Anonymous Quantum Sensing

Hiroto Kasai[1,2], Yuki Takeuchi[3], Hideaki Hakoshima[2,4],
Yuichiro Matsuzaki[2], Yasuhiro Tokura[1]

[1]Graduate School of Pure and Applied Sciences, University of Tsukuba
[2]Research Center for Emerging Computing Technologies,
National institute of Advanced Industrial Science and Technology (AIST)
[3]NTT Communication Science Laboratories, NTT Corporation
[4]Center for Quantum Information and Quantum Biology, Osaka University
E-mail: kasai-q@aist.go.jp

Purpose

Quantum anonymous communication :

Senders can send a message without revealing his identity to other parties[2-6].

Quantum remote sensing:

A client can obtain a value of the magnetic field generated at the server side without letting the server know the value[30],[31],[37].

Our paper **:**

The concept to combine quantum anonymous communication and quantum remote sensing is called “Anonymous Quantum Sensing” [43].

Quantum Sensors can broadcast values of magnetic field by hiding information about where magnetic fields exist. **Simply speaking, we do not want to obtain the position distribution of magnetic field $\boldsymbol{\omega(x)}$ but want to obtain exactly histogram of magnetic field $\mathbf{P(\omega)}$.** $\delta\omega(x) \to \infty, \delta P(\omega) \to 0$

Consider only attack in after the implementation of the protocol.
Attack during the implementation of the protocol is discussed in conclusion.

Definitions of entity

V : **Set of all n-agents** (Each has a quantum sensor). n is known. $\boldsymbol{n \geq 5}$.

S : **Set of all m-senders**. Whose quantum sensors with **non-zero magnetic fields** ($\omega > 0$). $m = 2$.

D : There is one distributer of quantum states.

M : There is a measurer of quantum states.

Initial state: $\rho_{init} \equiv q\,|\phi^n_{0,+}\rangle\langle\phi^n_{0,+}| + (1-q)\,|\phi^n_{a,+}\rangle\langle\phi^n_{a,+}| \quad (2 < a \leq [\frac{n}{2}], 0 \leq q \leq 1)$

Superposition of Dicke state :

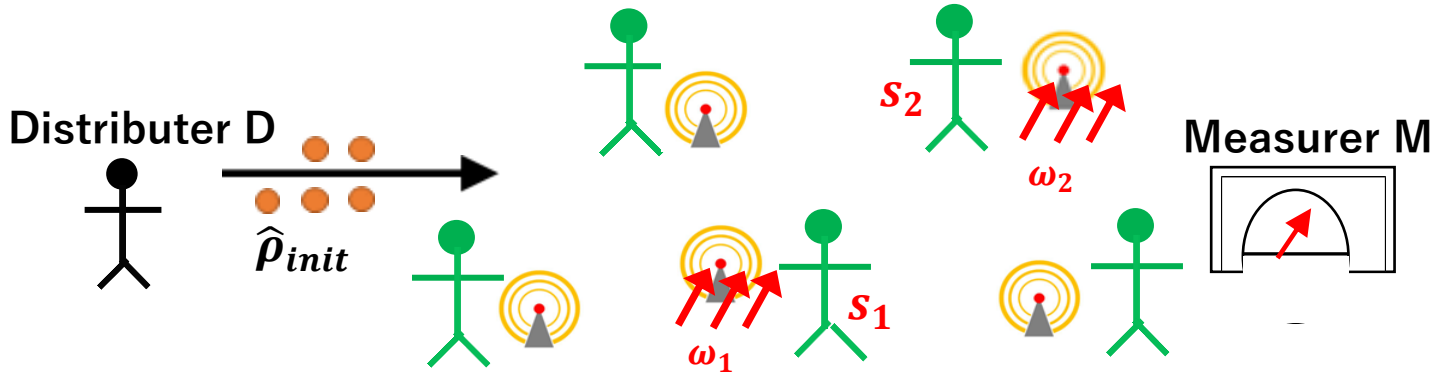
$$|\phi^n_{k,l}\rangle \equiv \begin{cases} \frac{1}{\sqrt{2}}\left(|D^n_k\rangle + l\,|D^n_{n-k}\rangle\right) \\ \quad (n \neq 2k, l = \pm) \\ 0 \quad (n = 2k, l = -) \\ |D^n_k\rangle\ (n = 2k, l = +) \end{cases}$$

Dicke state $|D^n_k\rangle$ **:** Coefficient equally weighted superposition of n-qubit state $|x\rangle$ whose hamming weight satisfies $hw(x) = k$ [38-40].

$$|D^n_k\rangle \equiv \frac{1}{\sqrt{{}_nC_k}} \sum_{\substack{x \in \{0,1\}^n \\ hw(x)=k}} |x\rangle$$

Where $k = 0, 1, \ldots, n$

Hamming weight $hw(x)$ **:**
The number of 1 in a bit string x.



All participants V:
In figure, n=5 green persons.

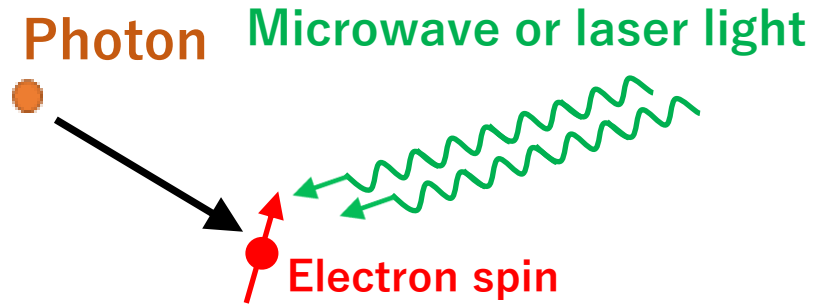
: 1-qubit

: Quantum sensor

: non-zero magnetic field

Transfer state from photon to spin

Irradiate external field (microwave or the laser light) to electron spin and photon which came in here. Then, state of photon-system is transferred to electron spin system.



The quantum circuit describing the following operation is called the SWAP gate.

$$\hat{U}_{SWAP}(|a\rangle_{photon} \otimes |b\rangle_{spin}) = |b\rangle_{photon} \otimes |a\rangle_{spin}$$

The definition of the SWAP gate is the following and this is the swap of 2-qubit state.

$$\hat{U}_{SWAP} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

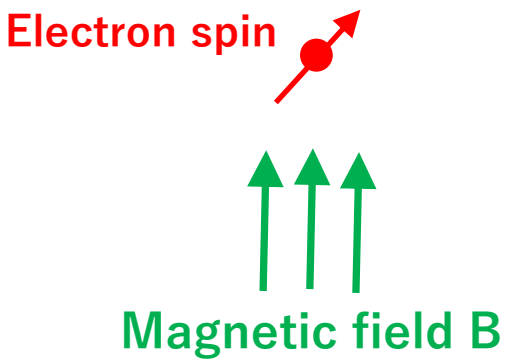
Interaction between electron spin and magnetic field

Consider measurement of magnetic field by using electron spin. In this presentation, we define the direction of magnetic field in figure as z-axis and z-component as B_z.

$\omega = \frac{\mu_B B_Z}{\hbar}$ is Angular frequency which **magnetic moment** of electron rotates around magnetic field.

In this protocol, strength of magnetic field B_z is independent on time and $\hbar = 1$ in the following slide.

magnetic moment $\vec{\mu} = -\frac{g_s \mu_B}{\hbar} \vec{S}$



g_s : g-factor of electron spin

μ_B : Bohr magneton

Mechanism of quantum magnetic-field sensor(1/2)

Preparation of initial state:

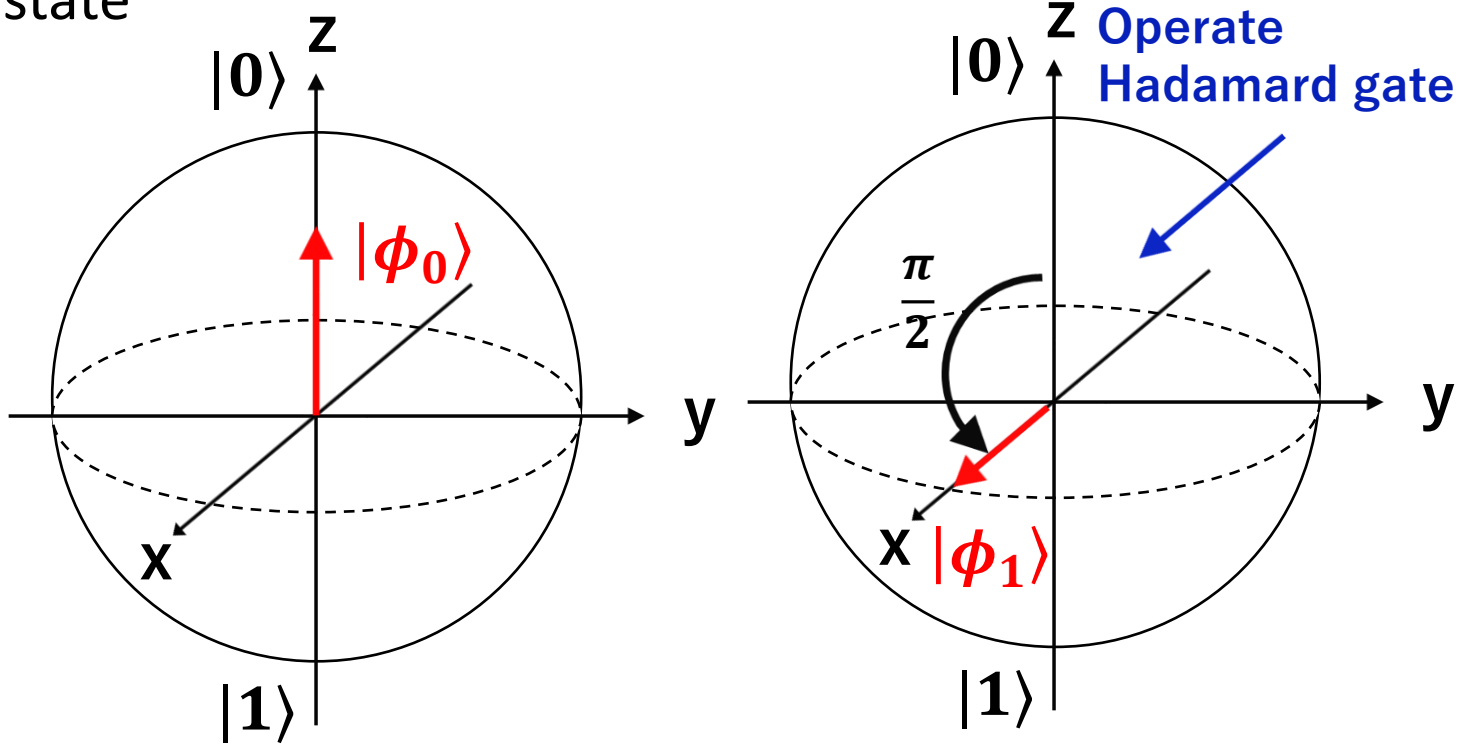
First, prepare initial state that spin directed direction of magnetic field B_z (=Eigenstate of physical quantity σ_z). $\text{Initial state}: \ |\phi_0\rangle = |0\rangle$

Then, operate Hadamard gate on initial state

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

As a result of operation, remain state is following.

$$|\phi_1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right)$$



Mechanism of quantum magnetic-field sensor(2/2)

Interaction between electron spin and magnetic field:

Operate Hamiltonian of magnetic-field sensor on state $|\phi_1\rangle$.

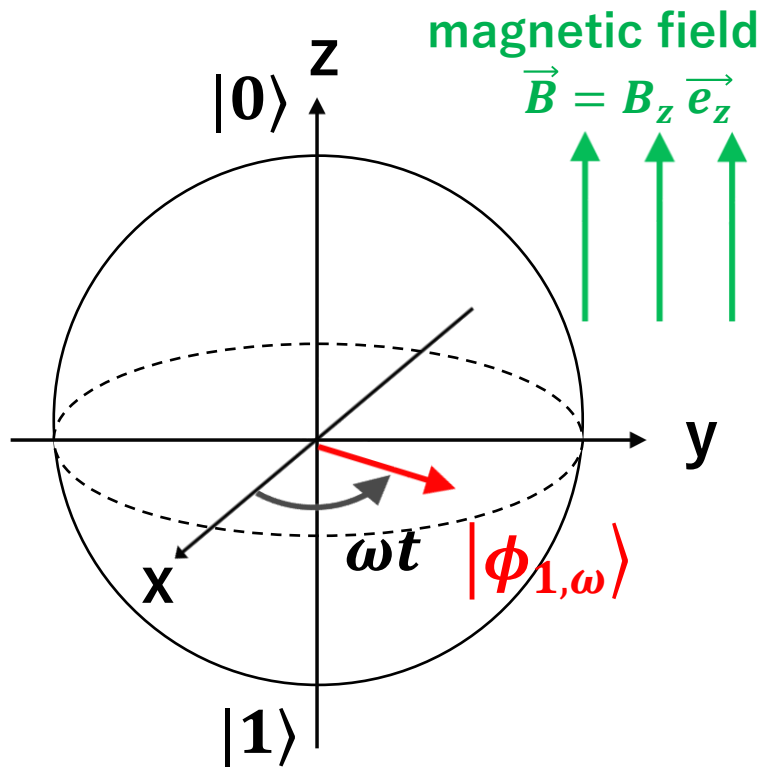
$$\hat{H} = \frac{\omega}{2}\sigma_z$$

The corresponding unitary operator as follows.

$$\hat{U} = e^{-i\hat{H}t} = e^{-\frac{i\omega t}{2}\sigma_z}$$

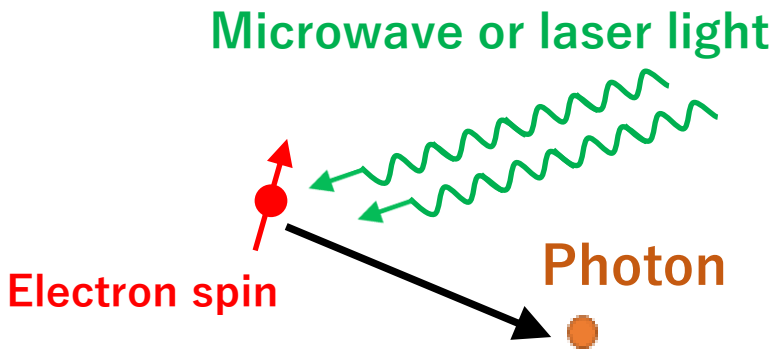
where interaction time that applying magnetic field on electron spin is known constant value t.

$$|\phi_{1,\omega}\rangle = e^{-i\hat{H}t}|\phi_1\rangle = e^{-\frac{i\omega t}{2}}\frac{1}{\sqrt{2}}(|0\rangle + e^{i\omega t}|1\rangle)$$



Transfer state from spin to photon

Irradiate external field (microwave or the laser light) to electron spin, then electron spin emits photon. So, state of electron spin system is transferred to photon-system.



The quantum circuit describing this operation is called the SWAP gate.

$$\hat{U}_{SWAP}(|a\rangle_{photon} \otimes |b\rangle_{spin}) = |b\rangle_{photon} \otimes |a\rangle_{spin}$$

Security Requirements

- **Definition of Attacker**

He cannot attack any quantum states but can steal all classical information after the implementation of the protocol.

- **Demanded Security**

Probability distribution of POVM (= positive operator-valued measure) measurement outcome is independent on the positions in which non-zero magnetic fields are generated.

- **Leak information**

All classical information are probability distribution of POVM, target parameter of estimation $\boldsymbol{\theta_1}, \boldsymbol{\theta_2}$ and sending information that values of non-zero magnetic field $\boldsymbol{\omega_1}, \boldsymbol{\omega_2}$. These quantities will be defined p11.

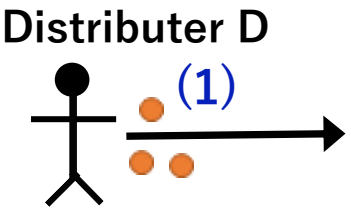
- **Verification**

If Initial state ρ_{init} and POVM is represented as Dick state $|\mathrm{D}_{\mathrm{k}}^{\mathrm{n}}\rangle$ or the superposition $|\phi_{k,\pm}^{n}\rangle$,
probability distribution of POVM measurement outcome is independent of who are senders.
Symmetry, due to the entanglement, helps to hide where the magnetic fields exist.

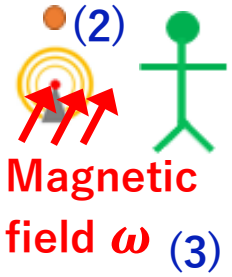
$\langle \mathrm{D}_{\mathrm{k}}^{\mathrm{n}}|U|\mathrm{D}_{\mathrm{k}}^{\mathrm{n}}\rangle, \langle \phi_{k,+}^{n}|U|\phi_{k,\pm}^{n}\rangle$ is independent of senders.

Protocol overview

(2)Each participant has an electron spin, and let the spin absorbs the photon from the distributer D.

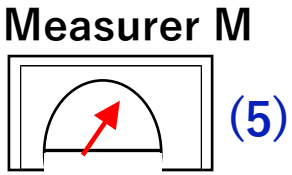


(1)The distributer D generates entangled photons, and distributes these to all participants .



(3)Each participant lets interact the electron spin with the magnetic fields ω at each position.

(4)Each participant converts the electron spin state to the state of the photon, and send them to the measurer M.



(5)The measurer M performs a POVM on the photons from the participants.

	Step (1), (2)	Step (3), (4)	Step (5)
Dependence of magnetic field	×	○	○
Anonymity		×	○

: 1-qubit

: Quantum sensor

: non-zero magnetic field

Setup

Hamiltonian of magnetic sensors which all senders have and the corresponding unitary operator for interaction time t are as follows.

$$\begin{cases} \hat{H} = \frac{1}{2}\sum_{j=1}^{m} w_j \hat{\sigma}_{z,s_j} \\ \hat{U} = e^{-\frac{it}{2}\sum_{j=1}^{m} w_j \hat{\sigma}_{z,s_j}} \end{cases}$$

POVM (for measurement) :

$$\begin{cases} \hat{E}_{0,\pm} = |\phi_{0,\pm}^{n}\rangle\langle\phi_{0,\pm}^{n}| \\ \hat{E}_{a,+} = |\phi_{a,+}^{n}\rangle\langle\phi_{a,+}^{n}| \ (2 < a \leq [\frac{n}{2}]) \\ \hat{E}_{f} = \hat{I} - (\hat{E}_{0,+} + \hat{E}_{0,-} + \hat{E}_{a,+}) \end{cases}$$

Probability distribution of measurement :

$$\begin{cases} P_{0,\pm} = q_0 |\langle\phi_{0,+}^{n}|\hat{U}|\phi_{0,\pm}^{n}\rangle|^2 \\ P_{a,+} = q_a |\langle\phi_{a,+}^{n}|\hat{U}|\phi_{a,+}^{n}\rangle|^2 \\ (2 < a \leq [\frac{n}{2}]) \\ P_{f} = 1 - (P_{0,+} + P_{0,-} + P_{a,+}) \end{cases}$$

Sending information: $\mathbf{0} < \boldsymbol{\omega_1}, \boldsymbol{\omega_2}$

Target parameter of estimation $\boldsymbol{\theta_1}, \boldsymbol{\theta_2}$:

$$\begin{cases} \theta_1 = (\omega_1 + \omega_2)t \\ \theta_2 = (\omega_1 - \omega_2)t \end{cases}$$

In finite time N measurement, considering estimation of unknown parameter $\vec{\varphi} = (\varphi_1, \varphi_2 \ldots, \varphi_m) \in R^m$. Lower limit of variance $(\Delta\varphi_i)^2$ of parameter φ_i $(i = 1,2,\ldots,m)$ is represented by **Cramer-Rao inequality** as following,

$$(\Delta\varphi_i)^2 \geq \frac{1}{N}(J^{-1})_{i,i}$$

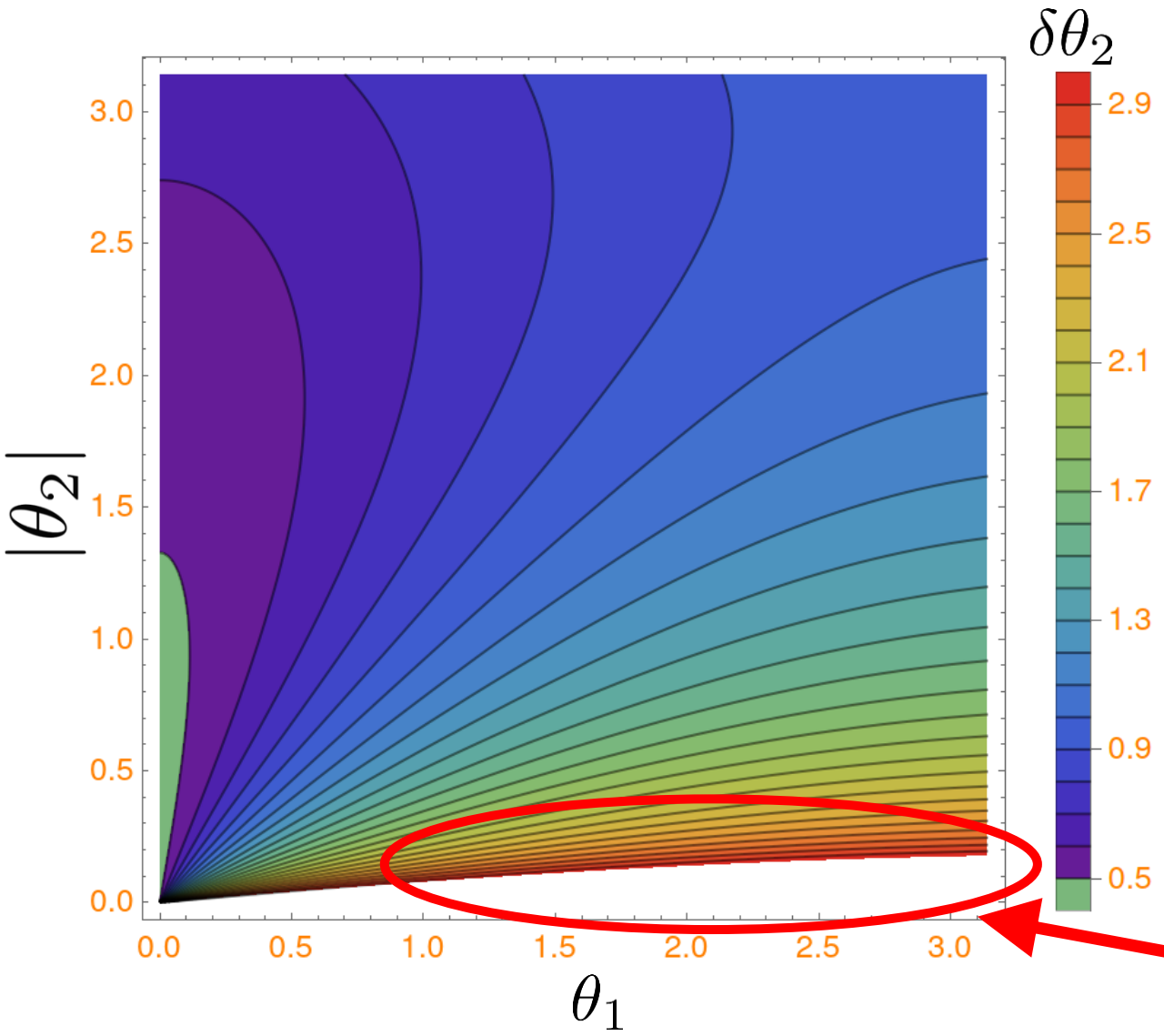
where J is Fisher information matrix.

Fisher information is represented as m-dimensions square matrix J and it is called **Fisher information matrix**. (i,j)-component of J is following.

$$J_{i,j} \equiv \sum_{x\in\chi} \frac{1}{p(x|\vec{\theta})} \frac{\partial p(x|\vec{\theta})}{\partial\theta_i} \frac{\partial p(x|\vec{\theta})}{\partial\theta_j}$$

Where $p(\cdot\,|\,\cdot)$ is probability distribution and $p(\cdot\,|\,\cdot)$ is set of outcome x of probability trial.

Ability of quantum sensing

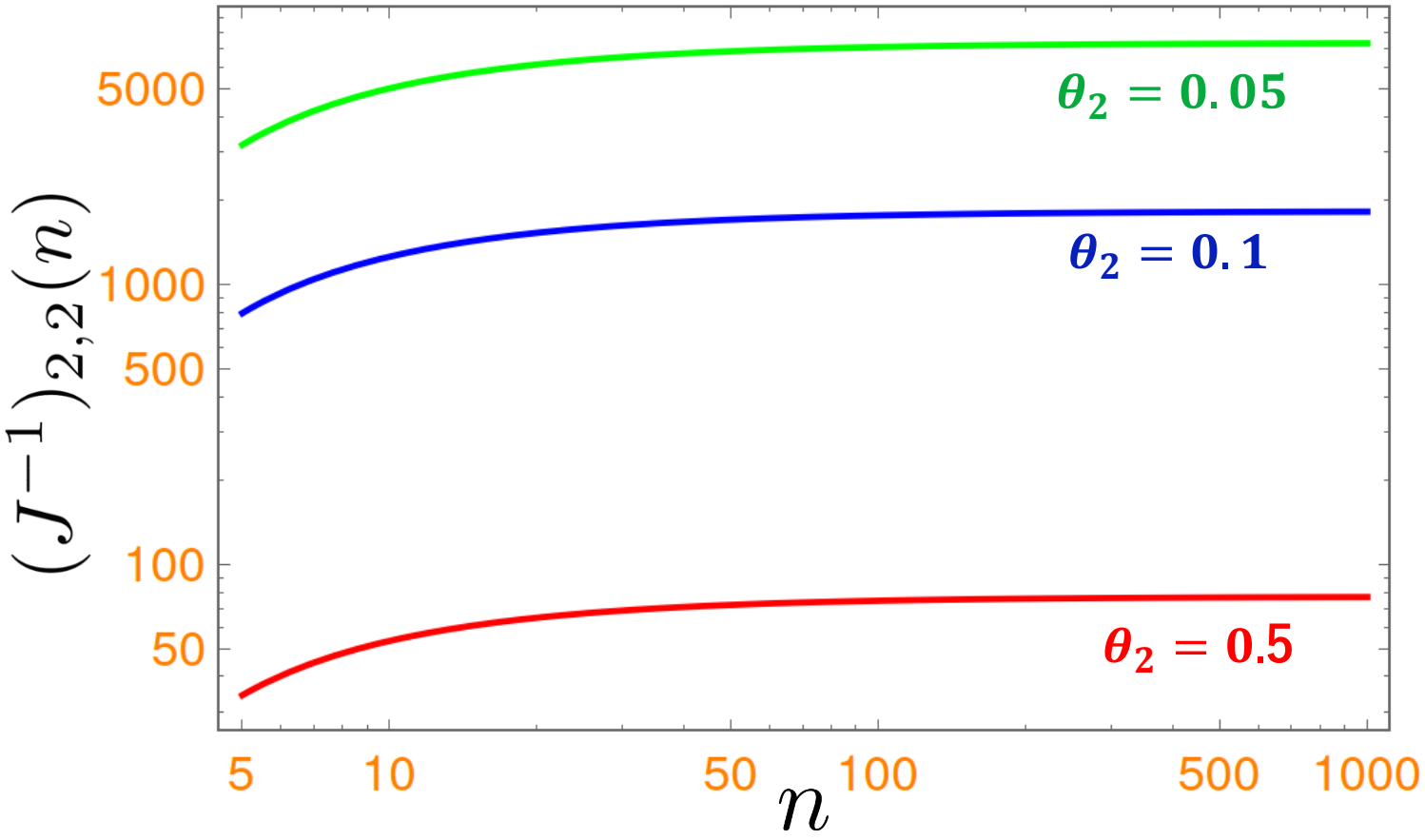


Assumes $\delta\theta_2 \equiv log_{10}\{(J^{-1})_{2,2}(n)\}$, $a = \frac{n}{2}$.
Plot of $\delta\theta_2$ against θ_1 and θ_2 with parameters of $q = 0.33$ and $n = \infty$. θ_1 and θ_2 defined in page 11.

Even if θ_1 changes, $\delta\theta_2$ does not diverge.
But if $|\theta_2|$ approaches zero, $\delta\theta_2$ approaches infinity.

In White zone, $\delta\,\theta_2$ diverges

Ability of quantum sensing



Plot of $(J^{-1})_{2,2}(n)$ against n with parameters of $q = 0.33$, $\theta_1 = 2$ and $\theta_2 = 0.5, 0.1, 0.05$.

As n decreases, $(J^{-1})_{2,2}(n)$ also decreases.

Conclusion and future work

Conclusion： We propose quantum sensing protocol using Dicke states as the following property,

・Values of non-zero magnetic fields can be broadcasted without revealing their positions.

・For $m = 2$ (two non-zero magnetic fields ω_1, ω_2), except when ω_1 is equal to ω_2, we can estimate values of magnetic fields with finite uncertainty of estimation.

Since the magnetic field sensor is used in medical science and material engineering, our protocol could play an important role to protect confidential information once quantum network becomes available.

Future work：

・Although we assume that the measurer obeys the instruction (to perform a specific POVM) in this work, we will relax this condition in the future work.

・We try to propose a protocol with finite estimation uncertainty for arbitrary values of non-zero magnetic fields.

・Consider only attack in after the implementation of the protocol as a first step. Attack during the implementation of the protocol should be consider for more secure protocol. However, in the present discussion, step3 in protocol flow, state verification of state which has unknown values of non-zero magnetic fields is difficult by existing techniques.

・It should be interesting to find other applications.

Ideas for other applications are welcome!

References(1/3)

[1] R. Dingledine, N. Mathewson, and P. Syverson, Proc. 13th Usenix Security Symposium, 2004, p. 303.
[2] M. Christandl and S. Wehner, International Conference on the Theory and Application of Cryptology and Information Security, 2005, p. 217.
[3] V. Lipinska, G. Murta, and S. Wehner, Phys. Rev. A 98, 052320 (2018).
[4] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, International Conference on the Theory and Application of Cryptology and Information Security, 2007, p. 460.
[5] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, Phys. Rev. Lett. 122, 240501 (2019).
[6] T.-Y. Wang, Q.-Y. Wen, and F.-C. Zhu, J. Phys. B 43, 245501 (2010).
[7] J. R. Maze, P. L. Stanwix, J. S. Hodges, S. Hong, J. M. Taylor, P. Cappellaro, L. Jiang, M. G. Dutt, E. Togan, A. Zibrov, A. Yacoby, R. Walsworth, and M. Lukin, Nature 455, 644 (2008).
[8] G. Balasubramanian, I. Chan, R. Kolesov, M. Al-Hmoud, J. Tisler, C. Shin, C. Kim, A. Wojcik, P. R. Hemmer, A. Krueger, T. Hanke, A. Leitenstorfer, R. Bratschitsch, F. Jelezko, and J. Wrachtrup, Nature 455, 648 (2008).
[9] J. Taylor, P. Cappellaro, L. Childress, L. Jiang, D. Budker, P. Hemmer, A. Yacoby, R. Walsworth, and M. Lukin, Nat. Phys. 4, 810 (2008).
[10] I. Kominis, T. Kornack, J. Allred, and M. V. Romalis, Nature 422, 596 (2003).
[11] M. Bal, C. Deng, J.-L. Orgiazzi, F. R. Ong, and A. Lupascu, Nat. Commun. 3, 1324 (2012).
[12] Z. Eldredge, M. Foss-Feig, J. A. Gross, S. L. Rolston, and A. V. Gorshkov, Phys. Rev. A 97, 042337 (2018).
[13] T. J. Proctor, P. A. Knott, and J. A. Dunningham, Phys. Rev. Lett. 120, 080501 (2018).
[14] M. W. Mitchell and S. P. Alvarez, Rev. Mod. Phys. 92, 021001 (2020).
[15] R. Schirhagl, K. Chang, M. Loretz, and C. L. Degen, Annu. Rev. Phys. Chem. 65, 83 (2014).

References(2/3)

[16] J. F. Barry, M. J. Turner, J. M. Schloss, D. R. Glenn, Y. Song, M. D. Lukin, H. Park, and R. L. Walsworth, Proc. Natl. Acad. Sci. U.S.A. 113, 14133 (2016).
[17] H. Xia, A. Ben-Amar Baranga, D. Hoffman, and M. Romalis, Appl. Phys. Lett. 89, 211104 (2006).
[18] C. L. Degen, F. Reinhard, and P. Cappellaro, Rev. Mod. Phys. 89, 035002 (2017).
[19] V. Giovannetti, S. Lloyd, and L. Maccone, Nature 412, 417 (2001).
[20] V. Giovannetti, S. Lloyd, and L. Maccone, J. Opt. B 4, S413 (2002).
[21] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. A 65, 022309 (2002).
[22] G. Chiribella, G. D'ariano, and M. Sacchi, Phys. Rev. A 72, 042338 (2005).
[23] G. Chiribella, L. Maccone, and P. Perinotti, Phys. Rev. Lett. 98, 120501 (2007).
[24] Z. Huang, C. Macchiavello, and L. Maccone, Phys. Rev. A 99, 022314 (2019).
[25] D. Xie, C. Xu, J. Chen, and A. M. Wang, Quantum Inf. Process. 17, 1 (2018).
[26] N. Shettell, E. Kashefi, and D. Markham, Phys. Rev. A 105, L010401 (2022).
[27] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. 96, 010401 (2006).
[28] V. Giovannetti, S. Lloyd, and L. Maccone, Nat. Photonics 5, 222 (2011).
[29] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photonics 12, 1012 (2020).
[30] H. Okane, H. Hakoshima, Y. Takeuchi, Y. Seki, and Y. Matsuzaki, Phys. Rev. A 104, 062610 (2021).
[31] P. Yin, Y. Takeuchi, W.-H. Zhang, Z.-Q. Yin, Y. Matsuzaki, X.-X. Peng, X.-Y. Xu, J.-S. Xu, J.-S. Tang, Z.-Q. Zhou, G. Chen, C.-F. Li, and G.-C. Guo, Phys. Rev. Appl. 14, 014065 (2020).

References(3/3)

[32] S.-R. Zhao, Y.-Z. Zhang, W.-Z. Liu, J.-Y. Guan, W. Zhang, C.-L. Li, B. Bai, M.-H. Li, Y. Liu, L. You, J. Zhang, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, Phys. Rev. X 11, 031009 (2021).
[33] G. Brida, M. Genovese, and I. R. Berchera, Nat. Photonics 4, 227 (2010).
[34] C. A. Pérez-Delgado, M. E. Pearce, and P. Kok, Phys. Rev. Lett. 109, 123601 (2012).
[35] T. Baumgratz and A. Datta, Phys. Rev. Lett. 116, 030801 (2016).
[36] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, Nat. Phys. 10, 582 (2014).
[37] Y. Takeuchi, Y. Matsuzaki, K. Miyanishi, T. Sugiyama, and W. J. Munro, Phys. Rev. A 99, 022325 (2019).
[38] K. Hepp and E. H. Lieb, Ann. Phys. 76, 360 (1973).
[39] R. H. Dicke, Phys. Rev. 93, 99 (1954).
[40] A. Bärtschi and S. Eidenbenz, International Symposium on Fundamentals of Computation Theory, 2019, p. 126.
[41] S. D. Barrett and P. Kok, Phys. Rev. A 71, 060310 (2005).
[42] S. C. Benjamin, D. E. Browne, J. Fitzsimons, and J. J. Morton, New J. Phys. 8, 141 (2006).
[43] H. Kasai, Y. Takeuchi, H. Hakoshima, Y. Matsuzaki, and Y. Tokura, Journal of the Physical Society of Japan 91, 074005 (2022).