High-dimensional cryptographic quantum parameter estimation

Dong Xie,* Chunling Xu, and Jianyong Chen
Faculty of Science, Guilin University of Aerospace Technology, Guilin, Guangxi, P.R. China.

An Min Wang
Department of Modern Physics , University of Science and Technology of China, Hefei, Anhui, China.

We investigate cryptographic quantum parameter estimation with a high-dimensional system that allows only Bob (Receiver) to access the result and achieve optimal parameter precision from Alice (Sender). Eavesdropper (Eve) only can disturb the parameter estimation of Bob, but she can not obtain the information of parameter. And Bob can still securely obtain a high-precision estimation of parameter by utilizing the parallel-entangled strategy and sequential strategy with a large repeat count of communication. We analyze the security and show that the high-dimensional system can help to utilize the resource to obtain better precision than the two-dimensional system. Finally, we generalize it to the case of multi-parameter.

PACS numbers: 03.67.Dd, 06.20.-f, 06.60.Ei

I. INTRODUCTION

Quantum cryptography[1] has been the first application of quantum mechanics at the single-quantum level[2]. Based on the laws of quantum mechanic physics, unconditional security is provided by quantum cryptograph, which performs better than classical cryptograph[3]. And the estimation of physical parameters and the improvement of measurement precision by employing quantum mechanics (quantum metrology), have attracted considerable attention[4–10].

In ref.[11], V. Giovannetti et al. detail a scheme that employs entanglement and squeezing to achieve a higher accuracy and cryptographic capabilities in position measurement, which do not allow an eavesdropper to obtain information on the position of Alice. And in ref.[12] they overcome the primary drawbacks of this scheme, which are the difficulty of creating the requisite entanglement and the sensitivity to loss. In ref.[13] they present a protocol that, using the frequency entangled state at the output of a parametric down conversion crystal, allows one to perform quantum crypto-positioning. In ref.[14] G. Chiribella et al. give a simple protocol that needs no entanglement and an entangled protocol that achieves the ultimate bounds in the precision of reference frame transmission.

Recently, Zixin Huang et al.[15] introduce a work for quantum cryptographic protocols specifically suited to the task of securing measurement out-comes (parameter estimation) with a two-dimensional system. In this article, we consider a new cryptographic quantum metrology with a high-dimensional probe system. Our quantum cryptographic protocol can perform better with the same number of probes than the one in[15]. It is because that utilizing high-dimensional probes need not decoy states to detect Eve. For a single parameter, the information of parameter is randomly encoded into any two dimensions of a multi-dimensional probe. Due to the indistinguishable encoded states of probes from Alice, Eve can not obtain the detail input states. We analyze the security and prove that Eve can not obtain the information of parameter without having been detected. Even though Eve does not worry to be detected, she still can not obtain the information of parameter due to that Alice does not tell Bob the information of prepared states with the classical communication after detecting Eve. Finally, we generalize it to cryptographic quantum multi-parameter estimation.

The rest of this article is arranged as follows. In Section II, we briefly introduce the quantum metrology of single parameter and multi-parameter, and the formula of Fisher information. In Section III, we detail the cryptographic quantum metrology protocol of a single parameter and show its security. Then, we generalize it to multi-parameter cryptographic quantum metrology protocol in section IV. A conclusion and outlook are presented in Section V.

II. REVIEW OF QUANTUM METROLOGY

Quantum metrology is a fundamental subject concerning the estimation of parameters under the constraints of quantum dynamics[7]. The famous Cramér-Rao bound[16, 17] offers a very good parameter estimation under the

*Electronic address: xiedong@mail.ustc.edu.cn

constraints of quantum physics:

$$(\delta x)^2 \geq \frac{1}{N\mathcal{F}_Q[\hat{\rho}(x)]}, \tag{1}$$

where N represents the total number of experiments. $\mathcal{F}_Q[\hat{\rho}(x)]$ denotes quantum Fisher information (QFI), which can be generalized from classical Fisher information. The classical Fisher information is defined by

$$f(x) = \sum_k p_k(x)[d\ln[p_k(x)]/dx]^2, \tag{2}$$

where $p_k(x)$ is the probability of obtaining the set of experimental results k for the parameter value x. Furthermore, the QFI is given by the maximum of the Fisher information over all measurement strategies allowed by quantum physics:

$$\mathcal{F}_Q[\hat{\rho}(x)] = \max_{\{\hat{E}_k\}} f[\hat{\rho}(x); \{\hat{E}_k\}], \tag{3}$$

where positive operator-valued measure $\{\hat{E}_k\}$ represents a specific measurement device. If the probe state is pure, $\hat{\rho}_S(x) = |\psi(x)\rangle\langle\psi(x)|$, the corresponding expression of QFI is

$$\mathcal{F}_Q[\hat{\rho}(x)] = 4[\frac{d\langle\psi(x)|}{dx}\frac{d|\psi(x)\rangle}{dx} - |\frac{d\langle\psi(x)|}{dx}|\psi(x)\rangle|^2]. \tag{4}$$

For the classical multi-parameter Cramér-Rao bound[6]:

$$\mathrm{Cov}(\widetilde{\mathbf{x}}) \geq F^{-1}, \tag{5}$$

where $\mathbf{x} = \{x_1, x_2, ..., x_m\}$, $\mathrm{Cov}(\widetilde{\mathbf{x}})$ refers to the covariance matrix for a locally unbiased estimator $\widetilde{\mathbf{x}}(k)$, $\mathrm{Cov}(\widetilde{\mathbf{x}})_{jk} = \langle(\widetilde{x}_j - x_j)(\widetilde{x}_k - x_k)\rangle$ and $\langle.\rangle$ represents the average with respect to the probability distribution $p_k(\mathbf{x})$. The classic Fisher matrix for m parameters as the $m \times m$ matrix with entries given by

$$F_{jk} = \sum_i p_k(x)\left(\frac{\partial\ln[p_i(x)]}{\partial x_j}\right)\left(\frac{\partial\ln[p_i(x)]}{\partial x_k}\right). \tag{6}$$

III. CRYPTOGRAPHIC QUANTUM METROLOGY PROTOCOL OF SINGLE PARAMETER

The task of cryptographic quantum metrology is that Alice sends a d ($d \geq 3$) dimension probe encoded with an unknown single parameter φ to Bob, then Bob obtains the parameter by measurement. The Hilbert space of a probe can be expressed by $(|1\rangle, |2\rangle, ..., |d\rangle)$. The parameter φ is encoded into any two levels by a unitary map $U(\varphi)$. When Alice prepares state $\frac{\sqrt{2}}{2}(|j\rangle + |k\rangle)$ ($j < k$ and $j, k = 1, 2, ..., n$), after the unitary map the encoded state is described by $\frac{\sqrt{2}}{2}(e^{-i\varphi/2}|j\rangle + e^{i\varphi/2}|k\rangle)$. For different prepared state, different unitary map is required. After repeating ν times estimation procedure, the precision can be obtained by Eq.(4)

$$\delta\varphi \geq 1/\sqrt{\nu}. \tag{7}$$

In order to improve the precision of parameter, parallel-entangled strategy and sequential strategy[15] can improve the precision to the Heisenberg limit. For the parallel-entangled strategy, the encoded state of n probes is $\frac{\sqrt{2}}{2}(e^{-in\varphi/2}|j\rangle^{\otimes n} + e^{in\varphi/2}|k\rangle^{\otimes n})$. For sequential strategy, after n times unitary maps the encoded state is $\frac{\sqrt{2}}{2}(e^{-in\varphi/2}|j\rangle + e^{in\varphi/2}|k\rangle)$. The corresponding precisions for two strategies are same, which is given by

$$\delta\varphi \geq 1/(n\sqrt{\nu}). \tag{8}$$

Next, we consider transforming the metrology protocols into quantum cryptographically secure ones with two strategies.

Sequential strategy- Firstly, for sequential strategy, cryptographical quantum metrology protocol of a single parameter can be described by the following six steps:

1. First step, Alice randomly prepares state $\frac{\sqrt{2}}{2}(|j\rangle \pm |k\rangle)$, in which, $j \neq k$,j, $k = 1, 2, ..., d$ and the operations "+" and "-" is also chosen uniformly at random;
2. Second step, Alice sequentially uses n times unitary map channel to encode the information of parameter φ, hence obtains state$\frac{\sqrt{2}}{2}(e^{-in\varphi/2}|j\rangle \pm e^{in\varphi/2}|k\rangle)$;
3. Third step, after Bob receives the encoded state from Alice (Alice determines that Bob has received the encoded state by classical communication), Alice tells Bob the measurement operators by classical communication, where the measurement operator can be described by POVM formalism (Positive Operator-Valued Measure)[18],
$$\{E_1 = \frac{1}{2}(|j\rangle + |k\rangle)(\langle j| + \langle k|), \ E_2 = \frac{1}{2}(|j\rangle - |k\rangle)(\langle j| - \langle k|), \ E_3 = 1 - |j\rangle\langle j| - |k\rangle\langle k|\}. \quad (9)$$
4. Fourth step, Bob tells Alice the measurement results. If Bob obtains the result E_3, the protocol is aborted due to that the parameter has been eavesdropped by Eve.
5. Fifth step, repeat the above four steps ν times.
6. Sixth step, Alice tells Bob the prepared states in order.
   Then Bob can obtain the information parameter and estimate the precision.

Then we show that it is unconditionally secure from two cases as following: first case, Eve can not let Bob obtain the wrong information of parameter φ without being detected; second case, Eve can not eavesdrop the information of parameter φ.

First case-If Eve just want to let Bob obtain the wrong information of φ without being detected, she can introduce additional $\Delta\varphi$ on the probe to bias Bobs estimation results. Due to that Eve do not know which subspace ($|j\rangle$, $|k\rangle$) is chosen each time by Alice to prepare the probe, so it is impossible to induce the same additional $\Delta\varphi$ on different encoded states. When Eve let the encoded probes go through a fixed channel, different additional $\Delta\varphi$ is encoded into different input probes. As a result, Bob receives the state $\frac{\sqrt{2}}{2}(e^{-i(n\varphi/2+\Delta\varphi_{jk})/2}|j\rangle \pm e^{i(n\varphi/2+\Delta\varphi_{jk})/2}|k\rangle)$. Then, Bob obtains different parameter value of φ by the measurement probability. So Eve will be detected. Eve need to randomly introduce different additional $\Delta\varphi_{jk}$, and the expectation value of $\Delta\varphi_{jk}$ should be same $\langle\Delta\varphi_{jk}\rangle = \Delta$ for different value of (j,k). And we note that $\Delta\varphi_{jk} = -\Delta\varphi_{kj}$. It can be proved easily. For example, Eve uses a Hamiltonian H to induce the additional phase. And ($|j\rangle$, $|k\rangle$) should be the eigenvectors of H. Otherwise, it is impossible to obtain the state $\frac{\sqrt{2}}{2}(e^{-i(n\varphi/2+\Delta\varphi_{jk})/2}|j\rangle \pm e^{i(n\varphi/2+\Delta\varphi_{jk})/2}|k\rangle)$. Then $\Delta\varphi_{jk} = (H_j - H_k)t$, where H_j denotes the jth eigenvalue of H. So $\Delta\varphi_{jk} = -\Delta\varphi_{kj}$. Namely the expectation value of $\langle\Delta\varphi_{jk}\rangle = -\langle\Delta\varphi_{jk}\rangle$. So Δ has to be 0. Therefore, Bob still obtains the value of parameter φ without a bias. Eve only reduces the precision. We consider that the probability distribution of $\Delta\varphi_{jk}$ is the Gaussian distribution $\frac{1}{\sqrt{2\pi}\delta}\exp[-\frac{(\Delta\varphi_{jk})^2}{2\delta^2}]$. The probability of result E_1 (E_2) is given by P (1-P),

$$P = \frac{1 + \cos(n\varphi)e^{-\delta^2/2}}{2}. \quad (10)$$

Substituting it into Eq.(6), the precision can be given by

$$\delta\varphi \geq \frac{\sqrt{1 - \cos^2(n\varphi)e^{-\delta^2}}}{n\sqrt{\nu\sin^2(n\varphi)e^{-\delta^2}}}. \quad (11)$$

Obviously, the precision of $\delta\varphi$ is reduced. For $\varphi \neq N\pi$ ($N = 0, \pm1, \pm2, ...$), the influence of Eve can be neglected by enhancing the repeat count ν and n. However, for $\varphi = N\pi$, the influence of Eve can not be reduced. Then Bob gives up the result. Then they perform the cryptographical quantum metrology protocol again, but Bob measures the encoded state with a new measurement operator in the third step

$$\{E_1 = \frac{1}{2}(e^{-i\pi/4}|j\rangle + e^{i\pi/4}|k\rangle)(e^{-i\pi/4}\langle j| + e^{i\pi/4}\langle k|), \ E_2 = \frac{1}{2}(e^{-i\pi/4}|j\rangle - e^{i\pi/4}|k\rangle)(e^{-i\pi/4}\langle j| - e^{i\pi/4}\langle k|),$$
$$E_3 = 1 - |j\rangle\langle j| - |k\rangle\langle k|\}. \quad (12)$$

In this way, Bob can obtain the parameter φ with a high precision for $\varphi = N\pi$,

$$\delta\varphi \geq \frac{\sqrt{1-e^{-\delta^2}}}{n\sqrt{\nu e^{-\delta^2}}}. \tag{13}$$

Second case-Even though Eve does not worry to be detected, she can not obtain the information of parameter φ from the decoded states. Because, after Eve is detected, she does not know the prepared states belonging to which one of $\frac{\sqrt{2}}{2}(|j\rangle + |k\rangle)$ and $\frac{\sqrt{2}}{2}(|j\rangle - |k\rangle)$. As a result, the probability of obtaining the results E_1 and E_2 is same, so that it is impossible to obtain the information of parameter. In order to obtain the information, Eve need to conceal herself. After Eve intercepts the encoded states, she has to send destroyed or forged states to Bob. Eve can try to eavesdrop the information by the following two ways.

First way, Eve does not perform a measurement on the encoded state before sending a state to Bob. Eve randomly sends a state from the set $\{\frac{\sqrt{2}}{2}(|j'\rangle \pm |k'\rangle)$, in which, $j' \neq k'$ and $j', k' = 1, 2, ..., d\}$. She can successfully conceal herself with the probability $(\frac{2}{d})^\nu$. For large dimension d and repeat count ν, Eve will be detected with the probability close to 1. If Eve sends the state $\frac{1}{\sqrt{d}}(|1\rangle + |2\rangle + , ..., + |d\rangle)$, she can conceal herself with probability $(\frac{2}{d})^\nu$. The successful probability is still close to 0. So, it is impossible to conceal herself without measurement on the encoded states in advance.

Second way, Eve performs a measurement on the encoded states and then sends a state to Bob. At this point, Eve does not know the measurement operator as shown in Eq.(9).

If Eve chooses a projective measurement, which is given by

$$P_k = |k\rangle\langle k|, \text{ in which, } k = 1, 2, ..., d. \tag{14}$$

Then, Eve sends the projective state $|k'\rangle$ to Bob. By this measurement operator, Eve obtains nothing about the parameter φ. Bob can not detect Eve directly in the above process. However, Bob can find that the probability of results E_1 and E_2 is same, so Bob need to give up the result. If Eve just wants to let Bob achieve the wrong information of parameter φ, she can measure a part of encoded state. This will reduce the precision of estimating parameter φ. When Eve randomly measures m encoded states. The final precision of parameter is achieved by Bob, which is given by

$$\delta\varphi \geq \frac{\sqrt{1-(1-m/\nu)^2\cos^2(n\varphi)}}{n(\nu-m)|\sin(n\varphi)|}. \tag{15}$$

For $\varphi \neq N\pi$ ($N = 0, \pm1, \pm2, ...$), the influence of Eve can be neglected by enhancing the repeat count ν to be much larger than m. However, for $\varphi = N\pi$, the influence of Eve can be very large. So, when Bob achieves the value of parameter $\varphi = N\pi$, Bob should not trust the result. Then they perform the cryptographical quantum metrology protocol again like the above way, and Bob measures the encoded state with the measurement operator in Eq.(12).

If Eve sends a superposition state $|k'\rangle + e^{i\theta}|k''\rangle$, where k' is the measurement result and $k'' \neq k'$ is randomly chosen from 1 to d, and θ is a random phase factor. Eve can conceal herself with probability $(\frac{d+1}{2d})^\nu$. For a large repeat count ν, Eve can be detected with the probability of 1.

In order to obtain the information of parameter, Eve maybe use POVM

$$P_{jk} = \frac{1}{2d-2}(|j\rangle + |k\rangle)(\langle j| + \langle k|), \text{ in which, } j < k = 1, 2, ..., d, \ P_0 = 1 - \sum_{j<k} P_{jk}. \tag{16}$$

Eve can conceal herself with the probability

$$\left\{\frac{1}{2} + \frac{3}{4(d-1)} + \left[\frac{1}{2} - \frac{3}{4(d-1)}\right]\frac{2d-1}{d(d-1)}\right\}^\nu. \tag{17}$$

For $\nu \gg 1$, Eve must be detected. So it is very secure. If Bob does not reveal Eve, Eve can obtain the information with the precision

$$\delta\varphi \geq \sqrt{\frac{8[d-1-\cos^2(n\varphi/2)]\cos^2(\frac{n\varphi}{2})}{\nu n^2\sin^2(n\varphi)}}. \tag{18}$$

For high dimension d, Eve only achieve a very low precision of parameter.

Besides the above two measurement ways, Eve can also use other measurements. However, due to the indistinguishable states (non-orthogonal states) prepared by Alice, Eve must be detected no matter which measurement is chosen.

In one word, our cryptographical quantum metrology protocol is secure. Bob will not obtain the wrong information of parameter and the information of parameter can not be eavesdropped by Eve.

Parallel-entangled strategy-Entangled states can also help to enhance the parameter estimation in quantum metrology[19, 20]. The corresponding cryptographical quantum metrology protocol of a single parameter can be modified as follows:

1. First step, Alice randomly prepares state of n probes $\frac{\sqrt{2}}{2}(|j\rangle^{\otimes n} \pm |k\rangle^{\otimes n})$, in which, $j < k,\ j, k = 1, 2, ..., d$; and the operations"+" and "-" is also chosen uniformly at random;
2. Second step, simultaneously use n unitary map channels to encode the information of parameter φ, hence obtain state$\frac{\sqrt{2}}{2}(e^{-in\varphi/2}|j\rangle^{\otimes n} \pm e^{in\varphi/2}|k\rangle^{\otimes n})$;
3. Third step, after Bob receives the encoded state from Alice, Alice tells Bob the measurement operators by classical communication, where the measurement operator can be described by POVM formalism,
$$\{E_1 = \frac{1}{2}(|j\rangle^{\otimes n} + |k\rangle^{\otimes n})(\langle j|^{\otimes n} + \langle k|^{\otimes n}),\ E_2 = \frac{1}{2}(|j\rangle^{\otimes n} - |k\rangle^{\otimes n})(\langle j|^{\otimes n} - \langle k|^{\otimes n}),\ E_3 = 1 - E_1 - E_2\}. \quad (19)$$
4. Fourth step, Bob tells Alice the measurement results. If Bob obtains the result E_3, the protocol is aborted due to that the parameter is eavesdropped by Eve.
5. Fifth step, repeat the above four steps ν times.
6. Sixth step, Alice tells Bob the prepared states in order.
Then Bob can obtain the information parameter and estimate the precision.

It is also secure like the case of sequential strategy due to the indistinguishable prepared states. Namely, entangled states can also realize the cryptographical quantum metrology with high precision.

IV. CRYPTOGRAPHIC QUANTUM METROLOGY PROTOCOL OF MULTI-PARAMETER

Recently, multi-parameter metrology has attracted a lot of attention[21–25]. Simultaneous estimation of multi-parameter can perform better than estimating each parameter independently. We generalize the above cryptographic quantum metrology protocol of a single parameter to the case of multi-parameter. We consider that Alice want to send m parameters to Bob securely.

The cryptographic quantum metrology protocol of m parameters can be summed as follows:

1. First step, Alice randomly prepares state $\frac{1}{\sqrt{m+1}}(|k_0\rangle \pm |k_1\rangle \pm |k_2\rangle \pm ... \pm |k_m\rangle)$, in which, (20)
   $\{k_a,\ k_b = 1, 2, ..., d\}, \{a, b = 0, 1, 2, ...m\},\ d > m+1,$ and $k_a \neq k_b$ for $a \neq b$;
2. Second step, sequentially use n times unitary operators $U(\varphi_1)$ to encode the information of parameter φ_1, according to this way, encode all parameters $\{\varphi_1, \varphi_2, ..., \varphi_n\}$ on the prepared state, hence obtain the state $\frac{1}{\sqrt{m+1}}(|k_0\rangle \pm e^{in\varphi_1}|k_1\rangle \pm e^{in\varphi_2}|k_2\rangle \pm ... \pm e^{in\varphi_m}|k_m\rangle$;
3. Third step, after Bob receives the encoded state from Alice, Alice tells Bob the measurement operators by classical communication, where the measurement operator can be described by POVM formalism
   $\{E_{1\pm} = \frac{1}{2}(\frac{1}{\sqrt{n}}|k_0\rangle \pm |k_1\rangle)(\frac{1}{\sqrt{n}}\langle k_0| \pm \langle k_1|),\ E_{2\pm} = \frac{1}{2}(\frac{1}{\sqrt{n}}|k_0\rangle \pm |k_2\rangle)(\frac{1}{\sqrt{n}}\langle k_0| \pm \langle k_2|),$
   $...,\ E_{m\pm} = \frac{1}{2}(\frac{1}{\sqrt{n}}|k_0\rangle \pm |k_m\rangle)(\frac{1}{\sqrt{n}}\langle k_0| \pm \langle k_m|),\ E_{m+1} = 1 - E_{1+} - E_{1-} - ... - E_{m+} - E_{m-}\}.$ (21)
4. Fourth step, Bob tells Alice the measurement result. If Bob obtains the result E_{m+1}, the protocol is aborted due to that the parameter is eavesdropped by Eve.
5. Fifth step, repeat the above four steps ν times.
6. Sixth step, Alice tells Bob the prepared states in order.
   Then Bob can obtain the information of m parameter by calculating the probability and estimate the precision.

When the protocol can perform without being aborted due to Eve, the probability of measurement result for $E_{j\pm}$ is given by $P_{j\pm} = \frac{1}{2m+2}[\frac{1}{m} + 1 \pm \frac{2}{\sqrt{m}}\cos[2n\varphi_j]]$, with $j = 1, 2, ..., m$. The precision of m parameters can be obtained by Eq.(5) and Eq.(6)

$$\delta\varphi_j \geq \sqrt{\frac{(m+1)^2 - 4m\cos^2(2n\varphi_j)}{\nu n^2 \sin^2\varphi_j}}. \tag{22}$$

Like the case of a single parameter, Eve can not eavesdrop the information of m parameters based on the undistinguished prepared states.

V. CONCLUSION AND OUTLOOK

The cryptographic quantum metrology of a single parameter with a high-dimensional system is studied. The high-dimensional system can satisfy the security by preparing the indistinguishable states. Decoy-state is not necessary to detect Eve for our protocol. We analyze the security and show that it is absolutely secure for a large repeat count. And parallel-entangled strategy and sequential strategy can be utilized to improve the parameter precision. We also utilize the techniques of multi-parameter quantum metrology and quantum cryptography to obtain the cryptographic quantum metrology protocol of multi-parameter.

In this article, we only consider the unitary parameters. Cryptographic quantum metrology protocol of the non-unitary parameters[26, 27] will worth to be the further exploration. And a lossy channel and imperfect measurement in cryptographic quantum metrology also will be researched.

Acknowledgement

This research was supported by the National Natural Science Foundation of China under Grant No. 11747008, Guangxi Natural Science Foundation 2016GXNSFBA380227 and Guangxi Base Promotion Project of Young and Middle-aged Teachers (NO.2017KY0857).

References

[1] C. H. Bennett, G. Brassard, and N. D. Mermin: Quantum cryptography without Bells theorem. Phys. Rev. Lett. **68**, 557 (1992).

[2] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002).

[3] W. C. Cheng and M. Aritsugi: A User Sensitive Privacy-preserving Location Sharing System in Mobile Social Networks. Procedia Computer Science **35**, 1692 (2014).

[4] J. P. Dowling: Quantum optical metrology-the lowdown on high-N00N states. Contemp. Phys. **49**, 125 (2008).

[5] C. W. Helstrom: Quantum Detection and Estimation Theory. Academic, New York (1976).

[6] S. L. Braunstein, C. M. Caves: Statistical distance and the geometry of quantum states. Phys. Rev. Lett. **72**, 3439 (1994).

[7] V. Giovannetti, S. Lloyd, and L. Maccone: Quantum-Enhanced Measurements: Beating the Standard Quantum Limit. Science **306**, 1330 (2004).

[8] Alessandro Farace, Antonella De Pasquale, Gerardo Adesso, and Vittorio Giovannetti: Building versatile bipartite probes for quantum metrology. New J. Phys. **18**, 013049 (2016).

[9] Thomas Unden, Priya Balasubramanian, Daniel Louzon, Yuval Vinkler, Martin B. Plenio, Matthew Markham, Daniel Twitchen, Igor Lovchinsky, Alexander O. Sushkov, Mikhail D. Lukin, Alex Retzker, Boris Naydenov, Liam P. Mcguinness, and Fedor Jelezko: Quantum Metrology Enhanced by Repetitive Quantum Error Correction. Phys. Rev. Lett. **116**, 230502 (2016).

[10] Dong Xie, Chunling Xu, and An Min Wang: Quantum metrology in coarsened measurement reference. Phys. Rev. A **95**, 012117 (2017).

[11] V. Giovannetti, S. Lloyd, and L. Maccone: Positioning and clock synchronization through entanglement. Phys. Rev. A **65**, 022309 (2002).

[12] V. Giovannetti, S. Lloyd, and L. Maccone: Quantum-enhanced positioning and clock synchronization. Nature **412**, 417 (2001).

[13] V. Giovannetti, S. Lloyd, and L. Maccone: Quantum cryptographic ranging. Journal of Optics B: Quantum and Semiclassical Optics **4**, 413 (2002).

[14] G. Chiribella, L. Maccone, and P. Perinotti: Secret Quantum Communication of a Reference Frame. Phys. Rev. Lett. **98**, 120501 (2007).

[15] Zixin Huang, Chiara Macchiavello, and Lorenzo Maccone: Cryptographic quantum metrology. arXiv:1706. 03894v1 (2017).

[16] H. Cramér: Mathematical Methods of Statistics. Princeton University, Princeton (1946).

[17] C. R. Rao: Linear Statistical Inference and Its Applications. John Wiley and Sons, New York (1973).

[18] Michael A. Nielsen, and Isaac L. Chuang: Quantum computation and quantum information. Cambridge University Press, Cambridge (2000).

[19] Bryn Bell, Srikanth Kannan, Alex McMillan, Alex S. Clark, William J. Wadsworth, and John G. Rarity: Multicolor Quantum Metrology with Entangled Photons. Phys. Rev. Lett. **111**, 093603 (2013).

[20] Jaewoo Joo, William J. Munro, and Timothy P. Spiller: Quantum Metrology with Entangled Coherent States. Phys. Rev. Lett. **107**, 083601 (2011).

[21] Lu Zhang, Kam Wai Clifford Chan: Quantum multiparameter estimation with generalized balanced multimode NOON-like states. Phys. Rev. A **95**, 032321 (2017).

[22] Nana Liu, Hugo Cable: Quantum-enhanced multi-parameter estimation for unitary photonic systems. Quantum Science and Technology **2**, 2 (2017).

[23] Magdalena Szczykulska, Tillmann Baumgratz, Animesh Datta: Multi-parameter quantum metrology. Advances in Physics: X **1**, 621 (2016).

[24] P. A. Knott, T. J. Proctor, A. J. Hayes, J. F. Ralph, P. Kok, J. A. Dunningham: Local versus global strategies in multiparameter estimation. Phys. Rev. A **94**, 062312 (2016).

[25] Kevin C. Young, Mohan Sarovar, Robert Kosut, K. Birgitta Whaley: Optimal quantum multiparameter estimation and application to dipole- and exchange-coupled qubits, Phys. Rev. A **79**, 062301 (2009).

[26] U. Dorner, R. Demkowicz-Dobrzanski, B. Smith, J. Lundeen, W. Wasilewski, K. Banaszek, andI.Walmsley: Optimal Quantum Phase Estimation. Phys. Rev. Lett. **102**, 040403 (2009).

[27] S. I. Knysh and G. A. Durkin: Estimation of Phase and Diffusion: Combining Quantum Statistics and Classical Noise. arXiv:1307. 0470 (2013).