



A Key Bit on a Chip

Dr. Matthias Harter
Circuit Design & Simulation
Univ. Mannheim

What we have to offer

An invention concerning **cryptographic keys in microelectronics** for secure mobile applications/devices such as multimedia-players, RFID, sensor networks, smart cards, smart labels, IP protection, ...

We offer:

- IP (patents) to be purchased or licensed
- A silicon proven technique (a prototype has been fabricated)
- Inventor can be „purchased“ for full- or part-time R&D collaboration
- 170 pages of documentation
- Estimated costs for further R&D: € 10T

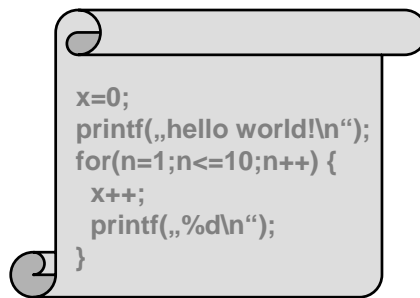


No security through obscurity

Kerckhoffs 1883:

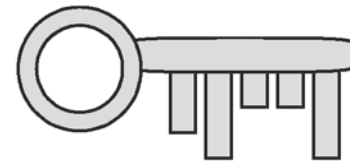
„The security of a cryptosystem must not rely on the secrecy of the algorithm. It is based only on the secrecy of the key.“

cryptographic algorithm



assumed to be **public**

cryptographic key



assumed to be **secure**

The challenge

In many data-processing applications (devices), the user of the data

- is not the owner of the data (e.g. IP-holder)
- must be restricted from full access to the data
- must therefore not hold the cryptographic keys

For this reason the cryptographic keys must

- reside in the device (i.e. microchip)
- never „leave“ the device
- not be fed into the device from outside
- therefore be generated inside the device

user of data
≠
owner of data

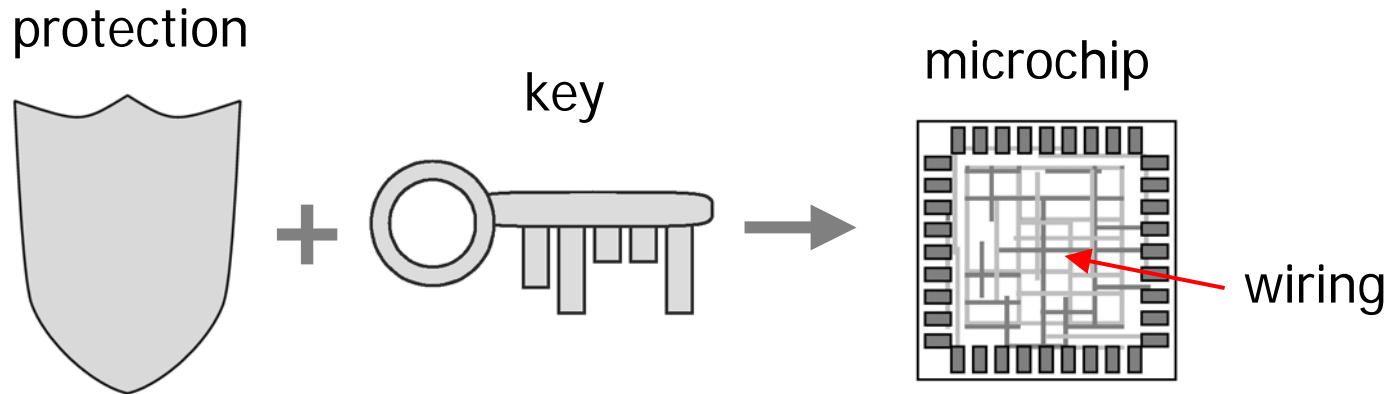


Source: Apple

The solution

Integration of the key into the microchip such that:

- the key is protected from attackers
- the key data is derived from a variable physical quantity of the chip
- the key data is always re-producible (no memory needed!)



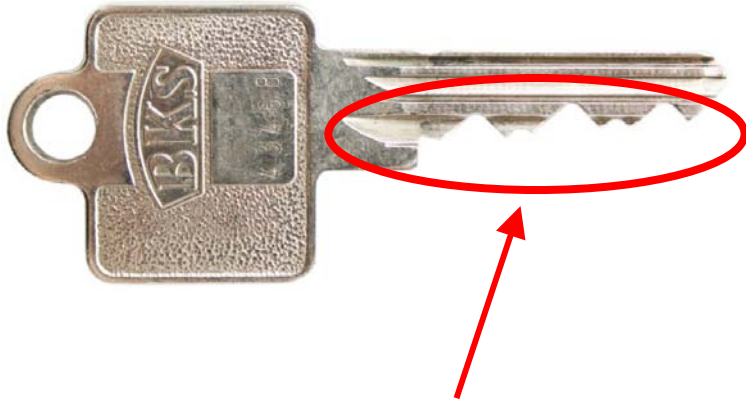
Idea: The internal wiring of a chip can be regarded as the analogy to the bits (teeth) of a „traditional“ key: Layers of various metal lines (up to 8-10 layers) arranged orthogonally like the streets in Manhattan.

The invention

Novel structures: 3D-clusters of randomly interwoven wires, generated from a special algorithm and used just like the bits of a traditional key.

Novel method: The electrical capacitance of a multiplicity of different clusters is measured and used as key data.

traditional key



indiv. structure, hard to guess
= „secret“ (unknown) key data

the invention



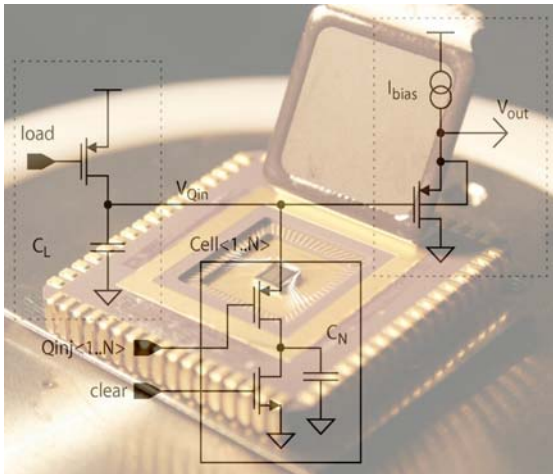
indiv. electrical capacitance, hard to
calculate = secret key data

The technique

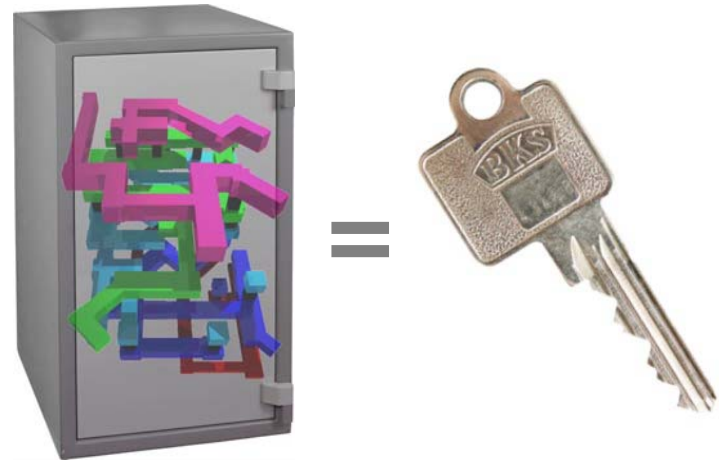
The invention comprises:

- Circuitry to measure ultra-low capacitances: 0.0.....01 Farad and below
- Circuitry to derive a digital key from the measured values
- Means for key protection: The shield and the key bits are identical!

15x
⏟



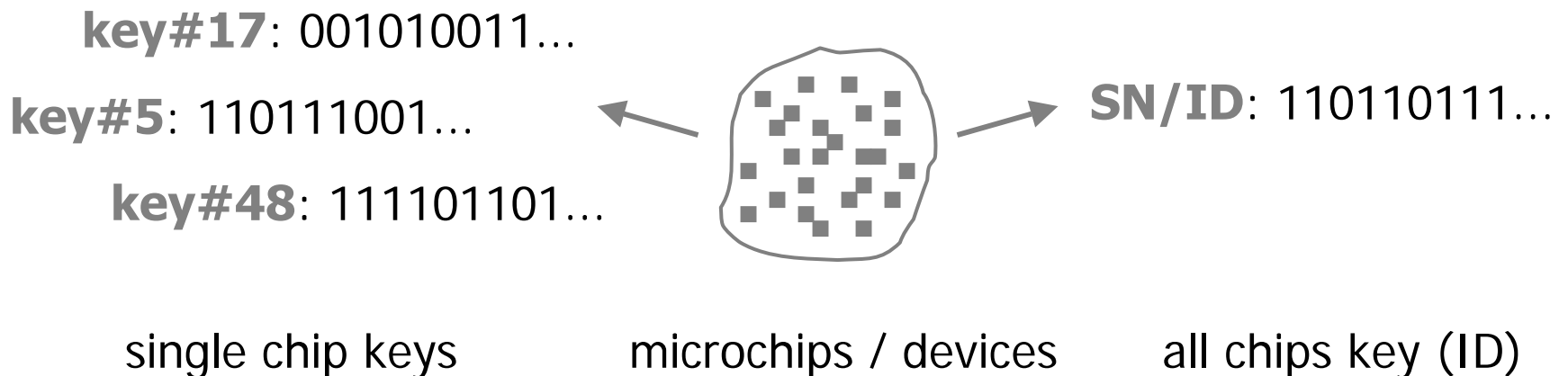
prototype / schematic



key / protection (shield)

The advantages

- **No costly shielding** or encapsulation is needed for key protection:
 - All circuitry and key data at risk is covered by the clusters
- **No sensors needed** to detect manipulation by attackers:
 - Invasive attacks change the clusters' capacitance and the key data
- **No need to store the key** in a non-volatile memory (e.g. E²PROM)
- No other known technique allows to provide at the same time:
 - Single chip keys, i.e. keys which differ from chip to chip
 - An all chips key, i.e. a secret ID or serial number shared by all chips



The applications

Securing the communication and data-processing of intelligent, distributed devices to which the user should not have full access

sensor networks



smart-cards



audio/video-player



access control



RFID



and many more...



Thank you for listening

matthias.harter@yahoo.de

tschurr@tlb.de

(Technologie u. Lizenzbüro, TLB)