

# *Lightweight Key Exchange and Stream Cipher based solely on Tree Parity Machines*

Markus Volkmer

Sebastian Wallner

markus.volkmer@tuhh.de

wallner@tuhh.de

**TUHH**

*Technische Universität Hamburg-Harburg*

***Hamburg University of Technology  
Computer Engineering VI***

1. Why consider alternative security primitives ?
2. Key Exchange by Tree Parity Machines (TPMs)
3. Security and Attacks
4. Trajectory Mode and Stream Cipher by TPMs
5. ASIC-Implementation: A serial TPMRA
6. Post-synthesis results
7. Conclusion

## ***Secure communication given limited resources***

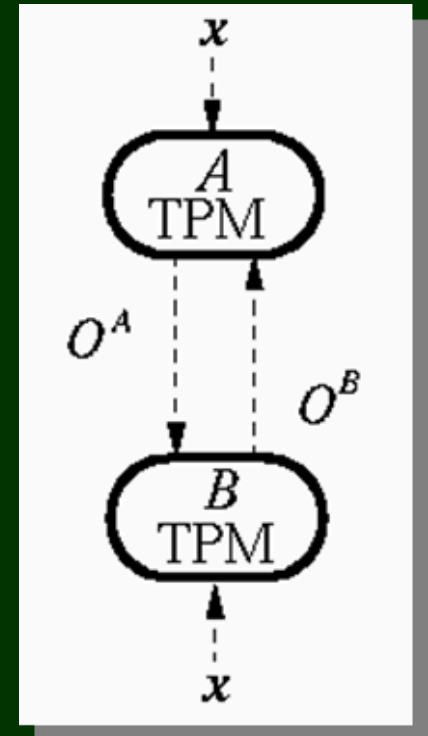
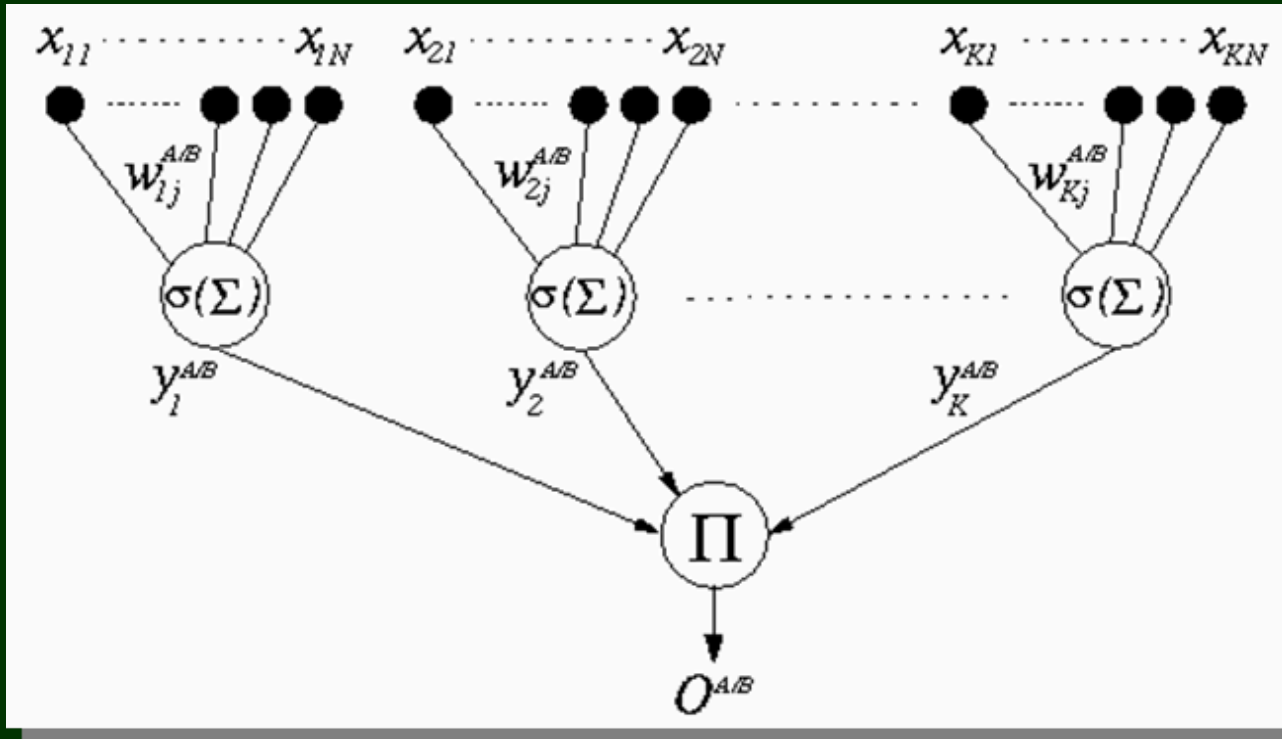
- Devices in RFID, Sensor Networks, NFC, ...
- Severe (and coupled) limitations:  
Size, computational power, power consumption, ...
- Key exchange most critical and complex
- 8-bit MC, RFID-Tag (~ 1000 gates, no MC):  
only symmetric algorithms and stream ciphers are considered applicable
- Practically trade-off: Level of security vs. resources (cost)

***Security and privacy is also economically important  
via customer acceptance***

## ***Fast synchronisation of two interacting Tree Parity Machines*** (Kanter, Kinzel, Kanter 2001)

- Symmetric key exchange
- Interaction protocol (parallel variant through bit packaging)
- Synchronisation time (distributed)
  - ~ distance of random initial coefficients (weights)
- Simple arithmetic on small (and bounded) integers

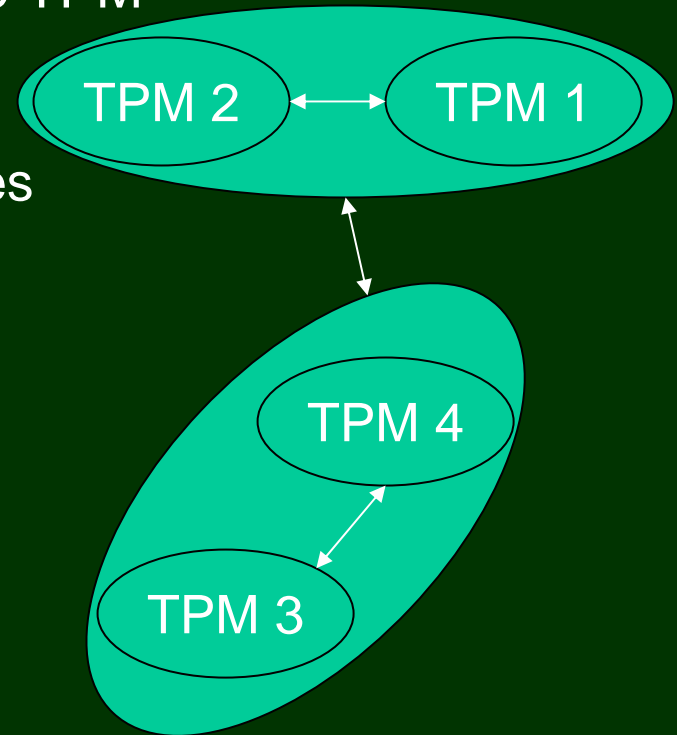
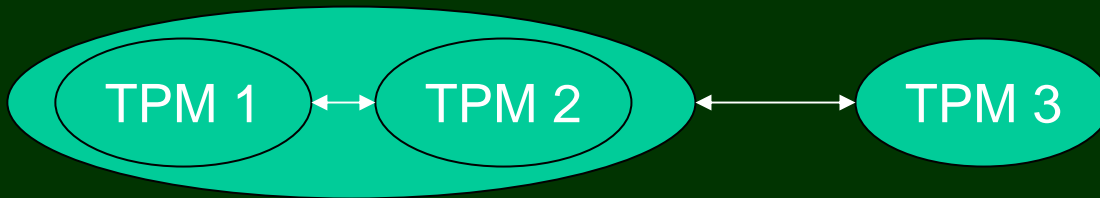
# Key Exchange by Tree Parity Machines



# Key Exchange between Multiple Parties

**Synchronous TPMs have identical internal states and remain synchronous**

- Regard synchronous TPMs as a single TPM
- Join / leave-action requires new key
- One group-sender, others only receive
- Sequential / parallel interaction processes



- Security scales inversely proportional to the number of parties

***Security can be accessed in terms of probabilities  
as in information-theoretic security primitives***

- Synchronisation (of A/B) is faster than learning (of E)  
~ advantage (of A/B) through interaction
- Security is strongly related to the mutual distances  
between the (random) initial weight vectors of A,B,E
- Successful attack = E synchronises with A or B before  
A and B are synchronous (strong definition)
- Attacks with TPMs on non-authenticated principle exist  
in which man-in-the-middle is possible as well
- Inherent entity authentication property  
(only common inputs allow for synchronisation)

- Flipping Attack (Shamir et al. 2002) „completely insecure“  
Countermeasure: increase  $L$  (Security  $\sim L^2$ )  
and make attack arbitrarily costly (Learning  $\sim e^{-L}$ )
- Majority Flipping Attack (Kanter, Kinzel et al. 2004)  
„Security does not scale with  $L$  (but still with  $K$ )“
  - Successful attack = 98 percent avg. overlap of  $E$  with weights of  $A$  or  $B$  when  $A$  and  $B$  are synchronous (achieved with Prob  $\frac{1}{2}$  independant of  $L$ )
  - overlap is a scalar product (and averaged) and thus ambiguous (only partial information on the key)
  - stronger definition of successful attack leads to fluctuating success probabilities

## ***Successful attacks on TPM key exchange ?***

## ***Synchronous TPMs have identical internal states and remain synchronous***

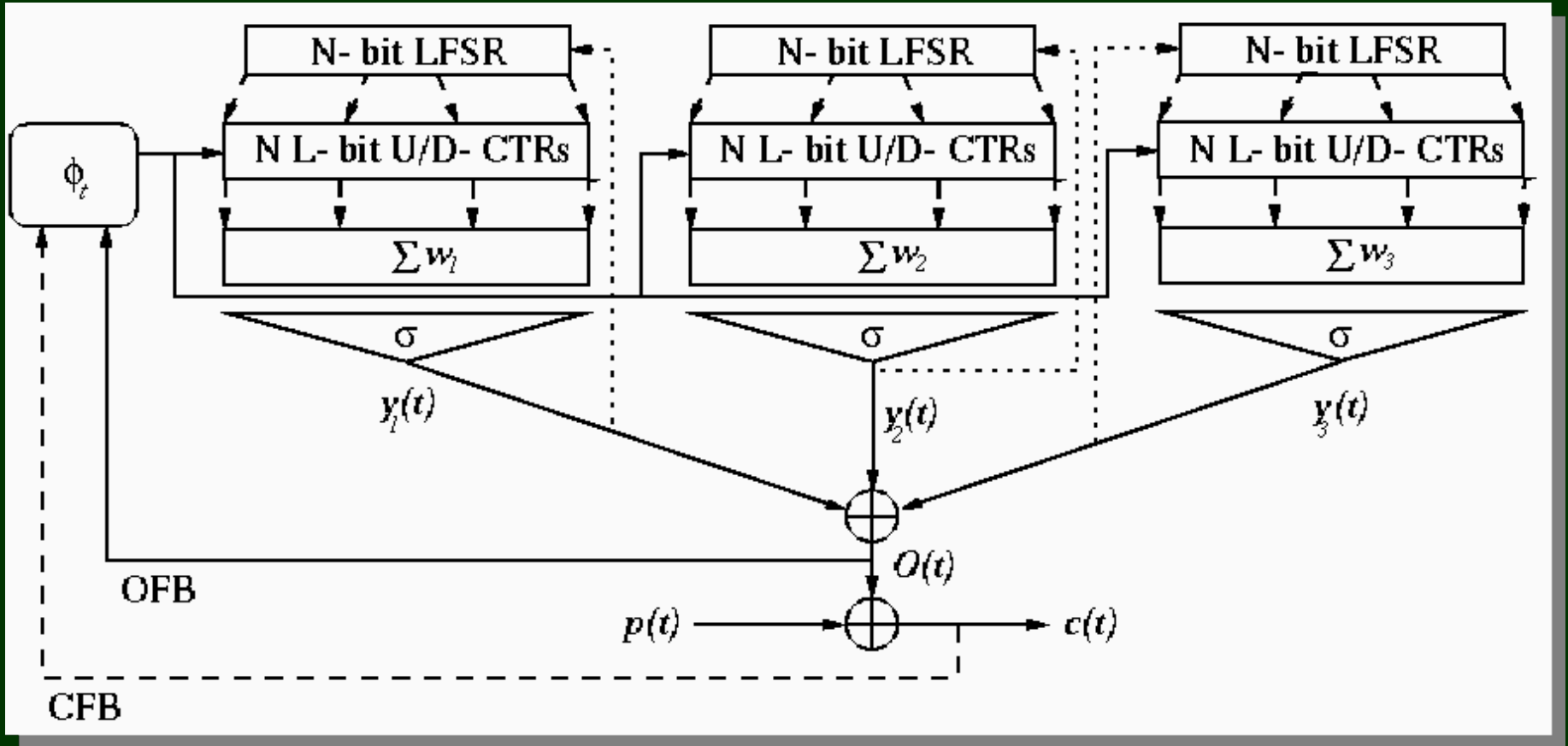
- Feedback own output (identical anyway)
- No further communication (and attacking by TPMs)
- State transition (adaptation) with own output
- A new internal state (key) from trajectory with every output

## ***TPM in „Trajectory Mode“***

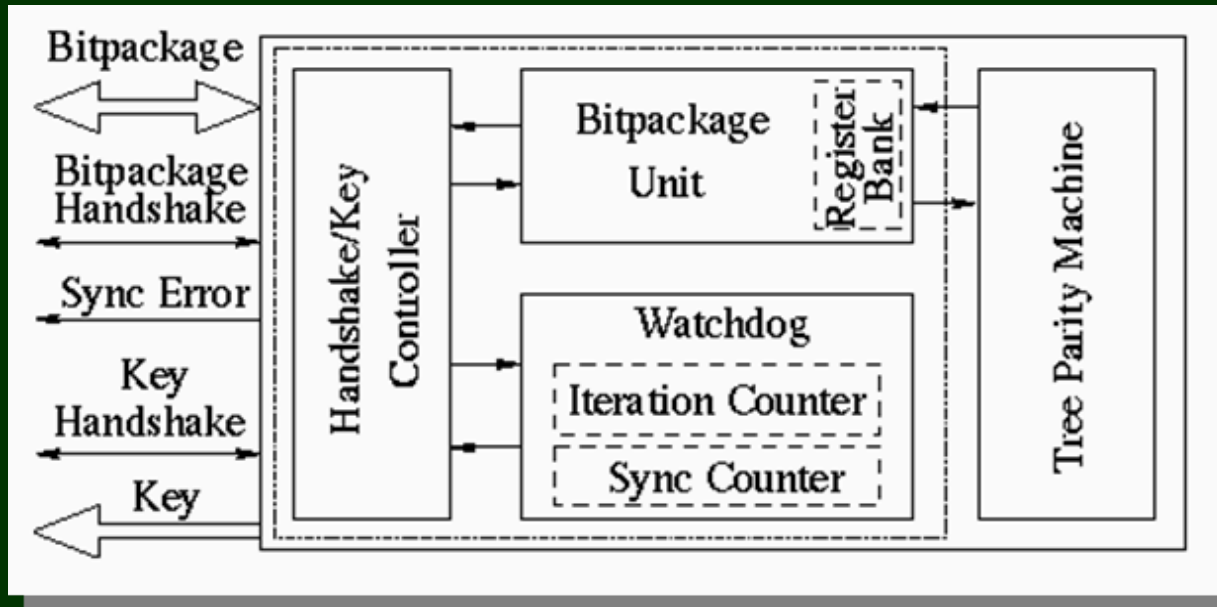
- Do not reuse keys! How get the new key?
- Use (public) IVs (?)
- Nonlinearity (state transitions, keystream), ...

## ***TPM in Trajectory Mode is a synchronous stream cipher***

- K dynamic non-linear filter generators
- Final static combiner
- TPM outputs = keystream
- TPM initial weight = key
- LFSR initialisation = IV (+ integrity mechanism)

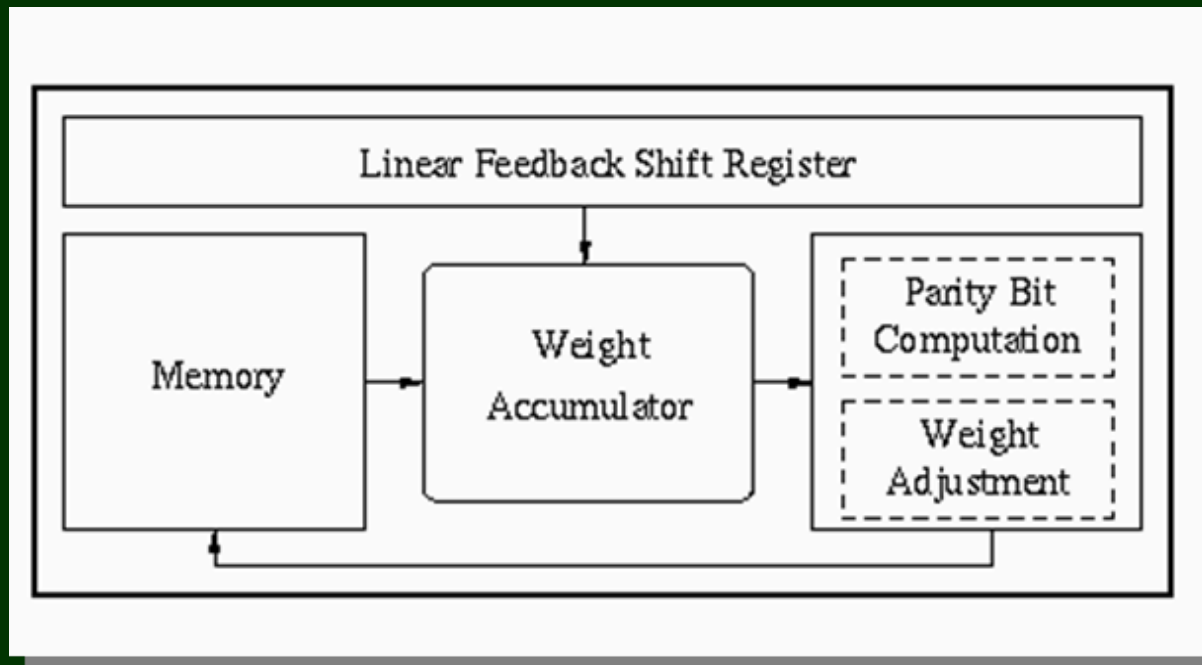


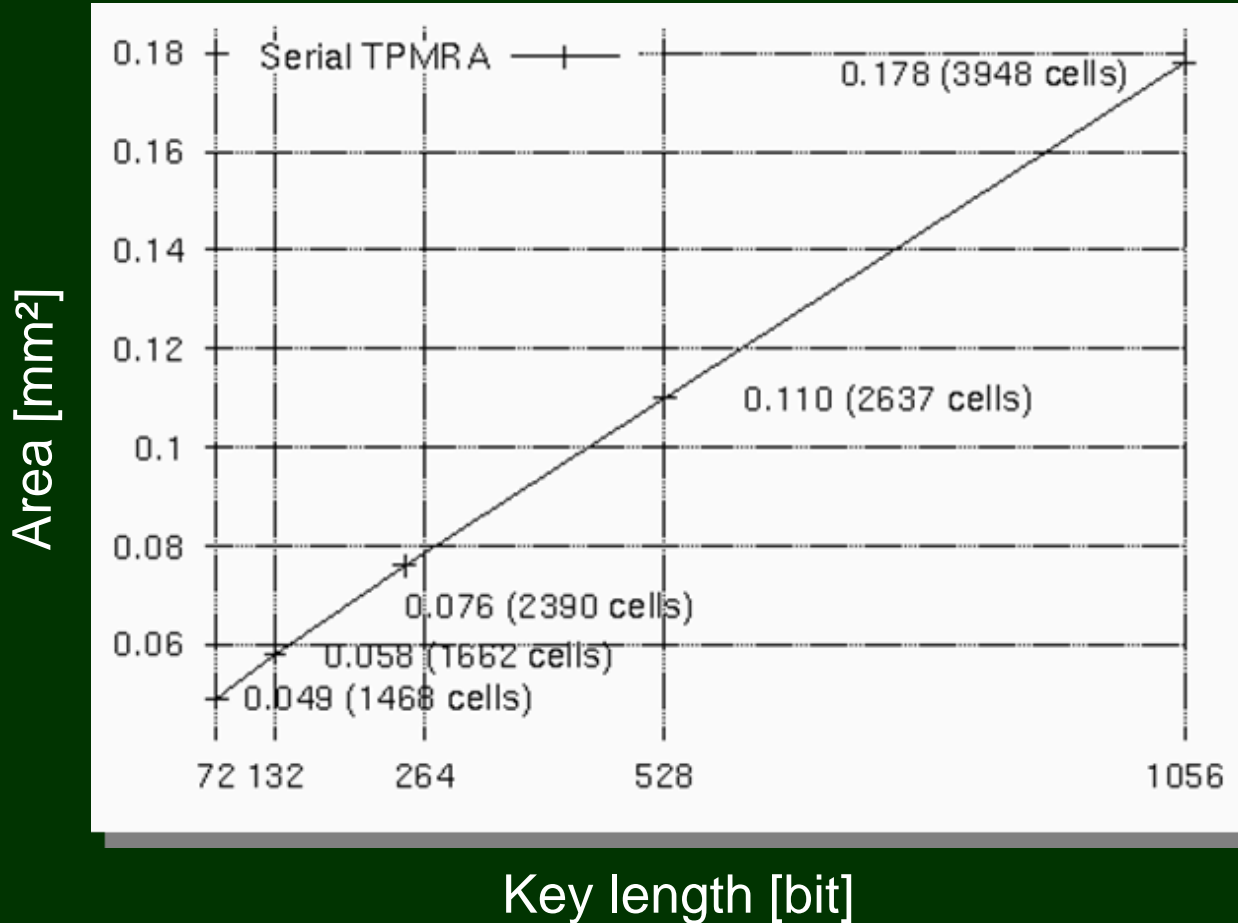
## Tree Parity Machine Rekeying Architectures (Volkmer / Wallner 2005)



Bit-packaging reduces communication down to a few packages!

- Single L-bit serial adder (used in time)
- Fully parameterizable hardware structure (K,N,L, Bit-Package-length)
- Memory (register bank) stores partial results, weights and output bits from the summation units for bit packaging

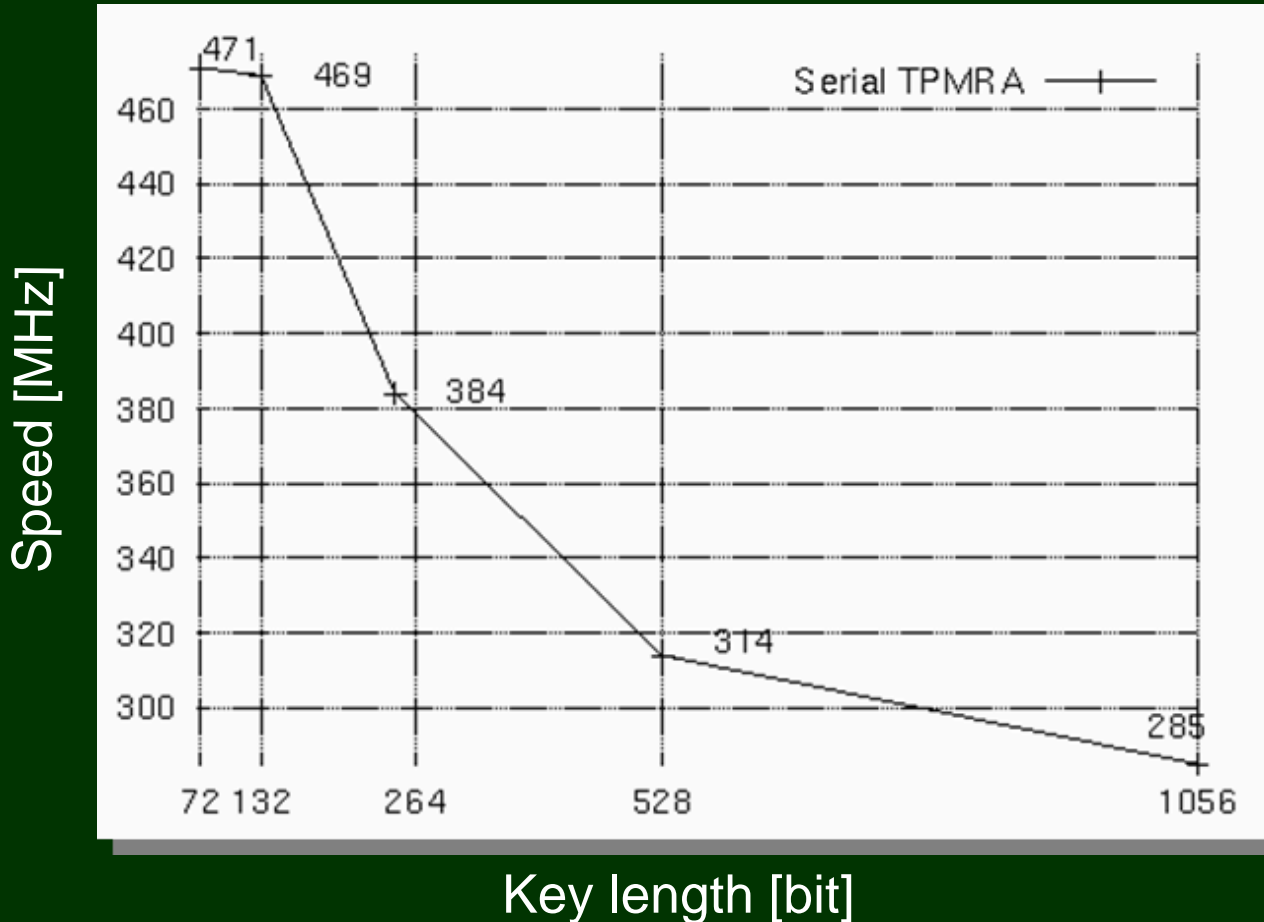




- Post-synthesis
- Area-optimized
- $K=3$ ,  $L=4$  and  $N=6, 11, 22, 44, 88$
- Apart from memory L-bit adder is most complex unit

\*0.18 micron six-layer CMOS, 1.8 V supply voltage UMC standard cell library

# Results\*: Achievable clock-frequency



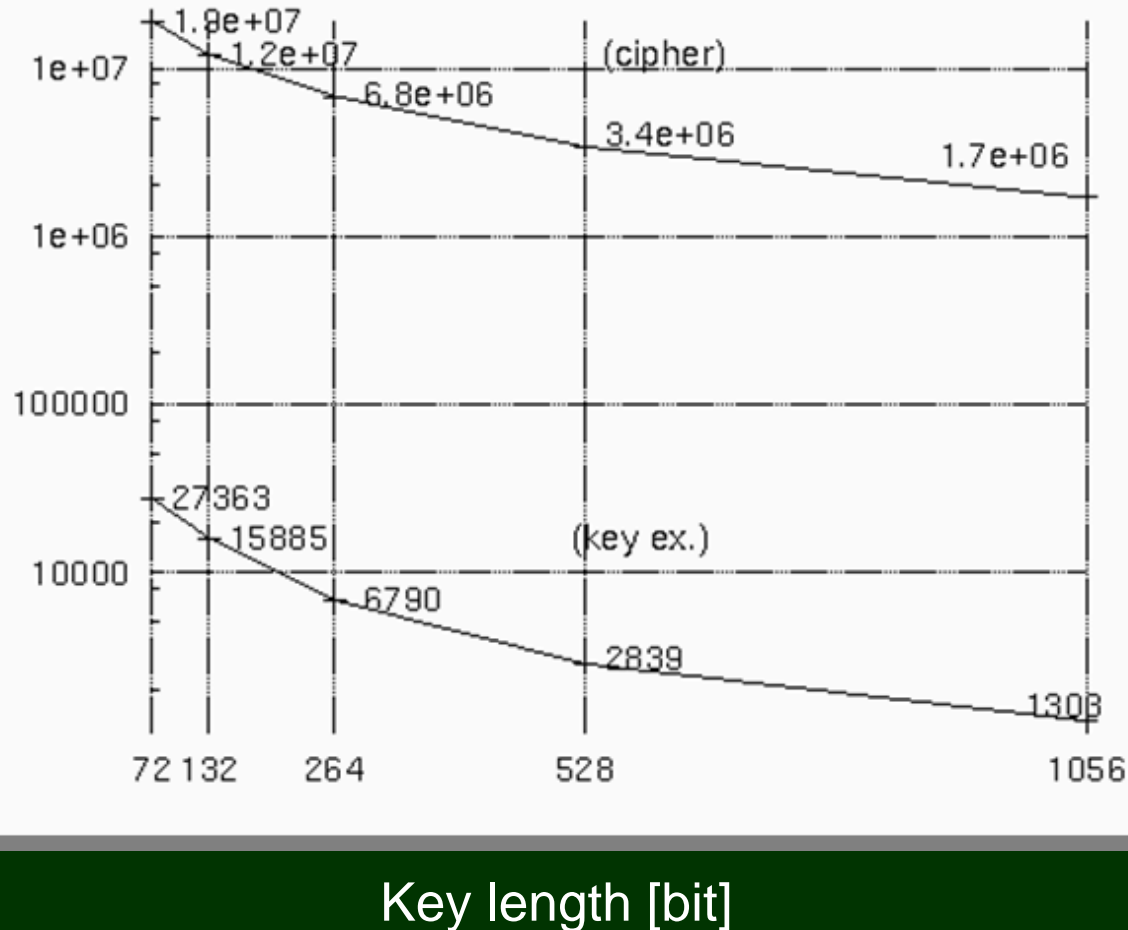
- Post-synthesis
- Area-optimized
- $K=3$ ,  $L=4$  and  $N=6, 11, 22, 44, 88$

- Critical path through memory

\*0.18 micron six-layer CMOS, 1.8 V supply voltage UMC standard cell library

## Results\*: Avg. key exchange rate and stream cipher bit-rate (theoretical max.)

Rate [Hz] (log-scaled)



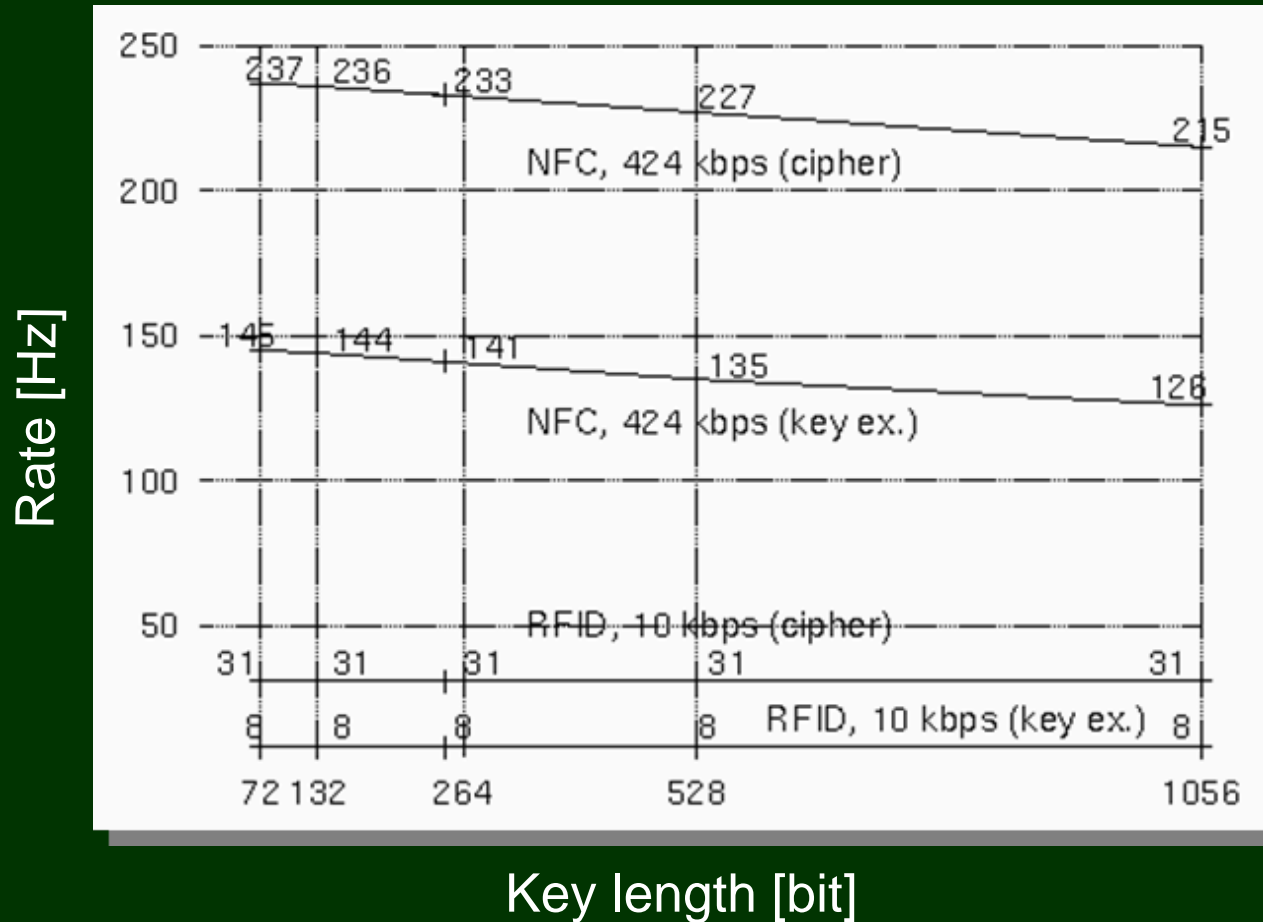
- Post-synthesis
- Area-optimized
- K=3, L=4 and N=6,11,22,44,88

- Influenced by speed

\*0.18 micron six-layer CMOS, 1.8 V supply voltage UMC standard cell library

The trajectory increases the throughput by two orders of magnitude!

# Results\*: Avg. key exchange rate and stream cipher bit-rate (RFID, NFC)



- Post-synthesis
- Area-optimized
- $K=3$ ,  $L=4$  and  $N=6, 11, 22, 44, 88$

- Determined by channel capacity

\*0.18 micron six-layer CMOS, 1.8 V supply voltage UMC standard cell library

The bottleneck is the communication channel!

## ***Three cryptographic functions from a single primitive:***

Symmetric Key Exchange + Stream Cipher  
+ Identification / Integrity Mechanism

- TPMRA has small footprint and allows for high throughput
- Some communication necessary for interaction

## ***Lightweight Primitive = Light Security ?***

- Security of TPM key exchange needs a fair evaluation
- Security of TPM stream cipher is still to be evaluated
- Power consumption, side channel attacks, ...

***Further investigations are welcome!***