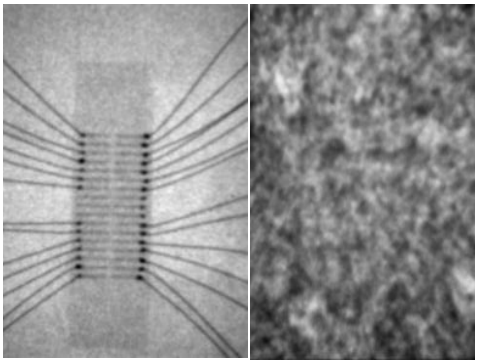
Anti-Tamper Technologies - Materials



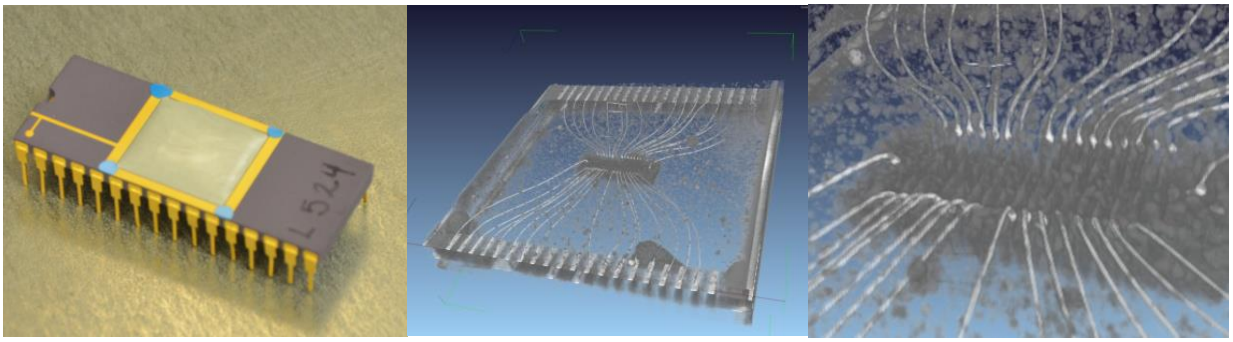
Images illustrating the XBS materials ability to block and scatter X-ray in order to keep the protected device forensically indiscernible. On the left, one can see the device imaged without the protection of XBS. The right image shows the same device protected with XBS.

XBS (X-Ray Blocking and Scattering) Nanocomposite

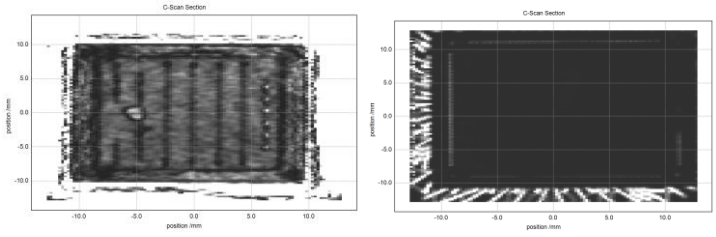
The XBS (X-Ray Blocking and Scattering) concept was developed specifically in an effort to conceal critical components from adversaries. Its opaque nature requires that an attacker to attempt to gain information by utilizing non-intrusive imaging, such as X-Ray Microscopy, or to physically destroy the device in order to gain information, compromising its functionality. When properly implemented, XBS has been proven effective in obfuscation of critical technology components against X-Ray and Terahertz Microscopy imaging attempts; this has been verified by in-house and independent laboratories. Obfuscation is accomplished by implementing a proprietary composite material that is effective in blocking and scattering incident radiation; thus, the radiation either does not reach the detector of the imaging equipment, or it has been scattered in a way that sufficiently distorts the image. We challenge anyone to image through XBS; we simply don't think it can be done.

Space Photonics is happy to tailor novel formulations of XBS for your unique application.

XBS is intended for coating, Glob-top, and Cavity fill in applications where protection of critical technology is desired.

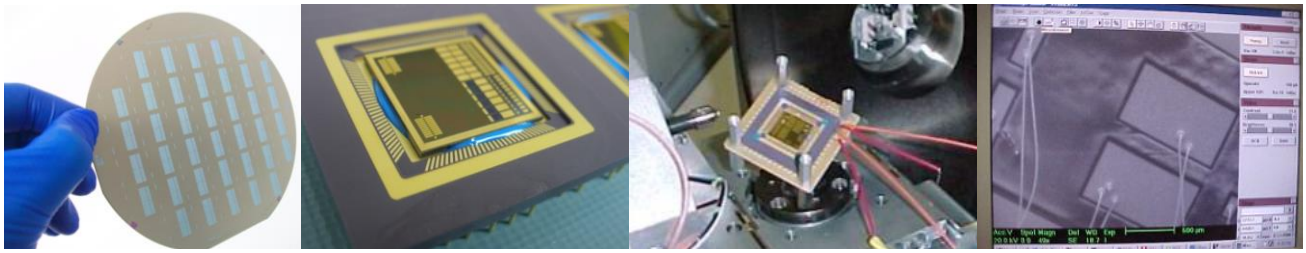


Above: Computed tomography (CT) images of device protected by XBS. Although large features, such as the gold wire bonds, are discernible, the circuitry of the silicon device is obfuscated.



Terahertz images are seen to the left: Image on left shows device encapsulated in thermally conductive COTs epoxy is able to be imaged. Right image shows an identical device encapsulated with XBS. Referenced images taken at 0.883 THz.

Nano-Mesh Ionizing Environment and Physical Intrusion Sensors



- Sensor produces a measurable DC voltage when in the presence of ionizing radiation
- Very thin structure (50 to 200 nm) is sensitive to violations by physical probing attempts
- Full processing compatibility with typical thin-film IC fabrication processes; assembly compatibility with typical IC and hybrid circuit packaging processes
- Passed preliminary screening and qualifications plans created based on MIL-STD-883, and EEE-INST-002
- Passed mechanical vibration testing, with g-force exceeding 70 G's / 24 hours per axis / 2-axis
- Deposition and fabrication processes may be utilized at the die or wafer-level – directly and non-intrusively integrated onto the surface of an IC or wafer of interest
- Can be monolithically integrated with other AT sensors onto a single substrate for application at the package level

E-beam Responsivity (mV)

vs. Beam Energy (keV)

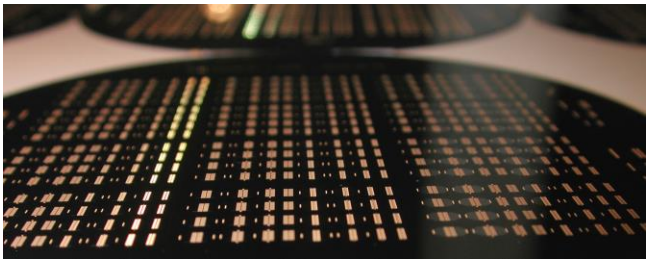
Beam Energy (keV)	DC Bias Response (mV)
1.0	0.0
2.0	0.1
5.0	0.4
10.0	0.6
15.0	0.7
20.0	0.8
25.0	1.0
30.0	0.8

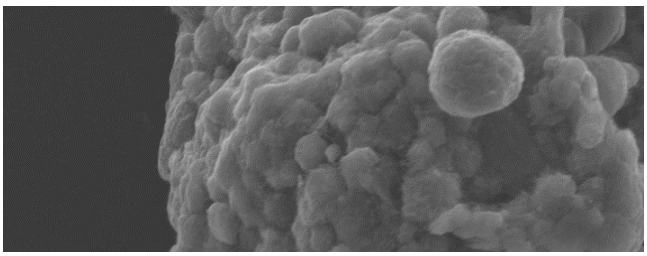
Nano-Lock Sensor Arrays

These nanomaterials based elemental arrays utilize the inherent randomness of nanomaterials and deposition techniques to ensure each manufacutured array is truely unique and imposible to reproduce exatly, even if the method of manufacture is known. Their predictable response to biasing could be leveraged for challenge-response authentication. These devices have passed preliminary screening based on MIL-STD-883, and mechanical vibration testing, with g-force exceeding 70 G's / 24 hours per axis / 2-axis.

Multiple applications, such as:

- Unique Key for Circuit Locking
- Intrusion Detection
- Random Number Generation
- Key Generation
- Physical Unclonable Function (PUF) Applications





TPOC: Brennen Freiburger, bfreiburger@spacephotonics.com , Ph. 479-936-6770