

SBIR 06.2 PHASE I - AWARD DETAILS

ORGANIZATION	AMRDEC (M)
TOPIC NUMBER	A06-030
CONTRACT NUMBER	
YEAR OF AWARD	
AWARD START DATE	
AWARD COMPLETION DATE	
PROPOSAL NUMBER	A062-030-2827
TITLE	Anti-Tamper Active and Passive Sensors for Use Inside an Integrated Circuit
PROJECT MANAGER	Lowell Smith (858) 495-0189 lowell.smith@ieee.org
COMPANY	Accord Solutions Inc. 3533 Albatross Street San Diego CA 92103-4807 Minority Owned: No Woman Owned: Yes Veteran Owned: No Number of Employees: 5
KEYWORDS	intrusion sensing, radiation sensitive materials, reconfigurable logic, anti-tamper circuits, non-intrusive penetrating radiation detection, in-chip anti-tamper, ball stack packaging, X-Ray detection
ABSTRACT	<p>The innovative in-chip sensor technology, integrated chip protection (ICP), proposed by Accord provides a new hardware design and production technique to delay reverse engineering and exploitation, denying an adversary information about the chip design. The target product is a device that secures integrated circuits from reverse engineering. Intrusive attacks, including minute modifications to a covering package, are detected by the proposed active sensing layer, which responds accordingly. Thus, the ICP anti-tamper technology provides very high sensitivity to physical tampering intrusion attacks. Integrated sensor and detection processing provides false alarm rejection and compensation for the environment's impact on the sensor. In addition, the innovation provides sensitive layers that can detect X-ray or other penetrating radiation that have impinged on the integrated circuit substrate and its package. If exposed to imaging levels of radiation during quiescence this detection layer enables secure circuit activation only if there has been no intrusion during the interim between powered missions.</p>
BENEFITS	<p>The result of Phase II will be a chip design methodology and a packaging technology that inherently protects the contents of a chip or a group of chips assembled into a ball stack. The steps in getting to the chip level will also lead to methods of applying tamper proofing appliques to the top and bottom of legacy chips, allowing for earlier insertion into present platforms. The proposed technology will inhibit an adversary's exploitation and/or reverse engineering effort in reverse engineering of chip and military package designs. It will require a significant resource investment to compromise chips protected by the propose technology.</p>