From Public Key Infrastructures to Secure Multiparty Computation

Yvo Desmedt

The University of Texas at Dallas
USA

and

University College London
UK

September 3, 2013

©Yvo Desmedt

Yvo Desmedt was partially supported by BT as BT Chair of Information Security, NSF ANI-0087641, EPSRC EP/C538285/1, the Australian ARC grants DP0344444 and DP0665035.

Part of this presentation is based on different papers with Mike Burmester, Gregory Kabatianskii Josef Pieprzyk, Ron Steinfeld, Huaxiong Wang and Yongge Wang.

OVERVIEW

1. DigiNotar: our 1996 prediction
2. Our proposal for a reliable PKI
3. Its generalization: Huawei & Schalkwijk's course
4. Secure multiparty computation: introduction
5. A two-dimensional variant
6. New results: a summary
7. Questions
8. More details

1. DIGINOTAR: OUR 1996 PREDICTION



In 1996, we, i.e., Burmester-D-Kabatianskii, (see also Reiter-Stubblebine) were worried about using “networks” with malicious nodes and pointed out that PKIs form a special case, since a PKI can be modeled by a directed graph.

In 2000, Adams-Burmester-D-Reiter-Zimmermann wrote:

hackers breaking into certifying entities

and the Burmester-D IWAP 2001 and CACM 2004 titles of papers were respectively:

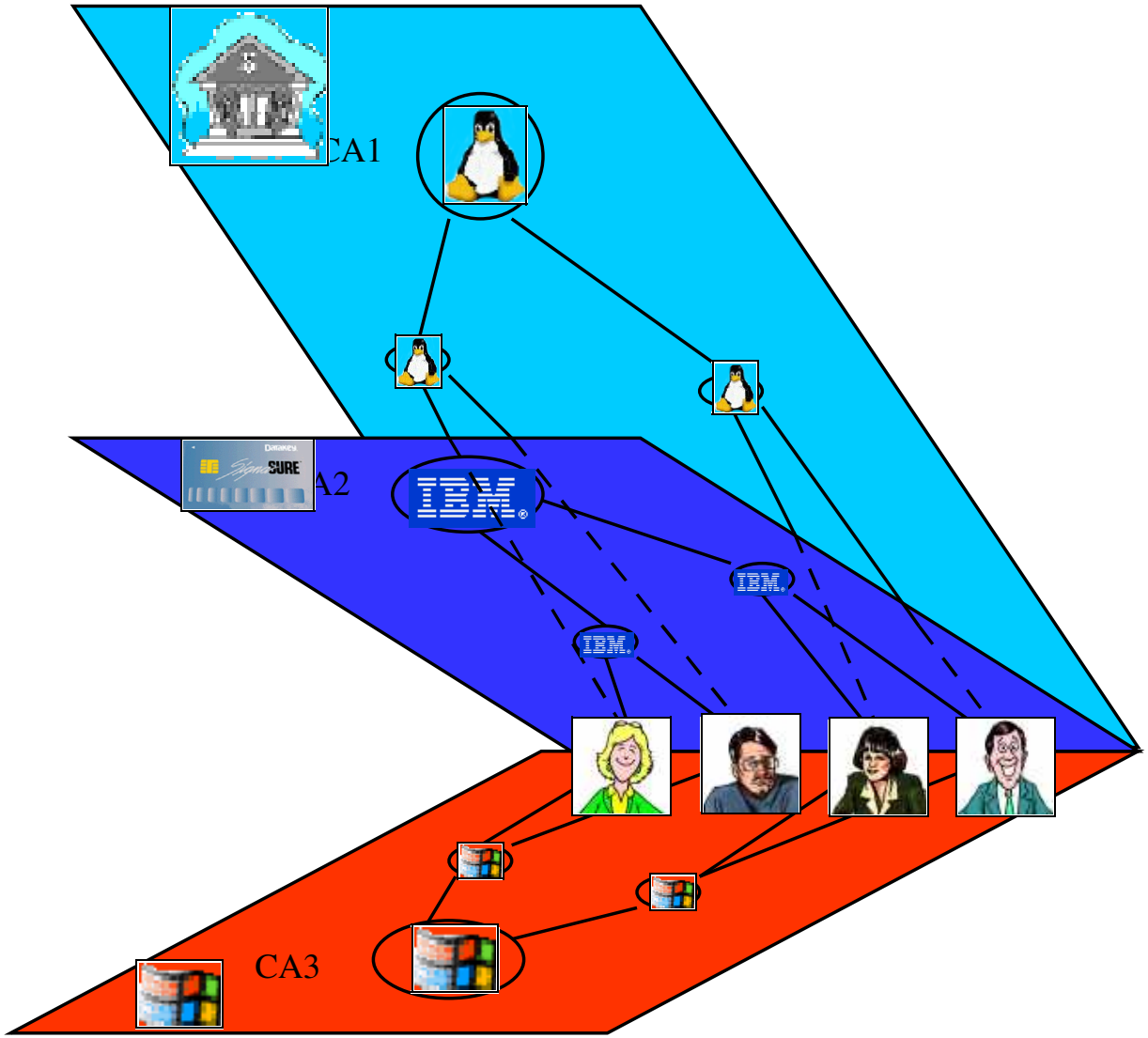
Hierarchical Public-Key Certification: The Next Target for Hackers?

and

Is hierarchical public-key certification the next target for hackers?

2. Our proposal for a reliable PKI

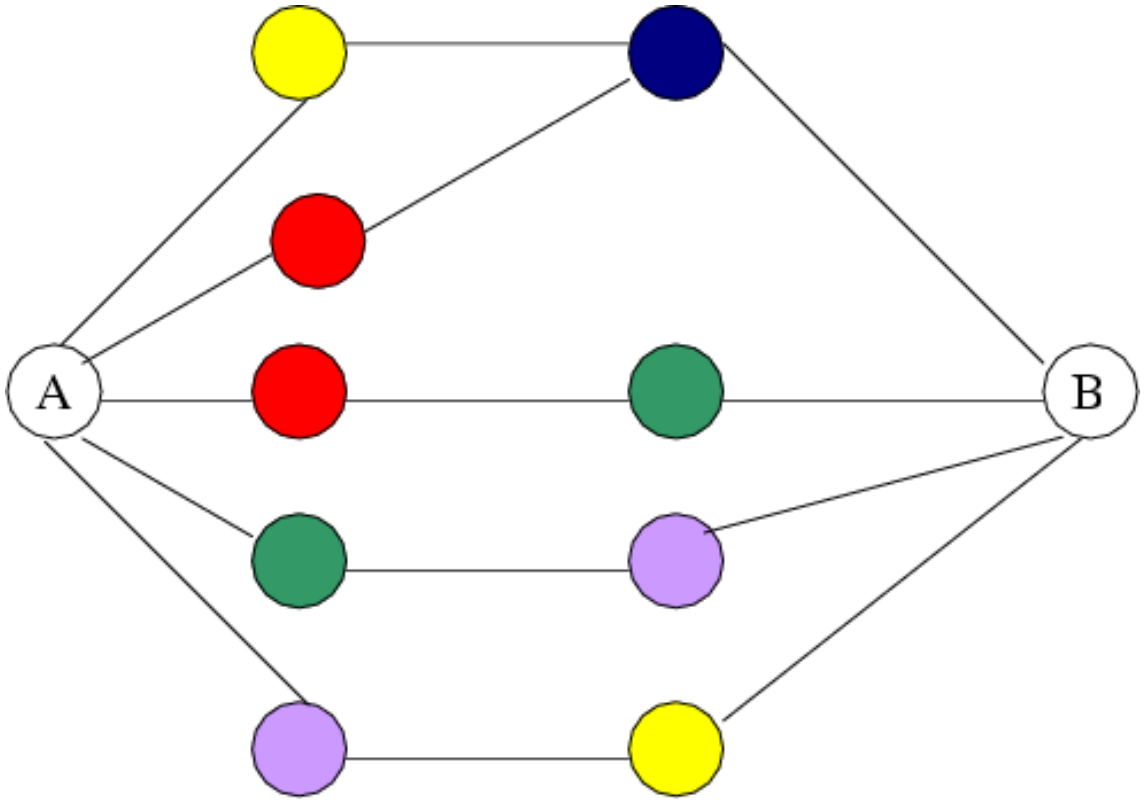
Our CACM 2004 paper had a solution, being:



3. ITS GENERALIZATION: HUAWEI & SCHALKWIJK'S COURSE

Existing PKI's do not necessarily correspond with our last solution!

In general, we wanted to study networks such as:



In 198? Schalkwijk (TU/e) taught a course on Information Theory and Codes, Joos and myself attended. We learned about Reed-Solomon codes (which use Linear Algebra) and Berlekamp-Massey.

In 1993, Dolev-Dwork-Waarts-Yung applied Reed-Solomon codes to achieve reliable and private communication, when the number of nodes the adversary controls are at maximum t. When not allowing interaction, the requirement for the network are to be:

- $2t + 1$-connected for reliability only,
- $3t + 1$-connected for reliability and privacy

As is well known by people in coding theory, when trying to solve a problem, generalizing it may make the problem easier. So, we

(D-Wang-Burmester, 2005) used the notion of general adversary structure.

What is a general adversary structure?

Given a set P (of nodes), one specifies what subsets might behave maliciously. So, as stated earlier:

Example set $P = \{1, 2, 3\}$ and $\mathcal{A}_P = \{\{1\}, \{2, 3\}, \{2\}, \{3\}, \emptyset\}$.
Maximal adversary set: $\mathcal{A}_P^* = \{\{1\}, \{2, 3\}\}$.

In the case the graph is colored and the adversary structure corresponds to an adversary that can choose any t colors and then remove nodes colored by these t colors, we call the adversary structure:

t-color adversary structure.

Applied to communication:

Let A and B be the sender and receiver. Let $Z_1, Z_2, Z_3 \in \Lambda_{V\setminus\{A,B\}}$.

A necessary and sufficient condition for A and B to

- privately and reliably communicate without feedback A, B remain connected when removing any nodes specified by any $Z_1 \cup Z_2 \cup Z_3$
- privately (only) communicate without feedback A, B remain connected when removing any nodes specified by any Z_1.

When in the last case we have a t-color adversary structure, we say A and B are not t-color separable.

Today's importance:

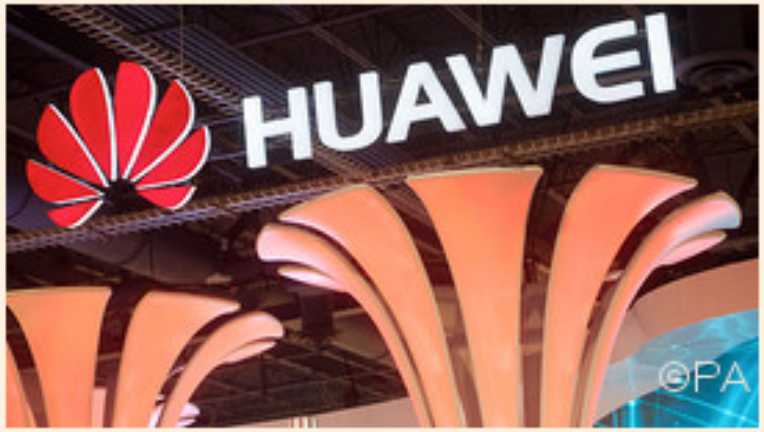
Welcome to FT.com, the global source of business n
analysis. Register now to receive 8 free articles per

Last updated: June 6, 2013 8:04 pm

Share Clip

UK security committee 'shocked' over Huawei contract with BT

By James Blitz and Daniel Thomas



A parliamentary committee has attacked the British government's failure to investigate the use of equipment from China's Huawei in the UK national telecommunications network, saying security issues "risked being overlooked".

EDITOR'S CHO
MARTIN WOLF


The danger of inflation is

4. SECURE MULTIPARTY COMPUTATION: INTRODUCTION

What is secure multiparty computation?

Example:

Imagine going to a medical doctor in Iraq who needs to prescribe some medication, which might be contraindicated. 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, contraindicated.

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.

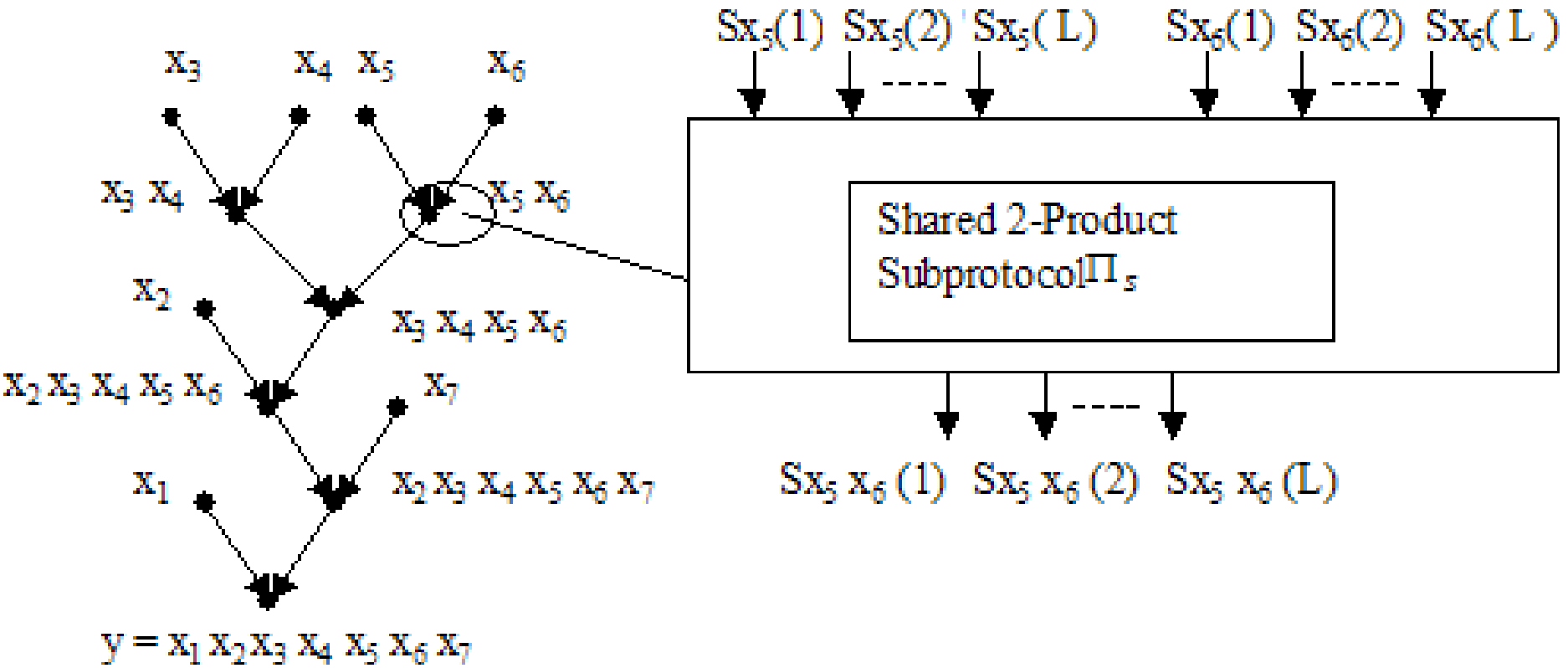
In our case: (D-Pieprzyk-Steinfeld-Wang, 2007)

> 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.

Classical techniques

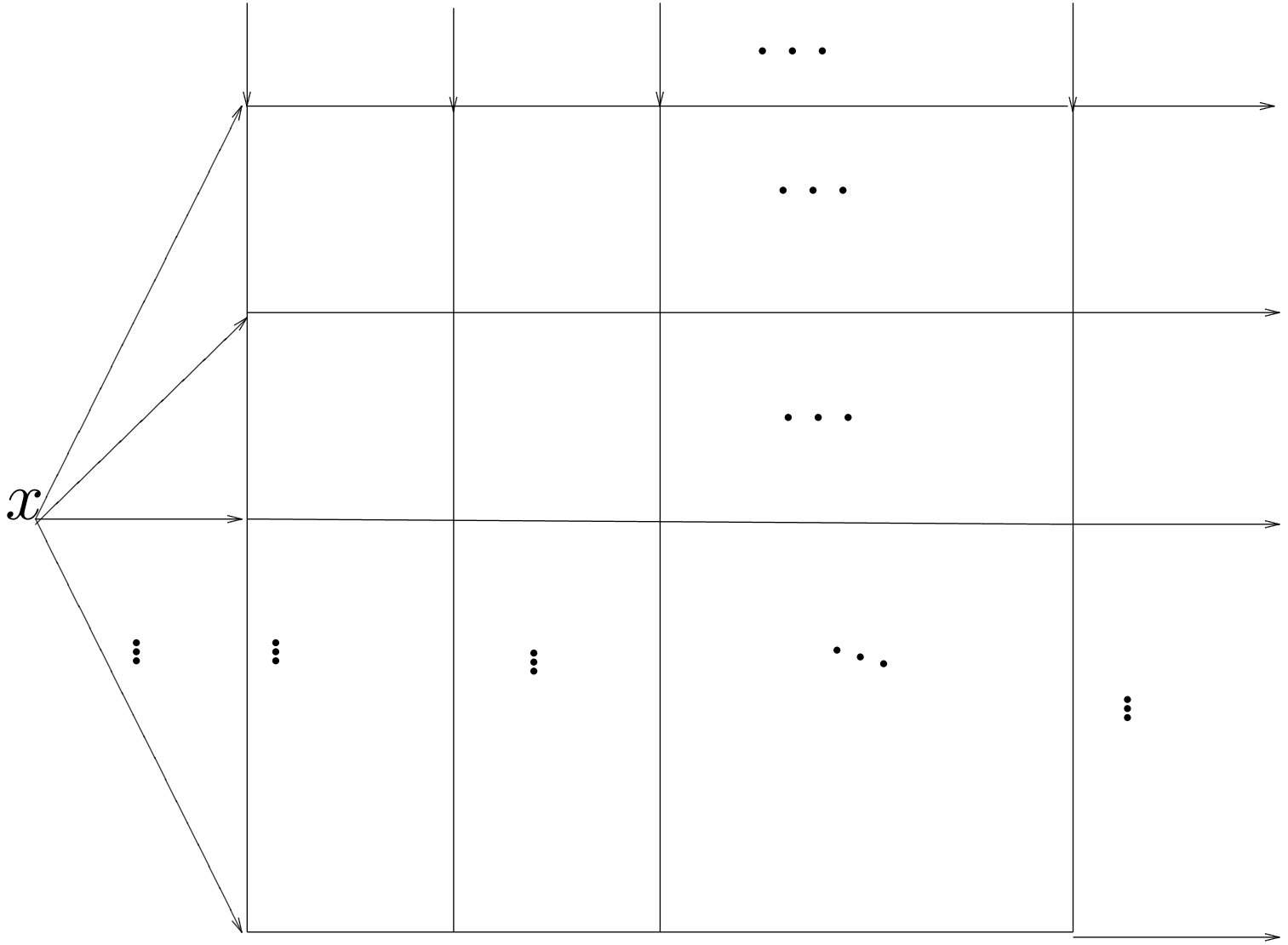
Execution tree: to privately compute $x_1 x_2 \cdots x_7$, we proceed as following:



In this execution tree, nodes correspond to the step in the distributed protocol. The shares coming out of the last "gate" are made public.

5. A TWO-DIMENSIONAL VARIANT

THE SUBPROTOCOL:



WHO COMPUTES WHAT?

To achieve the MPC for our motivation, we used the concept of t-color separable. Nodes in the graph will correspond to parties and we indicate these by colors. We introduced the following problem in graph theory:

Construct a planar vertex color graph $G(V, E)$ with subsets R, R', C, C' of V such that when adding to the graph:

- 4 extra vertices: called $V' = \{v_x, v'_x, v_y, v'_y\}$, which are not colored, and v_x is located above the graph G, v'_x is located below the graph G, v_y is located left of the graph G and v'_y is located right of the graph G,

- edges $E_x = \{(v_x, v) \mid \text{for each } v \in R\}$,

- edges $E'_x = \{(v, v'_x) \mid \text{for each } v \in R'\}$,
- edges $E_y = \{(v_y, v) \mid \text{for each } v \in C\}$,
- edges $E'_y = \{(v, v'_y) \mid \text{for each } v' \in C'\}$,

such that:

- $G'(V \cup V', E \cup E_x \cup E'_x \cup E_y \cup E'_y)$ is planar, and
- v_y and v'_y are not t-color separable in $G_H(V_H, E_H)$, where $V_H = V \cup \{v_y, v'_y\}$ and $E_H = E \cup E_y \cup E'_y$, and
- v_x and v'_x are not t-color separable in $G_V(V_V, E_V)$, where $V_V = V \cup \{v_x, v'_x\}$ and $E_V = E \cup E_x \cup E'_x$

We call such a graph an t-reliable n-coloring admissible planar graph.

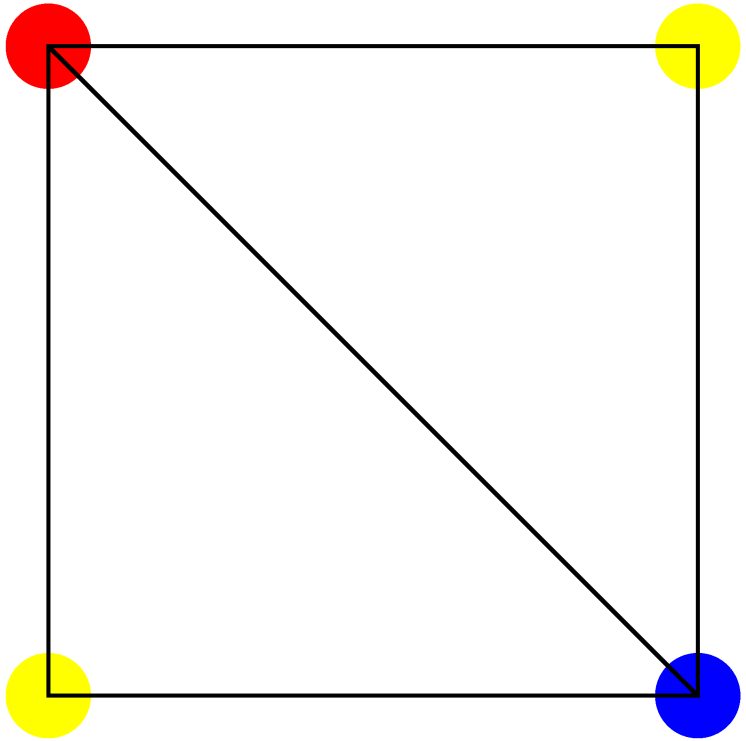


©Yvo Desmedt

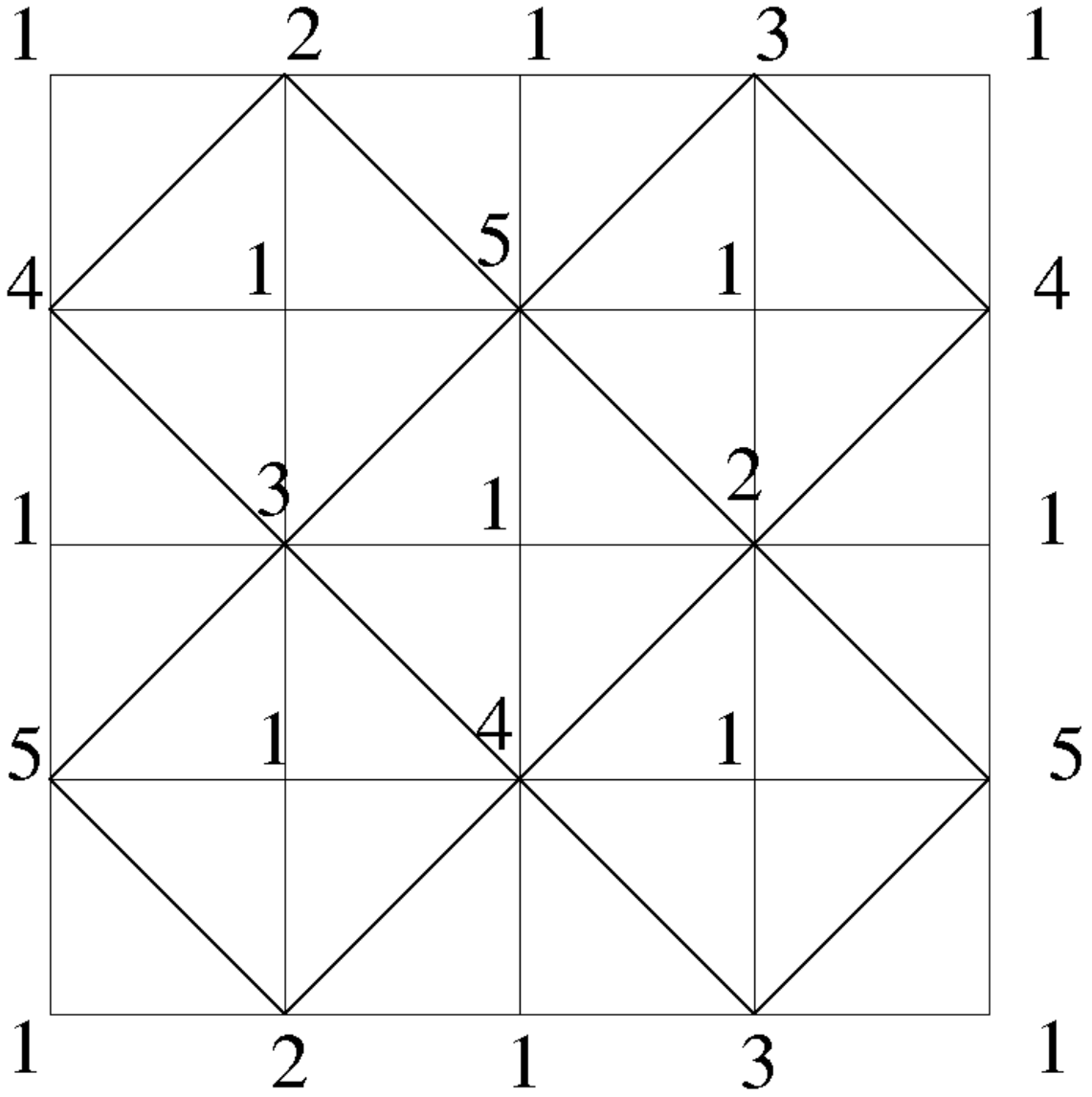


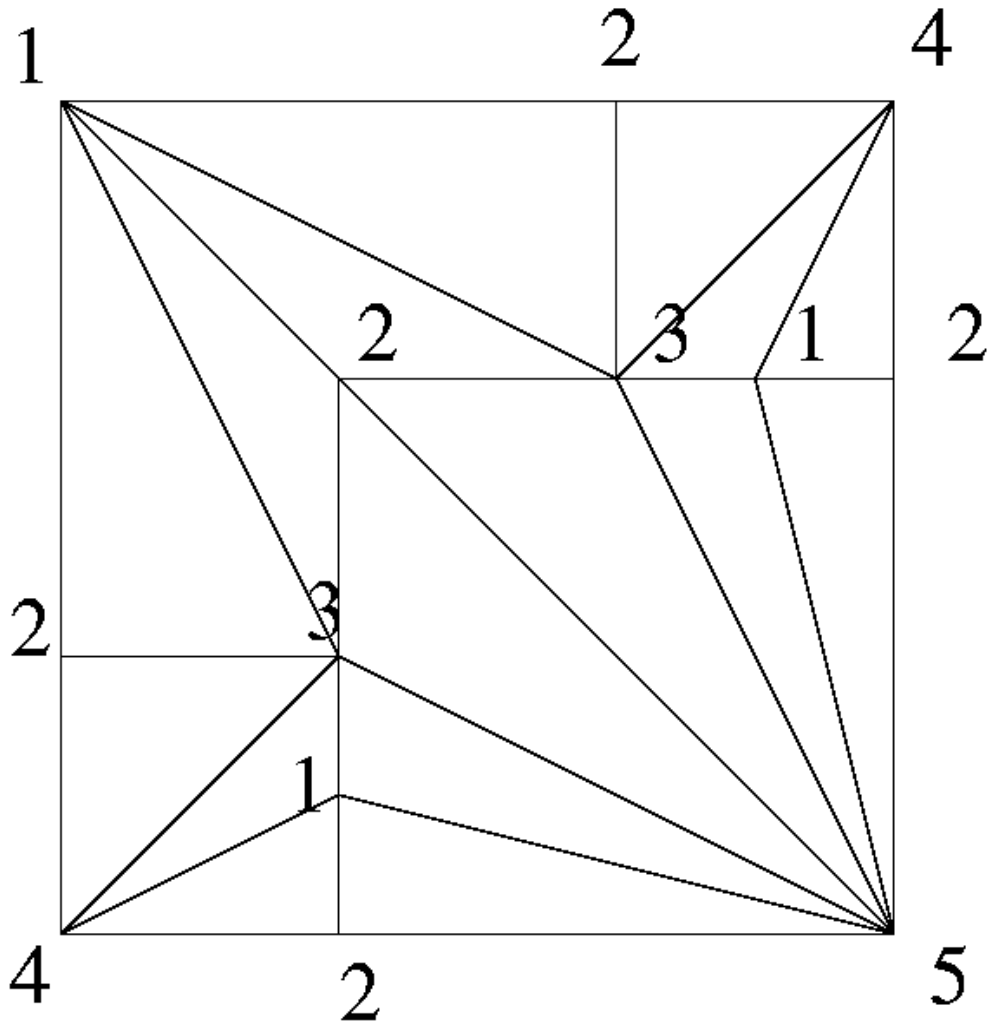
Some examples:

$t = 1$ and $n = 3$

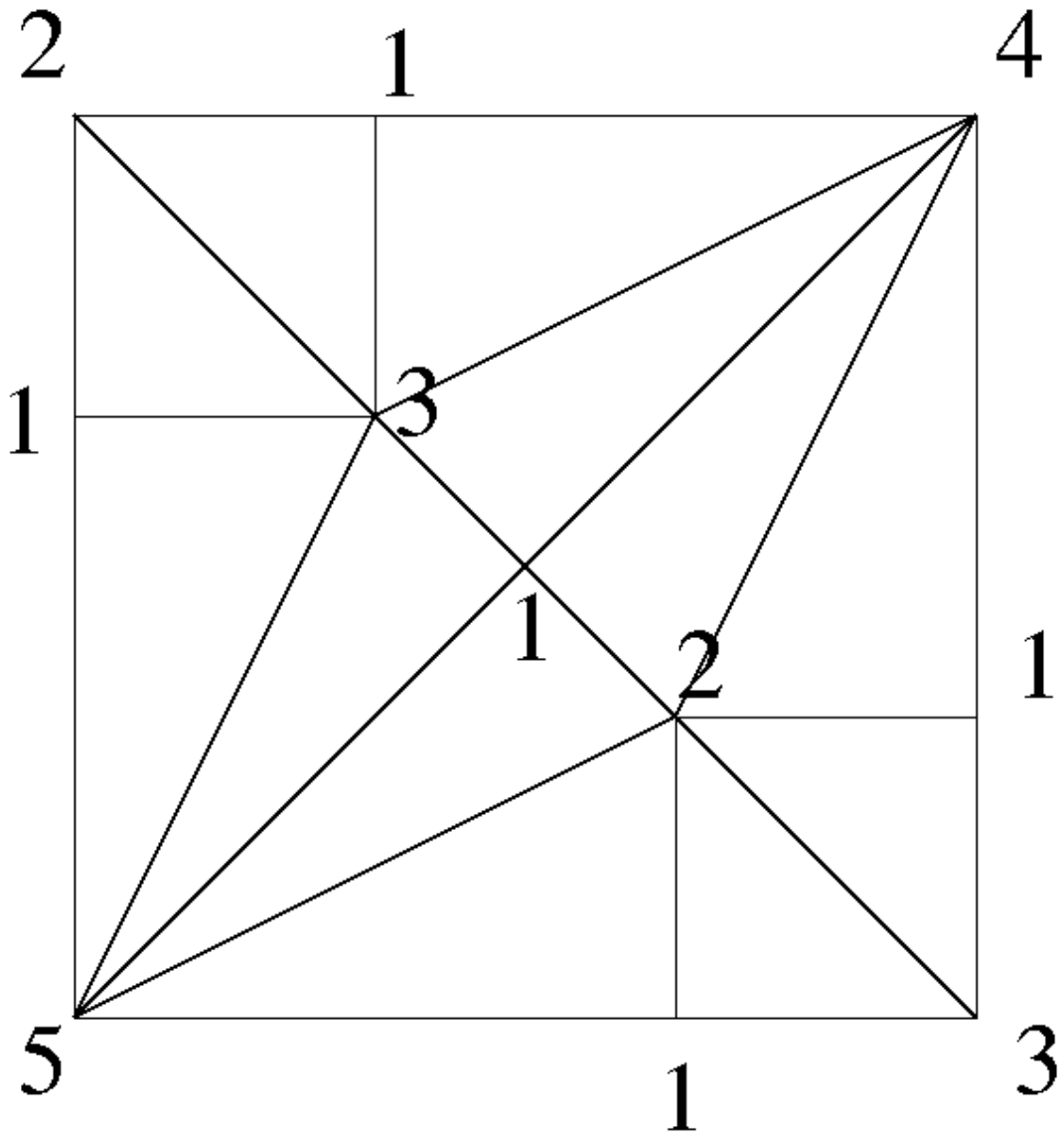


$t = 2$ and $n = 5$



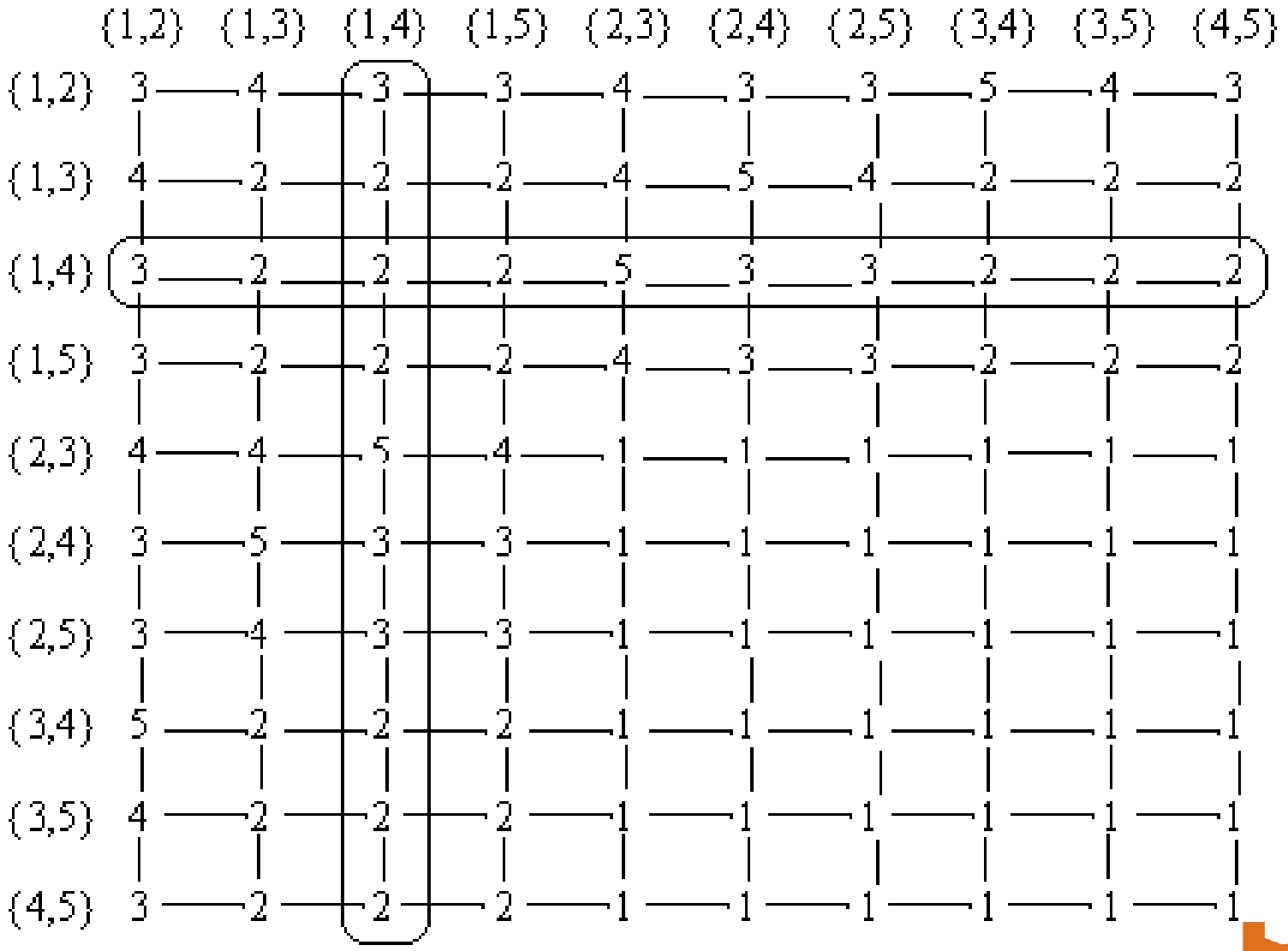

1
2
4
2
3
1
2
2
3
1
4
2
5

$t = 2$ and $n = 5$: less nodes (new)

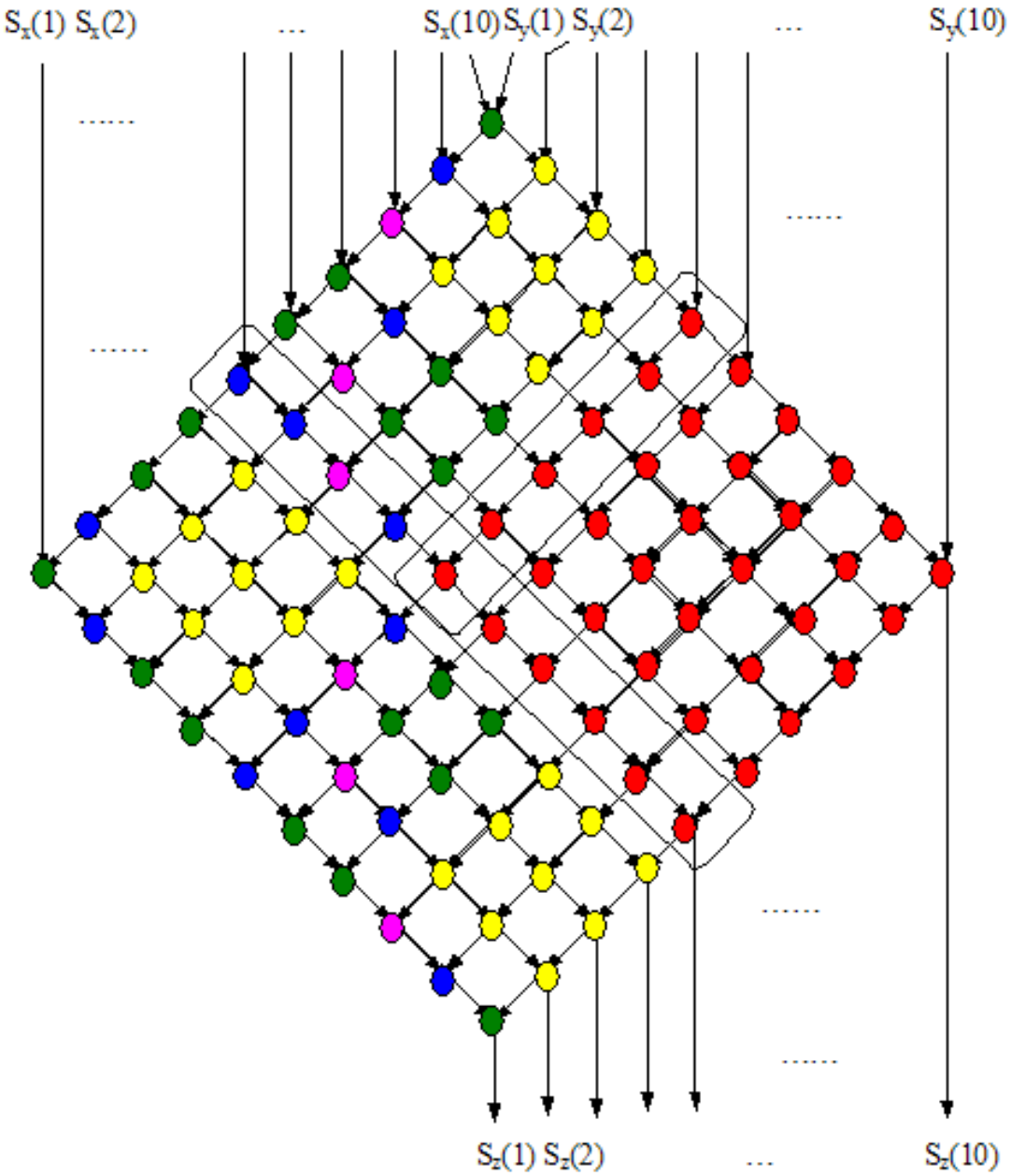


Any t, $n = 2t + 1$

We use an example to illustrate:



Another way to view it:



6. NEW RESULTS: A SUMMARY

More optimal graphs were constructed by Sun-Yao-Tartary (2008), see also D-Pieprzyk-Steinfeld-Sun-Tartary-Wang-Yao (2012).

The active case was addressed by D-Pieprzyk-Steinfeld (2012).

A different approach was used at Crypto 2013 by Cohen et al.

7. QUESTIONS

Questions

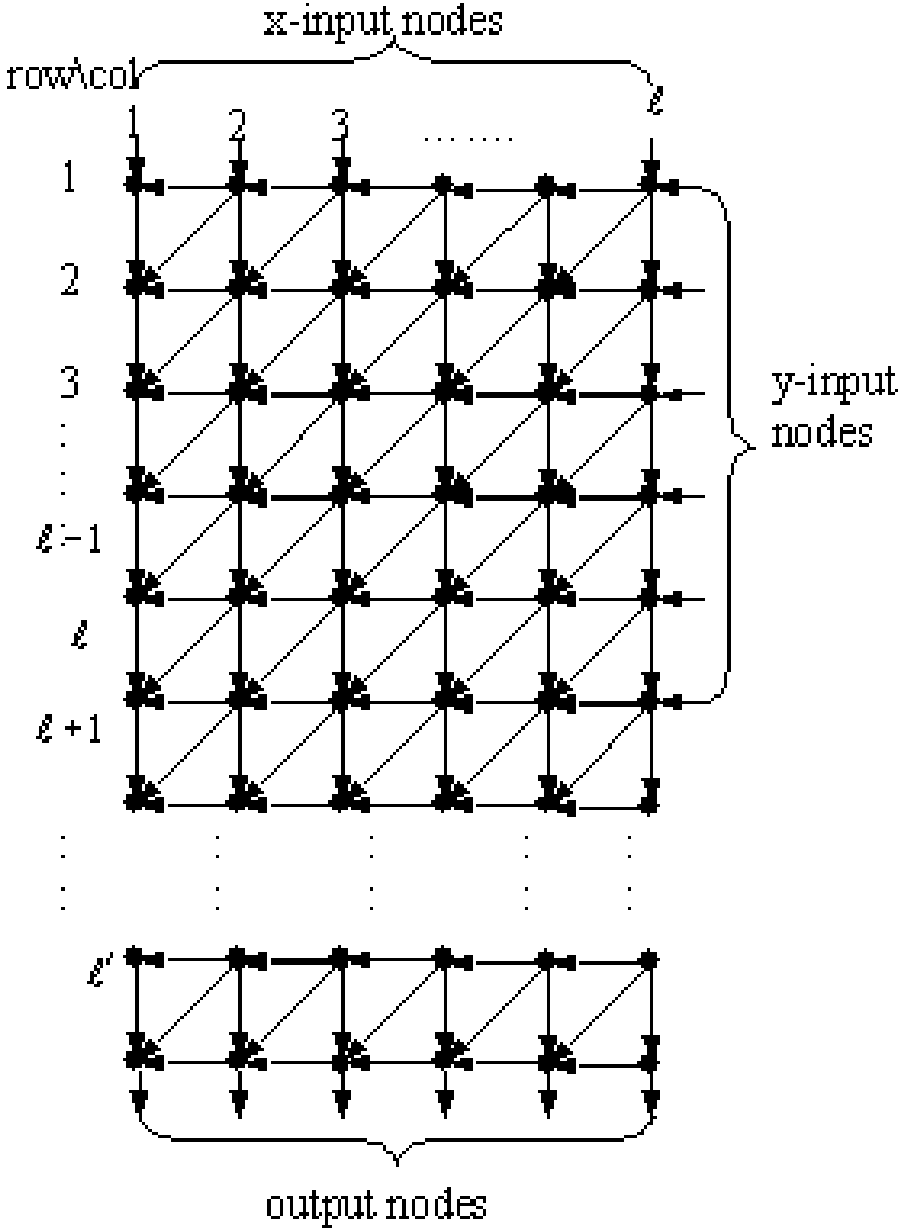
8. MORE DETAILS

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:

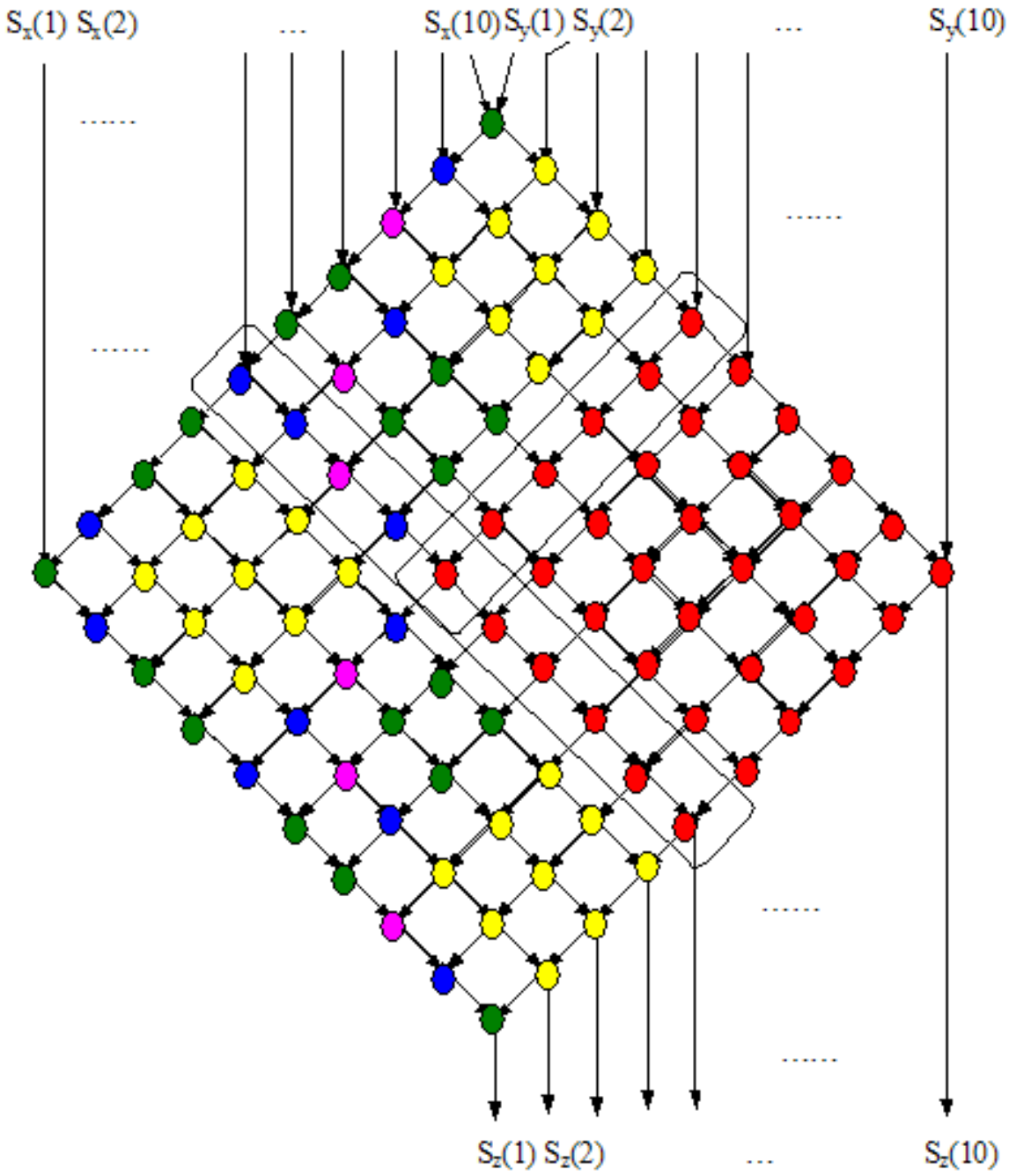

x-input nodes
row\col
1
2
3
ℓ
1
2
3
ℓ-1
ℓ
ℓ+1
ℓ'
y-input nodes
output nodes

Moreover:

- Using results by Desmedt-Wang-Burmester (2005) (generalizing Franklin-Yung (1995, 2004)) the privacy issue to protect against a conspiracy of t parties, corresponds to a communication problem in which when t colors are removed, one can still communicate.

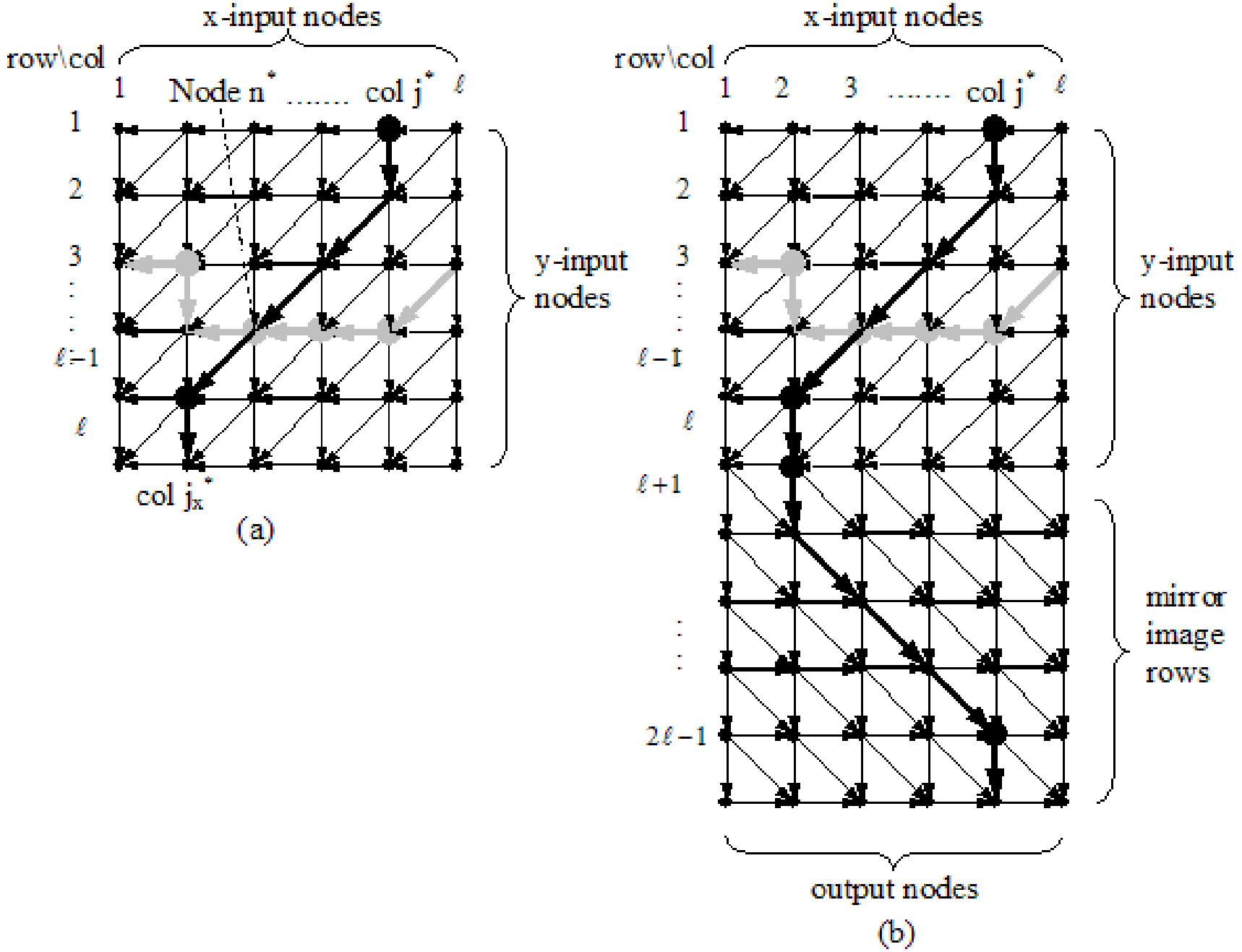
- the shares of x and the shares of y have to multiply, even if t nodes are "removed": easy to guarantee for a square solution.

We illustrate this as:


$S_x(1)$ $S_x(2)$ … $S_x(10)$ $S_y(1)$ $S_y(2)$ … $S_y(10)$
$S_z(1)$ $S_z(2)$ … $S_z(10)$

- 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:


x-input nodes
row\col
1
Node n*
col j*
ℓ
1
2
3
ℓ−1
ℓ
y-input nodes
col jx*
(a)
x-input nodes
row\col
1
2
3
col j*
ℓ
1
2
3
ℓ−1
ℓ
ℓ+1
2ℓ−1
y-input nodes
mirror image rows
output nodes
(b)

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.

How where the small t cases constructed?

For example, the solution for $t = 1$ was created from the exponential solution as follows.

Consider the "exponential" solution for $t = 1$:

	$\{1\}$	$\{2\}$	$\{3\}$
$\{1\}$	2 or 3	3	2
$\{2\}$	3	1 or 3	1
$\{3\}$	2	1	1 or 2

Now make appropriate choices where possible, giving e.g.:

	$\{1\}$	$\{2\}$	$\{3\}$
$\{1\}$	3	3	2
$\{2\}$	3	3	1
$\{3\}$	2	1	1

Merging nodes that have the same label into single nodes and calling the labels colors we obtain:

