COMBATING REVERSE ENGINEERING THROUGH TRANSIENCE

Dr. Troy Olsson, DARPA/MTO Program Manager

NDIA Trusted Microelectronics Workshop

August 16, 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Program</th>
<th>Loss of information</th>
<th>Fraudulent products</th>
<th>Loss of access</th>
<th>Malicious insertion</th>
<th>Quality and reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Government Intervention</td>
<td>Government-proprietary</td>
<td>Other</td>
<td>★</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fine Disaggregation and Transience</td>
<td>TIC (IARPA)</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VAPR</td>
<td>★</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional Disaggregation</td>
<td>SPADE</td>
<td>★</td>
<td></td>
<td>★</td>
<td>★</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DAHI</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHIPS</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRAFT</td>
<td></td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obscuration and Marking</td>
<td>eFuses</td>
<td>★</td>
<td></td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SHIELD</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification and Validation</td>
<td>IRIS</td>
<td>★</td>
<td></td>
<td>★</td>
<td>★</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TRUST</td>
<td>★</td>
<td></td>
<td>★</td>
<td>★</td>
<td></td>
</tr>
</tbody>
</table>

VAPR will help protect intellectual property in DoD microelectronics.
Develop a toolkit that allows for microelectronic systems to vanish in a controlled manner on command.

High performance Microsystems that physically disappear resulted from the program.
• Requirements were placed on the vanishing modality to ensure clandestine operations and environmental safety

• Camouflage was not considered vanishing
2.2. Central Tension Measurement

The measurement of compressive stress profiles in ion-exchange glasses is very tedious, and was not attempted for this study. However, the values of the compensating tensile stress in the bulk were obtained by using a set-up described in Ref. 14. A white light source was viewed through a crossed polarizer and analyzer set to obtain extinction. The samples were then introduced such that the light beam passed along the disk diameter. The birefringence introduced due to the internal tension led to the extinction condition being disturbed, and a particular fringe color was seen in the eyepiece. A Soliel-Babinet compensator and additional quarter wave-plates were then introduced in the light path to re-obtain extinction. Knowing the amount of retardation induced by the compensator-wave-plate combination to attain extinction and the stress optic coefficient of the glass, the central tension values in the samples were calculated.

2.3. Bi-Axial Strength Tests, Indentation Tests, and Fragmentation Observations

The strength values of the disks exchanged under various test conditions were measured using a ring-on-ring biaxial fixture made in accordance with ASTM C1499. For each test condition, one or two samples were fractured, and strength determined. In order to establish a baseline, the strength of five un-exchanged glass disks was measured. To probe the changes in the surface stress as a function of exchange time, Vickers indentation experiments were conducted. A Vickers indenter was loaded onto the surface in air at 40N and 50N peak applied loads, held for fifteen seconds, and then removed. The indentation site was examined within an hour after load removal. Fragmentation experiments on the test samples were conducted by progressively increasing the Vickers

Prince Rupert’s drop

- Formed by rapidly cooling molten glass
- Compressive stress on the surface and tensile stress at the core
- Stress gradient results in high toughness
- Surface damage results in rapid disintegration into fine particles

PARC’s transient substrate

- Stress gradient formed by ion exchange of glass
- Similar to Gorilla Glass process
- Highly controlled stress profile
VAPR glass substrate demonstration

Demo: Trigger initiates rapid heating and cooling above resistor to initiate crack formation

Demo: Robustness during handling and storage

Extremely Reliable and Stable until Triggered to Vanish!

Video not included here
VAPR glass substrate fragmentation

Time Evolution of Fracture

0 ms
0.13 ms
0.20 ms
0.96 ms
3.24 ms
10.07 ms

(U) 0.25 mA hr, peak current of 1 A

Video not included here

Image Courtesy: PARC
VAPR functional vanishing chips

- Enhanced security through vanishing electronics
- Strain energy transferred from PARC substrate to COTs chips
- Fragmentation of ICs and substrates to particle sizes < 250 μm
- Goal to achieve no visible remnants after triggering

Image Courtesy: PARC
• DARPA VAPR Program has demonstrated a frangible glass substrate that can fracture into < 250 μm particle upon triggering

• Robust handling and storage of the frangible glass has been shown

• Fracture propagation through diverse set of chips has been demonstrated

• Functional devices have been produced that demonstrate use of COTS devices, these devices can monitor temperature and receive RF signals