

Applying Recreational Mathematics to Secure Multiparty Computation

Yvo Desmedt

BT Chair of Information Security
University College London
UK

September 5, 2007

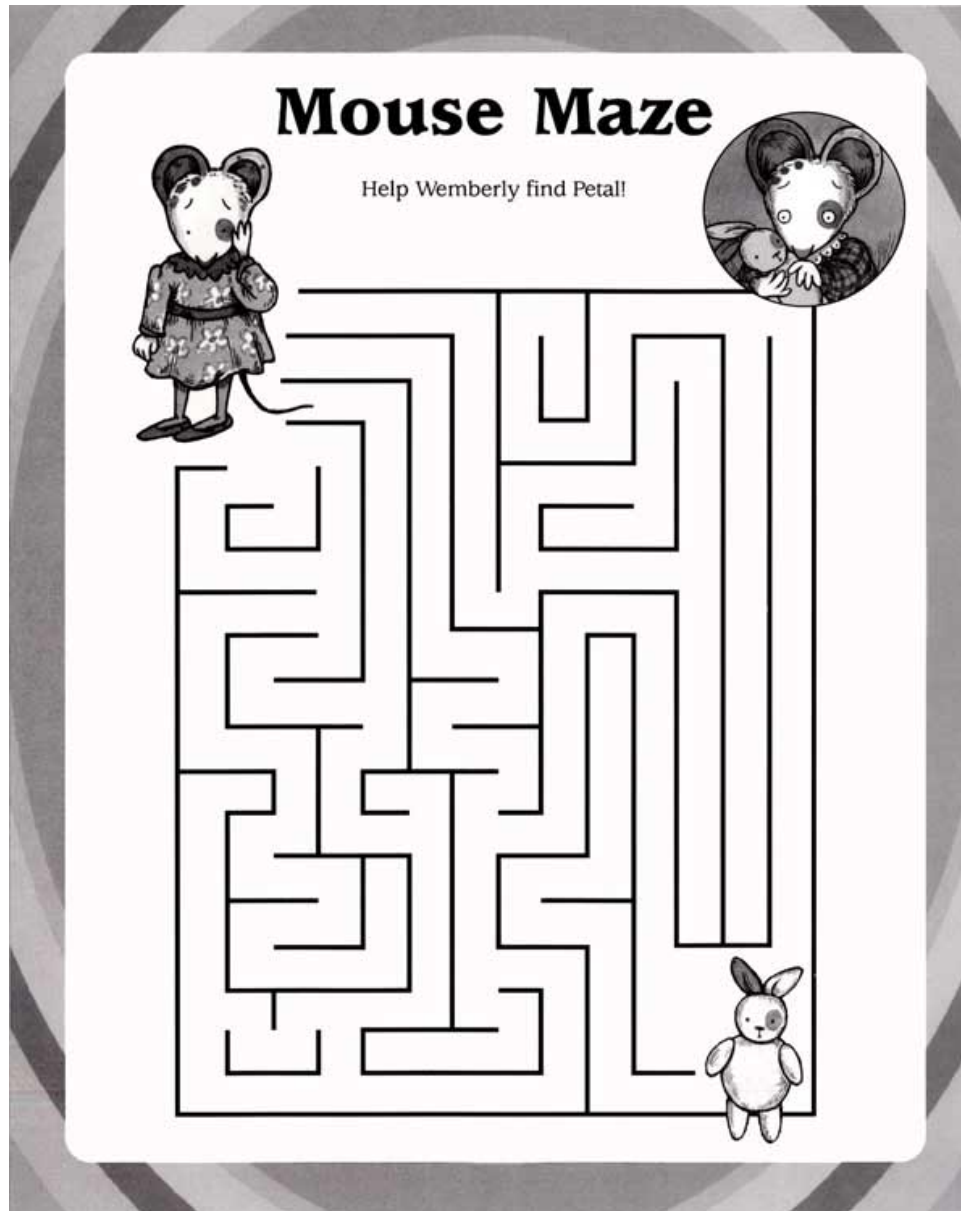
Yvo Desmedt was also partially supported by NSF ANI-0087641, EPSRC EP/C538285/1, the Australian ARC grants DP0344444 and DP0665035. He is also a courtesy professor at Florida State University (USA).

This presentation is based on joint work with Josef Pieprzyk, Ron Steinfeld and Huaxiong Wang. Parts of it were presented at Crypto 2007 and appeared in the proceedings.

OVERVIEW

1. The classical mouse traveling through a maze
2. A reliable variant
3. Three types of solutions to the problem
4. Applications
5. The link with secure multiparty computation
6. Open problems

1. THE CLASSICAL MOUSE TRAVELING THROUGH A MAZE



2. A RELIABLE VARIANT

Above maze can easily be represented by a planar graph on a grid. The problem of finding a path can easily be solved on a computer, e.g., using Dijkstra's shortest path algorithm.

We consider the following variant:

- Instead of using a planar graph, we deal with a vertex-colored planar graph.
- We demand reliability. Consider the case that each color corresponds to a platform. We allow up to t platforms to fail. That means:

for any t colors, one could remove all vertices that have these colors and their adjacent edges. We call the remaining graph a reduced grid.

- For any selection of these t colors: the mouse must be able to move in the reduced grid from the first row to the last row, and from the first column to the last column.

(See, further for examples and constructions.)

When the grid has size $m \times m$ and we have a coloring function $[m] \times [m] \rightarrow [n]$ such that above is satisfied, we call it an t -Reliable n -Colouring for a Planar Graph with size parameter m .

Note: not all grid points must contain vertices.

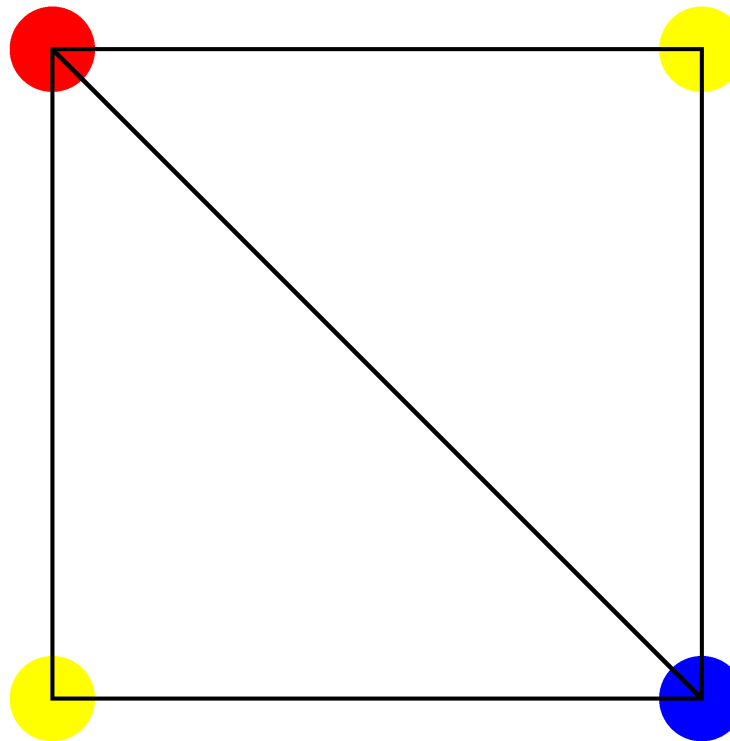
Observation: $n \geq 2t + 1$.

Proof: Suppose we use the colors C with $|C| = n = 2t$. Select a subset C' of t adversarial colors. A left \rightarrow right path free of these colors must exist. Its colors come from $C \setminus C'$. Since $|C \setminus C'| = t$, the set $C \setminus C'$ can stop any communication from top to bottom!

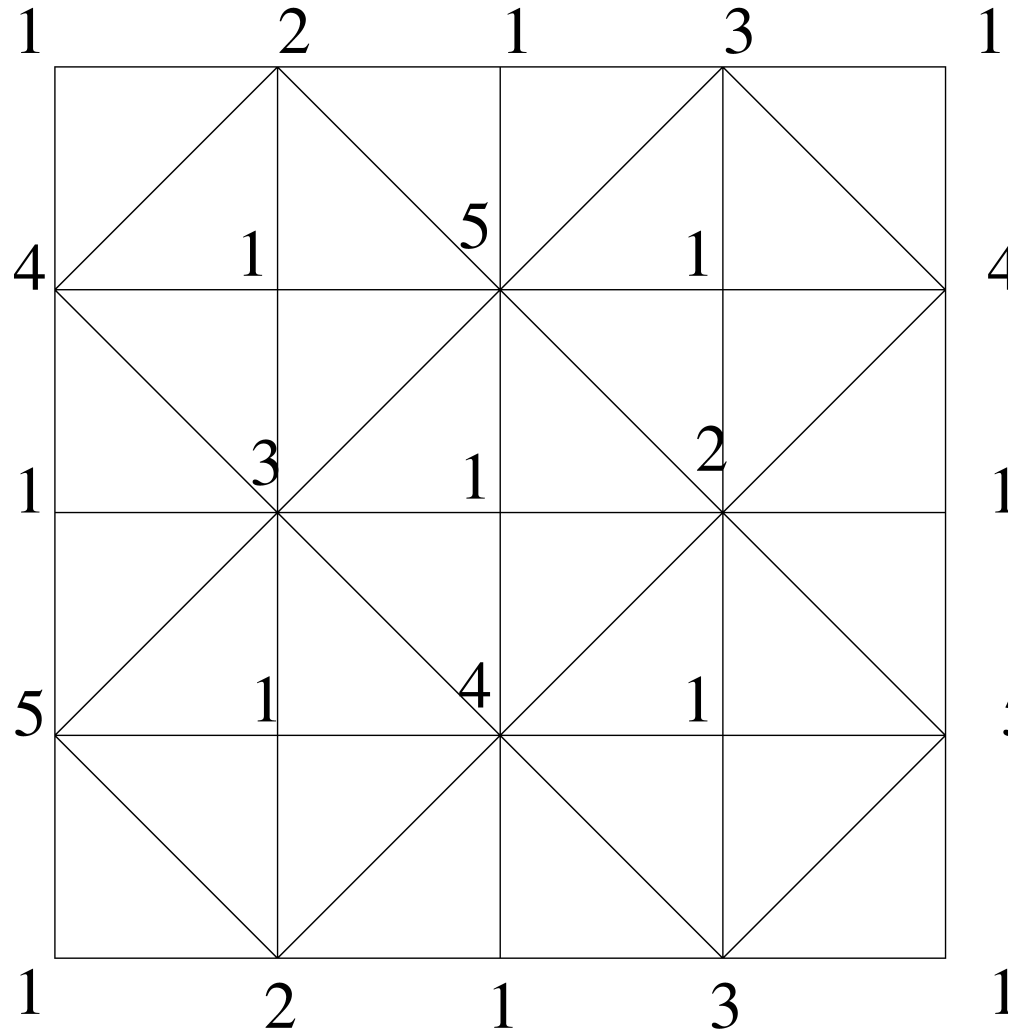
3. THREE TYPES OF SOLUTIONS TO THE PROBLEM

3.1. Small t

$$t = 1 \text{ and } n = 3$$



$t = 2$ and $n = 5$

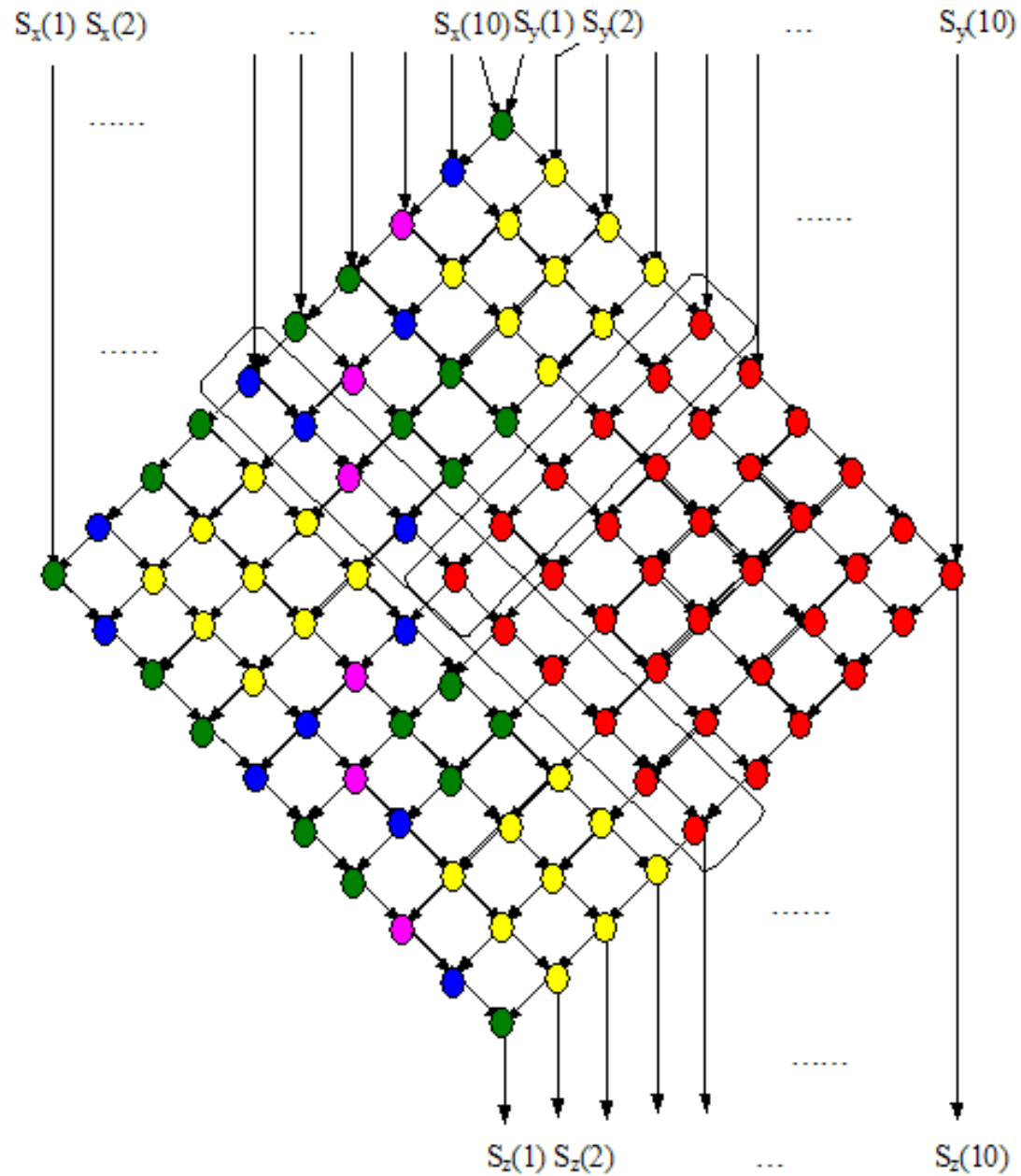


3.2. Any $t, n = 2t + 1$

We use an example to illustrate:

	{1,2}	{1,3}	{1,4}	{1,5}	{2,3}	{2,4}	{2,5}	{3,4}	{3,5}	{4,5}									
{1,2}	3	—	4	—	3	—	4	—	3	—	3	—	5	—	4	—	3		
{1,3}	4	—	2	—	2	—	4	—	5	—	4	—	2	—	2	—	2		
{1,4}	3	—	2	—	2	—	2	—	5	—	3	—	3	—	2	—	2	—	2
{1,5}	3	—	2	—	2	—	2	—	4	—	3	—	3	—	2	—	2	—	2
{2,3}	4	—	4	—	5	—	4	—	1	—	1	—	1	—	1	—	1	—	1
{2,4}	3	—	5	—	3	—	3	—	1	—	1	—	1	—	1	—	1	—	1
{2,5}	3	—	4	—	3	—	3	—	1	—	1	—	1	—	1	—	1	—	1
{3,4}	5	—	2	—	2	—	2	—	1	—	1	—	1	—	1	—	1	—	1
{3,5}	4	—	2	—	2	—	2	—	1	—	1	—	1	—	1	—	1	—	1
{4,5}	3	—	2	—	2	—	2	—	1	—	1	—	1	—	1	—	1	—	1

Another way to view it:



3.3. A polynomial size probabilistic solution

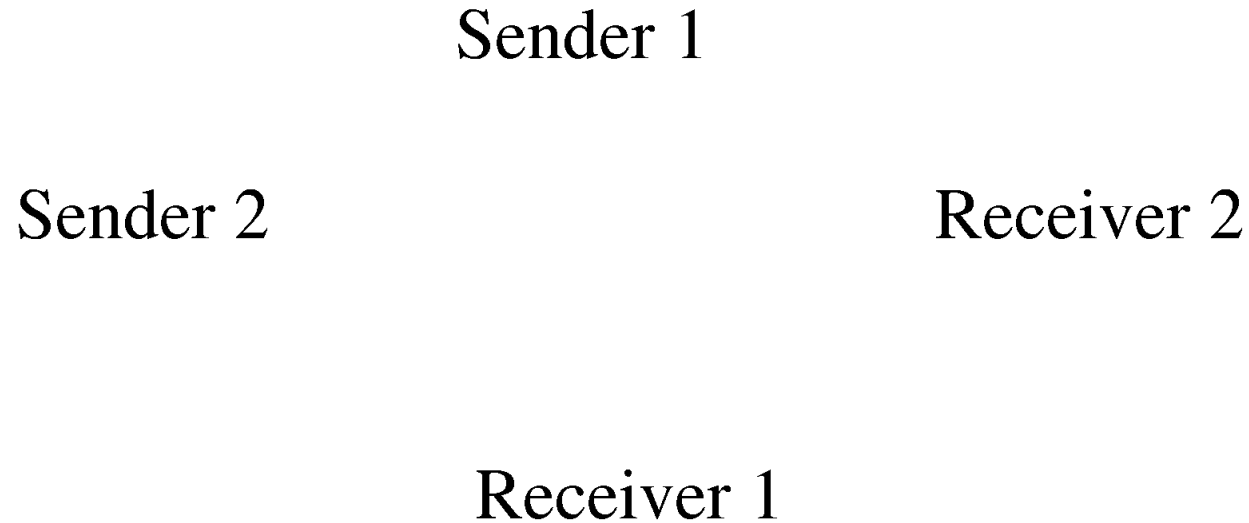
If $n > 2.948t$, and chooses the colors randomly, then m is linear in t .

Detailed proof: see Crypto 2007.

Very rough sketch: We use a state transition diagram and compute eigenvalues to compute 2.948. We then prove that the probability that the resulting coloring is not satisfactory is δ .

4. APPLICATIONS

An obvious application:



However, why use a planar solution in that case?

We use these grids to achieve secure multiparty computation.

What is secure multiparty computation?

Example:

Imagine going to a medical doctor in Iraq who needs to prescribe some medication, which might be counterindicated. The typical solution is to disclose all medical records to the doctor. If secure multiparty computation would be used, the medical doctor in Iraq only learns from the distributed medical databases whether the medication is, or is not, counterindicated.

In most work one maps the function into a Boolean circuit. This makes the solution slow and impractical.

Lately Black Box solutions have been analyzed, e.g., over a Black Box ring. Goal: avoid the mapping to a Boolean circuit.

In our case:

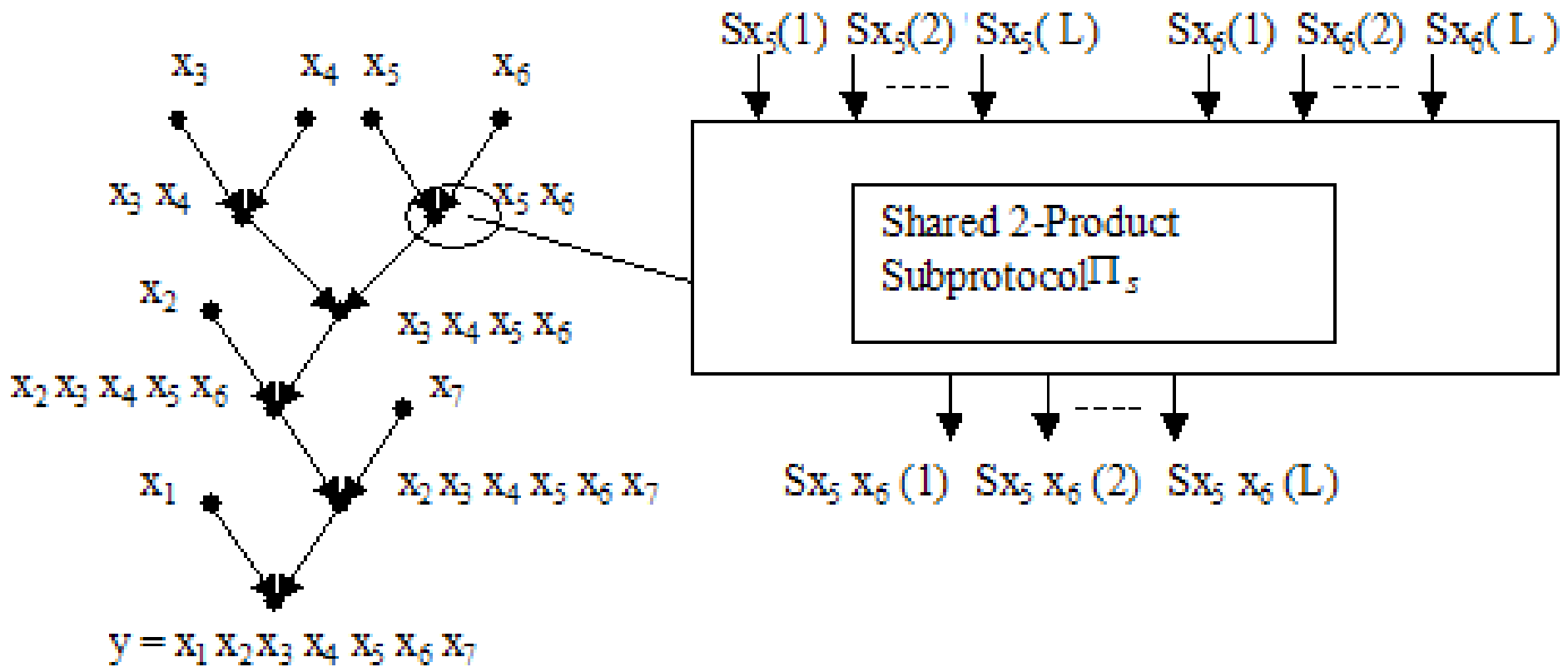
n parties want to compute the product of their secrets without leaking anything that does not follow trivially from the product. We want to protect against t passive eavesdroppers.

Our solution is black box, i.e., independent of the non-abelian group. This has applications to threshold block ciphers and post-quantum cryptography.

5. THE LINK WITH SECURE MULTIPARTY COMPUTATION

Preliminary: from Kushilevitz follows that $n \geq 2t + 1$. This is proven by demonstrating that there is no two-party private protocol to compute the commutator of their secrets, i.e. $x_1^{-1}x_2^{-1}x_1x_2$.

Execution tree: to privately compute $x_1x_2 \cdots x_7$, we proceed as following:



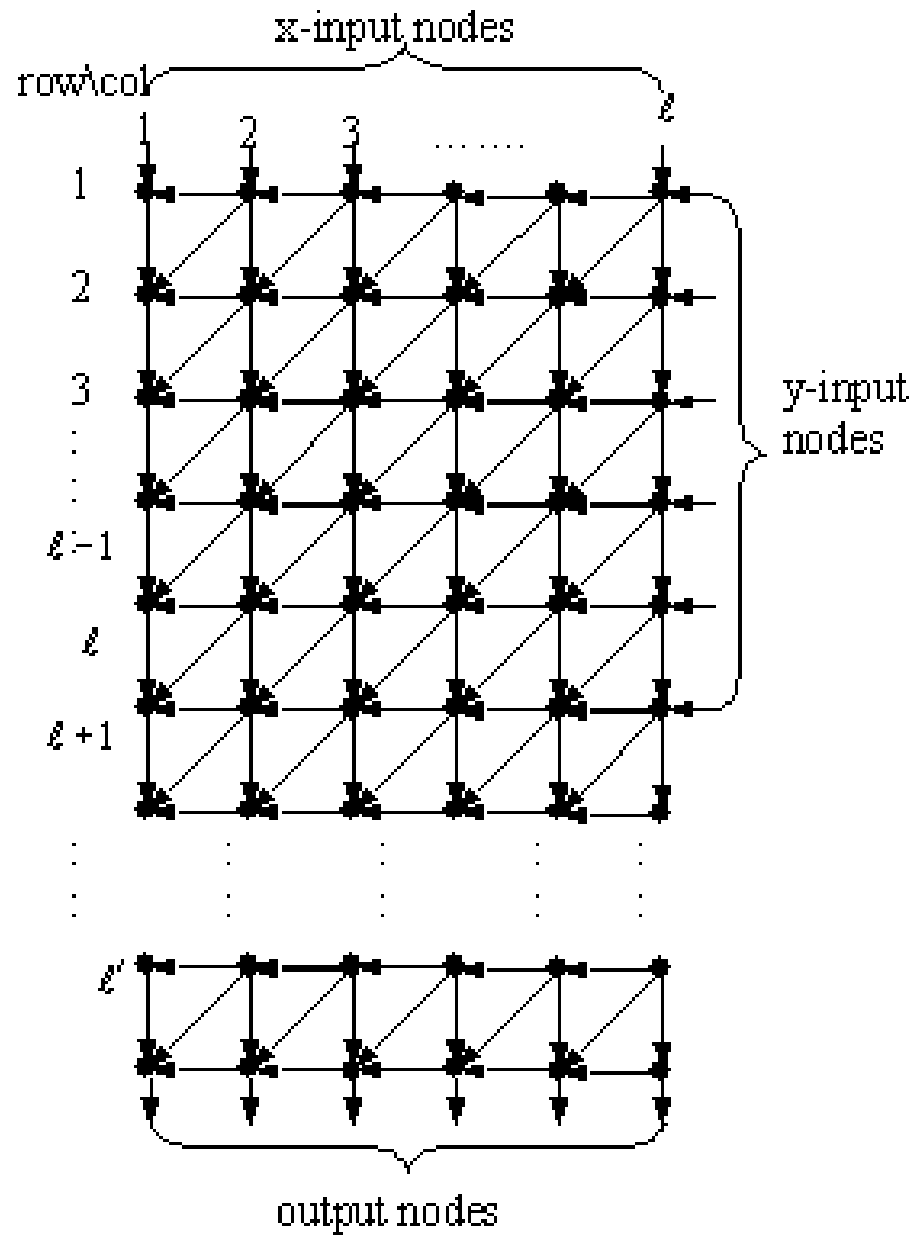
In this execution tree, nodes correspond to the step in the distributed protocol. Moreover, the color of the node indicate which party is doing the corresponding computation.

Tools we use to build the Shared-2 Subprotocol

We use a directed planar graph. **Planar:** non-abelian.

- The x and y inputs are split into m shares.
- Inside the subprotocol, we multiply all inputs and share the outputs using a k -out-of- k secret sharing scheme, where k is the out-degree of the internal node.

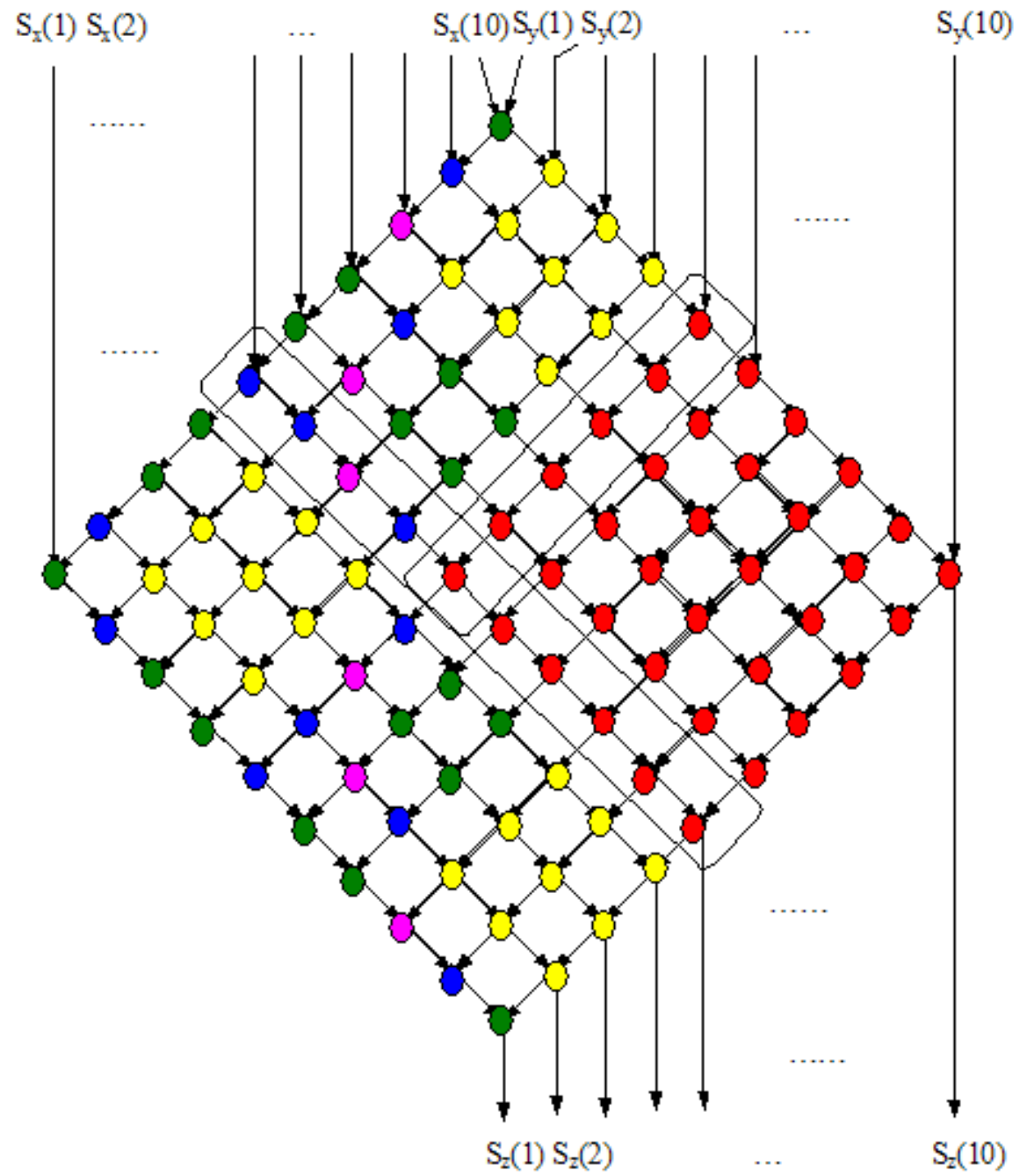
We illustrate this as:



Moreover:

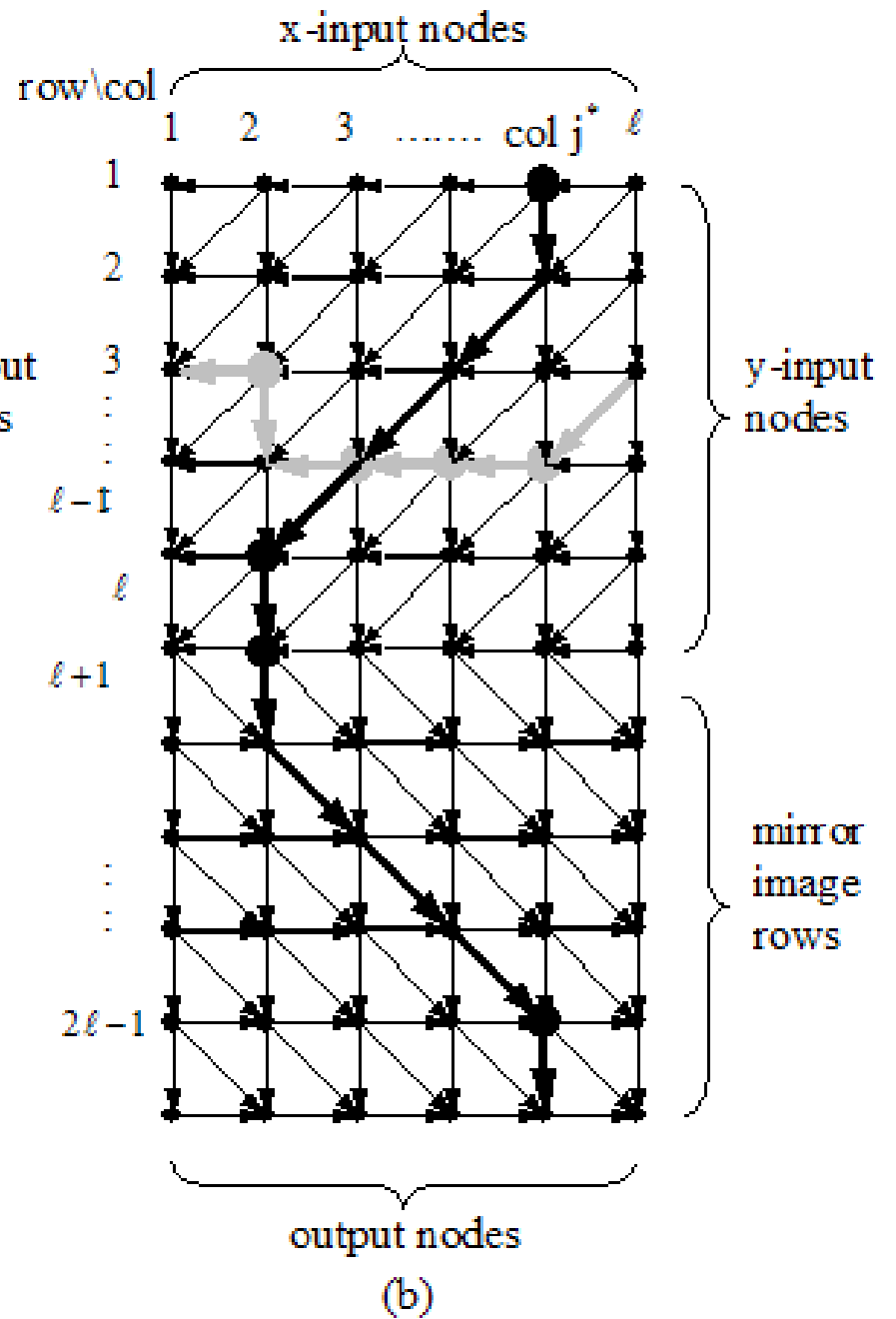
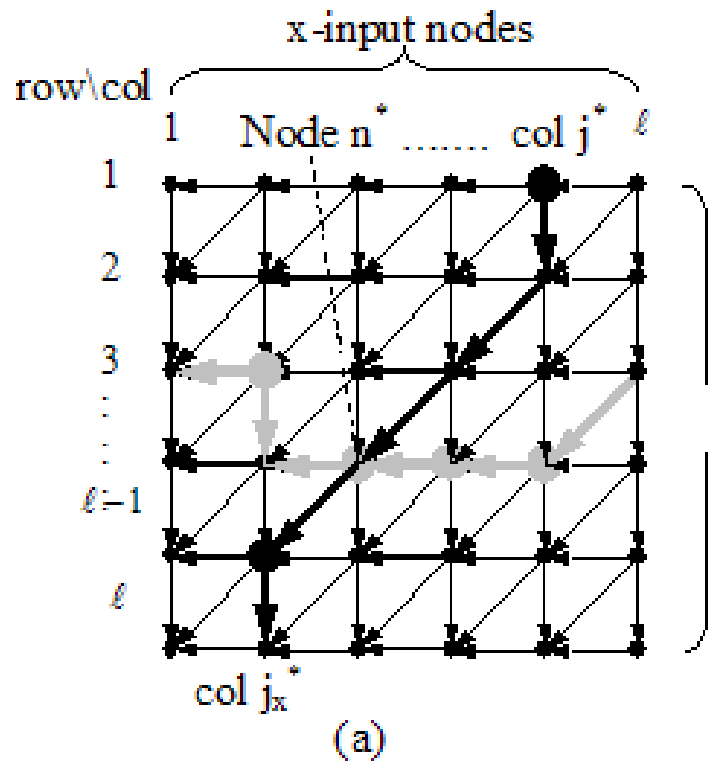
- Using results by Desmedt-Wang-Burmester (2005), the privacy issue to protect against a conspiracy of t parties, corresponds to a communication reliability when t colors are removed.
- the shares of x and the shares of y have to multiply, even if t nodes are “removed”: easy to guarantee for a square solution.

We illustrate this as:



- Since this removal happens in all subprotocols, one must guarantee the complete graph remains connected. This can be achieved by using a “mirror lemma”.

We illustrate this as:



One can formally prove that this implies the privacy condition (see Crypto 2007 proceedings).

Note that although the computation implies a directed planar graph, the conditions on horizontal as well as vertical communication allow to ignore the directed aspect.

6. OPEN PROBLEMS

The work implies several open problems, being, for example:

- Can this be extended to active adversaries?
- For $n = 2t + 1$, is there a polynomial size solution?
- Does the rectangular approach have advantages over the square one?