Menschen verwechseln reelle und reale Zahlen – mit Folgen für die IT-Sicherheit

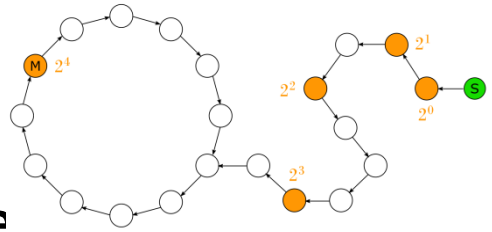
Jörg Keller
joint work with G. Spenger

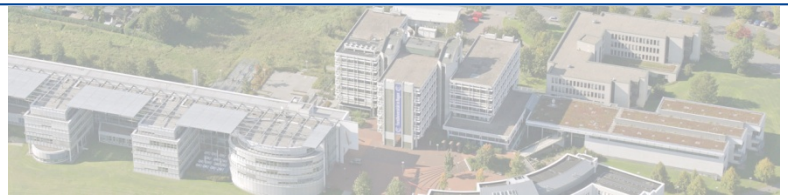
Forschungstag IT-Sicherheit NRW

Hagen, 26. Juni 2017

Motivation

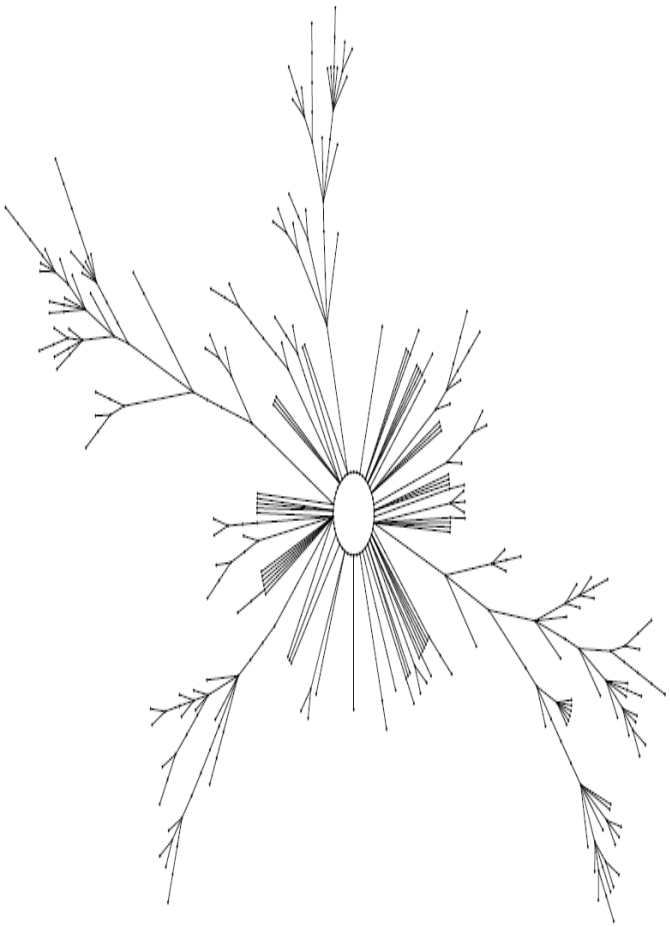
- Pseudo-random number generators = important for crypto
- Many requirements: difficult to design
- One requirement: long cycle → large state
- But: embedded computing restricts state space size
- Investigate „chaotic“ PRNGs

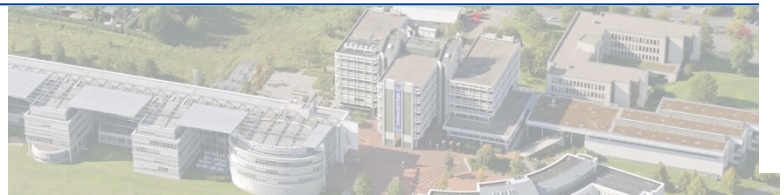




Basics

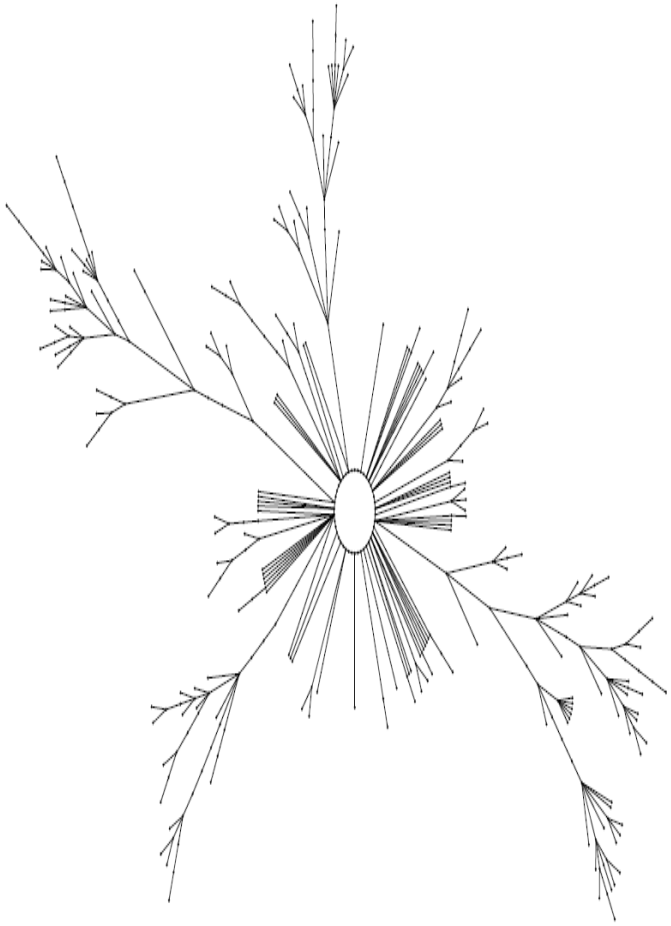
- S=set of n states, f:S→S state transition function
- Induces directed graph G=(V,E):
  V=S, E={ (x,f(x)) | x in S }
- Expected values (over all possible f):
  largest cycle size sqrt(n)

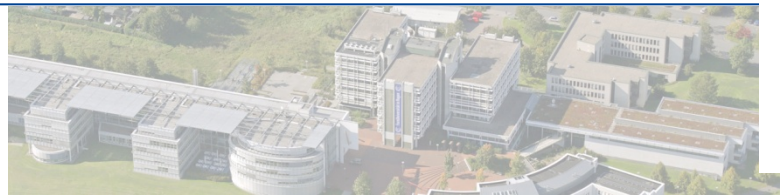




Chaotic PRNGs

- **Use transition function with chaotic properties**
- **Simple example: logistic function**
  f(x) = a * x * (1-x), a ~ 4
  x is a real in [0;1]
  → good properties provable
- **Usual implementation with floating point → short cycles**
- **Fix point implementations**
  → better but still short





Chaotic PRNGs

- Use tra nction with chaotic properties

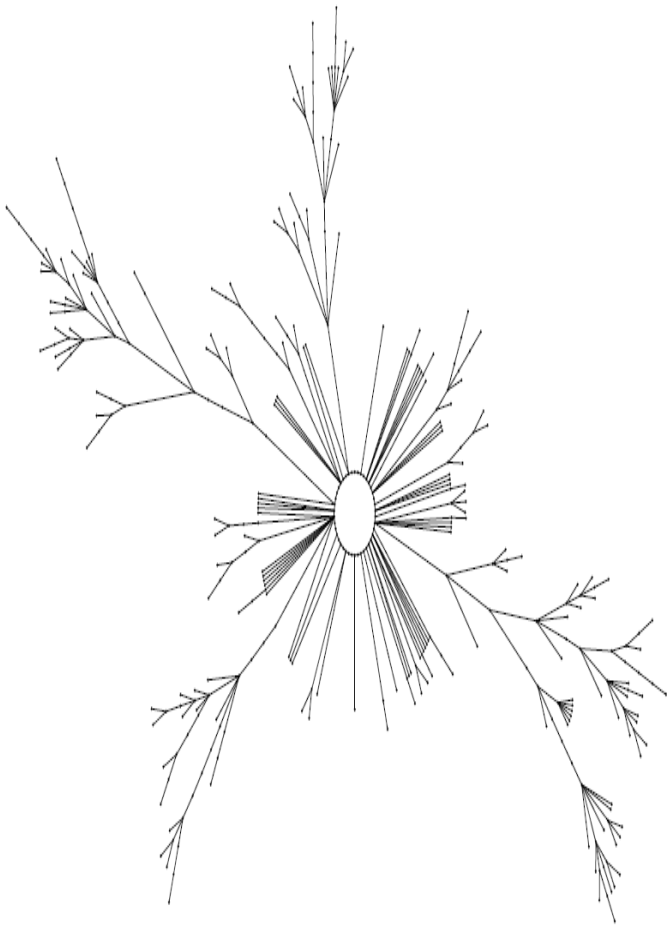
- Simple logistic function
  f(x) = a), a ~ 4
  x is a
  → goo es provable

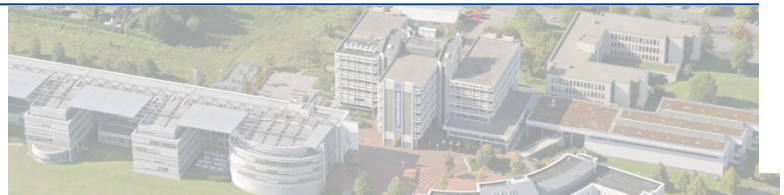
- Usual implementation with floating point → short cycles

- Fix point implementations
  → better but still short

32 bit state

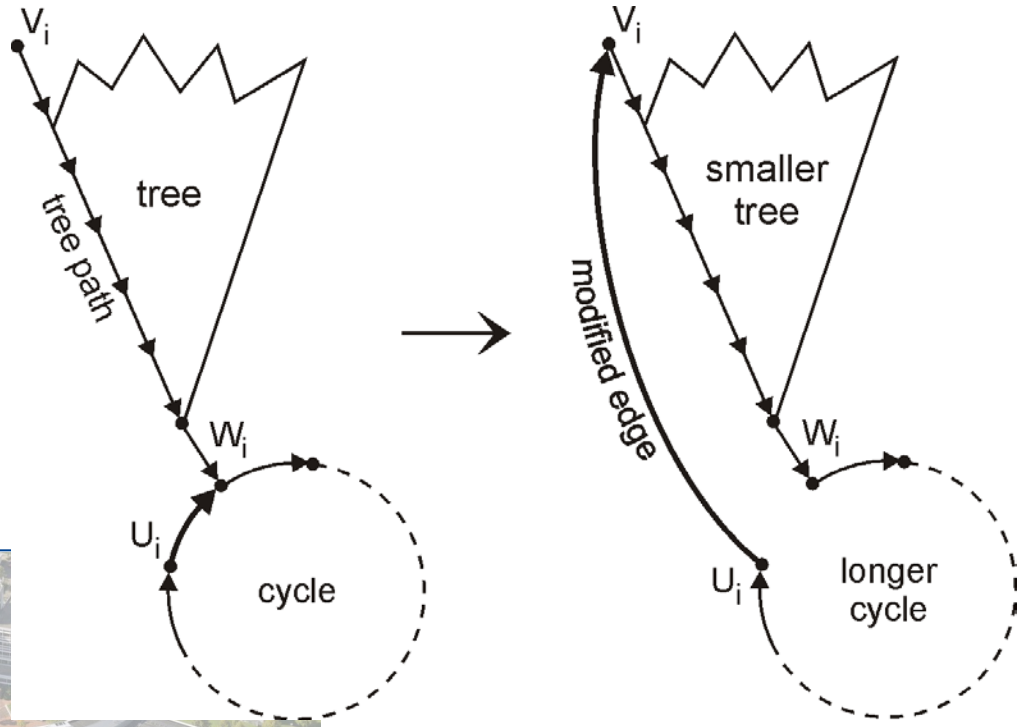
cycle length <1000

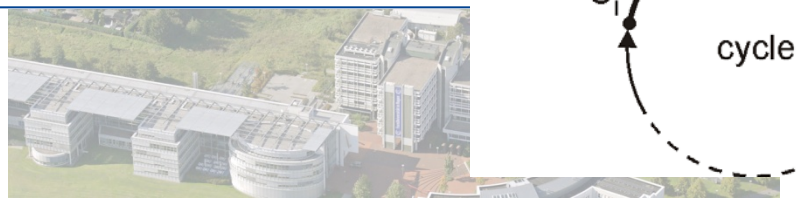




Repair of PRNGs

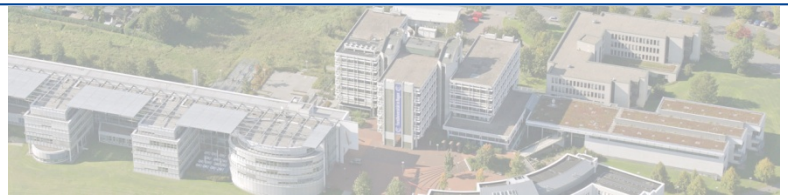
- **Modify small number of transitions**
- **Find out modifications once (offline problem)**
  Apply with table (low overhead online)
- **Choose m random points**
  For each starting point:
  Follow path till cycle
  Among starting points:
  seek edge modificat.
  to maximize cycle





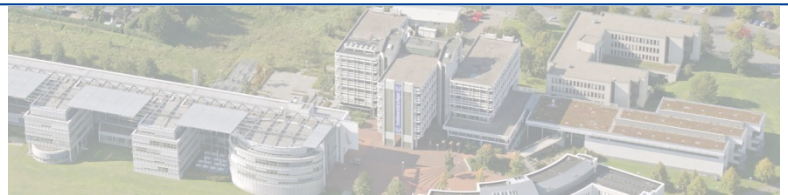
Repair Algorithm

- **Can be massively parallel**
  → state spaces up to 80 bit searchable
- **Small table (16 entries) mostly suffices**
  runtime overhead 5 to 10%
- **No adverse influence on output statistics observed**



Conclusions

- **Properties of real numbers fail with finite number representations**
- **Notable consequences for cycle lengths of PRNGs**
- **Repair possible for moderate state space**
- **Black-box approach (no offline phase) possible for larger state spaces, results not as good**



Thank you very much for your kind attention