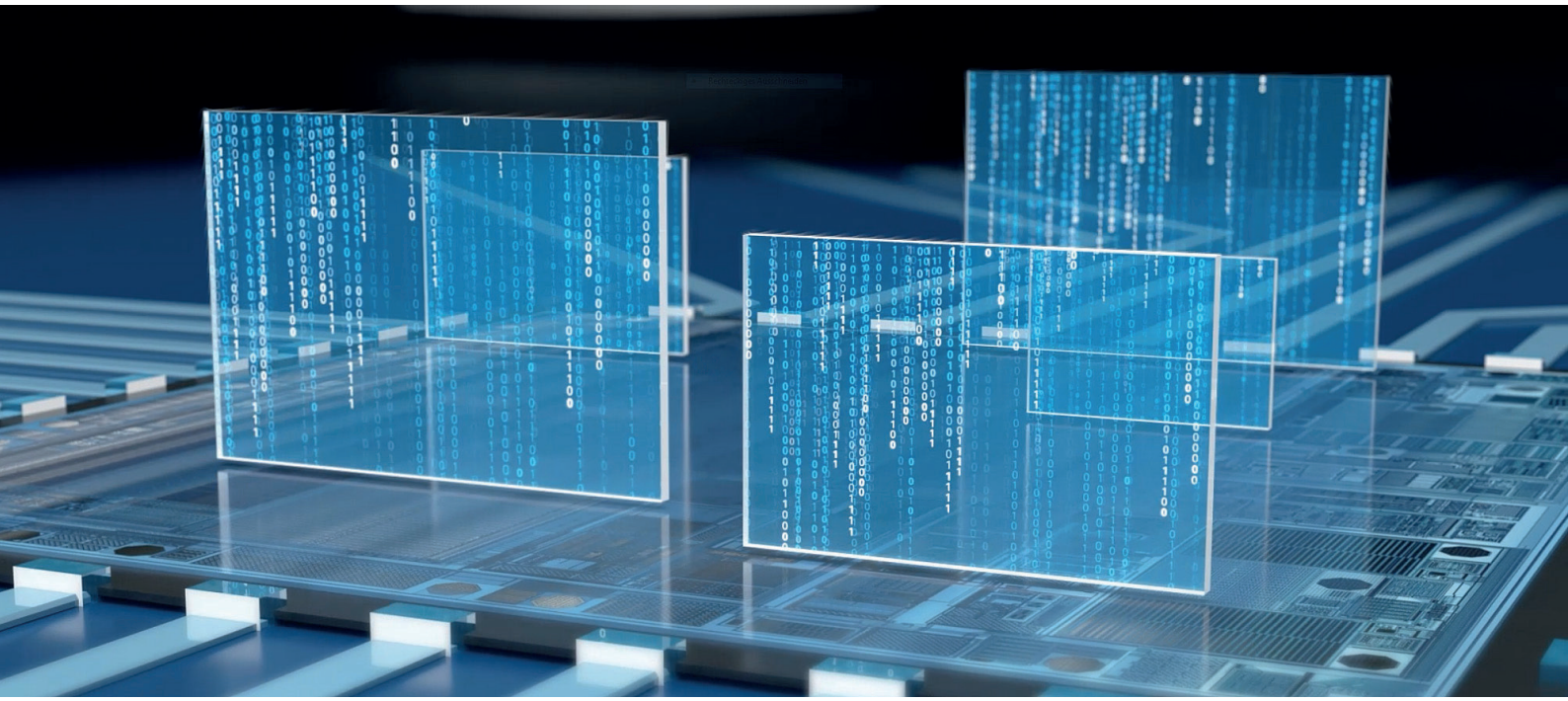
QRNG – Quantum Random Number Generator

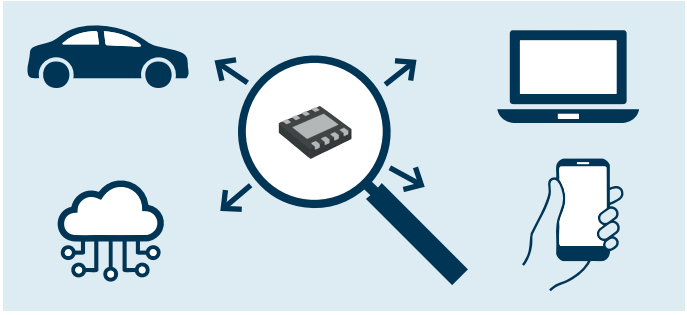
Smallest Integration of Quantum based Entropy Source for any Cybersecurity Application



- **Cybersecurity needs AI-/Quantum-safe encryption based on random numbers (RNG)**
- Existing **TRNG** based randomness mid term is vulnerable to classical physical effects like temperature and supply variation attacks supported by AI algorithms, Quantum Computers
- **QRNG** mitigates these risks and provides a smaller Risk Vector compared to TRNG

Elmos Innovation

- Elmos shows **ultra small,** vertically and monolithically integrated QRNG solution
- **Datarate scalable** from 500kbps up to multi mbps
- Very **low power** consumption and **low supply voltage** (down to 1.8V)
- Very **short warm up phase** compared to TRNG (get keys faster as with TRNG)
- **Versatile applications** including communication networks in **Automotive,** Mobile, IoT, ...
- The Elmos monolithic QRNG can be made available as **stand-alone IC** (DFN 2x2 package) **or integrable block** for higher level Designs/Technology nodes (µC, Sensors, Actuators, Interface Nodes...)
- **Randomness proven, Robustness vs. attacks by various measures, BSI/NIST Certification planned**



Elmos Semiconductor SE, Werkstättenstraße 18, 51379 Leverkusen, Germany, Phone: +49 (0) 2171 / 40 183-0, sales@elmos.com, www.elmos.com