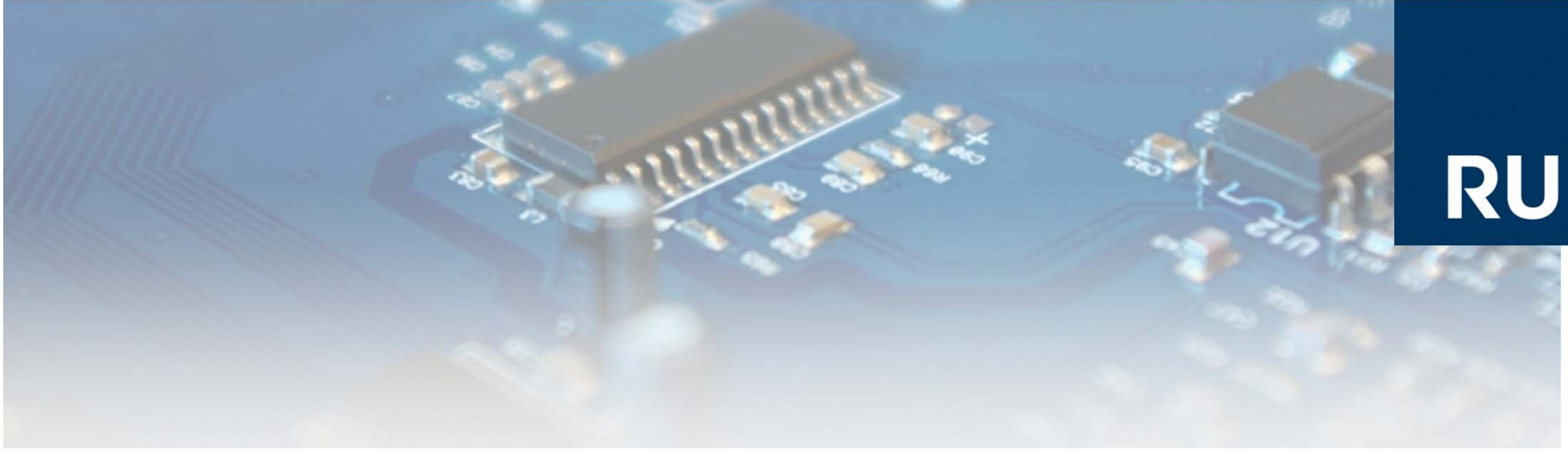


RUB

RUHR-UNIVERSITÄT BOCHUM

On the Implementation of Secure Symmetric Multi-Party Communication in a Game-Theoretic Setting using 877.5 + O(R) GE

CHES 2011 Rump Session, Nara, Japan

September 30, 2011

David Oswald
Chair for Embedded Security, Ruhr-University Bochum

hgi Horst-Görtz Institut für IT Sicherheit

EMSEC EmbeddedSecurity

Goals

- Distributed *multi-party* computation
- Game-theoretic setting
- *High* performance
- *Minimum* hardware footprint

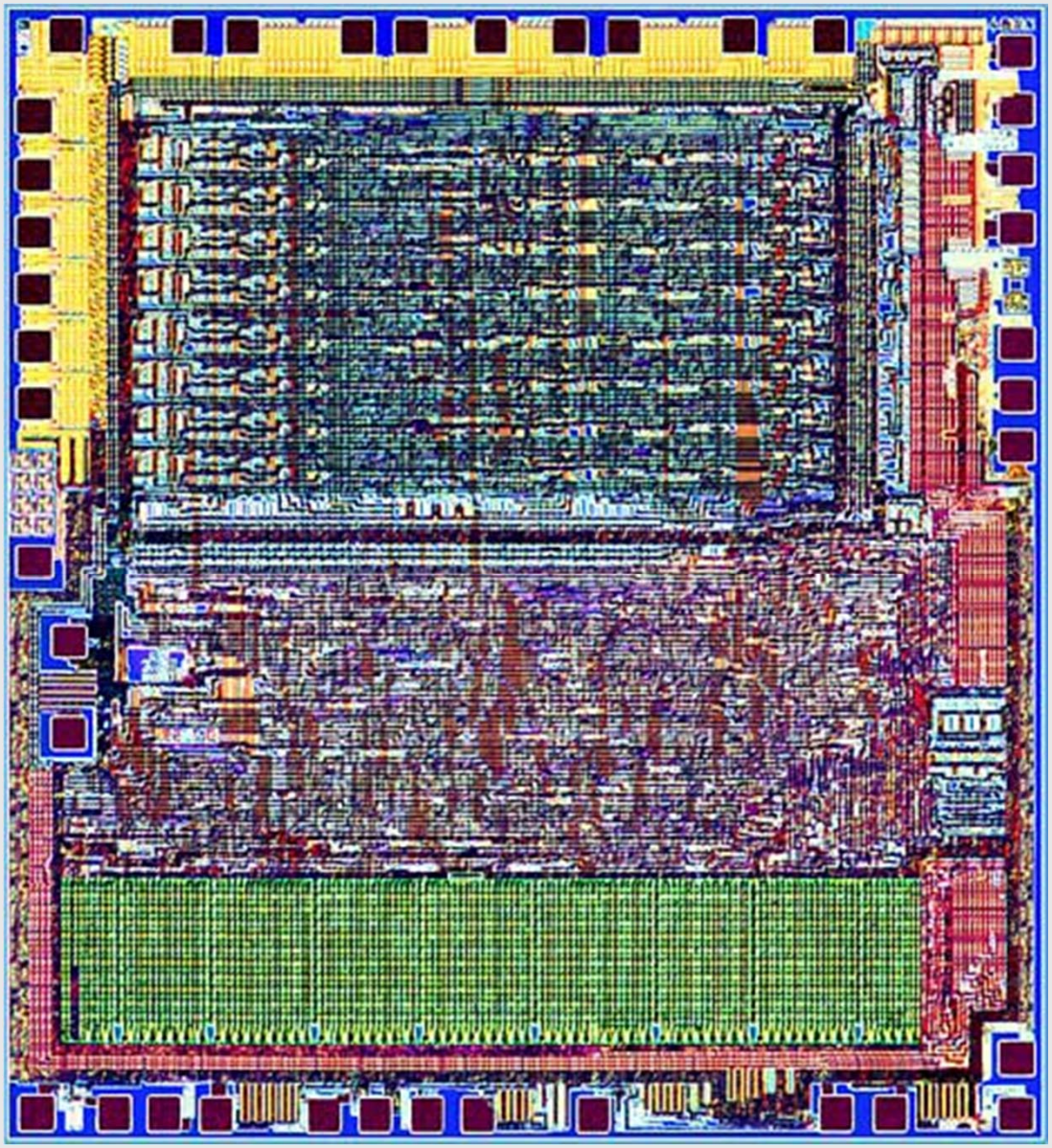
$\Rightarrow$ **Use AES**

- Prevent side-channel analysis => tamper-proof

Proposed hardware platform

RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security
David Oswald

Employed MCU: 6502



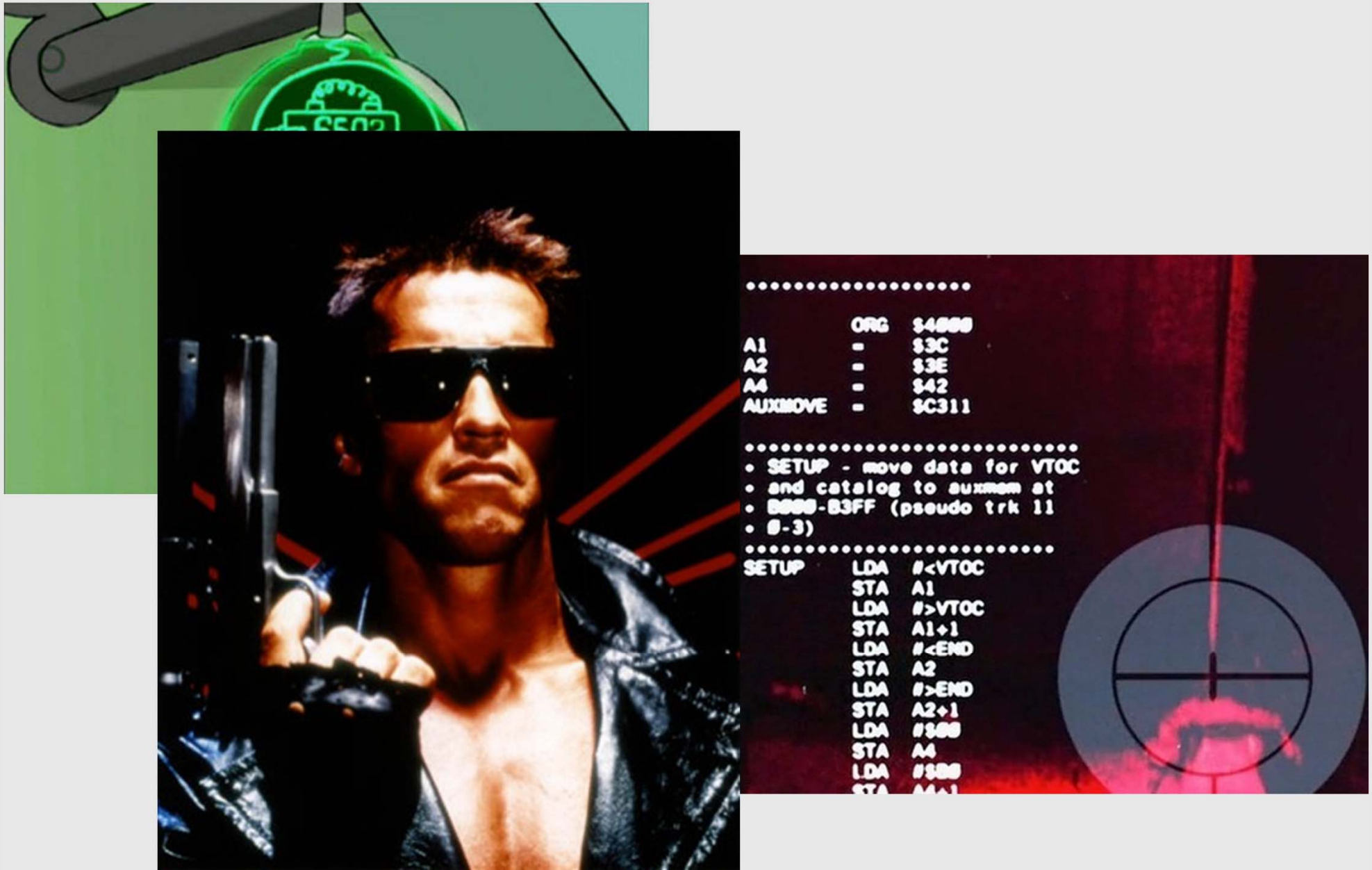
6502: Benefits

- Gate-level simulator in JavaScript: http://www.visual6502.org/
- **Simplicity:**

"An Intel Core 2 chip has hundreds of millions of transistors. The 6502 had 3,510, and an engineer — a person, not a computer — had to draw each one by hand to lay out the chip. Mainly it was a single engineer, Bill Mensch"

- **Wide-spread**

6502: Wide-spread, established platform

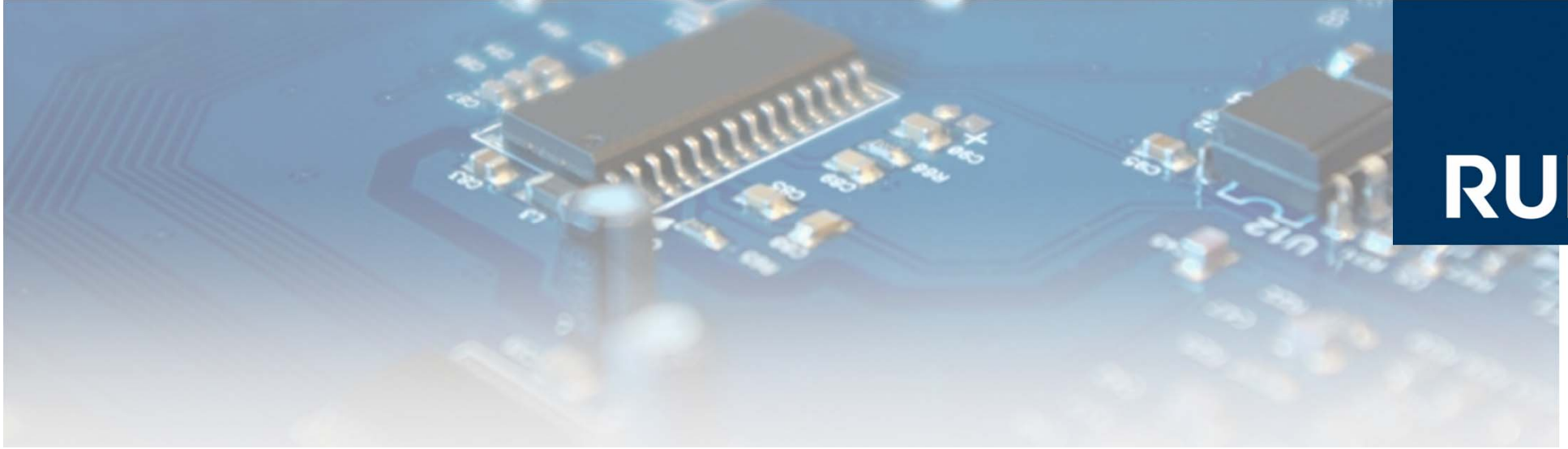


Our implementation

- Open source **AES** in 6502 assembly:

```
.ROUNDS: inc ROUND
jsr SUBBYTES
jsr SHIFTROWS
jsr MIXCOLUMNS
jsr ADDROUNDKEY
jsr UPDATEKEY
jsr PRINTSTATE
lda ROUND
cmp #9 ; count ?= 9
bne .ROUNDS ; if count != 12 goto loop
```

- On *single* 6502 + some RAM $\Rightarrow {}^{3510}/_{4} + O(R)$ GE
- **Live demo**



RUB

Thanks!
Questions?

hgi
Horst-Görtz Institut
für IT Sicherheit

David Oswald
Chair for Embedded Security, Ruhr-University Bochum

EMSEC
EmbeddedSecurity