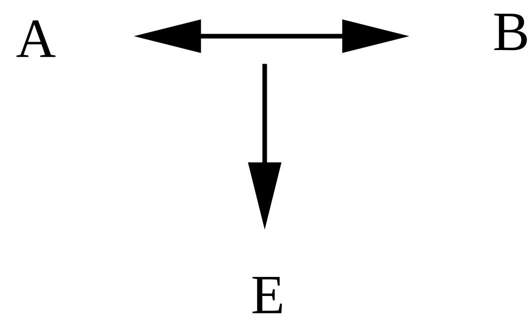
# Generating secrets over public channels


- Neural Cryptography
- Synchronization of chaotic systems

- Würzburg: Richard Metzler, Andreas Ruttor, W.K.
- Bar Ilan: I. Kanter, M. Rosen-Zvi, E. Klein, R. Mislovaty, L. Shacham, Y. Perchenok

# Key exchange protocol




Two partners A and B generate a common secret, without previous secret contact.
An attacker E can only listen to the communication, but otherwise E knows everything what A knows about B.

Is this possible?

# Number Theory

Diffie and Hellmann 1976,
Rivest Shamir Adelman (RSA), El Gamal

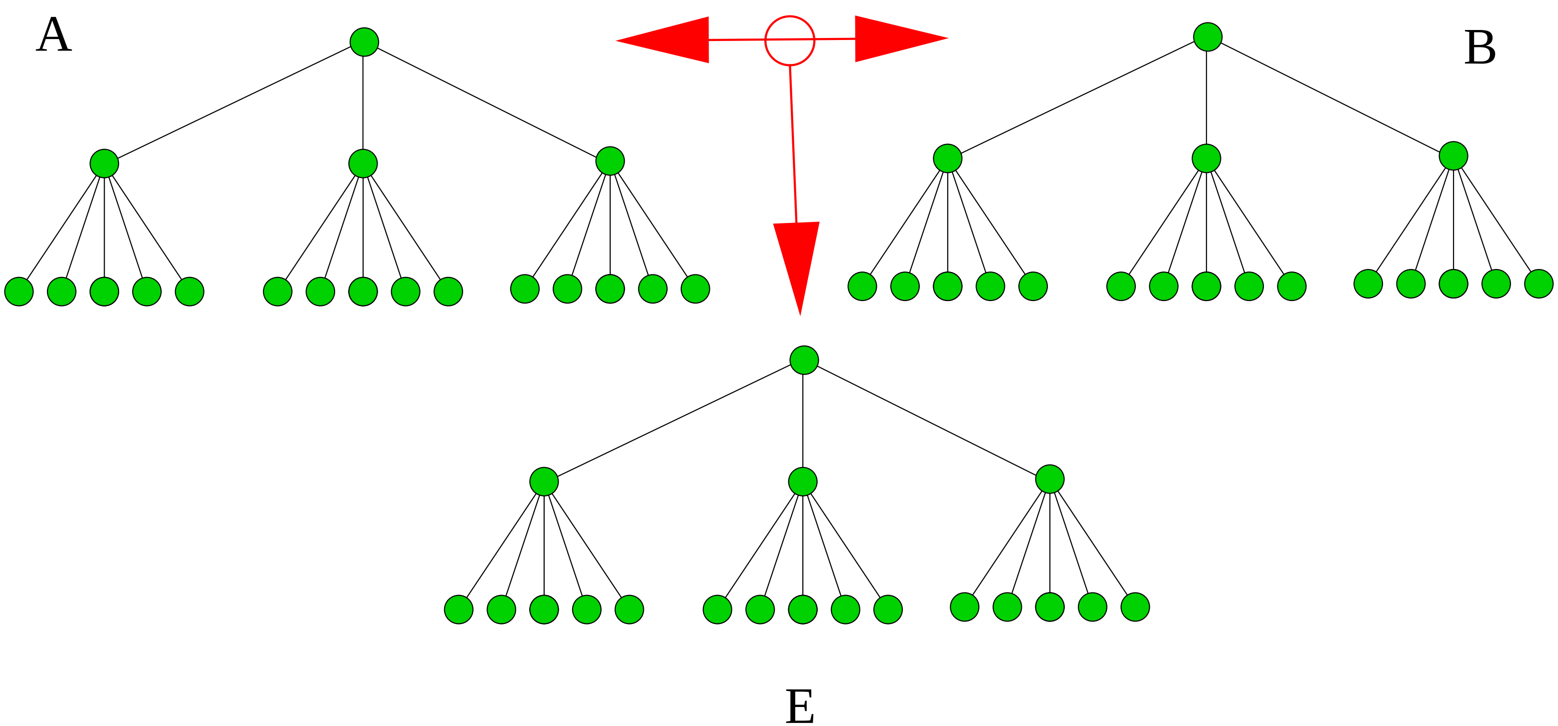
- Large integers: $a, b, c, p$. Public: $c, p$. Secret A:$a$, B:$b$
- A sends $y = (c^a)$ mod$p$ and B calculates $k = y^b$ mod$p$
- B sends $z = (c^b)$ mod$p$ and A calculates $k = y^a$ mod$p$
- $k$ is the secret key, which is used to encrypt secret messages
- $y = (c^a)$ mod$p$ is fast, $(\log y = a \log c)$ mod$p$ is non feasible

# Physics

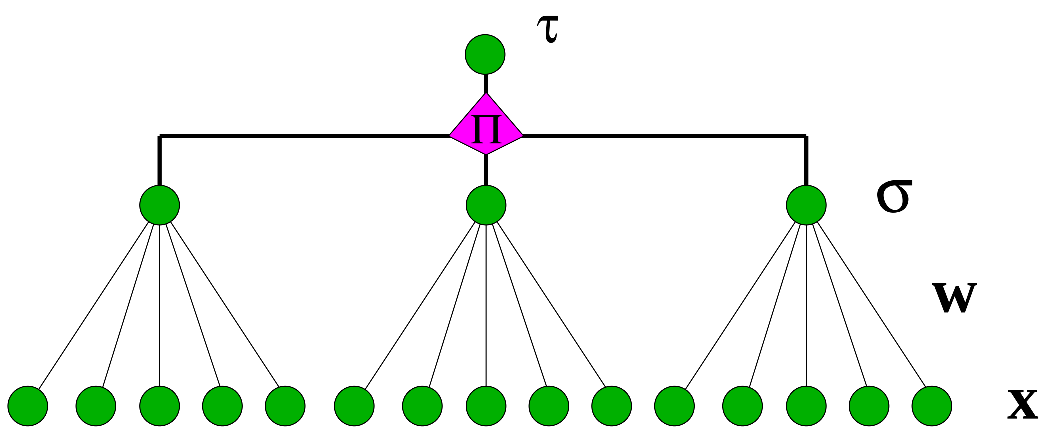
- Quantum mechanics
- Stochastic process:
  Synchronization of neural networks by mutual learning
  Ensemble of random walks with stochastic repulsive and attractive forces
- Nonlinear dynamics:
  Synchronization of chaotic differential equations

Mutual interaction has an advantage over one-directional information

# Neural Cryptography



# Realization: Tree Parity Machine



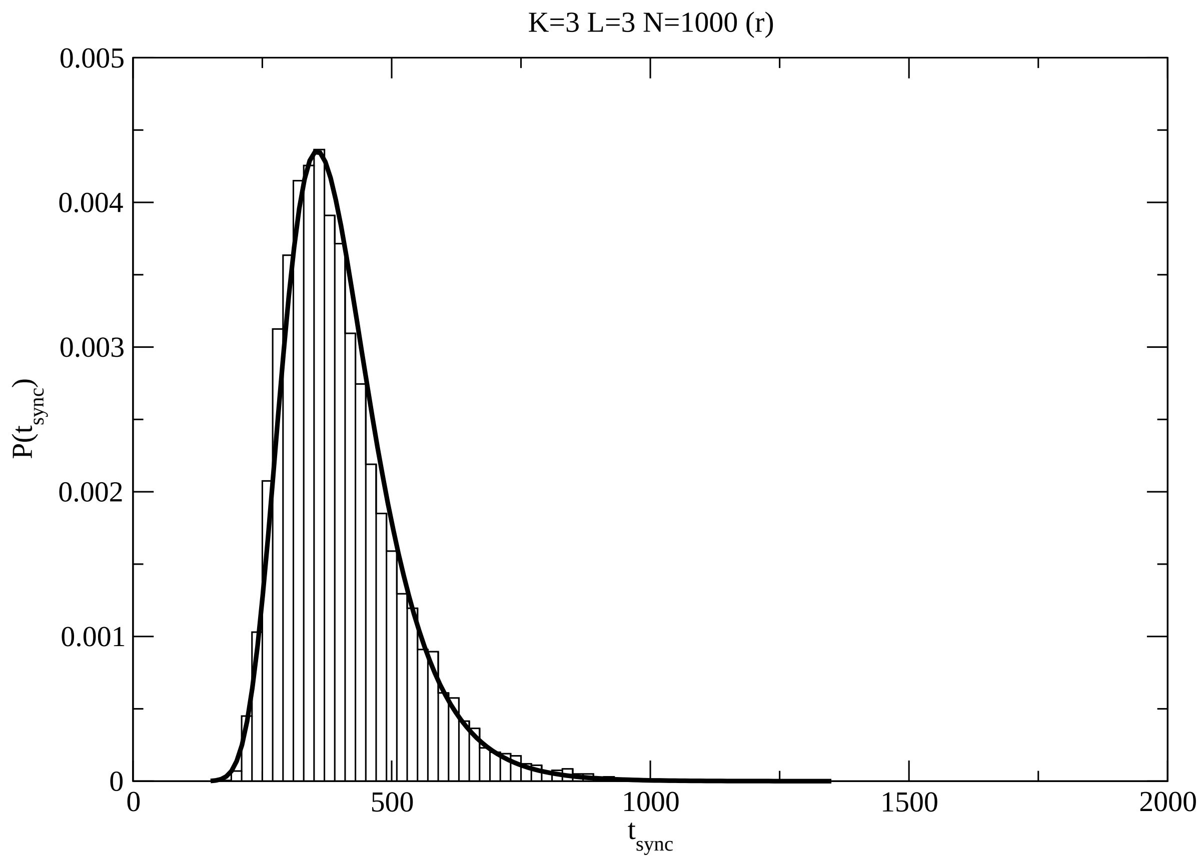

Discrete weights

$w_{k,i},\ k = 1, 2, 3,\ i = 1, ..., N,\ w_{k,i} \in \{-L, -L+1, ..., L-1, L\}$

$$\sigma_k = \text{sign}(\mathbf{w}_k \cdot \mathbf{x}_k), \quad \tau = \sigma_1 \sigma_2 \sigma_3$$

Secret key: Common time dependent weights $\mathbf{w}^A = \mathbf{w}^B$ after synchronization

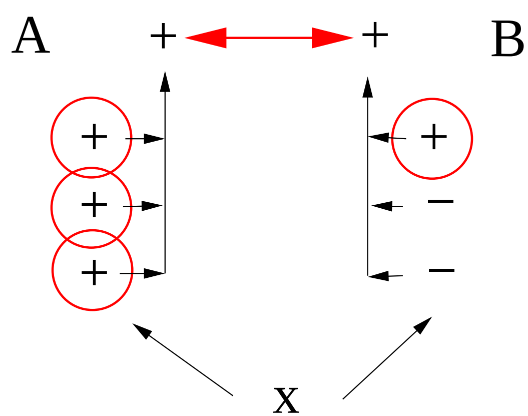
# Distribution of synchronization times



# Learning rule

Each participant has three units $k = 1, 2, 3$ and one output bit, which is sent to its partner,

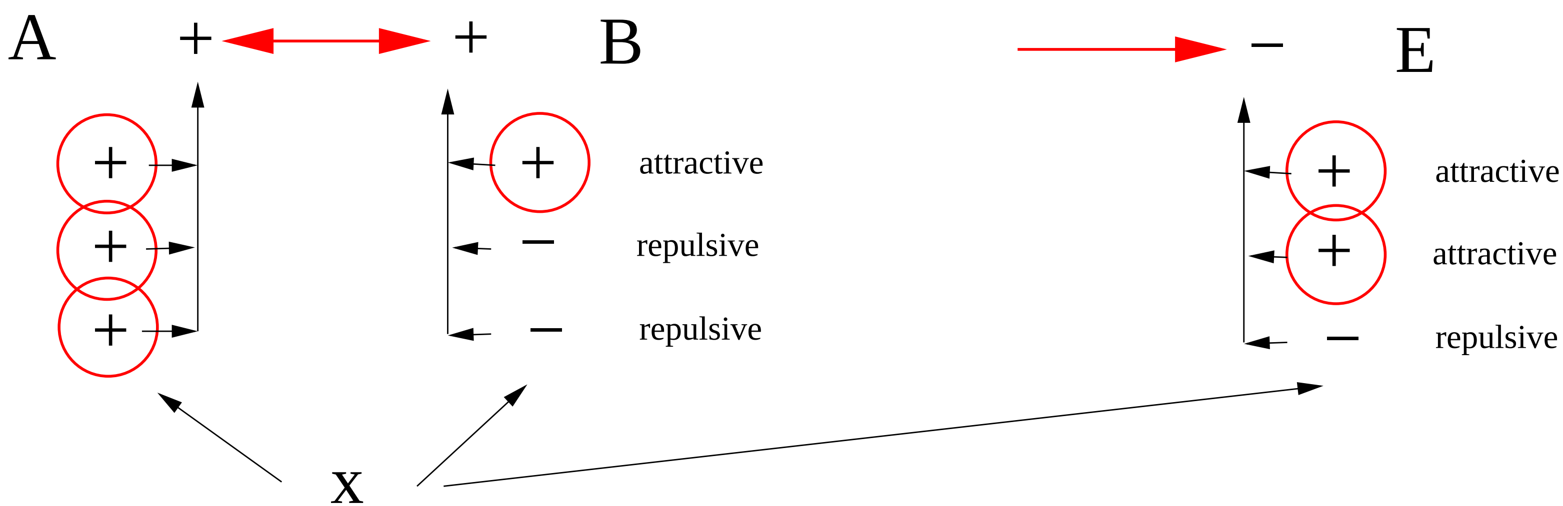
$$\tau^A = \sigma_1^A \cdot \sigma_2^A \cdot \sigma_3^A \qquad \tau^B = \sigma_1^B \cdot \sigma_2^B \cdot \sigma_3^B$$




Rule for A: If $\tau^A \neq \tau^B$ then do not move.
If $\sigma_k^A = \tau^A$ then move unit $k$.

# Stochastic forces

$\varepsilon$ = probability that two corresponding hidden units are different, synchronisation: $\varepsilon = 0$




Prob(A/B repulsive) $\propto \varepsilon^2$
Prob(A/E repulsive) $\propto \varepsilon$

# Scaling for large key size $N$

Average synchronisation time between A and B:

$$t_{sync} \propto L^2$$

Probability that an attacker E synchronises with A and B:

$$P_E \propto e^{-yL}$$

Security for $L \to \infty$

# Ongoing research

Advanced algorithms versus advanced attacks

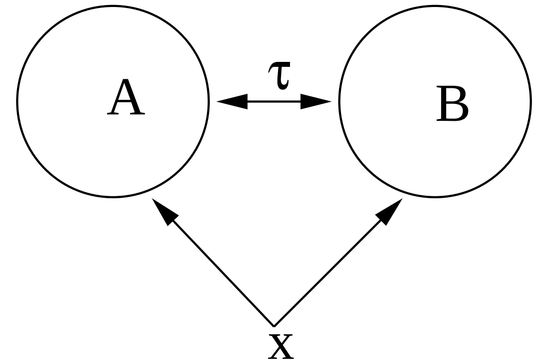
- Combination with chaotic maps
- Inputs from feeback
- Inputs with restrictions (queries)
- Attacking by ensembles
- Attacking by genetic algorithms

See 12 common publications since 2002

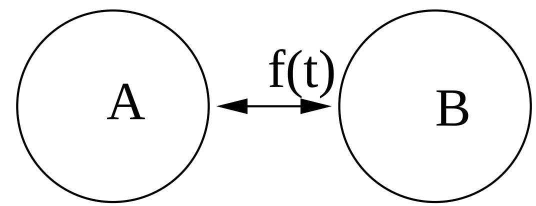
- Hardware: 20000 keys per second on an tiny chip
  Volkmer, Wallner, IEEE Trans. Comp. 2005

# Nonlinear dynamics

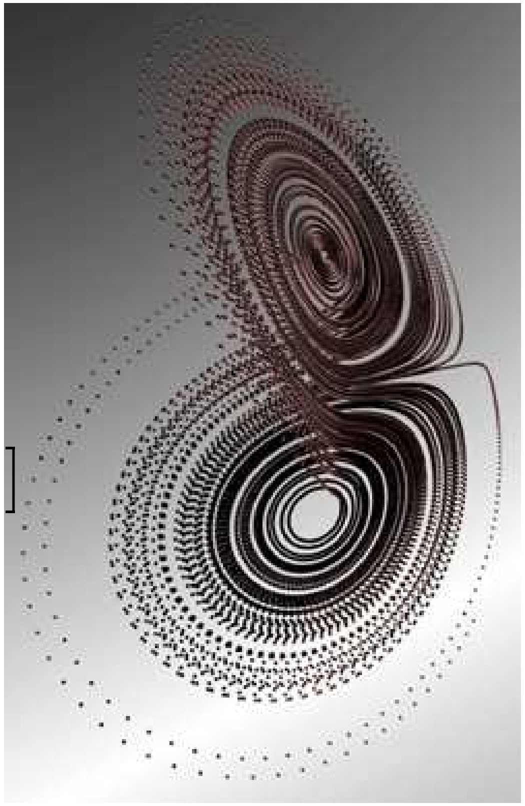
Neural cryptography




Synchronization of chaotic systems



# Lorenz equations

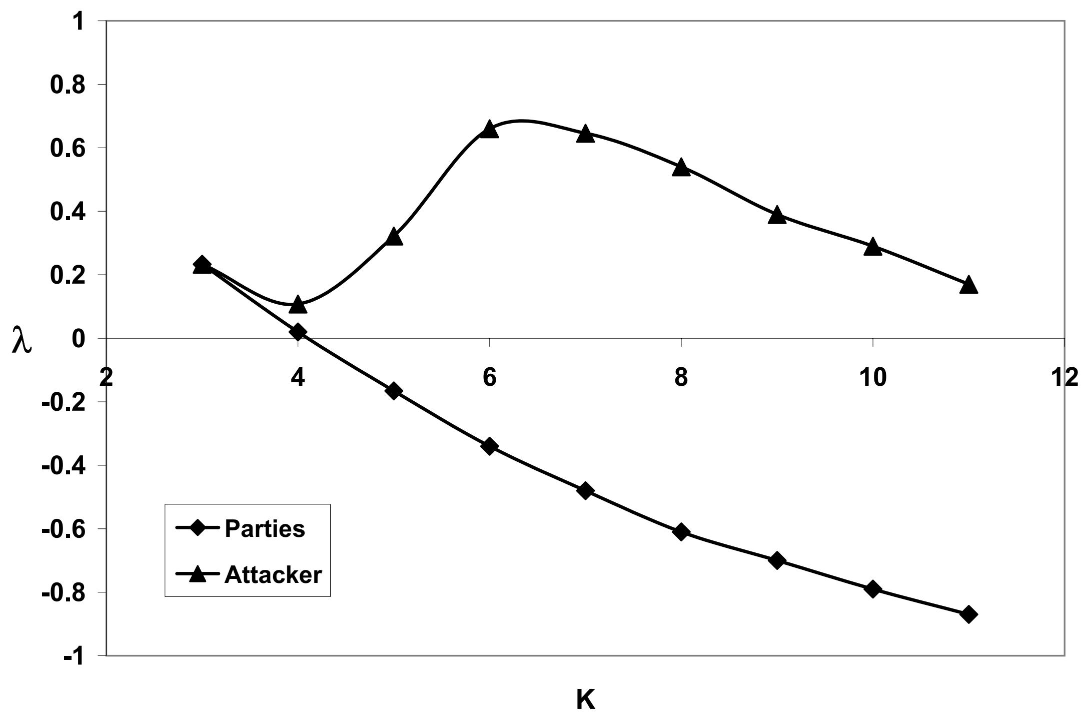


$$\frac{dx_A}{dt} = 10(y_A - x_A) + K[f_B(t) - f_A(t)]$$
$$\frac{dy_A}{dt} = 28x_A - y_A - x_A z_A$$
$$\frac{dz_A}{dt} = x_A y_A - \frac{8}{3} z_A$$
$$f_A(t) = x_A(t-\tau_1) + \text{sign}(x_A(t-\tau_1))\, A\, (x_A(t-\tau_1) - x_A(t-\tau_2$$

Exchange signal $f(t)$: nonlinear and time-delayed

# Synchronization

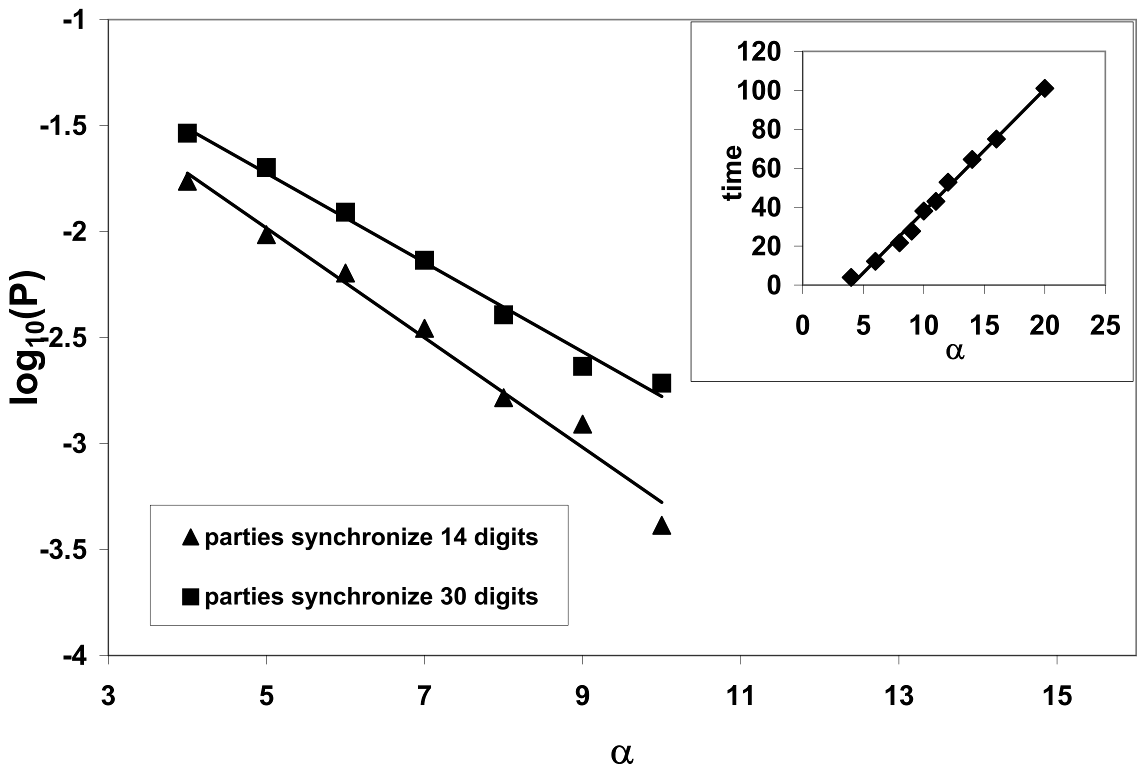
Lyapunov exponent $\lambda$:




Synchronization is possible for a limited range of coupling strenght $K$ and delay times $\tau_i$.

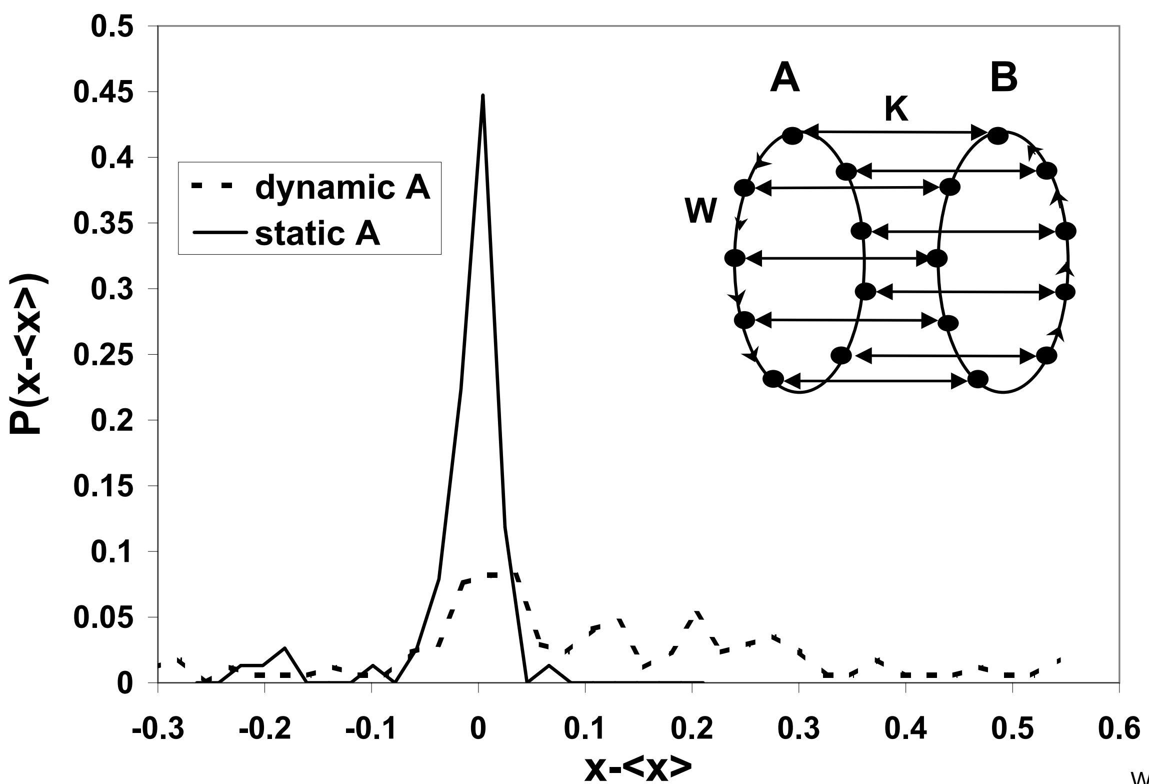
# Attack 1

Synchronization of single Lorenz systems:
Success probability $P$ and synchronization time $t$ as a function of the number $\alpha$ of recognized digits of $x_A(t)$.



# Attack 2

Calculating $x_A(t)$ from $f_A(t)$:
Record $F_A(t) = (f_A(t), f_A(t-\tau), f_A(t-2\tau))$ and measure the volume in $x$ space which belongs to a tiny volume in $F$-space.

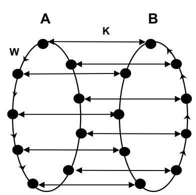


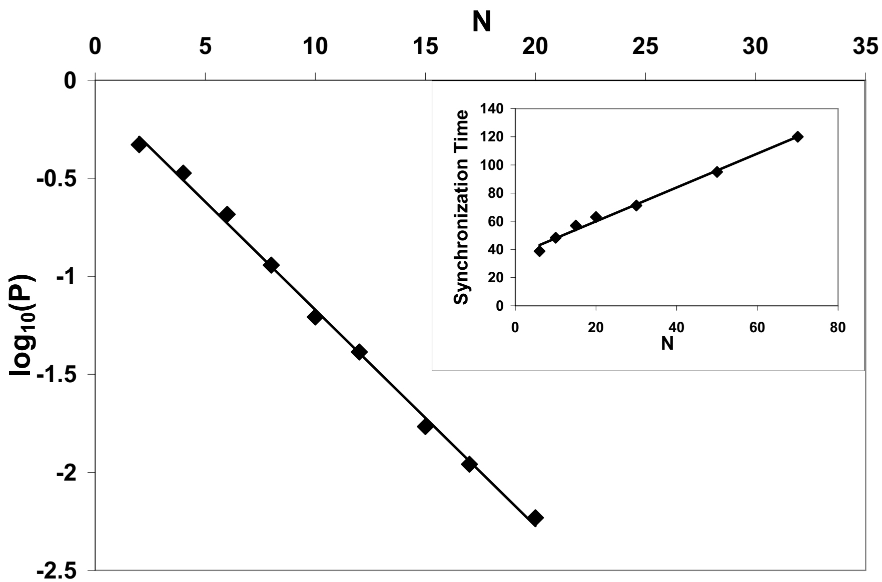
# Improving security

- Dynamic amplitude of the nonlinearity of $f_A(t)$:

$$A(t) = \frac{1}{C_1\,|f_A(t) - f_B(t)|^\rho + C_2}$$

- Ring of $N$ Lorenz equations with directed internal couplings $W$.



# Summary

- Secret keys can be generated over public channels by physical mechanisms.
- Neural Cryptography:
  - Mutual learning of neural networks
  - Stochastic attractive and repulsive forces
  - Scaling relation for the security
  - Fast and simple
  - many keys per transaction
  - realization in small chips
- Lorenz Synchronization:

- Lorenz Synchronization:
  - Synchronization of chaotic differential equations with nonlinear and time-delayed couplings
  - Scaling relation for the security
  - Analog signals
  - Electronic circuits, chaotic lasers