Cryptographic quantum metrology

Zixin Huang,[1,2] Chiara Macchiavello,[3] and Lorenzo Maccone[3]
[1]*Department of Physics & Astronomy, University of Sheffield, United Kingdom*
[2]*School of Physics, University of Sydney, New Spith Wales 2006, Australia*
[3]*Dipartimento di Fisica and INFN Sezione di Pavia, University of Pavia, via Bassi 6, I-27100 Pavia, Italy*

(Received 11 September 2018; published 13 February 2019)

We develop a general framework for parameter estimation that allows only trusted parties to access the result and achieves optimal precision. The protocols are designed such that adversaries can access some information indeterministically, but only at the risk of getting caught (cheat sensitivity); under the assumption that the adversary can access the channel only once, then the protocol is unconditionally secure. By combining techniques from quantum cryptography and quantum metrology, we devise cryptographic procedures for single-parameter estimation when an arbitrary number of parties are involved.

DOI: 10.1103/PhysRevA.99.022314

I. INTRODUCTION

Classical protocols for sharing measurement results, e.g., secret location sharing [1–4], use classical encryption schemes that rely on assumptions such as a bounded computational capacity of the adversaries. Quantum cryptography [5–7] instead promises unconditional security: the only assumptions are the laws of physics and a correct implementation.

Here we introduce a general framework for quantum cryptographic protocols specifically for rendering a parameter estimation secure, while retaining the highest precision allowed by quantum mechanics. Clearly, one could perform optimal parameter estimation and then use conventional quantum cryptography to securely transmit the result. As we show here, thanks to the quantum nature of the states employed in quantum metrology, simple modifications of conventional quantum metrology protocols allow secure transmission of the estimated parameter.

While a few such schemes have appeared in the literature [8–12], they were suited only to specific cases. The need for a central trusted party was also not considered, except in Ref. [12]. Here we give a general framework that can be applied to any quantum metrology protocol, which can be adapted into a secured one easily. For sub-shot-noise estimation security here is intended as cheat sensitivity [13,14]: adversaries can access information but only at the risk of being caught. This security model is appropriate only for situations in which the penalty of being caught is higher than the payoff of syphoning some information. The presented protocols can also achieve unconditional security under the hypothesis that Eve can interact with the probes only once.

Our goal is to securely and optimally estimate an arbitrary parameter φ, encoded onto a probe through a unitary operator $U_\varphi = e^{-i\varphi H}$, where H is a known Hermitian operator, in an ideal noiseless scenario.

In our framework, a trusted party, Charlie, holds the black box which encodes the unitary U_φ. He can switch between implementing $U_{\varphi+\pi m/N}$ and $U_{\pi m/N}$, where $m \in \{0, \dots, N-1\}$, and we will see later on why this is needed. Charlie does not need to know φ: he just has to add an additional phase in the first case and reroute the probes in the second. Charlie can classically communicate with the other trusted parties (Alice and Bob), but cannot prepare quantum states.

Charlie can be a sensor at a remote location where the trusted parties do not have easy access, e.g., a small device which collects data at a remote location, and has limited experimental capabilities. The phase to be measured can reflect an optical path length, a time delay, the strength of a magnetic or gravitational field, the temperature, etc.

As is customary, we allow the eavesdropper Eve complete control of the channel where the probes travel. The main idea is simple: in quantum metrology the measurement probes are prepared in an entangled state (e.g., the NOON state) which has the feature that separate measurements on each probe give no information on the parameter until they are jointly processed, because of the entanglement. Moreover, a test of correlations on a complementary observable of the probes can test for the presence of Eve as in conventional quantum cryptography: any action by Eve will ruin the correlation in at least one of two complementary properties. If she is detected, the protocol is terminated. For example, in the secret estimation of the distance between two parties [8–11,15], H and φ represent the energy and the time of arrival of the probes, respectively, which are the two complementary observables that must be tested to exclude the presence of Eve.

The optimality of the parameter estimation is achieved through quantum metrology [16–19], and the security of the protocol is based on the BB84 [5] protocol as its unconditional security has been firmly established. It establishes the best precision attainable in terms of the resources devoted to it: if one is allowed N uses of the transformation U_φ, one can at most achieve the Heisenberg limit scaling of $1/N^2$ in the variance (both in the finite dimensional [18] and in the infinite dimensional [20,21] cases). Among the strategies to achieve the Heisenberg limit [18,22] here we use the parallel-entangled scheme where an entangled state of N probes goes through N maps U_φ in parallel (see Fig. 1). In the latter

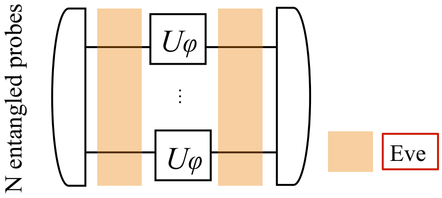

FIG. 1. A strategy that achieves the Heisenberg limit: the parallel-entangled strategy: a state of N probes goes through N maps in parallel. The channel U_φ encodes the parameter to be estimated onto the probe states. The channels are also subjected to possible manipulation by an eavesdropper, Eve, denoted by the shaded regions.

case, entanglement among the N probes is necessary, whereas separable states can only achieve the standard quantum limit scaling of $1/N$ [18]. If the number of probes does not need to be restricted, then classical estimation techniques are sufficient. Nonetheless, the use of quantum metrology in our protocols implies that it will enjoy its benefits.

The outline of the paper follows. In the next section, we summarize the key results of quantum metrology; then we detail how it can be turned into cryptographic protocols involving one, two, or an arbitrary number of parties.

II. QUANTUM METROLOGY

Quantum metrology deals with the optimal estimation of a parameter φ which is encoded into a probe by a unitary map $U_\varphi = \exp[-iH\varphi]$, where H is the Hermitian generator. The optimal initial states of the probe are the ones that have a maximum spread for the generator: for the parallel-entangled strategy an optimal state for the N probes is the NOON state

$$(|\lambda_m\rangle^{\otimes N} + |\lambda_M\rangle^{\otimes N})/\sqrt{2}, \tag{1}$$

where $|\lambda_m\rangle, |\lambda_M\rangle$ are the eigenvectors of H corresponding to the minimum and maximum eigenvalues [18,23]. After the evolution, the state is transformed into

$$e^{iN\varphi\lambda_m}|\lambda_m\rangle^{\otimes N} + e^{iN\varphi\lambda_M}|\lambda_M\rangle^{\otimes N}. \tag{2}$$

The ultimate achievable precision is given by the quantum Cramer-Rao (QCR) bound [16,24–26]. It is a lower bound to the variance φ. For unbiased estimators, $\Delta\varphi^2 \geqslant 1/\nu J(\rho_\varphi)$, where ν is the number of times the estimation is repeated, and J is the quantum Fisher information (QFI) associated with the global state ρ_φ of probes and ancillae (after the interaction $\mathcal{E}_\varphi$ with the probed system). When there is a unique most probable estimate, the bound is achievable in the asymptotic limit that $\nu \to \infty$. The QFI is

$$J(\rho_\varphi) = \sum_{j,k:\lambda_j+\lambda_k\neq 0} 2|\langle j|\rho'_\varphi|k\rangle|^2/(p_j + p_k), \tag{3}$$

where $\rho'_\varphi = \partial\rho_\varphi/\partial\varphi$, and p_j and $|j\rangle$ are the eigenvalues and eigenvectors of ρ_φ. The map $\mathcal{E}_\varphi$ encodes the phase parameter φ onto the probes: $\rho_\varphi = \mathcal{E}_\varphi[\rho]$, ρ being the initial state.

The QCR bound can be achieved by the observable $O_N^+ = (\hat{O}^+)^{\otimes N}$, with

$$O^\pm = (|\lambda_m\rangle \pm |\lambda_M\rangle)/\sqrt{2}. \tag{4}$$

The observable has an expectation value $\cos[N\varphi(\lambda_M - \lambda_m)]$, whence one can estimate the parameter φ. After repeating the estimation procedure ν times, the error in the estimation asymptotically in ν attains the inequality [18]

$$\Delta\varphi^2 \geqslant 1/\nu[N(\lambda_M - \lambda_m)]^2, \tag{5}$$

which corresponds to the Heisenberg limit. However, using purely N-probe NOON states only allows the phase to be estimated modulo $2\pi/N$ because there are N fringes in 2π. To resolve this ambiguity, smaller NOON states with $N = 1, 2, 4, \ldots$ also have to be used, adding a small overhead to the precision in Eq. (5) [27–29].

III. SINGLE-PARTY SECURE ESTIMATION

Transforming a metrology protocol into a quantum cryptographically secure one is simple in the one-party scenario, where Alice is in charge of both the preparation and measurement. The protocol is designed such that Eve cannot extract information on φ or bias the measurement results without risking being caught, even if she has complete access to the channel between Alice and the unitary U_φ. Eve can perform arbitrary joint transformations on the probes both after Alice's preparation and before Alice's measurement.

Alice chooses randomly to prepare the states $|\Psi_N^\pm\rangle$ each with probability $P_a/2$, and $\{|\lambda_0\rangle, |\lambda_1\rangle\}$ each with probability $(1 - P_a)/2$. These are defined as

$$|\Psi_N^\pm\rangle = 1/\sqrt{2}(|\lambda_m\rangle^{\otimes N} \pm |\lambda_M\rangle^{\otimes N}), \tag{6}$$

$$|\lambda_0\rangle = |\lambda_m\rangle^{\otimes N}, \tag{7}$$

$$|\lambda_1\rangle = |\lambda_M\rangle^{\otimes N}. \tag{8}$$

Alice sends the probes through one by one, and only sends the next probe after the previous one returns.[1]

Charlie keeps count of the number of probes going through the devices, and if there are too many many probes, it means that Eve is using her own, and they abort the protocol. On each state $|\Psi_N^\pm\rangle$ that Alice sends, he chooses to randomly implement $U_{\varphi+\pi m/N}$ and $U_{m\pi/N}$ with probabilities P_c and $(1 - P_c)$, respectively. These are summarized in Table I.

The respective probabilities and states retrieved by Alice are as follows:

$$P_aP_c : 1/\sqrt{2}(e^{i(N\varphi+m\pi)\lambda_m}|\lambda_m\rangle^{\otimes N} \pm e^{i(N\varphi+m\pi)\lambda_M}|\lambda_M\rangle^{\otimes N}), \tag{9}$$

$$P_a(1 - P_c) : 1/\sqrt{2}(|\lambda_m\rangle^{\otimes N} \pm |\lambda_M\rangle^{\otimes N}), \tag{10}$$

$$(1 - P_a) : |\lambda_0\rangle, |\lambda_1\rangle. \tag{11}$$

Equation (9) is a phase-sensitive state, while Eqs. (10) and (11) are decoy states. Here the term "decoy" denotes a state that is not encoded with the parameter φ, which can be used to implement security checks. To maximize security, the

[1] For large N, if Alice sends the entire state through all at once, then Eve can easily estimate the phase unitary herself, apply her guess to Alice's state, and send it back to Alice; here Eve will get away with much greater probability.

TABLE I. Fraction of Alice's state preparation and Charlie's phase implementation.

Alice's state	Probability
$\|\Psi_N^+\rangle$	$P_a/2$
$\|\Psi_N^-\rangle$	$P_a/2$
$\|\lambda_0\rangle$	$(1-P_a)/2$
$\|\lambda_1\rangle$	$(1-P_a)/2$
Charlie's U	Fraction
$U_{\varphi+\pi m/N}$	P_c
$U_{\pi m/N}$	$1-P_c$

decoy states in Eqs. (10) and (11) need to occur with equal probability, therefore

$$P_a(1-P_c)=(1-P_a),\quad \to P_a(2-P_c)=1. \tag{12}$$

If Alice had prepared $|\Psi_N^+\rangle$ ($|\Psi_N^-\rangle$), after the U_φ interactions, she measures the observable $\hat{O}_N^+$ ($\hat{O}_N^-$). Instead, when she had prepared $|\lambda_0\rangle, |\lambda_1\rangle$, she measures in the basis $\{|\lambda_0\rangle, |\lambda_1\rangle\}$. If she prepares $|\Psi_N^\pm\rangle$ and finds that the measurement does not match the preparation, she informs Charlie, which will in turn reveal whether he applied the check $U_{m\pi/N}$. If he did, measuring $\hat{O}_N^\pm$ on $|\Psi_N^\pm\rangle$ will yield the outcome ±1, since

$$U_{m\pi/N}|\Psi_N^\pm\rangle=\begin{cases}|\Psi_N^\pm\rangle, & \text{if } m \text{ is even},\\ |\Psi_N^\mp\rangle, & \text{if } m \text{ is odd}.\end{cases} \tag{13}$$

From the states in which Charlie has applied the check unitary, they can deduce whether Eve has biased the measurement. If Charlie applied U_φ, Alice keeps the result and uses it later for estimation.

Now, the protocol is designed such that, without knowing m, the channel is dephasing. This is achieved with Charlie implementing $U_{\varphi+m\pi/N}$ with random $m\in[0,\dots,N-1]$. For both of the check cases, if the measurement outcome does not match the state preparation and/or evolution, Alice knows Eve has been tampering and the protocol is terminated, or they can estimate Eve's bias.

As the last step in the protocol, if the check shows that the process has been noiseless, only then does Charlie reveal the value of m on each probe state, and Alice then computes the observable

$$\langle\hat{O}_N^+\rangle+\langle\hat{O}_N^-\rangle=\cos[(N\varphi+m\pi)(\lambda_M-\lambda_m)], \tag{14}$$

from which she obtains φ. All public communication is useless to a third party.

Asymptotically, the achievable rms error is

$$\Delta\varphi^2\geqslant 1/P_aP_c\nu[N(\lambda_M-\lambda_m)]^2. \tag{15}$$

With probability $P=1-P_aP_c$, Alice would have a decoy state at hand, and if Eve tampers with the estimation, she will be discovered with probability $(1-\frac{P}{4})^\kappa$, where κ is the number of states she tampers with.

Eve does not get caught if Alice prepares a probe state. Eve always makes a guess on the decoy state basis that Alice chose and performs a von Neumann measurement in that basis. When a decoy state is prepared, Eve will make an incorrect guess 1/2 of the time. When she is correct, the state she sends back to Alice will correlate with Alice's preparation and she is undetected. When Eve is incorrect, she sends a state in the wrong basis; but half the time when measured, it will collapse to the "right" state. Therefore in a one-party scenario, the probability of Eve's cheat being undetected is

$$\left(1-\frac{(1-P_aP_c)}{4}\right)^\kappa. \tag{16}$$

Eve cannot gain information on φ deterministically; to estimate φ, Eve needs to have hijacked Alice's probes while the phase unitary was applied, and not have been caught previously. If she is discovered, Charlie keeps the value of m to himself, and Eve estimates $\varphi+\pi m/N$ with an unknown m, which is useless. The maximum QFI Eve gains is κN^2, where κ is the number of probe states she tampers with, and this occurs with exponentially small probability $(P_c)^\kappa$. Note that if Eve cannot access the channel twice (and can only attempt to recover φ by measuring Alice's probes), then the protocol is unconditionally secure, since from her point of view the state propagating in the channel is a mixed state,

$$[(|\lambda_m\rangle\langle\lambda_m|)^{\otimes N}+(|\lambda_M\rangle\langle\lambda_M|)^{\otimes N}]/2, \tag{17}$$

which is useless for parameter estimation since it does not acquire any phase during the interaction U_φ.

TABLE II. Fraction of Bob's measurement.

Bob's measurement	Probability
$\hat{O}_N^+$	$(1-P_a)/(1-P_aP_c)$
$\|\lambda_0\rangle, \|\lambda_1\rangle$	$1-(1-P_a)/(1-P_aP_c)$

IV. TWO-PARTY SECURE ESTIMATION

In two-party protocols Alice is in charge of the state preparation and Bob is responsible for the measurements (e.g., a distance measurement using light pulses and synchronized clocks). They both wish to recover the parameter in a way that is at least cheat sensitive. The procedure is inspired by the BB84 protocol.

The state preparation is the same as for the single-party protocol: Alice chooses randomly to prepare $|\Psi_N^\pm\rangle$ each with probability $P_a/2$, and $|\lambda_{0/1}\rangle$ each with probability $(1-P_a)/2$.

Bob independently chooses to measure either $\hat{O}_N^+$ or projects onto $\{|\lambda_0\rangle, |\lambda_1\rangle\}$, with probabilities given in Table II. After Bob's measurement, they use a public channel to check their choice of measurement basis and discard all the cases when they do not agree (see Fig. 2). The exchange of classical information can be done at the end of the protocol as follows:

(1) Alice reveals the basis of state preparation, Alice and Bob check for correlations on $|\lambda_{0/1}\rangle$. If the correlations are perfect, they proceed.

(2) Charlie reveals to which states he has applied the check unitary $U_{m\pi/N}$.

(3) On the states Charlie has applied $U_{m\pi/N}$, Alice reveals whether $|\Psi_N^+\rangle$ or $|\Psi_N^-\rangle$ was prepared, and they check for correlations using Eq. (13). If they decided that no one

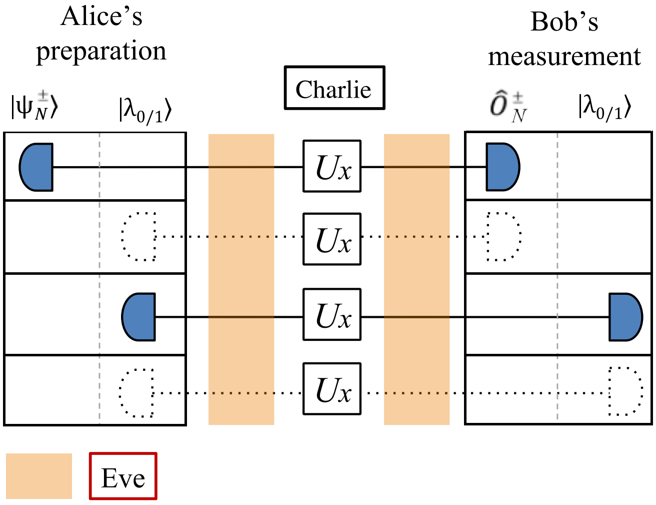

FIG. 2. Alice sends either $|\Psi_N^\pm\rangle$ or $|\lambda_{0/1}\rangle$ into the quantum channel which encodes the parameter φ onto the probes. Charlie implements the unitary $U_x, x \in \{\varphi + \frac{\pi m}{N}, m\pi/N\}$. Bob randomly chooses to measure the observable $\hat{O}_N^\pm$ or projects onto one of the basis of the decoy states. They retain only the copies for which their choice of basis agree, denoted by the solid blue markers. The probes are also subjected to possible manipulation by an eavesdropper, Eve, denoted by regions shaded orange.

has tampered with the communication, Charlie discloses the values of m on the states to which he applied $U_{\varphi+\frac{\pi m}{N}}$.

(4) Alice reveals her preparation on half the probe states, and Bob reveals his measurement outcomes on the other half.

They now can compute $\hat{O}_N^\pm$ correspondingly, where the sum of the expectation values is once again $\cos[(N\varphi + m\pi)(\lambda_M - \lambda_m)]$, whence they can both obtain φ. Four states are necessary for the two-party protocol, because alternating between the plus or minus probe state ensures that their communication is meaningless to a third party.

We now calculate the probability of Eve being undetected. If Eve wants to minimize her probability of getting caught while still obtaining some information, her best strategy is to try to discriminate which decoy state Alice has prepared, and send this to Bob. For the decoy states we have considered, the maximum discrimination probability is $2/S$, where S is the number of symmetric states in the set [30].

If Bob chooses the measurement basis $\hat{O}_N^+$ ($|\lambda_{0/1}\rangle$) with probability η $(1-\eta)$, for the decoy states to occur with equal probability, he chooses

$$P_a(1-P_c)\eta = (1-P_a)(1-\eta) \tag{18}$$

$$\rightarrow \eta = \frac{1-P_a}{1-P_aP_c}. \tag{19}$$

Now, the probability that Bob has received a decoy state and measured in the correct basis is given by

$$P_a(1-P_c)\eta + (1-P_a)(1-\eta) = \frac{2(1-P_a)P_a(1-P_c)}{(1-P_aP_c)}. \tag{20}$$

The probability of Eve successfully evading detection would be $1/4$, when this occurs, therefore if Eve tampers with κ probes, the probability is given by

$$\left(1 - \frac{2(1-P_a)P_a(1-P_c)}{4(1-P_aP_c)}\right)^\kappa. \tag{21}$$

This can be improved if Alice and Bob share a secret bit string in advance such that Bob knows which basis to choose, in which case Eve's probability of being undetected is $(1-\frac{1-P_aP_c}{4})^\kappa$. Once again, if Eve only has access to one end of the channel, her information gain is zero even if she intercepts all the quantum and classical communication between Alice and Bob.

The achievable precision on φ for each party is

$$\Delta\varphi^2 \geqslant 2/\left[\nu\left(\frac{1-P_a}{1-P_aP_c}\right)P_aP_c[N(\lambda_M-\lambda_m)]^2\right]. \tag{22}$$

The factor of 2 comes from the fact that P_a fraction of the time Alice sends out a phase-sensitive state, $\frac{1-P_a}{1-P_aP_c}$ fraction of the time Bob measures in the correct basis, P_c fraction of the time Charlie applies the phase unitary, and each party estimates the parameter from only half the remaining copies of the probe states. This reduction is only a constant factor. For small N the efficiency of the scheme can be improved by using techniques such as those described in Ref. [31].

The difference between the two-party protocol described above, and one where Alice simply performs the estimation and encrypts and sends it via the quantum key is that this protocol can be tailored to the scenario where Alice (or Bob) does not learn the parameter. In the former protocol or in any classical protocol, this is impossible.

V. MULTIPLE-PARTY ESTIMATION

We now examine the multiple-party scenario. Alice and Charlie wish to measure and transmit the parameter to some trusted parties, but she wants them to uncover the parameter only when they meet and collaborate, analogously to quantum-secret-sharing schemes [32–37]. Here Alice is in charge of state preparation and we assume that φ is encoded by Charlie in the channel that separates her from Bob. If the secret is to be shared among k trusted parties excluding Alice, she prepares $|\Phi_N^\pm\rangle$ with probability P_a and $|\Lambda_0\rangle, |\Lambda_1\rangle$ each with probability $(1-P_a)/2$, where

$$|\Phi_N^\pm\rangle = \frac{1}{\sqrt{2}}(|\lambda_m\rangle^{\otimes N+k-1} \pm |\lambda_M\rangle^{\otimes N+k-1}) \tag{23}$$

and

$$|\Lambda_0\rangle = |\lambda_m\rangle^{\otimes N+k-1}, \quad |\Lambda_1\rangle = |\lambda_M\rangle^{\otimes N+k-1}. \tag{24}$$

When she prepares $|\Phi_N^\pm\rangle$, she sends N probes from the state into the quantum channel to Bob, and one each to the other $k-1$ parties. The state $|\Phi_N^\pm\rangle$ evolves to

$$\begin{aligned}|\Phi_N^\pm\rangle \rightarrow \frac{1}{\sqrt{2}}[&e^{i(N\varphi+m\pi)\lambda_m}|\lambda_m\rangle^{\otimes N+k-1}\\ &\pm e^{i(N\varphi+m\pi)\lambda_M}|\lambda_M\rangle^{\otimes N+k-1}].\end{aligned} \tag{25}$$

Now, if every party independently chooses randomly an observable to measure, the scheme would be exponentially inefficient. To overcome this, they need to first agree on a sequence of measurement basis in a secure way: Alice can perform a BB84 quantum key distribution separately with each participant. Then she will share a unique secret bit string with each of them. She then compares these bit strings, uses one as a reference, and instructs the rest to match theirs to it by performing a series of bit flip operations. This is a secure step as she is just instructing which bit to flip, never communicating the bit's initial or final value. Alternatively, multipartite conference key distribution protocol can be employed in order to establish a shared secret key [38].

The parties then agree to project onto the $|\pm\rangle$ bases at the jth iteration of the protocol if the jth two-bit value is 0, given Alice will send $|\Phi_N\rangle$. If the bit value is 1, then they project onto the computational basis, as Alice will send $|\Lambda_{0/1}\rangle$. Measuring $\hat{O}^{\pm}_{N+k-1}$ on $|\Phi^{\pm}_N\rangle$ will deterministically yield the outcome ±1.

As Alice sends through the states, they check the outcomes on the decoys: if the measurements of all k parties do not match Alice's preparation, they know an eavesdropper is present and they abort the protocol.

The rest of the protocol then follows trivially from the two-party version. At the end of the protocol (this stage can be delayed arbitrarily), Alice announces her state preparation on half the copies, and the rest of the parties reveal their respective measurement outcomes on the other half. Alice now possesses information on all the probes, and can deduce the parameter by computing the observable $\hat{O}_{N+k-1} = (|+\rangle\langle+| - |-\rangle\langle-|)^{\otimes N+k-1}$, which has expectation value $\cos[(N\varphi + m\pi)(\lambda_M - \lambda_m)]$. The precision of her estimate is $2/\nu P_a P_c[N(\lambda_M - \lambda_N)]^2$. As for the other parties, they now need to correlate their measurement outcomes in order to uncover φ. They do so by also calculating $\langle\hat{O}_{N/2+k-1}\rangle$. Without information from any of the participants, the rest of the results are useless, since this would be equivalent to tracing out one probe from a maximally entangled state, which renders the measurement outcomes of the rest completely random. The additional resources used are of $2k\nu$ qubits used for quantum key distribution and the $\nu(k-1)$ extra probes that do not interact with U_φ.

VI. CONCLUSION

By combining techniques from quantum metrology and quantum cryptography, we have defined a general framework for quantum cryptographic protocols specifically suited to the task of securing parameter estimation while retaining the highest available precision. Adversaries can gain some information on the parameter, but at the risk of being detected. We devised protocols for single-parameter estimation involving an arbitrary number of parties.

ACKNOWLEDGMENT

We acknowledge funding from University of Pavia "Blue sky" Project, Grant No. BSR1718573. Z.H. is funded by EPSRC Quantum Communications Hub, Grant No. EP/M013472/1.

[1] W. C. Cheng and M. Aritsugi, Procedia Comp. Sci. **35**, 1692 (2014).

[2] M. Herrmann, A. Rial, C. Diaz, and B. Preneel, in *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks* (ACM Press, New York, 2014), pp. 87–98.

[3] C. Dong and N. Dulay, in *Proceedings of the IFIP International Conference on Trust Management* (Springer, Berlin, 2011), pp. 133–148.

[4] K. P. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. El Abbadi, C. Kruegel, and B. Y. Zhao, IEEE Trans. Mobile Comput. **13**, 159 (2014).

[5] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[7] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[8] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. A **65**, 022309 (2002).

[9] V. Giovannetti, S. Lloyd, and L. Maccone, Nature **412**, 417 (2001).

[10] V. Giovannetti, S. Lloyd, and L. Maccone, J. Opt. B **4**, S413 (2002).

[11] G. Chiribella, L. Maccone, and P. Perinotti, Phys. Rev. Lett. **98**, 120501 (2007).

[12] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, Nat. Phys. **10**, 582 (2014).

[13] L. Hardy and A. Kent, Phys. Rev. Lett. **92**, 157901 (2004).

[14] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **100**, 230502 (2008).

[15] G. Chiribella, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **72**, 042338 (2005).

[16] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).

[17] V. Giovannetti, S. Lloyd, and L. Maccone, Science **306**, 1330 (2004).

[18] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **96**, 010401 (2006).

[19] W. van Dam, G. M. D'Ariano, A. Ekert, C. Macchiavello, and M. Mosca, Phys. Rev. Lett. **98**, 090501 (2007).

[20] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **108**, 260405 (2012).

[21] V. Giovannetti and L. Maccone, Phys. Rev. Lett. **108**, 210404 (2012).

[22] R. Demkowicz-Dobrzański and L. Maccone, Phys. Rev. Lett. **113**, 250801 (2014).

[23] J. P. Dowling, Contemp. Phys. **49**, 125 (2008).

[24] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (Springer Science & Business Media, New York, 2011).

[25] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[26] I. Afnan, R. Banerjee, S. L. Braunstein, I. Brevik, C. M. Caves, B. Chakraborty, E. Fischbach, L. Lindblom, G. Milburn, S. Odintsov *et al.*, Ann. Phys. (NY) **247**, 447 (1996).

[27] D. W. Berry, B. L. Higgins, S. D. Bartlett, M. W. Mitchell, G. J. Pryde, and H. M. Wiseman, Phys. Rev. A **80**, 052114 (2009).

[28] B. L. Higgins, D. Berry, S. Bartlett, M. Mitchell, H. M. Wiseman, and G. Pryde, New J. Phys. **11**, 073023 (2009).

[29] B. L. Higgins, D. W. Berry, S. D. Bartlett, H. M. Wiseman, and G. J. Pryde, Nature **450**, 393 (2007).

[30] S. L. Zhang, X. B. Zou, K. Li, C. H. Jin, and G. C. Guo, Phys. Rev. A **77**, 044302 (2008).

[31] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).

[32] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[33] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[34] Z.-j. Zhang, Y. Li, and Z.-x. Man, Phys. Rev. A **71**, 044301 (2005).

[35] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[36] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).

[37] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[38] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, New J. Phys. **19**, 093012 (2017).