

Nanotechnology Based Optical Computing and its Cryptographic Application

Eyal Cohen

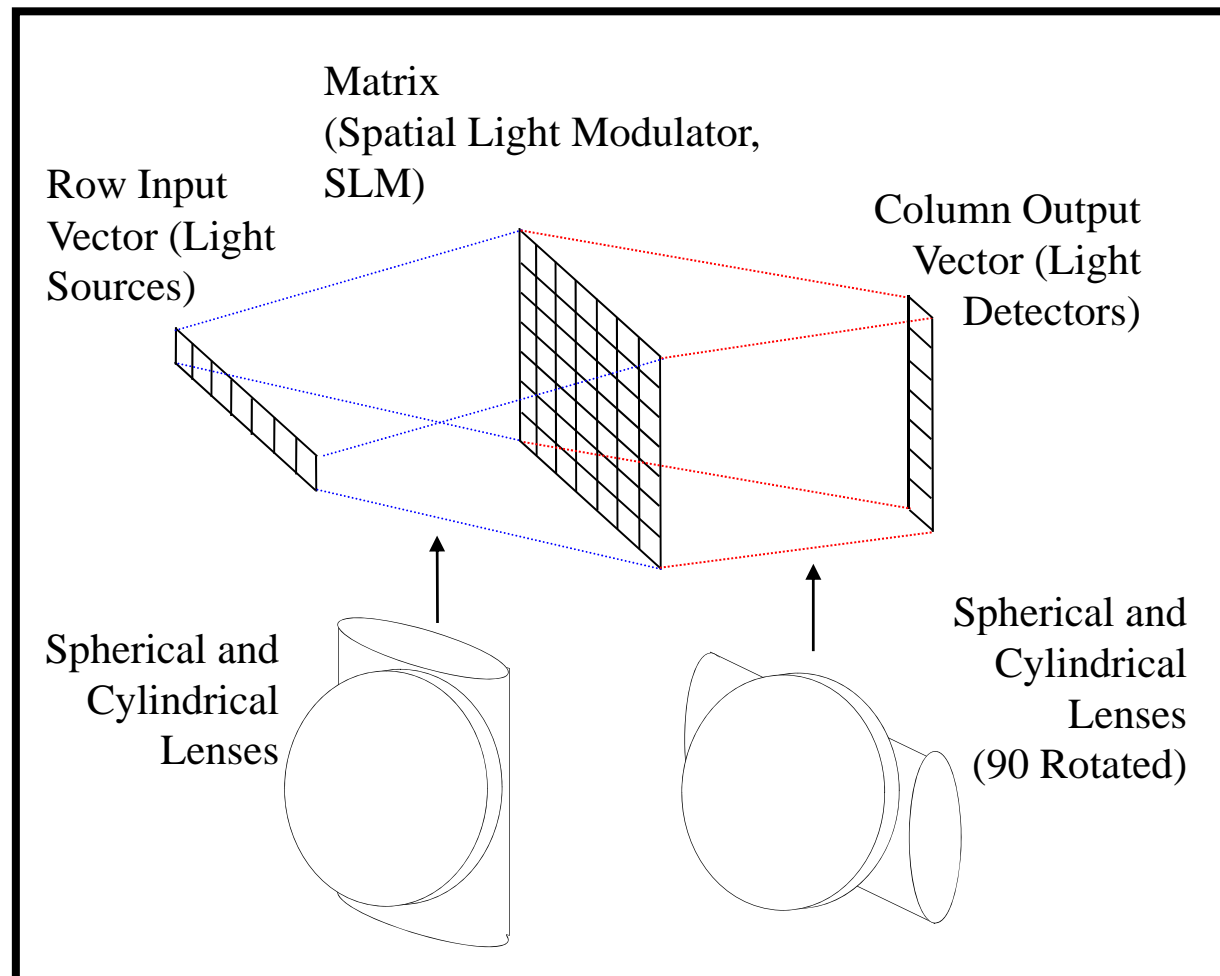
Shlomi Dolev, Sergey Frenkel, Rami Puzis,
Michael Rosenblit
BGU

Objectives

- NP problems
 - Polynomial pre-processing
 - Mask-copying using Lithography
 - e.g. Hamiltonian-Cycle, TSP...
- Microscopic using nano-technology
- Solving larger instances
- Applications:
Unidirectional Encryption problem...

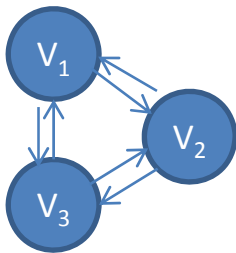
Previous work

- Stanford Optical VMM

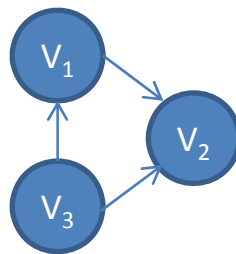


Hamiltonian cycle

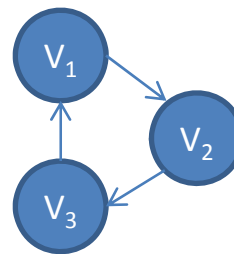
- A closed route that passes through all vertices only once.
- # of vertices, $n=3$



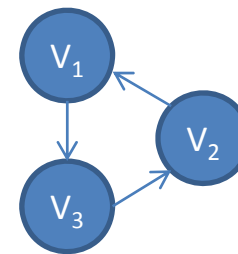
Full Graph



Impossible
Cycle



Clockwise



Counter-Clockwise

of edges, $n(n-1)$

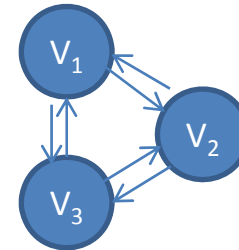
of possible routes, $(n-1)!$

Hamiltonian Cycle

- Binary Matrix, $n=3$

e_{12}	e_{13}	e_{21}	e_{23}	e_{31}	e_{32}
1	0	0	1	1	0
0	1	1	0	0	1

$n=3$



Each column represents an edge.

Each row represents a possible cycle.

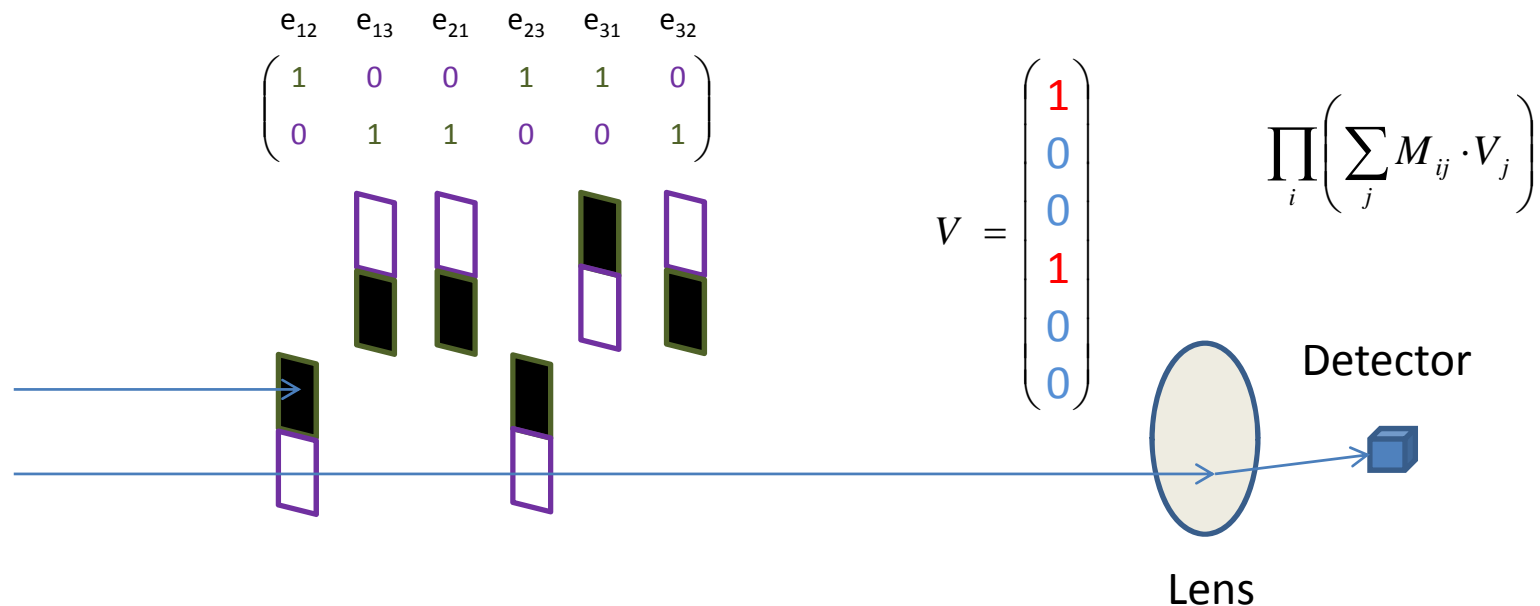
If an edge is part of a possible cycle the cell value is 1.

If an edge is **not** part of a possible cycle the cell value is 0.

The Architecture

If a matrix element is 1, the corresponding mask pixel is **opaque**.

If a vector element is 0, the corresponding mask pixel is **transparent**.



If a vector element is 1, the corresponding mask participates.

If a vector element is 0, the corresponding mask does not participate.

Creating Masks

Initial Matrix, $n=3$

e_{12}	e_{13}	e_{21}	e_{23}	e_{31}	e_{32}
1	0	0	1	1	0
0	1	1	0	0	1

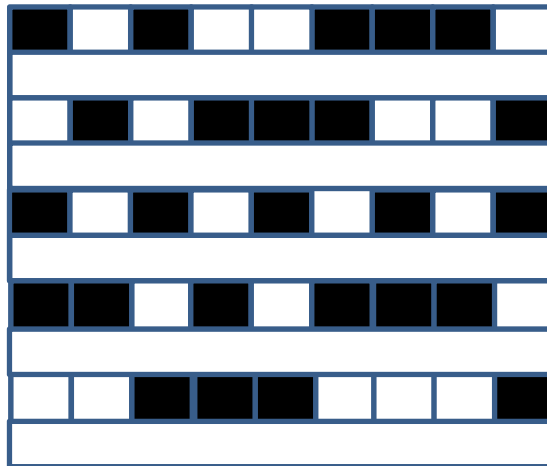
Extended Matrix, $n=4$

e_{12}	e_{13}	e_{14}	e_{21}	e_{23}	e_{24}	e_{31}	e_{32}	e_{34}	e_{41}	e_{42}	e_{43}
1	0	0	0	1	0	0	0	1	1	0	0
1	0	0	0	0	1	1	0	0	0	0	1
0	1	0	0	0	1	0	1	0	1	0	0
0	1	0	1	0	0	0	0	1	0	1	0
0	0	1	1	0	0	0	1	0	0	0	1
0	0	1	0	1	0	1	0	0	0	1	0

Lithography- copying an entire block at once
Trading space with time

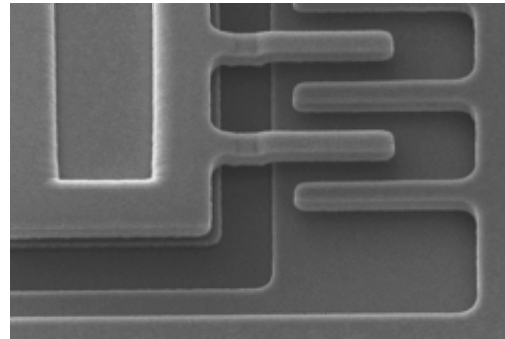
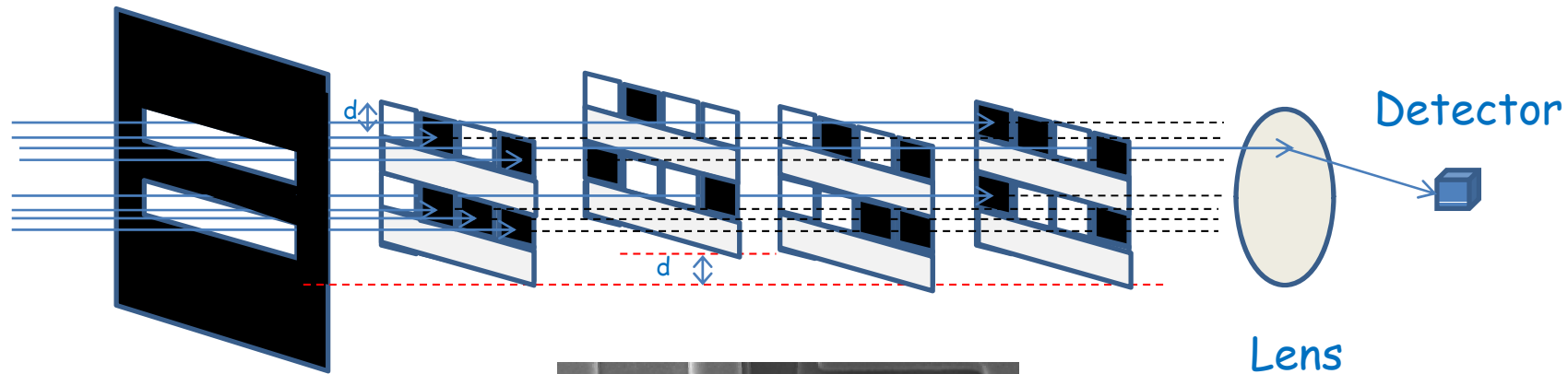
Microarchitecture

- Changing the mask to fit a microarchitecture



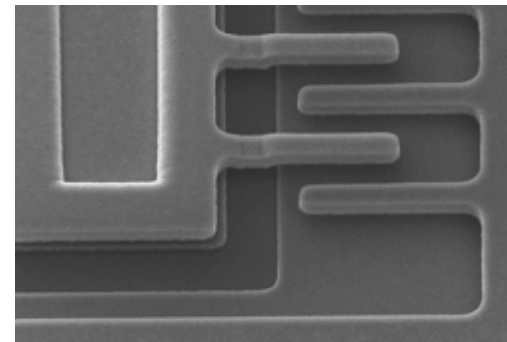
Microarchitecture

- Using MEMS as Actuators



Methods

- Using MEMS
- Diffraction limit:
 - Monolithic structure
 - Near Field
 - Higher frequency



Conclusions

- Masks Copying using Lithography.
 - Trades space with time.
- Complexity of creating **Factorial** sized Mask is **Polynomial** in time.
- Microarchitectures are preferable in cases where the instance is large.