Counting Method for Multi-party Computation over Non-abelian Groups

Youming Qiao[1] and Christophe Tartary[1,2]

[1] Institute for Theoretical Computer Science
Tsinghua University
Beijing, 100084
People's Republic of China
[2] Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
jimmyqiao86@gmail.com,
ctartary@ntu.edu.sg

Abstract. In the Crypto'07 paper [5], Desmedt et al. studied the problem of achieving secure n-party computation over non-Abelian groups. The function to be computed is $f_G(x_1, \ldots, x_n) := x_1 \cdot \ldots \cdot x_n$ where each participant P_i holds an input x_i from the non-commutative group G. The settings of their study are the passive adversary model, information-theoretic security and black-box group operations over G.

They presented three results. The first one is that honest majority is needed to ensure security when computing f_G. Second, when the number of adversary $t \leq \lceil \frac{n}{2} \rceil - 1$, they reduced building such a secure protocol to a graph coloring problem and they showed that there exists a deterministic secure protocol computing f_G using exponential communication complexity. Finally, Desmedt et al. turned to analyze random coloring of a graph to show the existence of a probabilistic protocol with polynomial complexity when $t < n/\mu$, in which μ is a constant less than 2.948.

We call their analysis method of random coloring the *counting method* as it is based on the counting of the number of a specific type of random walks. This method is inspiring because, as far as we know, it is the first instance in which the theory of self-avoiding walk appears in multiparty computation.

In this paper, we first give an altered exposition of their proof. This modification will allow us to adapt this method to a different lattice and reduce the communication complexity by $1/3$, which is an important saving for practical implementations of the protocols. We also show the limitation of the counting method by presenting a lower bound for this technique. In particular, we will deduce that this approach would not achieve the optimal collusion resistance $\lceil \frac{n}{2} \rceil - 1$.

Keywords: Multiparty Computation, Passive Adversary, Non-Abelian Groups, Graph Coloring, Neighbor-Avoiding Walk, Random Walk.

M.K. Franklin, L.C.K. Hui, and D.S. Wong (Eds.): CANS 2008, LNCS 5339, pp. 162–177, 2008.

1 Introduction

Multi-party computation allows multiple parties to cooperatively compute the value of a common function while keeping their own personal inputs secret. Since its introduction by Yao [17], it has become one of the major topics in cryptographic research, having applications in distributed voting, auctions, private information retrieval for instance [8]. The reader may be aware of a recent large-scale implementation of protocols for auction and benchmarks by Bogetoft et al. [**?**]. Many cryptographic primitives are based on mathematical structures being at least Abelian groups [13] as in [7, 10, 11, 12]. Similarly, numerous protocols for multiparty computation are designed over such structures [1, 3, 4]. However, the discovery of quantum algorithm to solve the factoring problem and the discrete logarithm problem [16] prevents many existing cryptographic schemes to be used on quantum computers. Since those machines seem to compute less efficiently over non-Abelian groups, designing cryptographic protocols over such mathematical structures becomes important.

The first multiparty computation protocol for non-Abelian group was designed by Desmedt et al. in [5]. They studied the existence of secure n-party protocols to compute the n-product function $f_G(x_1, \ldots, x_n) := x_1 \cdot \ldots \cdot x_n$ where each participant is given the private input x_i from some non-Abelian group G. They considered the passive (or semi-honest) adversary model [6] and information-theoretic security. They assumed that the parties were only allowed to perform black-box operations in the finite group G. This assumption means that the n parties can only perform three operations in $(G, \cdot)$: the group operation $((x, y) \mapsto x \cdot y)$, the group inversion $(x \mapsto x^{-1})$ and the uniformly random group sampling $(x \in_R G)$.

Their results are as follows: first, if the number of adversaries $t \geq \lceil \frac{n}{2} \rceil$ (dishonest majority) then it is impossible to construct a t-private protocol to compute f_G. Second, if $t < \lceil \frac{n}{2} \rceil$, they could reduce building a secure protocol to a graph coloring problem, and designed a deterministic t-private protocol computing f_G with exponential communication complexity of $O(n \binom{2\,t+1}{t}^2)$ group elements (when $t = O(n)$). Third, by using a probabilistic argument based on random coloring, they showed the existence of t-private protocols computing f_G with polynomial communication complexity of $O(n\,t^2)$ group elements when $t < \frac{n}{\mu}$, in which μ is a constant less than 2.948.

Since computationally bounded multi-party computation protocols for classical computers are often based on information theoretically secure ones, we believe that this result would show some insight on how to design computationally bounded multi-party computation algorithms relying on non-Abelian structures to be used over quantum machines.

In this paper, we further explore their analysis method of random graph coloring. We call this technique the *counting method* as it relies on counting the number of a specific type of random walks. This counting method is interesting for two reasons: not only it give us a cryptographic protocol for computing f_G due to the reductions presented by Desmedt et al., but to the best of our knowledge, it is also the first instance that applies the theory of self-avoiding walks to cryptography.

Our results are as follows: first, we give an alternative proof of the counting method from [5]. This modified demonstration will ensure that the protocol computing f_G remains secure when this method is applied to a different lattice as in Sect. 4. In this case, we will be able to reduce the communication complexity by $1/3$, which is an important saving for practical implementation of the protocol. However, the collusion resistance is not as good as the original case in [5]. Second, we give a lower bound on collusion resistance for the original case, showing that the counting method cannot give us the optimal collusion resistance $\lceil \frac{n}{2} \rceil - 1$.

In this article, we will first shortly recall the reduction proposed in [5] that relates the problem of designing a secure protocol computing f_G to a graph coloring problem. In Sect. 3, we show the outline of the counting approach, and construct a lower bound on the collusion resistance we can get from this method. In Sect. 4, we apply this method to square lattices which allows us to reduce the communication cost of the protocol by a third. Finally, we conclude our paper with remaining open questions about this method.

2 Reduction from Secure Computation to Graph Coloring

Since majority is required to ensure secure computation, we assume that $t < \lceil \frac{n}{2} \rceil$ in the remaining of the paper. In such a case, Desmedt et al. reduced the problem of designing protocol of securely computing the n-product function to the n-coloring for some specific graphs. In this section, we present these different reductions of their construction. First, we recall the definition of secure multi-party computation in the passive, computationally unbounded attack model, restricted to deterministic symmetric functionalities and perfect emulation as in [6].

We denote $[n]$ as the set of integers $\{1, \ldots, n\}$ and $\{0,\, 1\}^*$ as the set of all finite binary strings. $|A|$ denotes the cardinality of the set A.

Definition 1 ([6]). *We denote $f\,:\,(\{0,\,1\}^*)^n \mapsto \{0,\,1\}^*$ an n-input and single-output function. Let Π be an n-party protocol for computing f. We denote the n-party input sequence by $\mathbf{x} = (x_1, \ldots, x_n)$, the joint protocol view of parties in subset $I \subset [n]$ by $\mathbf{VIEW}_I^{\Pi}(\mathbf{x})$, and the protocol output by $\mathbf{OUT}^{\Pi}(\mathbf{x})$. For $0 < t < n$, we say that Π is a t-*private protocol for computing *f if there exists a probabilistic polynomial-time algorithm S, such that, for every $I \subset [n]$ with $|I| \leq t$ and every $\mathbf{x} \in (\{0,\,1\}^*)^n$, the random variables*

$$\langle S(I,\, \mathbf{x}_I,\, f(\mathbf{x})),\, f(\mathbf{x})\rangle \text{ and } \left\langle \mathbf{VIEW}_I^{\Pi}(\mathbf{x}),\, \mathbf{OUT}^{\Pi}(\mathbf{x})\right\rangle$$

are identically distributed, where $\mathbf{x}_I$ denotes the projection of the n-ary sequence $\mathbf{x}$ on the coordinates in I.

In the remaining of this paper, we assume that party P_i has a personal input $x_i \in G$ (for $i \in [n]$) and the function to be computed is the n-product $f_G(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$.

In the first step of the reduction, Desmedt et al. proved that if one can construct a symmetric (strong) t-private protocol Π' to compute the shared 2-product function $g_G(x,\, y) = x \cdot y$ where the inputs x and y are distributed among the n parties, then, $(n-1)$ iterations of Π' would give us a t-private n-party protocol for f_G. Note that the output $g_G(x,\, y)$ of Π' is to be distributed amongst the n parties, too.

The second phase of reduction in [5] consists of constructing a t-private n-party shared 2-product Π' from a suitable coloring over particular planar directed graphs.

In that model, the colors stand for the n participants, each directed edge represents one group element sent from one party to another and the non-commutativity of G is reflected in the planar property of the graph.

Finally, Desmedt et al. showed that it was sufficient to color triangular lattices defined as in Definition 2 using a coloring following the requirements of Definition 4.

Definition 2. *The graph $G_{tri}(\ell', \ell)$ is an $\ell' \times \ell$ undirected grid such that:*

- *[horizontal edges] for $i \in [\ell']$ and for $j \in [\ell - 1]$, there is an edge between nodes (i, j) and $(i, j+1)$,*
- *[vertical edges] for $i \in [\ell' - 1]$ and for $j \in [\ell]$, there is an edge between nodes (i, j) and $(i+1, j)$,*
- *[diagonal edges] for $i \in [\ell' - 1]$ and for $j \in \{2, \ldots, \ell\}$, there is an edge between nodes (i, j) and $(i+1, j-1)$.*

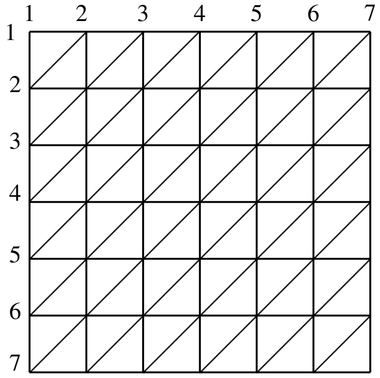

Fig. 1. The grid $G_{tri}(6, 6)$

The security requirement of the protocol is reflected in the following constraint for the coloring of $G_{tri}(\ell, \ell)$ (i.e. when $\ell' = \ell$).

Definition 3. *Let $C : [\ell] \times [\ell] \mapsto [n]$ be a n-coloring for $G_{tri}(\ell, \ell)$. Denote I a subset of $[n]$. Let $\mathcal{P}$ be a path in $G_{tri}(\ell, \ell)$. We say that $\mathcal{P}$ is a I-*avoiding path *if all its nodes are colored only with colors from $[n] \setminus I$.*

Definition 4 ([5]). *We say that $C : [\ell] \times [\ell] \mapsto [n]$ is a* weakly t-reliable n-coloring *for $G_{tri}(\ell, \ell)$ (or* good $(n,\ t)$ *coloring for convenience), if for each t-color subset $I \subset [n]$:*

- *There exists an I-avoiding path $\mathcal{P}_x$ in $G_{tri}(\ell, \ell)$ from a node on the top row to a node on the bottom row. Such a path is called an I-*avoiding top-bottom *path.*
- *There exists an I-avoiding path $\mathcal{P}_y$ in $G_{tri}(\ell, \ell)$ from a node on the rightmost column to a node on the leftmost column. Such a path is called an I-*avoiding right-left *path.*

Remark 1. Note that in the second phase, we need a directed graph, while here we define $G_{tri}(\ell', \ell)$ as undirected. This is allowed since Desmedt et al. showed that for avoiding paths, the direction does not matter.

From the reductions above, Desmedt et al. have demonstrated that it was sufficient to get a weakly t-reliable n-coloring for some $G_{tri}(\ell, \ell)$ in order to construct a t-private protocol for computing the n-product f_G. The cost communication of this protocol is $n-1$ times the number of edges of $G_{tri}(2\,\ell - 1, \ell)$ where $G_{tri}(2\,\ell - 1, \ell)$ is obtained from $G_{tri}(\ell, \ell)$ by a mirror process. Thus, the communication cost of the whole protocol computing f_G is $O(n\,\ell^2)$ group elements.

3 Random Coloring and Counting Method

In this graph coloring problem, two important parameters with respect to the number of parties n are to be taken into account. The first parameter is t, the number of adversaries the protocol must be secure against. Since honest majority is needed to ensure security, we know $t < \lceil \frac{n}{2} \rceil$. If a protocol is secure when $t < \frac{n}{\mu}$, we denote its (largest) collusion resistance as μ. We would like μ to be as close to 2 as possible. The second parameter is the size of the grid side ℓ. Since the number of edges of $G_{tri}(\ell, \ell)$ is a factor of the communication cost of the protocol, we would like to minimize this parameter as much as possible. That is, we want ℓ to be a polynomial in n.

Designing a deterministic coloring method achieving good parameters for t and ℓ at the same time seems quite difficult. In [5], Desmedt et al. turned to analyze the performance of randomly coloring the node of $G_{tri}(\ell, \ell)$ and they developed what we call the *counting method*. In short, they first counted the number of a specific type of random walks. Then, by establishing the equivalence of minimal cutsets and random walks, they plugged the number of random walks into a probabilistic argument which resulted in the existence of good (n, t) colorings when $t < \frac{n}{2.948}$.

Our observation is that, this analysis involves two combinatorial objects: (a specific type of) random walks and minimal cutsets. The central object is the minimal cutset, which has a close relation to good colorings. Then, the equivalence between minimal cutsets and random walks is used to bound the number of such cutsets. In our exposition of the counting method, we emphasize on the importance of minimal cutsets. We use minimal cutsets during the whole proof and only show the equivalence between minimal cutsets and random walks in the last step of the demonstration. Thus, we can adapt the first part of the proof to square lattices without modification to the part involving minimal cutsets as in Sect. 4.

Theorem 1 ([5]). *For any constant $R > 2.948$, if $t \leq \frac{n}{R}$, there exists a black-box t-private protocol for f_G with communication complexity $O(n^3)$ group elements.*

Proof. The algorithm is simple: set $G_{tri}(\ell, \ell)$ with $\ell = O(n)$ (the explicit value of the parameter ℓ will be given later) and we choose a color for each vertex independently and uniformly at random from the set $[n]$. Next, we use the counting method to analyze the effect of this random coloring. The central combinatorial object in this method is *the minimal left-to-right (top-to-bottom) cutset* of $G_{tri}(\ell, \ell)$.

Definition 5 (Cutset/Minimal Cutset). *A set of nodes S in $G_{tri}(\ell, \ell)$ is called a* top-bottom cutset *(resp.* right-left cutset*) if all top-bottom paths (resp. right-left paths) in $G_{tri}(\ell, \ell)$ go through at least one node in S. A cutset S is called* minimal *if removing any node from S destroys the cutset property.*

It is easy to see that every cutset contains a minimal cutset. The relation between minimal cutsets and good (n, t) colorings is established in the following lemma, which will allow us to use this method to a different type of lattices in Sect. 4.

Lemma 1. *Let C be an n-coloring of $G_{tri}(\ell, \ell)$. If every minimal cutset contains more than t colors then C is a good (n, t) coloring for $G_{tri}(\ell, \ell)$.*

Proof. We demonstrate this result by contradiction. Suppose that C is not a good (n, t) coloring for $G_{tri}(\ell, \ell)$. Then, we know that there exists a t-color subset $I \subset [n]$, such that (w.l.o.g) no I-avoiding left-right paths exist in this graph.

We denote the reduced graph of vertices colored in I as H_I, and the reduced graph of vertices colored in $[n]\backslash I$ as $\bar{H}$. We claim that H_I forms a right-left cutset. If it is not the case, then there exists some right-left path in $\bar{H}$ due to planarity and connectivity. This contradicts the hypothesis that no I-avoiding paths exist in $G_{tri}(\ell, \ell)$. So, there is a minimal cutset $S_I \subset H_I$, and the vertices of S_I are only colored with colors in I, forming a contradiction. □

Given this lemma, we can analyze the effect of random coloring as follows. Suppose that we could count the number of minimal cutsets of size k on $G_{tri}(\ell, \ell)$. Then, over the random colorings of $G_{tri}(\ell, \ell)$, we could bound the probability that there exists some minimal cutset that contains no more than t colors. If this probability could be shown to be less than 1 when ℓ is $O(n)$, then we would deduce that there exists some coloring C that is a good $(n,\ t)$ coloring for $G_{tri}(\ell, \ell)$ according to Lemma 1. Then, using the reduction introduced in Sect. 2 would complete the proof of Theorem 1.

Now, two points remain to be done: first, to bound the number of minimal cutsets; second, to perform the probabilistic analysis. The second point is similar to what Desmedt et al. showed in [5] except that we replace the term *path* employed in [5] with *cutset*. We just include the probabilistic argument here for completeness.

Let $N_P(k, \ell)$ denote the total number of minimal right-left cutsets in $G_{tri}(\ell, \ell)$ of size k. Let $p_x(I)$ $(p_y(I))$ denote the probability that there exists a minimal right-left (top-bottom) cutset P whose node colors are all in the t-subset I representing the set of colluders. We also denote $p(I)$ the probability there exists some minimal cutset that contains only colors in I.

Since node colors are chosen independently and uniformly in $[n]$, each minimal right-left cutset of size k has probability $\left(\frac{t}{n}\right)^k$ to have all its node colors in I. It is clear that $\ell \leq k \leq \ell^2$. So, summing over all possible minimal cutset sizes, we have: $p_x(I) \leq \sum_{k=l}^{\ell^2} N_P(k, \ell) \left(\frac{t}{n}\right)^k$. By symmetry, we have $p_y(I) \leq \sum_{k=l}^{\ell^2} N_P(k, \ell) \left(\frac{t}{n}\right)^k$. So, an upper bound on the probability $p(I)$ is: $p(I) \leq 2 \sum_{k=l}^{\ell^2} N_P(k, \ell) \left(\frac{t}{n}\right)^k$.

Finally, taking a union bound over all $\binom{n}{t}$ possible t-color subsets I, we get an upper bound on the probability p that the random coloring C is not a good $(n,\ t)$ coloring as

$$p \leq 2 \sum_{k=\ell}^{\ell^2} N_P(k, \ell) \left(\frac{t}{n}\right)^k \binom{n}{t} \tag{1}$$

Now, we bound the number of minimal cutsets with respect to their respective size k. This is where the counting method is interesting. Instead of directly counting the number of minimal cutsets, we will prove that minimal cutsets, a static structure, are equivalent to some type of random walks, which is a dynamic structure. Then, we will simply bound the number of such walks, which is the subject of investigations in Physics with a rich theory on its own respect.

On an *infinite* planar lattice, a random walk starts from some node and, at each step, it randomly chooses some point from the neighbors of its current vertex as the next step. A *Self-Avoiding Walk* (SAW) is a random walk such that the walker has a memory so that he will avoid any vertex which has been visited previously [15]. It is useful in Physics and Chemistry when people try to model the structure of polymer chain. Here, our focus is on a generalization of SAW: *Neighbor-Avoiding Walk* (NAW). As its name suggests, a NAW is a random walk that avoids the neighbors of this walk. We introduce the following definition for the finite grid $G_{tri}(\ell, \ell)$.

Definition 6 (Restricted NAW). *A* restricted *right-left (resp. top-bottom)* NAW *on $G_{tri}(\ell, \ell)$ is a* NAW *such that:*

- its starting node is on the rightmost column (top row);
- its ending node is on the leftmost column (bottom row);
- and no internal nodes are on the rightmost (top) or leftmost column (bottom row).

The study of NAW is a novelty that we introduce with respect to [5]. The following is an adaptation of Lemma 4.6 from [5]. An illustration is given on Fig. 2 when $\ell = 6$.

Lemma 2. *On $G_{tri}(\ell, \ell)$, a set of nodes is a right-left minimal cutset if and only if it forms a restricted top-bottom* NAW.

There is a rich literature on bounding the number of SAWs on different lattices. Lin and Hsaio showed in [14] that the number N of SAWs or NAWs with respect to number of steps already taken k had the following form:

$$N \approx A\mu^k k^\gamma$$

in which A, μ and γ are constants depending on the type of lattice (triangular, square,...) and walk (SAWs, NAWs,...). Since μ^k constitutes the major fraction of N, μ plays a central role in estimating N. This value μ is called the *connective constant* of the lattice (related to the type of walk). For any walk on any lattice, we define μ as $\mu := \lim_{n\to\infty} (N(k)^{1/k})$. Compared to SAWs, the estimation of μ of NAWs receives far less attention [9]. Desmedt et al. bounded this number on their own as follows.

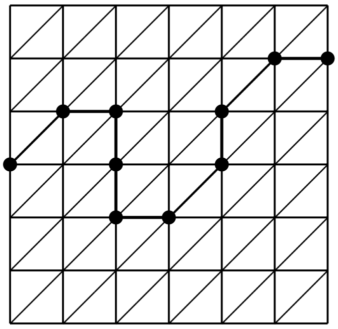

Fig. 2. A NAW on $G_{tri}(6,\ 6)$ which is a minimal cutset

Lemma 3 ([5]). *The number $M_P(k,\ell)$ of* NAW*s of length k on infinite triangular lattice is upper bounded as:*

$$M_P(k) \leq c(\mu)\, \mu^k$$

for some constants μ, $c(\mu)$, with $\mu \leq 2.948$. Here, μ is just the connective constant *of* NAW*s on infinite triangular lattices.*

Remark 2. Note that the set of NAWs on $G_{tri}(\ell,\ell)$ of length k is a subset of NAWs on infinite triangular lattices of length k, so the number of restricted right-left NAWs is upper bounded by $\ell M_P(k) = c(\mu)\,\ell\,\mu^k$ as we have ℓ starting points at the rightmost column.

Remark 3. Note that we bounded the number of NAWs on infinite lattices instead of that of restricted NAWs on $G_{tri}(\ell,\ell)$. Since the set of restricted NAWs on $G_{tri}(\ell,\ell)$ is a subset of NAWs on infinite triangular lattices, finding a specific bound for $G_{tri}(\ell,\ell)$ may lead to some improvements on the value of the connective constant over such graphs.

Given the equivalence between minimal cutsets and restricted NAWs, we get: $N_P(k,\ell) \leq c(\mu)\,\ell\,\mu^k$. So, after substituting $N_P(k,\ell)$ in (1) with $c(\mu)\,\ell\,\mu^k$, we have:

$$p \leq 2\,c(\mu)\,\ell^3 \left(\frac{\mu\, t}{n}\right)^{\ell} \binom{n}{t}$$

Thus, if $\frac{n}{t} \geq R > \mu$ on $G_{tri}(\ell,\ell)$, then it is clear that this upper bound on p is less than 1 for sufficiently large ℓ. It is sufficient to have $\ell = O(\log(\binom{n}{t})/\log(n/(\mu t))) = O(n)$, as claimed. This finishes the analysis of the counting approach. □

To summarize what we have done so far, we showed the relation between good coloring and minimal cutset, and use a probabilistic argument to show the existence of such a good coloring. Then, we established the equivalence between minimal cutset and restricted NAW on $G_{tri}(\ell,\ell)$, and bounded the number of restricted NAWs to complete the proof.

One last thing to notice is that the collusion resistance of the protocol is just the connective constant μ. Here, we only have an upper bound for μ in Lemma 3, so one might guess that μ is quite close to 2, giving us a good collusion resistance. However, we now prove that it is not the case by showing that $\mu \geq 1 + \sqrt{2} \approx 2.414$. So, simply improving μ would not give us information about protocols whose collusion resistances are in $(2,\ 2.414)$. In other words, the counting method on $G_{tri}(\ell, \ell)$ cannot be used to prove the existence of t-private protocol for computing f_G when $\frac{n}{2.414} < t < \frac{n}{2}$.

Theorem 2. *The connective constant μ of* NAWs *on triangular lattices is at least* $1 + \sqrt{2}$.

Proof. We show a family of NAWs with connective constant $\mu' = 2.414$ by considering a random walker who moves on the infinite triangular lattice following some constraints. Call the node where the walker is currently located the *current* node, and the node before the current node the *last* node.

Consider such a family of random walks formed by the following rule:

1. The walker starts at the origin point. It has three choices: up ($\uparrow$), right ($\rightarrow$) and up-right diagonal($\nearrow$);
2. The possible choices of the walker depend on its last move:

Last Move	Possible Choices
$\uparrow$	$\uparrow, \nearrow$
$\nearrow$	$\uparrow, \rightarrow, \nearrow$
$\rightarrow$	$\rightarrow, \nearrow$

We need to prove that this forms a family of NAWs. First, at every step the walker avoids the neighbors of the last node due to its possible choices. Second, the neighbors of the nodes before the last node lie on the left lower side of the current node, while the walker will only go to the right upper side. So, the set of all such walks forms a family of NAWs.

One can count the number $T(k)$ of NAWs with respect to the number of steps k ($k \geq 1$) already taken as follows. Let f_k be the number of NAWs of length k, when the walker has three choices for the next step (e.g. the last move is $\nearrow$). Let g_k be the number of NAWs of length k, when the walker has two choices for the next move (e.g. the last move is $\uparrow$ or $\rightarrow$). We have the following recursive equations:

$$\begin{cases} f_{k+1} = f_k + g_k \\ f_0 = 1 \end{cases} \qquad \begin{cases} g_{k+1} = 2\,f_k + g_k \\ g_0 = 0 \end{cases}$$

We get:

$$T(k) = \frac{1}{2}\left(\left(1+\sqrt{2}\right)^{(k+1)} + \left(1-\sqrt{2}\right)^{(k+1)}\right)$$

Recall the definition of connective constant, and we have $\mu' = 1 + \sqrt{2}$. Since this is just a subset of NAWs, we have: $\mu \geq \mu' = 1 + \sqrt{2}$. □

4 The Counting Method on Square Lattices

Let $G_{sqr}(\ell,\ell)$ be the graph after removing the diagonal edges of $G_{tri}(\ell,\ell)$. So, G_{sqr} (ℓ,ℓ) is just the square grids of side size ℓ. In this section, we adapt the counting method to $G_{sqr}(\ell,\ell)$ and get a protocol that saves about $1/3$ communication complexity compared to the triangular lattices case. However, the collusion resistance of this protocol is not as good as the original one: we show a trivial upper bound 5. Though, we do not get a lower bound, we believe that the collusion resistance is larger than 3 in this case.

Remark 4. We would like to explain why we can color G_{sqr} instead of G_{tri} and still get a protocol for computing f_G. We reason as follows. Remember that in order for an n-coloring C on G_{tri} to be (n,t) good, we require that, for every $I \subset [n]$ of size t, there exist I-avoiding top-bottom and right-left paths. If the diagonal edges in G_{tri} are not used for any I-avoiding paths of $I \subset [n]$, then to consider colorings on $G_{sqr}(\ell,\ell)$ is sufficient.

To apply the counting method to square lattices $G_{sqr}(\ell,\ell)$, we need to examine the proof presented in Sect. 3. It is easy to see that the proof is still valid (by replacing G_{tri} with G_{sqr}) on square lattices up to the point where we need to bound the number of minimal cutsets on square lattices. In the G_{tri} case, we bounded the number of minimal cutsets by showing the equivalence of minimal cutsets and restricted NAWs and bounding the number of the walks instead. It seems difficult to proceed identically over square lattices since it could be shown that a minimal cutset on square lattices may not need to be a *walk*, as shown on Fig. 3.

However, we could show that restricted NAWs on a graph $G_{dia}(\ell,\ell)$ related to $G_{sqr}(\ell,\ell)$ are just minimal cutsets on $G_{dia}(\ell,\ell)$. The graph $G_{dia}(\ell,\ell)$ is simple: you just connect both diagonals of every 1×1 grid in $G_{sqr}(\ell,\ell)$ (see Figure 3). The restricted NAWs on $G_{dia}(\ell,\ell)$ are defined similarly as in Definition 6.

Lemma 4. *A set of nodes S on $G_{sqr}(\ell,\ell)$ is a minimal top-bottom (resp. right-left) cutset if and only if it forms a restricted right-left (resp. top-bottom)* NAW *on $G_{dia}(\ell,\ell)$.*

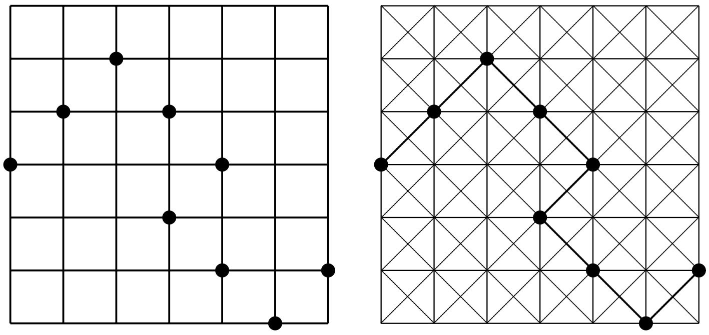

Fig. 3. $G_{sqr}(6,6)$ and its corresponding $G_{dia}(6,6)$. The node set presented in the graph is a minimal cutset of $G_{sqr}(6,6)$. It is not a walk on G_{sqr}, but it is an NAW on G_{dia}.

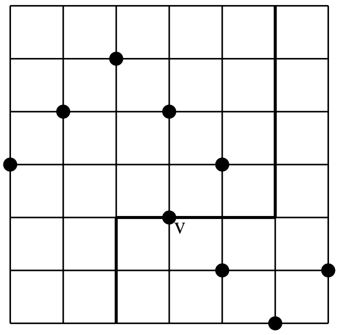

Fig. 4. Unique paths of v

Proof. We first demonstrate the necessary condition: since G_{sqr} is planar, we know S forms a cutset. Then, we claim that it is minimal. First, observe that, on G_{sqr}, we can reach every neighbor of S from the leftmost or the rightmost column. Otherwise, there would be a cycle around the particular neighbor on G_{dia}, which is not allowed for NAWs. Call a neighbor v of S a *left neighbor* if there is a path on G_{sqr} between v and the leftmost column without crossing nodes in S. A *right neighbor* is defined similarly. Thus, a neighbor of S is either a right neighbor or a left neighbor. We have three cases for $u \in S$:

1. u is not on the leftmost or rightmost column: in this case, it could be shown that u must have right and left neighbors at the same time (by enumerating all configurations of NAWs on G_{dia}). So, after removing u from S, we just need to connect its left and right neighbors through u on G_{sqr} to get a right-left path.
2. u is on the leftmost or rightmost column except the four corners: suppose u is on the leftmost column. Then, u must have a right neighbor due to the configurations of NAWs on G_{dia}. So, removing u from S would also give us a right-left path;
3. u is at the four corners of G_{sqr}: since S is restricted, removing u we would immediately get a right-left path (it is the top row or the bottom row).

Now, we look at the sufficient condition. First, we have a simple lemma about minimal cutsets. An illustration is given as Fig. 4.

Lemma 5. *A right-left cutset S is minimal if and only if for all $v \in S$, there is some right-left path P_v, such that the only node from S on P_v is v. For some node v in a minimal cutset S, such a P_v is called the* unique path *of v.*

Proof. The necessary condition: in this case, after removing any $v \in S$, the unique path P_v of v is just a right-left path that does not meet any node in S, destroying the cutset property.

The sufficient condition: suppose there exists $v \in S$ such that for every right-left path P crossing v would cross some other node in S. Then, removing v would not destroy the cutset property, contradicting the assumption about the minimality of S. □

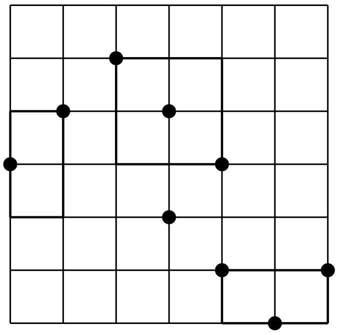

Fig. 5. Different windows of nodes in a minimal cutset of G_{sqr}

Unique paths play an important role in this proof. By using unique paths and the planarity of $G_{sqr}(\ell, \ell)$, we could show the following properties of minimal cutset on G_{sqr} (detailed proofs of those properties are in Appendix A).

Lemma 6. *A minimal right-left cutset contains exactly one node on the top row and one node on the bottom row.*

Lemma 7. *A* 1×1 *grid contains at most two nodes in a minimal cutset.*

Definition 7. *The* window *of some node v from some node set S that is not on the sides is the* 2×2 *grid with v at its center. If v is on the leftmost column (or rightmost) column, we call the* 2×1 *grid with v at the center of its left (or right) column the* half window *of v. If v is on the top row (or bottom) row, we call the* 1×2 *grid with v at the center of its top row (or bottom row) the* half window *of v.*

Lemma 8. *For minimal right-left cutset, each window contains exactly* 3 *nodes. For half windows, we have each left/right half window contains exactly 3 nodes, while each top/bottom half window contains exactly* 2 *nodes.*

We could show that these three properties, plus the minimality property fully characterize restricted top-bottom NAWs on G_{dia}.

Lemma 9. *The minimal right-left cutset S on G_{sqr} is a restricted top-bottom* NAW *on G_{dia}.*

Proof. The cutset S can be viewed as a walk on G_{dia} under such guidance: the walker starts from the unique node on the top row, and goes to the only node at its half window. While it is not on the bottom row, it always has a unique next step to take according to its current window specified in Lemma 8. Finally, it would reach the bottom row. At that point, it has to stop since he has no choices any longer.

First, notice that such a walk would cross all nodes in S. Otherwise, due to planarity, removing the vertex not on the walk would not destroy S's cutset property. This walk is also restricted due to Lemma 6.

To make this random walk a restricted NAW, we need to show that the walker always avoids the neighbors. First, due to Lemma 7, the next step of the walker avoids the neighbors of the last node. Second, it would also avoids the neighbors of the nodes before the last node due to Lemma 8. Thus, we proved that a minimal cutset on G_{sqr} is also a restricted NAW on G_{dia}. □

This last lemma completes the proof of Lemma 4. □

Having established the equivalence between minimal cutsets on G_{sqr} and restricted NAWs on G_{dia}, we can now apply the counting method to G_{sqr}. Another concern is the connective constant μ_{dia} of restricted NAWs on G_{dia}. By considering 1-step history of NAWs, we could get a trivial upper bound of 5.

Thus, we adapted the counting method to square lattices. Note that the number of edges in G_{sqr} is roughly $2/3$ of the number of edges in G_{tri}. So, we saved the communication complexity of the whole protocol by $1/3$. Table 1 summarizes the comparison of the counting method applied on G_{tri} and G_{sqr}.

Table 1. Statistics of the counting method

	On $G_{tri}(l,\ l)$	On $G_{sqr}(l,\ l)$
Communication Complexity	$c = O(n^3)$	$\frac{2}{3}c$
Collusion Resistance	$2.414 \leq \mu \leq 2.948$	$\mu \leq 5$

5 Conclusion and Open Problems

We showed that the counting method could be applied to square lattices and save communication complexity of the protocol by $1/3$, which is important when implementing the multiparty protocol. We also gave a lower bound of this method for collusion resistance on triangular lattices which shows the limitation of this method on $G_{tri}(\ell, \ell)$.

Note the comparison of applying the counting method to G_{sqr} and G_{tri}. There seems to be a tradeoff between communication complexity and collusion resistance. We think this tradeoff is due to the structure of the lattice and the minimal cutset on this lattice. The interplay between minimal cutset and a specific random walk is important as well. We ask the question of generalizing this method to other types of planar lattices and find which type of random walk corresponds to the minimal cutsets on that lattice.

We emphasize that we bounded the number of walks with respect to number of steps taken on infinite lattices. Due to the reduction of Desmedt et al., we really need to bound the number of random walks on finite lattices and we might hope to obtain security for larger $t = \frac{n}{\mu} > \frac{n}{2.948}$ using particular graphs. So, whether there is difference between those two cases is also an interesting problem.

Acknowledgments

The authors would like to thank Professor Xiaoming Sun for valuable discussions on secret sharing. The authors are also grateful to the anonymous reviewers for their comments to improve the quality of this paper. The two authors' work was sponsored by the

National Natural Science Foundation of China grant 60553001 and the National Basic Research Program of China grants 2007CB807900 and 2007CB807901. Christophe Tartary's research was also financed by the Ministry of Education of Singapore under grant T206B2204.

References

[1] Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: 20th Annual ACM Symposium on Theory of Computing, Chicago, USA, May 1988, pp. 1–10. ACM Press, New York (1988)

[2] Bogetoft, P., Christensen, D.L., Damgård, I.B., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M., Toft, T.: Multiparty computation goes lives. Cryptology ePrint Archive, Report 2008/068 (January 2008), http://eprint.iacr.org/2008/068.pdf

[3] Cramer, R., Damgård, I.B., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000)

[4] Damgård, I.B., Ishai, Y.: Scalable secure multiparty computation. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 501–520. Springer, Heidelberg (2006)

[5] Desmedt, Y., Pieprzyk, J., Steinfeld, R., Wang, H.: On secure multi-party computation in black-box groups. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 591–612. Springer, Heidelberg (2007)

[6] Goldreich, O.: Foundations of Cryptography. Basic Applications, vol. II. Cambridge University Press, Cambridge (2004)

[7] Goldreich, O., Vainish, R.: How to solve any protocol problem - an efficiency improvement. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 73–86. Springer, Heidelberg (1988)

[8] Goldwasser, S.: Multi-party computations: Past and present. In: 16th annual ACM symposium on Principles of Distributed Computing, Santa Barbara, USA, August 1997, pp. 1–6. ACM Press, New York (1997)

[9] Guttmann, A.J., Parviainen, R., Rechnitzer, A.: Self-avoiding walks and trails on the 3.12 lattice. Journal of Physics A: Mathematical and General 38, 543–554 (2004)

[10] Hirt, M., Maurer, U.: Robustness for free in unconditional multi-party computation. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 101–118. Springer, Heidelberg (2001)

[11] Hirt, M., Maurer, U., Przydatek, B.: Efficient secure multi-party computation. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 143–161. Springer, Heidelberg (2000)

[12] Hirt, M., Nielsen, J.B.: Robust multiparty computation with linear communication complexity. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 463–482. Springer, Heidelberg (2006)

[13] Lang, S.: Algebra (Revised Third Edition). Springer, Heidelberg (2002)

[14] Lin, K.-Y., Hsaio, Y.C.: Self-avoiding walks and related problems. Chinese Journal of Physics 31(6-I), 695–708 (1993)

[15] Madras, N., Slade, G.: The Self-Avoiding Walk. Probability and Its Applications. Birkhäuser, Basel (1996)

[16] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26(5), 1484–1509 (1997)

[17] Yao, A.C.-C.: Protocols for secure computations. In: 23rd Annual IEEE Symposium on Foundations of Computer Science, Chicago, USA, November 1982, pp. 80–91. IEEE Press, Los Alamitos (1982)

A Proofs of Three Properties of Right-Left Minimal Cutsets on $G_{sqr}(\ell, \ell)$

Since the basic ideas of these properties are quite similar, we provide a detailed demonstration for Lemma 10 and we simply show the outline of the proofs for the remaining two properties.

Lemma 10. *A minimal right-left cutset contains exactly one node on the top row and one node on the bottom row.*

Proof. We demonstrate this result by contradiction. Suppose that, for some right-left cutset S, there exist two nodes u and v at the top row and $u, v \in S$. Suppose that u lies on the mth column and v lies on the nth column. Consider the unique paths P_u for u and P_v for v (see Fig 6 for a rough representation of this situation). We can make the assumption that P_u crosses u only once, and P_v crosses v only once.

Now, let the walker A move along P_u from the leftmost column, and walker B move along P_v from the rightmost column. Due to the planarity of the grid, we know that the paths of A and B would meet at some node w that lies on column k, $m \leq k \leq n$ after they cross u and v respectively. Now, if we connect the rest of P_u and the rest of P_v through w we will get a path Q that does not cross any node in S, contradicting with its cutset property. □

Lemma 11. *A* 1×1 *grid contains at most two nodes in a minimal cutset.*

Proof. We prove this result by contradiction. Assume that, for some minimal top-bottom cutset S, there exists a 1×1 grid in which there are three nodes u, v and $w \in S$. So, we have such a configuration for unique paths P_u, P_v and P_w as shown on Fig. 7.

In this case, if the walker follows P_w from bottom to top, then it is clear that P_w would have no choices but to intersect with P_u or P_v after it crosses w (and after P_u crosses u/P_v crosses v). This would destroy the cutset property of S. □

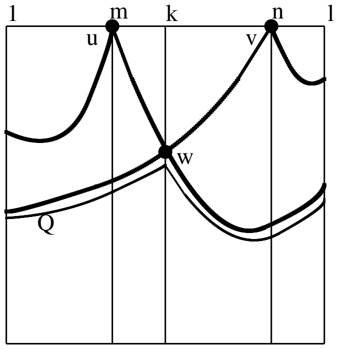

Fig. 6. The path Q does not cross any node in S

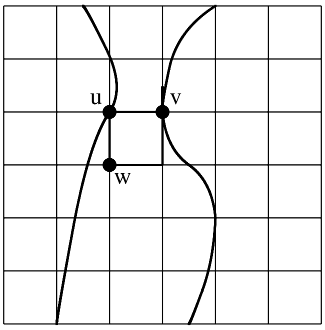

Fig. 7. When some 1×1 grid contains three points from a minimal cutset S

Lemma 12. *For minimal top-bottom cutset, each window contains exactly* 3 *nodes. For half windows, we have each left/right half window contains exactly* 2 *nodes, while each top/bottom half window contains exactly* 3 *nodes.*

Proof. This proof is quite similar to the demonstration of Lemma 11. We just illustrate the configuration of unique paths when the window of v has u, w and t in it. This is a special case, but one can enumerate all cases and find that they are all similar to this one.

From Fig. 8, we can see the unique path of t has to intersect with P_u of P_v after it crosses t (and after P_u crosses u/P_v crosses v), thus destroying the cutset property. □

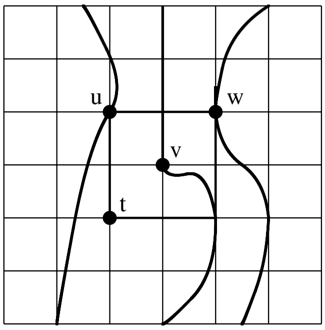

Fig. 8. When some 2×2 grid contains four points from a minimal cutset S