Percolation of secret correlations in a network

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1103/PhysRevA.84.032329">http://dx.doi.org/10.1103/PhysRevA.84.032329</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>American Physical Society (APS)</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Accessed</td>
<td>Fri Dec 14 13:46:19 EST 2018</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/69134">http://hdl.handle.net/1721.1/69134</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td></td>
</tr>
</tbody>
</table>
Percolation of secret correlations in a network

Anthony Leverrier
ICFO–Institut de Ciències Fotòniques, 08860 Castelldefels (Barcelona), Spain

Raúl García-Patrón
Research Laboratory of Electronics, MIT, Cambridge, MA 02139, USA, and
Max-Planck Institut für Quantenoptik, Hans-Kopfermann Str. 1, D-85748 Garching, Germany

(Received 8 July 2011; published 20 September 2011)

In this work, we explore the analogy between entanglement and secret classical correlations in the context of large networks—more precisely, the question of percolation of secret correlations in a network. It is known that entanglement percolation in quantum networks can display a highly nontrivial behavior depending on the topology of the network and on the presence of entanglement between the nodes. Here we show that this behavior, thought to be of a genuine quantum nature, also occurs in a classical context.

DOI: 10.1103/PhysRevA.84.032329

PACS number(s): 03.67.Dd

I. INTRODUCTION

In 1993, Maurer introduced an information-theoretically secure secret-key agreement scenario where two honest parties, Alice and Bob, have access to many independent outcomes of random variables $A,B$ correlated with the eavesdropper’s (Eve) variable $E$ through the probability distribution $P_{A,B,E}(a,b,e)$. Their goal is to extract a secret key from their data with the help of (i) local manipulations of their respective variables, using protocols such as error correction codes and privacy amplification, and (ii) communicating over a public channel, i.e., using local operations and public communication.

It was later observed in [2,3] that Maurer’s scenario shares a lot of similitude with the quantum scenario where Alice, Bob, and Eve share an initial quantum state $\rho_{ABE}$ and Alice and Bob’s task is to distill a maximum amount of entanglement qubits (ebits), i.e.,

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}([00] + [11]),$$

using local operations and classical communication. In the same way as entanglement can be seen as a resource that cannot increase under local operations and classical communication, secret classical correlations are measured in secret bits (sbits), i.e.,

$$P_{A,B,E}(a,b,e) = \frac{1}{2} \delta_{a,b} P_{E}(e),$$

a universal resource that cannot increase under local operations and public communication. In this expression, $\delta_{a,b} = 1$ if $a = b$ and $\delta_{a,b} = 0$ otherwise and $P_{E}(e)$ refers to any possible distribution of Eve’s random variable $e$, which is therefore completely uncorrelated with Alice and Bob’s variables. In [2], it was shown that many quantum information processing protocols have an equivalent protocol in Maurer’s secure secret-key scenario. For example, the analog of quantum teleportation is simply a one-time pad; see Fig. 1(b). Similarly, entanglement distillation, entanglement dilution, and (probabilistic) single-copy conversion were also shown to have secure secret-key analogous protocols. It is not surprising then that entanglement measures, such as the entanglement distillation and entanglement of formation, have corresponding secure secret-key measures [1,4,5]. The connection between entanglement and secure secret key has benefited the research in both fields. On one hand, Gisin and Wolf asked whether a classical secrecy analog of bound entanglement [4] existed. This question was positively answered in [6], where a tripartite (plus Eve) distribution $P_{ABCE}(a,b,c,e)$ was shown to need previously established secrecy between the honest parties to be generated, but from which no secret key could be distilled. Despite further results [7,8], it is still an open question whether bipartite bound secrecy exists, while bipartite bound entanglement is known to exist. On the other hand, the secrecy measure intrinsic information, introduced in [9] and shown to be a lower bound of the secret distillation and an upper bound of the secret of formation in [5], was generalized to the quantum scenario in [10]. There, the authors introduced the squashed entanglement measure, which has recently received a lot of attention [11,12].

In this paper, we want to explore the analogy between entanglement and secret classical correlations in the context of large networks. More precisely, we study the percolation of secret correlations in lattices. In the quantum case, when the goal is to establish ebits between two arbitrary nodes of a quantum lattice, there exists a phase transition for entanglement percolation for which the success probability does not decrease exponentially with the distance between the two nodes [13]. More interestingly, Ref. [13] gave the first example of a quantum protocol that changes the topology of the network, making possible the distillation of a perfect entanglement link in a regime where traditional percolation would fail. This phenomenon was further studied in [14–18] and extended to the mixed-state scenario [19–21]. In the present work, we show that the same phenomenon already happens in the purely classical context of Maurer’s secret-key agreement scenario.

II. SECRET-KEY NETWORKS

In this work, we study secrecy distribution in secret-key networks; see Fig. 1(a). More precisely, we are interested in secret-key networks in which each edge $ab$,
distribution of parameter $B$ publicly announces the value of $A$ nodes to establish an unbiased secret bit between previously unconnected connected by a link (edges of the graph). (b) One-time pad: In order distributed with a given geometry, sharing secrecy correlations when key network is composed of a set of nodes (vertices of the graph) there exists a strategy succeeding with average probability $\frac{1}{2}$ given by Eq. (3). The results for probabilistic conversion of [2] (see Appendix, Sec. 1) show that the probability of converting this biased secret bit into an unbiased one is equal to $2p$. A protocol achieving this optimal value is as follows: Let $a$ be Alice and Bob’s bit. If $a = 0$ (which happens with probability $1 - p = 1/2$, Alice tosses a biased coin that gives “heads” with probability $(1 - 2p)/(1 - p)$. If she gets heads, she tells Bob to abort the protocol; otherwise, they keep $a$ as the final sbit. It is easy to check that conditioned on the fact that the protocol did not abort, the value of $a$ is unbiased.

A chain with 2 links. Consider the scenario shown in Fig. 1(b), with three nodes where $A$ and $B$ share a biased secret bit ($a = a_1$) while $B$ and $C$ share a second biased secret bit $b_2 = c$. The probability of establishing an unbiased bit between nodes $A$ and $C$ can only be less than or equal to the probability of conversion of a single link. Surprisingly, there exists a strategy succeeding with average probability $2p$. This strategy uses one-time pad, the secret-key protocol analogous to quantum teleportation: node $B$ simply publicly announces the value of $b_1 \oplus b_2$. If $b_1 \oplus b_2 = 1$, which happens with probability $2p(1 - p)$, $C$ flips his bit and obtains an unbiased secret bit shared with $A$. If $b_1 \oplus b_2 = 0$, $A$ and $C$ secret-key (unnormalized) distribution becomes

$$P_{A, C, E}(a, c, e) \propto [(1 - p)^2 \delta_{a, c, 0} + p^2 \delta_{a, c, 1}]P_E(e),$$

which has a conversion probability $P_{\text{succ}} = 2p(1 - p) + 2p^2 = 2p$. Putting everything together gives an average probability of success of $P_{\text{succ}} = P(b_1 \oplus b_2 = 1) + P(b_1 \oplus b_2 = 0)P_c = 2p(1 - p) + 2p^2 = 2p$.

Two parallel links. If nodes $A$ and $B$ share two biased secret bits $a_1$ and $a_2$ (with $p \leq 1 - \sqrt{2}$), the optimal probabilistic conversion strategy (see Theorem 2 of Sec. A1) consists for nodes $A$ and $B$ in mapping their two bits into a new bit $a_\parallel$ such that $a_\parallel = 0$ if $a_1 = a_2 = 0$ and $a_\parallel = 1$ otherwise. The bit $a_\parallel$ then follows a Bernoulli distribution with parameter $(1 - p)^2$ and the probability of converting it into an unbiased secret bit is $2[1 - (1 - p)^2] = 2p(2 - p)$.

B. The straightforward strategy

As in the quantum scenario [13], there exists one natural strategy to distill an unbiased secret bit between two arbitrary nodes, $A$ and $B$, of a given lattice $\mathbb{L}$. This protocol consists of trying to convert each biased secret bit (corresponding to each edge of the lattice) into an unbiased secret bit, each conversion succeeding with some probability $p_{\text{succ}}$. If there exists a path among the edges of the unbiased secret bit graph connecting nodes $A$ and $B$, then, using one-time pad along this path, one can produce a secret bit between nodes $A$ and $B$. Based on percolation theory, one can show that the probability that two arbitrary nodes are connected by a path does not depend on their distance in the graph if $p_{\text{succ}}$ is larger than the critical percolation threshold probability $p_{c, L}$. For $p_{\text{succ}} \leq p_{c, L}^L$ the success probability of the overall procedure decreases exponentially with the distance in the lattice between the two nodes (see Sec. A2 for details). The question that one wishes to answer is whether or not this simple strategy is optimal and whether the bound corresponding to $p_{c, L}^L$ is tight. In the case of entanglement percolation, it was shown in [13] that the strategy described above is asymptotically optimal in the case of one-dimensional chains but not in general for two-dimensional lattices. In the following, we show that these two statements also apply to the case of secret classical correlations.

III. ONE-DIMENSIONAL CHAIN

A. Presentation of the problem

Let us consider a one-dimensional chain with $n$ links and $n + 1$ nodes: $A_0, A_1, \ldots, A_n$. Each link $i$ corresponds to a pair of biased perfectly correlated variables, as in Eq. (3). Because each pair is perfectly correlated, we simplify the discussion by noting $a_i$ the single bit shared by $A_{i-1}$ and $A_i$, as shown in Fig. 2. In this model, the eavesdropper has no prior information on the bits $a_i$ (except for the value of $p$), meaning that her initial probability distribution is uncorrelated.
with \((a_1, \ldots, a_n)\). We will now show that the probability of establishing a perfect secret bit between the extremities of a chain (between \(A_0\) and \(A_n\)) decreases exponentially fast with \(n\), except if the chain is initially composed of perfect secret bits, i.e., if \(p = 1/2\). Hence, with that respect, distribution of secrecy and distribution of entanglement display the same behavior in the case of one-dimensional chains.

B. Description of the optimal protocol

Let us first start with the smallest, but nontrivial, case of two links. The general proof will then follow by induction. As shown in Fig. 2, nodes \(A_0\) and \(A_1\) share the biased secret bit \(a_1\) and nodes \(A_1\) and \(A_2\) share \(a_2\). Both bits, \(a_1\) and \(a_2\), are biased and have value 0 with probability 1 \(-\) \(p\). The goal is for \(A_0\) and \(A_2\) to distill a secret bit unknown to Eve, who had no prior information on \(a_1\) and \(a_2\).

In order to succeed, node \(A_1\) has to publicly announce some information \(z_1\) depending on its own bits \(a_1\) and \(a_2\) and possibly on some random ancillary bits. This public information should allow nodes \(A_0\) and \(A_2\) to distill a secret bit, without giving any information to Eve. In full generality, node \(A_1\) may use a probabilistic strategy to generate \(z_1\). However, because every probabilistic strategy is a convex combination of deterministic ones, a probabilistic strategy cannot be better than the best deterministic one. Therefore, it is sufficient to consider the set of deterministic functions \(z_1 = f(a_1, a_2)\). Since \(A_1\) simply needs to tell node \(A_2\) whether it should keep its bit \(a_2\) or flip it in order to match the secret bit \(a_1, z_1\) only needs to take two possible values: 0 or 1. As a consequence, we only need to analyze 16 possible functions \(f\) of \(a_1\) and \(a_2\). The constraints of the problem help us find the only possibility for \(f\). First, node \(A_2\) should be able to recover \(a_1\) from the knowledge of \(a_2\) and \(z_1\), imposing \(f(0, a_2) \neq f(1, a_2)\). Second, Eve should not learn any information about \(a_1\), imposing \(\sum_{a_2} f(0, a_2) = \sum_{a_2} f(1, a_2)\). Up to a relabeling, the only function that satisfies these constraints is the exclusive or (XOR): \(f(a_1, a_2) = a_1 \oplus a_2\). It is not surprising that we obtain exactly the one-time pad protocol, which achieves a success probability of \(2p\) for a three node chain, as shown before.

**Generalization to \(n\) links.** In a scenario with more links, it is easy to see that the same reasoning applies. In particular, all the intermediate nodes should announce the XOR of their two bits, up to some relabeling. The protocol is therefore as follows: Each intermediate node \(A_i\) (for \(1 \leq i \leq n-1\)) publicly announces \(z_i = a_i \oplus a_{i+1}\). The final node can then compute the value of \(a_1\) since \(a_1 = a_n \oplus z_{n-1} \oplus z_{n-2} \oplus \cdots \oplus z_1\). Once nodes \(A_0\) and \(A_n\) share this (biased) secret bit, they can proceed with the optimal probabilistic conversion protocol of Theorem 2 and end up with an unbiased secret bit. The average success probability reads

\[
p_n = \sum_{z_1, \ldots, z_{n-1}} p(z_1, \ldots, z_{n-1})p(\text{success}|z_1, \ldots, z_{n-1}),
\]

where \(p(\text{success}|z_1, \ldots, z_{n-1})\) corresponds to the success probability of conversion of the bit given that the vector announced by the intermediate nodes is \((z_1, \ldots, z_{n-1})\). The success probability is equal to (twice) the first half of the binomial expansion (see Appendix, Sec. 3):

\[
p_n = 2 \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} p^{n-k}(1 - p)^k,
\]

which can be lower bounded, as shown in the Sec. A3, by

\[
p_n \leq \left[2 \sqrt{p(1-p)}\right]^n.
\]

Despite doing better than the straightforward strategy, which gives a success probability of \((2p)^n\), it still decreases exponentially fast with \(n\) for initial unbiased secret bit (\(p \neq 1/2\)), similarly as in the quantum scenario [13]. This result is not surprising as for percolation to occur, it is crucial that the topology of the network allows for many different paths between two given nodes to exist, which is not possible in a one-dimensional chain.

IV. TWO-DIMENSIONAL CASE

A possible strategy to distill a secret-key between arbitrary nodes of a lattice consists of using the straightforward strategy presented in Sec. II B. First, one tries to distill a secret bit over each link in the lattice. If the probability of success is above the percolation threshold of the lattice, then with a positive probability, this procedure creates a path consisting of secret bits between the two arbitrary nodes. This path can then be used to establish a secret bit between these two nodes thanks to one-time pad.

Following Ref. [13], we now give an explicit example of a two-dimensional lattice where local preprocessing and public communication allow one to change the topology of the initial lattice into another one with a lower percolation threshold. This shows that there exist nontrivial strategies that succeed in establishing a secret bit between two nodes when the naive strategy would fail. The protocol involves three basic operations that were described in Sec. II: (i) the conversion of a single link into an sbit with success probability \(p_s = 2p\); (ii) the conversion of two consecutive links into an sbit, also
percolation in networks. More precisely, we have shown that local operations and public communication can be used to change the topology of a secrecy network and to establish a secret key between nodes, in a regime where the initial lattice configuration is not compatible with percolation of secrecy. This effect was already known to exist in quantum entanglement networks. Our work shows that this phenomenon, thought to be of a genuine quantum nature, already appears in the context of classical secret correlations.

ACKNOWLEDGMENTS

The authors acknowledge fruitful discussions with Antonio Acín. A.L. received financial support from the EU ERC Starting grant PERCENT. R.G.-P. acknowledges financial support from the W. M. Keck Foundation Center for Extreme Quantum Information Theory and the Alexander von Humboldt foundation.

APPENDIX

1. Pure-state conversions

In Ref. [2], the authors characterized the set of transformations which are allowed among probability distributions. Their characterization is reminiscent of the quantum case [22] and uses the same notion of majorization.

**Theorem 1** (Deterministic conversion [2]). If Alice and Bob begin with an arbitrary classical bipartite pure state $P_{ABE}(i,j,k) = \delta_{i,j} p_i P_E(k)$, then they can produce a new state $P'_{ABE}(i,j,k) = \delta_{i,j} q_i P_E(k)$ if and only if $\vec{q}$ majorizes $\vec{p}$.

Recall that the vector $\vec{q} = \{q_i\}$ is said to majorize the vector $\vec{p} = \{p_i\}$ (with $p_1 \geq p_2 \geq \cdots$ and $q_1 \geq q_2 \geq \cdots$) if

$$\sum_{i=1}^k q_i \geq \sum_{i=1}^k p_i \quad \forall k.$$  \hfill (A1)

Whereas Theorem 1 is only concerned with conversion strategies which work with probability 1, the following result deals with strategies which work with a finite probability. Note that again, one recovers the same result as in the quantum case [23].

**Theorem 2** (Probabilistic conversion [2]). If Alice and Bob begin with an arbitrary classical bipartite pure state $P_{ABE}(i,j,k) = \delta_{i,j} p_i P_E(k)$, then the maximal probability with which they can produce a new state $P'_{ABE}(i,j,k) = \delta_{i,j} q_i P_E(k)$ is given by

$$\min_k \frac{1 - \sum_{i=1}^k p_i}{1 - \sum_{i=1}^k q_i}.$$  \hfill (A2)

2. Bond percolation in lattices

The percolation behaviors that appear in the context of quantum networks or secrecy networks are closely related to the concept of bond percolation. The scenario of bond percolation is the following: Consider a lattice $L$ such that for each edge of $L$, the bond is open (or equivalently, the edge is present) with probability $p$. Taking the limit where the...
size of $L$ is infinite, one can define the probability $\theta(p)$ that a randomly chosen node belongs to a cluster of infinite size. Then, there exists a critical percolation probability $p_c^L$ such that

1. $\theta(p) > 0$ if $p > p_c^L$.
2. $\theta(p) = 0$ if $p < p_c^L$.

The link to our problem is immediate. Given two arbitrary nodes of the lattice, one is interested in whether an unbiased secret bit can be established between them. In the case where there exists an infinite size component, then both nodes belong to this cluster with probability $\theta^2(p)$ and an unbiased secret bit can be established between them. Otherwise, if there is no cluster of infinite size, the probability of establishing an unbiased secret bit decreases exponentially with the distance between the nodes in the lattice $L$.

3. Analysis of the protocol of Sec. III B

Let us consider the same scenario of a chain of $n$ links where each link is a biased secret bit that takes value 1 with probability $p \leq 1/2$, and bound the probability of creating a secret bit between the extremities.

As we saw in Sec. III B, the protocol consists first in publicly announcing the vector $z = (z_1, \ldots, z_{n-1})$, and then conditionally on the value of $z$, try to convert the bit shared by $A_0$ and $A_1$ into an sbit. The probability of success $p_n$ of this procedure is therefore given by

$$p_n = \sum_{z_1, \ldots, z_{n-1}} p(z_1, \ldots, z_{n-1})p(\text{success}|z_1, \ldots, z_{n-1}), \quad (A3)$$

where $p(\text{success}|z_1, \ldots, z_{n-1})$ corresponds to the success probability of conversion of the bit given that the vector announced by the intermediate nodes is $(z_1, \ldots, z_{n-1})$.

The probability that the public communication is described by $z = (z_1, \ldots, z_{n-1})$ is

$$p(z) = p(a_1 = 0, a_2 = z_1, \ldots, a_n = \bigoplus_k z_k)$$

$$+ p(a_1 = 1, a_2 = 1 \oplus z_1, \ldots, a_n = 1 \oplus z_k).$$

Given a particular value of $z$, the success probability for the probabilistic conversion of Theorem 2 reads

$$p(\text{success}|z) = \frac{\min[p(a_1=0, \ldots, a_n=\bigoplus z_k), p(a_1=1, \ldots, a_n=1 \oplus z_k)]}{p(a_1=0, \ldots, a_n=\bigoplus z_k) + p(a_1=1, \ldots, a_n=1 \oplus z_k)}.$$

Putting everything together, one has

$$p_n = 2 \sum_a \min[p(a_1, \ldots, a_n), p(\overline{a_1}, \ldots, \overline{a_n})]$$

$$= 2 \sum_a \min[p^{u(a)}(1-p)^{n-u(a)}, p^{-n-u(a)}(1-p)^{n-u(a)}]$$

$$= 2 \sum_a p^{u(a)}(1-p)^{n-k}(1-p)^k,$$

where $a = (a_1, \ldots, a_n), \overline{a} := 1 \oplus a$, $w(a)$ denotes the Hamming weight of the vector $a$ and “first half” means that the sum contains exactly the first half of the binomial expansion, that is, the first $2^{n-1}$ terms of this expansion.

This probability is achieved if all the intermediate nodes ($n - 1$ such nodes) reveal the value of the XOR of their two bits.

This success probability is equal to (twice) the first half of the binomial expansion. Let us bound this quantity:

$$p_n = 2 \sum_{\text{first half}} \binom{n}{k} p^{k-n}(1-p)^k$$

$$\leq 2p^{[n/2]}(1-p)^{[n/2]} \sum_{\text{first half}} \binom{n}{k}$$

$$\leq p^{[n/2]}(1-p)^{[n/2]} \sum_{k=0}^{n} \binom{n}{k}$$

$$\leq 2^n p^{[n/2]}(1-p)^{[n/2]}$$

$$\leq [2\sqrt{p(1-p)}]^n,$$

which goes down to 0 exponentially fast with $n$ for $p \neq 1/2$.