Classical analog of the quantum marginal problem

Olga Leskovjanová and Ladislav Mišta, Jr.
Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic

(Received 30 December 2019; accepted 25 February 2020; published 23 March 2020)

We construct a classical cryptographic analog of multipartite entanglement which can be verified solely from separable marginals. That is a set of marginal classical probability distributions carrying no secret correlations, which are compatible only with a joint distribution containing secret correlations. This demonstrates that the emergent correlation properties do not exist only in the quantum world. Viewed from a different perspective, our result reveals another possible application of the quantum marginal problems in that they can help us to design and solve interesting classical marginal problems.

DOI: 10.1103/PhysRevA.101.032341

I. INTRODUCTION

The question of the relationship between the whole and its parts arises in many branches of natural science. One class of such problems appears in mathematical statistics under the name of marginal problem. In its basic formulation one wants to identify a set of all joint probability distributions compatible with a given set of reduced probability distributions (marginals). The origin of the problem dates back the 1940s [1] and since then many variants of the problem have been analyzed for discrete as well as continuous random variables both in bipartite and multipartite scenarios [2].

The classical marginal problem has a quantum counterpart called the quantum marginal problem. Here, instead of a set of marginal distributions one is given a set of reduced density matrices and the goal is to find the set of global density matrices compatible with them. The problem originally addressed a question about the representability of a set of two-electron density matrices by an N-electron wave function [3], but with the advent of quantum information theory several other kinds of the problem have been analyzed and solved [4]. This includes the quantum marginal problem for finite-dimensional quantum systems [5] as well as various forms of the problem for bosonic Gaussian states [6,7].

The quantum marginal problem appears in numerous tasks of quantum information theory ranging from classification [8] and quantification [9] of quantum entanglement to extendibility of quantum states [10,11]. Another use of the problem concerns detection of a global property of a composite quantum system from its parts. In this case, we aim at answering the question of what can be said about the global properties of the system using only the partial information contained in a given set of reduced density matrices. This task is particularly interesting when the reductions do not carry any signatures of the sought property, because then it can be viewed as a means of detection of an "emergent property," i.e., a property appearing only at a certain level of the complexity of the investigated system, from simpler constituents which do not carry the property. The utility of the quantum marginal problem in this context is twofold. In the first instance [12] we apply the solution of an already solved quantum marginal problem to a given set of reduced density matrices to identify all global density matrices compatible with the reductions. In the next step, we check whether all the density matrices carry the global property of our interest, which would be a successful confirmation of the property from reductions. The other application is more involved. Namely, finding examples of systems whose global property can be inferred from its parts lacking the property is a nontrivial marginal problem itself and so far it has been solved only for several special cases. A common feature of all currently known examples is that the investigated global properties are exclusively nonclassical correlation properties in quantum systems, which encompass quantum entanglement [13–16] and quantum nonlocality [17]. But is there also an example of the considered marginal problem for ordinary classical probability distributions?

Intuitively, we would expect that this is indeed the case because it is possible to practically systematically construct classical analogs of quantum phenomena. The basis of the construction is the fact [18,19] that an entangled quantum state, i.e., a quantum state which cannot be prepared by local operations and classical communication, can be mapped by a measurement onto a classical probability distribution with secret correlations, i.e., correlations which cannot be prepared by local operations and public communication (LOPC). If the original quantum state carries some special form of entanglement, e.g., bound entanglement, and the measurement is chosen suitably, the obtained classical probability distribution can carry a special form of secret correlations analogous to bound entanglement. Starting with construction of potential examples of such so-called bipartite bound information [20], this method has been used to construct several other classical analogs of quantum concepts. This includes an example of multipartite bound information for binary [21] and Gaussian [22] random variables, a classical analog of negative information [23], a protocol for secrecy distribution by nonsecret correlations [24], superactivation of bound information [25], percolation of secret correlations [26], and reversibility of secret correlations [27]. A natural question that arises in this context is whether also a quantum marginal problem can be mapped onto its classical cryptographic analog.

In this paper we answer this question in the affirmative. Specifically, we use the mapping of quantum states onto classical probability distributions [18] and map an already solved quantum marginal problem [15] onto its classical counterpart. At the same time, all separability properties of the mother quantum problem are transferred onto secrecy properties of the daughter classical problem. Recall that the global property to be inferred in the quantum marginal problem [15] is genuine multipartite entanglement—the strongest form of multipartite entanglement—which cannot be prepared by mixing of states which are separable across different bipartitions. The problem then asks for the existence of a triple of unentangled (separable) two-qubit density matrices which are compatible only with genuine multipartite entangled global states. The particular solution of the problem given in Ref. [15] then consists of three two-qubit density matrices which are compatible with a single three-qubit genuine multipartite entangled state. The classical analog of the quantum problem constructed by us then consists of a triple of marginals, none of which contains secret correlations, which are nevertheless compatible with a single global probability distribution carrying secret correlations. This demonstrates that the possibility to infer a global property of a composite system from its parts which do not possess the property exists also in the realm of classical probability distributions. In a broader sense it manifests the possibility to map a quantum marginal problem with separability constraints on the involved density matrices onto a classical marginal problem with constraints on the secrecy content of the involved probability distributions.

The paper is organized as follows. In Sec. II we briefly explain the concept of secret correlations and its connection with quantum entanglement. Section III contains the construction of the studied classical marginal problem. Finally, Sec. IV contains the discussion and conclusions.

II. MAPPING ENTANGLEMENT ONTO SECRET CORRELATIONS

Construction of classical cryptographic analogs of quantum phenomena is based on mapping of quantum states on probability distributions by a quantum measurement [18]. More precisely, consider a density matrix ρ_{AB} of two two-level quantum systems (qubits) and take its purification $|\psi\rangle_{ABE}$, $\rho_{AB} = \mathrm{Tr}_E(|\psi\rangle\langle\psi|_{ABE})$, where E labels the purifying system. By carrying out local projective measurements P_i, $i = A, B, E$, on all subsystems of the purification one establishes the following probability distribution of measurement outcomes [18]:

$$P(A, B, E) = \mathrm{Tr}(P_A \otimes P_B \otimes P_E|\psi\rangle\langle\psi|_{ABE}). \qquad (1)$$

Provided that the original state ρ_{AB} carries a quantum property of our interest and we choose a suitable measurement, the obtained probability distribution may inherit a classical cryptographic analog of this property.

Typically, the quantum property is a certain form of quantum entanglement and the respective classical analog is the corresponding kind of secret correlations. For instance, making use of the previous mapping one finds that a classical analog of the maximally entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$ is the so-called secret bit [18], which is a basic unit of secret correlations given by the probability distribution satisfying $P(A, B, E) = P(A, B)P(E)$ and $P(A = B = 0) = P(A = B = 1) = 1/2$. The concept of secret correlations has been developed in the context of classical secret-key agreement protocol [28]. Here, two honest parties, Alice and Bob, and an adversary Eve, share independent realizations of three random variables A, B, and E, characterized by the probability distribution $P(A, B, E)$. The goal of Alice and Bob is to extract from their variables by LOPC a secret key, i.e., a common string of random bits about which Eve has practically no information. For this to be possible it is necessary for the distribution $P(A, B, E)$ to contain secret correlations, which is defined as a distribution that cannot be created by LOPC. A key tool for detection of secret correlations is the intrinsic information defined as [29]

$$I(A; B \downarrow E) = \inf_{E\to\tilde{E}}[I(A; B|\tilde{E})]. \qquad (2)$$

Here,

$$I(A; B|E) = H(A, E) + H(B, E) - H(A, B, E) - H(E) \qquad (3)$$

where $H(X)$ is the Shannon entropy, is the conditional mutual information and the minimization is performed over all channels $E \to \tilde{E}$. Namely, it holds that a probability distribution contains secret correlations if, and only if, $I(A; B \downarrow E) > 0$ [24,30]. Hence, to certify that the distribution $P(A, B, E)$ does not contain secret correlations it is thus sufficient to show that $I(A; B \downarrow E) = 0$. This can be done as follows [21,24,25]. We find a suitable channel $E \to \tilde{E}$ which nullifies the conditional mutual information. As a result, the intrinsic information (2) vanishes and there are no secret correlations in the investigated distribution.

Let us move to detection of the presence of secret correlations. A straightforward way would be to show strict positivity of the intrinsic information (2), but it is a hardly tractable task owing to the optimization in its definition. Instead, we use the fact that the intrinsic information is an upper bound on the secret key rate $S(A; B||E)$ [29] which is in turn lower bounded as [31]

$$S(A; B||E) \geqslant \max[I(A; B) - I(A; E), I(A; B) - I(B; E)] \quad (4)$$

with $I(X; Y) = H(X) + H(Y) - H(X, Y)$ being the mutual information. Consequently, strict positivity of the right-hand side (r.h.s.) of the latter inequality implies a strict positivity of the intrinsic information and therefore the presence of secret correlations in the analyzed distribution.

Most of the known cryptographic analogs of quantum phenomena are multipartite. The same holds true also for the concept studied here, which is tripartite, and thus one has to generalize the previous approach to three honest parties. Here, one starts with a three-qubit density matrix ρ_{ABC} carrying the required quantum property. Next, we construct a purification $|\psi\rangle_{ABCE}$ of the state, $\rho_{ABC} = \mathrm{Tr}_E(|\psi\rangle\langle\psi|_{ABCE})$, and perform suitable projective measurements P_i, $i = A, B, C, E$, on the purification. The obtained measurement outcomes are then distributed according to the four-variate probability distribution of the form

$$P(A, B, C, E) = \mathrm{Tr}(P_A \otimes P_B \otimes P_C \otimes P_E|\psi\rangle\langle\psi|_{ABCE}). \quad (5)$$

In what follows, we will need to show the absence of secret correlations in marginals obtained by dropping one of the variables A, B, and C. As the resulting distributions will be always trivariate, the previously described approach based on vanishing of the intrinsic information (2) perfectly suffices for our purposes. On the other hand, for verification of the presence of secret correlations in the global distribution, we need a multipartite generalization of the lower bound (4). As far as the secret correlations across the $A|BC$ bipartition are concerned, one can use the following lower bound:

$$S(A;BC||E) \geqslant \max[I(A;BC) - I(A;E), I(A;BC) - I(BC;E)]. \quad (6)$$

Similarly to the bipartite case, if the r.h.s. is strictly positive, A shares secret correlations with BC.

III. GLOBAL SECRECY VERIFIABLE FROM LOCAL NONSECRET CORRELATIONS

The distribution we are looking for can be derived from a tripartite state found in Ref. [15],

$$\rho = \tfrac{2}{3}|\xi\rangle\langle\xi| + \tfrac{1}{3}|111\rangle\langle 111|, \quad (7)$$

where

$$|\xi\rangle = \frac{1}{2}|010\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{2}}|001\rangle. \quad (8)$$

As we have already mentioned, the state is genuine multipartite entangled, while at the same time all its three two-qubit reduced density matrices are separable. Interestingly, the reductions determine the global state uniquely, which implies that one can really infer genuine multipartite entanglement of the global state from its separable parts.

Following a generic method of construction of classical analogs of quantum phenomena [18], we now derive a purification of the state (7), which reads as

$$|\psi\rangle_{ABCE} = \sqrt{\frac{2}{3}}|\xi\rangle|0\rangle + \sqrt{\frac{1}{3}}|111\rangle|1\rangle. \quad (9)$$

The candidate for the sought probability distribution $P(A, B, C, E)$ is then obtained by measuring the purification (9) in the computational basis. Making use of formulas (9) and (5), we arrive at the probability distribution with nonzero probabilities summarized in Table I.

For the needs of our further explanation we also compute marginals $P(A, B, E)$, $P(A, C, E)$, and $P(B, C, E)$. Since the distributions $P(A, C, E)$ and $P(B, C, E)$ coincide, here we write down explicitly only the distribution $P(A, C, E)$.

TABLE I. Probability distribution of outcomes of the measurement of the purification (9) in the computational basis.

A	B	C	E	$P(A, B, C, E)$
0	0	1	0	1/3
0	1	0	0	1/6
1	0	0	0	1/6
1	1	1	1	1/3

TABLE II. Marginal $P(A, B, E)$.

A	B	E	$P(A, B, E)$
0	0	0	1/3
0	1	0	1/6
1	0	0	1/6
1	1	1	1/3

Both the distributions mentioned above are given in Tables II and III.

Now, our goal is to show that the constructed distributions carry a classical analog of multipartite entanglement verifiable from separable reductions. That is, we need to show that the marginals $P(A, B, E)$, $P(A, C, E)$, and $P(B, C, E)$ do not carry secret correlations, yet one can infer from them the presence of secret correlations in all global distributions which are compatible with them. The proof consists of three steps. First, we determine all global distributions compatible with the given reduced distributions. Next, we show that all the global distributions carry secret correlations. Finally, we prove that all the marginals indeed do not carry secret correlations, which completes construction of the sought classical concept.

Let us start with finding of all the global distributions which can have the distributions $P(A, B, E)$, $P(A, C, E)$, and $P(B, C, E)$ as marginals. This amounts to solving a set of twenty-four equations corresponding to twenty-four elements of the three marginals for sixteen unknown probabilities of the global distribution. Additionally, the unknowns are subject to the constraint that they are probabilities. Since many of the equations give unique solutions and some equations in the remaining set of equations are not independent, one ends up with a set of five independent equations for five variables (see the Appendix for details of the calculations). By solving the latter set of equations one finds finally that there is just *one* global probability distribution given in Table I compatible with the marginals given in Tables II and III. Thus interestingly, the property that the reduced density matrices ρ_{AB}, ρ_{BC}, and ρ_{AC} uniquely determine the global state was transferred to their classical counterparts.

In the next step we show that the global probability distribution found in the first step carries secret correlations across all three bipartitions $A|BC$, $B|AC$, and $C|AB$. As the distribution is symmetric under the exchange of bits A and B, it is sufficient to prove the presence of secret correlations with respect to only two bipartite splittings, say $A|BC$ and $C|AB$. Making use of formula (6) and Table I, one finds for the splitting $A|BC$ a strictly positive lower bound on the secret key rate of approximately 0.541, whereas for the other

TABLE III. Marginal $P(A, C, E)$. The table of the marginal $P(B, C, E)$ is obtained from previous table by replacing A with B in the first row of the table.

A	C	E	$P(A, C, E)$
0	0	0	1/6
0	1	0	1/3
1	0	0	1/6
1	1	1	1/3

TABLE IV. New marginal $P(A, B, \tilde{E})$.

A	B	$\tilde{E}$	$P(A, B, \tilde{E})$
0	0	0	1/3
0	1	0	1/6
1	0	0	1/6
1	1	0	1/12
1	1	1	1/4

splitting $C|AB$ it is equal to 2/3. This signifies that the global distribution in Table I indeed contains secret correlations across all three bipartitions, as we set out to prove.

Lastly, we need to prove that, contrary to the global distribution, the marginals do not contain any secret correlations. According to results of Ref. [29] a probability distribution does not carry secret correlation if its intrinsic information (2) vanishes. Therefore, if, e.g., for the marginal $P(A, B, E)$ given in Table II we find a suitable channel $E \rightarrow \tilde{E}$ such that for the new probability distribution $P(A, B, \tilde{E})$ the conditional mutual information $I(A; B|\tilde{E})$ vanishes, the distribution does not contain secret correlations.

First, assume that the marginal $P(A, B, E)$ is subject to a channel $E \rightarrow \tilde{E}$ characterized by the conditional probability distribution $P_{\tilde{E}|E}(0, 0) = 1$, $P_{\tilde{E}|E}(1, 0) = 0$, $P_{\tilde{E}|E}(0, 1) = 1/4$, and $P_{\tilde{E}|E}(1, 1) = 3/4$. The obtained marginal $P(A, B, \tilde{E})$ is displayed in Table IV.

Now, if we calculate for the new distribution the conditional mutual information using formula (3) we find that $I(A; B|\tilde{E}) = 0$. This implies that the intrinsic information $I(A; B \downarrow E)$ of the original distribution $P(A, B, E)$ vanishes and therefore the distribution does not contain secret correlations, as required.

Moving to the second marginal $P(A, C, E)$, consider the variable E to be transformed by the channel $E \rightarrow \tilde{E}$ described by the conditional probability distribution $P_{\tilde{E}|E}(0, 0) = P_{\tilde{E}|E}(0, 1) = 0$ and $P_{\tilde{E}|E}(1, 0) = P_{\tilde{E}|E}(1, 1) = 1$. This gives rise to a new marginal $P(A, C, \tilde{E})$, given explicitly in the Table V.

Making use once again of the formula (3), we get that $I(A; C|\tilde{E}) = 0$ and therefore there are no secret correlations also in the marginal $P(A, C, E)$. Finally, from equality of the marginals $P(A, C, E)$ and $P(B, C, E)$ it follows immediately that neither of the latter distributions carries secret correlations, which completes our construction of the sought concept.

IV. DISCUSSION AND CONCLUSIONS

We have shown that one can map a quantum marginal problem with separability constraints on the involved density matrices onto a classical marginal problem with constraints on the secrecy content of the appearing probability distributions. In this way, we obtained a triple of trivariate marginal probability distributions carrying no secret correlations, which are compatible only with one four-variate probability distribution possessing secret correlations. This demonstrates that the possibility to detect a global correlation property from marginals which lack the property is not only an exclusive attribute of quantum mechanics, but it can be found also in the classical world. Let us note further that the global probability distribution obtained by us carries secret correlations across any of three splittings of honest parties into two groups and therefore it can be viewed as a classical analog of a fully inseparable state. However, the original state of Ref. [15], which was used to construct the distribution, carries a stronger form of multipartite entanglement known as genuine multipartite entanglement which cannot be prepared even by mixing of states which are separable across different bipartite splittings. The question that arises in this context is whether there is also a classical analog of the genuine multipartite entanglement given by a probability distribution which cannot be expressed as a convex mixture of distributions which do not contain secret correlations across different bipartitions. If this is the case, it would be also interesting to know whether there exists a case when the genuine multipartite secret correlations can be certified solely from marginals which do not have any secret correlations.

Another interesting question concerns the existence of other distributions with the property presented here. We believe that such distributions indeed exist. This is because there is another state whose genuine multipartite entanglement can be detected solely from separable marginals [16]. The state is more complex than the state used by us, but anyway one can map it onto a probability distribution and analyze its secrecy properties. However, in contrast with the present case, the marginals of the distribution are compatible with a one-parametric family of global distributions. Unfortunately, in a certain region of the parameter the global distribution possesses a negative lower bound (6). This indicates that the proof of the presence of secret correlations in the global distribution is much more involved compared to the present case, and therefore it is deferred for further research.

Let us remark further on the distinction between the quantum marginal problem [15] and the classical problem constructed here. While in the quantum problem one works with *all* two-qubit reduced density matrices, in the present classical problem we looked for a global probability distribution compatible with *fewer* marginals encompassing three out of four possible marginals. Needless to say, this is inevitable if we consider a marginal problem with a constraint on the secrecy content of the marginals. Namely, the remaining fourth marginal $P(A, B, C)$ does not contain the variable E of an adversary. The concept of secret correlations thus cannot be introduced for this marginal and therefore it has to be omitted from the set of specified marginals. In this respect, the classical marginal problem solved here resembles more the quantum problem [32] investigating states whose genuine multipartite entanglement can be verified from strictly less than all reduced density matrices.

TABLE V. New marginal $P(A, C, \tilde{E})$. The marginal $P(B, C, \tilde{E})$ is obtained by replacing A with B in the first row of the table.

A	C	$\tilde{E}$	$P(A, C, \tilde{E})$
0	0	1	1/6
0	1	1	1/3
1	0	1	1/6
1	1	1	1/3

Note, finally, that here we proved the presence of secret correlations in a global distribution from marginals by finding all the distributions compatible with the given marginals, which was in our case just one, and showing that it carries secret correlations. Since in quantum scenario one does not have to certify multipartite entanglement from separable marginals by solving the marginal problem but one can just find a suitable witness operator instead [16], which raises the question of what a classical analog of this operator would be and, if something like this exists, whether one can use it in the present classical task.

In conclusion, we have shown that the link between quantum entanglement and secret classical correlations also allows one to design and solve novel types of classical marginal problems. We hope that our finding will further boost exploration of links between quantum and classical marginal problems as well as transferability of other quantum concepts into the classical world.

ACKNOWLEDGMENT

O.L. acknowledges support from IGA-PrF-2019-010.

APPENDIX: UNIQUENESS OF THE GLOBAL DISTRIBUTION

In this Appendix we show that marginals $P(A, B, E)$, $P(A, C, E)$ and $P(B, C, E)$, in Tables II and III are compatible only with probability distribution $P(A, B, C, E)$ in Table I. We use the marginal probabilities as known variables and the global probabilities as unknown variables. The marginal $P(A, B, E)$ can be received from the global probability distribution by the equation

$$P_{ABE}(i, j, k) = P_{ABCE}(i, j, 0, k) + P_{ABCE}(i, j, 1, k), \quad \text{(A1)}$$

where $i, j, k = 0, 1$. Other marginals can be obtained analogously. Altogether this gives twenty-four equations for sixteen variables. Moreover, every variable we are looking for is constrained by an inequality $0 \leqslant P_{ABCE}(i, j, k, l) \leqslant 1$. It seems that this system is overdetermined. However, many marginal probabilities are equal to zero, so with inequalities it gives us eleven variables equal to zero. More precisely, one gets $P(0, 0, 0, 1) = P(0, 0, 1, 1) = P(0, 1, 0, 1) = P(0, 1, 1, 0) = P(0, 1, 1, 1) = P(1, 0, 0, 1) = P(1, 0, 1, 0) = P(1, 0, 1, 1) = P(1, 1, 0, 0) = P(1, 1, 0, 1) = P(1, 1, 1, 0) = 0$. This reduces the number of equations to be solved to eight, for five unknown variables. Further, there are two pairs of identical equations and one equation is a linear combination of the others. Thus we are left with the set of five equations for five variables which give directly the values of the remaining five variables: $P(0, 0, 0, 0) = 0$, $P(0, 0, 1, 0) = P(1, 1, 1, 1) = 1/3$, $P(0, 1, 0, 0) = P(1, 0, 0, 0) = 1/6$. Therefore, the global distribution is unequivocally given.

[1] W. Hoeffding, Masstabinvariante Korrelationstheorie, Schriften des Mathematischen Instituts und des Instituts für Angewandte Mathematik der Universität Berlin **5**, 179 (1940).

[2] D. A. Conway, Multivariate distributions with specified marginals, Technical Report No. 145, Dept. of Statistics, Stanford University, 1979, https://statistics.stanford.edu/research/multivariate-distributions-specified-marginals.

[3] A. J. Coleman, Structure of fermion density matrices, Rev. Mod. Phys. **35**, 668 (1963).

[4] A. A. Klyachko, Quantum marginal problem and N-representability, J. Phys.: Conf. Ser. **36**, 72 (2006).

[5] A. Klyachko, Quantum marginal problem and representations of the symmetric group, arXiv:quant-ph/0409113.

[6] J. Eisert, T. Tyc, T. Rudolph, and B. C. Sanders, Gaussian quantum marginal problem, Commun. Math. Phys. **280**, 263 (2008).

[7] M. Krbek, T. Tyc, and J. Vlach, Inequalities for quantum marginal problems with continuous variables, J. Math. Phys. **55**, 062201 (2014).

[8] M. Walter, B. Doran, D. Gross, and M. Christandl, Entanglement polytopes: Multiparticle entanglement from single-particle information, Science **340**, 1205 (2013).

[9] M. Christandl and A. Winter, Squashed entanglement: An additive entanglement measure, J. Math. Phys. **45**, 829 (2004).

[10] J. Chen, Z. Ji, D. Kribs, N. Lütkenhaus, and B. Zeng, Symmetric extension of two-qubit states, Phys. Rev. A **90**, 032318 (2014).

[11] L. Lami, S. Khatri, G. Adesso, and M. M. Wilde, Extendibility of Bosonic Gaussian States, Phys. Rev. Lett. **123**, 050501 (2019).

[12] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. **474**, 1 (2009).

[13] G. Tóth, Entanglement witnesses in spin models, Phys. Rev. A **71**, 010301(R) (2005).

[14] G. Tóth, C. Knapp, O. Gühne, and H.-J. Briegel, Optimal Spin Squeezing Inequalities Detect Bound Entanglement in Spin Models, Phys. Rev. Lett. **99**, 250405 (2007).

[15] L. Chen, O. Gittsovich, K. Modi, and M. Piani, Role of correlations in the two-body-marginal problem, Phys. Rev. A **90**, 042314 (2014).

[16] N. Miklin, T. Moroder, and O. Gühne, Multiparticle entanglement as an emergent phenomenon, Phys. Rev. A **93**, 020104(R) (2016).

[17] L. E. Würflinger, J.-D. Bancal, A. Acín, N. Gisin, and T. Vértesi, Nonlocal multipartite correlations from local marginal probabilities, Phys. Rev. A **86**, 032117 (2012).

[18] A. Acín and N. Gisin, Quantum Correlations and Secret Bits, Phys. Rev. Lett. **94**, 020501 (2005).

[19] D. Collins and S. Popescu, Classical analog of entanglement, Phys. Rev. A **65**, 032321 (2002).

[20] N. Gisin and S. Wolf, Linking Classical and Quantum Key Agreement: Is There "Bound Information"?, in *Proceedings of CRYPTO 2000*, edited by M. Bellare, Lecture Notes in Computer Science Vol. 1880 (Springer-Verlag, Berlin, 2000), p. 482.

[21] A. Acín, J. I. Cirac, and Ll. Masanes, Multipartite Bound Information Exists and Can Be Activated, Phys. Rev. Lett. **92**, 107903 (2004).

[22] L. Mišta, Jr. and N. Korolkova, Gaussian multipartite bound information, Phys. Rev. A **86**, 040305(R) (2012).

[23] J. Oppenheim, R. W. Spekkens, and A. Winter, A classical analogue of negative information, arXiv:quant-ph/0511247.

[24] J. Bae, T. Cubitt, and A. Acín, Nonsecret correlations can be used to distribute secrecy, Phys. Rev. A **79**, 032304 (2009).

[25] G. Prettico and J. Bae, Superactivation, unlockability, and secrecy distribution of bound information, Phys. Rev. A **83**, 042336 (2011).

[26] A. Leverrier and R. García-Patrón, Percolation of secret correlations in a network, Phys. Rev. A **84**, 032329 (2011).

[27] E. Chitambar, B. Fortescue, and M.-H. Hsieh, Classical Analog to Entanglement Reversibility, Phys. Rev. Lett. **115**, 090501 (2015).

[28] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).

[29] U. M. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, IEEE Trans. Inf. Theory **45**, 499 (1999).

[30] R. Renner and S. Wolf, New Bounds in Secret-Key Agreement: The Gap between Formation and Secrecy Extraction, in *Advances in Cryptology, EUROCRYPT 2003*, Lecture Notes in Computer Science Vol. 2656 (Springer-Verlag, Berlin, 2003), p. 562.

[31] I. Csiszár and J. Körner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory **24**, 339 (1978).

[32] M. Paraschiv, N. Miklin, T. Moroder, and O. Gühne, Proving genuine multiparticle entanglement from separable nearest-neighbor marginals, Phys. Rev. A **98**, 062102 (2018).