囚禁离子中量子互文性保证的量子随机数生成与验证研究

（申请清华大学理学博士学位论文）

培养单位：交叉信息研究院
学　　科：物理学
研 究 生：严马可
指导教师：金奇奂 副教授

二〇一九年六月

Quantum randomness certification secured by quantum contextuality with trapped ion system

Thesis Submitted to
Tsinghua University
in partial fulfillment of the requirement
for the professional degree of
Doctor of Philosophy

by

Mark Um
(Physics)

Thesis Supervisor : Professor Kihwan Kim

June, 2019

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应遵守此规定）

作者签名：______________　　导师签名：______________

日　　期：______________　　日　　期：______________

摘 要

借助量子力学本质上的不确定性，通过观察到以 Kochen-Specker (KS) 定理为基础的量子互文性不等式的破坏值，我们可以验证量子随机数生成器输出的随机量。虽然经典隐变量模型可以描述量子力学的概率性特点，但 KS 定理可以在一个三能级系统给的单粒子系统中甚至不需要纠缠就可以显示非互文隐变量模型与量子力学之间的区别。在互文性测试实验中，仍未有人彻底解决如何在同时测量中解决相容性的问题。我对 Klyachko-Can-Binicioğlu-Shumovsky 不等式进行了修补，实验要求比使用贝尔测试的设备简单了很多。我在一个 $^{138}\mathrm{Ba}^+$ 离子系统中成功地破坏了互文性不等式，实现了关闭探测漏洞的自验证量子随机数延展器。

我的第二个课题考虑到单个量子能力操作对于操控一个量子态是非常重要的。单粒子中的产生与湮灭算符依赖于所处态的粒子个数，因此具有概率性，在迄今发表的实验中成功率不高。我在玻色子中实现确定性的算术操作，我采用的玻色子是具有谐振子结构的离子中的振动声子。实验中，将声子耦合到二能级系统，应用非跃迁的绝热操作。我在相干态与 Fock 态叠加态演示算术操作。这个操作对应于经典的加法与减法，观察到了从一个经典态确定性地生成了一个非经典态，显示出简单重复该操作可以让量子态操控变得更加容易。除了在量子信息处理与量子态操控上的应用以外，该加法与减法的叠加可用作一个相位算符。

有了在 $^{171}\mathrm{Yb}^+$ 离子振动模式中借助拉曼跃迁的声子操作，我们可以展望通过 $^{138}\mathrm{Ba}^+$ 离子与 $^{171}\mathrm{Yb}^+$ 离子纠缠实现完美的相容性测量。

关键词：随机性；KCBS 不等式；量子互文性；声子；绝热

Abstract

The output randomness from a random number generator can be certified by observing the violation of quantum contextuality inequalities based on the Kochen-Specker (KS) theorem, benefiting from the unpredictable nature of quantum mechanics. Although classical hidden-variable models have intended to describe the probabilistic features of quantum mechanics, KS theorem shows the conflict between noncontextuality hidden-variable models and quantum mechanics even with a single three-level quantum system without entanglement. However, it is not yet resolved how to ensure compatibilities for sequential measurements that is required in contextuality tests. I employ a modified Klyachko-Can-Binicioğlu-Shumovsky contextuality inequality, which can simplify the strict compatibility requirement on measurements compared to devices using Bell test. I demonstrate a experimental violation of the contextuality inequality on a trapped single $^{138}\mathrm{Ba}^{+}$ ion system and realize self-testing quantum random number expansion by closing detection loopholes.

Background of second project lies on the single-quantum level operations which are important tools to manipulate a quantum state. Annihilation or creation of single particles are probabilistic due to dependency on the particles originally in the state, and the success rate has yet been low in their experimental realization. I implement near deterministic arithmetics of a bosonic particle, in particular a phonon of ionic motion in a harmonic potential. The operations are realized by coupling phonons to an auxiliary two-level system and applying transitionless adiabatic passage. I perform these operations in coherent states and superpositions of Fock states. Furthermore, I observe that the seemingly simple operations which match to classical concepts of subtraction and addition bring a classical state into a non-classical state nearly deterministically, as showing that the easy repetition of the operations makes quantum state engineering handy. Apart from the implications in quantum information processing and quantum state engineering, the superposition of such the subtraction and addition operations is a phase operator.

Based on development of phonon operations based on raman transitions dealing with the motions of $^{171}\mathrm{Yb}^{+}$ ion, perfect compatibility measurement through entanglement of $^{138}\mathrm{Ba}^{+}$ and $^{171}\mathrm{Yb}^{+}$ ions looks promising and not far from experimental realization.

Key words: randomness; KCBS inequality; contextuality; phonon; adiabatic

目 录

第 1 章 Introduction 1
1.1 Random numbers 1
1.2 Quantum contextuality 2
1.3 Trapped ion system 3
第 2 章 Trapped ^{171}Yb^{+} ion system 6
2.1 Ionization, doppler cooling, optical pumping, detection 6
2.2 Motional structure of an ^{171}Yb^{+} Ion 9
2.3 Stimulated Raman Transition 11
2.4 Sideband cooling 16
第 3 章 Trapped ^{138}Ba^{+} ion system 20
3.1 Ionization, doppler cooling, optical pumping, detection 20
3.2 Quantum manipulation with 1762 nm laser 26
3.3 Coherence time 26
第 4 章 Phonon arithmetics with a trapped ^{171}Yb^{+} ion 29
4.1 Definition of conventional arithmetics 29
4.2 Rapid Adiabatic Transition Process 31
4.3 Experimental setup 36
4.4 Reconstruction of density matrix and wigner function measurement 38
4.5 Conventional phase-coherent addition operation 41
4.6 Conventional subtraction operation 44
4.7 Commutation relation of addition and subtraction operations 47
4.8 Extention on compatibility measurement for randomness certifacation 48
第 5 章 Randomness expansion secured by quantum contextuality with a trapped ^{138}Ba^{+} ion 49
5.1 Modified KCBS inequality 49
5.2 Randomness expansion protocol and security proof in practical case 53
5.3 Randomness generation rate 58
5.4 Experimental schematic and procedure 63
5.5 Randomness expansion data 66

5.6 Extractor and random test 68
第 6 章 Conclusion and outlook 71
6.1 Improvement of random number generation speed 71
6.2 Randomness amplification 72
6.3 Randomness certification with 2 species ions achieving perfect compatibility measurement 72
插图索引 74
表格索引 81
公式索引 82
参考文献 85
致 谢 91
声 明 92
个人简历、在学期间发表的学术论文与研究成果 93

主要符号对照表

AOM	Acousto Optic Modulators
AWG	Arbitrary Waveform Generator
BSB	Blue sideband
CCD	Charge-coupled device
EIT	Electromagnetically induced
EOM	Electro-optic modulator transparency
KCBS	Klyachko-Can-Binicioğlu-Shumovsky
KS	Kochen-Specker
PMT	Photomultiplier tube
RSB	Red sideband

第 1 章　Introduction

1.1　Random numbers

Randomness is a critical resource for information processing with applications ranging from computer simulations[1] to cryptography[2]. For cryptographic purposes, in which the randomness is most widely used, streams of random numbers should have good statistical behavior and unpredictability against adversaries[3,4]. Genuine random numbers can never be generated by a classical device because any classical device bears in principle a deterministic description. In reality, random numbers produced by an algorithm or a classical chaotic process allow an adversary with the information of the device to find a pattern. On the other hand, quantum mechanics provides a foundation for genuine randomness since the nature of quantum mechanics is fundamentally random. Based on the unpredictable behavior of quantum mechanics, various quantum random number generators have been proposed and implemented[5–7]. However, if an adversary partially manipulates the devices or the devices are exposed to imperfection or malfunction, the security can be jeopardized. In order to address this realistic issue, the device-independent protocols have been proposed to guarantee the generated randomness without relying on detailed knowledge of uncharacterized devices[8–17].

In the device-independent schemes, one can guarantee the randomness of the generated numbers from devices that were even provided by a malicious manufacturer with full quantum capability. The essence of device-independent randomness is the fact that unpredictability of measurement results could be shown by the violation of nonlocality inequalities[18]. This area is started by the recent security proofs which show that randomness can be certified under the device-independent scenario by a class of Bell inequalities[8–14], and the experimental realization of loophole-free violations of Bell's inequality have been demonstrated[19–21]. Theses device-independent schemes often rely on the real-time Bell test during the generation of random strings. Quantum random number generation schemes which apply violation of such inequalities have also been demonstrated[22,23]. However, the randomness certification requires high-fidelity entanglement sources. Furthermore, in order to rule out the locality loophole, it requires a large space separation between two detection sites. Strict experimental requirements make the experimental system uncompact, and also result in low generation rate. In a standard

Bell test where for each trial two bits randomness are consumed, device-independent randomness is generated at cost of consuming more randomness as input, which is not randomness expansion where the output randomness is larger than input randomness. A real efficient randomness expansion protocol can generate net randomness from a small input randomness and the input randomness cannot be reused for the generation. So far, loophole-free Bell tests based randomness expansion still has not been demonstrated and remained as an experimental challenge.

1.2 Quantum contextuality

In order 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, we use quantum contextuality manifested through the violation of certain Kochen-Specker (KS) inequality, similar to the Bell theorem, to certify the generated random numbers. Kochen-Specker theorem[24,25] states that quantum mechanics is contextual and cannot be fully explained by classical models, *i.e.*, noncontextual hidden variables models that have definite predetermined values for measurement outcomes. 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. Instead of Clauser-Horn-Shimony-Holt (CHSH) inequality, we use the Klyachko-Can-Binicioğlu-Shumovsky (KCBS) inequality[26], which is a particular type of the KS inequality, to test the contextuality with a single system. In this way, the experimental requirements can be significantly reduced comparing to the nonlocality test. Inequalities based on the Kochen-Specker theorem can provide alternatives for randomness certification, which has been studied in both theory and experiment[14,27,28]. A contextuality test contains a set of contexts, which are composed of a certain number of compatible, $i.e.$, commuting in quantum mechanics, measurements. Note that the measurements in the nonlocality Bell test can also be regarded as compatible measurements. Although the randomness certification has been proven for the case with perfectly compatible measurements[14], it is difficult to establish the perfect compatibility between sequential measurements when the contextuality test is performed on a single party in reality. Till now, a couple of experimental demonstration of randomness certification with the KCBS inequality have been reported[27,28], but the security of the scheme still has not been fully resolved.

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. It guarantees the identity of qubits as it uses the qubits based on atomic energy levels. There have been several types of ion traps developed, including four-rod trap, blade trap, various shape of surface traps, monolithic three dimensional trap. Each of them are connected to an ultra-high vacuum (UHV) chamber which helps the whole system to be well isolated from the environment noise. Figure 1.2 shows an example of our Tsinghua four-rod ion trap setup. In our experimental setup, we use a Ti-sublimation pump and the ion-pump to suppress the vacuum at the level of 10^{-11} Torr, which is small enough to neglect the background collisions from the background particles. Furthermore, the advantage of long coherence time[29] 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[30]. This technique is applicable to a large number of qubits in scalable trap structures.

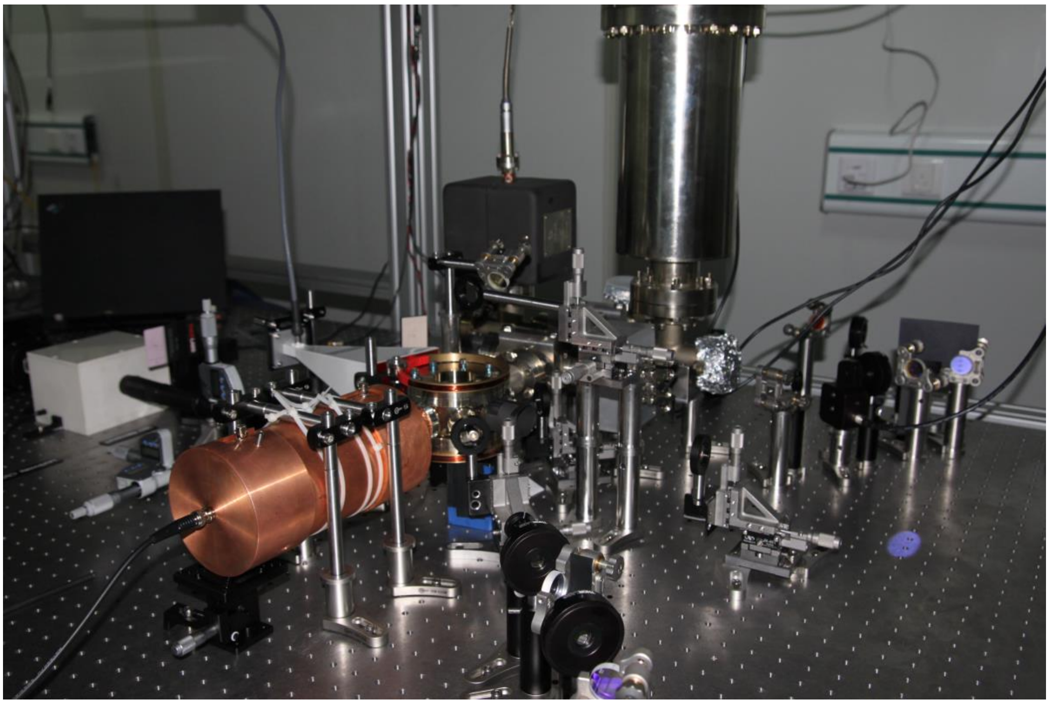


图 1.1 Tsinghua ion trap. RF signal is amplified and connected to the trap through a helical resonator. An ion pump and a Ti sublimation pump is connected to the trap to make ultra-high vacuum environment lower than 10^{-11} Torr.

We perform the test of the experiment with a single trapped 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[31,32]. The RF ion trap, so called Paul trap, provides a combination of static electric field and oscillating electric field and form the potential that confines the ions in space. This RF ion trap system has been widely applied in various fields, such as quantum information processing, precision measurement, quantum cryptography, atomic clocks and frequency spectroscopy. Refer to randomness certifacation, we have to notice the qubits readout procedure which is based on the fluorescence detection scheme. After constructing an imaging system, the fluorescence photons are collected the delivered to a Photomultiplier detector (PMT) as a photon counting device with close to perfect fidelity. The tests of the KCBS inequality with the photonic system[33,34] require the fair-sampling assumption due to the low photon detection efficiency and thus subject to the detection efficiency loophole. By using a single trapped ion, we fully close the detection efficiency loophole. In my thesis, the randomness expansion experiment is done with a trapped Barium $^{138}\mathrm{Ba}^{+}$ ion, while the phonon arithmetics experiment is done with an Ytterbium ^{171}Yb$^+$ ion.

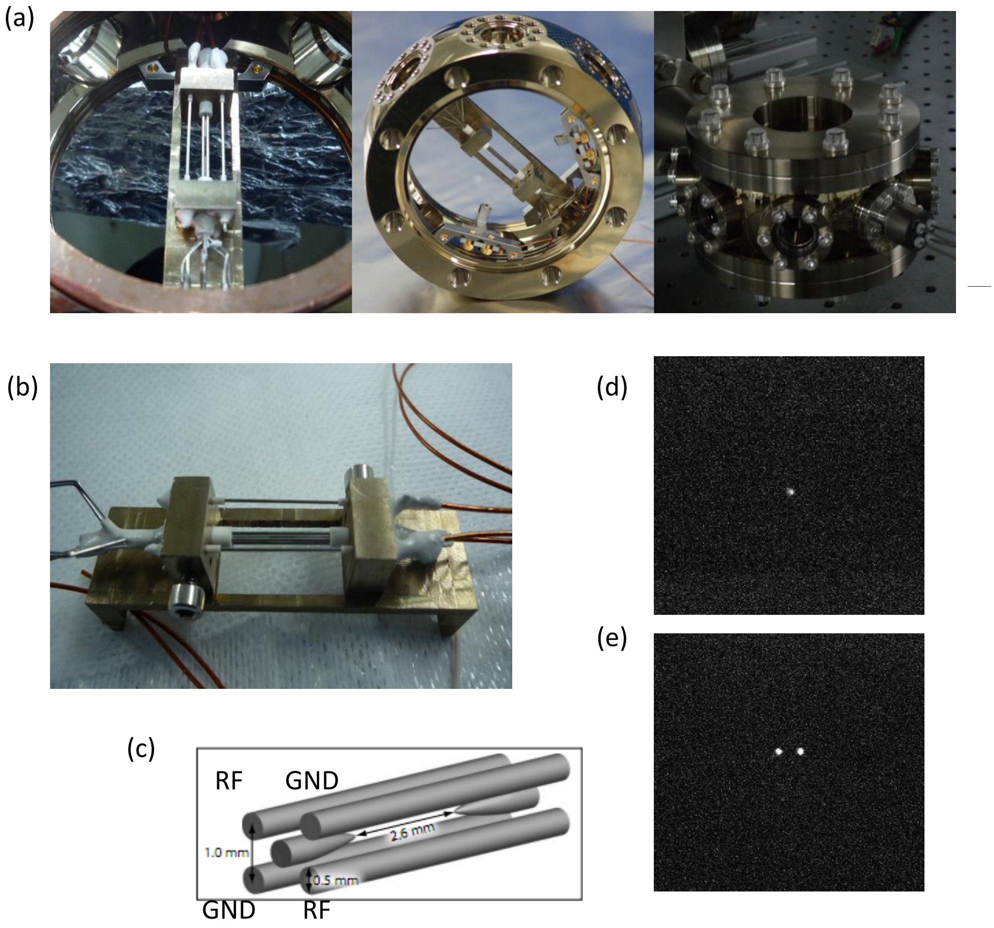


图 1.2 Four-rod trap and pictures of ^{171}Yb$^+$ ion. (a) Connection of the trap and oven of ^{171}Yb$^+$ ion in an octagon. The lasers pass shine into the trap through viewports. (b) Assembly of the four-rod trap with two micromotion compensation electrodes on the top. (c) Schematic of the four-rod trap. Among the four rods, two connect to RF while the other two are ground (GND) electrodes. The two ground electrodes are given 10.6 V 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.

My thesis is organized as follows: I will first describe ^{171}Yb$^+$ ion system and ^{138}Ba$^+$ ion system in chapter 2 and chapter 3, then demonstrate the two experimental projects – phonon arithmetics in chapter 4 and randomness expansion secured by quantum contextuality in chapter 5. Chapter 6 will conclude my work and discuss further outlook and extention for future work.

第 2 章　Trapped $^{171}\mathrm{Yb}^{+}$ ion system

2.1　Ionization, doppler cooling, optical pumping, detection

We use a hydrogen-like ^{171}Yb^{+} ion as our qubit and qutrit system because it has a strong dipole transition between $^2S_{1/2}$ and $^2P_{1/2}$ and has hyperfine structures. Recently, it has reported a new record of 10 minutes coherence time of the qubit[29]. The lasers required for all the operations, including 370 nm, 399 nm, 638 nm, 935 nm, are in quite a reasonable wavelength. Above all, ^{171}Yb^{+} ion allows simple and efficient preparation and detection with fast speed and close to perfect fidelity.

Figure 2.1 is the schematic of ^{171}Yb^{+} energy levels. Figure 2.1(a) shows the usages of 369 nm, 638 nm and 935 nm lasers. Figure 2.1(b) is the qubit and qutrit setting of a ^{171}Yb^{+} ion. Detection covers $^2S_{1/2}\,|F=1, m_F=0\rangle \leftrightarrow^2 P_{1/2}\,|F=0, m_F=0\rangle$ without any modulation because $^2P_{1/2}\,|F=0, m_F=0\rangle$ decays to the $^2S_{1/2}\,|F=1, m_F=0, 1, -1\rangle$ states as the blue arrows. Doppler cooling covers both 12.6428 GHz and 2.105 GHz, optical pumping covers 2.105 GHz. ω_1 and ω_2 are resonant to the transitions between $|1\rangle$ and $|3\rangle$, and between $|2\rangle$ and $|3\rangle$.

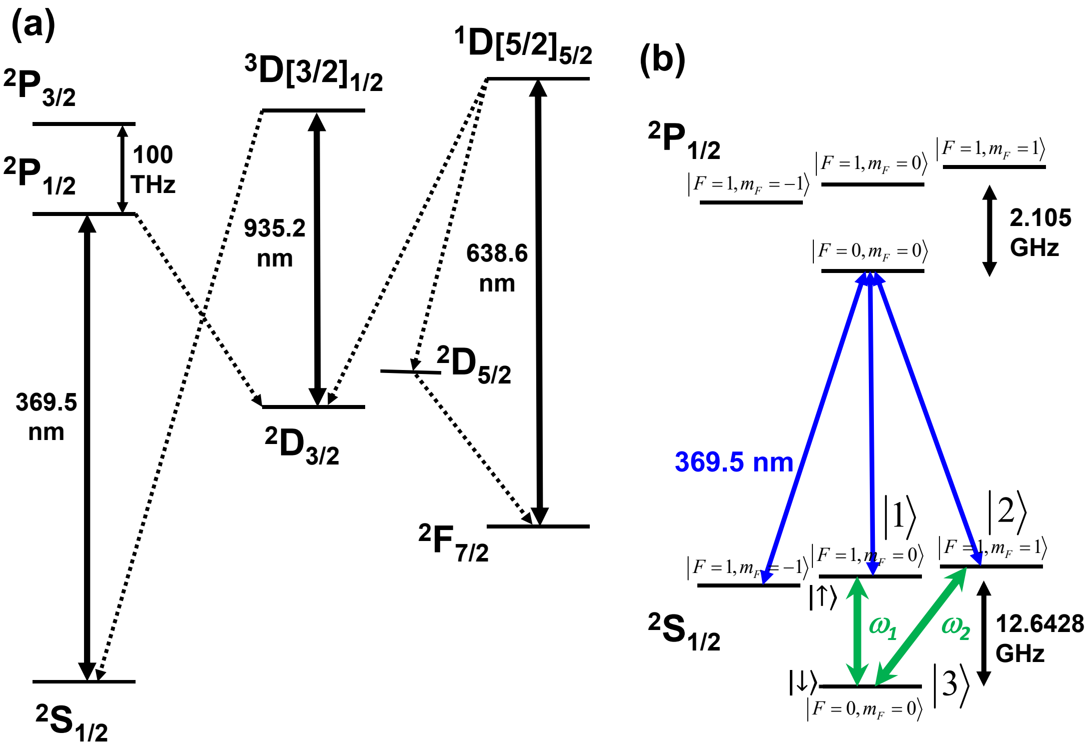


图 2.1 Energy levels of ^{171}Yb^{+} . (a) The usages of 369 nm, 638 nm and 935 nm lasers. (b) Qubit(blue) and qutrit(black) setting of a ^{171}Yb^{+} ion.

For ionization process, we first turn on the electric current to heat up the oven inside the trap which emits neutral atom. We use focused 398.9108 nm laser and strong (around 2 mW) 369.5263 nm laser to shine the atom beam, s.t. the Ytterbium atoms are photoionized by resonantly assisted dichroic two-photon transition. Then the ions are trapped by the confinement of the electric field.

We need Doppler cooling process since the ion contains quite big kinetic energy after it is ionized. A red detuned diode laser from the resonance of the transition $^2S_{1/2}$ and $^2P_{1/2}$ by about 20 MHz is used, helps the ion absorb a photon and acquire a recoil momentum. As seen in Figure 2.2, our Doppler cooling beam has to cover the transitions between $^2S_{1/2}$ and $^2P_{1/2}$. We take an Electro-optic Modulator (EOM) with the input modulation frequency of 7.37 GHz and use its second-order sideband, which is 14.74 GHz, to cover all the relevant energy levels. For motion related experiments, including phonon arithmetics project which I will talk in Chapter 4, additional sideband cooling is required right after Doppler cooling to cool the ion to the motional ground state, it will be described in section 2.4.

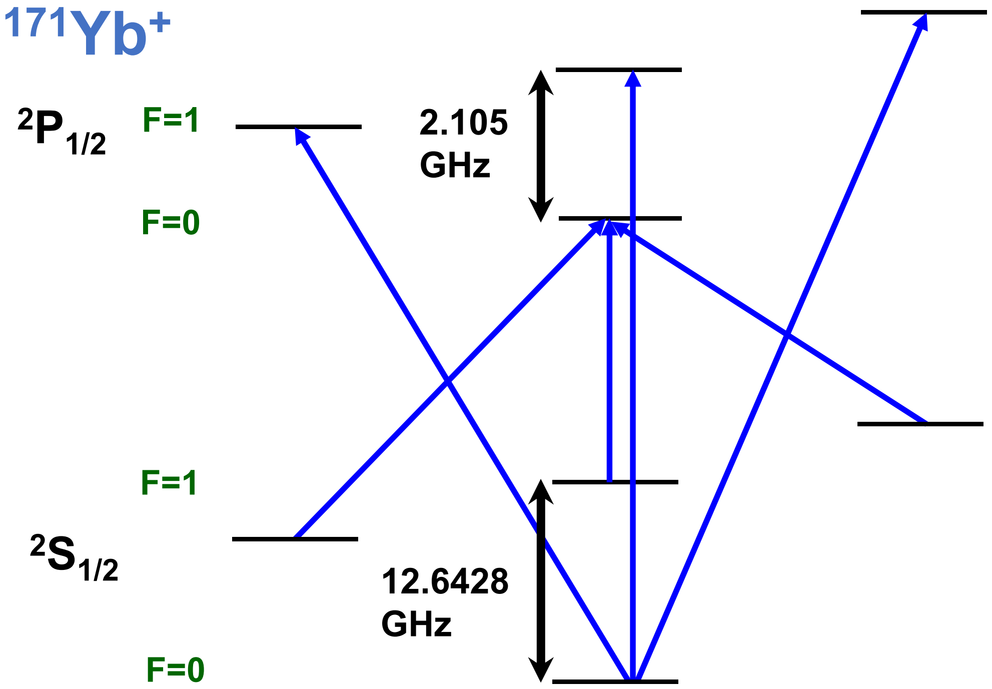


图 2.2 Schematic of Doppler cooling of ^{171}Yb^{+} . Doppler cooling laser has to cover all the energy levels in the $^2S_{1/2}$ and $^2P_{1/2}$. We achieve it by generating the second sidebands of the 7.37 GHz EOM.

As shown in figure 2.1(a), there is a 0.5% probability of decaying out from the cycling transition to $^2D_{3/2}$ state, also, sometimes the collisions make the ion transit to $^2F_{7/2}$ state. So a 935.1882 nm laser and a laser of which wavelength is scanning between 638.6101 nm and 638.6151 nm are applied as repumping lasers that bring the ion back to the Doppler cooling cycle.

The next procedure is optical pumping that initializes the ion to the hyperfine ground state $|\downarrow\rangle$. We only need a 2.105 GHz EOM to cover transitions between $^2S_{1/2}\,|F=1\rangle \leftrightarrow^2 P_{1/2}\,|F=1\rangle$ and $^2P_{1/2}\,|F=0\rangle$, as shown in blue arrows of figure 2.3. However, our optical pumping beam is far detuned from $^2S_{1/2}\,|F=0\rangle$, thus not affecting $|\downarrow\rangle$ state. Eventually all the others states will be driven and initialized to $|\downarrow\rangle$ state by spontaneously emission (red arrows of figure 2.3). We achive around 99.5% fidelity.

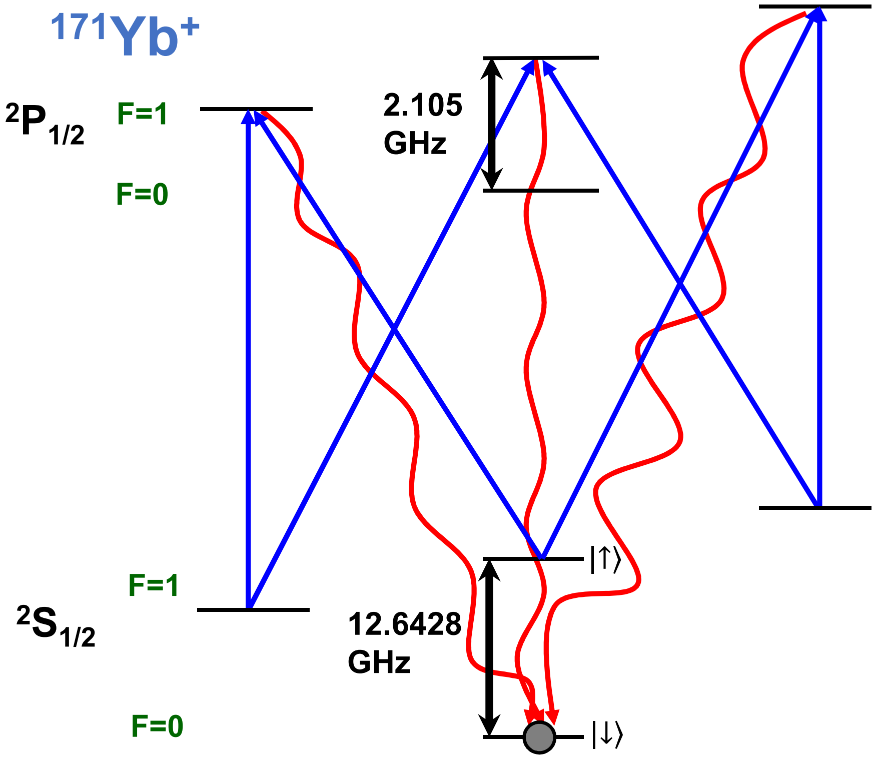


图 2.3　Schematic of optical pumping of ^{171}Yb^{+} . Optical pumping laser only needs the first sideband of the 2.105 GHz EOM. Note that it has no influence on the $|\downarrow\rangle$ state since it is far detuned from the $|\downarrow\rangle$ state

The fluorescence detection scheme serves as the qubits readout. We only need to cover transitions between $^{2}S_{1/2}\,|F = 1\rangle \leftrightarrow^{2} P_{1/2}\,|F = 1\rangle$ (he blue arrows of figure 2.1(b)), so a 369.5263 nm laser beam without sideband is enough. We use two devices: PMT or Electron-Multiplying charge coupled device (EMCCD) to check the collected fluorescence photons. In my experiments, I use the PMT to count the photon and detect the state. We set a threshold of the emission rate, if smaller than that, the state is $^{2}S_{1/2}\,|F = 0\rangle$, otherwise, we consider the state as $^{2}S_{1/2}\,|F = 1\rangle$.

2.2　Motional structure of an ^{171}Yb^{+} 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 controling 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:

$$\hat{H}^{(m)} = \frac{\hat{P}^2}{2M} + \frac{1}{2}M\omega_X^2\hat{X}^2 \tag{2-1}$$

where M is the mass of the ion, ω_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 $\omega_X = (2\pi)3.18$ 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 10.6V DC voltage to the two ground electrodes of the four rods in Figure 1.2(c). In our experiment, we only care $\hat{X}$ and $\hat{P}$, which are position and momentum operators respectively. The framework of this quantum system is defined by its eigenstates $|n\rangle_M, n = 0, 1, ...$, with eigenenergies $E_n = h\omega_X(n + 1/2)$. 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

$$\hat{a}^\dagger = \sqrt{\frac{M\omega_X}{2h}}\hat{X} + \frac{i}{\sqrt{2Mh\omega_X}}\hat{P}, \tag{2-2}$$

$$\hat{a} = \sqrt{\frac{M\omega_X}{2h}}\hat{X} - \frac{i}{\sqrt{2Mh\omega_X}}\hat{P}, \tag{2-3}$$

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

$$\hat{a}^\dagger |n\rangle_M = \sqrt{n+1}\,|n+1\rangle_M, \hat{a}\,|n\rangle_M = \sqrt{n}\,|n-1\rangle_M, \tag{2-4}$$

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

$$\hat{H}^{(m)} = h\omega_X(\hat{a}^\dagger\hat{a} + \frac{1}{2}). \tag{2-5}$$

2.3 Stimulated Raman Transition

The total Hamiltonian of the system can be written now as [35,36]

$$\hat{H} = \hat{H}^{(e)} + \hat{H}^{(m)} + \hat{H}^{(i)}. \tag{2-6}$$

$\hat{H}^{(e)}$ characterizes the internal electronic state of the ion, $\hat{H}^{(i)}$ describes the interaction of ion to the applied light fields. With the denotation $\hat{\sigma}_+ := \left|\uparrow\right\rangle\left\langle\downarrow\right|$ and $\hat{\sigma}_- := \left|\downarrow\right\rangle\left\langle\uparrow\right|$, the coupling Hamiltonian has the form [37]

$$\hat{H}^{(i)} = \frac{1}{2}h\Omega(\hat{\sigma}_+ + \hat{\sigma}_-)(e^{i(k\hat{X}-\omega_L t)} + e^{-i(k\hat{X}-\omega_L t)}), \tag{2-7}$$

with rabi frequency Ω measures the strength of the coupling and ω_L is the effective frequency of the light field. $k = 2\pi/\lambda$ is the wave number with λ being the wavelength of the light field. Introducing the Lamb-Dicke parameter $\eta = k\sqrt{h/2M\omega_X}$, 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 $\hat{H}_0 = \hat{H}^{(e)} + \hat{H}^{(m)} = h\omega_{HF}\hat{\sigma}_z/2 + h\omega_X(\hat{a}^\dagger + \hat{a} + 1/2)$ (Figure 2.4). When the transformation with the unitary transformation $U_0 = e^{-(i/h)\hat{H}_0 t}$ 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

$$\hat{H}_{int} = U_0^\dagger\hat{H}^{(i)}U_0 = \frac{1}{2}h\Omega(\hat{\sigma}_+ e^{i\Delta t}\exp(i\eta(\hat{a}^\dagger e^{i\omega_L t} + \hat{a}e^{-i\omega_L t})) + h.c.). \tag{2-8}$$

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[38], we can simplify the model to

$$\hat{H}_{int} = \frac{1}{2}h\Omega\hat{\sigma}_+[1 + i\eta(\hat{a}^\dagger e^{i\omega_L t} + \hat{a}e^{-i\omega_L t})]e^{i\Delta t} + h.c.. \tag{2-9}$$

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 $|\downarrow, n\rangle$. The sidebands of the transition occur in the absorption or emission processes, leads to the transfer or the energy difference $h\Delta$ in kinetic energy of the ion changing the phonon number n.

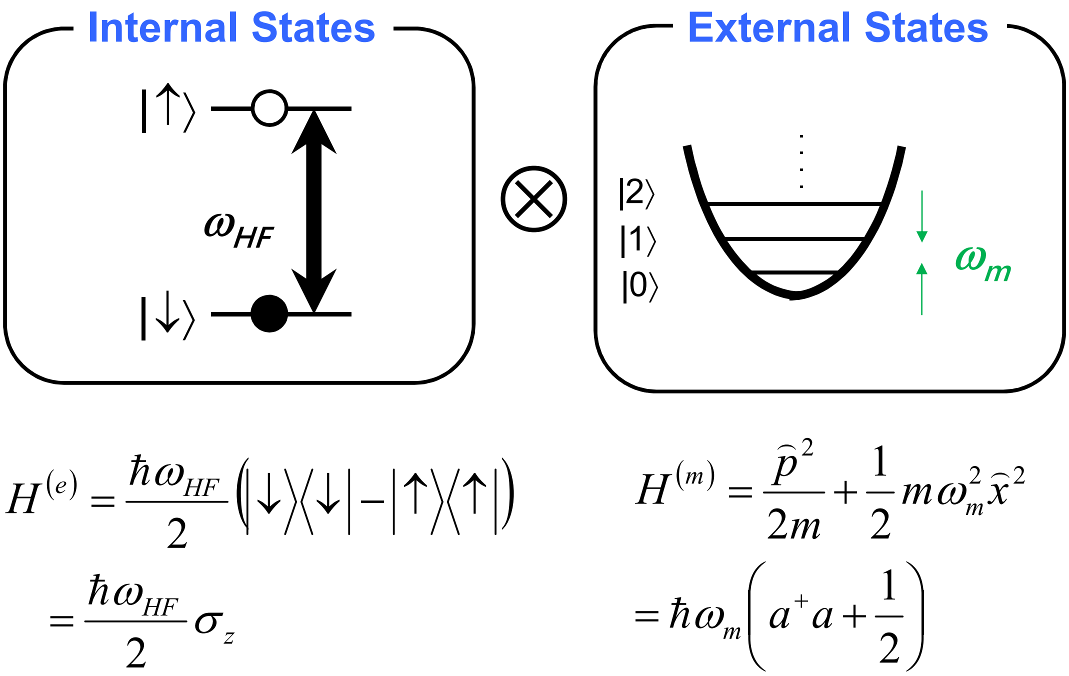

Internal States
$|\uparrow\rangle$
ω_{HF}
$|\downarrow\rangle$
$\otimes$
External States
$|2\rangle$
$|1\rangle$
$|0\rangle$
ω_m
$H^{(e)} = \frac{\hbar\omega_{HF}}{2}\left(|\downarrow\rangle\langle\downarrow| - |\uparrow\rangle\langle\uparrow|\right) = \frac{\hbar\omega_{HF}}{2}\sigma_z$
$H^{(m)} = \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega_m^2\hat{x}^2 = \hbar\omega_m\left(a^+a + \frac{1}{2}\right)$

图 2.4　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 $h\omega_X$ energy difference.

From Eq. (2-9), it is clear to identify three most commonly used transitions defined as follows considering respective levels

$$\text{Carrier}: |\downarrow, n\rangle \leftrightarrow |\uparrow, n\rangle, \tag{2-10}$$

$$\text{Blue Sideband}: |\downarrow, n\rangle \leftrightarrow |\uparrow, n+1\rangle, \tag{2-11}$$

$$\text{Red Sideband}: |\downarrow, n\rangle \leftrightarrow |\uparrow, n-1\rangle. \tag{2-12}$$

Schematics of all three transitions are depicted in Figure 2.5. Neglect the terms proportional to η, the first resonance, carrier transition, is excited when the frequency is tuned to $\Delta = 0$. The Hamiltonian reads

$$\hat{H}_{car} = \frac{1}{2}h\Omega\hat{\sigma}_{+}e^{i\Delta t} = \frac{1}{2}h\Omega_{n,n}\,|\uparrow, n\rangle\,\langle\downarrow, n|\,e^{-i\Delta t}, \tag{2-13}$$

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.

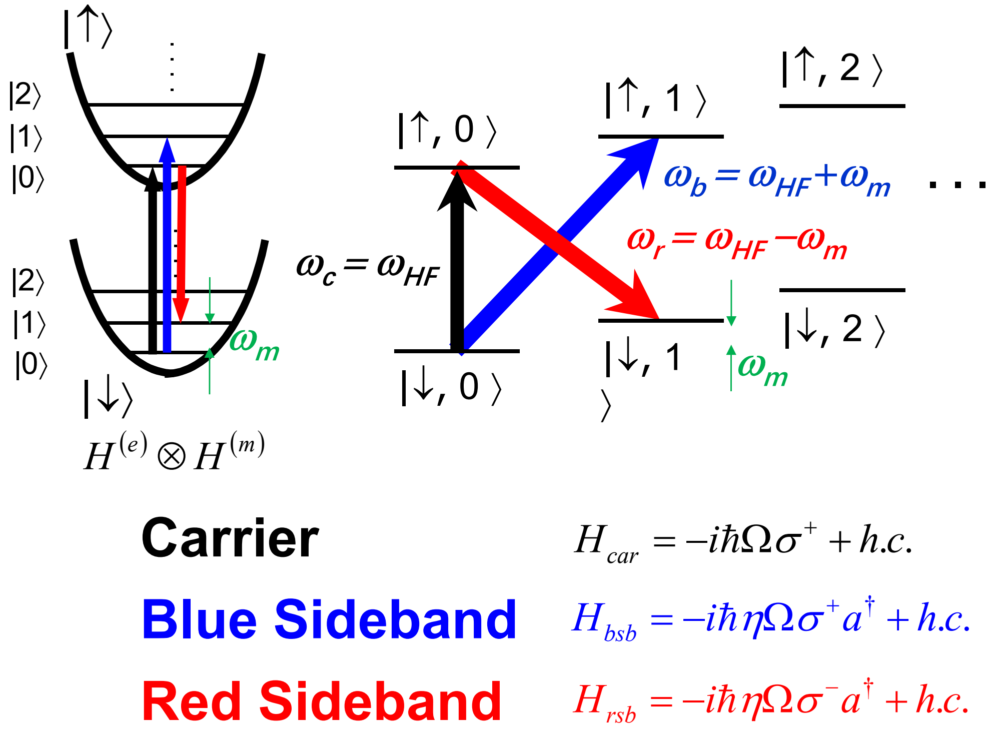


图 2.5　Schematic of three typical transitions (carrier, blue sideband and red sideband). They are shown in the view of (a) harmonic oscillation potential, (b) motional state with two levels.

When the resonance of the laser is detuned by one unit of the trap frequency to have $\Omega = \omega_X$, the blue sideband (bsb) transition is excited with the form [38,39]

$$\hat{H}_{blue} = \frac{1}{2}h\Omega\hat{\sigma}_{+}i\eta(\hat{a}^{\dagger}e^{i\omega_L t})e^{i\Delta t} = \frac{1}{2}h\Omega_{n,n+1}\,|\uparrow, n+1\rangle\,\langle\downarrow, n|\,e^{-i\Delta t}, \tag{2-14}$$

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. Figure 2.7 shows rabi oscillation of carrier and blue sideband transition in real experiment.

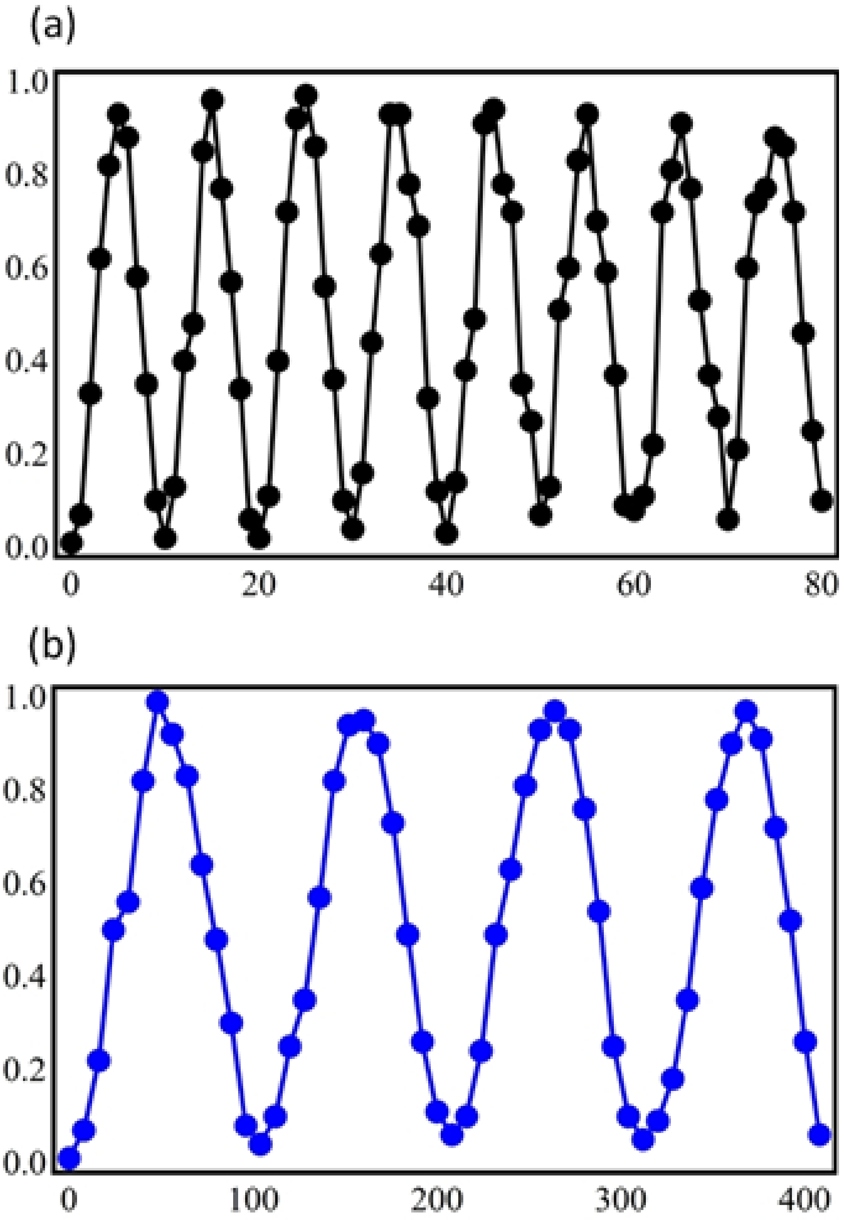


图 2.6 Rabi oscillation of carrier and blue sideband transition. (a) Rabi oscillation on the carrier transition in the spin qubit between $|\downarrow, 0\rangle$ and $|\uparrow, 0\rangle$. (b) Rabi oscillation on the blue transition between $|\downarrow, 0\rangle$ and $|\uparrow, 1\rangle$. The vertical axis shows the probability of detecting the ion in the 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.

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

$$\hat{H}_{red} = \frac{1}{2}h\Omega\hat{\sigma}_{+}i\eta(\hat{a}e^{i\omega_L t})e^{-i\Delta t} = \frac{1}{2}h\Omega_{n,n-1}ket\uparrow, n-1\left\langle\downarrow, n\right| e^{-i\Delta t}, \quad \text{with } \Omega_{n,n-1} = \eta\sqrt{n}\Omega_0, \tag{2-15}$$

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 $|e\rangle$[40], 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 $|\downarrow\rangle \leftrightarrow |e\rangle$ needs to be much shorter than the transitions $|\downarrow\rangle \leftrightarrow |\uparrow\rangle$. Thus the frequency difference of the two light fields make ω_L. Raman detuning Δ_e of this virtual level from the $P_{1/2}$-level is determined by the wavelength of the counter-propagating laser beams. Figure 2.7 shows the Raman transition configuration for ^{171}Yb^{+} ion.

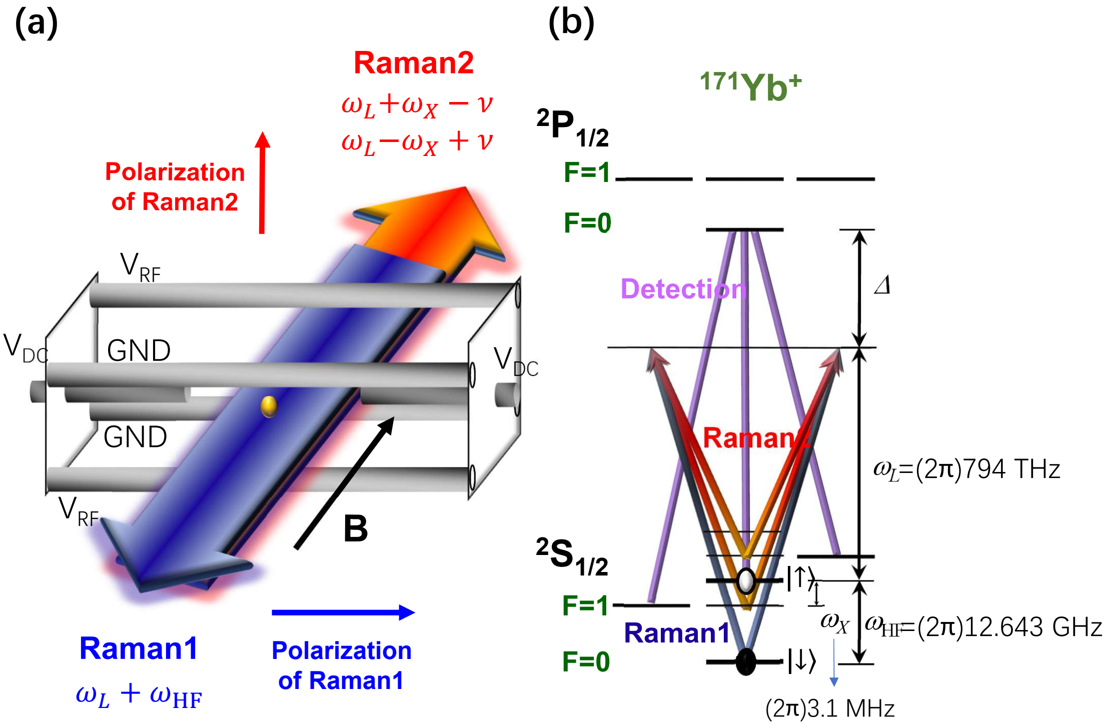


图 2.7　Raman transition configuration. (a) Raman beams applied to the trapped ion. (b) Raman transition via an excited state. Light fields couple the qubit levels between $|{\downarrow}\rangle$ and $|{\uparrow}\rangle$ at frequency $\Delta = \omega_L - \omega_{HF}$. Blue sideband and red sideband can be realized by blue and red detuning of ω_X amount at laser frequency ω_L.

2.4　Sideband cooling

Although the ion is Doppler cooled in the trap, due to the average energy $\langle E\rangle = k_B T = nh\omega_X$ 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[37,39]. The idea of the process that substract 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 π-pulse of red sideband, for which the frequency of the laser is tuned to $\omega_{HF} - \omega_X$, excites the ion from $|{\downarrow}, n\rangle \leftrightarrow |{\uparrow}, n-1\rangle$ 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 $|{\downarrow}, 0\rangle$. As 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 2.8(a) shows the scheme of sideband cooling.

According to the definition of red sideband transition, its π-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 π-pulse from $|\downarrow, 1\rangle$ to $|\uparrow, 0\rangle$ and optical pumping. The schematic of all the sequences is depicted in Figure 2.8(b). Effect of sideband cooling is clearly shown in Figure 2.9, complete suppression of the red sideband transition implies the ion is cooled to the ground state.

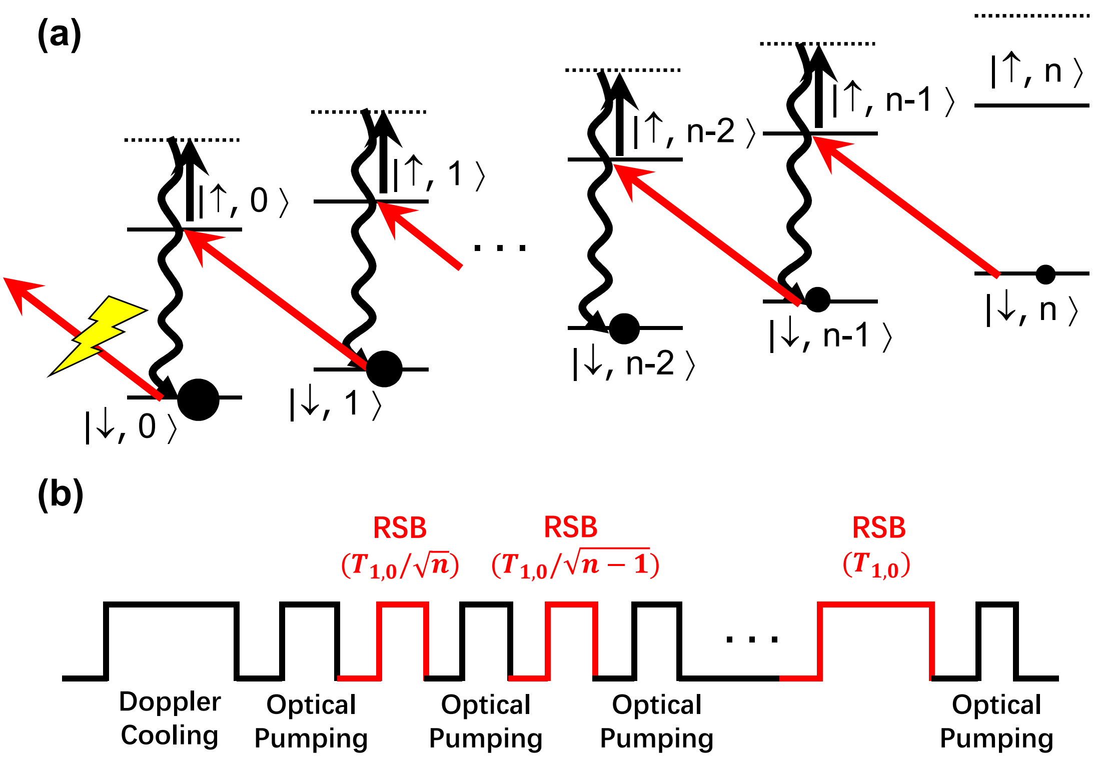


图 2.8 Schematic and procedure of Raman sideband cooling. (a) Raman sideband cooling process starts from Doppler cooling and optical pumping, then the ion is supposed to be in $|\downarrow, n\rangle$ state. A π-pulse of red sideband transition reduces the vibrational motion state by one as the spin is flipped to $|\uparrow\rangle$ state. When followed by optical pumping, the ion is transferred to $|\uparrow, n-1\rangle$ 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 π-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.

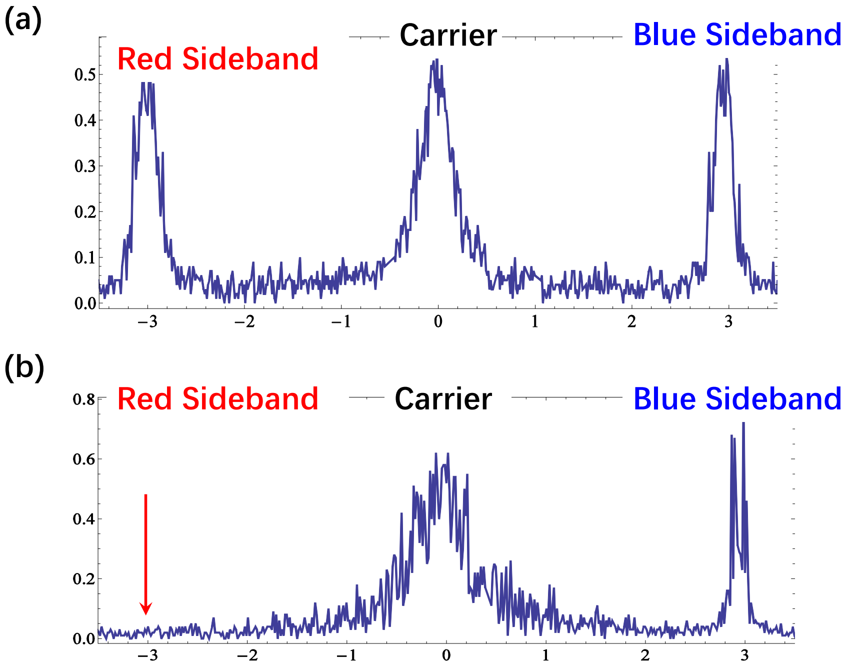


图 2.9　Effect of sideband cooling shown by spectrum. (a) Spectrum before sideband cooling. (b) Spectrum after sideband cooling. Red sideband transition is completely suppressed.

第 3 章 Trapped $^{138}\mathrm{Ba}^{+}$ ion system

3.1 Ionization, doppler cooling, optical pumping, detection

Figure 3.1(a) shows usage of lasers and energy levels of a ^{138}Ba^{+} ion, which has no nuclear spin. The main advantage of using ^{138}Ba^{+} ion is the shelving states in $^{5}D_{5/2}$. When we select two of the zeeman states in $^{5}D_{5/2}$ as $|1\rangle$ and $|2\rangle$ of the qutrit system, the measurement at $|3\rangle$ does not affect them at all.

Similar to ^{171}Yb^{+} , we apply photoionization to load ^{138}Ba^{+} ions. To start the loading procedure, we turn on the current to around 3.5 A to heat up the Barium oven which is located in the same trap, then we shine 413 nm, 493 nm, and 650 nm lasers to the atomic beam. 413 nm laser first excites the atoms from $^{1}S_{0}$ to $^{3}D_{1}$, then 493 nm laser ionizes ^{138}Ba^{+} ions at the trapping zone.

For Doppler cooling procedure, we apply a slightly red-detuned 493 nm laser to cover all the possible cyclic transitions between between $^{6}P_{1/2}$ and $^{6}S_{1/2}$. However, due to the

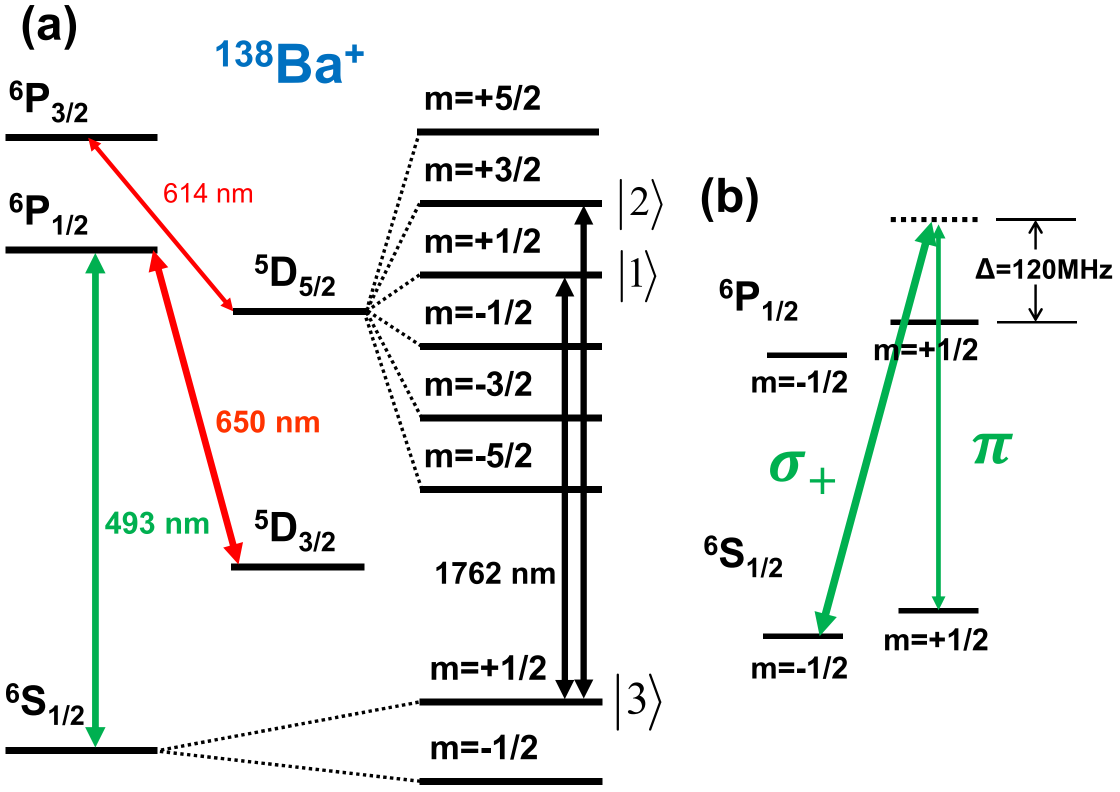


图 3.1 (a) Energy levels of ^{138}Ba^{+} . (b) Structure of EIT cooling.

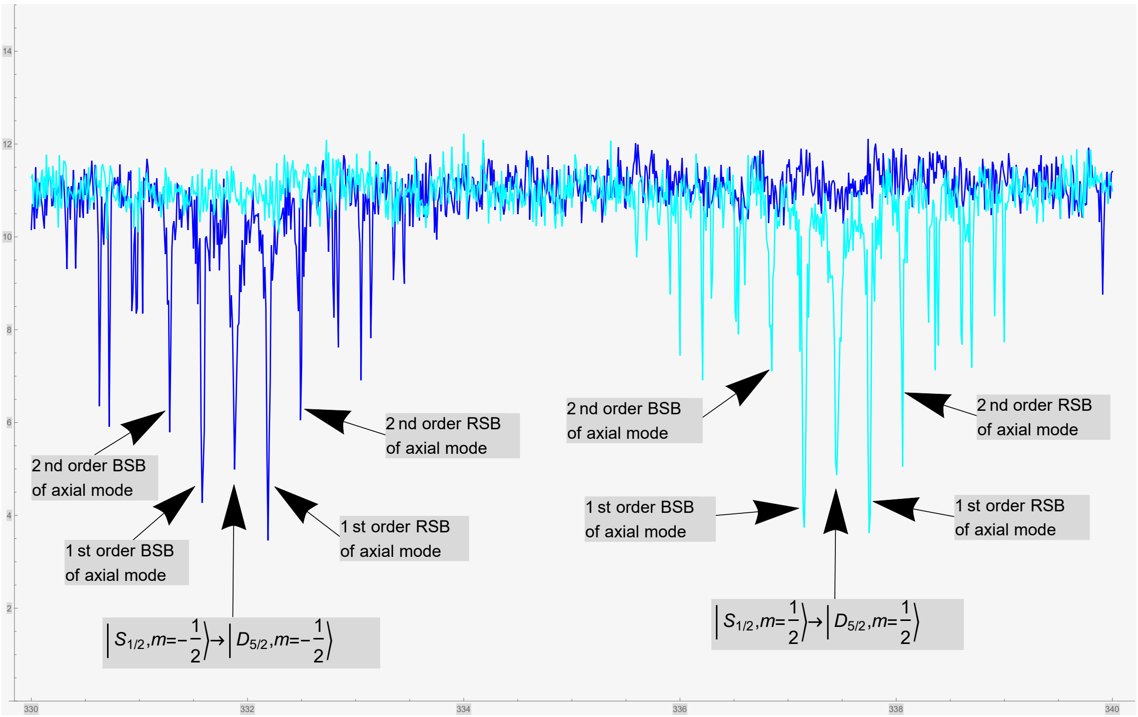


图 3.2 Transitions when we select σ_- polarization (blue) and σ_+ polarization (red) respectively.

25% probability of decay from $^6P_{1/2}$ to $^5D_{3/2}$, a 650 nm laser beam has to turn on all the time to repump from $^5D_{3/2}$ state. Frequency configurations of 493 nm and 650 nm lasers is described in[41]. We need an additional 614 nm laser, which is frequency-doubled from a 1228 nm diode laser with a periodically polarized lithium niobate (PPLN) crystal in real experiment, also has to be applied to repump the from $^5D_{5/2}$ state. The 614 nm laser is locked to the wavelength meter.

Optical pumping is also served as state initialization. Different from ^{171}Yb^{+} , we need to carefully control the polarization of the 493 nm laser beam in order to choose one of the two zeeman sublevels $|m_S = +1/2\rangle$ and $|m_S = -1/2\rangle$ in $^6S_{1/2}$. Figure 3.2 shows the clear difference. Blue line is all the transitions when we select σ_- polarization and initialized to $|m_S = -1/2\rangle$ state, while the red line is the transitions when we select σ_+ polarization and initialized to $|m_S = +1/2\rangle$. When we either of the two polarization, we can clearly suppress the other one. In my experiment, I select σ_+ polarization to initialize the population to $|3\rangle$ state in our qutrit setup.

Besides the typical Doppler cooling, we need another electromagnetically induced transparency (EIT) cooling[42] procedure. EIT cooling is based on a Γ-type three level system (Figure 3.1(b)), it is a coherent population trapping in these three levels. We need to apply a strong pump beam and a weak probe beam at the same time with a common

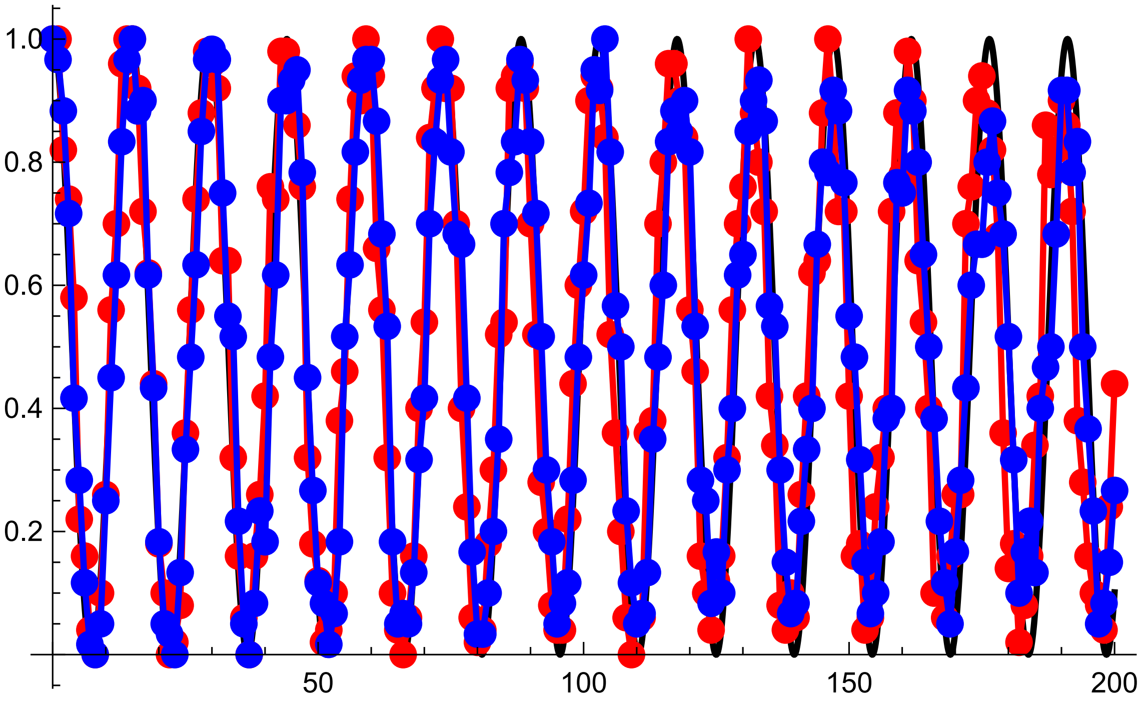


图 3.3　Rabi oscillation of $|S_{1/2}, m = \frac{1}{2}\rangle \longrightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ carrier transition with (red) and without (blue) EIT cooling. Black line is the theoretical line.

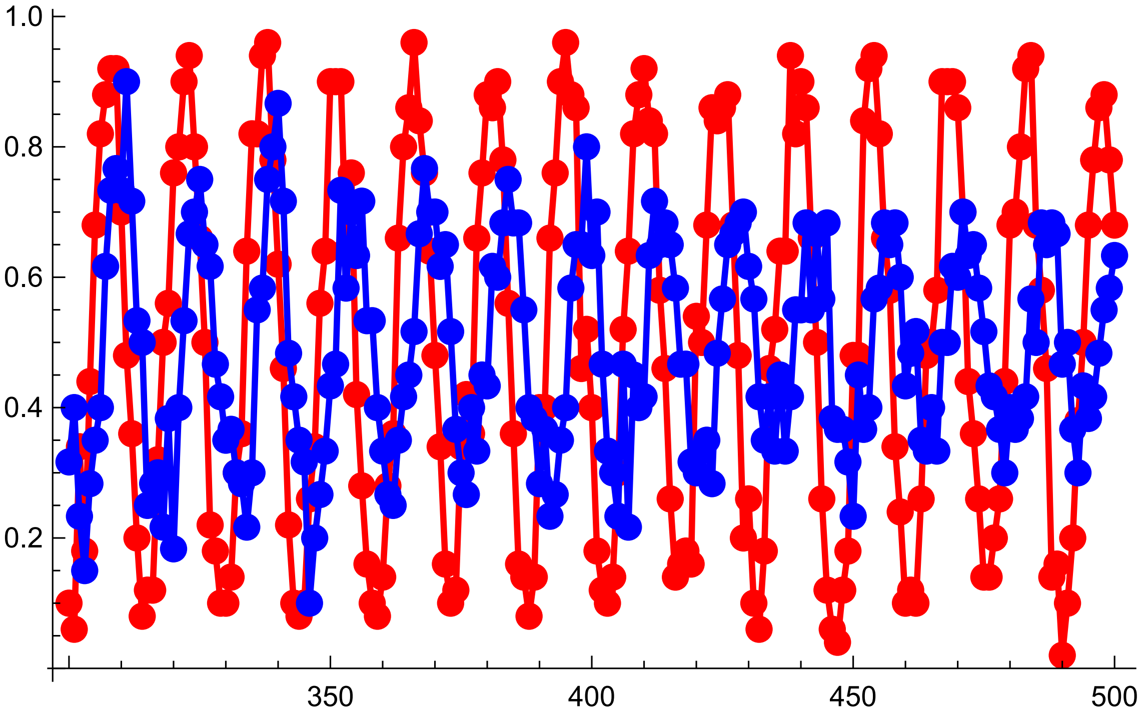


图 3.4　Rabi oscillation of $|S_{1/2}, m = \frac{1}{2}\rangle \longrightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ carrier transition with (red) and without (blue) EIT cooling.

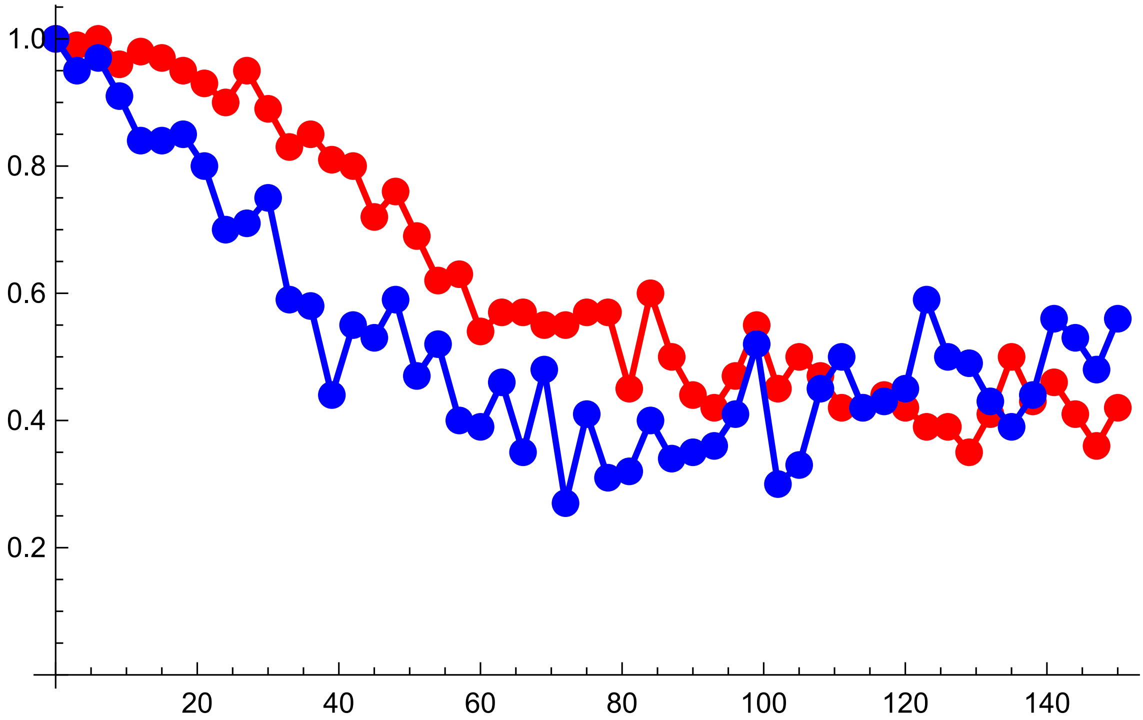


图 3.5 Ramsey measurement of $|S_{1/2}, m = \frac{1}{2}\rangle \rightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ 1st order RSB transition with (red) and without (blue) EIT cooling.

detuning to the upper level. We use optical pumping beam as the strong pump beam, and carefully adjust the power and the frequency of the probe and pump beam by optimizing $|S_{1/2}, m = \frac{1}{2}\rangle \rightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ carrier and RSB transition shown in figure 3.2. After EIT cooling, the cooling limit is much lower than the Doppler cooling. Effect of EIT cooling can be clearly seen in the following figures. Figures 3.4 and 3.3 are rabi oscillation of $|S_{1/2}, m = \frac{1}{2}\rangle \rightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ carrier transition. The advantage of EIT cooling is not obvious in short term (figures 3.3), but clear enough after 300 μs (figures 3.4). We observe the EIT cooling effect by ramsey measurement of the 1st order RSB transition of $|S_{1/2}, m = \frac{1}{2}\rangle \rightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ (figures 3.5).

The detection of the ion is implemented in the same way, we excite the cyclic transitions between $^6P_{1/2}$ and $^6S_{1/2}$ with 493 nm laser to collect the scattered fluorescence photons.

We use a scheme described in Ref.[43,44], which is called modulation transfer spectroscopy (MTS), to stabilize 493 nm and 650 nm laser. The whole stabilization system for 493 nm laser can be seperated to two steps: first narrowing the linewidth of the diode laser by a Fabri-Perot cavity, then stabilizing the cavity by a tellurium (Te_2) vapor cell as the absolute reference with Doppler-free spectroscopy. The method of 650 nm laser

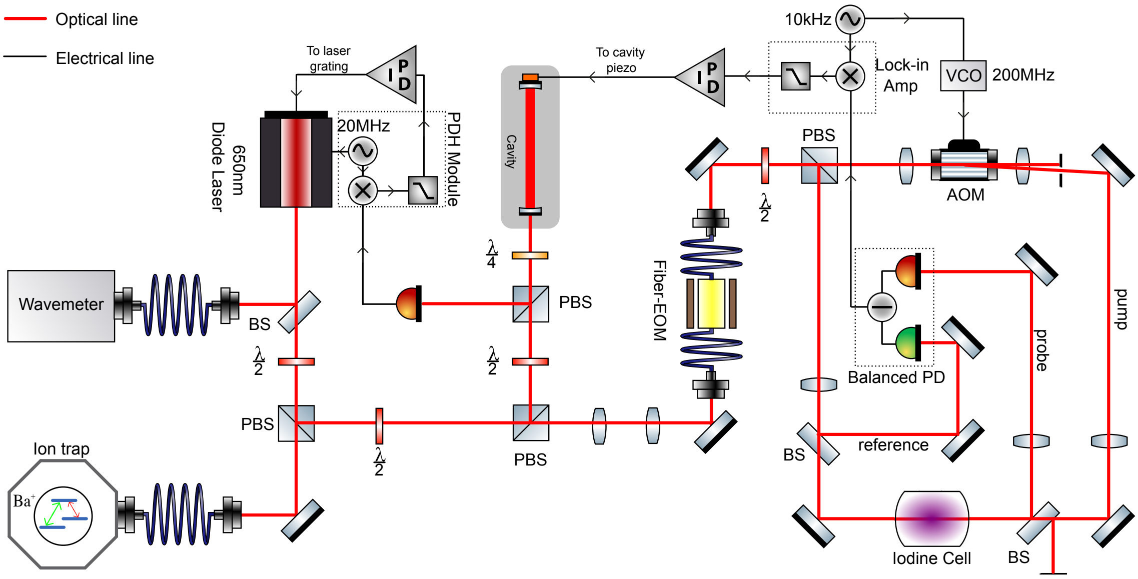


图 3.6　This is figure 1 of ref.[45]. Frequency stabilization system of the 650 nm laser to Te_2 reference through an optical cavity. The thick red lines show the optical path and the thin black lines with arrows indicate electrical connections.

stabilization is the same except using an iodine (I_2) cell. The reason of using a vapor cell is the length drift of the optical cavity due to the temperature fluctuation. Ref.[45] describes the locking system of 650 nm laser, figure 3.6 (figure 1 of ref.[45]) shows the whole stabilization scheme. The output of the 650 nm laser is split into several beams by combination of several beam splitters (BS) and half wave plates (HWP) and polarizing beam splitters (PBS). They go to a wavemeter from HighFinesse, the ion trap for experiment, the optical cavity and finally couple to a specific small optical table for the I_2 setup through a fiber-coupled EOM.

On the I_2 table, the laser beam is again split into two beams using a HWP and a PBS. The transmitted beam passes through an AOM, the 1st order forms a pump beam. The reflected beam is again split into a reference beam which goes to one port of a balanced photodiode (PD) and a probe beam. This stronger modulated pump beam and the weaker probe beam are counter propagating, and pass through a vapor cell heated to around 56°C. The other input of the balanced PD is split from the pump beam, and its output is sent to a lock-in amplifier.

The basic idea of Doppler-free spectroscopy production is that, a single laser beam produces a doppler broadened absorption spectrum when it is tuned to the right resonant frequency of the atoms. With two laser beams tuned to the same resonant frequency, the doppler free dips could be observed in the doppler broadened absorption spectrum

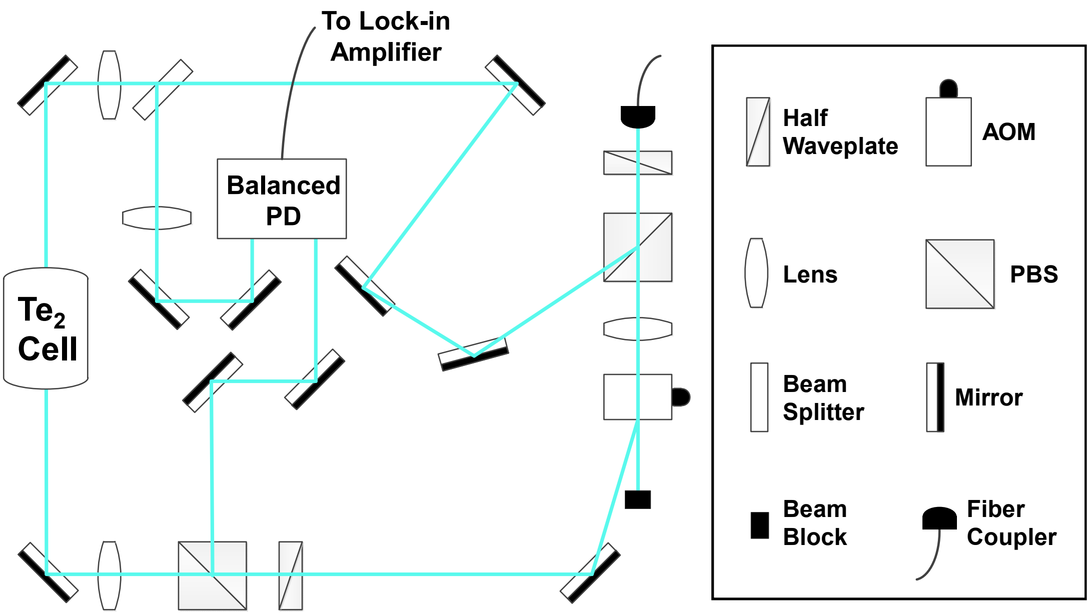


图 3.7　Frequency stabilization system of the 493 nm laser to Te_2 reference. The cyan lines show the optical path and the black line indicates electrical connections from the balanced PD to lock-in amplifier.

corresponding to the frequency of the transitions. In order to implement Doppler free Spectroscopy, we use a voltage-controlled oscillator (VCO) which scans from 190–210 MHz at a scanning frequency of 10 kHz to modulate the AOM for the pump beam. This 10 kHz is also used as the reference for the lock-in amplifier. VCO signal is processed by a servo PID board to stabilize the cavity length by the piezo voltage control. The linewidth of the laser frequency is obtained by recording the Pound–Drever–Hall (PDH) signal after locking and converting its standard deviation to frequency. We choose a proper peak from all the zero-crossing dispersive error signals as the absolute reference according to the ^{138}Ba^{+} ion spectroscopy.

Locking system of 493 nm laser is same to that of 650 nm laser except using a Te_2 vapor cell which perform Doppler-free spectroscopy at around 600°C. The 1st part beam paths including going into the wavelength meter and the optical cavity and the trap can be referred to Figure 3.2 of[41]. The 2nd part beam paths of Te_2 spectroscopy on the specific optical table are shown in Figure 3.7, which is almost identical to 650 nm I_2 table.

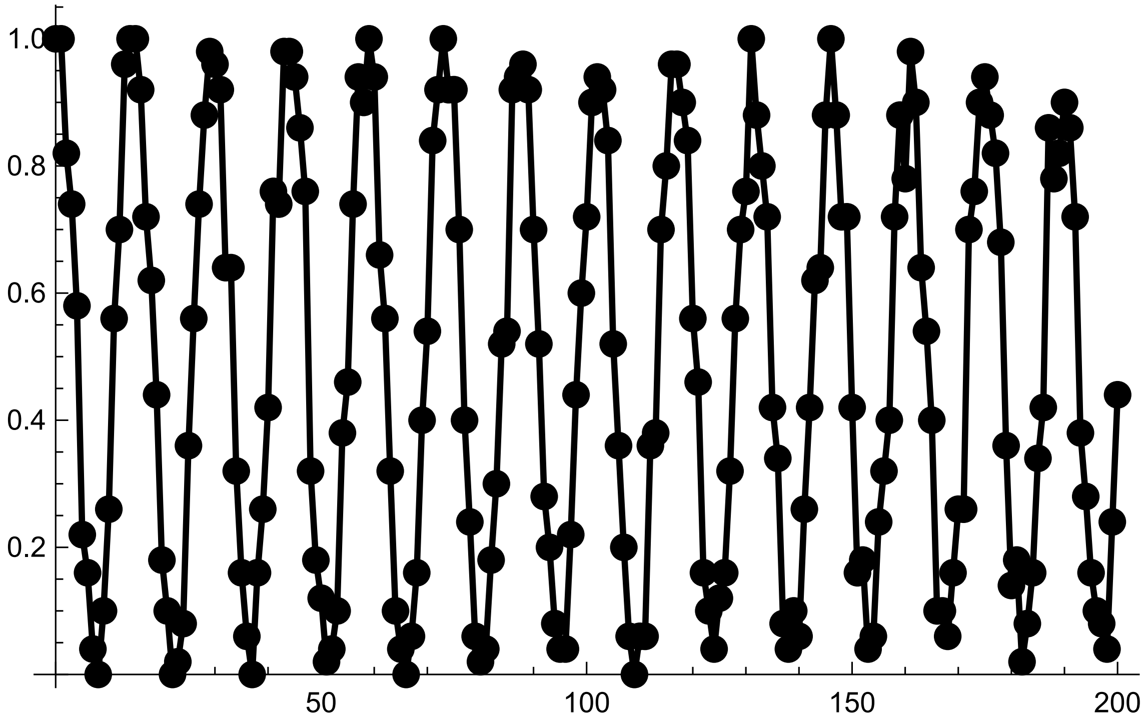


图 3.8　Rabi oscillation of $|1\rangle \leftrightarrow |3\rangle$ by 1762 nm quadrupole transition.

3.2 Quantum manipulation with 1762 nm laser

The operations between $|1\rangle \leftrightarrow |3\rangle\,(\Delta m = 0)$ and $|2\rangle \leftrightarrow |3\rangle\,(\Delta m = 1)$ of the qutrit system are realized by electric quadrupole transition. This electric quadrupole transition couples transitions with $\Delta m \leq 2$ among 2 Zeeman sublevels in $^6S_{1/2}$ and 6 Zeeman sublevels in $^5D_{5/2}$ as figure 3.1(a) shows.

The laser for quadrupole transition is a narrow linewidth 1762 nm fiber laser. It is locked to an ultra-low expansion (ULE) cavity system at around 1 Hz. Before going into the trap, we use a boosted optical amplifier (BOA) to amplify the stabilized laser. Figure 3.8 shows rabi oscillation of $|1\rangle \leftrightarrow |3\rangle$ transition.

3.3 Coherence time

In the randomness expansion experiment, we have two detections, the first one is 600 μs and the second 300 μs. Considering other operations, the coherence time of the qutrit system has to exceed at least 1000 μs. To ensure long enough coherence time, we add spin echo pulses during detection procedure, which is a π-pulse of $|2\rangle \leftrightarrow |3\rangle$ transition, then a π-pulse of $|1\rangle \leftrightarrow |3\rangle$ transition, followed by a π-pulse of $|2\rangle \leftrightarrow |3\rangle$ transition (Figure 3.9). Figure 3.10 shows the ramsey measurement between $|1\rangle \leftrightarrow |3\rangle$, Figure 3.11 shows the ramsey measurement between $|2\rangle \leftrightarrow |3\rangle$. The coherence time could be even longer

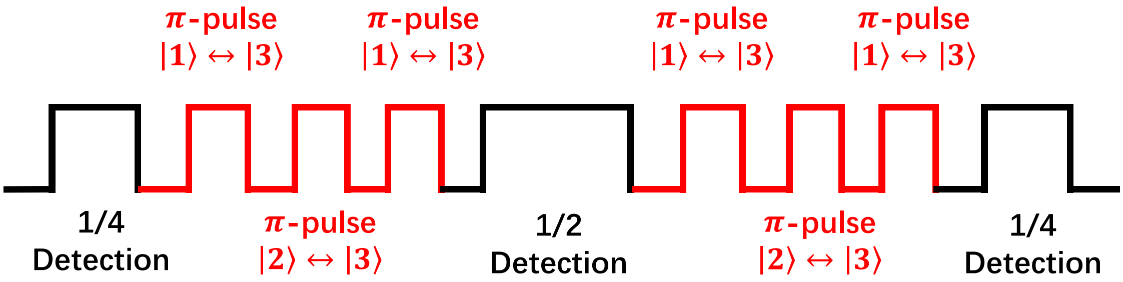


图 3.9　Schematic of spin echo pulses during the detection.

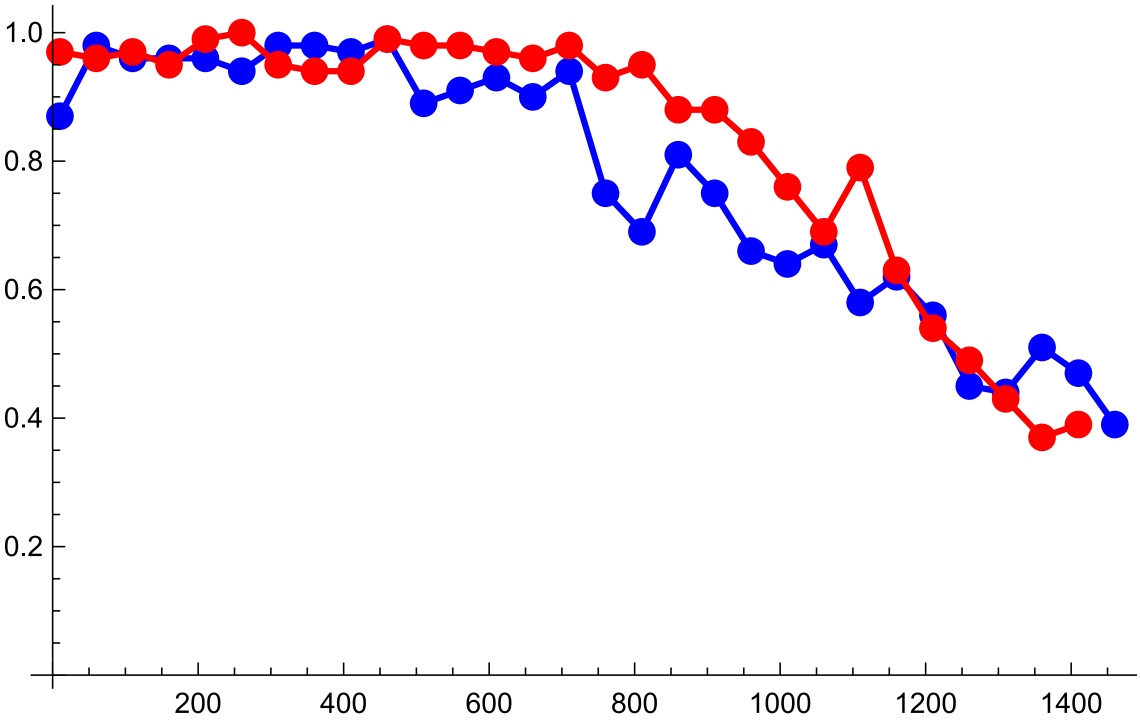


图 3.10　Ramsey measurement of $|1\rangle \leftrightarrow |2\rangle$ transition with (red) and without (blue) EIT cooling.

when we apply a line trigger[46] to the pulse sequencer. But line trigger makes the whole experiment speed much slower, and coherence time without line trigger is already long enough for the randomness expansion experiment.

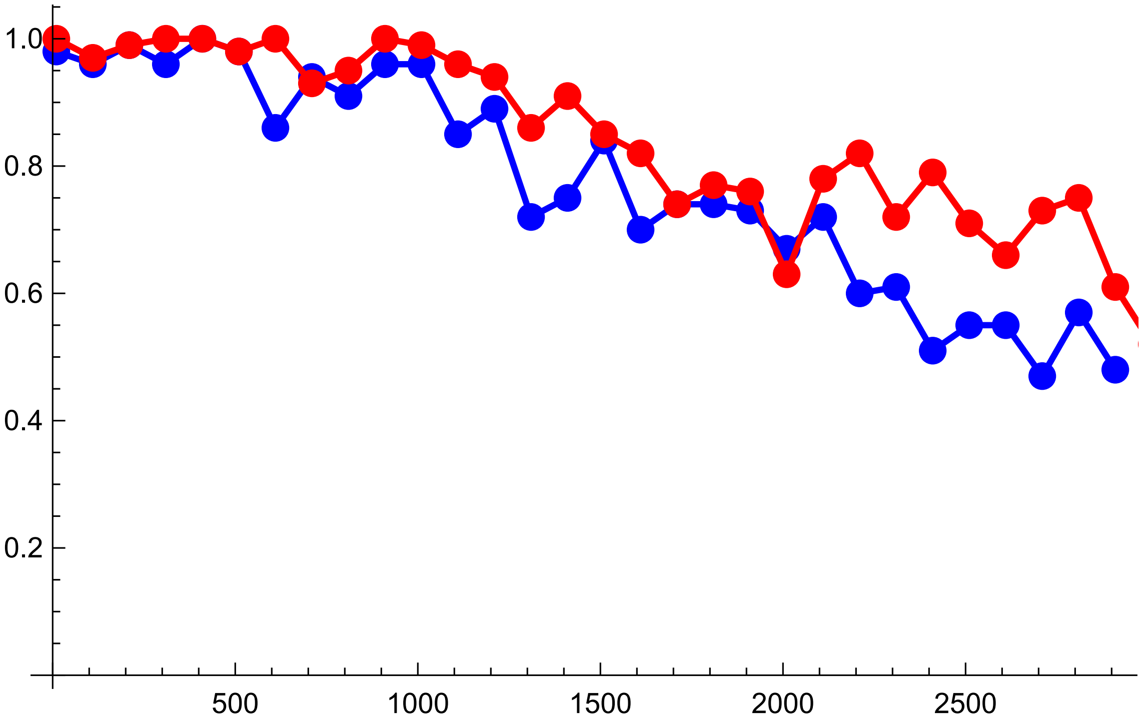


图 3.11　Ramsey measurement of $|1\rangle \leftrightarrow |3\rangle$ transition with (red) and without (blue) EIT cooling.

第 4 章　Phonon arithmetics with a trapped $^{171}\mathrm{Yb}^+$ ion

4.1　Definition of conventional arithmetics

In quantum-mechanics, creation $\hat{a}^\dagger$ and annihilation $\hat{a}$ operators in Eq. (2-4) can be rewritten as the following form, which bear the operator relations (2-4) can be rewritten as

$$\hat{a}^\dagger = \sum_{n=0} \sqrt{n+1}\,|n+1\rangle\langle n|, \quad \hat{a} = \sum_{n=0} \sqrt{n}\,|n-1\rangle\langle n|. \tag{4-1}$$

To implement creation, a π-pulse of blue sideband transition followed by a π-pulse of carrier transition will map the ion from $|\downarrow, 0\rangle \to |\uparrow, 1\rangle \to |\downarrow, 1\rangle$, thus increases the phonon number by one. This scheme can be applied for any vibrational number state $|\downarrow, n\rangle$, but the π-pulse period of blue sideband transition changes on the dependency of n, which makes it difficult to simultaneously apply exact π-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 π-pulse of carrier transition followed then a π-pulse of blue sideband transition. Furthermore, the creation and annihilation operators $\hat{a}^\dagger$ and $\hat{a}$ do not simply add and subtract phonons, but also bring modification to the state amplitudes with $\sqrt{n}$ factors. The proportionality factors $\sqrt{n+1}$ and $\sqrt{n}$ appear due to the symmetric indistinguishable nature of bosons[47]. Therefore, pure arithmetics independent of phonon number n, actually bare addition and subtraction of phonons, are required besides the creation $\hat{a}^\dagger$ and annihilation $\hat{a}$.

The conventional addition and subtraction of a particle can be written as

$$\hat{S}^+ = \sum_{n=0} |n+1\rangle\langle n|, \quad \hat{S}^- = \sum_{n=1} |n-1\rangle\langle n|, \tag{4-2}$$

where $|n\rangle$ stands for a Fock state of n bosons. $\hat{S}^+$ takes the n-particle state to the $(n+1)$ state representing an addition, while the subtraction operation, $\hat{S}^-$, brings the n state to the $(n-1)$ state without $\sqrt{n}$ dependency. These operations correspond to conventional arithmetic which is commonly used in everyday life but they do not come out naturally in quantum mechanics.

As seen from the operations in Eq. (4-2), $\hat{S}^+$ is a deterministic process while $\hat{S}^-$ may not be, as it is not possible to subtract a particle from vacuum $|0\rangle$. When the vacuum component of the initial state is small, the subtraction can be done near-deterministically. In recent times, there have been theoretical proposals of the operations (4-2) for the generation of an arbitrary quantum state[48], the measurement of vacuum[49], the transformation to a non-classical state[50] and the amplification of a quantum state[51]. In particular, such arithmetic operations form an important component of a qubit gate operation for ions in a harmonic potential[52]. The operations (4-2) were also suggested as the elements of a phase operator[53]. Beyond the quantum-state engineering, the subtraction can be used for the sub-Doppler cooling in the trapped ion system[54].

While the quantum operators (4-1) have been experimentally demonstrated[55–61], the realization of the conventional operations (4-2) is still to be attested in the quantum regime. Indeed, the $\hat{S}^+$ and $\hat{S}^-$ operators were suggested as the elements of a phase operator by Susskind and Glogower[53]. Thus realization of such operations would serve as an important stepping stone to study the properties of the Susskind-Glogower phase operator experimentally. In this paper, we demonstrate the operations in a near deterministic manner, also showing that the technique is a resource to create non-Gaussian states efficiently[49,50]. We show that classical states are turned into nonclassical ones manifesting highly sub-Poissonian photon statistics and negativity in the Wigner function. The versatility of the operations for quantum state engineering is demonstrated by various sequences of the single-phonon operations. This is contrasted to the bosonic operations realized so far[55–61]. Their success probability is intrinsically low, since the higher the fidelity of the operations, the lower the success rate; hence a repetition of such the operations is practically limited.

In my research, we experimentally demonstrate deterministic addition and near-deterministic subtraction of a bosonic particle, in particular, a phonon of a ^{171}Yb$^+$ ion trapped in a harmonic potential. We realize the operations by coupling phonons to an auxiliary two-level system, so called, the hybrid scheme of discrete and continuous variable[62] and applying a transitionless quantum driving scheme. We perform the operations on superpositions of Fock states and coherent states and we demonstrate that our single-phonon operations are (near) deterministic and preserve coherence. By applying a sequence of operations deterministically, we show that classical states are turned into nonclassical ones manifesting highly sub-Poissonian statistics and negativity in the Wigner function.

4.2 Rapid Adiabatic Transition Process

We implement the $\hat{S}^{+}$ and $\hat{S}^{-}$ operations of (4-2) on a vibrational mode of frequency ω_{X} for a single trapped ^{171}Yb^{+} ion in a three-dimensional harmonic potential[63] through its interaction with the two-level system of atomic energy levels. The harmonic potential is generated by an oscillating electric field in the radial axis with trap frequency $\omega_{\mathrm{X}} = (2\pi)2.8$ MHz. The two-level system is represented by two hyperfine states $|F = 1, m_F = 0\rangle \equiv |\uparrow\rangle$ and $|F = 0, m_F = 0\rangle \equiv |\downarrow\rangle$ of the $S_{1/2}$ manifold with the transition frequency $\omega_{\mathrm{HF}} = (2\pi)12.6428$ GHz. As shown in Figure 4.1(a), the anti-Jaynes-Cummings (aJC) interaction or blue-sideband transition, $H_{\mathrm{aJC}} = \frac{\eta\Omega}{2}\hat{a}^{\dagger}\hat{\sigma}_{+}e^{i\Delta t} + \mathrm{h.c.}$, is realized by the stimulated Raman laser beams with beat-note frequency $(\omega_{\mathrm{R1}} - \omega_{\mathrm{R2}}) = (\omega_{\mathrm{HF}} + \omega_{\mathrm{X}}) + \Delta$. Here, Ω is the Rabi frequency of the two-level system, $\eta = \Delta k\sqrt{\hbar/2M\omega_{\mathrm{X}}}$ the Lamb-Dicke parameter, Δk the net wave-vector of the Raman laser beams and M the mass of ^{171}Yb^{+} ion. The aJC coupling produces the transition between $|\downarrow, n\rangle$ and $|\uparrow, n+1\rangle$ with the oscillation frequency of $\sqrt{n+1}\eta\Omega$, where the $\sqrt{n+1}$ factor comes from the fundamental property of $\hat{a}^{\dagger}$ and $\hat{a}$ operators in (4-1). Therefore, the application of the simple aJC interaction does not transfer $|\downarrow, n\rangle$ to $|\uparrow, n+1\rangle$ in an n-independent manner at a fixed duration of time.

The full population transfer independent of the initial motion state, the uniform blue-sideband transition, $\sum_{n=0} |\uparrow, n+1\rangle \langle\downarrow, n| + \mathrm{h.c.}$, can be obtained by the application of the stimulated Raman adiabatic passage[65–67]. The adiabatic scheme provides a robust transfer against the variations in the transition rate either from the intensity change of the control Raman beams or from the property of the transitions[66]. Therefore, a properly designed adiabatic passage would allow a decent state transfer for a wide range of phonon number states through the aJC interaction, despite the $\sqrt{n+1}\eta\Omega$ dependence, as shown in Figure 4.2(a)(c). In the adiabatic passage, typically $\eta\Omega$ slowly increases at the beginning and decreases at the end, $i.e$, $\Omega(t) = \Omega_0 \sin(\pi t/T)$, while the detuning Δ changes according to $\Delta(t) = \Delta_0 \cos(\pi t/T)$, where T is the total transfer time, across the resonance. For the applicability of the scheme to a wide range range of initial phonon numbers with high fidelity, however, we should set Δ_0 as high as $\sqrt{n_{\mathrm{M}}+1}\eta\Omega_0/2$, where n_{M} is the largest phonon number for the transfer and should fulfill the adiabatic condition, $T \gg 1/\eta\Omega_0$. In our experimental conditions, the reasonable duration T for such the adiabatic transfer is around 21 times of π-pulse duration for the blue-sideband transition of the ground state,

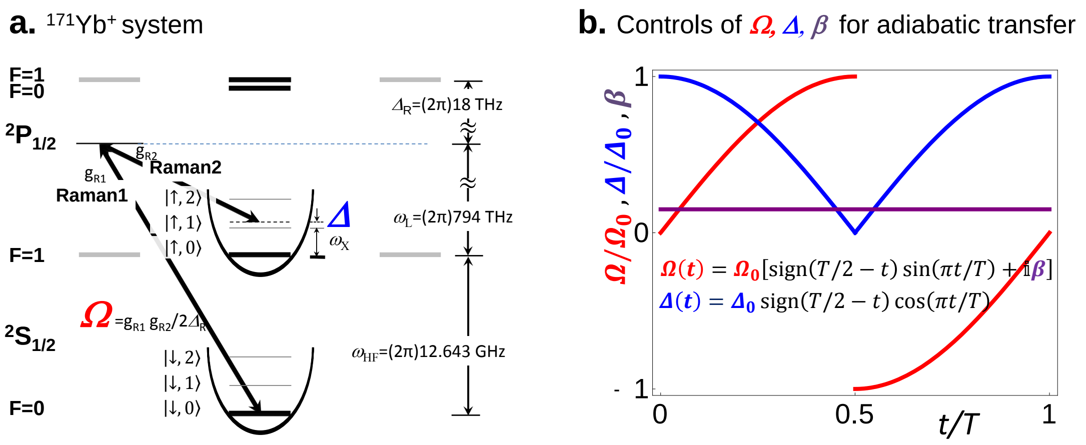
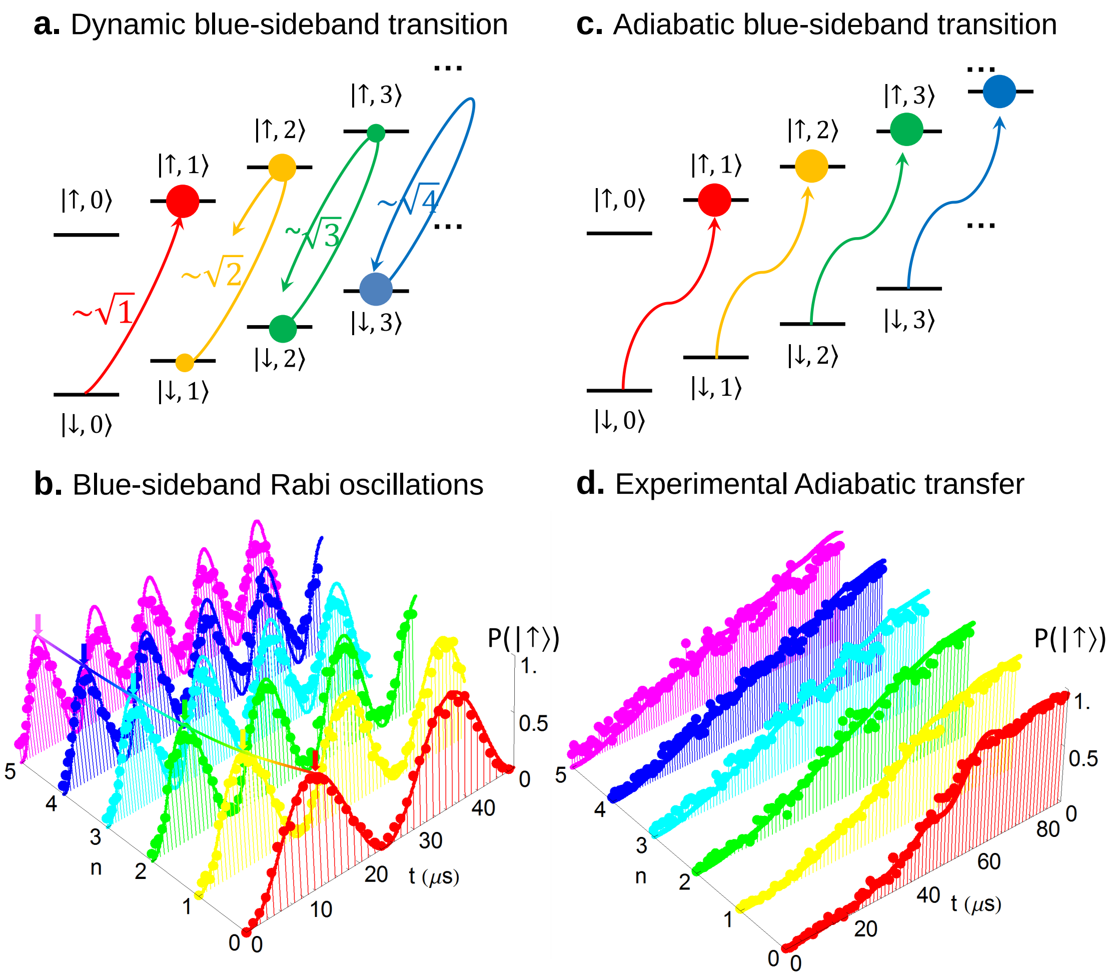


图 4.1　Experimental scheme and parameter control. (a) ^{171}Yb^{+} system in a harmonic potential. The qubit level in $S_{1/2}$ manifold, $|F=0,m_F=0\rangle \equiv |\downarrow\rangle$ and $|F=1,m_F=0\rangle \equiv |\uparrow\rangle$ are coupled by the Raman laser beams, where the beat-note frequency is near resonant to the qubit levels, ω_{HF}. When the beat-note frequency is tuned to $\sim \omega_{\mathrm{HF}}+\omega_{\mathrm{X}}$, the scheme produces the anti-Jaynes-Cummings interaction or blue-sideband transition. We denote Ω as the Rabi-frequency on the qubit transition and the Δ is the frequency difference between the beat-note frequency of Raman beams and $\omega_{\mathrm{HF}}+\omega_{\mathrm{X}}$. The Raman beams are realized by pico-second pulse train similar to the scheme in Ref.[64]. (b) For the adiabatic blue-sideband transition whose frequency is independent of motional quantum number n, Ω and Δ are controlled as the red and blue curves. The phase $i\beta$ in Ω is the counter-diabatic term to suppress the transition during the evolution. Here $\Omega_0=(2\pi)38.5$ kHz, $\beta=0.075$, and $\Delta_0=1.6\Omega_0$.

$\pi/\eta\Omega_0$, when we include up to the maximum phonon number $n_{\mathrm{M}}=6$.

Recently, the transitionless quantum driving scheme[68–71] has been developed to speed up the adiabatic control. When the transfer is non-adiabatic, it introduces an additional term in the Hamiltonian of the instantaneous basis, which is $-i\beta\frac{\eta\Omega(t)}{2}\hat{a}^{\dagger}\hat{\sigma}_{+}e^{i\Delta t}+$ h.c., where β is in the order of $\pi/\eta\Omega_0/2T$, the ratio between the π-pulse duration and the total operation time. By adding a counter-diabatic term in the control, we can suppress the non-adiabatic excitation with a reasonable speed up over the adiabatic passage. For the aJC interaction, the optimal values of Δ_0 and β are dependent on the phonon number n for the given Ω_0. In our experiment, we optimize Δ_0 and β for the case of the geometric average of the minimum and maximum phonon number, $n_{\mathrm{O}}=\sqrt{1\times(n_{\mathrm{M}}+1)}$. By doing this, we are able to reduce the total duration of the operation from 21 to 7 times $\pi/\eta\Omega_0$ without sacrificing the fidelity of the rapid adiabatic passage for the same range of phonons $n_{\mathrm{M}}=6$. Figures 4.2(b)(d) show the experimental results and difference of the aJC interaction and the rapid adiabatic passage. Figure 4.3 shows the traces of the rapid adiabatic passage for different phonon number n on a bloch sphere.



a. Dynamic blue-sideband transition

c. Adiabatic blue-sideband transition

b. Blue-sideband Rabi oscillations

d. Experimental Adiabatic transfer

图 4.2　Experimental scheme and dynamic and adiabatic transition by anti-Jaynes-Cummings (blue-sideband) interaction. (a) The diagram for the standard blue-sideband transition. The Hilbert space is composed of the qubit states, $|\uparrow\rangle$and $|\downarrow\rangle$, and phonon states of n excitations, $|n\rangle$. The transition rate of the blue-sideband interaction between $|\uparrow, n\rangle$ and $|\downarrow, n-1\rangle$ depends on n; the higher the n value, the more frequent the transition is. The transitions between $|\downarrow, n\rangle$ and $|\uparrow, n+1\rangle$ would experience evolutions $\sqrt{n+1}$ times faster than the transition between $|\downarrow, 0\rangle$ to $|\uparrow, 1\rangle$. (b) Probability of finding the ion in $|\uparrow, n\rangle$ state as a function of time. We see that the transition frequency clearly manifests $\sqrt{n+1}$-dependence. The arrow at the first peak of each oscillation indicates the duration of a π-pulse for the corresponding transition. The π-pulse duration, T_π, of the fundamental blue-sideband transition (red) is 13 μs. The dots represent experimental data and solid lines are from the fitting to $\sin^2\left(\frac{\sqrt{n+1}\pi}{2T_\pi}t\right)$. (c) The conceptual diagram for the adiabatic blue-sideband transition without the $\sqrt{n+1}$-dependence. (d) The experimental demonstration of the adiabatic blue-sideband transitions realized by the transitionless quantum driving. The total time to execute the transitions is 91μs for any $|n\rangle$, which is about 7 times T_π.

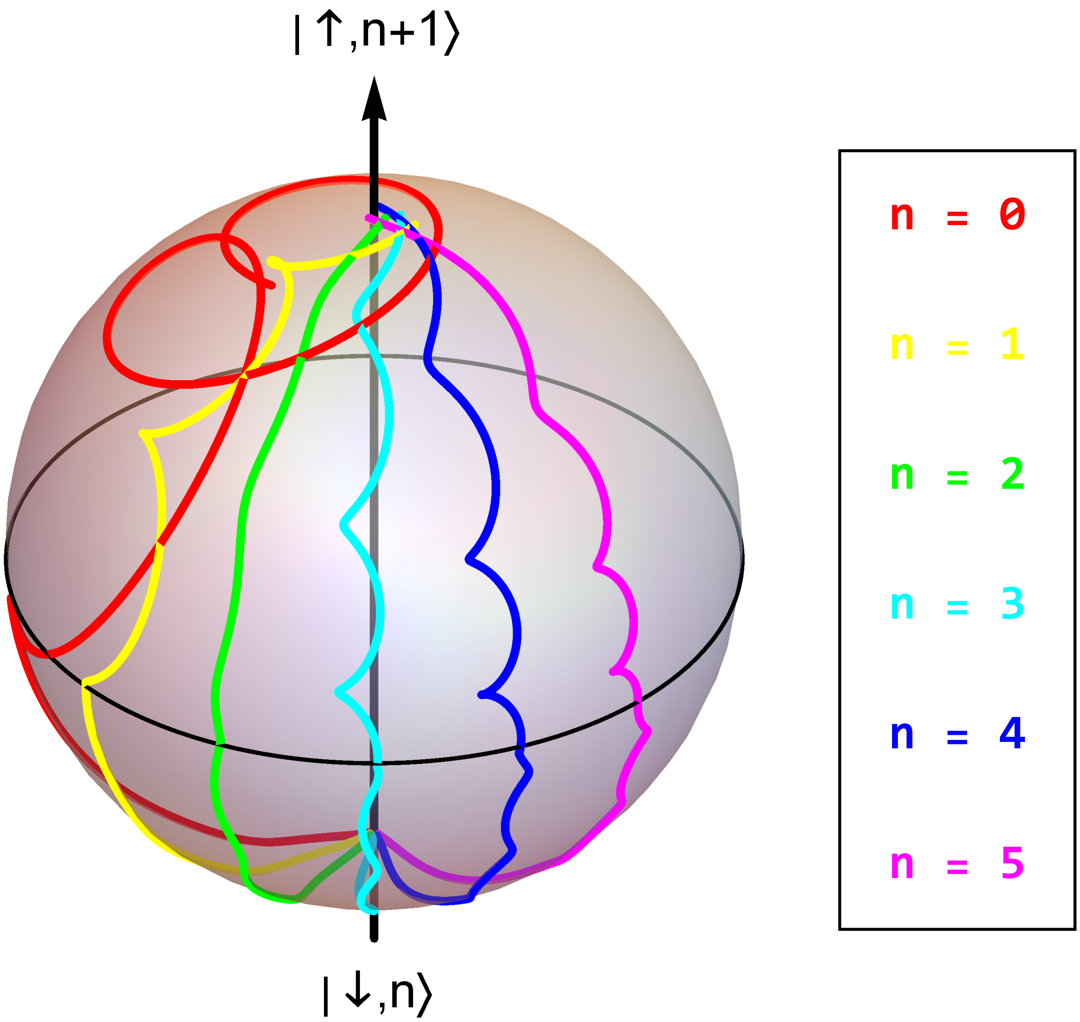


图 4.3　The rapid adiabatic passage traces for phonon number $n = 0$ to 5 respectively on a bloch sphere.

In order to rigorously achieve the uniform blue-sideband operation $\sum |\uparrow, n+1\rangle\langle\downarrow, n| +$ h.c., it is important not only to increase the phonon number but also to preserve the relative phases between component states of the quantum state. For our previous realization[63], the different extra phases were accumulated depending on the phonon number of the initial state which prevented from keeping the initial phase coherences. In our work, we have developed a sequence of operations compensating the phonon-number dependent phases based on the spin-echo principle. As shown in Figure 4.1(b), we invert the sign of Ω and reverse the control of Δ in the middle of the sequence of the operation, which symmetrizes the whole operation and produces the accumulated phases of opposite signs before and after the inversion and reverse. Therefore, the total phases are canceled out at the end of the operation.

The AC Stark shift in the adiabatic operations mainly come from the off-resonant coupling to the carrier transition, the transition between $S_{1/2} \leftrightarrow P_{1/2}$ states of ^{171}Yb^{+} ion, and the other radial motional mode ($\omega_{\mathrm{Y}} \approx \omega_{\mathrm{X}} + (2\pi)0.4$ MHz). The dominant AC stark shift comes from the carrier transition of frequency $\frac{\Omega_0^2}{2\omega_{\mathrm{X}}\eta^2} \sim (2\pi)33$ kHz with $\Omega_0 = (2\pi)38.5$ kHz and the Lamb-Dicke parameter $\eta = 0.089$. The amount of the shift brought by the Y mode is given by $\frac{\Omega_{0\mathrm{Y}}^2}{2(\omega_{\mathrm{Y}}-\omega_{\mathrm{X}})}$ that is about 20 times smaller than that from the carrier coupling. The AC stark shift between qubit states from the Raman laser beams due to $S_{1/2} \leftrightarrow P_{1/2}$ transition is $\frac{g_{R1}^2+g_{R2}^2}{2\Delta_R}\frac{\omega_{\mathrm{HF}}}{\Delta_R} \sim (2\pi)1$ kHz, where g_{R1} and g_{R2} are the coupling strengths of Raman 1 and Raman 2 beams, respectively and the $\Delta_R = (2\pi)$ 18 THz is the detuning from the level of $^2P_{1/2}$.

We consider total AC stark shift as the form of $\frac{|\Omega(t)|^2}{2\Delta_{\mathrm{total}}}$, where Δ_{total} is the detuning effectively including all the possible origin of AC stark shifts discussed above. We obtain $\omega_{\mathrm{bsb}}^{\mathrm{org}}$ and Δ_{total} by fitting the several points of $\{\omega_{\mathrm{bsb}}^{\mathrm{act}}, \Omega_{\mathrm{bsb}}\}$ with the equation $\omega_{\mathrm{bsb}}^{\mathrm{act}} = \omega_{\mathrm{bsb}}^{\mathrm{org}} + \frac{\Omega_{\mathrm{bsb}}^2}{2\Delta_{\mathrm{total}}}$. The actual frequency of blue-sideband $\omega_{\mathrm{bsb}}^{\mathrm{act}}$ is measured by observing the resonant excitation. Including the AC stark shift, the actual waveform of $\Omega(t)$ that we apply on our arbitrary waveform generator is as follows.

$$
\begin{aligned}
\Omega(t) &= \Omega_0\left[\sin(\pi t/T)\cos\left(\phi(t)\right) - \beta\sin\left(\phi(t)\right)\right], \\
\phi(t) &= \int_0^t \left\{\omega_{\mathrm{bsb}}^{\mathrm{act}}(t') + \Delta(t')\right\} dt'.
\end{aligned}
\tag{4-3}
$$

Here $\Delta(t') = \Delta_0\cos(\pi t/T)$ and we note that the imaginary part in original form of $\Omega(t) = \Omega_0\left[\sin(\pi t/T) + i\beta\right]$ is changed to sin-wave which has the $\frac{\pi}{2}$ phase difference.

Here, $\phi(t)$ is calculated as follows,

$$\begin{aligned}
\phi(t) &= \int_0^t \left\{\omega_{\mathrm{bsb}}^{\mathrm{act}} + \Delta(t')\right\} dt' = \int_0^t \left\{\omega_{\mathrm{bsb}}^{\mathrm{org}} + \frac{|\Omega(t)|^2}{2\Delta_{\mathrm{total}}} + \Delta_0 \cos(\pi t/T)\right\} dt' && \text{(4-4)}\\
&= \omega_{\mathrm{bsb}}^{\mathrm{org}} t + \frac{\Omega_0^2}{2\Delta_{\mathrm{total}}} \int_0^t \left\{\sin^2(\pi t/T) + \beta^2\right\} dt' + \Delta_0 \frac{T}{\pi} \sin(\pi t/T) && \text{(4-5)}\\
&= \omega_{\mathrm{bsb}}^{\mathrm{org}} t + \frac{\Omega_0^2}{4\Delta_{\mathrm{total}}} \left[(1 + 2\beta^2)t + \frac{T}{2\pi} \sin(2\pi t/T)\right] + \Delta_0 \frac{T}{\pi} \sin(\pi t/T). && \text{(4-6)}
\end{aligned}$$

4.3 Experimental setup

The laser source of the Raman transition is a Coherent Mira 900 mode-locked Titanium:Sapphire (Ti:S) laser (Figure 4.4) 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 2.2 W 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 166th and 167th which is closest to ω_{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 RF source which provide frequency modulation(FM). Finally, the stabilized frequency is applied to the Acousto-Optic Modulator (AOM1 in Figure 4.5) 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.

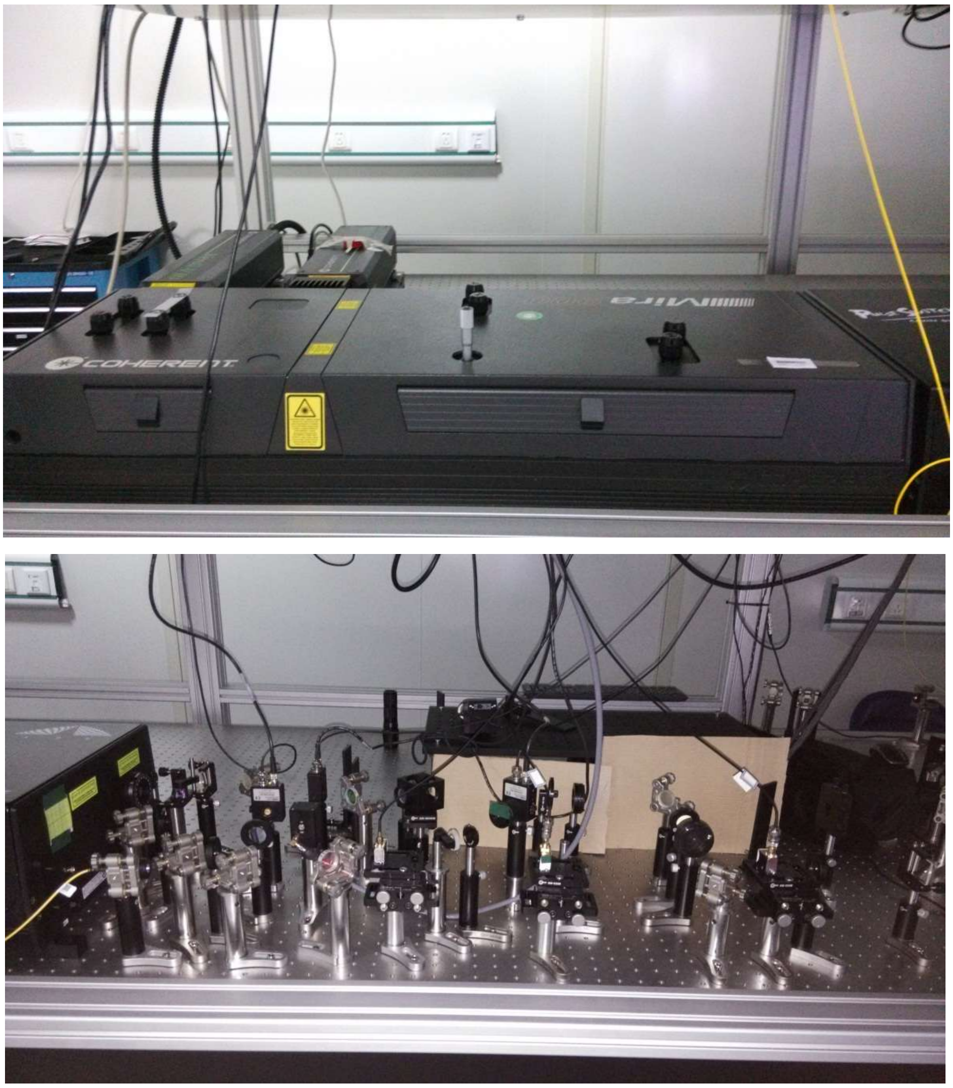


图 4.4　Coherent Mira 900 laser and beam path.

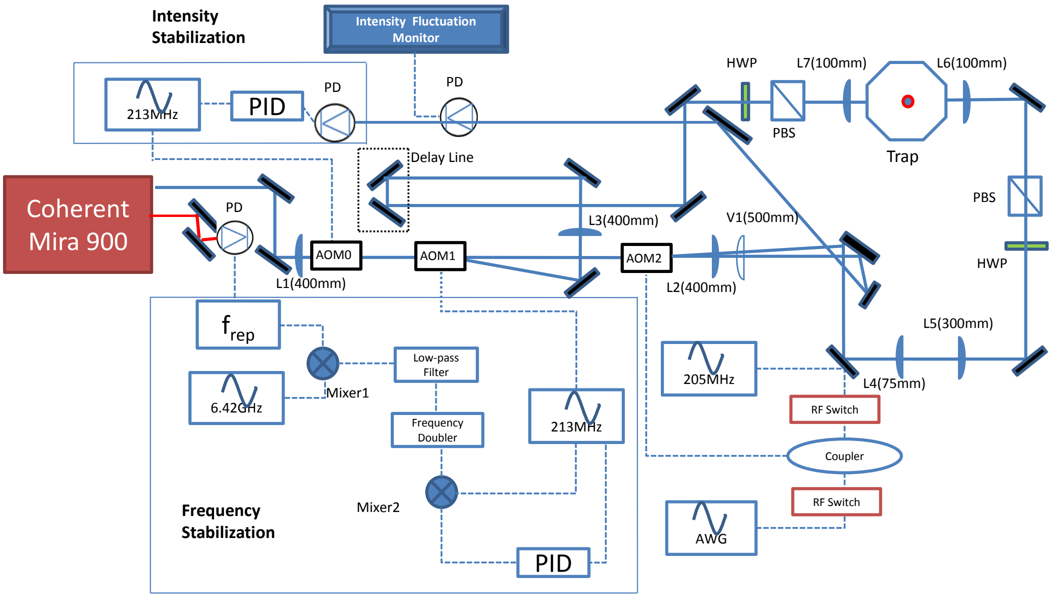


图 4.5 Setup of the Raman beams. The schematics of the Raman set up optics with Coherent Mira 900. Raman1 and Raman2 are separated by AOM1, they are the first order of AOM1 and AOM2, respectively. Intensity stabilization is applied using the zeroth order of AOM2 then feedback to AOM0. The output of frequency stabilization system feedback to AOM1. The 756 nm laser shown in red is used to monitor the repetition rate and stabilize the frequency. The spherical lenses are shown in blue and the vertical cylindrical lens is in white.

The laser is first focused at AOM1 position with a 400mm lens (L1), L2 and L3 with the same focal length collimate Raman1 and Raman2 respectively. A vertical cylindrical lens V1 converges the height. 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 AOM2 to the image of AOM1 in the trap is lowered to 0.2 mm which is close enough to keep both the strength of the transition and convergency of the laser alignment with various frequencies.

4.4 Reconstruction of density matrix and wigner function measurement

We use an iterative algorithm proposed in Ref.[72] for the reconstruction of an unknown state. It consists of a maximum-likelihood estimation solved by expectation-maximization algorithm followed by a unitary transformation of the eigenbasis of the density matrix ρ. The density matrix is reconstructed by using the iterative maximum-likelihood algorithm[72] on the phonon number distributions for eight different angles as shown in Figure 4.6. The relation of displacement amount and duration in our experiment is depicted in Figure 4.7, the direction of displacement is achieved by controling the phase. We refer to this comparison for deciding displacement duration both for reconstructing density matrix and preparing initial coherent states for addition, subtraction and commutation relation tests.

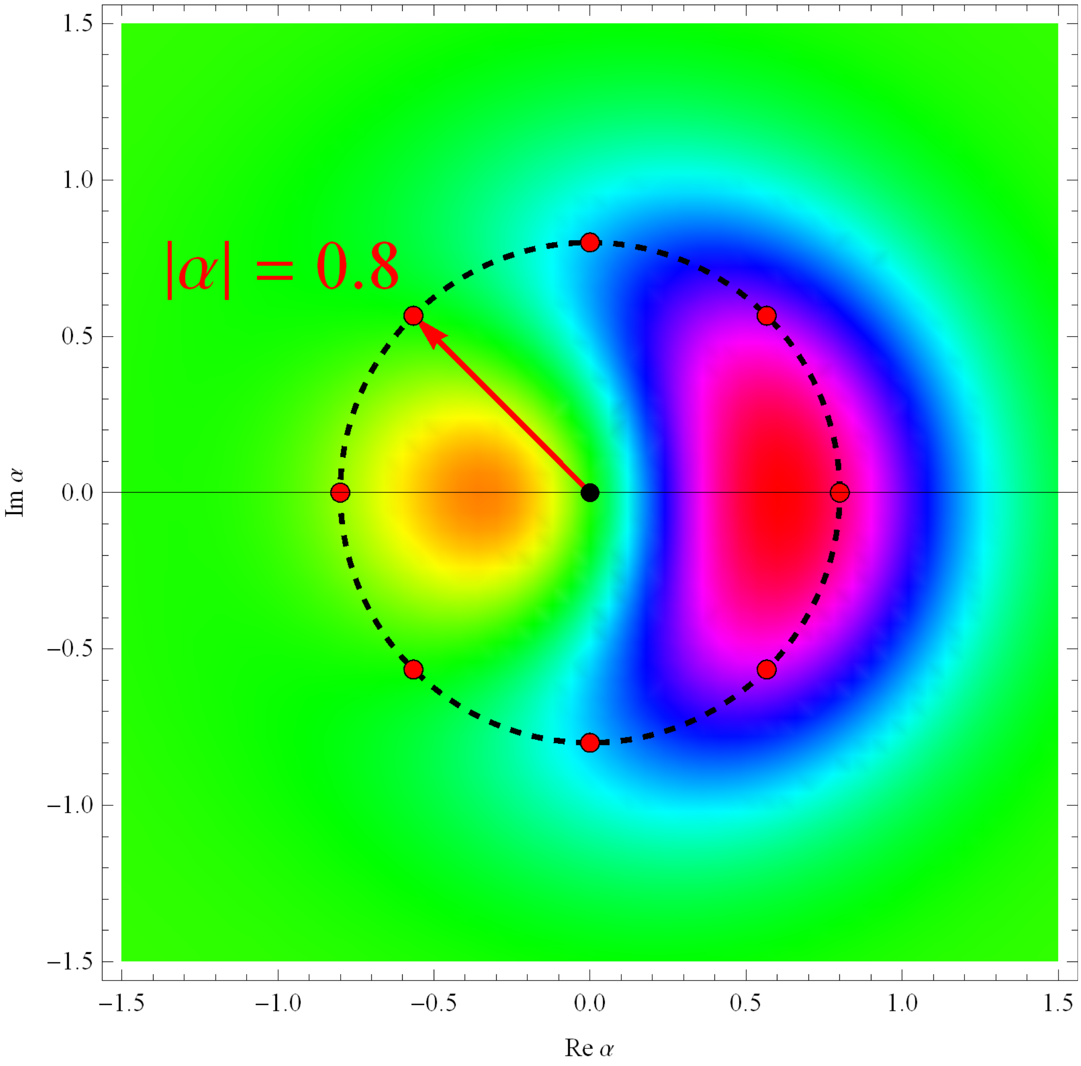


图 4.6　Eight measurements for density matrix reconstruction of coherent states $|\alpha = 0.8\rangle$.

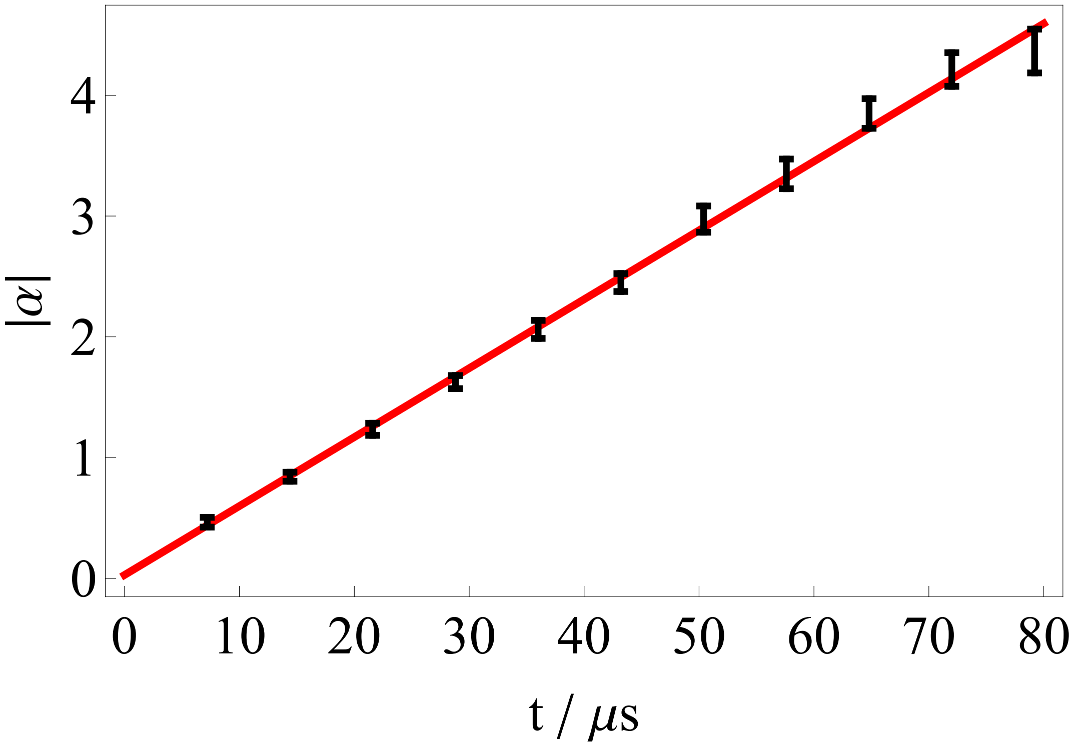


图 4.7　Relation on coherent $|\alpha\rangle$ amount and displacement duration.

Based on the measured phonon distribution f_n of N measurements by different displacement, we aim to get real probabilities $p_n = \langle n|\,\rho\,|n\rangle$ that are as close to the observed frequencies f_n as possible, which can be subject to the maximum-likelihood functional

$$\ln L(\rho) = \ln \prod_n \langle n|\,\rho\,|n\rangle^{f_n} = -\sum_n f_n \ln p_n, \tag{4-7}$$

from which we reconstruct ρ. This likelihood functional can be interpreted as a linear and positive (LP) problem in the classical signal processing:

$$p_n = \sum_i r_i h_{in}, \tag{4-8}$$

where r_i are eigenvalues of ρ and h_{in} is a positive kernel. We can solve this LP problem with the expectation-maximization algorithm[73,74]:

$$r_i^{(k)} = r_i^{(k-1)} \sum_n \frac{h_{in} f_n}{p_n\left(\mathbf{r^{(k-1)}}\right)}, \tag{4-9}$$

which is initially set to a positive vector $\mathbf{r}$ ($r_i > 0\ \forall i$).

The second part aims at getting the eigenbasis diagonalizing the density matrix. This part consists of two steps: reconstruction of the eigenvectors of ρ in a fixed basis, and rotation of the basis using a unitary transformation

$$|\phi_n^{'}\rangle \langle\phi_n^{'}| = U |\phi_n\rangle \langle\phi_n| U^\dagger \tag{4-10}$$

with the infinitesimal form $U \equiv e^{i\epsilon G} \approx 1 + i\epsilon G$ and ϵ is a small positive real number. $G = i [\rho, R]$ is chosen as a Hermitian generator of the unitary transformation, where R is a semipositive definite Hermitian operator $R = \sum_n \frac{f_n}{p_n} |n\rangle \langle n|$.

Starting from some positive initial density matrix ρ, we continue repetition of first finding new eigenvalues r_i using the expectation-maximization iterative algorithm (4-9) and then finding new eigenvectors ϕ_i by unitarily transforming the old ones. The likelihood of the estimate p_n is increased and we finally reach to determine the density matrix

$$\rho = \sum_n r_n |\phi_n\rangle \langle\phi_n| . \tag{4-11}$$

4.5 Conventional phase-coherent addition operation

We implement the addition operation $\hat{S}^+$ in (4-2) by first applying the uniform blue-sideband transfer $\sum_{n=0} |\uparrow, n+1\rangle \langle\downarrow, n| + \text{h.c.}$ and then π-pulse of carrier transition $\sum_{n=0} |\downarrow, n\rangle \langle\uparrow, n| + \text{h.c.}$ as shown in Figure 4.8(a). Our addition scheme deterministically adds one phonon independent of the initial phonon number state. We observe that quantum coherence is preserved in the addition operations. We prepare an initial state $\frac{1}{\sqrt{2}} (|n=0\rangle + |n=1\rangle)$, apply the additions up to three times and measure the density matrix of the resulting phonon states. As shown in Figure 4.8(b), the coherences represented by the off-diagonal terms of the density matrix clearly remain after the multiple addition processes up to three times. The reconstructed density matrices, only the real part of them, indicate the fidelity 0.99 (< 0.01) of the initially prepared state and those of the final states 0.96(0.01), 0.92(0.01) and 0.87(0.01) after one, two and three times addition, respectively. The purities of the output states are 0.92(0.01), 0.81(0.03), and 0.71(0.06), respectively. The numbers in the parentheses represent the sizes of error estimated by the maximal-likelihood methods.

As a second example, we prepare an initial coherent state $|\alpha = 0.81\rangle$ by displacing the vacuum, and apply the addition operations. Results are shown in Figures 4.8(c) and (d), the density matrix is reconstructed by using the iterative maximum-likelihood algorithm as described in section 4.4. The phonon number distributions are obtained by observing the time evolutions of the standard blue-sideband transitions, similar to the direct reconstruction scheme of the phonon density matrix[75]. Figure 4.9 shows the experimental obtained phonon distribution of initial coherent state $|\alpha = 0.81\rangle$. One immediate consequence of the addition operations on the coherent state is the production of sub-Poissonian phonon statistics because the addition increases the average phonon number but not the shape of the distribution and variance. We observe that our addition operations shift up the populations on phonon numbers while keeping the variance the same, making the variance over average phonon number $\langle n\rangle/\sigma^2$, which is initially set to 1, reduce to 0.43, 0.39, 0.26 as the average phonon number is increased by one, two, and three (Figure 4.8(c)). Applying the first addition operation, we detect negativity in the Wigner function as shown in the second column of Figure 4.8(d). It is important to note that the addition operation, which converts a coherent state to a highly non-Gaussian state, is nearly deterministic unlike the case of $\hat{a}^{\dagger}$ operation[57–59]. There is a limit in the number of additions we can apply, due to the validity of the adiabatic approximation and the heating process of phonons[76]. Under this limitation, we could perform the operations three times without the significant loss of fidelity. As shown in Figure 4.8(d), the experimental results and the theoretical predictions for the Wigner functions are in excellent agreement. The upper figures are theoretical and the lower figures are experimental. Observed negative values in the Wigner function proves the production of non-Gaussian state. The fidelities are reduced from 0.97(0.01) for the initial state to 0.87(0.01) (one single-phonon addition), 0.84(0.01)(two additions), 0.85(0.02) (three additions) and purities are changed from 0.99 to 0.93(0.02), 0.93(0.02), 0.80(0.03). This is significant in comparison to the photonic realization of bosonic operations of single photon creation and annihilation[59]. Here we obtain the Wigner function of the state from the reconstructed density matrix.

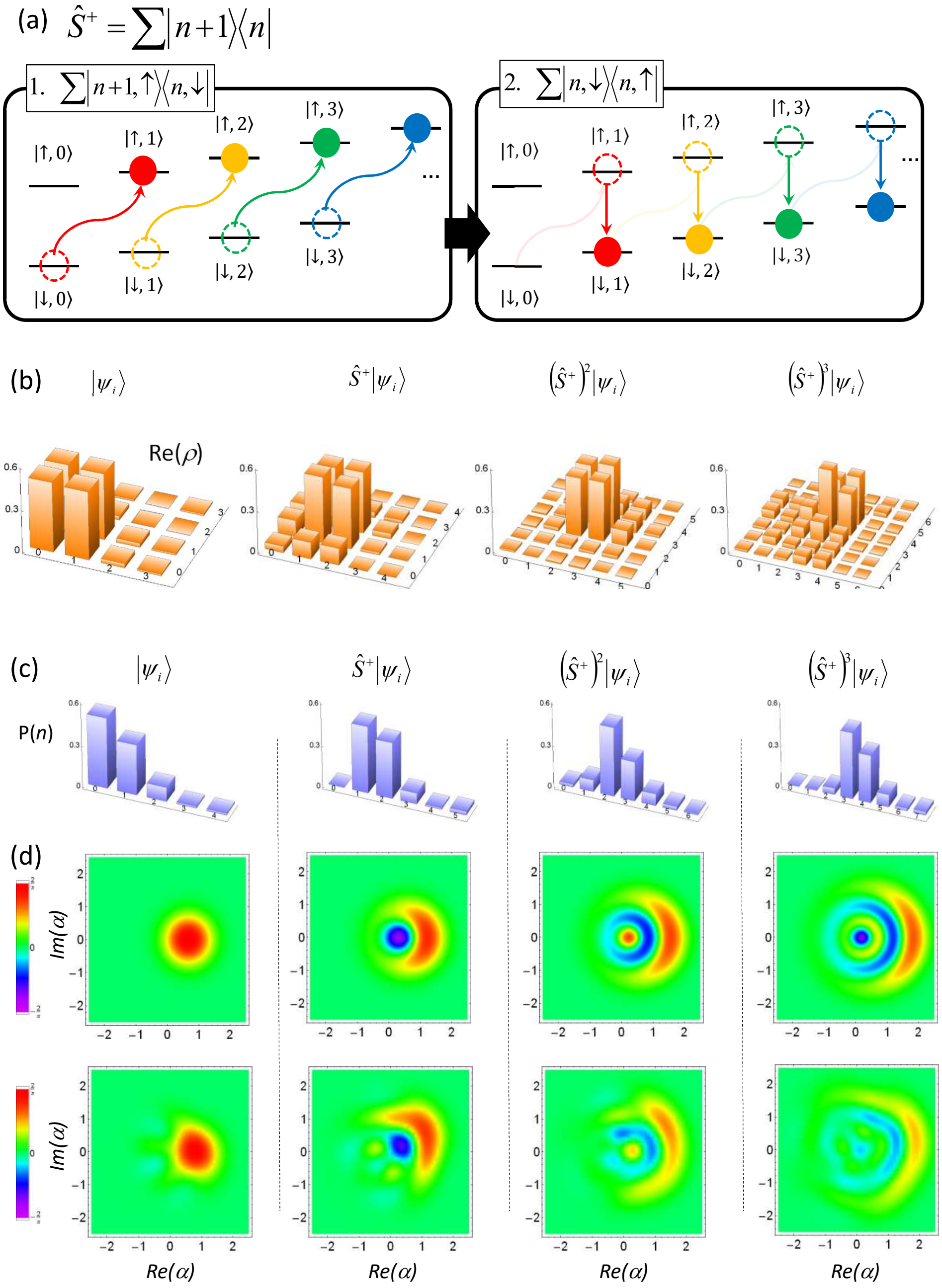


图 4.8 Schematic diagram and experimental results for the phonon addition. (a) Implementation of addition $\hat{S}^+$ is composed of a π-pulse of uniform blue-sideband transition $\sum |\uparrow, n+1\rangle\langle\downarrow, n|$+h.c., followed by a π-pulse of carrier transition $\sum |\downarrow, n\rangle\langle\uparrow, n|$ + h.c.. (b) Additions on a superposition state $|\psi_i\rangle = (|n=0\rangle + |n=1\rangle)/\sqrt{2}$ clearly shows the capability of keeping coherence. (c) Phonon distributions after the addition on a coherent state $|\psi_i\rangle = |\alpha = 0.81\rangle$. (d) Wigner functions of the coherent state $|\psi_i\rangle = |\alpha = 0.81\rangle$ after performing the addition operation n-times (n = 0 to 3).

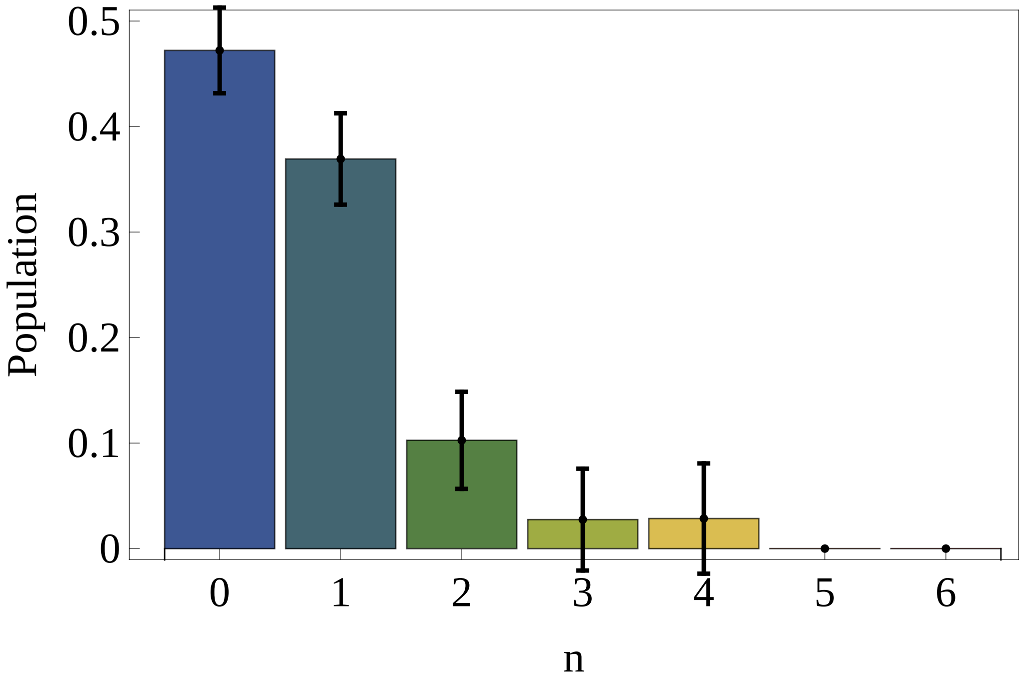


图 4.9 Phonon distribution of initial coherent state $|\alpha = 0.81\rangle$.

4.6 Conventional subtraction operation

The subtraction operation $\hat{S}^-$ in (4-2) is realized by reversing the sequence of the addition operation, that is, the application of the π-pulse of carrier transition and the uniform blue-sideband transfer $\sum_{n=1} |\downarrow, n-1\rangle\langle\uparrow, n| + \mathrm{h.c.}$, followed by the fluorescent detection as shown in Figure 4.10(a). This takes the phonon state from $|\downarrow, n+1\rangle$ to $|\downarrow, n\rangle$ except $|n=0\rangle$ where $|\downarrow, 0\rangle$ transfers to $|\uparrow, 0\rangle$. The $|\uparrow, 0\rangle$ state is eliminated after the subtraction, which is implemented by the conditional measurement in our experimental scheme. After the detection sequence, we only collect the data with no fluorescence, which has the success rate given by the probability of the non-zero phonon states. We examine the performance of the subtraction operation with an initial phonon superposition state $\frac{1}{\sqrt{2}}(|n=2\rangle + |n=3\rangle)$. As shown in Figure 4.10(b), the subtraction operation reduces the phonon excitation by one quanta. The initial fidelity and purity of the state are 0.83(0.02) and 0.73(0.03). The fidelities are changed to 0.77(0.02) and 0.83(0.01) after one and two times subtraction, respectively. The purities become 0.65(0.02) and 0.75(0.02). In the preparation and displacement operations for the superposition states with fluorescent detection, the zero components are increased due to unexpected experimental imperfections, which accidentally increase the fidelity and purity for the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. After the second application of the subtraction, the off-diagonal terms of the density matrix are significantly reduced, which shows the current limit in experiments due to the heating of the system. We also prepare a coherence state $|\alpha = 1.2\rangle$ and apply the subtraction twice. Figure 4.11 shows the experimental obtained phonon distribution of initial coherent state $|\alpha = 1.2\rangle$. Figure 4.10(c) shows that qualitatively the subtraction works for any initial quantum state. The initial fidelity of the state is 0.96(0.01) and the fidelities are reduced to 0.92(0.01) and 0.66(0.01) after one and two times subtraction, respectively. The subtraction operation can squeeze a coherent state which is different from annihilation that has the coherence state as its eigenstate. However, our experimental precision is not high enough to observe the squeezing effect.

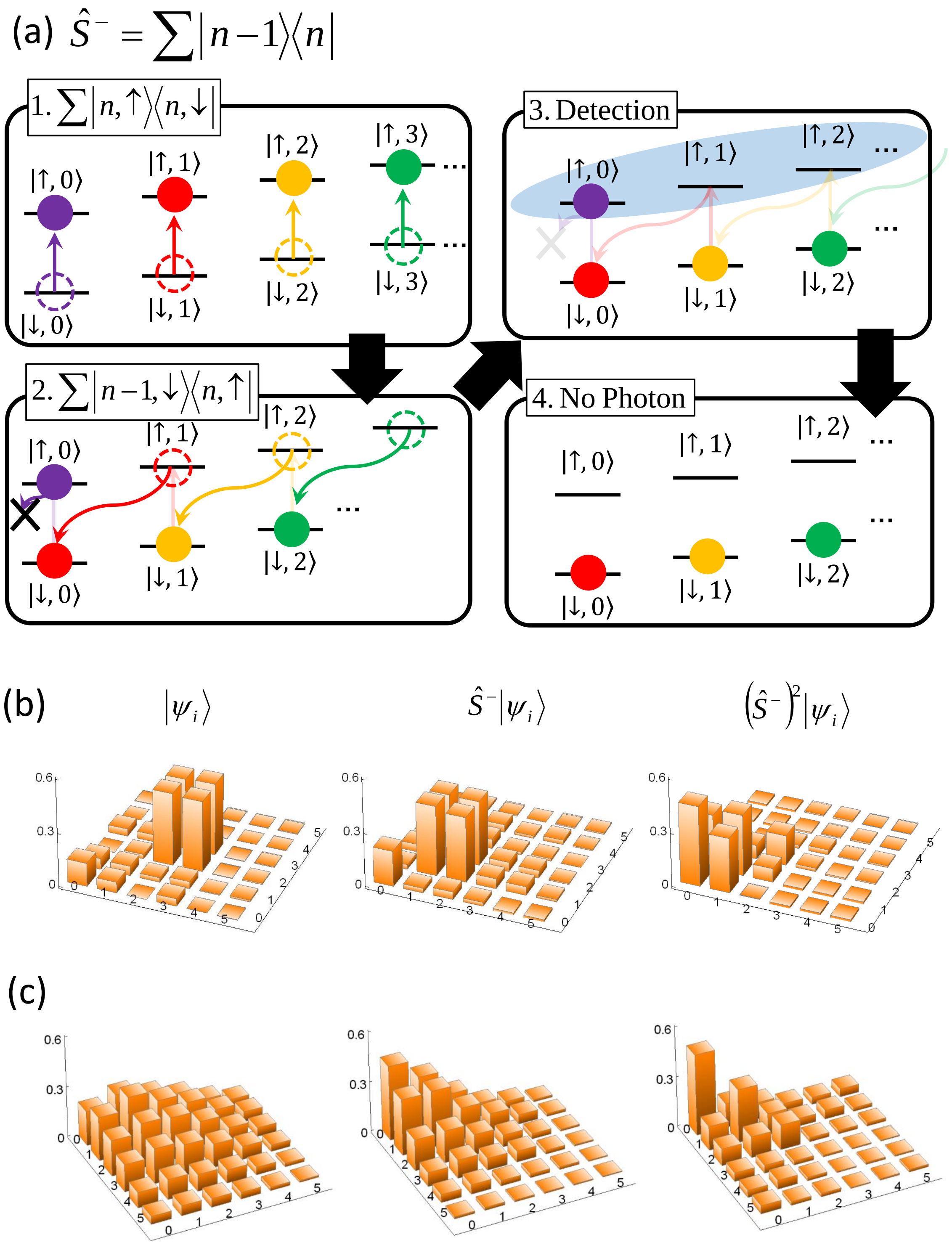


图 4.10　Schematic diagram and experimental results of phonon subtraction. (a) Sequence of subtraction operations: the sequence of the operations for addition is reversed, *i.e.*, a π-pulse of carrier transition followed by a π-pulse of adiabatic blue-sideband transition. (b) Subtraction on a superposition state $|\psi_i\rangle = (|n=2\rangle + |n=3\rangle)/\sqrt{2}$. The population is reduced and the coherence is conserved. (c) Subtraction from an initial coherent state $|\alpha = 1.2\rangle$.

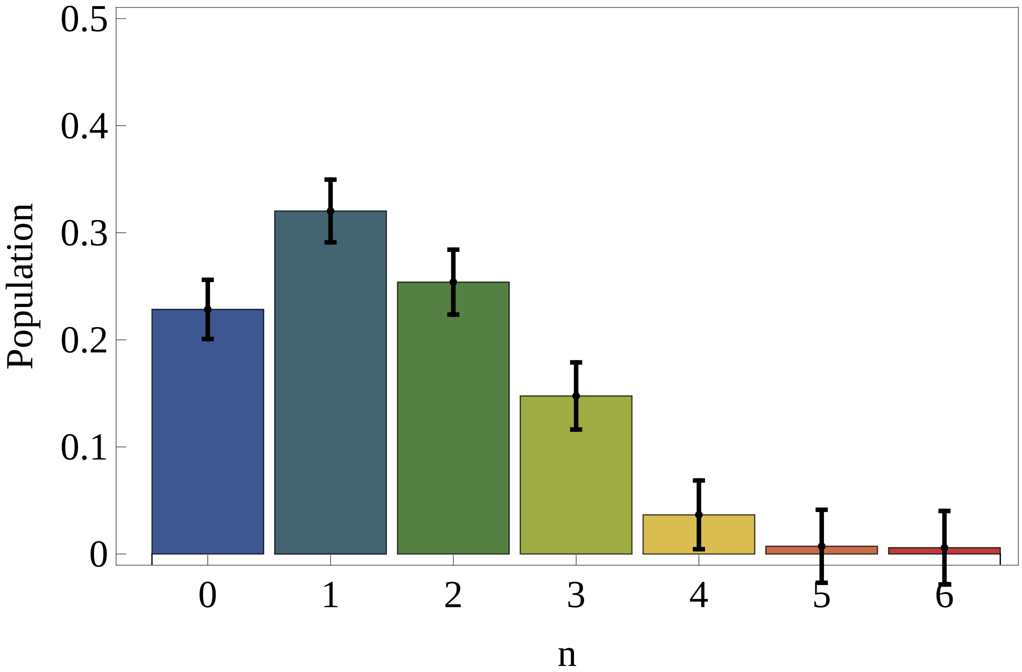


图 4.11 Phonon distribution of initial coherent state $|\alpha = 1.2\rangle$.

4.7 Commutation relation of addition and subtraction operations

We study experimentally how the quantum states are changed depending on the order of the addition and subtraction for an initial coherent state $|\psi_i\rangle = |\alpha = 1.2\rangle$. If we add then subtract $\hat{S}^{-}\hat{S}^{+}|\psi_i\rangle$, the state after the sequence is the same as the original one, since there is no amplitude modification. For the case of subtraction-then-addition $\hat{S}^{+}\hat{S}^{-}|\psi_i\rangle$, the final state does not have vacuum component because the vacuum state is removed at the first subtraction. Figure 4.12(b) shows the experimental result of $\hat{S}^{-}\hat{S}^{+}|\psi_i\rangle$, which is basically identical to the initial state of Figure 4.12(a). Figure 4.12(c) shows the result after the operation of $\hat{S}^{+}\hat{S}^{-}|\psi_i\rangle$, where there is no significant vacuum component in the density matrix. The vacuum component is not perfectly removed because of the detection error during the projective measurement based on the atomic fluorescence and heating of the system. The fluorescent detection duration is comparable to the motional coherence time of our system, which makes the off-diagonal part of the final state suppressed significantly. Our experimental result is well in line with the non commuting relation of the Susskind-Glogower's phase operators, *i.e.*, $[\hat{S}^{-}, \hat{S}^{+}] = |0\rangle\langle 0|$[53].

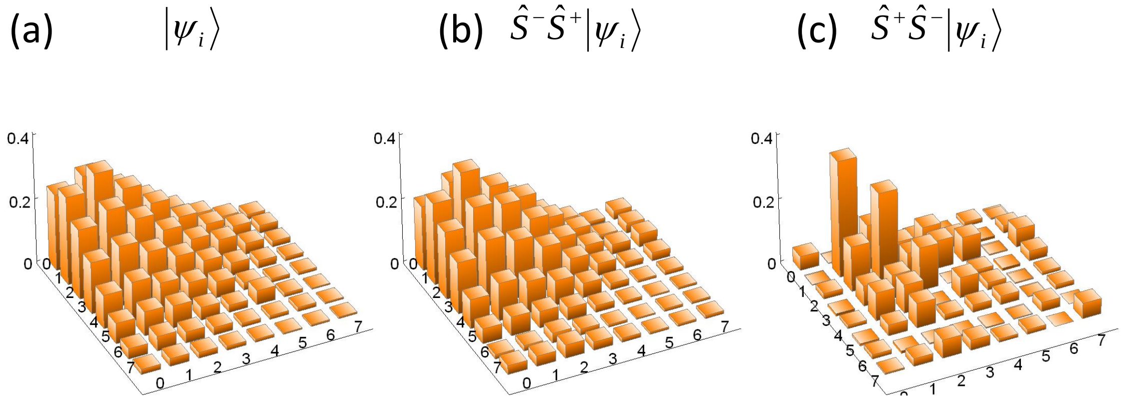


图 4.12 Experimental results after addition-then-subtraction and subtraction-then-addition, respectively. Only the real part of experimentally measured density matrices is shown (a) for an initial coherent state $|\psi_i\rangle = |\alpha = 1.2\rangle$, (b) single-phonon added-then-subtracted $\hat{S}^{-}\hat{S}^{+}|\psi_i\rangle$ state and (c) single-phonon subtracted-then-added $\hat{S}^{+}\hat{S}^{-}|\psi_i\rangle$ state. (b) The state after addition-then-subtraction is basically identical to the original state. The fidelity of the $\hat{S}^{-}\hat{S}^{+}|\psi_i\rangle$ state to the original state $|\psi_i\rangle$ is 0.97(0.01) and the purity is 0.96(0.01). (c) The state after subtraction-then-addition is not same as the original state, because the vacuum component is thrown away during the projective measurement. The small population in zero component mainly comes from the imperfection of the fluorescence detection and heating of the system, which is in good agreement with numerical simulation.

4.8 Extention on compatibility measurement for randomness certifacation

As further improvement of the randomness expansion experiment which I will talk in next chapter, though we have already practically closed compatilibity loophole by modifying KCBS inequality, we look forward to achieve perfect compatibility measurement by entangling ^{171}Yb^{+} ion and ^{138}Ba^{+} ion. In order to implement the most well known Mølmer-Sørenson gate, we will need to apply the Raman laser beams for ^{171}Yb^{+} ion and for ^{138}Ba^{+} ion to create entanglement with motional modes. Phonon arithmetics experiment of this chapter has already paved the way. By further setup of Raman laser system for ^{138}Ba^{+} ion, this extention could be straightforward for experimental implementation.

第 5 章　Randomness expansion secured by quantum contextuality with a trapped $^{138}\text{Ba}^+$ ion

In my work, first, we experimentally demonstrate the violation of a modified KCBS inequality[77,78], which reveals quantum correlations without the requirement of the perfect compatibility on sequential measurements. Then we employ it for a spot-checking protocol of randomness expansion with exponential gain[14], which is the first experimental demonstration of the strict randomness expansion. Our scheme is not a fully device-independent protocol, since it requires a few assumptions on the device, in particular, the assumption of approximate compatibilities on the measurement settings[6,79]. However, we do not need the perfect compatibility, since the imperfections in control and the disturbances from classical and quantum noisy-environment are characterized and compensated in the modified KCBS inequality. In this scenario, we can expand the randomness from the generated strings merely based on the experimental observed data that violate the modified KCBS inequality , which is in a self-testing manner[6,79]. We implement the protocol with a single trapped $^{138}\text{Ba}^+$ ion instead of a $^{171}\text{Yb}^+$ ion which was used for the previous demonstration[28] in order to fully address the experimental requirements in a modified KCBS inequality[77,78]. The $^{138}\text{Ba}^+$ ion has long-lived states that can be used for the coherent shelving of a quantum state during the sequential measurements. We develop a narrow-line laser system that is stabilized to a high-finesse cavity to precisely manipulate the long-lived states and observe sufficient amount of violation for the randomness expansion with large enough number of trials. We perform 1.29×10^8 trials of experiments and extract the randomness of 5.28×10^5 bits with the speed of 270 bits s^{-1}.

5.1 Modified KCBS inequality

In order to test contextuality, various inequalities have been proposed[26,80] and demonstrated in diverse physical systems, including trapped ion system[31,81,82], photonic system[33,34], and superconducting system[83]. Among the contextuality inequalities, the KCBS inequality, which uses five observables A_i taken ±1, shows that there is no hidden variables models in the smallest dimension $d = 3$[26],

$$\langle A_1 A_2 \rangle + \langle A_3 A_2 \rangle + \langle A_3 A_4 \rangle + \langle A_5 A_4 \rangle + \langle A_5 A_1 \rangle \geq -3. \tag{5-1}$$

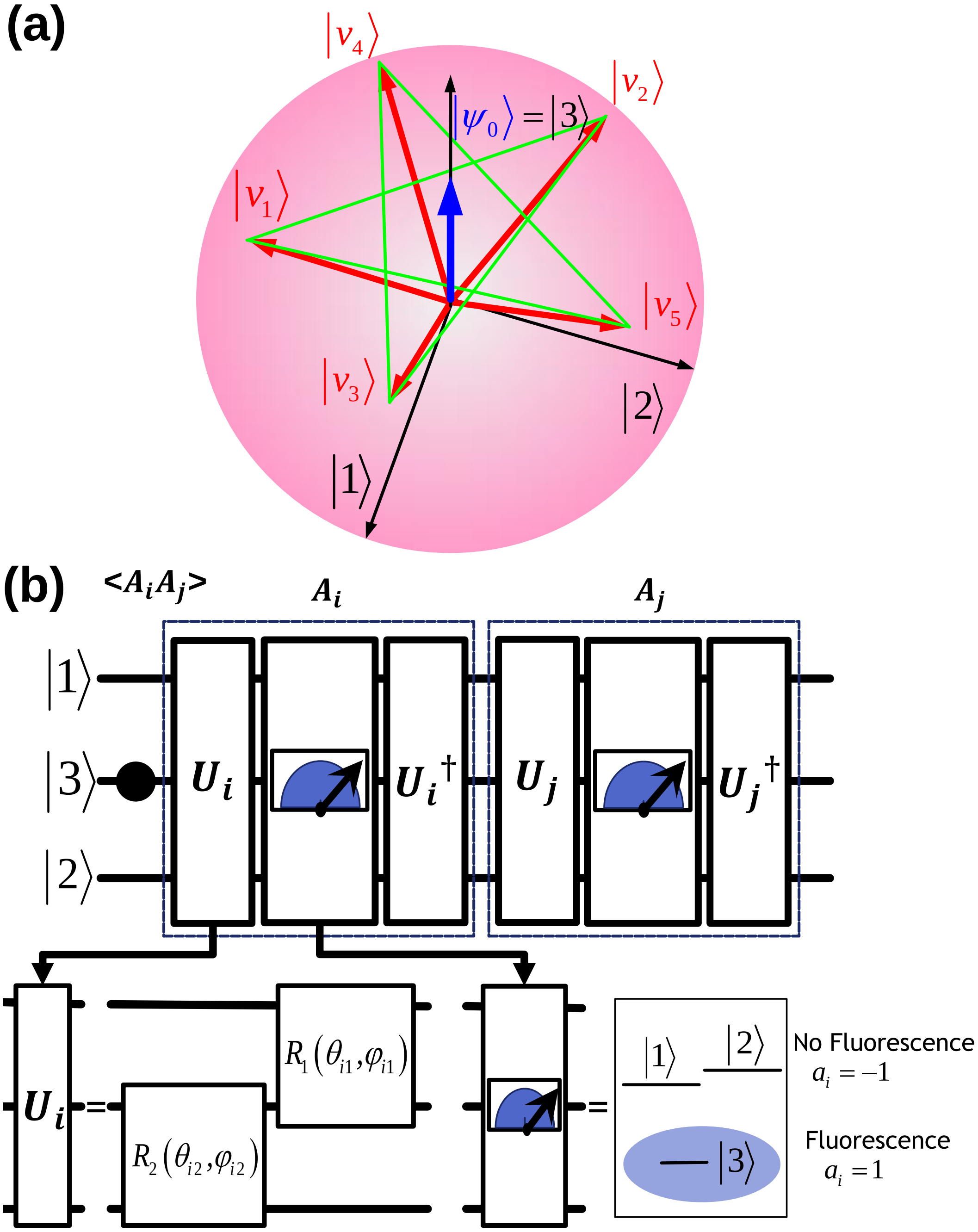


图 5.1　KCBS pentagram and experimental procedure. (a) Initial state and five axes which form a pentagram in d=3 space. The five observables $A_1, A_2, \ldots, A_5$ are the projectors on the axes respectively. The connected axes $|v_i\rangle$ and $|v_{i+1}\rangle$ are orthogonal, representing compatibility of the corresponding observables A_i and A_{i+1}. (b) Initially, we prepare $|3\rangle$ state, then perform two sequential measurements of A_i and A_j. Each sequential measurement contains a unitary rotation U_i, projective measurement, and an inverse unitary rotation $U_i^\dagger$. Each unitary rotation U_i is comprised of first $R_2(\theta_{2i}, \phi_{2i})$ then $R_1(\theta_{1i}, \phi_{1i})$. In projective measurement, we assign $a_i = 1(-1)$ if flourescence is (not) detected.

If all the five observables are predetermined, the inequality of (5-1) always holds. In quantum mechanics, on the other hand, the inequality can be violated for a specific state with properly arranged observables A_i. In the case of $d = 3$, denote the basis states by $|1\rangle$, $|2\rangle$ and $|3\rangle$. Design the observable $A_i = 1 - 2|v_i\rangle\langle v_i|$ to be the projector along the axis of $|v_i\rangle$. The maximal violation of the inequality (5-1) is achieved when five state vectors, $\{|v_i\rangle\}$, form a regular pentagram, and the initial state vector passes through the center of the pentagram, as shown in Figure 5.1. In this case, the sum of all the terms in (5-1) achieves $5 - 4\sqrt{5} \approx -3.944$. The assumption behind the above contextuality inequality is that the observables A_i and A_{i+1} (let $A_6 \equiv A_1$) are compatible. However, in an actual experiment using sequential measurements, the compatibility is difficult to verify, which leads to open the compatibility loophole. The issues of the compatibility in sequential measurements have been addressed by modifying the KCBS inequality[77,78].

In practice, the observables $\langle A_i A_j \rangle$ have to be implemented in a sequential measurement. We denote the observalble A_i with superscript m, A_i^m as the measurement of A_i at the position m in the sequence. For example, $A_i^1 A_j^2$ denotes the sequence of measuring A_i first, then A_j.

Noncontexual HV model requires that the outcomes of any observable A_i does not depend on other compatible jointly measured observables with A_i. To be more specific, we take A_1 as an example. It is compatible with A_2 and A_5. We denote the obtained value as v, then have $v(A_1^1) = v(A_1^2|A_2^1 A_1^2)$ and $v(A_1^1) = v(A_1^2|A_5^1 A_1^2)$.

The assumption behind the above contextuality inequality is that the observables A_i and A_{i+1} (let $A_6 \equiv A_1$) are compatible. However, in an actual experiment using sequential measurements, the compatibility is not perfect which leads to the compatibility loophole.

In[77], this imperfection can be quantified by

$$p^{flip}[A_1A_2] = p[(A_2^1(+)|A_2^1)\ and\ (A_2^2(-)|A_1^1A_2^2)] + p[(A_2^1(-)|A_2^1)\ and\ (A_2^2(+)|A_1^1A_2^2)]. \tag{5-2}$$

Here +, − denote the obtained value and this probability can be understood as the A_1 flips the predetermined value of A_2. Then using the fact $\langle A_1A_2\rangle \leq \langle A_1^1A_2^2\rangle + 2p^{flip}[A_1A_2]$, the inequality can be modified as

$$\begin{aligned}&\langle A_1^1A_2^2\rangle + \langle A_3^1A_2^2\rangle + \langle A_3^1A_4^2\rangle + \langle A_5^1A_4^2\rangle + \langle A_5^1A_1^2\rangle \geq \\ &-3 - 2(p^{flip}[A_1A_2] + p^{flip}[A_3A_2] + p^{flip}[A_3A_4] + p^{flip}[A_5A_4] + p^{flip}[A_5A_1]).\end{aligned} \tag{5-3}$$

Note that this inequality holds for any HV models. In the experiment, p^{flip} is not achieveable and different approaches are proposed to estimated with different assumptions. Here we use ϵ_{ij} to quantify the difference between a same pair of obervables A_i and A_j in different time order, A_iA_j and A_jA_i, which can be regarded as the bound of incompatibility of these sequential measurements,

$$\left|\left\langle A_j|A_jA_i\right\rangle - \left\langle A_j|A_iA_j\right\rangle\right| \leq \epsilon_{ij}. \tag{5-4}$$

For experimentally accessible distributions,

$$|p(A_i = a|A_iA_{i+1}) - p(A_i = a|A_{i+1}A_i)| \leq \epsilon_{ij}/2, \tag{5-5}$$

where $a \in \{+, -\}$. We assume that the underlaying probability distributions have the same properties as all accessible distributions. Then $p^{flip}[A_1A_2]$ can be bounded by $\epsilon_{12}/2$ which is obtained in the experiments, $p^{flip}[A_1A_2] \leq \epsilon_{12}/2$. However, the probability distributions of a general HV model may not belong to the set of experimentally accessible probability distributions. We assume that this difference is negligible and that the properties verified in accessible experiments hold also for some of HV models.

We combine the two modifications of the KCBS inequality to relax the condition of the perfect compatibility, which introduce additional terms of ϵ's[77] and $\langle A_1A_1\rangle$[78],

$$\begin{aligned}\langle \chi_{KCBS}\rangle &= \langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle + \langle A_5A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \\ &\geq -4 - (\epsilon_{12} + \epsilon_{32} + \epsilon_{34} + \epsilon_{54} + \epsilon_{51} + \epsilon_{11}).\end{aligned} \tag{5-6}$$

Here, $\langle A_iA_j\rangle$ denotes the expectation value of the measurement results in the time order of A_iA_j for the sequential measurements. For simplicity, we omit the time order superscript and $\langle A_iA_j\rangle$ denotes the expectation value of the measurement results in the time order of A_iA_j for the sequential measurements. The term of $\langle A_1A_1\rangle$ is later introduced to address different types of incompatibility, which cannot be excluded with the terms of ϵ_{ij}[78]. In our work, we include both of the modifications that address all types of incompatibility discussed in the Refs[77,78].

The above modifications of the inequality can be understood from the point of view of the game, which is played by two players $Alice$ and Bob who receive random inputs for measurement settings without knowing the other's, similar to the Bell-inequality nonlocal game[8,10,11]. The score of each trial is calculated according to the inputs and outputs. Each nonlocal game can be transformed into a contextuality game because no-communication local measurements is a stronger assumption and satisfy the compatible assumption. But on the contrary, not every contextuality game can be transformed into a nonlocal game. The inequality with only terms of ϵ_{ij} is not a Bell inequality because it can also be violated by a simple classical strategy, two players output always opposite results. Thus it is critical to have the term of $-\langle A_1A_1\rangle$. In the following, it can be proved that the modified KCBS inequality even without ϵ_{ij} terms is a Bell inequality which cannot be violated by all classical local hidden means. Inspired by a modified KCBS inequality, we propose a new Bell inequality, we assume that the measurements in different time order can not communicate with each other. With local hidden variable, the l.h.s of the inequality is no less than -4.

$$\langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle + \langle A_5A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \geq -4. \tag{5-7}$$

证明

$$\begin{aligned}
&\langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle + \langle A_5A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \\
=& \langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle - \langle A_1A_4\rangle + \langle A_5A_4\rangle + \langle A_1A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \\
\geq& \langle A_1(A_2 - A_4)\rangle + \langle A_3(A_2 + A_4)\rangle - 2
\end{aligned} \tag{5-8}$$

The inequality holds because with local hidden variable, $\langle A_5A_4\rangle + \langle A_1A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \geq -2$, which is a CHSH inequality. $A_i \in \{\pm 1\}$, either $A_2 + A_4 = 0$ or $A_2 - A_4 = 0$ will hold, thus $\langle A_1(A_2 - A_4)\rangle + \langle A_3(A_2 + A_4)\rangle \geq -2$. The l.h.s is no less than -4 with local hidden variable. □

From the view of nonlocal game, it is critical to have the term $-\langle A_1A_1\rangle$ in Eq. (5-6).

5.2 Randomness expansion protocol and security proof in practical case

The violation of the KCBS inequality implies the existence of quantum randomness which cannot be imitated by classical variables, which is not only fundamentally interesting but also posses the values for practical applications. The noncontextuality inequalities provide an alternative way of generating secure randomness. Similar to Bell inequality, in each trial, certain bits of randomness are consumed. Thus in order to efficiently expand the randomness from small input randomness, the idea of spot checking is necessary in our scheme. Recently, a robust (error-tolerant) randomness expansion scheme has been proposed[14], which is a spot-checking protocol that achieves exponential expansion. The protocol is shown in as follows with our experimental settings.

Denotation

- G : KCBS game with 11 random inputs $\{\{1,2\},\{2,1\},\{2,3\},\{3,2\},\{3,4\},$ $\{4,3\},\{4,5\},\{5,4\},\{5,1\},\{1,5\},\{1,1\}\}$ for the game rounds, and the input $\{1,2\}$ is also for the generation rounds
- D: a quantum device compatible with G
- Output length N: $N_{exp} = 1.29 \times 10^8$ in experiment
- Test probability $q \in (0,1)$: $q_{exp} = 10^{-4}$ in experiment
- Score threshold $\chi_g \in (0,1)$: $\chi_g = 2/3$ in this KCBS game

Protocol R_{gen}

1. Choose a bit $t \in \{0,1\}$ according to the Binomial distribution $(1-q, q)$.
2. If $t = 1$ (“game round"), the game G is played with D and the output is recorded. Outputs of game rounds are additionally collected for checking.
3. If $t = 0$ (“generation round"), $\{1,2\}$ is given to D and the output is recorded.
4. Steps 1-3 are repeated N times.
5. Calculate the score g_{KCBS} from all game round outputs. If $g_{KCBS} < \chi_g$, then abort. Otherwise, move to to randomness extraction.

图 5.2　The main spot-checking protocol and related denotation.

According to the definition of Ref.[14], the score of the KCBS game is given by $g \in \{0,1\}$. Thus, Eq. (5-6) can be rewritten in the form KCBS game G,

$$\begin{aligned} g_{KCBS} = -\frac{1}{6}(&\langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle + \langle A_5A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \\ &+\epsilon_{12} + \epsilon_{32} + \epsilon_{34} + \epsilon_{54} + \epsilon_{51} + \epsilon_{11}). \end{aligned} \tag{5-9}$$

The classical winning probability is $\chi_g = 2/3$ (see Prop. 5.1 for details) and the achievable maximal quantum winning probability is $\chi_g' = (4\sqrt{5}-4)/6 \approx 0.824$. The gap between χ_g and χ_g' enables randomness expansion.

In our scheme, the amount of randomness quantified by the min-entropy is related to the violation of the KCBS inequality. For a given game, if the device obtains a super-classical average score, then it must exhibit certain quantumness, which implies random behavior. This quantum randomness produced by the devices could be extracted. The violation is only based on the observation of experimental data, and can be independent of the sources of prepared states and other device specifications. Therefore, our protocol is self-testing provided that the following assumptions. In our scheme, there are three underlying main assumptions: (1) the input is chosen from an independent random distribution uncorrelated with the system; (2) the measurement outcomes cannot be leaked directly to adversaries; (3) The first and the second measurements in a context are approximately compatible and can be characterized by ϵ_{ij} and $\langle A_1 A_1 \rangle$ in (5-6). The assumptions (1) and (2) are widely used in other self-testing tasks, such as device-independent quantum random number generators[11,14,16]. The assumption (3) is related to the validity of the quantum contextuality test, which would be similar to all the other experimental tests with sequential measurements. We note that we do not require the perfect compatibility. Instead, we assume approximate compatibility, which can be quantified by the terms of ϵ_{ij} and $\langle A_1 A_1 \rangle$ in (5-6). Due to those terms, the violation of the inequality of (5-6) is getting difficult if two sequential measurements are deviated from the perfect compatibility. However, in our scheme, two measurements in a context are performed on a single system, which makes it impossible to exclude the possibility that a malicious manufacturer sabotage the compatibility assumption by registering the setting and results of the first measurements and using them for the second measurements. Therefore, our protocol can not be viewed as a fully-device independent scenario. We need the trust of the device that the measurement settings are close enough to be compatible, but it is fine to have imperfections in the realization and disturbance from classical or quantum noisy environments since the amount of introduced incompatibilities are quantified. Our protocol is well fitted to a scenario of trusted but error-susceptible devices. Given these assumptions, the generated randomness is certified by only experimental statistics.

Now, we mainly focus on the work[14] and overview their security proof.

The min entropy is used for evaluating the randomness. Given the output X , conditioned on input A and adversary' system E, the smooth min entropy $H^{\delta}_{min}(X|AE)$ is defined as

$$H^{\delta}_{min}(X|AE) = \max_{\|\Gamma' - \Gamma_{AEX}\| \leq \delta} H_{min}(X|AE)_{\Gamma'} \tag{5-10}$$

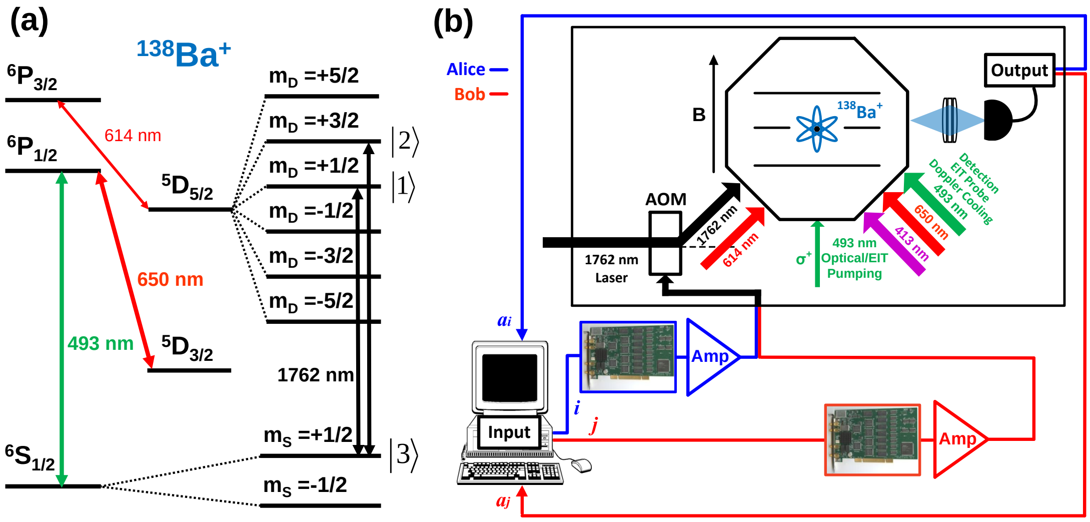


图 5.3　Experimental setup of the ^{138}Ba$^+$ ion system. (a) The energy level diagram of a ^{138}Ba$^+$ ion for a qutrit system, which is represented by two Zeeman sublevels $|m_D = +1/2\rangle \equiv |1\rangle$, $|m_D = +3/2\rangle \equiv |2\rangle$ in the $^5D_{5/2}$ manifold, and $|m_S = +1/2\rangle \equiv |3\rangle$ sublevel in the $^6S_{1/2}$ manifold. The quadrupole transitions between $^6S_{1/2}$ and $^5D_{5/2}$ are coherently manipulated using narrow-line 1762 nm laser which is stabilized to a high-finesse cavity. The 493 nm and 650 nm lasers are used for Doppler cooling, EIT cooling, optical pumping and detection. The 614 nm laser is used for depopulation of $^5D_{5/2}$ level to $^6S_{1/2}$ level. (b) The experimental setup of a trapped ^{138}Ba$^+$ ion for testing KCBS inequality and for the spot checking random number expansion. One of 11 measurement configurations $\{A_i, A_j\}$ is randomly selected. When Alice and Bob receive i and j, they could not know the setting of the other since each observable is included in at least two different contexts. For example, when Alice receives $i = 3$, Bob could be either $j = 2$ or $j = 4$. Their pulse sequences are independently generated by their own Direct Digital Synthesizer (DDS) and amplifiers, sent to the acousto-optic modulator (AOM) through independent paths, and finally applied to the ion on different time order. Fluorescence is observed by PMT on different time order and the values of the observables are assigned accordingly.

The direct estimation of min entropy is generally hard, thus their security proof applied Renyi entropy to give the lower bound of min entropy. For a quantum state ρ, its smooth min-entropies satisfy

$$H^{\delta}_{min}(\rho) = H_{1+\varepsilon}(\rho) - \frac{\log(1/\delta)}{\varepsilon} \tag{5-11}$$

where $H_{1+\varepsilon}(\rho) = -\frac{1}{\varepsilon}\log \mathrm{Tr}[\rho^{1+\varepsilon}]$. The randomness in its output is quantified by this $(1+\varepsilon)$-randomness. The main tool proposed in this proof is a $(1+\varepsilon)$-uncertain relation. After a projective measurement, the amount of randomness ($(1+\varepsilon)$-randomness) obtained from a measurement is related to the degree of disturbance caused by the measurement, shown in Proposition 4.4. For a given fixed input, the device has a classically predicable output and can achievable maximal score is w. Then if device obtains a score higher than this threshold w, then there must be unpredictable randomness in the output of this device. The rate curve is achieved in Corollary 6.11. This security proof is general for not only nonlocal game but also for contextuality. The uncertain relation is only relevant to the size of output alphabet and the measurement in contextuality can fit this proposition. For different schemes, the major differences is the classically predicable bound w. Note that this bound w is the maximal score for devices which has classically predictable outputs on an input. It is different with the classical strategy bound by hidden variable C_G in general. Though different in the definition, the value can be the same for some specific cases, for example, nonlocal game with binary input in each party and contextuality shown in Appendix D of[14]. However, in the practical case, the measurements in contextuality is not compatible. Though the uncertain relation in Proposition 4.4 still holds, the remained problem is to calculate w and check whether it equals to the classical bound achieved by approximately contextuail hidden variable. We express this KCBS game as

$$\begin{aligned} G(A_1, A_2, A_3, A_4, A_5) = -\frac{1}{6}(&A_1^1A_2^2 + A_3^1A_2^2 + A_3^1A_4^2 + A_5^1A_4^2 + A_5^1A_1^2 - A_1^1A_1^2 \\ &+\epsilon_{12} + \epsilon_{32} + \epsilon_{34} + \epsilon_{54} + \epsilon_{51} + \epsilon_{11}). \end{aligned} \tag{5-12}$$

命题 5.1： Let G be the game given above, $w = 2/3$

证明 With the approximately noncontextual hidden variable, the maximal score is $C_G = 2/3$. This strategy is classically predictable, thus the maximal score w with an input classically predictable should not be less than C_G, *i.e.* $w \geq C_G$. We suppose that there is a device D (can be quantum) applied in KCBS game which outputs a score above 2/3, and which gives a deterministic output on input 1,

$$-4 \geq \langle \chi_{KCBS} \rangle, \tag{5-13}$$

where $\langle \chi_{KCBS} \rangle = \left\langle A_1^1 A_2^2 \right\rangle + \left\langle A_3^1 A_2^2 \right\rangle + \left\langle A_3^1 A_4^2 \right\rangle + \left\langle A_5^1 A_4^2 \right\rangle + \left\langle A_5^1 A_1^2 \right\rangle - \left\langle A_1^1 A_1^2 \right\rangle + \epsilon_{12} + \epsilon_{32} + \epsilon_{34} + \epsilon_{54} + \epsilon_{51} + \epsilon_{11}$ is the practical mean value with sequential measurements. Due to $\left\langle A_i A_j \right\rangle \geq -1 + |\, \langle A_i \rangle + \left\langle A_j \right\rangle |$, $\left\langle A_i A_j \right\rangle \leq \left\langle A_i^1 A_j^2 \right\rangle + 2p^{flip}[A_i A_j]$ and $p^{flip}[A_i A_j] \leq \epsilon_{ij}$, we have

$$\begin{aligned}
\langle \chi_{KCBS} \rangle &\geq -6 + |\, \langle A_1 \rangle + \langle A_2 \rangle \,| + |\, \langle A_3 \rangle + \langle A_2 \rangle \,| + |\, \langle A_3 \rangle + \langle A_4 \rangle \,| \\
&\qquad + |\, \langle A_5 \rangle + \langle A_4 \rangle \,| + |\, \langle A_5 \rangle + \langle A_1 \rangle \,| \\
&\geq -6 + |\, \langle A_1 \rangle + \langle A_2 \rangle \,| + |\, \langle -A_2 \rangle - \langle A_3 \rangle \,| \\
&\qquad + |\, \langle A_3 \rangle - \langle -A_4 \rangle \,| + |\, \langle -A_4 \rangle - \langle A_5 \rangle \,| + |\, \langle A_5 \rangle - \langle -A_1 \rangle \,|.
\end{aligned} \tag{5-14}$$

Therefore, with the triangle inequality,

$$-4 \geq -6 + |\, \langle A_1 \rangle - \langle -A_1 \rangle \,|. \tag{5-15}$$

The fixed input 1 is deterministic, thus $\langle A_1 \rangle = \pm 1$, this is a contradiction. Thus $w \leq C_G = 2/3$ and $w = 2/3$. □

With this proposition, any score above w can be used to generate randomness though the observables are approximately compatible.

5.3 Randomness generation rate

Here, we consider the case that the average probability of measurement setting choice is unbiased, $p(a) = 1/11$, $a \in \{(i, i+1), (i+1, i), (1, 1)\} (i = 1, 2, \ldots, 5)$. The violation of the inequality in Eq. (5-6), indicates the presence of genuine quantum randomness in the measurement outcomes. The amount of secure randomness can be quantified by the smooth min-entropy $H_{min}^{\delta}(X|AE)$, which is bounded by

$$H_{min}^{\delta}(X|AE) \geq N R_{gen}(g_{KCBS}, q, \epsilon, N, \delta), \tag{5-16}$$

where X and A denote the output and input sequences, respectively; E denotes the system of an quantum adversary; δ is the smoothing parameter representing the security failure probability; g_{KCBS} is the KCBS game score; N is the total number of experiment trials; q is the probability of choosing game round; ϵ is the parameter of Schatten norm, in the security analysis, $(1+\epsilon)$-Schatten norm is applied; R_{gen} is the lower bound of randomness generation on average for each trial. In order to achieve the maximal randomness expansion, we also need to consider the input randomness for each trial,

$$R_{In} = q \log 11 + H(q), \tag{5-17}$$

and the randomness expansion rate can be expressed as $R_{exp} = R_{gen} - R_{In}$. The output randomness rate R_{gen} is given by

$$R_{gen} = \pi(\chi) - \Delta, \tag{5-18}$$

where

$$\begin{aligned}
&\chi = g_{KCBS} - \chi_g, \\
&\pi(\chi) = 2\frac{\log(e)\chi^2}{r-1}, \\
&\Delta = \frac{\epsilon}{q}\frac{8\log(e)\chi^2}{(r-1)^2} + \frac{\log(2/\delta^2)}{N\epsilon} + 2rq + O\left(\left(\frac{\epsilon}{q}\right)^2\right).
\end{aligned} \tag{5-19}$$

Here, all the log is base 2 throughout the paper, r is the output alphabet size, which is $r=4$ in our KCBS game. Now we show the explicit form of $O\left(\left(\frac{\epsilon}{q}\right)^2\right)$ and derivation of Eq. (5-19) which are based on the work[14] we give an exact result for the randomness expansion rate.

The min entropy is used for evaluating the randomness. Combining Theorem 4.1 and Proposition 6.8 in[14] yields

$$H_{min}^{\delta}(X|AE) \geq N[\pi(\chi) - O(q + \epsilon/q + \frac{\log(2/\delta^2)}{N\epsilon})] \tag{5-20}$$

where $O(\frac{\log(2/\delta^2)}{N\epsilon})$ and $O(q+\epsilon/q)$ come from Theorem 3.2 and Proposition 6.8, respectively. From Theorem 3.2, we can let $O(\frac{\log(2/\delta^2)}{N\epsilon}) = \frac{\log(2/\delta^2)}{N\epsilon}$. $O(q+\epsilon/q)$ comes from Proposition

6.5, the combination of Proposition 6.3 and 6.4. In the proof of Proposition 6.4, from Eq.(6.25) to Eq.(6.26) is equivalent to

$$\frac{\sum_x \langle \rho_{\bar{a}}^x \rangle_{1+\epsilon}}{\langle \rho \rangle_{1+\epsilon}} \geq 1 - O(\epsilon) \tag{5-21}$$

where x is the output with output alphabet size r, and $\bar{a}$ is the input. According to the Proposition B.2 and Proposition B.3 in Carl's paper, we apply the induction, $\sum_x \langle \rho_{\bar{a}}^x \rangle_{1+\epsilon} \geq (1-\epsilon)^r \langle \sum_x \rho_{\bar{a}}^x \rangle_{1+\epsilon}$ and $\langle \sum_x \rho_{\bar{a}}^x \rangle_{1+\epsilon} \geq (1-\epsilon)^r \langle \rho \rangle_{1+\epsilon}$. Thus $\frac{\sum_x \langle \rho_{\bar{a}}^x \rangle_{1+\epsilon}}{\langle \rho \rangle_{1+\epsilon}} \geq (1-\epsilon)^{2r} \geq 1 - 2r\epsilon$ and $O(\epsilon) = 2r\epsilon$. Consequently, the term in Proposition 6.4 $O(q) = 2rq$.

The estimation in Proposition 6.3 comes from the second order terms in Taylor expansion in Eq.(6.20) and Eq.(6.21). For a function $F(x)$, its Taylor expansion at a is as follows,

$$F(b) = F(a) + F^{'}(a)(b-a) + \frac{F^{''}(a)}{2}(b-a)^2 + \frac{F^{'''}[a+\theta(b-a)]}{6}(b-a)^3, \theta \in (0,1) \tag{5-22}$$

where the fourth term is third order Taylor Lagrange remainder. Here $F(b) = 2^{\epsilon s H(a,x)/q}$ and $a = 0$.

$$\begin{aligned} 2^{\epsilon s H(a,x)/q} - 1 &= \epsilon s\,(\ln 2)\,H(a,x)/q + \frac{1}{2}\left(\frac{\epsilon s\,(\ln 2)\,H(a,x)}{q}\right)^2 + R_3 \\ R_3 &= \frac{1}{6}\left(\frac{\epsilon s\,(\ln 2)\,H(a,x)}{q}\right)^3 2^{\theta \epsilon s H(a,x)/q}, \theta \in (0,1) \end{aligned} \tag{5-23}$$

where the term R_3 is the third order Taylor Lagrange remainder. Substitute this expression in Eq.(6.20), we have

$$\begin{aligned} &\sum_{a,x} p(a)\left[\frac{1}{2}\left(\frac{\epsilon s\,(\ln 2)\,H(a,x)}{q}\right)^2 + R_3\right]\langle \rho_a^x \rangle_{1+\epsilon} \\ &\leq \left[\frac{1}{2}\left(\frac{\epsilon s\,(\ln 2)}{q}\right)^2 + \frac{1}{6}\left(\frac{\epsilon s\,(\ln 2)}{q}\right)^3 2^{\epsilon s/q}\right]\sum_{a,x} p(a) H(a,x) \langle \rho_a^x \rangle_{1+\epsilon} \\ &\leq \frac{1}{2}\left(\frac{\epsilon s\,(\ln 2)}{q}\right)^2 + \frac{1}{6}\left(\frac{\epsilon s\,(\ln 2)}{q}\right)^3 2^{\epsilon s/q} \end{aligned} \tag{5-24}$$

After applying the function $-\frac{1}{\epsilon}\log()$, we have a more precise result similar to Proposition 6.3. The difference is we replace the $O(\epsilon/q)$ by $\frac{\epsilon}{q}\frac{(\ln 2)s^2}{2} + (\frac{\epsilon}{q})^2\frac{(\ln 2)^2 s^3}{6}2^{\epsilon s/q}$. In the Theorem

6.7, we let the parameter s be $\pi^{'}(\chi)$. In the Theorem 5.8, we know that

$$\begin{aligned}\pi(\chi) &= 2\frac{\log(e)(\chi - w)^2}{r-1} \\ \pi^{'}(\chi) &= 4\frac{\log(e)(\chi - w)}{r-1}\end{aligned} \tag{5-25}$$

Thus

$$O(\epsilon/q) = \frac{\epsilon}{q}\frac{8\log(e)(\chi - w)^2}{(r-1)^2} + \left(\frac{\epsilon}{q}\right)^2 \frac{32\log(e)(\chi - w)^3}{3(r-1)^3} 2^{\epsilon 4 \frac{\log(e)(\chi - w)}{(r-1)q}} \tag{5-26}$$

Result 1

$$\begin{aligned}&H^{\delta}_{min}(X|AE) \geq N[\pi(\chi) - \Delta] \\ &\pi(\chi) = 2\frac{\log(e)(\chi - w)^2}{r-1} \\ &\Delta = \frac{\epsilon}{q}\frac{8\log(e)(\chi - w)^2}{(r-1)^2} + \left(\frac{\epsilon}{q}\right)^2 \frac{32\log(e)(\chi - w)^3}{3(r-1)^3} 2^{\frac{\epsilon}{q}\frac{4\log(e)(\chi - w)}{r-1}} + \frac{\log(2/\delta^2)}{N\epsilon} + 2rq\end{aligned} \tag{5-27}$$

where $\chi \in [0, 1]$ is the score obtained in experiments, w is the classical bound for a certain game, r is the number of total outputs, q is the probability for test round, N is the total round number, δ is the failure probability, $\epsilon \in (0, 1]$ is the . The randomness expansion, generation, and input rate per round are

$$\begin{aligned}R_{exp} &= R_{gen} - R_{In}, \\ R_{gen} &= \pi(\chi) - \Delta, \\ R_{In} &= q\log 11 + H(q).\end{aligned} \tag{5-28}$$

If we focus on the randomness expansion instead of the generation randomness, we should consider the random seed $H(q) + q\log 11$ used for random inputs. Different target function have different optimal result, the figures in main text shows the effect of optimization parameter. Note that from the Result 1, the generated randomness is $O(N)$, and we take the probability $q \sim (\log^3 N)/N$, then the initial random seed required is $q\log 11 + H(q)$. And due to $\log N < N$, $q\log 11 + H(q) \sim O(q) + q\log\left(\left(\log^3 N\right)/N\right) < O\left(\log^4 N\right)$. Thus compared with the generated randomness $O(N)$, exponential randomness expansion is achieved.

Denote the above bound as Miller-Shi (MS) bound[14] and afterwards a tighter bound is obtained, referred as Huang-Shi (HS) bound without the dependence of r[84]. For the experiment, we perform the parameter optimization of q and ϵ to achieve the maximal randomness expansion rate R_{exp} with MS bound and also show the final randomness rate for two different bounds.

The important uncertain relation is related to the output alphabet size r. A larger r will lead to a bad performance. This disadvantage is removed by an improved uncertain relation. HS bound, which is a tighter bound of Proposition 4.4 proposed by Ref.[84], is as follows.

引理 5.1： For any finite dimensional Hilbert space V , any positive semidefinite operator $\tau : V \longrightarrow V$, and any projective measurement $\{P_0, P_1, \cdots, P_n\}$ on V , the following holds. Let $\tau^{'} = \sum_i P_i \tau P_i$. Then

$$\|\tau^{'}\|^2_{1+\epsilon} \leq \|\tau\|^2_{1+\epsilon} - \epsilon\|\tau - \tau^{'}\|^2_{1+\epsilon} \tag{5-29}$$

for all $\epsilon \in (0, 1)$. Consequently,

$$\|\tau^{'}\|_{1+\epsilon} \leq \|\tau\|^2_{1+\epsilon} - \epsilon/2\|\tau - \tau^{'}\|^2_{1+\epsilon}. \tag{5-30}$$

This result can be applied in Theorem 5.8 and obtain a new rate curve,

$$\pi(\chi) = 2\log(e)(\chi - w)^2 \; if \; \chi \geq w. \tag{5-31}$$

Consequently, we have $\pi^{'}(\chi) = 4log(e)(\chi - w)$, and let the parameter s be $\pi^{'}(\chi)$ in $O(\epsilon/q)$ by $\frac{\epsilon}{q}\frac{(\ln 2)s^2}{2} + (\frac{\epsilon}{q})^2\frac{(\ln 2)^2 s^3}{6}2^{\epsilon s/q}$. Then

$$O(\epsilon/q) = \frac{\epsilon}{q} 8\log(e)(\chi - w)^2 + \left(\frac{\epsilon}{q}\right)^2 \frac{32\log(e)(\chi - w)^3}{3} 2^{\frac{\epsilon}{q}4\log(e)(\chi - w)}. \tag{5-32}$$

Result 2

$$
\begin{aligned}
&H^{\delta}_{min}(X|AE) \geq N[\pi(\chi) - \Delta] \\
&\pi(\chi) = 2log(e)(\chi - w)^2 \\
&\Delta = \frac{\epsilon}{q} 8log(e)(\chi - w)^2 + \left(\frac{\epsilon}{q}\right)^2 \frac{32log(e)(\chi - w)^3}{3} 2^{\epsilon 4 \frac{log(e)(\chi - w)}{q}} + \frac{log(2/\delta^2)}{N\epsilon} + 2rq
\end{aligned}
\tag{5-33}
$$

5.4 Experimental schematic and procedure

There have been demonstrated the randomness expansion based on the experimental violations of the KCBS inequality using a single trapped ^{171}Yb^{+} ion[28]. In the demonstration, however, it is not possible to test the modified KCBS inequality, Eq. (5-6), due to lack of capability in obtaining all correlations. For example, when we observe fluorescence in the first measurement, the second measurement does not provide any useful information[28]. Instead, we develop a single ^{138}Ba^{+} ion system[85,86] with which we can obtain full-correlation results from the sequential measurements by using long-lived shelving states in $^5D_{5/2}$ manifold similar to ^{40}Ca^{+} ion[87]. We choose two Zeeman sub-levels ($|m_j = +1/2\rangle \equiv |1\rangle$, $|m_j = +3/2\rangle \equiv |2\rangle$) in the $^5D_{5/2}$ manifold, and one Zeeman sub-level ($|m_j = +1/2\rangle \equiv |3\rangle$) in the $^6S_{1/2}$ manifold to represent the qutrit system as shown Figure 5.3(a). In the projective measurement, we observe fluorescence when the state is projected to $|3\rangle$ and no fluorescence for all the other projections on the subspace that consists of $|1\rangle$ and $|2\rangle$ basis while conserving coherence. Different from the ^{171}Yb^{+} ion realization, since the coherence is not destroyed even when we observe fluorescence in the first measurement, we can get meaningful outcomes in the second measurement. The transitions between $^6S_{1/2}$ and $^5D_{5/2}$ are coherently manipulated by a narrow-line laser with the wavelength of 1762 nm, which is stabilized to a high-finesse optical cavity. The coherent rotations $R_1(\theta_1, \phi_1)$ (5-34) between $|1\rangle$ to $|3\rangle$ and $R_2(\theta_2, \phi_2)$ (5-35) between $|2\rangle$ to $|3\rangle$ are realized by applying the 1762 nm laser beam, where θ and ϕ are controlled by the duration and the phase of the laser beam, respectively, using an AOM.

The procedure of the experimental test of the KCBS inequality consists of Doppler and electromagnetically induced transparency (EIT) cooling[42,88,89], initialization, the first projective measurement of observable A_i and the second projective measurement of A_j. The initialization to the state $|3\rangle$ is performed by applying the optical pumping beam of 493 nm with σ^{+} polarization shown in Figure 5.3(b). The first measurement of the observable A_i is realized by the rotation U_i, the projective measurement, and the reverse of the rotation $U_i^\dagger$. The U_i shown in Tab. 5.1 maps the axis $|v_i\rangle$ to the axis $|3\rangle$ and the projective measurement can be described as the projector $M_{|3\rangle} = 2\,|3\rangle\,\langle 3| - 1$. Thus A_i is assigned to value $a_i = 1$ when fluorescence is observed and $a_i = -1$ when no fluorescence is observed. The projective measurement consists of the state-dependent fluorescence detection and the optical pumping sequence. The second measurement of the observable A_j is realized by the same scheme to that of the first measurement. Unitary rotations of A_i(Alice) and A_j(Bob) are realized by different signal generators and amplifiers, their results are also collected independently.

Each round comprises Doppler cooling, EIT cooling, optical pumping, rotation (U_i), the first projective measurement, inverse rotation ($U_i^\dagger$), rotation (U_j), the second projective measurement, inverse rotation ($U_j^\dagger$). The ^{138}Ba$^+$ ion is first cooled down with 500 μs Doppler cooling and 1000 μs EIT cooling. Optical pumping procedure initializes the internal state of the ion to $|m_S = +1/2\rangle$ by carefully adjusting the polarization of 493 nm laser beam. We manipulate the states between $|1\rangle$ and $|3\rangle$, and between $|2\rangle$ and $|3\rangle$ by applying 1762 nm laser with different frequencies and amplitudes controlled by AOM. The 1762 nm fiber laser is stabilized with a high-finesse cavity to achieve a linewidth below 1 Hz using Pound-Drever-Hall technique. The cavity is made of ultra-low-expansion material and is mounted in a vacuum cavity with active temperature stabilization to maximize the stability of its length. Frequency and amplitude of RF signal for AOM inputs are generated by two independent pairs of DDS (AD9910) for A_i and A_j measurements, which represent Alice and Bob, ensuring they are compatible without communication. The 2π time for both Rabi oscillations are adjusted to 37 μs, that is $\Omega = (2\pi)\,27$ kHz. Every rotation U_i is performed with same duration of no longer than 16 μs.

EIT cooling implements the asymmetry profile of the absorption spectrum to cancel the heating effect caused by carrier transition meanwhile strength the red-sideband transition to hold the cooling function[42,88,89]. EIT cooling only need three level, however there are four Zeeman states of ^{138}Ba$^+$ ion. Though with only doppler cooling and EIT cooling the ion is not perfectly cooled to the ground state without sideband cooling (average phonon number $\langle \bar{n} = 0.1 \rangle$), the carrier transition operated by stabilized 1762 nm laser has enough fidelity due to the small Lamb-Dicke parameter $\eta = 0.07$.

Our projective measurement includes state discrimination and state re-preparation. We differentiate one state versus the other two states of a qutrit using the standard fluorescent-detection method. For the $|3\rangle$ state, average of 32 photons at 493 nm can be detected during 600 μs and no photons for the $|1\rangle$ or the $|2\rangle$ state. In experiment, perfect state detection fidelity is achieved for $|3\rangle$, while the error of $|1\rangle$ and $|2\rangle$ is 1.3%. Duration of the first projective measurement is set to 600 μs with discrimination $n_{\mathrm{ph}} = 3$ while the second projective measurement is 300 μs and $n_{\mathrm{ph}} = 1$. Fluorescence detection duration is longer than the coherence time between $|1\rangle$ and $|2\rangle$, which is around 200 μs. Therefore we add spin echo pulses during the fluorescence detection to keep the coherence until the second measurement is done. Re-preparation to $|3\rangle$ state, which is realized by optical pumping without 614 nm laser, keeps the coherence between $|1\rangle$ and $|2\rangle$ in $^5D_{5/2}$ manifold. Since the second projective measurement is the end of the experiment without further operations, we do not apply spin echo pulses and state re-preparation, which results in shorter duration.

To describe our unitary rotation, We first define $R_1(\theta_1, \phi_1)$ and $R_2(\theta_2, \phi_2)$ as

$$R_1(\theta_1, \phi_1) = \begin{pmatrix} \cos\frac{\theta_1}{2} & 0 & -ie^{i\left(\phi_1+\frac{\pi}{2}\right)}\sin\frac{\theta_1}{2} \\ 0 & 1 & 0 \\ -ie^{-i\left(\phi_1+\frac{\pi}{2}\right)}\sin\frac{\theta_1}{2} & 0 & \cos\frac{\theta_1}{2} \end{pmatrix}, \tag{5-34}$$

$$R_2(\theta_2, \phi_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\frac{\theta_2}{2} & -ie^{-i\left(\phi_2+\frac{\pi}{2}\right)}\sin\frac{\theta_2}{2} \\ 0 & -ie^{i\left(\phi_2+\frac{\pi}{2}\right)}\sin\frac{\theta_2}{2} & \cos\frac{\theta_2}{2} \end{pmatrix}. \tag{5-35}$$

Then, the Unitary rotations U_i in the measurement configurations shown in Figure 5.1(b) are realized by corresponding $R_2(\theta_{2i}, \phi_{2i})$ then $R_1(\theta_{1i}, \phi_{1i})$, while $U_i^{\dagger}$ are composed of $R_1(\theta_{1i}, \pi - \phi_{1i})$ then $R_2(\theta_{2i}, \pi - \phi_{2i})$, where the specific U_i are listed in Tab. 5.1.

表 5.1　Unitary rotations U_i.

U	Rotation
U_1	$R_1(0.531\pi, \pi) \cdot R_2(0.066\pi, 0)$
U_2	$R_1(0.442\pi, 0) \cdot R_2(0.328\pi, 0)$
U_3	$R_1(0.191\pi, \pi) \cdot R_2(0.506\pi, \pi)$
U_4	$R_1(0.104\pi, \pi) \cdot R_2(0.526\pi, 0)$
U_5	$R_1(0.377\pi, 0) \cdot R_2(0.404\pi, \pi)$

5.5 Randomness expansion data

To test the modified KCBS inequality (5-6), we need to measure the eleven combinations of sequential measurements, which include five terms explicitly shown in the inequality (5-6) as $\langle A_1A_2\rangle$, $\langle A_3A_2\rangle$, $\langle A_3A_4\rangle$, $\langle A_5A_4\rangle$, and $\langle A_5A_1\rangle$, the other five terms with reverse order ($\langle A_2A_1\rangle$, $\langle A_2A_3\rangle$, $\langle A_4A_3\rangle$, $\langle A_4A_5\rangle$, $\langle A_1A_5\rangle$), and $\langle A_1A_1\rangle$. The reversed-order terms are necessary to observe ϵ_{12}, ϵ_{32}, ϵ_{34}, ϵ_{54}, and ϵ_{51} and evaluate incompatibility from experimental imperfections. The detailed experimental results of the measurements are summarized in Table 5.2.

表 5.2 Experimental results for different observables and compatibility terms for the KCBS inequality (5-6). Total game rounds are 1.2×10^4. The standard deviations of the final result are 0.015 and 0.023 for the single observables and correlations, respectively, 10^{-3} order for the compatibility terms, all as shown in the parenthesis. The standard deviation for the violation σ is 0.101 and our experimental data shows the violation of the extended inequality (5-6) with 7 σ.

$\{i, j\}$	$\langle A_iA_j\rangle$	$\langle A_i\rangle$	$\langle A_j\rangle$	ϵ_{ij}
{1,2}	**-0.768(23)**	0.082(15)	0.091(15)	**0.005(21)**
{2, 1}	-0.783(23)	0.096(15)	0.065(15)	0.017(21)
{2, 3}	-0.767(22)	0.098(14)	0.088(14)	0.019(21)
{3,2}	**-0.750(23)**	0.107(15)	0.098(15)	**0.000(21)**
{3,4}	**-0.773(23)**	0.084(15)	0.082(15)	**0.040(20)**
{4, 3}	-0.762(22)	0.122(14)	0.068(14)	0.016(21)
{4, 5}	-0.782(23)	0.095(15)	0.075(15)	0.019(21)
{5,4}	**-0.789(22)**	0.056(15)	0.094(15)	**0.002(21)**
{5,1}	**-0.773(22)**	0.100(14)	0.069(14)	**0.041(20)**
{1, 5}	-0.767(23)	0.109(15)	0.066(15)	0.033(20)
{1,1}	**0.977(21)**	0.106(15)	0.108(15)	**0.001(21)**
$g_{KCBS} = 4.742(101)/6 = 0.790(17)$				

For the spot-checking protocol, we choose $\{A_1, A_2\}$ as the setting for generation rounds, *i.e.*, $\{1, 2\}$ as the distinguished input of our KCBS game G. At each round, a string of trusted random bits t decides each round is generation round or game round. If it is generation round, we perform the sequential measurement $\{A_1, A_2\}$ and record the output $\{a_1, a_2\}$. If it is game round, we randomly choose one of the 11 configurations of Eq. (5-6) and save the result $\{a_i, a_j\}$ after performing the sequential measurement $\{A_i, A_j\}$.

From the Eq. (5-19), we can see that when the violation is small, the total rounds N is a critical parameter. A positive generation rate requires a sufficiently large N. Thus we give the minimum required rounds for different violations, which is instructive for experiments. Figure 5.4(a) shows the minimum total rounds N_{min} to obtain net randomness depending on the KCBS game score g_{KCBS}, where N_{min} can be obtained with an optimal q. In order to gain net randomness at our experimentally observed $g_{KCBS} = 0.790$, we perform $N_{exp} = 1.29 \times 10^8$ rounds, which is sufficiently larger than $N_{min} = 6.2 \times 10^7$. At our experimental condition of N_{exp}, Figure 5.4(b) shows the generation rate of net randomness depending on g_{KCBS}. If $g_{KCBS} \leq 0.77$, we can not observe net randomness regardless of q. When $g_{KCBS} > 0.77$, there exist optimal q values. If q is bigger than proper range, input randomness increases thus no net randomness is produced. If q is smaller than proper range, due to the increase of Δ in Eq. (5-18), we also cannot gain net randomness. In our experiment, we choose $q_{exp} = 10^{-4}$ as shown in red circle of Figure 5.4(b).

Meanwhile, we also apply HS bound to our experimental data as shown in Figure 5.4. The HS bound produces a bigger generation rate than the MS bound, thus we are able to reduce smoothing parameter δ to 10^{-4}, which is the security failure probability. We find that the optimal q for the HS bound is different from that of the MS bound, but our q_{exp} is still good enough to generate net randomness as shown in Figure 5.4(d).

We play $N_{exp} = 1.29 \times 10^8$ (129421072) rounds and observe the left hand side of the inequality Eq. (5-6), $\langle \chi_{KCBS} \rangle = -4.831$, and the right hand side $-4 - (\epsilon_{12} + \epsilon_{32} + \epsilon_{34} + \epsilon_{54} + \epsilon_{51} + \epsilon_{11}) = -4.088$. The detailed experimental results of are summarized in Tab. 5.2. The obtained final score of KCBS game is $g_{KCBS} = 4.742(101)/6 = 0.790(17)$, which violates the inequality (5-6) by 11 standard deviations. Our test probability is $q_{exp} = 10^{-4} \sim O((\log^3 N_{exp})/N_{exp})$, and the required amount of initial random seed is $O(\log^4 N_{exp})$ bits (see SM.III. and IV. for details). The min-entropy of final randomness is 5.3×10^{-3} per bit, thus the output random bits is $\Theta(N_{exp})$, achieving exponential randomness expansion. In real number, we get 5.73×10^5 bits of min-entropy which exceeds 2.35×10^5 bits of input randomness, resulting 3.38×10^5 net random bits, expansion rate per round is 2.6×10^{-3}.

When we apply the HS bound to the experimental data, we get larger min-entropy and expansion rate. Note that δ is two order smaller than that of the MS bound. The min-entropy of final randomness is 4.1×10^{-3} per bit, and the expansion rate per round is 2.3×10^{-3}. We get 5.28×10^5 bits of min-entropy which exceeds 2.35×10^5 bits of input randomness, resulting 2.92×10^5 net random bits. If we use an optimized q based on the calculation using the MS bound, we can get even larger min-entropy and expansion rate.

5.6 Extractor and random test

A random number extractor is a hashing function transforming a non-perfect random number string $\{0,1\}^N$ to a nearly perfect one $\{0,1\}^m$. In our experiment, the length of the input string is $N_{exp} = 1.29 \times 10^8$ and $H_{min}(X|IE) = 4.1 \times 10^{-3}$ per bit. According to leftover hash lemma[90]

$$m \leq NH_{min}(X|IE) - 2\log\frac{1}{\epsilon_h}, \tag{5-36}$$

we set the security parameter ϵ_h to be a typical value $\epsilon_h = 2^{-100}$, and the length of the output string is $m = 5.28 \times 10^5$. Here we apply a random $m \times N_{exp}$ Toeplitz matrix[91] as the hashing function. The input random seed $\{0,1\}^s$ $(s = m + N_{exp} - 1)$ is from[92].

We apply the random test[93] to the extracted data. The tests include 'Frequency', 'Block Frequency (BFreq)', two 'Cumulative Sums (CuSm)' tests, 'Runs', 'Longest-Run-of-Ones in a Block (LROB)', 'Rank', 'Fast Fourier Transform (FFT)', 'Serial'. The p-values are distributed in the interval (0, 1), which show the probabilities that an ideal random number generator would produce less random sequence than the tested one. If p-value is taken 0, it means the tested data is fully non-random, while 1 means completely random. The threshold we set for accepting the data as random is 0.01. As shown in Figure 5.5, the outputs strings ${a_i}^N$ and ${a_j}^N$ pass all tests. However, as expected, the combined outputs $(a_i a_j)^N$ do not pass all tests because since the measurement outputs of two observables are correlated thus are not independent random variables.

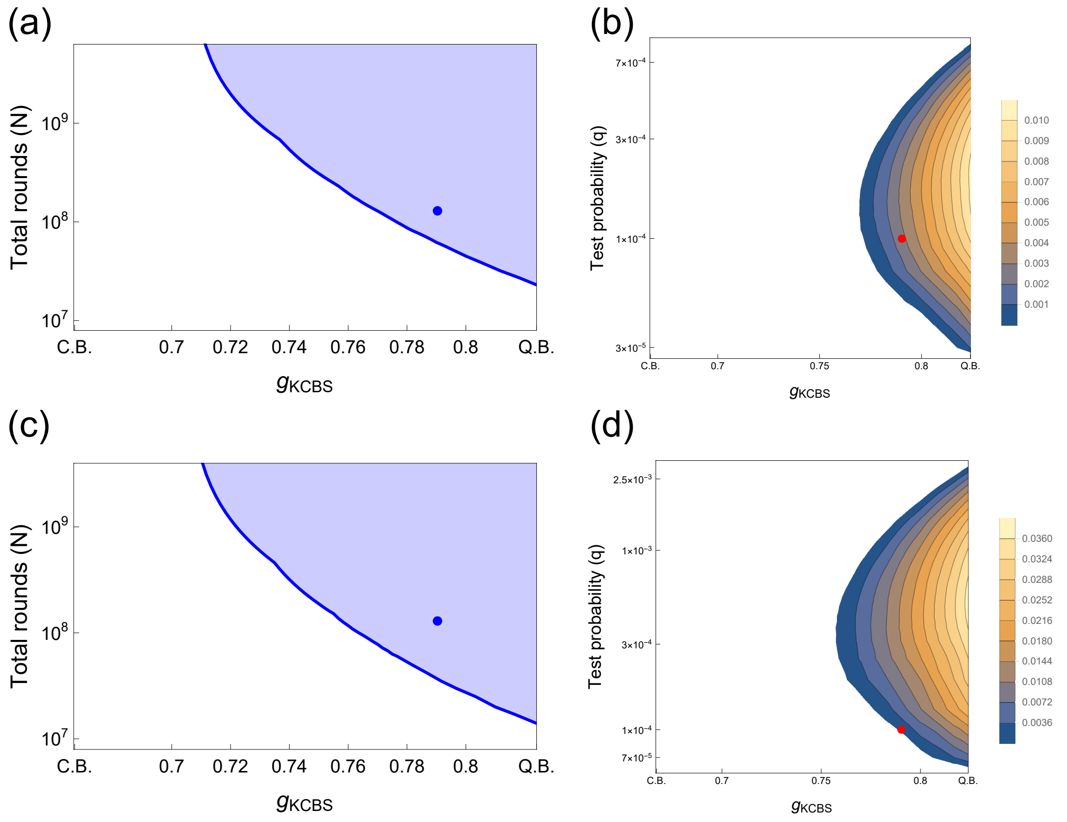


图 5.4　(a-b) For MS-bound the relation of the score of KCBS game g_{KCBS}, number of total rounds N, test probability q, and randomness expansion rate with smoothing parameter $\delta = 10^{-2}$ in (5-16). (a) The minimum number of rounds to have net randomness depending on the score g_{KCBS}. The minimum N decreases as g_{KCBS} increases. We can get net randomness only within the shadow area. Our experimental $g_{KCBS} = 0.790$ and $N_{exp} = 1.29 \times 10^{8}$ are shown as the green circle. (b) Randomness expansion rate at different g_{KCBS} and q for our N_{exp}. Only with the combination of large enough g_{KCBS} and proper q can we obtain net randomness. Our experimental $g_{KCBS} = 0.790$ and $q_{exp} = 0.0001$ are shown as the red circle, resulting expansion rate 2.6×10^{-3} per bit. (c-d) For HS-bound the relation of the score of KCBS game g_{KCBS}, number of total rounds N, test probability q, and randomness expansion rate with smoothing parameter $\delta = 10^{-4}$ in Eq. (5-16). (c) The minimum number of rounds to have net randomness depending on the score g_{KCBS}. Our experimental condition is shown as the green circle. (d) Randomness expansion rate at different g_{KCBS} and q for our N_{exp}. Our experimental $g_{KCBS} = 0.790$ and $q_{exp} = 0.0001$ are shown as the red circle, resulting expansion rate 2.3×10^{-3} per bit, although our q_{exp} is not optimal for this case.

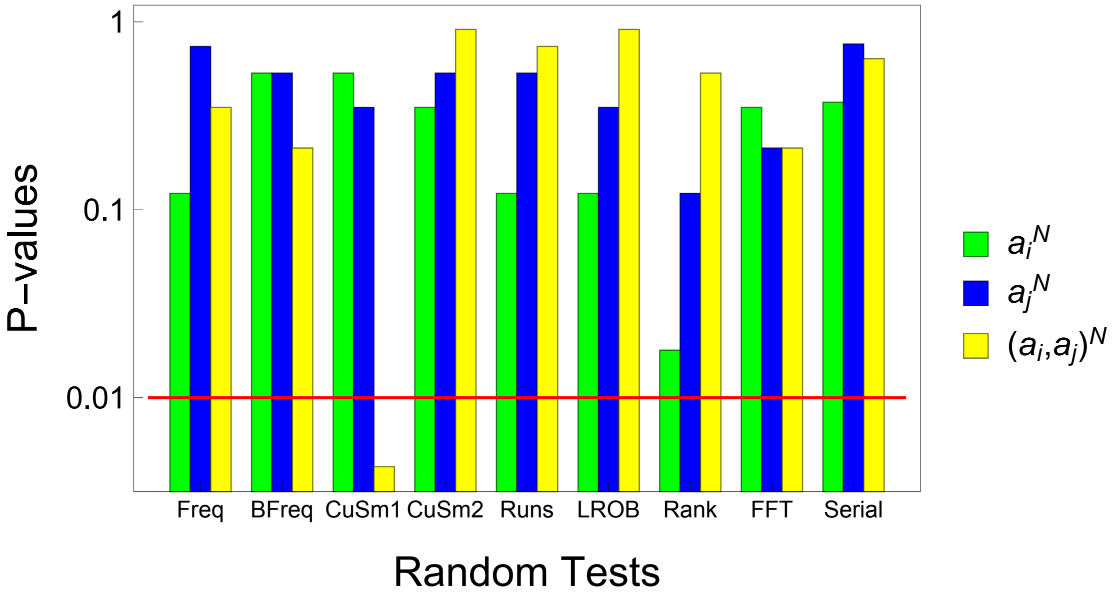


图 5.5　The results for random tests[93] of the outputs of the first measurement a_i and the second measurement a_j, and both measurement $a_i a_j$. Outputs of $a_i{}^N$ and $a_j{}^N$ pass the listed tests since all p-values exceed the threshold 0.01, while the outputs of $(a_i a_j)^N$ failed to pass the first test of 'Cumulative Sums (CuSm)'.

第 6 章　Conclusion and outlook

In this work, we achieve an exponential randomness expansion secured by quantum contextuality. Regardless of imperfections and experimental noises, the observed violation of the modified KCBS inequality, Eq. (5-6), verifies the generated randomness. In our protocol, we can guarantee the randomness without the i.i.d. assumption even when imperfections or noises may originate from quantum mechanics, which would be our quantum adversary. Note that there are other types of quantum contextuality inequalities that do not require sequential measurements, which could also ensure the no-disturbance condition. Our work can be easily extended to these proposals as well.

6.1　Improvement of random number generation speed

Due to the advantage of using contextuality for randomness certification, our current generation speed is 270 bits s^{-1} and 1.7 bits s^{-1} after applying Toeplitz matrix hashing, which is faster than that of using Bell's inequality[9,22]. We believe we can achieve orders of magnitude higher generation speed by several improvements in duration of cooling, optical pumping, and detection, coherence time of qutrit, and coherent operation time. Currently, each round costs 3700 μs, which is consisted of 1500 μs cooling process, two detections procedures 900 μs in total, 140 μs spin echo pulses for the first detection, two optical pumping pulses 60 μs in total, rotations 60 μs in total, some short gaps between sequences to make sure they do not affect each other, and around 1000 μs communication time. However, there is room for technical improvement as follows. By extending coherence time between qutrit, spin echo will not be required. Detection time could be reduce to around 100 μs by replacing a high numerical aperture (NA) lens from 0.2 to 0.6. By amplifying 1762 μm laser power 10 times, Rabi oscillations between $|1\rangle$ and $|3\rangle$, and between $|2\rangle$ and $|3\rangle$ can be at least 3 times faster, so as the rotation. Each optical pumping could be reduced to 1 μs by further optimization. Currently we apply 1500 μs cooling process each round, but it will be possible to apply only one cooling process per ten rounds after some improvements. With all the development above, we can achieve at least one order faster generation speed.

From the theoretical aspect, though the generation rate used in our scheme is robust and noise-tolerable, a large number of trials are still required which costs a lot of efforts.

An improved generation rate based on general contextuality inequality is still an open problem. Recently, entropy accumulation theory has been applied in device-independent protocols[94,95] and may be a potential tool for achieving a near optimal generation rate using contextuality inequality.

Fully device-independent random number generation puts a very high requirement on implementation devices. In practice, it is meaningful to pursue alternative randomness generation schemes with additional reasonable assumptions, such as Bell test with certain loopholes[7], uncertainty principles, or contextuality[96]. Our scheme is not fully device-independent due to the approximate compatibility assumption on measurements. On the other hand, our scheme does enjoy the self-testing properties on both source and measurement. Note that the self-testing protocols with proper assumptions on the device have also been proposed to deal with other quantum information processing tasks[79,97].

The security proof in[14] only considers the perfect case without imperfections of compatible or no-disturbance. Here we characterize this imperfections and modify the score of KCBS game. We assume the imperfections in experiments does not affect the adversary and security proof in[14] and only leads to a modified classical bound. The rigorous proof of a self-testing random number generator with limited compatibility is an interesting open problem and we will leave it as a future theoretical work.

6.2 Randomness amplification

Moreover, quantum contextuality can also provide an alternative means for randomness amplification. In principle, we can individually manipulate multiple ions and use them to generate random numbers simultaneously, which could lead to orders of magnitude faster generation speed. Such kind of multiple ion system can be applied to realize randomness amplification protocol[15], which generates true randomness out of weak randomness input. The protocol can be implemented by the multiple of our developed randomness expansion systems and the exclusive-OR of their outputs.

6.3 Randomness certification with 2 species ions achieving perfect compatibility measurement

Another improvement is using entangled 2 ions to fully close the compatilibity loophole. As I have done two experiments using a $^{171}\mathrm{Yb}^+$ ion and a $^{138}\mathrm{Ba}^+$ ion respectively, we are not far from entanglement of these two ions. We aim on entangling a $^{171}\mathrm{Yb}^+$ ion with either a ^{138}Ba^{+} ion or a ^{137}Ba^{+} ion. The scheme is shown in figure 6.1, here we take entanglement of a ^{171}Yb^{+} ion and a ^{137}Ba^{+} ion as an example. We can proceed operations and detections indepently to achieve randomness certifacation with perfect compatibility measurement. Firstly, we may need three-stage cooling of Doppler cooling, the EIT cooling and the sideband cooling on ^{138}Ba^{+} ion to prepare all the motional states to near the ground state. Then entangle them using Raman laser beams of 355 nm for ^{171}Yb^{+} ion and 532 nm for ^{138}Ba^{+} ion through Mølmer-Sørenson interaction. For detection, we measure the pairs of the joint observables simultaneously using the standard fluorescence scheme instead of the sequential measurements with totally different wavelength of laser beams for each ion.

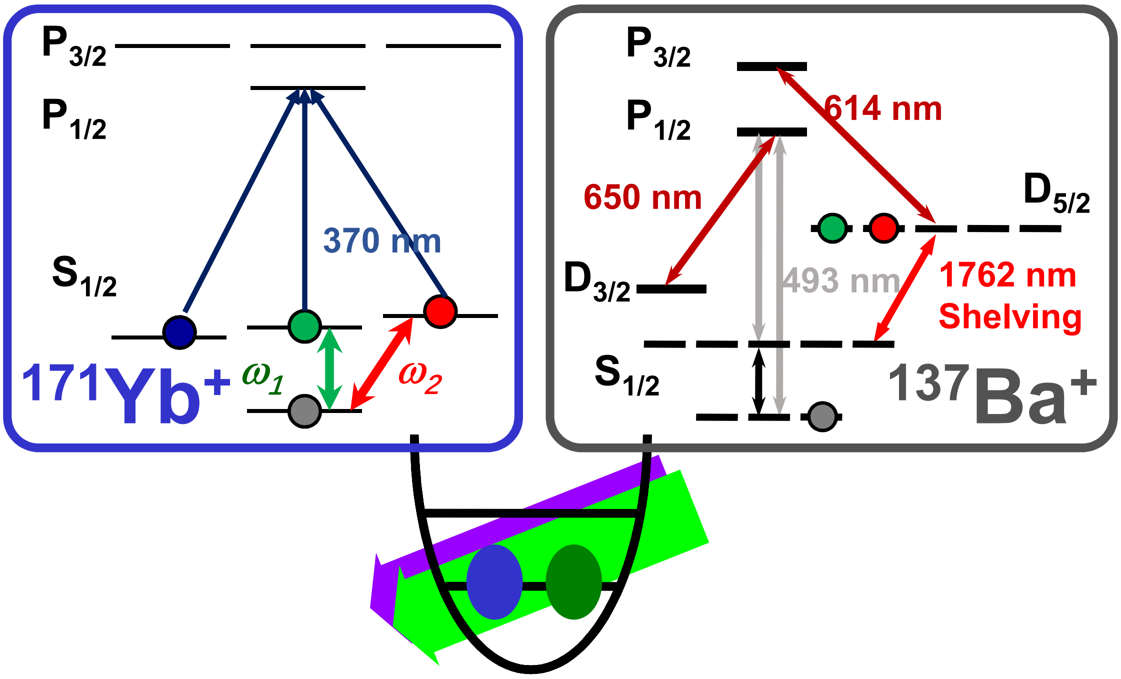


图 6.1　Scheme of a ^{171}Yb^{+} ion and a ^{137}Ba^{+} ion entanglement for perfect compatibility measurement.

插图索引

图 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 is connected to the trap to make ultra-high vacuum environment lower than 10^{-11} Torr. ... 4

图 1.2 Four-rod trap and pictures of $^{171}\mathrm{Yb}^{+}$ ion. (a) Connection of the trap and oven of $^{171}\mathrm{Yb}^{+}$ ion in an octagon. The lasers pass 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. The two ground electrodes are given 10.6 V DC voltage to differentiate the two transverse modes clearly (380 KHz apart). (d)(e) Pictures of one/two trapped $^{171}\mathrm{Yb}^{+}$ ion on the CCD camera. 5

图 2.1 Energy levels of $^{171}\mathrm{Yb}^{+}$. (a) The usages of 369 nm, 638 nm and 935 nm lasers. (b) Qubit(blue) and qutrit(black) setting of a $^{171}\mathrm{Yb}^{+}$ ion. 7

图 2.2 Schematic of Doppler cooling of $^{171}\mathrm{Yb}^{+}$. Doppler cooling laser has to cover all the energy levels in the $^2S_{1/2}$ and $^2P_{1/2}$. We achieve it by generating the second sidebands of the 7.37 GHz EOM. 8

图 2.3 Schematic of optical pumping of $^{171}\mathrm{Yb}^{+}$. Optical pumping laser only needs the first sideband of the 2.105 GHz EOM. Note that it has no influence on the $|\downarrow\rangle$ state since it is far detuned from the $|\downarrow\rangle$ state 9

图 2.4 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 $h\omega_X$ energy difference. 12

图 2.5 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. 13

图 2.6 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 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 14

图 2.7 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 frequency $\Delta = \omega_L - \omega_{HF}$. Blue sideband and red sideband can be realized by blue and red detuning of ω_X amount at laser frequency ω_L. 16

图 2.8 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 π-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 $|\uparrow, n-1\rangle$ 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 π-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........ 18

图 2.9 Effect of sideband cooling shown by spectrum. (a) Spectrum before sideband cooling. (b) Spectrum after sideband cooling. Red sideband transition is completely suppressed. 19

图 3.1 (a) Energy levels of ^{138}Ba$^+$. (b) Structure of EIT cooling........ 20

图 3.2 Transitions when we select σ_- polarization (blue) and σ_+ polarization (red) respectively........ 21

图 3.3 Rabi oscillation of $|S_{1/2}, m = \frac{1}{2}\rangle \longrightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ carrier transition with (red) and without (blue) EIT cooling. Black line is the theoretical line. 22

图 3.4 Rabi oscillation of $|S_{1/2}, m = \frac{1}{2}\rangle \longrightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ carrier transition with (red) and without (blue) EIT cooling. 22

图 3.5 Ramsey measurement of $|S_{1/2}, m = \frac{1}{2}\rangle \rightarrow |D_{5/2}, m = \frac{1}{2}\rangle$ 1st order RSB transition with (red) and without (blue) EIT cooling. 23

图 3.6 This is figure 1 of ref.[45]. Frequency stabilization system of the 650 nm laser to Te_2 reference through an optical cavity. The thick red lines show the optical path and the thin black lines with arrows indicate electrical connections... 24

图 3.7 Frequency stabilization system of the 493 nm laser to Te_2 reference. The cyan lines show the optical path and the black line indicates electrical connections from the balanced PD to lock-in amplifier........................ 25

图 3.8 Rabi oscillation of $|1\rangle \leftrightarrow |3\rangle$ by 1762 nm quadrupole transition. 26

图 3.9 Schematic of spin echo pulses during the detection............................ 27

图 3.10 Ramsey measurement of $|1\rangle \leftrightarrow |2\rangle$ transition with (red) and without (blue) EIT cooling. 27

图 3.11 Ramsey measurement of $|1\rangle \leftrightarrow |3\rangle$ transition with (red) and without (blue) EIT cooling. 28

图 4.1 Experimental scheme and parameter control. (a) $^{171}Yb^+$ system in a harmonic potential. The qubit level in $S_{1/2}$ manifold, $|F = 0, m_F = 0\rangle \equiv |\downarrow\rangle$ and $|F = 1, m_F = 0\rangle \equiv |\uparrow\rangle$ are coupled by the Raman laser beams, where the beat-note frequency is near resonant to the qubit levels, ω_{HF}. When the beat-note frequency is tuned to $\sim \omega_{\mathrm{HF}} + \omega_{\mathrm{X}}$, the scheme produces the anti-Jaynes-Cummings interaction or blue-sideband transition. We denote Ω as the Rabi-frequency on the qubit transition and the Δ is the frequency difference between the beat-note frequency of Raman beams and $\omega_{\mathrm{HF}} + \omega_{\mathrm{X}}$. The Raman beams are realized by pico-second pulse train similar to the scheme in Ref.[64]. (b) For the adiabatic blue-sideband transition whose frequency is independent of motional quantum number n, Ω and Δ are controlled as the red and blue curves. The phase $i\beta$ in Ω is the counter-diabatic term to suppress the transition during the evolution. Here $\Omega_0 = (2\pi)38.5$ kHz, $\beta = 0.075$, and $\Delta_0 = 1.6\Omega_0$.. 32

图 4.2 Experimental scheme and dynamic and adiabatic transition by anti-Jaynes-Cummings (blue-sideband) interaction. (a) The diagram for the standard blue-sideband transition. The Hilbert space is composed of the qubit states, $|\uparrow\rangle$and $|\downarrow\rangle$, and phonon states of n excitations, $|n\rangle$. The transition rate of the blue-sideband interaction between $|\uparrow, n\rangle$ and $|\downarrow, n-1\rangle$ depends on n; the higher the n value, the more frequent the transition is. The transitions between $|\downarrow, n\rangle$ and $|\uparrow, n+1\rangle$ would experience evolutions $\sqrt{n+1}$ times faster than the transition between $|\downarrow, 0\rangle$ to $|\uparrow, 1\rangle$. (b) Probability of finding the ion in $|\uparrow, n\rangle$ state as a function of time. We see that the transition frequency clearly manifests $\sqrt{n+1}$-dependence. The arrow at the first peak of each oscillation indicates the duration of a π-pulse for the corresponding transition. The π-pulse duration, T_π, of the fundamental blue-sideband transition (red) is 13 μs. The dots represent experimental data and solid lines are from the fitting to $\sin^2\left(\frac{\sqrt{n+1}\pi}{2T_\pi}t\right)$. (c) The conceptual diagram for the adiabatic blue-sideband transition without the $\sqrt{n+1}$-dependence. (d) The experimental demonstration of the adiabatic blue-sideband transitions realized by the transitionless quantum driving. The total time to execute the transitions is 91μs for any $|n\rangle$, which is about 7 times T_π. 33

图 4.3 The rapid adiabatic passage traces for phonon number $n = 0$ to 5 respectively on a bloch sphere. 34

图 4.4 Coherent Mira 900 laser and beam path.. 37

图 4.5 Setup of the Raman beams. The schematics of the Raman set up optics 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. The output of frequency stabilization system feedback to AOM1. The 756 nm laser shown in red is used to monitor the repetition rate and stabilize the frequency. The spherical lenses are shown in blue and the vertical cylindrical lens is in white.. 38

图 4.6 Eight measurements for density matrix reconstruction of coherent states $|\alpha = 0.8\rangle$. 39

图 4.7 Relation on coherent $|\alpha\rangle$ amount and displacement duration. 40

图 4.8 Schematic diagram and experimental results for the phonon addition. (a) Implementation of addition $\hat{S}^{+}$ is composed of a π-pulse of uniform blue-sideband transition $\sum|\uparrow,n+1\rangle\langle\downarrow,n|+\text{h.c.}$, followed by a π-pulse of carrier transition $\sum|\downarrow,n\rangle\langle\uparrow,n|+\text{h.c.}$. (b) Additions on a superposition state $|\psi_i\rangle=(|n=0\rangle+|n=1\rangle)/\sqrt{2}$ clearly shows the capability of keeping coherence. (c) Phonon distributions after the addition on a coherent state $|\psi_i\rangle=|\alpha=0.81\rangle$. (d) Wigner functions of the coherent state $|\psi_i\rangle=|\alpha=0.81\rangle$ after performing the addition operation n-times ($n=0$ to 3). ... 43

图 4.9 Phonon distribution of initial coherent state $|\alpha=0.81\rangle$. ... 44

图 4.10 Schematic diagram and experimental results of phonon subtraction. (a) Sequence of subtraction operations: the sequence of the operations for addition is reversed, *i.e.*, a π-pulse of carrier transition followed by a π-pulse of adiabatic blue-sideband transition. (b) Subtraction on a superposition state $|\psi_i\rangle=(|n=2\rangle+|n=3\rangle)/\sqrt{2}$. The population is reduced and the coherence is conserved. (c) Subtraction from an initial coherent state $|\alpha=1.2\rangle$. ... 46

图 4.11 Phonon distribution of initial coherent state $|\alpha=1.2\rangle$ ... 47

图 4.12 Experimental results after addition-then-subtraction and subtraction-then-addition, respectively. Only the real part of experimentally measured density matrices is shown (a) for an initial coherent state $|\psi_i\rangle=|\alpha=1.2\rangle$, (b) single-phonon added-then-subtracted $\hat{S}^{-}\hat{S}^{+}|\psi_i\rangle$ state and (c) single-phonon subtracted-then-added $\hat{S}^{+}\hat{S}^{-}|\psi_i\rangle$ state. (b) The state after addition-then-subtraction is basically identical to the original state. The fidelity of the $\hat{S}^{-}\hat{S}^{+}|\psi_i\rangle$ state to the original state $|\psi_i\rangle$ is 0.97(0.01) and the purity is 0.96(0.01). (c) The state after subtraction-then-addition is not same as the original state, because the vacuum component is thrown away during the projective measurement. The small population in zero component mainly comes from the imperfection of the fluorescence detection and heating of the system, which is in good agreement with numerical simulation. ... 48

图 5.1 KCBS pentagram and experimental procedure. (a) Initial state and five axes which form a pentagram in d=3 space. The five observables $A_1, A_2, \ldots, A_5$ are the projectors on the axes respectively. The connected axes $|v_i\rangle$ and $|v_{i+1}\rangle$ are orthogonal, representing compatibility of the corresponding observables A_i and A_{i+1}. (b) Initially, we prepare $|3\rangle$ state, then perform two sequential measurements of A_i and A_j. Each sequential measurement contains a unitary rotation U_i, projective measurement, and an inverse unitary rotation $U_i^{\dagger}$. Each unitary rotation U_i is comprised of first $R_2\left(\theta_{2i}, \phi_{2i}\right)$ then $R_1\left(\theta_{1i}, \phi_{1i}\right)$. In projective measurement, we assign $a_i = 1(-1)$ if flourescence is (not) detected. 50

图 5.2 The main spot-checking protocol and related denotation. 54

图 5.3 Experimental setup of the ^{138}Ba^{+} ion system. (a) The energy level diagram of a ^{138}Ba^{+} ion for a qutrit system, which is represented by two Zeeman sublevels $|m_D = +1/2\rangle \equiv |1\rangle$, $|m_D = +3/2\rangle \equiv |2\rangle$ in the $^5D_{5/2}$ manifold, and $|m_S = +1/2\rangle \equiv |3\rangle$ sublevel in the $^6S_{1/2}$ manifold. The quadrupole transitions between $^6S_{1/2}$ and $^5D_{5/2}$ are coherently manipulated using narrow-line 1762 nm laser which is stabilized to a high-finesse cavity. The 493 nm and 650 nm lasers are used for Doppler cooling, EIT cooling, optical pumping and detection. The 614 nm laser is used for depopulation of $^5D_{5/2}$ level to $^6S_{1/2}$ level. (b) The experimental setup of a trapped ^{138}Ba^{+} ion for testing KCBS inequality and for the spot checking random number expansion. One of 11 measurement configurations $\left\{A_i, A_j\right\}$ is randomly selected. When Alice and Bob receive i and j, they could not know the setting of the other since each observable is included in at least two different contexts. For example, when Alice receives $i = 3$, Bob could be either $j = 2$ or $j = 4$. Their pulse sequences are independently generated by their own Direct Digital Synthesizer (DDS) and amplifiers, sent to the acousto-optic modulator (AOM) through independent paths, and finally applied to the ion on different time order. Fluorescence is observed by PMT on different time order and the values of the observables are assigned accordingly. 56

图 5.4 (a-b) For MS-bound the relation of the score of KCBS game g_{KCBS}, number of total rounds N, test probability q, and randomness expansion rate with smoothing parameter $\delta = 10^{-2}$ in (5-16). (a) The minimum number of rounds to have net randomness depending on the score g_{KCBS}. The minimum N decreases as g_{KCBS} increases. We can get net randomness only within the shadow area. Our experimental $g_{KCBS} = 0.790$ and $N_{exp} = 1.29 \times 10^8$ are shown as the green circle. (b) Randomness expansion rate at different g_{KCBS} and q for our N_{exp}. Only with the combination of large enough g_{KCBS} and proper q can we obtain net randomness. Our experimental $g_{KCBS} = 0.790$ and $q_{exp} = 0.0001$ are shown as the red circle, resulting expansion rate 2.6×10^{-3} per bit. (c-d) For HS-bound the relation of the score of KCBS game g_{KCBS}, number of total rounds N, test probability q, and randomness expansion rate with smoothing parameter $\delta = 10^{-4}$ in Eq. (5-16). (c) The minimum number of rounds to have net randomness depending on the score g_{KCBS}. Our experimental condition is shown as the green circle. (d) Randomness expansion rate at different g_{KCBS} and q for our N_{exp}. Our experimental $g_{KCBS} = 0.790$ and $q_{exp} = 0.0001$ are shown as the red circle, resulting expansion rate 2.3×10^{-3} per bit, although our q_{exp} is not optimal for this case. 69

图 5.5 The results for random tests[93] of the outputs of the first measurement a_i and the second measurement a_j, and both measurement $a_i a_j$. Outputs of ${a_i}^N$ and ${a_j}^N$ pass the listed tests since all p-values exceed the threshold 0.01, while the outputs of $(a_i a_j)^N$ failed to pass the first test of 'Cumulative Sums (CuSm)'. 70

图 6.1 Scheme of a $^{171}\mathrm{Yb}^+$ ion and a $^{137}\mathrm{Ba}^+$ ion entanglement for perfect compatibility measurement............ 73

表格索引

表 5.1　Unitary rotations U_i. 65

表 5.2　Experimental results for different observables and compatibility terms for the KCBS inequality (5-6). Total game rounds are 1.2×10^4. The standard deviations of the final result are 0.015 and 0.023 for the single observables and correlations, respectively, 10^{-3} order for the compatibility terms, all as shown in the parenthesis. The standard deviation for the violation σ is 0.101 and our experimental data shows the violation of the extended inequality (5-6) with 7 σ. 66

公式索引

公式 2-1 ……………………………………………………………10
公式 2-2 ……………………………………………………………10
公式 2-3 ……………………………………………………………10
公式 2-4 ……………………………………………………………10
公式 2-5 ……………………………………………………………11
公式 2-6 ……………………………………………………………11
公式 2-7 ……………………………………………………………11
公式 2-8 ……………………………………………………………11
公式 2-9 ……………………………………………………………11
公式 2-10 ……………………………………………………………12
公式 2-11 ……………………………………………………………12
公式 2-12 ……………………………………………………………12
公式 2-13 ……………………………………………………………13
公式 2-14 ……………………………………………………………13
公式 2-15 ……………………………………………………………15
公式 4-1 ……………………………………………………………29
公式 4-2 ……………………………………………………………29
公式 4-3 ……………………………………………………………35
公式 4-4 ……………………………………………………………36
公式 4-5 ……………………………………………………………36
公式 4-6 ……………………………………………………………36
公式 4-7 ……………………………………………………………40
公式 4-8 ……………………………………………………………40

公式 4-9 ……………………………………………………………………40
公式 4-10 ……………………………………………………………………41
公式 4-11 ……………………………………………………………………41
公式 5-1 ……………………………………………………………………49
公式 5-2 ……………………………………………………………………51
公式 5-3 ……………………………………………………………………51
公式 5-4 ……………………………………………………………………52
公式 5-5 ……………………………………………………………………52
公式 5-6 ……………………………………………………………………52
公式 5-7 ……………………………………………………………………53
公式 5-8 ……………………………………………………………………53
公式 5-9 ……………………………………………………………………54
公式 5-10 ……………………………………………………………………55
公式 5-11 ……………………………………………………………………57
公式 5-12 ……………………………………………………………………57
公式 5-13 ……………………………………………………………………58
公式 5-14 ……………………………………………………………………58
公式 5-15 ……………………………………………………………………58
公式 5-16 ……………………………………………………………………58
公式 5-17 ……………………………………………………………………59
公式 5-18 ……………………………………………………………………59
公式 5-19 ……………………………………………………………………59
公式 5-20 ……………………………………………………………………59
公式 5-21 ……………………………………………………………………60
公式 5-22 ……………………………………………………………………60
公式 5-23 ……………………………………………………………………60

公式 5-24 ……………………………………………………………………60
公式 5-25 ……………………………………………………………………61
公式 5-26 ……………………………………………………………………61
公式 5-27 ……………………………………………………………………61
公式 5-28 ……………………………………………………………………61
公式 5-29 ……………………………………………………………………62
公式 5-30 ……………………………………………………………………62
公式 5-31 ……………………………………………………………………62
公式 5-32 ……………………………………………………………………62
公式 5-33 ……………………………………………………………………63
公式 5-34 ……………………………………………………………………65
公式 5-35 ……………………………………………………………………65
公式 5-36 ……………………………………………………………………68

参考文献

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

[2] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography[J]. Rev. Mod. Phys., 2002, 74: 145.

[3] Fiorentino M, Santori C, Spillane S M, et al. Secure self-calibrating quantum random-bit generator[J]. Phys. Rev. A, 2007, 75: 032334.

[4] Goldreich O. Foundations of cryptography[M]. Cambridge, UK: Cambridge University Press, 2007

[5] Ma X, Yuan X, Cao Z, et al. Quantum random number generation[J]. Npj Quantum Information, 2016, 2: 16021.

[6] Herrero-Collantes M, Garcia-Escartin J C. Quantum random number generators[J/OL]. Rev. Mod. Phys., 2017, 89: 015004. https://link.aps.org/doi/10.1103/RevModPhys.89.015004.

[7] Liu Y, Yuan X, Li M H, et al. High-speed device-independent quantum random number generation without a detection loophole[J/OL]. Phys. Rev. Lett., 2018, 120: 010503. https://link.aps.org/doi/10.1103/PhysRevLett.120.010503.

[8] Colbeck R. Quantum and relativistic protocols for secure multi-party computation[D]. UK: University of Cambridge, 2007.

[9] Pironio S, Acin A, Massar S, et al. Random numbers certified by bell's theorem[J]. Nature, 2010, 464: 1021.

[10] Colbeck R, Kent A. Private randomness expansion with untrusted devices[J]. Journal of Physics A: Mathematical and Theoretical, 2011, 44(9): 095305.

[11] Vazirani U, Vidick T. Certifiable quantum dice[J]. Phil. Trans. R. Soc. A., 2012, 370: 3432–3448.

[12] Pironio S, Massar S. Security of practical private randomness generation[J]. Phys. Rev. A, 2013, 87(1): 012336.

[13] Coudron M, Vidick T, Yuen H. Robust randomness amplifiers: Upper and lower bounds[M]// Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. [S.l.]: Springer, 2013: 468–483

[14] Miller C A, Shi Y. Universal security for randomness expansion from the spot-checking protocol [J]. Siam J. Comput., 2017, 46(4): 1304–1335.

[15] Chung K M, Shi Y, Wu X. Physical randomness extractors: Generating random numbers with minimal assumptions[J]. arXiv preprint arXiv:1402.4797, 2014.

[16] Rotem A F, Renato R, Thomas V. Simple and tight device-independent security proofs[J]. arXiv preprint arXiv:1607.01797, 2016.

[17] Acin A, Masanes L. Certified randomness in quantum physics[J]. Nature, 2016, 540(7632): 213–219.

[18] Bell J S. On the einstein-podolsky-rosen paradox[J]. Physics Physique Fizika, 1964, 1(3): 195.

[19] Hensen B, Bernien H, Dréau A E, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres[J]. Nature, 2015, 526(7575): 682–686.

[20] Shalm L K, Meyer-Scott E, Christensen B G, et al. Strong loophole-free test of local realism [J]. Phys. Rev. Lett., 2015, 115(25): 250402.

[21] Giustina M, Versteegh M A, Wengerowsky S, et al. Significant-loophole-free test of bell's theorem with entangled photons[J]. Physical review letters, 2015, 115(25): 250401.

[22] Bierhorst P, Knill E, Glancy S, et al. Experimentally generated randomness certified by the impossibility of superluminal signals[J]. Nature, 2018, 556(7700): 223.

[23] Liu Y, Zhao Q, Li M H, et al. Device-independent quantum random-number generation[J]. Nature, 2018, 562(7728): 548.

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

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

[26] Klyachko A A, Can M A, Binicioğlu S, et al. Simple test for hidden variables in spin-1 systems [J/OL]. Phys. Rev. Lett., 2008, 101: 020403. https://link.aps.org/doi/10.1103/PhysRevLett.101.020403.

[27] Deng D L, Zu C, Chang X Y, et al. Random numbers certified vis kochen-specker theorem[J]. arXiv: 1301.5364, 2013.

[28] Um M, Zhang X, Zhang J, et al. Experimental certification of random numbers via quantum contextuality[J]. Sci. Rep., 2013, 3: 1627.

[29] Wang Y, Um M, Zhang J, et al. Single-qubit quantum memory exceeding ten-minute coherence time[J]. Nat. Photonics., 2017, 11: 646–650.

[30] Cirac J I, Zoller P. Quantum computation with cold trapped ions[J]. Phys. Rev. Lett., 1995, 74: 4091–4094.

[31] Zhang X, Um M, Zhang J, et al. State-independent experimental tests of quantum contextuality in a three dimensional system[J]. Phys. Rev. Lett., 2013, 110: 070401.

[32] Olmschenk S, Younge K C, Moehring D L, et al. Manipulation and detection of a trapped Yb^+ hyperfine qubit[J]. Phys. Rev. A, 2007, 76(5): 052314.

[33] Lapkiewicz R, Li P, Schaeff C, et al. Experimental non-classicality of an indivisible quantum system[J]. Nature, 2011, 474: 490–493.

[34] Xiao Y, Xu Z P, Li Q, et al. Experimental observation of quantum state-independent contextuality under no-signaling conditions[J]. Opt. Express, 2018, 26(1): 32–50.

[35] Cummings F W. Stimulated emission of radiation in a single mode[J]. Phys. Rev., 1965, 140: A1051.

[36] Jaynes E, Cummings F W. Comparison of quantum and semiclassical radiation theories with application to the beam maser[J]. Proceedings of the IEEE, 1963, 51: 89.

[37] Liebfried D, Blatt R, Monroe C, et al. Quantum dynamics of single trapped ions[J]. Rev. Mod. Phys., 2003, 75: 281–324.

[38] Walls D, Milburn G J. Quantum optics[C]//Quantum Optics. [S.l.]: Springer-Verlag Berlin Heidelberg, 2008.

[39] Häffner H, Roos C F, Blatt R. Quantum computing with trapped ions[J]. Phys. Rep., 2008, 469 (155–203).

[40] Nagourney W, Sandberg J, Dehmelte H. Shelved optical electron amplier: Observation of quantum jumps[J]. Phys. Rev. Lett, 1986, 56: 2797–2799.

[41] Zhang J. Quantum Operation of Phonons and Entanglement of Multi-Species Ions[D]. China: Tsinghua University, 2017.

[42] Lechner R, Maier C, Hempel C, et al. Electromagnetically-induced-transparency ground-state cooling of long ion strings[J/OL]. Phys. Rev. A, 2016, 93: 053401. https://link.aps.org/doi/10.1103/PhysRevA.93.053401.

[43] Raab C, Bolle J, Oberst H, et al. Diode laser spectrometer at 493 nm for single trapped ba+ ions[J]. Appl. Phys. B, 1998, 67: 683–688.

[44] Chew A. Doppler-free spectroscopy of iodine at 739nm[J]. Bachelor. thesis, University of Maryland, 2008.

[45] Xie T, Jin N, Wang Y, et al. Frequency stabilization of a 650 nm laser to an I_2 spectrum for trapped $^{138}Ba^+$ ions[J]. JOSAB, 2019, 36: 243–247.

[46] Smith A, Anderson B E, Chaudhury S, et al. Three-axis measurement and cancellation of background magnetic fields to less than 50 ug in a cold atom experiment[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2011, 44: 205002.

[47] Dirac P A M. The principles of quantum mechanics[M]. [S.l.]: Oxford University Press, Oxford, 1957

[48] Pregnell K L, Pegg D T. Retrodictive quantum optical state engineering[J]. J. Mod. Opt., 2004, 51: 1613.

[49] Oi D K L, Potocek V, Jeffers J. Nondemolition measurement of the vacuum state or its complement[J]. Phys. Rev. Lett., 2013, 110: 210504.

[50] Govia L C G, Pritchett E J, Wilhelm F K. Generating nonclassical states from classical radiation by subtraction measurements[J]. New J. Phys., 2014, 16: 045011.

[51] Kim H J, Lee S Y, Ji S W, et al. Quantum linear amplifier enhanced by photon subtraction and addition[J]. Phys. Rev. A, 2012, 85: 013839.

[52] Schneider S, James D F V, Milburn G J. Method of quantum computation with "hot" trapped ions[J]. Preprint at http://arxiv.org/abs/quant-ph/9808012, 1998.

[53] Susskind L, Glogower J. Quantum mechanical phase and time operator[J]. Physics, 1964, 1: 49–61.

[54] Eschner J, Appasamy B, Toschek P E. Hybrid discrete- and continuous-variable quantum information[J]. Phys. Rev. Lett., 1995, 74: 2435–2438.

[55] Ourjoumtsev A, Tualle-Brouri R, Laurat J, et al. Generating optical schrödinger kittens for quantum information processing[J]. Science, 2006, 312: 83–86.

[56] Neergaard-Nielsen J S, Nielsen B M, Hettich C, et al. Generation of a superposition of odd photon number states for quantum information networks[J]. Phys. Rev. Lett., 2006, 97: 083604.

[57] Parigi V, Zavatta A, Kim M S, et al. Probing quantum commutation rules by addition and subtraction of single photons to/from a light field[J]. Science, 2007, 317: 1890–1893.

[58] Kim M S, Jeong H, Zavatta A, et al. Scheme for proving the bosonic commutation relation using single-photon interference[J]. Phys. Rev. Lett., 2008, 101: 260401.

[59] Zavatta A, Parigi V, Kim M S, et al. Experimental demonstration of the bosonic commutation relation via superpositions of quantum operations on thermal light fields[J]. Phys. Rev. Lett., 2009, 103: 140406.

[60] Namekata N, Takahashi Y, Fujii G, et al. Non-gaussian operation based on photon subtraction using a photon-number-resolving detector at a telecommunications wavelength[J]. Nature Photon., 2010, 4: 655–660.

[61] Kumar R, Barrios E, Kupchak C, et al. Experimental characterization of bosonic creation and annihilation operators[J]. Phys. Rev. Lett., 2013, 110: 130403.

[62] Andersen U L, Neergaard-Nielsen J S, van Loock P, et al. Hybrid discrete- and continuous-variable quantum information[J]. Nature Phys., 2015, 11: 713–719.

[63] An S, Zhang J N, Um M, et al. Experimental test of the quantum jarzynski equality with a trapped ion system[J]. Nature Phys., 2014, 11: 193–199.

[64] Hayes D, Matsukevich D N, Maunz P, et al. Entanglement of atomic qubits using an optical frequency comb[J]. Phys. Rev. Lett., 2010, 104: 140501.

[65] Bergmann K, Theuer H, Shore B W. Coherent population transfer among quantum states of atoms and molecules[J]. Rev. Mod. Phys., 1998, 70: 1003–1025.

[66] laas Bergmann, Vitanov N V, Shore B W. Perspective: Stimulated raman adiabatic passage: The status after 25 years[J]. J. Chem. Phys., 2015, 142: 170901.

[67] Gebert F, Wan Y, Wolf F, et al. Detection of motional ground state population of a trapped ion using delayed pulses[J]. New J. Phys., 2016, 18: 13037–13047.

[68] Berry M V. Transitionless quantum driving[J]. J. Phys. A, 2009, 42: 365303.

[69] Chen X, Lizuain I, Ruschhaupt A, et al. Shortcut to adiabatic passage in two- and three-level atoms[J]. Phys. Rev. Lett., 2010, 105: 123003.

[70] Bason M G, Viteau M, Malossi N, et al. High-fidelity quantum driving[J]. Nature Phys., 2012, 8: 147.

[71] Zhang J, Zhang J, Zhang X, et al. Realization of geometric landau-zener-stückelberg interferometry[J]. Phys. Rev. A, 2014, 89: 013608.

[72] Řeháček J, Hradil Z, Ježek M. Iterative algorithm for reconstruction of entangled states[J]. Phys. Rev. A, 2001, 63: 040303(R).

[73] Dempster A P, Laird N M, Rubin D B. Maximum likelihood from incomplete data via the em algorithm[J]. Journal of the Royal Statistical Society. Series B (Methodological), 1977: 1–38.

[74] Vardi Y, Lee D. From image deblurring to optimal investments: Maximum likelihood solutions for positive linear inverse problems[J]. Journal of the Royal Statistical Society. Series B (Methodological), 1993: 569–612.

[75] Leibfried D, Meekhof D M, King B E, et al. Experimental determination of the motional quantum state of a trapped atom[J]. Phys. Rev. Lett., 1996, 76: 4281–4285.

[76] Myatt C J, King B E, Turchette Q A, et al. Decoherence of quantum superpositions through coupling to engineered reservoirs[J]. Nature, 2000, 403: 269–273.

[77] Gühne O, Kleinmann M, Cabello A, et al. Compatibility and noncontextuality for sequential measurements[J]. Phys. Rev. A., 2010, 81: 022121.

[78] Szangolies J, Kleinmann M, Gühne O. Tests against noncontextual models with measurement disturbances[J]. Phys. Rev. A., 2013, 87: 050101.

[79] Lunghi T, Brask J B, Lim C C W, et al. Self-testing quantum random number generator[J]. Phys. Rev. Lett., 2015, 114(15): 150501.

[80] Cabello A. Experimentally testable state-independent quantum contextuality[J]. Phys. Rev. Lett., 2008, 101: 210401.

[81] Kirchmair G, Zähringer F, Gerritsma R, et al. State-independent experimental test of quantum contextuality[J]. Nature, 2009, 460: 494–497.

[82] Malinowski M, Zhang C, Leupold F M, et al. Probing the limits of correlations in an indivisible quantum system[J/OL]. Phys. Rev. A, 2018, 98: 050102. https://link.aps.org/doi/10.1103/PhysRevA.98.050102.

[83] Jerger M, Reshitnyk Y, Oppliger M, et al. Contextuality without nonlocality in a superconducting quantum system[J]. Nat. Commun., 2016, 7: 12930.

[84] Huang C, Shi Y. Private communications[M]. [S.l.: s.n.], 2017.

[85] Dietrich M R, Kurz N, Noel T, et al. Hyperfine and optical barium ion qubits[J/OL]. Phys. Rev. A, 2010, 81: 052328. https://link.aps.org/doi/10.1103/PhysRevA.81.052328.

[86] Slodička L, Hétet G, Röck N, et al. Interferometric thermometry of a single sub-doppler-cooled atom[J/OL]. Phys. Rev. A, 2012, 85: 043401. https://link.aps.org/doi/10.1103/PhysRevA.85.043401.

[87] Leupold F M, Malinowski M, Zhang C, et al. Sustained state-independent quantum contextual correlations from a single ion[J/OL]. Phys. Rev. Lett., 2018, 120: 180401. https://link.aps.org/doi/10.1103/PhysRevLett.120.180401.

[88] Morigi G, Eschner J, Keitel C H. Ground state laser cooling using electromagnetically induced transparency[J]. Phys. Rev. Lett., 2000, 85: 4458.

[89] Lin Y, Gaebler J P, Tan T R, et al. Sympathetic electromagnetically-induced-transparency laser cooling of motional modes in an ion chain[J/OL]. Phys. Rev. Lett., 2013, 110: 153002. https://link.aps.org/doi/10.1103/PhysRevLett.110.153002.

[90] Russell I, A L L, Michael L. Pseudo-random generation from one-way functions[C]// Proceedings of the twenty-first annual ACM symposium on Theory of computing. [S.l.]: ACM, 1989: 12–24.

[91] N W M, Lawrence C J. New hash functions and their use in authentication and set equality[J]. J. Comput. Syst. Sci., 1981, 22(3): 265–279.

[92] You-Qi N, Leilei H, Yang L, et al. The generation of 68 gbps quantum random number by measuring laser phase fluctuations[J]. Rev. Sci. Instrum., 2015, 86(6): 063105.

[93] Rukhin A, Soto J, Nechvatal J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. NIST special publication, 2010, 800-22: Rev. 1–a.

[94] Dupuis F, Fawzi O, Renner R. Entropy accumulation[J]. arXiv preprint arXiv:1607.01796, 2016.

[95] Arnon-Friedman R, Dupuis F, Fawzi O, et al. Practical device-independent quantum cryptography via entropy accumulation[J]. Nat. Commun., 2018, 9(1): 459.

[96] Kulikov A, Jerger M, Potočnik A, et al. Realization of a quantum random generator certified with the kochen-specker theorem[J]. Phys. Rev. Lett., 2017, 119(24): 240501.

[97] Fiorentino M, Santori C, Spillane S, et al. Secure self-calibrating quantum random-bit generator [J]. Phys. Rev. A, 2007, 75(3): 032334.

致 谢

衷心感谢导师金奇奂教授及全家对本人的学术与人格全方位的精心指导，如同第二位父亲一样，他的言传身教将使我终生受益。感谢清华大学量子信息中心离子量子计算实验室的所有同学们，张翔、张君华、安硕明、吕定顺、汪野、沈杨超、路尧、王鹏飞、乔木、张宽、张帅宁、栾春阳、陈文涛等每一位都像兄弟一样提供了很多的帮助。感谢张静宁研究员、在最后一个课题中一起合作的马雄峰教授和赵琦同学提供了很多理论上的支持，他们为我和我们合作的实验付出了很多。也感恩与隔壁实验室的赵琦、祖充、刘可、侯攀宇、张文纲等很多同学们一起度过的 8 年时光。

感恩上苍，感谢父母和兄长、妻子与女儿、岳父岳母不遗余力的支持和鼓励，感谢你们背后默默付出的所有。

感谢在学校和社团中认识并帮助我的所有弟兄姐妹们，你们让我的生活更有意义。

荣幸成为第一个清华韩国物理博士。感谢覆盖硕士博士 8 年全额奖学金的中国政府。本课题承蒙国家自然科学基金资助，特此致谢。

12 年整一轮，清华求学梦醒来，唯有满满的感恩。

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：______________ 日　期：______________

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，2011 年 7 月本科毕业并获得工学学士学位。

2011 年 9 月免试进入清华大学交叉信息研究院计算机科学与技术方向，2014 年 7 月硕士毕业并获得工学硕士学位。

2014 年 9 月免试进入清华大学交叉信息研究院物理学方向攻读博士学位至今。

发表的学术论文

[1] Um M, Zhang J, et al. Phonon arithmetic in a trapped ion system. Nature Communications, 2016, 7:11410.

[2] Zhang J, Um M(共同一作), et al. NOON States of Nine Quantized Vibrations in Two Radial Modes of a Trapped Ion. Phys. Rev. Lett., 2018, 121:160502.

[3] An S, Zhang J, Um M, et al. Experimental Test of the Quantum Jarzynski Equality with a Trapped Ion System. Nature Phys., 2014, 11:193-199.

[4] Wang Y, Um M, et al. Single qubit quantum memory exceeding ten-minute coherence time. Nature Photonics. 2017, 11(10):646.

[5] Lv D, An S, Um M, et al. Reconstruction of the Jaynes-Cummings field state of ionic motion in a harmonic trap. Phys. Rev. A, 2018, 95:043813.

[6] Park J, Zhang J, Um M, et al. Testing Nonclassicality and Non-Gaussianity in Phase Space. Phys. Rev. Lett. 2015, 114:190402.

[7] Xie T, Jin N, Um M, et al. Frequency stabilization of a 650 nm laser to an I2 spectrum for trapped ^{138}Ba^{+} ions. JOSA B, 2019, 36:243−247.

研究成果