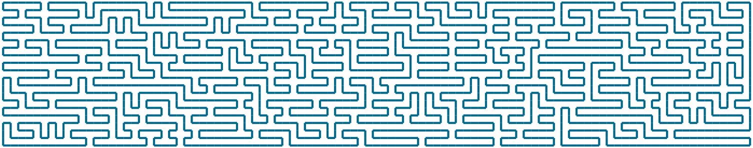
3D Hardware Canaries

Jean-Michel Cioranesco

Paris 2 University Université Panthéon-Assas *and Altis Semiconductor* Altis

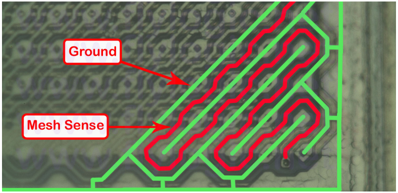
Common work with: Sébastien Briais, Stéphane Caron, Jean-Luc Danger, Sylvain Guilley, Jacques-Henri Jourdan, Arthur Milchior, David Naccache, Thibault Porteboeuf



NEEDS OF 3D INTEGRATION

- 3D integration is currently seen as the future of chip manufacturing.
- 3D integration opens new opportunities for implementing physical chip protections.
- In particular creating active shields for an entire chip stack, and not only the topmost die. Such shields might protect against a wider range of attacks than conventional active shields.

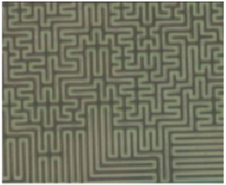
STATE OF THE ART



ST Microelectronics active shield in ST16 smartcard:

- active shield pattern that carries supply voltage
- hacked without the use of FIB on 0,18μ technology

(Photo's courtesy of C.Tarnovsky)



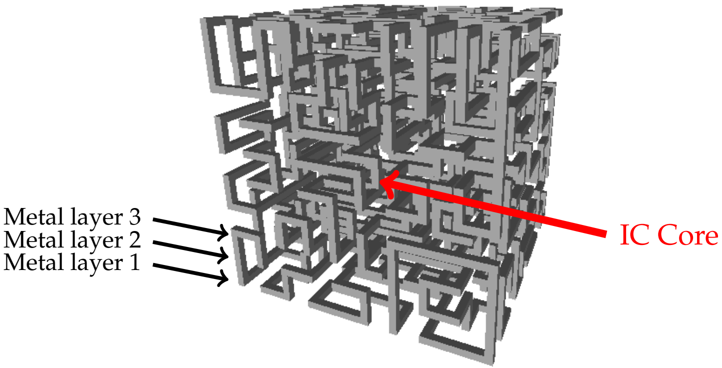
Atmel active shield in a ATSHA 204 chip:

- full serpentine over the entire chip
- active shield patterns detects disconnections and short circuits
- no probe points or test pads

(Photo's courtesy of www.digikey.com)

OUR IDEA

- Build a Hamiltonian mesh to completely surround the protected chip.
- Cage spread on several metal layers and/or dies.
- Vertical connections are made using via.

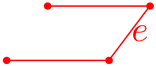


TOOLBOX FOR GENERATING HAMILTONIAN STRUCTURES

- We investigated several Hamiltonian path generators, using different approaches.
- Looking for a trade-off between computation time and randomness.
- Our algorithms can be extended to generate several interleaved Hamiltonian circuits.

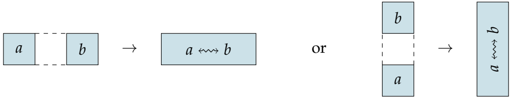
STRETCHING ALGORITHM

- This algorithm maintains and extends a set of edges in one of the four possible extension directions.
- If the algorithm doesn't find an available extension, then it resumes the search.
- The algorithm is very slow, 30 hours for generating a cube of size 8 on a server.

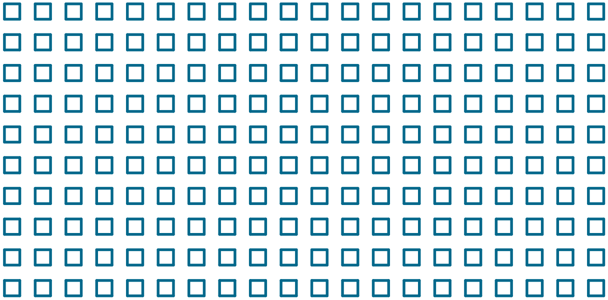


SQUARE ASSOCIATION

- Two elementary squares can be associated in only two ways

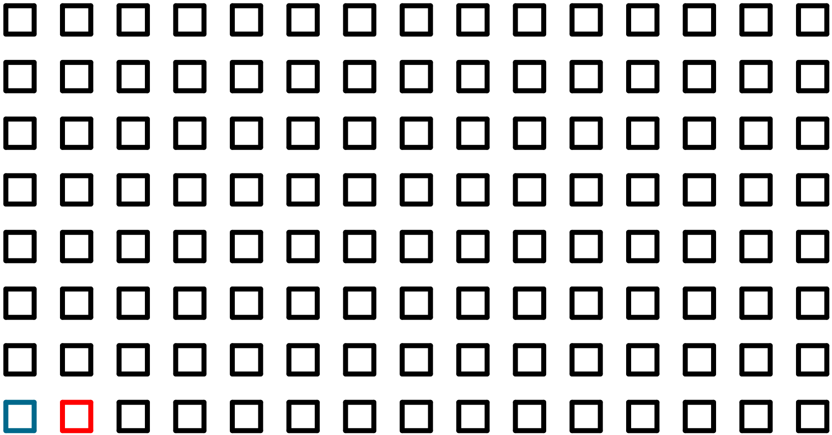


- We map the plan with elementary squares and associate them randomly until one single Hamiltonian path is obtained



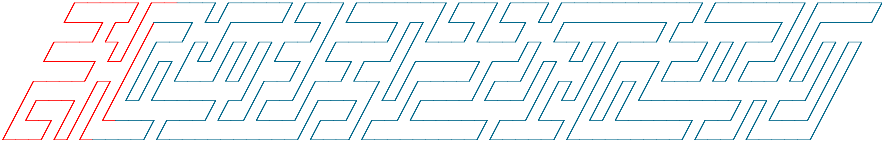
MORE THAN ONE PATH

In the same way we can create several Hamiltonian paths interleaved on a unique metal layer in the interest of cost.



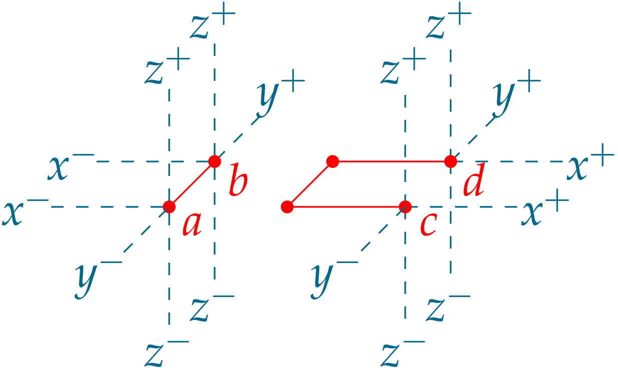
From 2D to 3D Structures

- We can now fold a planar structure as we would fold a sheet of paper.
- With a regular folding we obtain a predictable shape. However, more technical folding techniques result in more intricate 3D structures.



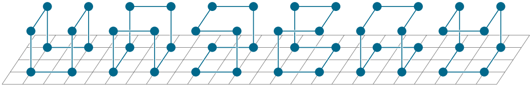
Randomizing

Folding a planar structure, even randomly, creates regular and hence predictable structures. We randomize the resulting structure using a 3D rewriting rule.

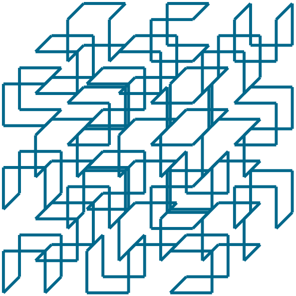


Cube association

- There are six different elementary Hamiltonian cubes

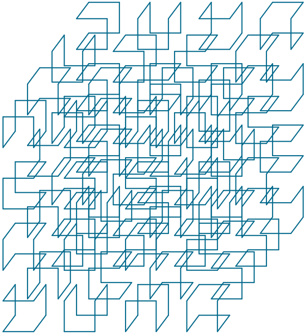


- Fill the volume to cover with randomly picked elementary cubes

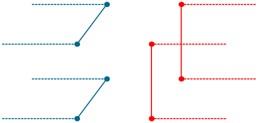


CUBE ASSOCIATION

- Associate randomly the elementary cubes (two by two) until a single Hamiltonian cycle is obtained

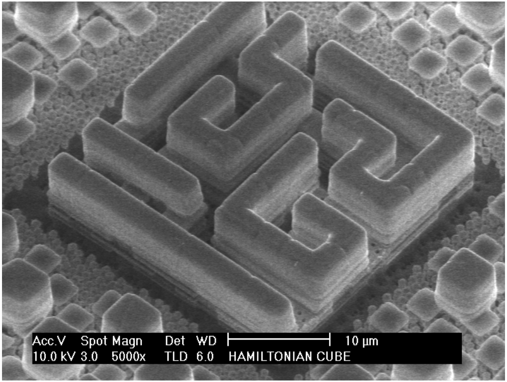


- Another association rule



SILICON EXPERIMENTS

We made a silicon prototype to illustrate the idea, a cage covering an 8-bit register. The cage stretches over six metal layers on a 130nm technology.



INTEGRATION INTO DESIGN TOOLS

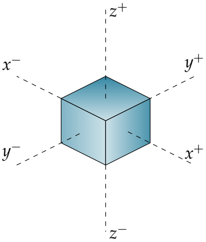
- Our prototype layout was "handmade", this limited us to a certain size.
- Our lightweight algorithms can be integrated within a design environment to automate the active shield's layout generation.
- The shield has to comply with manufacturing constraints regarding metal line spacing and minimal metal line width.

FROM PASSIVE TO DYNAMIC SHIELDING

- If mesh geometries are predictable, attacks (strapping) become easier.
- Digital signal transmission provides a way of ensuring shield integrity.
- Re-routing dynamically a logic signal between switch-boxes allows the creating of a unique cryptographic response per configuration.
- Our shield purpose is to warn the protected circuit of any attack, in same way canaries were used in coal mines to detect poisonous gazes.

THE CANARY SWITCH-BOXES

- A network made of subtrate-level switch-boxes forming a cage surrounding the protected chip.
- Each switch-box has programmable routing and cryptographic capabilities that make the network dynamic.
- The network acts as a verification circuit creating different cryptographic responses for different inputs.



signal output

signal input

$w_i \searrow$	x^+	x^-	y^+	y^-	z^+	z^-
x^+	–	00	01	02	03	04
x^-	10	–	05	06	07	08
y^+	11	15	–	09	0A	0B
y^-	12	16	19	–	0C	0D
z^+	13	17	1A	1C	–	0E
z^-	14	18	1B	1D	1E	–

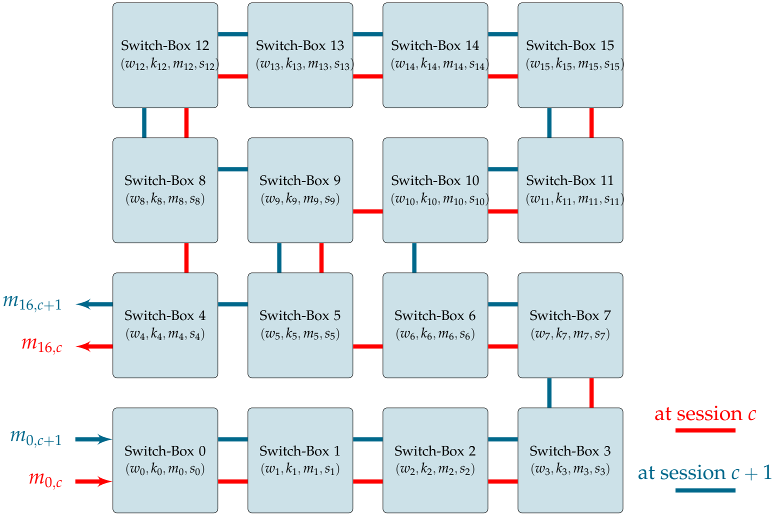
SWITCH-BOX FUNCTIONS

- Several cell-level parameters are used to define each switch-box: A coordinate identifier i, a session identifier c, a key k_i, a routing configuration w_i and a state variable $s_{i,c}$, computed and stored at each clock cycle from the incoming data $m_{i,c}$ and the preceding state $s_{i,c-1}$.

$$\begin{cases} m_{i+1,c} & = & F(m_{i,c}, k_i, w_{i,c}, s_{i,c}) \\ s_{i,c+1} & = & G(m_{i,c}, k_i, w_{i,c}, s_{i,c}) \end{cases}$$

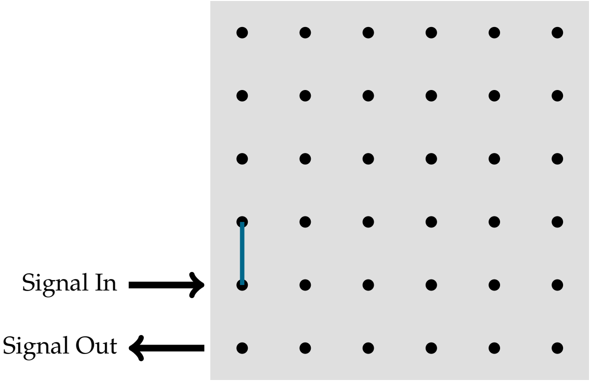
- The output data $m_{i+1,c}$ is computed by box i using the input data $m_{i,c}$ and an integrated cryptographic function F, serving as a lightweight MAC.

$m_{16,c} \neq m_{16,c+1}$



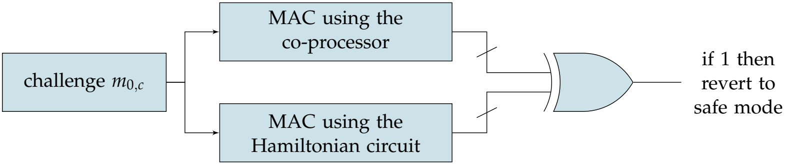
DYNAMIC ACTIVE SHIELD

- Each node represents a switch Box
- Each network configuration gives a different datapath defining a different mathematical function.



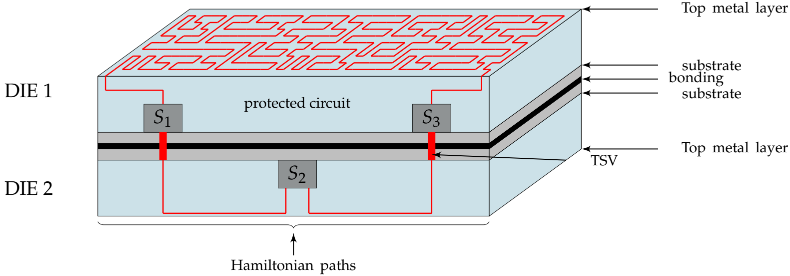
MIRROR VERIFICATION CIRCUIT

- Our "hardware canary" is formed by a spatially distributed chain of functions F_i positioned at the vertices of a 3D cage surrounding a protected circuit.
- In essence, a correct answer $(F_n \circ \ldots \circ F_1)(m)$ to a challenge m will attest the canary's integrity.



POSSIBLE EMBODIMENT

- Switch-boxes can spread over several dies.
- The number of switch-boxes doesn't have to be very big.



CONCLUSIONS

- The proposed dynamic active shield can be built using a small number of switch-boxes.
- The main limitation is the number of layers used for the shield to keep manufacturing costs reasonable along with the design rules that have to be followed.
- Timing can be an issue for LSI as well as the power needed to drive signals through long serpentines (cf FDTC'12 "Random active shield").

Thank you for your attention