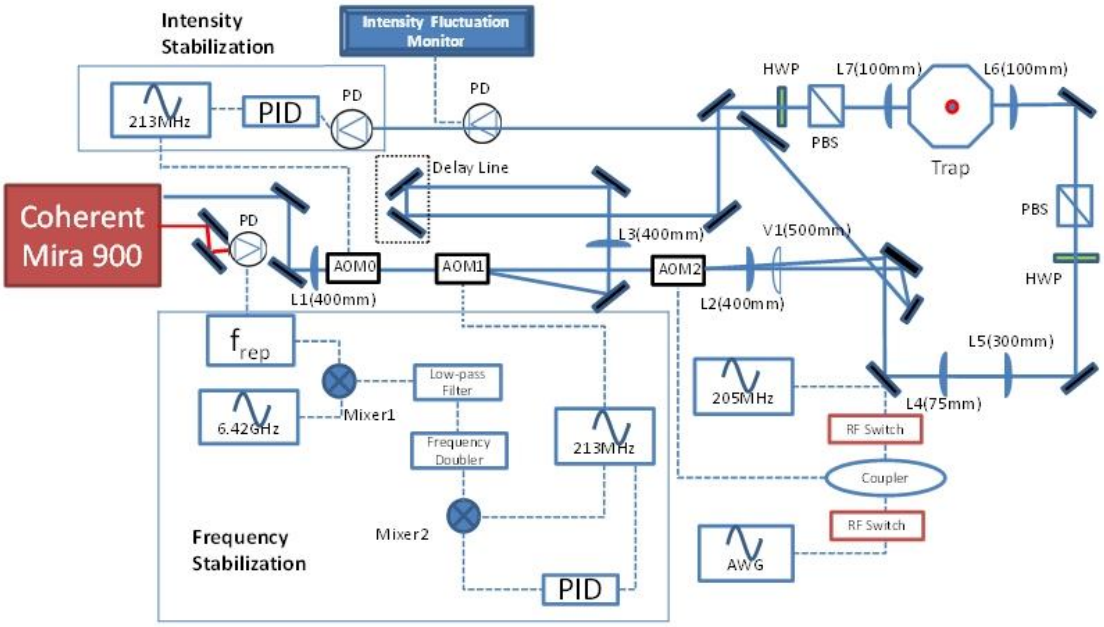



Figure 3.8 The schematics of the Raman set up with Coherent Mira 900. Raman1 and Raman2 are separated by AOM1, they are the first order of AOM1 and AOM2, respectively. Intensity stabilization is applied using the zeroth order of AOM2 then feedback to AOM0. Feedback of frequency stabilization system goes to AOM1. The 756 nm laser shown in red is used to monitor the repetition rate and stabilize the frequency. The lenses are shown in blue and the vertical cylindrical lens V1 is in white.

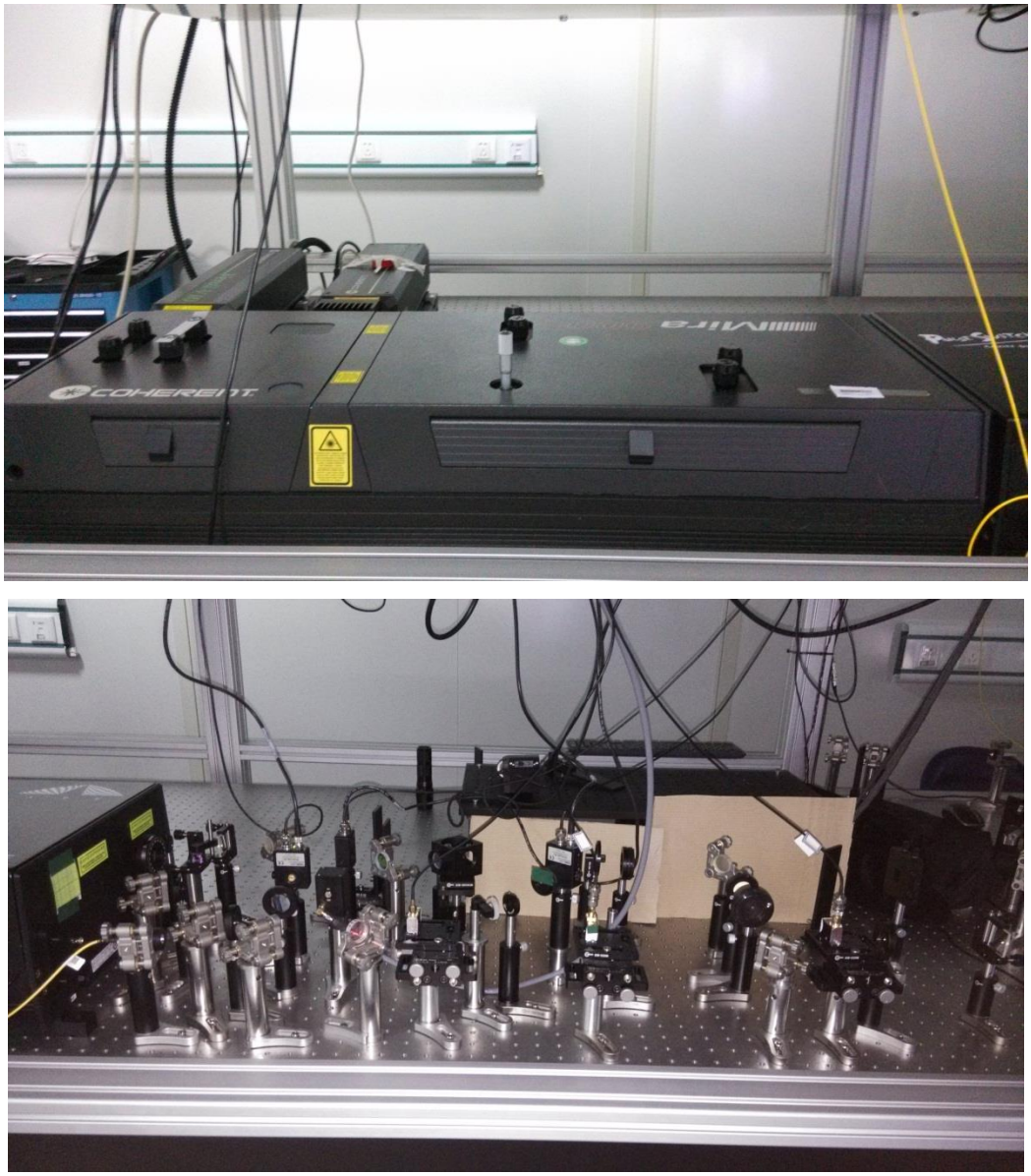



Figure 3.9 Coherent Mira 900 laser and beam path.

## 3.6 Experimental Result

As the first attempt, phonon addition to a coherent state of $\alpha$=0.5 is experimentally operated. Although there are several technical aspects to be improved, the phonon distribution of initial state is shifted by one after phonon addition operation (Figure 3.10). Furthermore, we successfully observed negative value when measuring Wigner function of this phonon added coherent state. This result is shown in Figure 3.11.

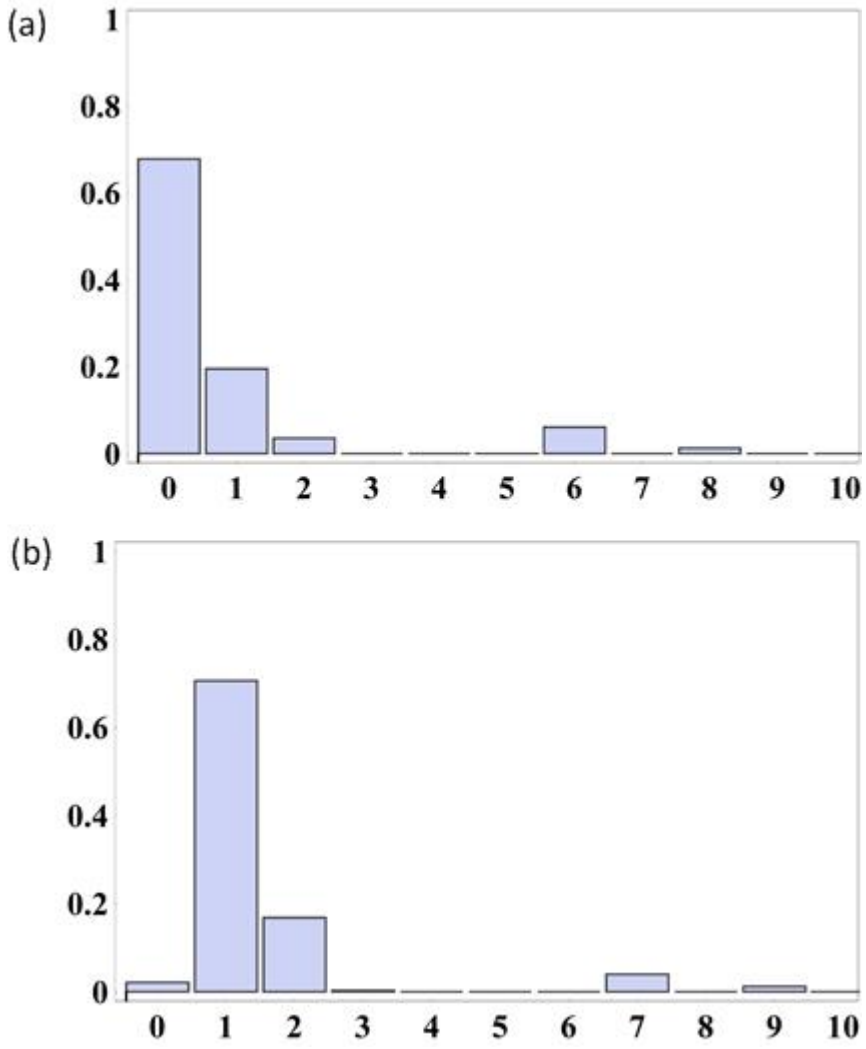



Figure 3.10 Phonon addition of α=0.5 coherent state shown by measuring phonon distribution. (a) Original phonon distribution after preparing α=0.5 coherent state. (b) Phonon distribution after phonon addition operation.

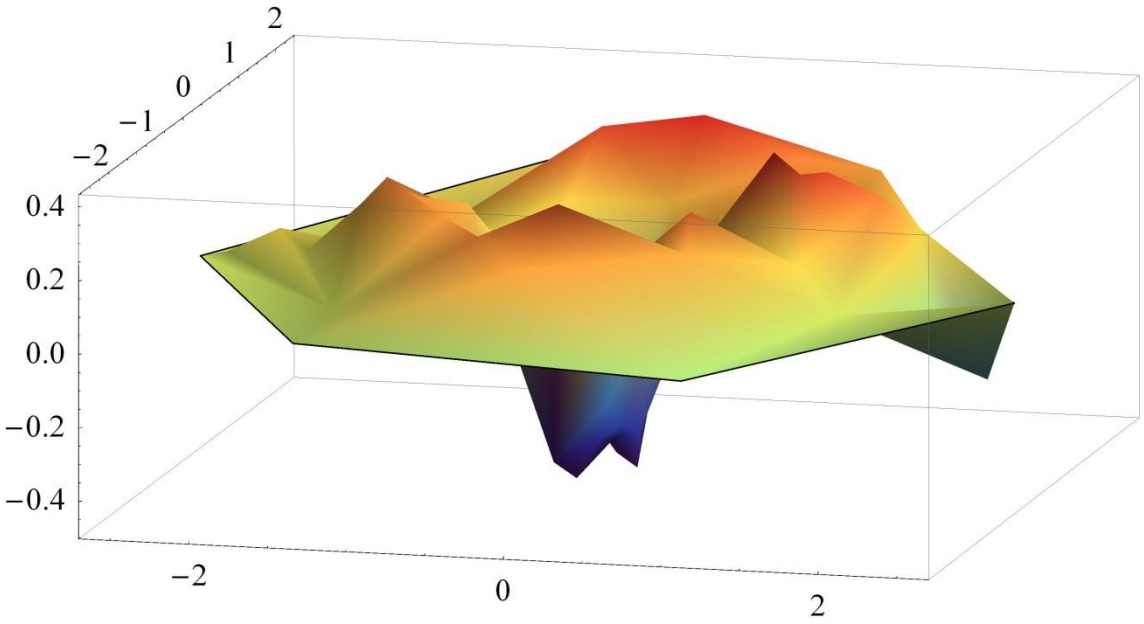



Figure 3.11 Wigner function measurement of α=0.5 coherent state after phonon addition operation. Obvious observation of negative value (with minimum of -0.48) proves generation of non-classical state of phonon.

## 3.7 Related Work

There has been another project of testing Quantum Jarzynski Equality with a trapped ion system in our lab. Being a milestone in the development of non-equilibrium statistical mechanics, Jarzynski equality relates the free energy difference $\langle W \rangle$ between two equilibrium states and the work $\Delta F$ done on the system through far from equilibrium processes[59]. The Jarzynski equality has the form

$$\left\langle e^{-(W-\Delta F)/k_B T} \right\rangle = 1, \qquad (3.7.1)$$

here $T$ is the initial temperature of the system in the thermal equilibrium and $k_B$ is Boltzmann constant.

Our project developed an experimental scheme as a test of the quantum Jarzynski equality with a single $^{171}Yb^{+}$ ion trapped in harmonic potential, also performed projective measurements on phonon[36] to determine the initial eigenstate from thermal distribution and the standard phonon distribution measurement after work is done on the projected eigenstate to find work distribution. This work is also done by applying laser induced

force on the projected energy eigenstate, and finding transition probabilities to final energy eigenstates after the work is done. In classical regime, this equation has been successfully performed in various systems[37,38,39,40,41]. Work distribution is described by

$$P(W)=\sum_{n,\bar{n}}\delta\left[W-\left(E_{\bar{n}}(\tau)-E_n(0)\right)\right]P_{\bar{n}\leftarrow n}P_n^{th}, \qquad (3.7.2)$$

where $P_n^{th}=\exp\left(-E_n(0)/k_BT\right)/\left[\sum_n\exp\left(-E_n(0)/k_BT\right)\right]$ shows the initial thermal distribution and $P_{\bar{n}\leftarrow n}=\left|\left\langle\bar{n}(\tau)\middle|\hat{U}\middle|n(0)\right\rangle\right|^2$ is the transition probability from the initial state $\left|n(0)\right\rangle$ to the final state $\left|\bar{n}(\tau)\right\rangle$ under the evolution operator $\hat{U}$.

For the test of the validity of the Jarzynski equality, we observed that the average of the exponentiated work $\left\langle\exp\left(-W/k_BT\right)\right\rangle=\sum P(W)\exp\left(-W/k_BT\right)$ does not depend on the protocol of applying the work from quasi-static to far-from equilibrium. It is observed by obtaining the conditional probability from the projected energy eigenstate out of thermal distribution to the final eigenstate after the work is done on the projected state. The experiment is processed as following four stages: 1. Preparation of thermal State; 2. Projection to an energy eigenstate; 3. Application of work on the eigenstate; 4. Measurement of final phonon distribution. The procedure is repeated to obtain statistically meaningful result.

Figure 3.12 illustrates the result. Phonon number state $\left|n\right\rangle$ is prepared up to $n=5$ with over 90% fidelity (Figure 3.12(a)). Then the laser induced force is applied on the prepared state for the durations of 5 $\mu$s, 25 $\mu$s and 45 $\mu$s with the linear increase of the strength to the same maximum value as shown in Figure 3.12(b). Figure 3.12(c) summarizes the final phonon distributions depending on the speed of applying work on a Fock state, which are the transition probabilities $P_{\bar{n}\leftarrow n}$. Figure 3.12(d) shows the probability distribution of dissipated work, $W-\Delta F$ constructed from $P_{\bar{n}\leftarrow n}$ with the phonon distribution $P_n^{th}$ of effective temperature $T=480$ nK calculated from the initial average phonon number $\left\langle n\right\rangle=0.157$. It is clear that the ramping of the force with the duration $\tau$ = 45 $\mu$s is close to adiabatic, the mean value and the width of the distribution

of the dissipated work increase with the pulling speed. The dissipated work for the case of $\tau = 5\ \mu$s shows non-Gaussian distribution, which strongly indicates the process is far-from equilibrium.

Our experiment demonstrate the validity of Jarzynski equality when other estimations deviate from the ideal values in far-from equilibrium regime[60]. The main error in the experiments come from the heating of phonon modes, but the effect of the heating in the Jarzynski estimation is less than experimental uncertainties according to our numerical simulations. Our experimental developments pave the way for further investigation of the equality in an open quantum system and may shed light on the understanding of work and heat in quantum regime[47,42]. This demonstration could lead to some applications in quantum heat engine[43,44] as well as for the quantum information processing[42,45,46] and would be able to provide an experimental tool for Boson-sampling problem[36].

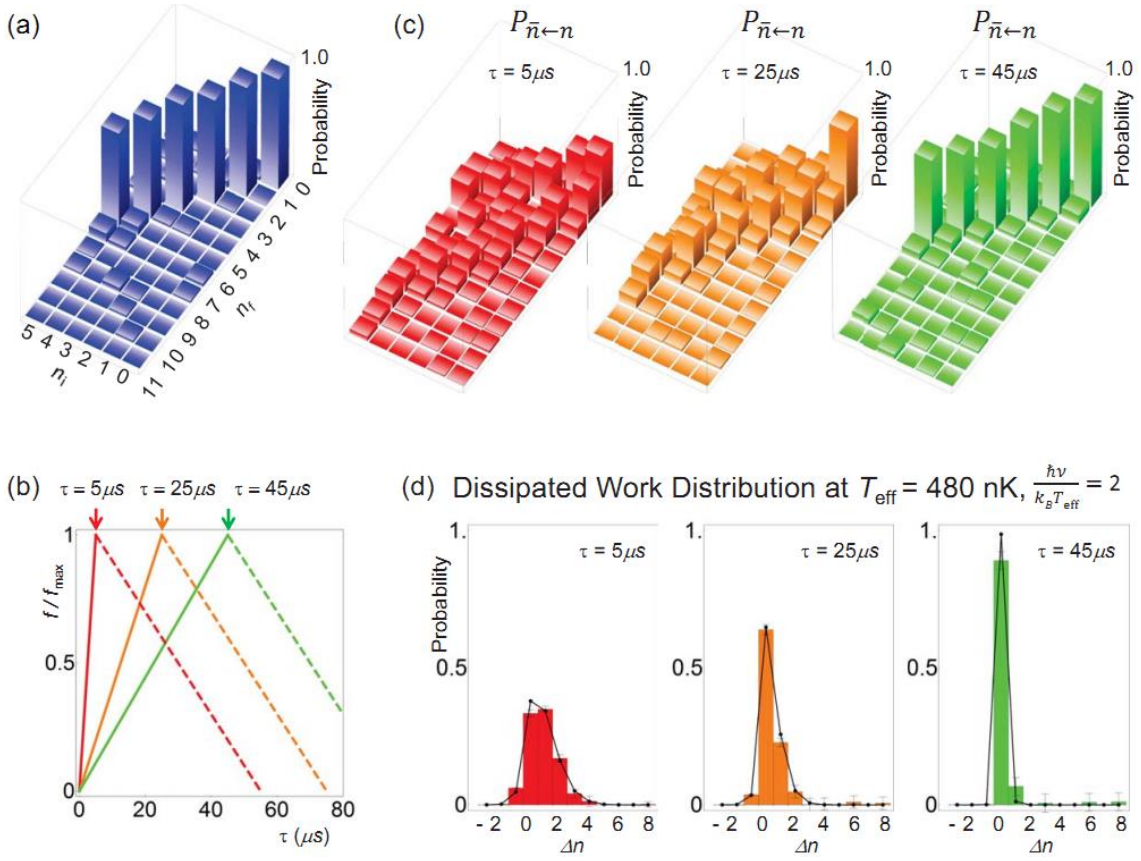



Figure 3.12 The dissipated works and the transition probabilities of three different speeds of ramping up the force. (a) The fidelity of phonon Fock state from $n$ = 0 to 5. (b) The force is linearly increased to the maximum value in three different durations, which are corresponding to far-from equilibrium (5 $\mu$s), intermediate (25 $\mu$s) and near adiabatic (45 $\mu$s) processes of work. The dashed line shows the adiabatic process to bring the system to the lab frame in 50 $\mu$s. (c) The transfer probabilities from initial state $|n(0)\rangle (n(0) = 0,1,...,5)$ to the final state $|\bar{n}(\tau)\rangle$ with three speeds measured by maximal-likelihood method after the work process. (d) The distributions of dissipated works at $\langle n\rangle = 0.157$ have full information to test the validity of quantum Jarzynski equality, Eq. (3.7.1). The data (bars) are resulted from the transfer probability (c). The three distributions of dissipated works show the characteristics of far-from equilibrium, intermediate and adiabatic processes.

# Chapter 4 Conclusion

## 4.1 Experimental Conclusion

In summary, we have demonstrated violations of the KCBS inequality using a single trapped ion, with the detection efficiency loophole closed for the first time. We use quantum contextuality to certify randomness of the measurement outcomes. The randomness of our device is ensured by observing violations of the inequality independent of experimental details. With our device, we already obtained a net output entropy.

## 4.2 Outlook

In the future, our device can generate random numbers with a higher speed and better security. We plan to use a $^{137}Ba^{+}$ ion which has a stable shelving state as a qutrit to achieve loophole-free random number generation. After developing Barium ion trapping, an even better device with perfect sequential measurement by hybrid trapping of a Barium ion and an Ytterbium ion are expected to totally complete our random number generator which is important for practical applications. As we have been dealing the motion of the ion by ion-laser interaction, this promising improvement is already on the way.

# Bibliography

[1] Coddington P D. Analysis of random number generators using monte carlo simulation. Northeast Parallel Architecture Center Paper 14 (1994).

[2] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev. Mod. Phys. 74, 145 (2002).

[3] Goldreich O. Foundations of Cryptography (Cambridge University Press, Cambridge, UK, 2007).

[4] Isida M, Ikeda Y. Random number generator. Ann. Inst. Stat. Math. 8, 119–126 (1956).

[5] Stefanov A, Gisin N, Guinnard O, Guinnard L, Zbinden H. Optical quantum random number generator. J. Mod. Opt. 47, 595–598 (2000).

[6] Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. Rev. Sci. Instrum. 71, 1675–1680 (2000).

[7] Ma H Q, Xie Y J, Wu L A. A random number generator based on quantum entangled photon pairs. Chin. Phys. Lett. 21, 1961–1964 (2004).

[8] Kwon O, Cho Y-W, Kim Y-H. Quantum random number generator using photon-number path entanglement. Appl. Opt. 48, 1774–1778 (2009).

[9] Qi B, Chi Y-M, Lo H-K, Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt. Lett. 35, 312–314 (2010).

[10] Gabriel C, et al. A generator for unique quantum random numbers based on vacuum states. Nature Photonics 4, 711–715 (2010).

[11] Bustard P J, et al. Quantum random bit generation using stimulated raman scattering. Opt. Exp. 19, 25173–25180 (2011).

[12] Symul T, Assad S M, Lamb P K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. Appl. Phys. Lett. 98, 231103 (2011).

[13] Fiorentino M, Santori C, Spillane S M, Beausoleil R G. Secure selfcalibrating quantum random-bit generator. Phys. Rev. A 75, 032334 (2007).

[14] Pironio S, et al. Random numbers certified by bell's theorem. Nature 464, 1021 (2010).

[15] Colbeck R. Quantum and relativistic protocols for secure multi-party computation. Ph.D. thesis, University of Cambridge (2007).

[16] Vazirani U, Vidick T. Certifiable quantum dice. Phil. Trans. R. Soc. A 370, 3432–3448 (2012).

[17] Pironio S, Massar S. Security of practical private randomness generation. Phys. Rev. A 87, 012336 (2013).

[18] Deng D L, et al. Exploring quantum contextuality to generate true random numbers. arXiv:1301.5364 (2013).

[19] Abbott A A, Calude C S, Conder J, Svozil K. Kochen-specker theorem revisited and strong incomputability of quantum randomness. arXiv:1207.2029 (2012).

[20] Kochen S, Specker E P. The problem of hidden variables in quantum mechanics. J. Math. Mech. 17, 59–87 (1967).

[21] Bell J S. On the problem of hidden variables in quantum mechanics. Rev. Mod. Phys. 38, 447–452 (1966).

[22] Klyachko A A, Can M A, Binicioglu S, Shumovsky A S. Simple test for hidden variables in spin-1 systems. Phys. Rev. Lett. 101, 020403 (2008).

[23] Lapkiewicz R, et al. Experimental non-classicality of an indivisible quantum system. Nature 474, 490–493 (2011).

[24] Yu S, Oh C H. State-independent proof of kochen-specker theorem with 13 rays. Phys. Rev. Lett. 108, 020403 (2012).

[25] Zu C, et al. State-independent experimental test of quantum contextuality in an indivisible system. Phys. Rev. Lett. 109, 150401 (2012).

[26] Zhang X, et al. State-independent experimental tests of quantum contextuality in a three dimensional system. Phys. Rev. Lett. 110, 070401 (2013).

[27] Kong X, et al. An experimental test of the non-classicality of quantum mechanics using an unmovable and indivisible system. arXiv:1210.0961 (2012).

[28] Silman J, Pironio S, Massar S. Device-independent randomness generation in the presence of weak cross-talk. Phys. Rev. Lett. 110, 100504 (2013).

[29] Olmschenk S, et al.Manipulation and detection of a trapped Yb1 hyperfine qubit. Phys. Rev. A 76, 052314 (2007).

[30] Fehr S, Gelles R, Schaffner C. Security and composability of randomness expansion from bell inequalities. Phys. Rev. A 87, 012335 (2013).

[31] Rukhin A, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST special publication 800–22, Rev. 1–a (2010).

[32] J Cirac and P Zoller. Quantum computation with cold, trapped ion. Phys. Rev. Lett., 74(20):4091-4094, 1995.

[33] Junhua Zhang, et al. PRA 89, 013608 (2014).

[34] Chr Wunderlich, et al. Journal of Modern Optics 54, 11, 1541-1549 (2007).

[35] Daniel K L Oi, et al. PRL 110, 210504 (2013).

[36] Shen C, Zhang Z, Duan L-M. Scalable implementation of boson sampling with trapped ions. Phys. Rev. Lett. 112 , 050504 (2014).

[37] Hummer G, Szabo A. Free energy reconstruction from nonequilibrium single-molecule pulling experiments. Proc. Natl. Acad. Sci. USA 98, 3658–3661 (2001).

[38] Liphardt J, Bustamante C, et al. Equilibrium information from nonequilibrium measurements in an experimental test of the Jarzynski equality. Science 296 , 1832–1835 (2002).

[39] Douarche F, Ciliberto S, Petrosyan A, Rabbiosi I. An experimental test of the Jarzynski equality in a mechanical experiment. Europhys. Lett. 70, 593–599 (2005).

[40] Harris N C, Song Y, Kiang C-H. Experimental free energy surface reconstruction from single-molecule force spectroscopy using Jarzynski's equality. Phys. Rev. Lett. 99 , 068101 (2007).

[41] Saira O-P, et al. Test of the Jarzynski and Crooks fluctuation relations in an electronic system. Phys. Rev. Lett. 109, 180601 (2012).

[42] Campisi M, et al. Colloquium: Quantum fluctuation relations: Founda-tions and applications. Rev. Mod. Phys. 83, 771–791 (2011).

[43] Quan H T, Liu Y X, Sun C P, Nori F. Quantum thermodynamic cycles and quantum heat engines. Phys. Rev. E 76, 031105 (2007).

[44] Abah O, et al. Single-ion heat engine at maximum power. Phys. Rev. Lett. 109, 203006 (2012).

[45] Ohzeki M. Quantum annealing with the Jarzynski equality. Phys. Rev. Lett. 105, 050401 (2010).

[46] Dorner R, Goold J, Cormick C, Paternostro M, Vedral V. Emergent thermodynamics in a quenched quantum many-body system. Phys. Rev. Lett. 76, 1796–1799 (1996).

[47] Esposito M, Harbola U, Mukamel S. Nonequilibrium fluctuations, fluctuation theorems, and counting statistics in quantum systems. Rev. Mod. Phys. 81, 1665–1702 (2009).

[48] N Kurz, M R Dietrich, Gang Shu, T Noel, B B Blinov. Measurement of Lande g factor of 5D5/2 state of Ba II with a single trapped ion. Phys. Rev. A 82, 030501(R) (2010).

[49] M R Dietrich, N Kurz, T Noel, G Shu, B. B Blinov. Hyperfine and Optical Barium Ion Qubits. Phys. Rev. A 81, 052328 (2010).

[50] D Leibfried, R Blatt, C Monroe, D Wineland, Quantum dynamics of single trapped ions. Rev. Mod. Phys. 75, 281 (2003)

[51] F W Cummings. Stimulated Emission of Radiation in a Single Mode. Phys. Rev. 140, A1051 (1965).

[52] E Jaynes, F Cummings. Comparison of quantum and semiclassical radiation theories with application to the beam maser. Proceedings of the IEEE 51, 89 (1963).

[53] D Walls, G J Milburn. Quantum Optics. Springer-Verlag Berlin Heidelberg, 2008.

[54] H Häffner, C F Roos. R Blatt. Quantum computing with trapped ions. Physics Reports-review Section of Physics Letters, vol. 469, pp. 155–203.

[55] W Nagourney, J Sandberg, H Dehmelt. Shelved optical electron amplifier: Observation of quantum jumps. Phys. Rev. Lett. 56, pp. 2797–2799, 1986.

[56] Navascues M, Pironio S, Acin A. Bounding the Set of Quantum Correlations. Phys. Rev. Lett. 98 , 010401 (2007).

[57] Navascues M, Pironio S, Acin A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New J. Phys. 10, 073013 (2008).

[58] Sturm J. SeDuMi, a MATLAB to olb ox for optimization over symmetric cones. http://sedumi.mcmaster.ca.

[59] Jarzynski C. Nonequilibrium equality for free energy differences. Phys. Rev. Lett. 78, 2690–2693 (1997).

[60] Hendrix D A, Jarzynski C. A ”fast growth” method of computing free energy differences. J. Chem. Phys. 114, 5974–5981 (2001).

# 致　谢

衷心感谢导师金奇奂教授对本人的精心指导。他在理论和实验研究上的言传身教将使我终生受益。

感谢交叉信息研究院计算机科学与技术方向的姚期智教授和物理方向的段路明教授的悉心教导与帮助；清华大学量子信息中心，以及实验室全体老师和同学们的热情帮助和支持！

本课题承蒙国家自然科学基金资助，特此致谢。

# 声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：严马可　日　期：2014.5.2

# 个人简历、在学期间发表的学术论文与研究成果

## 个人简历

1989 年 6 月 29 日出生于韩国首尔市。

2007 年 9 月考入清华大学计算机科学与技术系计算机科学与技术专业，2007 年 7 月本科毕业并获得工学学士学位。

2011 年 9 月进入清华大学交叉信息研究院攻读计算机科学与技术硕士至今。

## 发表的学术论文

[1] Mark U, Xiang Z, Junhua Z, et al. Experimental Certification of Random Numbers via Quantum Contextuality. Scientific Reports 3, 1627; DOI:10.1038/srep01627 (2013). (SCI 收录, 检索号:122PX.)

[2] Zhang X, et al. State-independent experimental tests of quantum contextuality in a three dimensional system. Physical Review Letters. 110, 070401 (2013). (SCI 收录, 检索号: 088WS.)

[3] 严马可，金奇奂. 2012 年诺贝尔物理学奖：大卫•维因兰德. 物理, 2013, 42(04): 236.

## 研究成果

[1] 清华之友-百度未来之星奖学金，院设特等.

[2] 开发用于量子计算的一体式离子阱，面上项目，国家自然科学基金委员会.

[3] 清华-密西根量子信息联合中心，清华大学国际科技合作项目，密西根大学.