The development of Public Key Cryptography *a personal view*

Ralph C. Merkle

Georgia Tech College of Computing

Fall 1974

- No terminology
- No understanding of problem
- Talking with people about the problem now called public key distribution produced confusion

Fall 1974

- **Undergraduate at Berkeley**
- **Enrolled in CS 244, "Computer Security Engineering," Lance Hoffman**
- **Required to submit two project proposals**
  - —One was data compression.
  - —The other….

Fall 1974

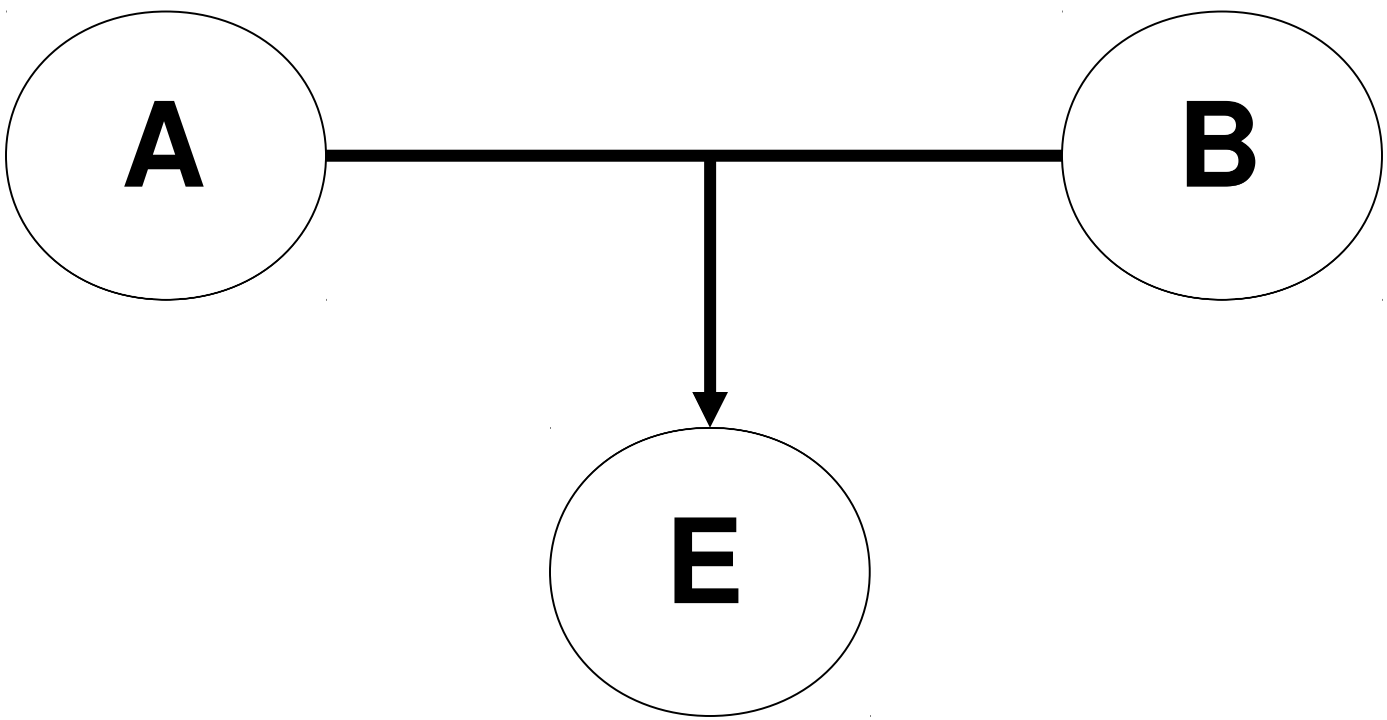
- One way functions could protect passwords even if system security were completely compromised
- But encryption keys, once compromised, required establishing new keys
- Could new keys (between e.g. a terminal and the system) be established over normal channels?

Fall 1974

- **This is the public key distribution problem.**
- **First thought: this must be impossible, let’s prove that it can’t be done**
- **Easy to prove that PKD is impossible if either communicant is fully deterministic and I/O is monitored.**

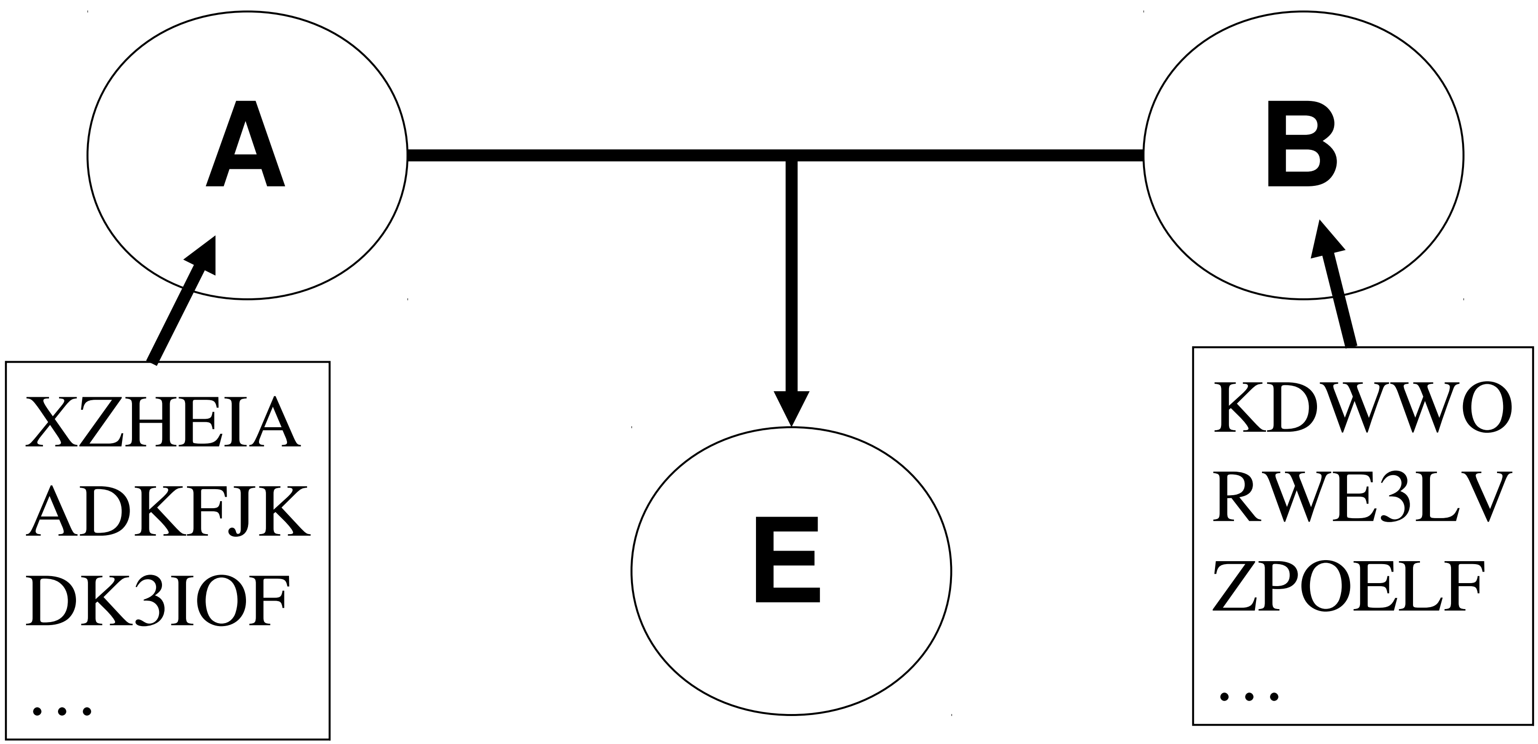
Fall 1974

PKD impossible if
A or B is deterministic



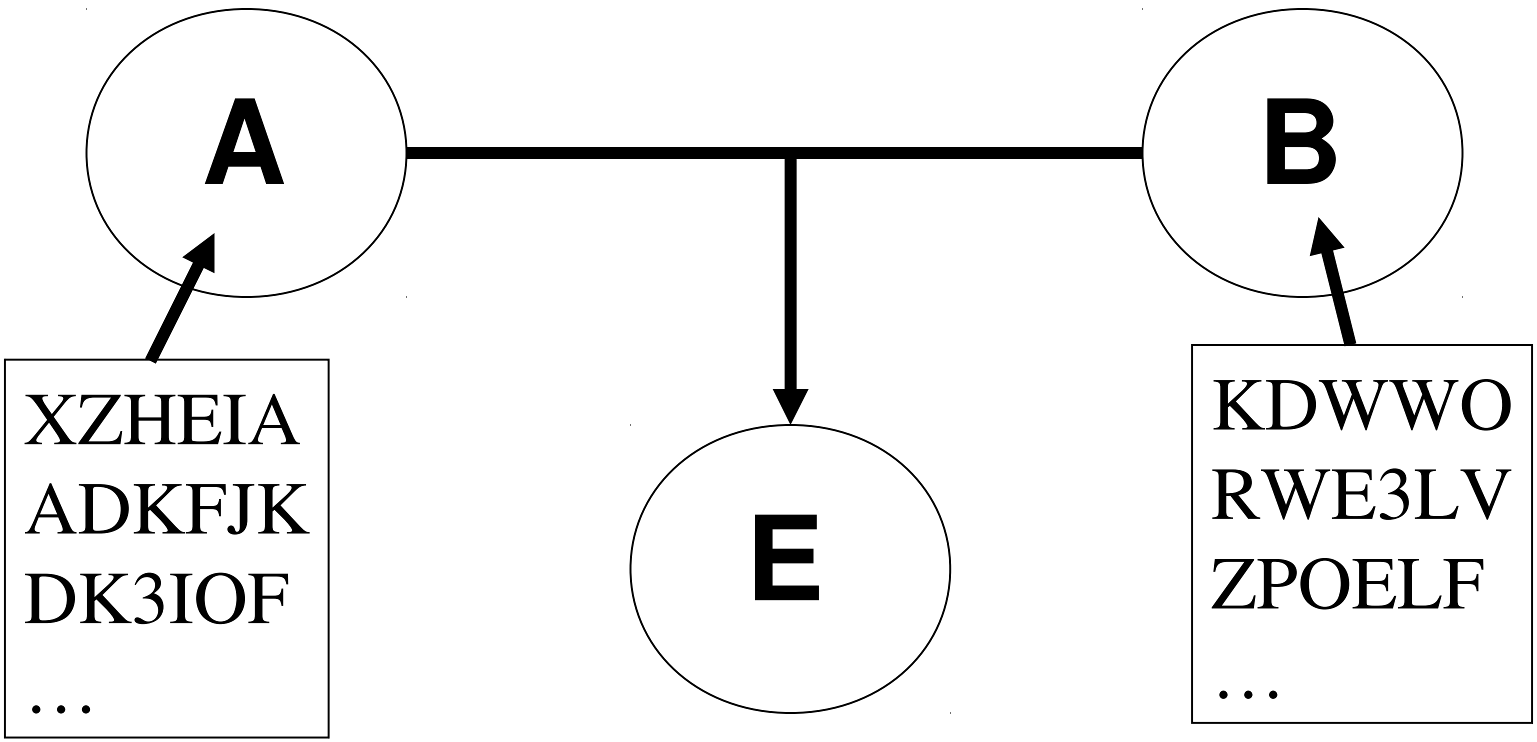
Fall 1974

But what if A and B
both have random number generators?



Fall 1974

How do A and B
differ from E?

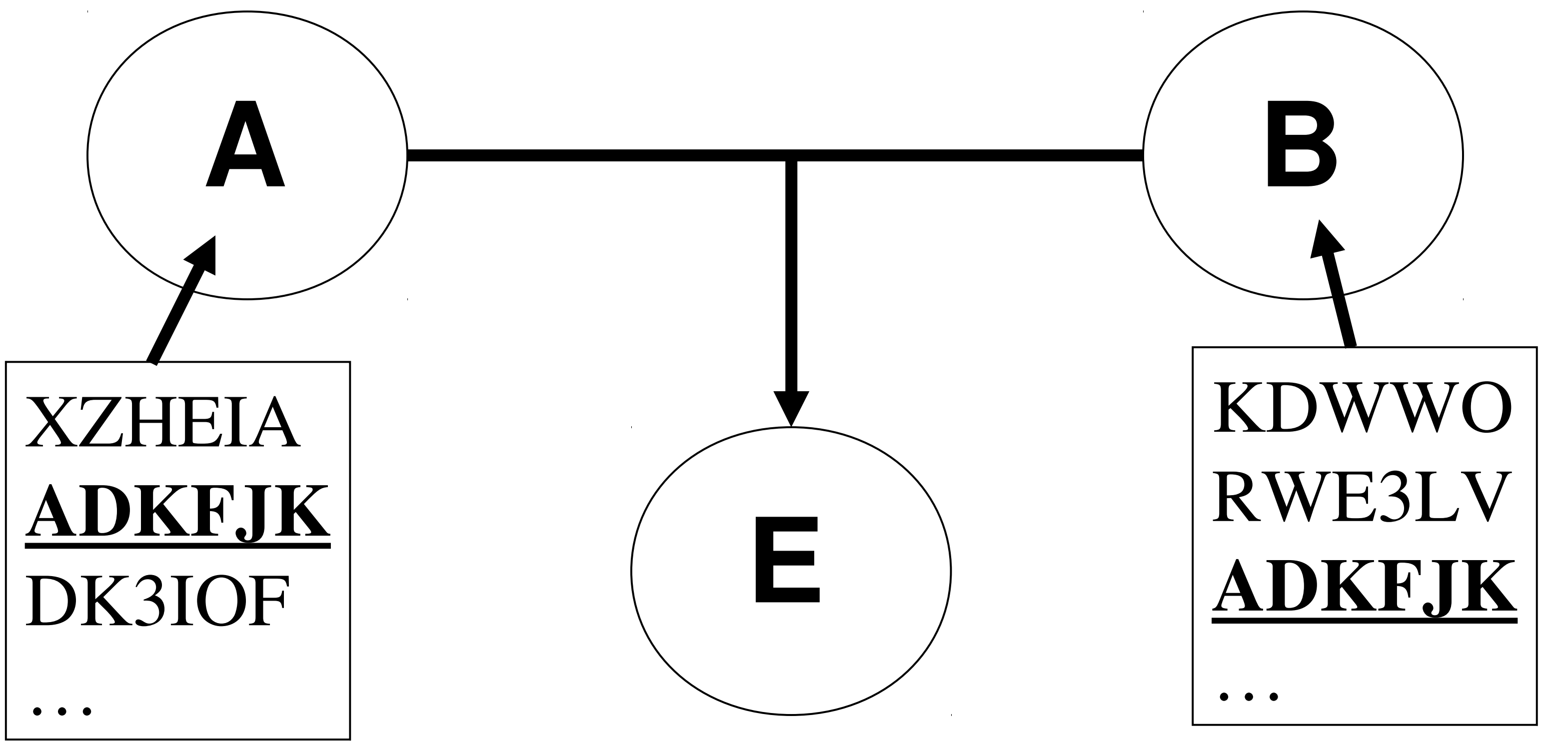


Fall 1974

- Failed to prove PKD impossible if random numbers are provided
- Switched gears – how to do it
- Aha! A and B might generate the same random number by chance!

Fall 1974

By chance, A and B
might generate the same number



Fall 1974

- **If A and B select N random numbers from a space of N^2 possible numbers, there is a good probability of a collision.**
- **So just keep picking random numbers until a collision occurs, which it will with high probability if A and B keep generating random numbers**

Fall 1974

- But how to detect a collision?
- Have A apply a one way function F to each random number r_i, and send $F(r_i)$ to B
- B applies the same one way function to his random numbers and looks for a collision.
- When B finds a collision, A and B are in possession of a common key

Fall 1974

- The enemy, E, saw ~N values $F(r_i)$ go from A to B, and saw one value $F(r_{common})$ returned from B to A.
- Total effort by both A and B was about N.
- Total effort by E to analyze r_{common} will be about N^2.

Fall 1974

- This was the method as first conceived, and best illustrates the development of the idea
- The method as published is different, using “puzzles” to minimize both A and B’s storage requirements (which in the simple method are ~N)

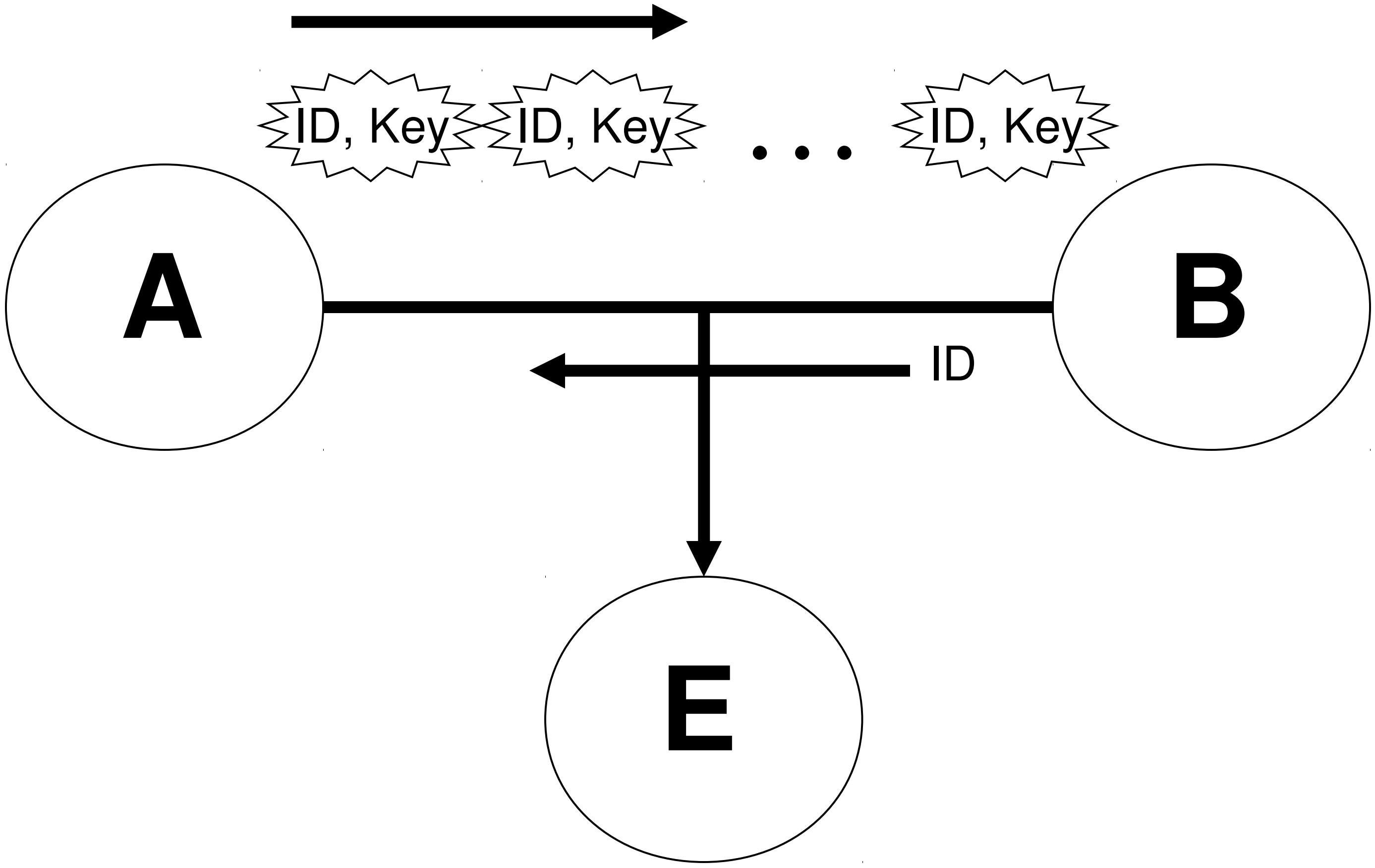
Puzzles

- **Puzzles are created by selecting a random key from one of N possibilities, then encrypting a random puzzle id, a random cryptographic key, and some redundant information.**
- **A puzzle is broken by exhaustively searching the space of N possible keys**

Puzzles

- A creates N puzzles and sends them to B
- B randomly selects one puzzle, discarding all the others
- B spends ~N effort to crack the chosen puzzle
- B sends the puzzle ID back to A

Puzzles



Idea meets people

- **New ideas are typically rejected, and so it was with this strange key distribution problem and CS 244: after repeated rejection I dropped the course**
- **But kept working on the idea.**

Idea meets people

- **Among others, I explained the puzzles method to Peter Blatman who, as it happened, knew Whit Diffie.**

Idea meets people

- **“I was convinced you couldn't do it [PKD] and I persuaded Blatman you couldn't do it. But I went back to thinking about the problem. And so I think Merkle plays a very critical role.”**

  —Whitfield Diffie, circa 1974/1975

Idea meets people

- **Sounding out faculty members at Berkeley produced mostly negative results (i.e., “No, I couldn’t supervise a thesis in this area because <fill in blank>”)**
- **Bob Fabry, however, read my draft paper and said “Publish, win fame and fortune!”**
- **So I submitted to CACM in August 1975**

Idea meets people

- The response from CACM:
- "Enclosed is a referee report by an experienced cryptography expert on your manuscript…"
- "I am sorry to have to inform you that the paper is not in the main stream of present cryptography thinking and I would not recommend that it be published…"

Linking up

- **February 7th 1976: "About 3 days ago, a copy of your working paper, Multiuser Cryptographic Techniques, fell into my hands."**
- **And the rest is history**

Some thoughts on nanotechnology

Crypto and nano

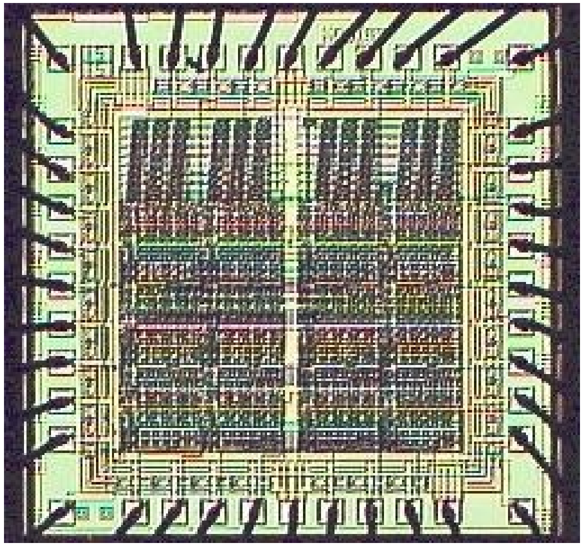
Today's crypto systems must resist attack by tomorrow's computers

Nanotechnology explores the limits of what we can make

Future computers will likely benefit decisively from nanotechnology

Arranging atoms

- Flexibility
- Precision
- Cost



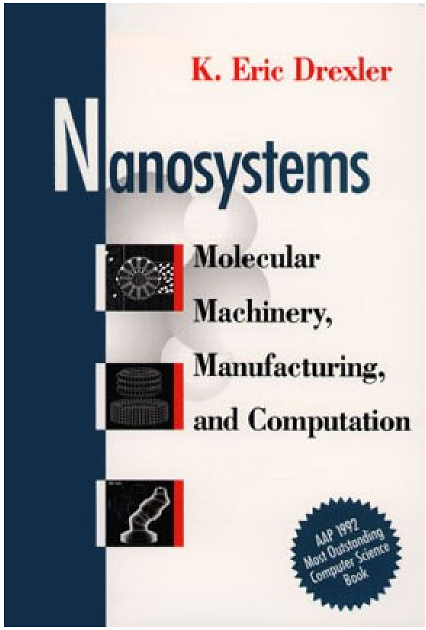
Richard Feynman,1959

There's plenty of room at the bottom

http://www.zyvex.com/nanotech/feynman.html

Experiment and theory

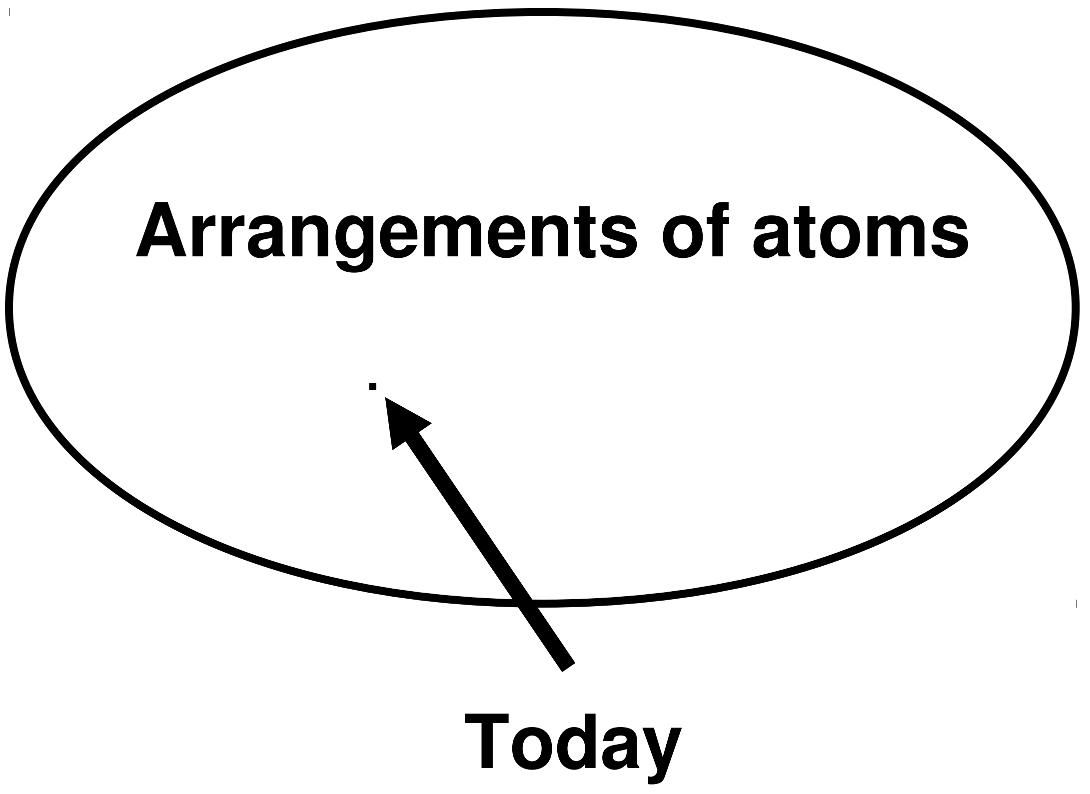
First STM
By Binnig and Rohrer



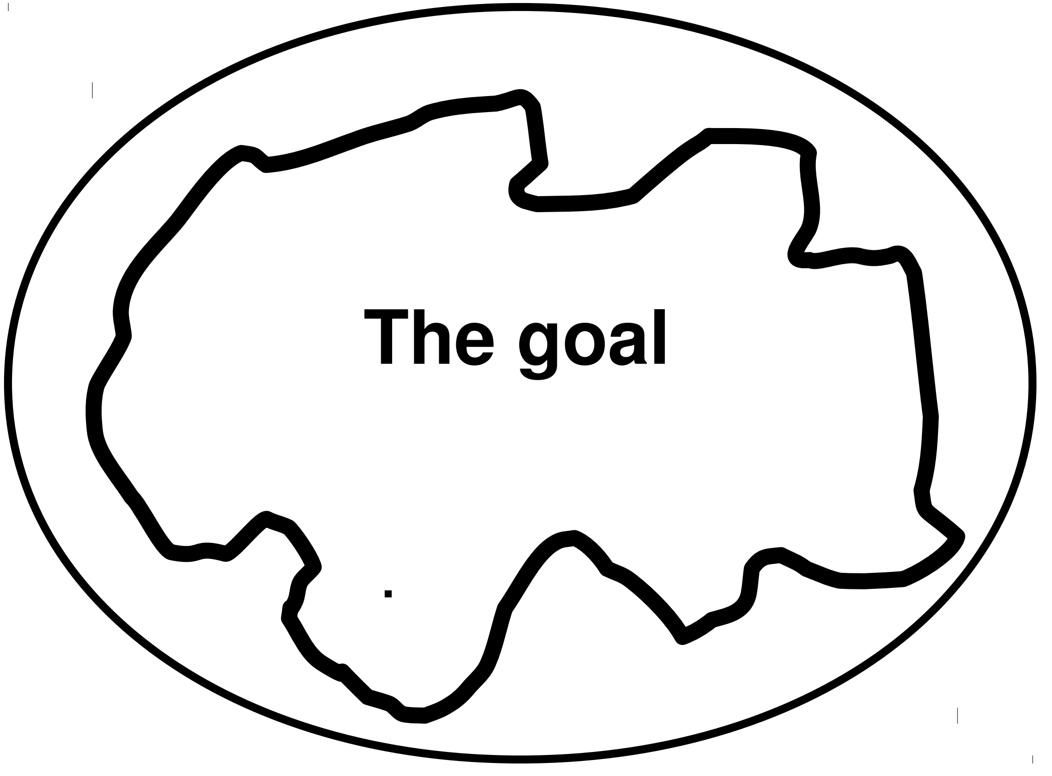
President Clinton, 2000

The National Nanotechnology Initiative

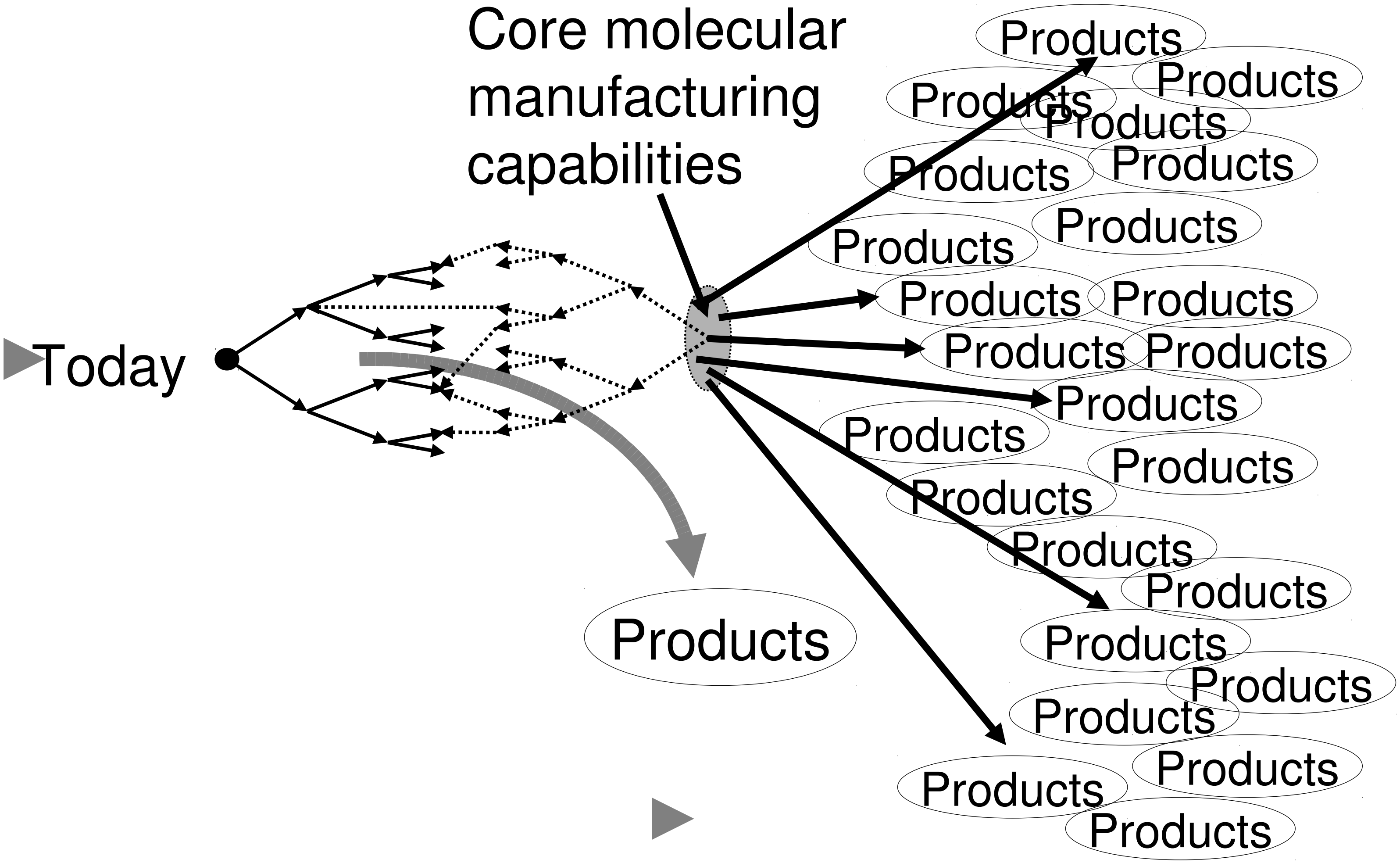
"Imagine the possibilities: materials with ten times the strength of steel and only a small fraction of the weight -- shrinking all the information housed at the Library of Congress into a device the size of a sugar cube -- detecting cancerous tumors when they are only a few cells in size."


Arrangements of atoms
Today

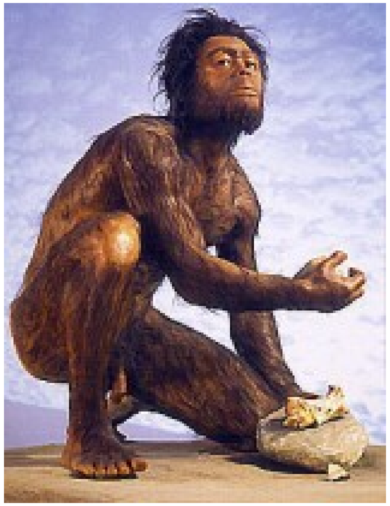
The goal

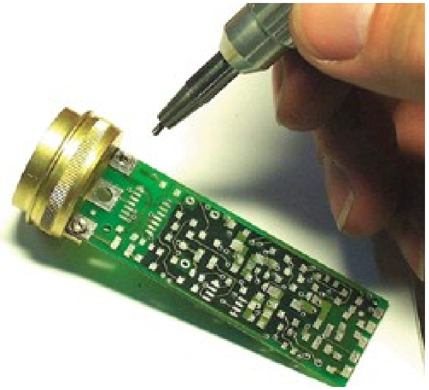


Many routes

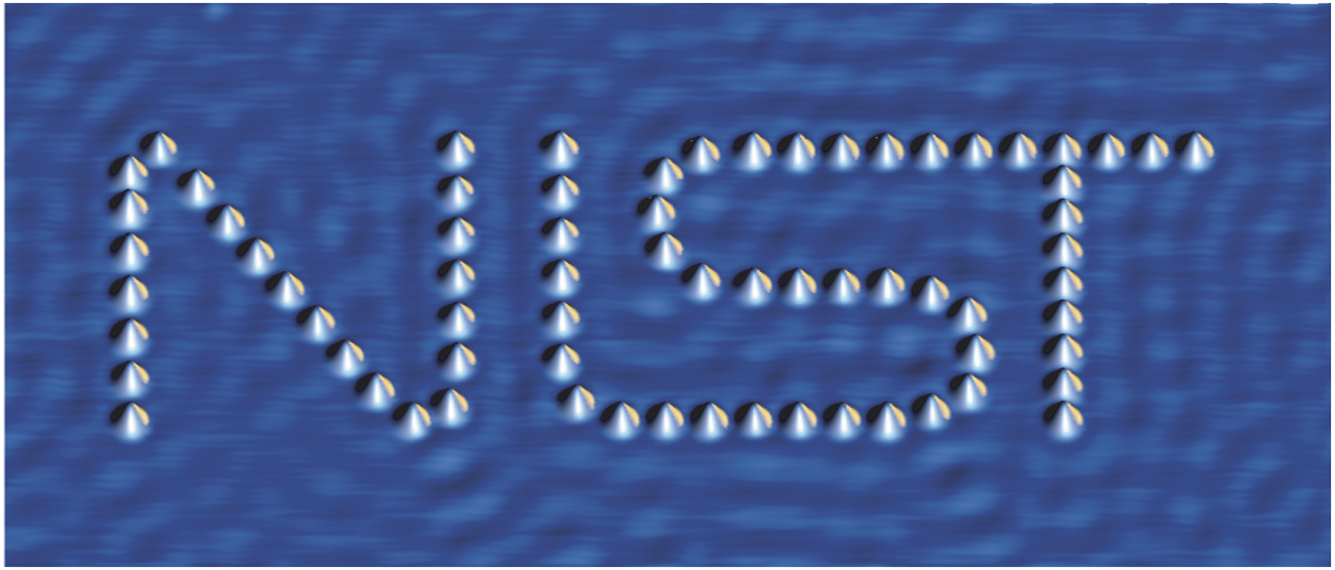

Core molecular manufacturing capabilities
Today
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products

A powerful method: positional assembly



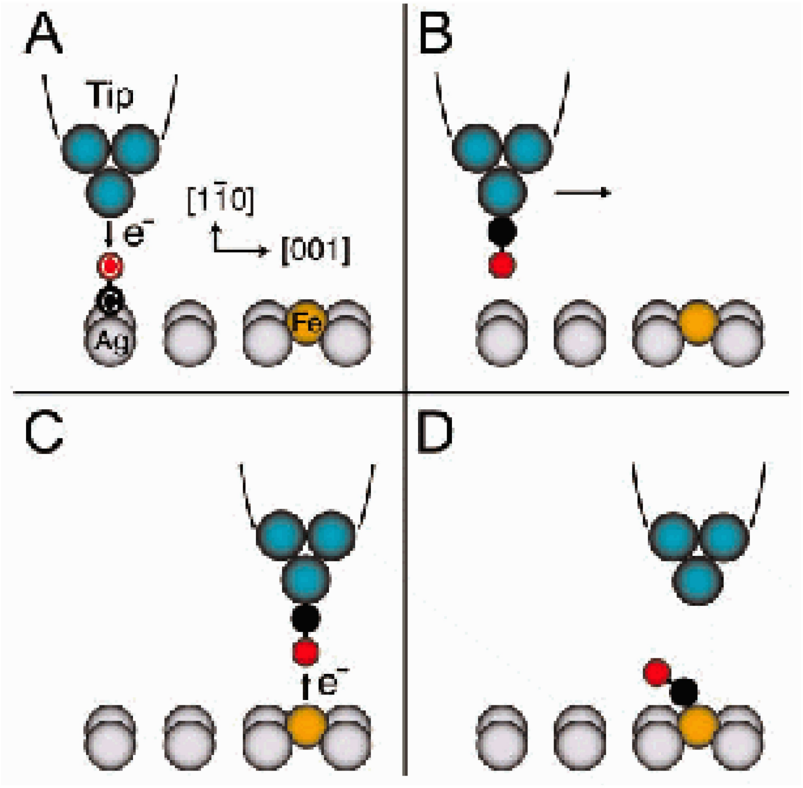
Experimental



A 40-nanometer-wide NIST logo made with cobalt atoms on a copper surface

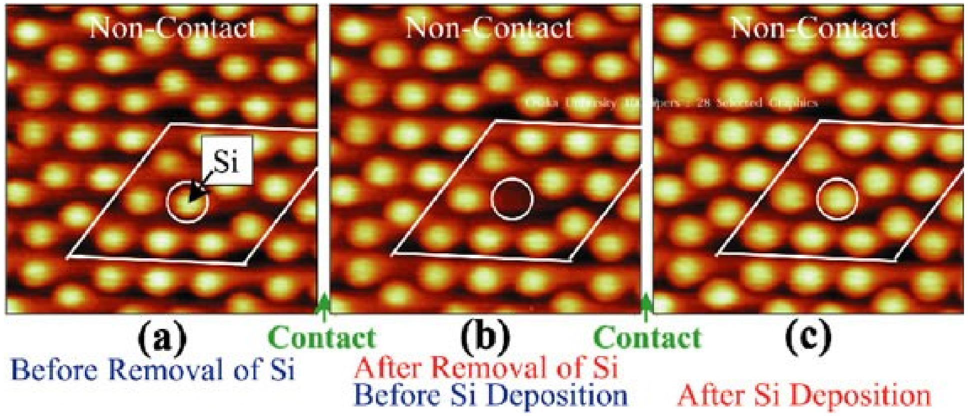
Controlling the Dynamics of a Single Atom in Lateral Atom Manipulation
Joseph A. Stroscio and Robert J. Celotta, Science, Vol 306, Issue 5694, 242-247, 8 October 2004
http://www.nist.gov/public_affairs/releases/hiphopatoms.htm

Experimental



H. J. Lee and W. Ho, SCIENCE **286,** p. 1719, NOVEMBER 1999

Experimental



Mechanical vertical manipulation of selected single atoms by soft nanoindentation using near contact atomic force microscopy, Noriaki Oyabu, Oscar Custance, Insook Yi, Yasuhiro Sugawara, Seizo Morita1, *Phys. Rev. Lett.* 90(2 May 2003):176102.

Theoretical

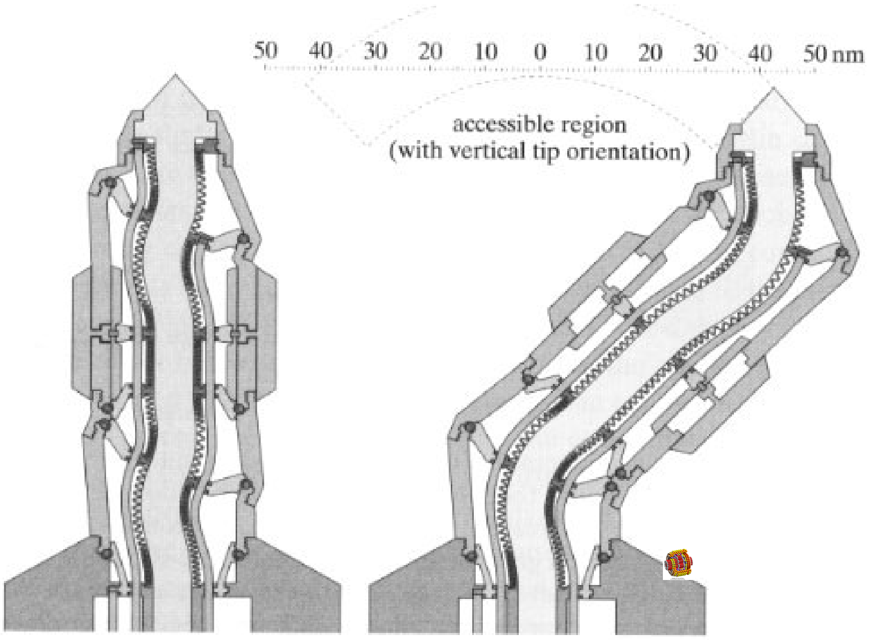
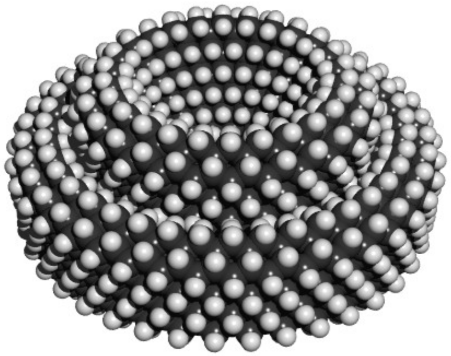
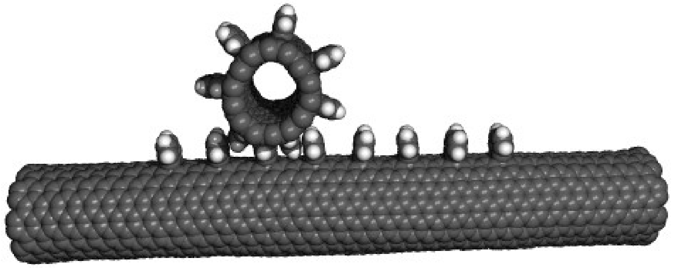
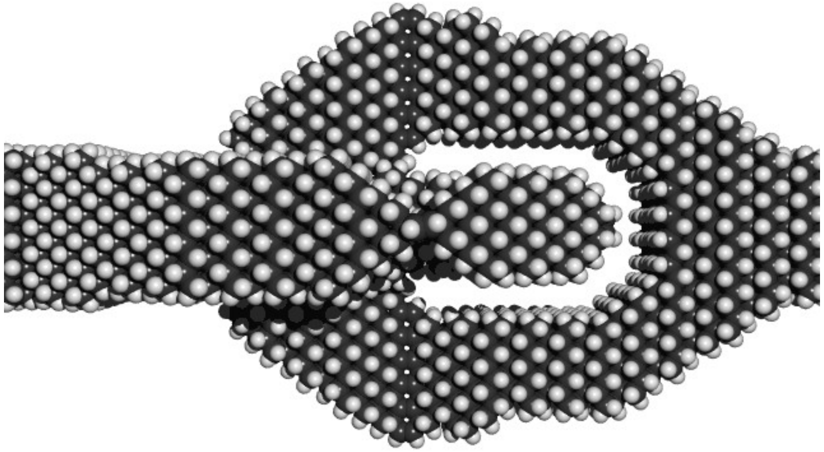


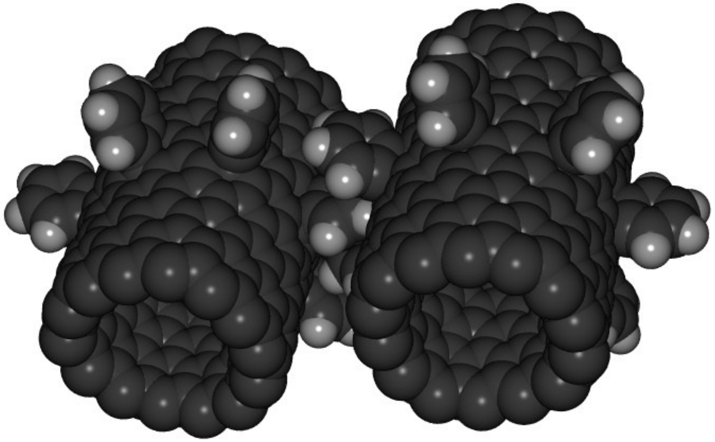
Figure 13.14. Cross section of a stiff manipulator arm, showing its range of motion (schematic).

Hydrocarbon machines

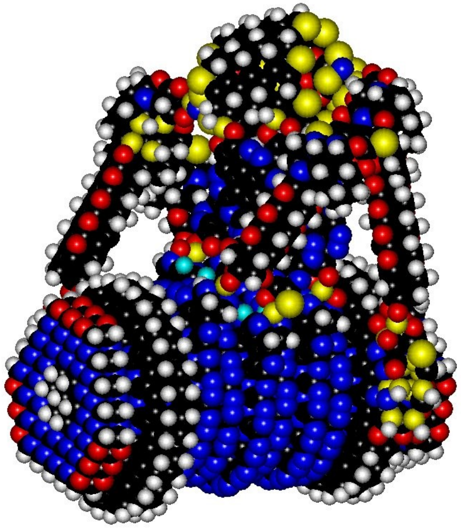


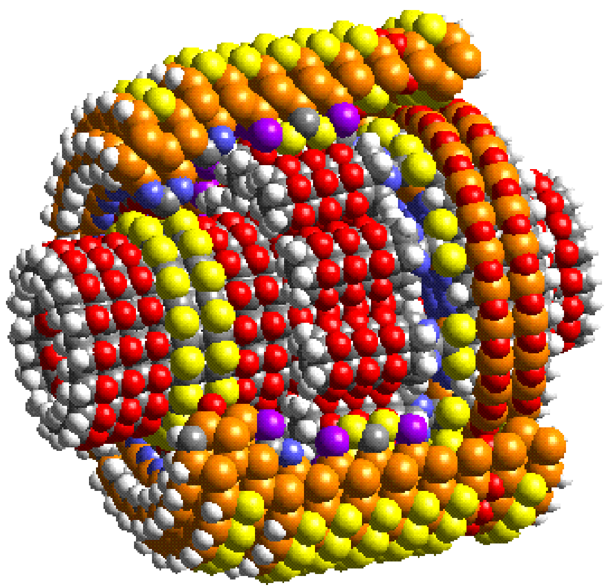


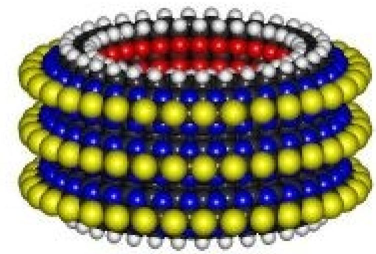


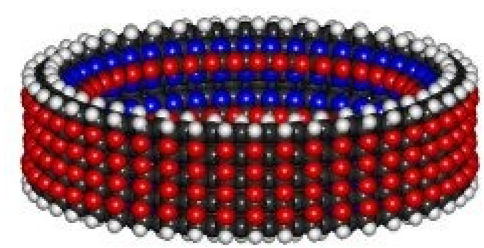


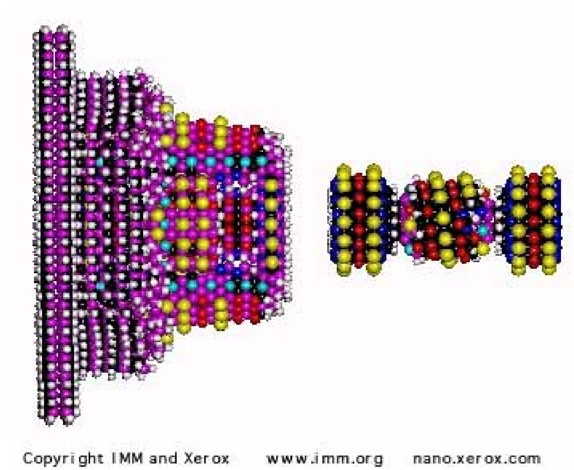
Molecular machines











Molecular robotics

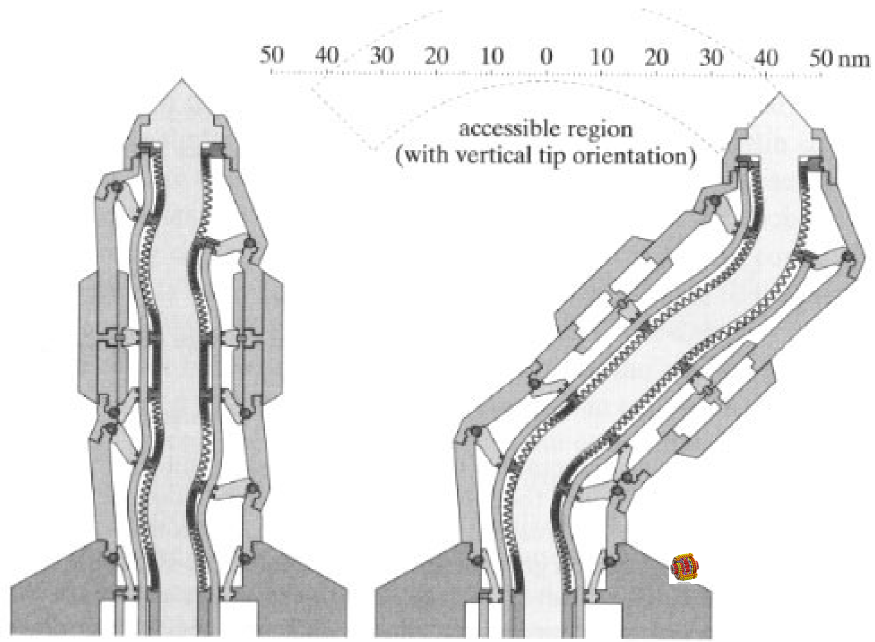


Figure 13.14. Cross section of a stiff manipulator arm, showing its range of motion (schematic).

Diamond physical properties

Property	Diamond's value	Comments
Chemical reactivity		Extremely low
Hardness (kg/mm2)	9000	CBN: 4500 SiC: 4000
Thermal conductivity (W/cm-K)	20	Ag: 4.3 Cu: 4.0
Tensile strength (pascals)	3.5×10^{9} (natural)	10^{11} (theoretical)
Compressive strength (pascals)	10^{11} (natural)	5×10^{11} (theoretical)
Band gap (ev)	5.5	Si: 1.1 GaAs: 1.4
Resistivity (W-cm)	10^{16} (natural)	
Density (gm/cm3)	3.51	
Thermal Expansion Coeff (K-1)	0.8×10^{-6}	SiO2: 0.5×10^{-6}
Refractive index	2.41 @ 590 nm	Glass: 1.4 - 1.8
Coeff. of Friction	0.05 (dry)	Teflon: 0.05

Source: Crystallume

Making diamond today

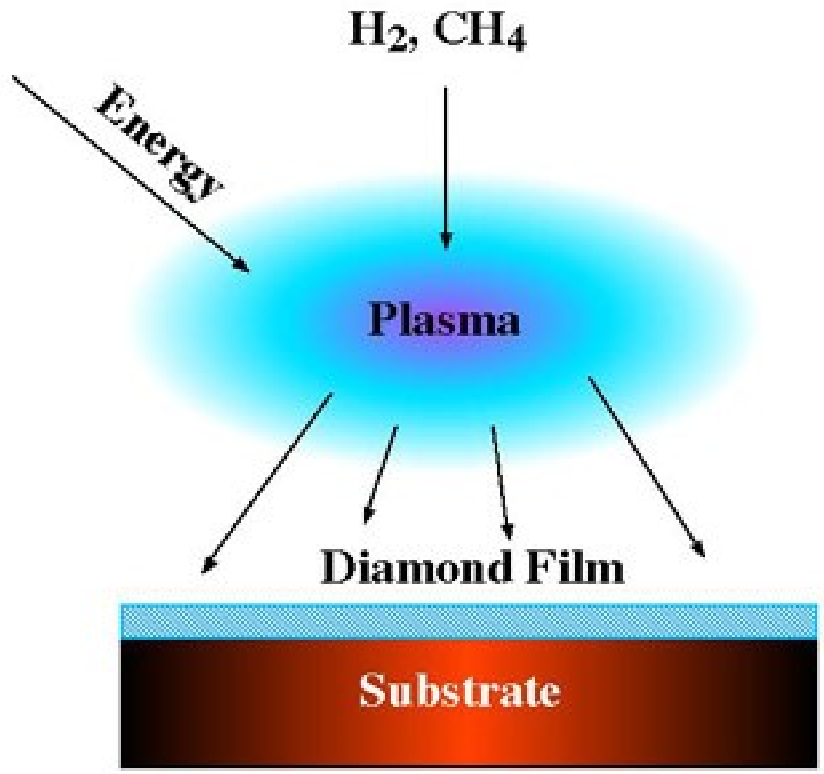
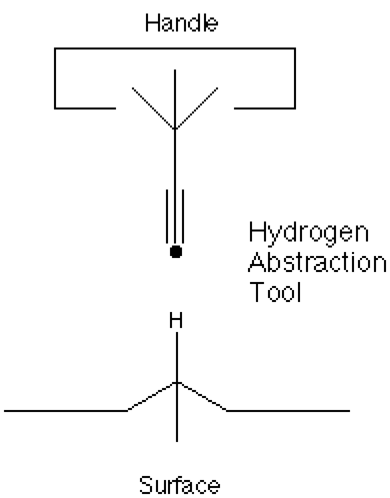
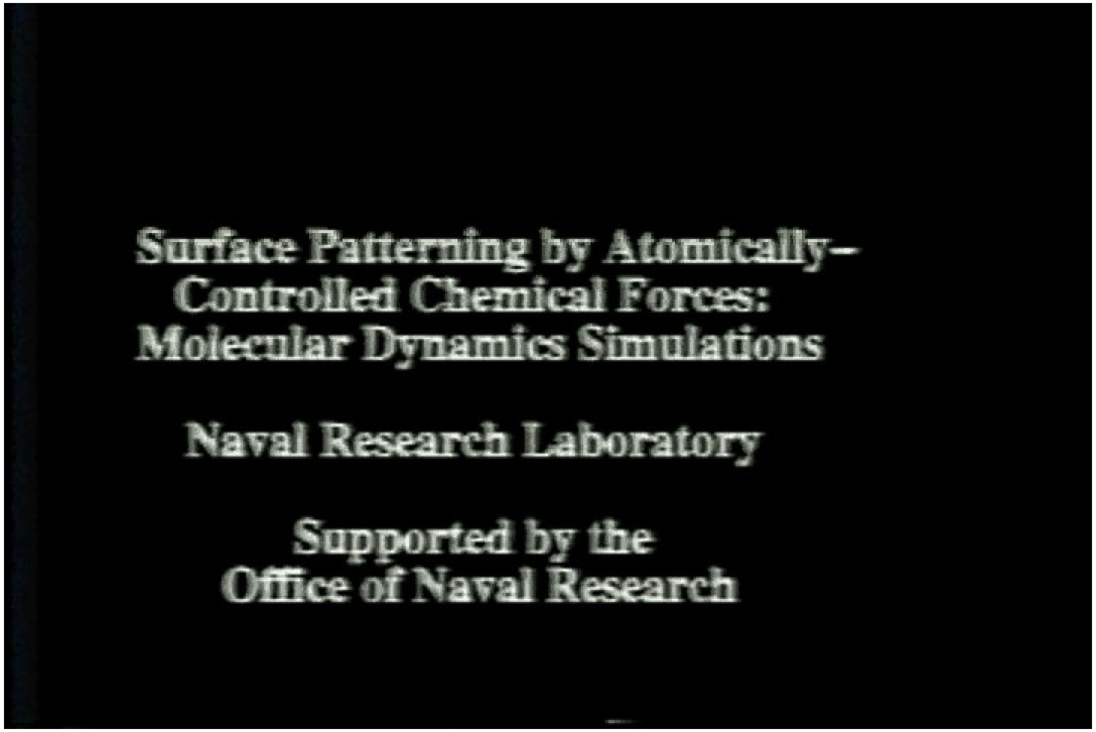


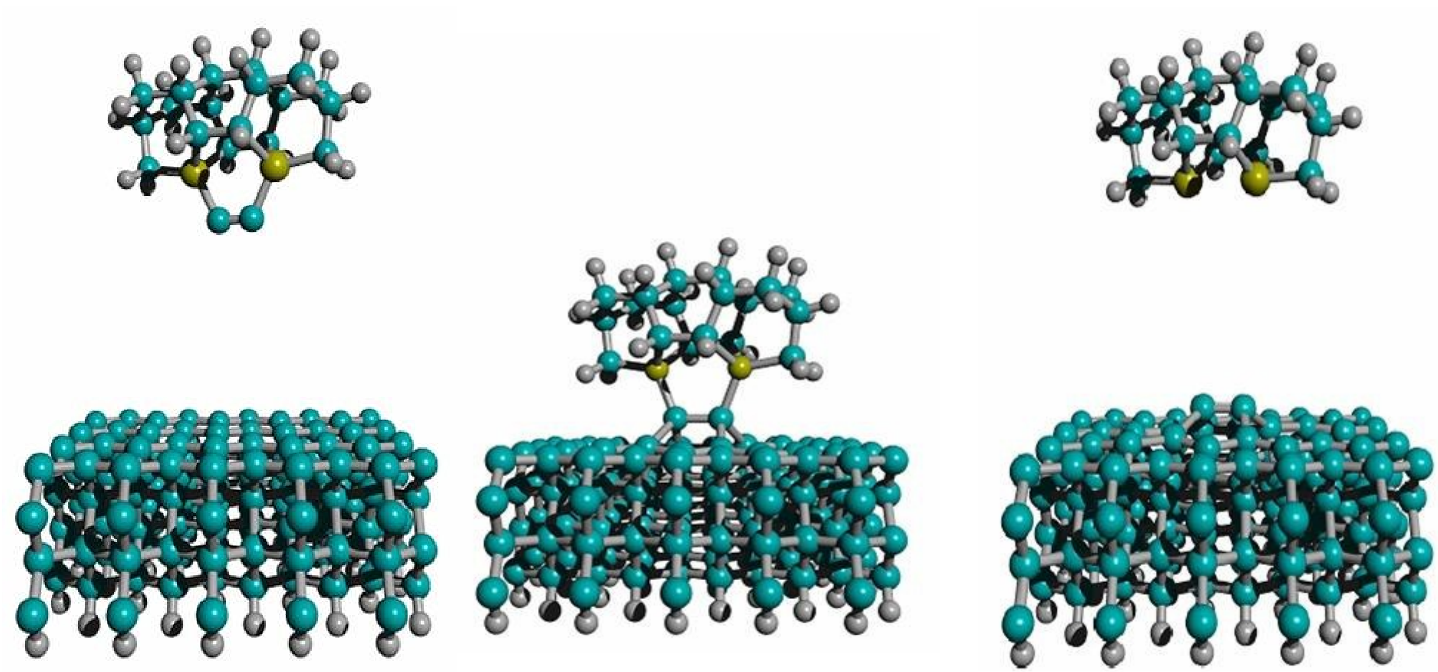
Illustration courtesy of P1 Diamond Inc.

Hydrogen abstraction tool



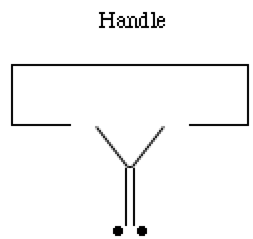


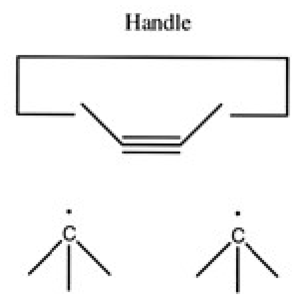
Adding carbon

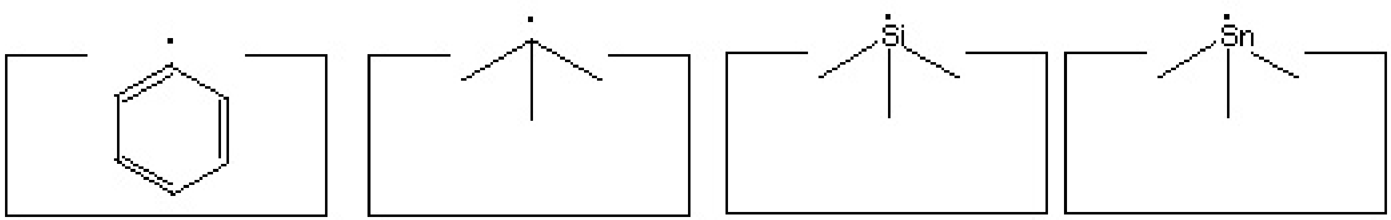


Theoretical Analysis of Diamond Mechanosynthesis. Part II. C2 Mediated Growth of Diamond C(110) Surface via Si/Ge-Triadamantane Dimer Placement Tools, J. Comp. Theor. Nanosci. 1(March 2004). David J. Mann, Jingping Peng, Robert A. Freitas Jr., Ralph C. Merkle, In press.

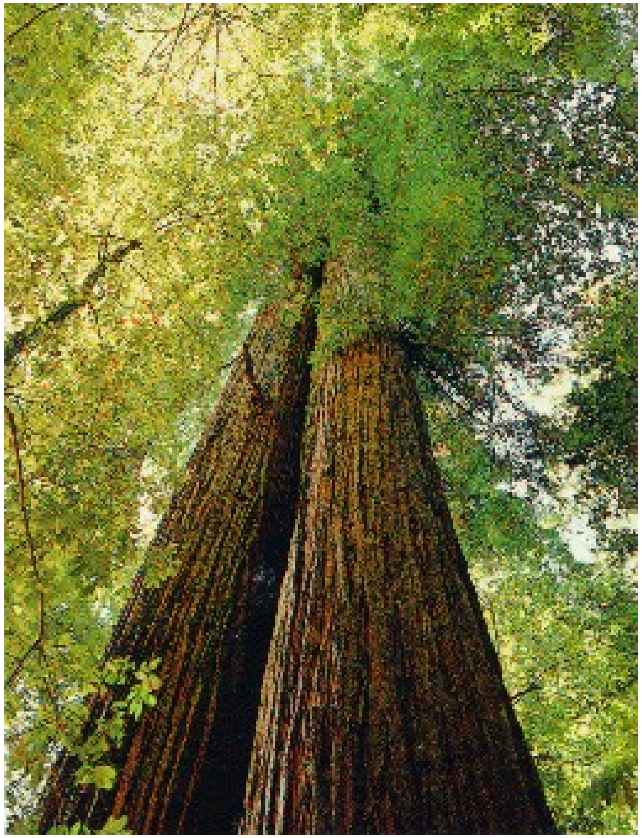
Other molecular tools







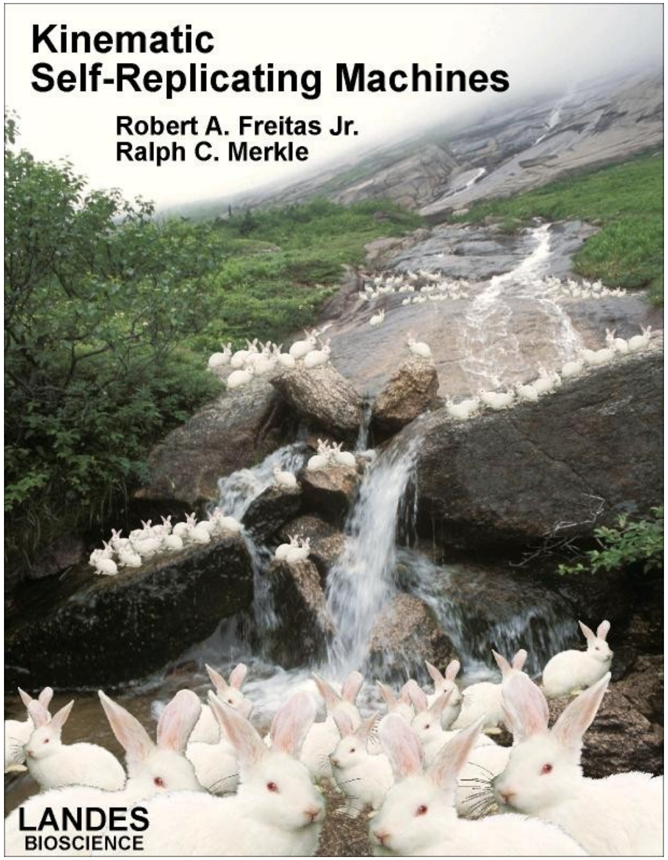
Self replication



A redwood tree
(*sequoia sempervirens*)
112 meters tall
Redwood National Park

http://www.zyvex.com/nanotech/selfRep.html

Self replication

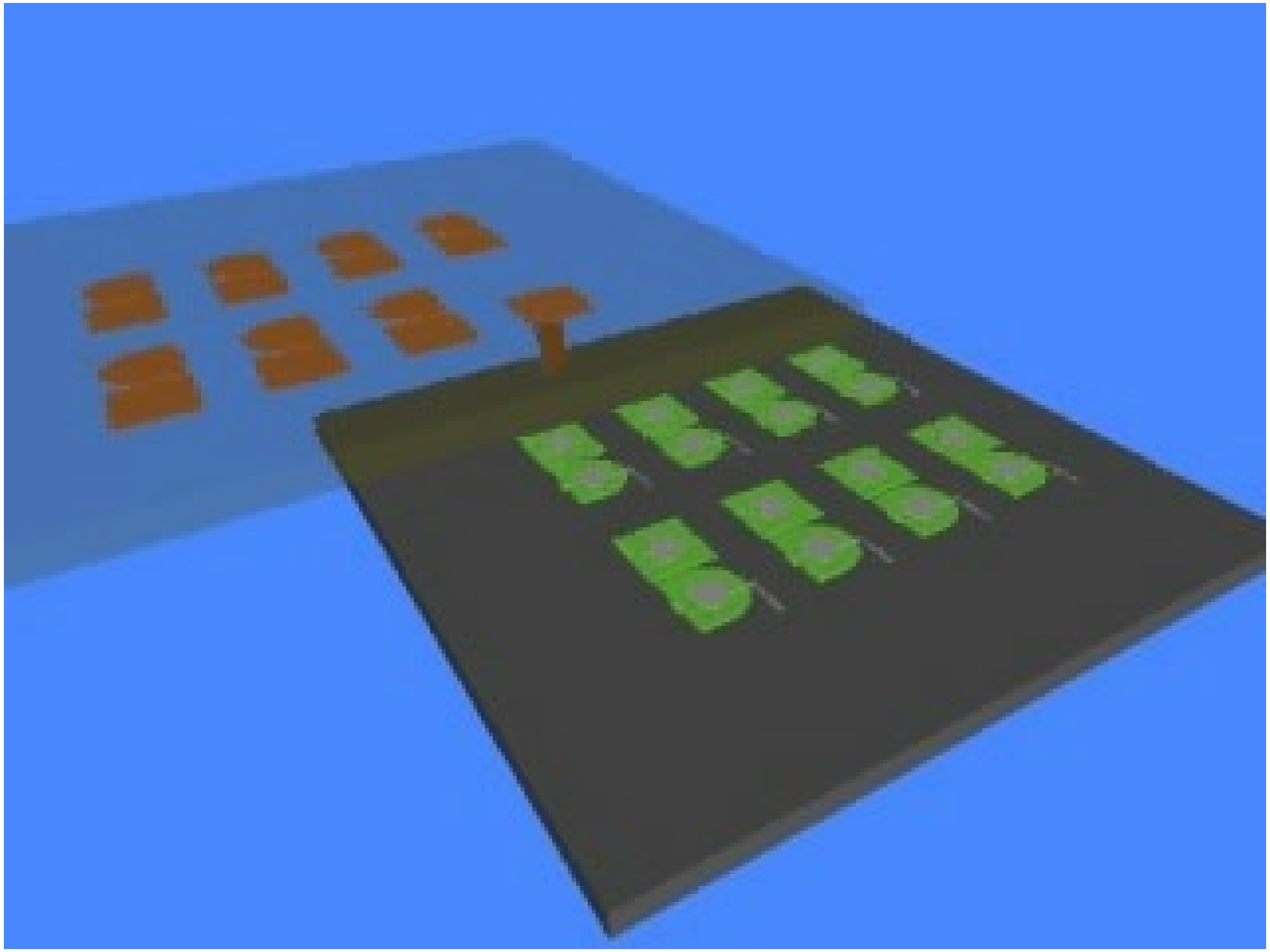


Kinematic
Self-Replicating Machines
(Landes Bioscience, 2004)

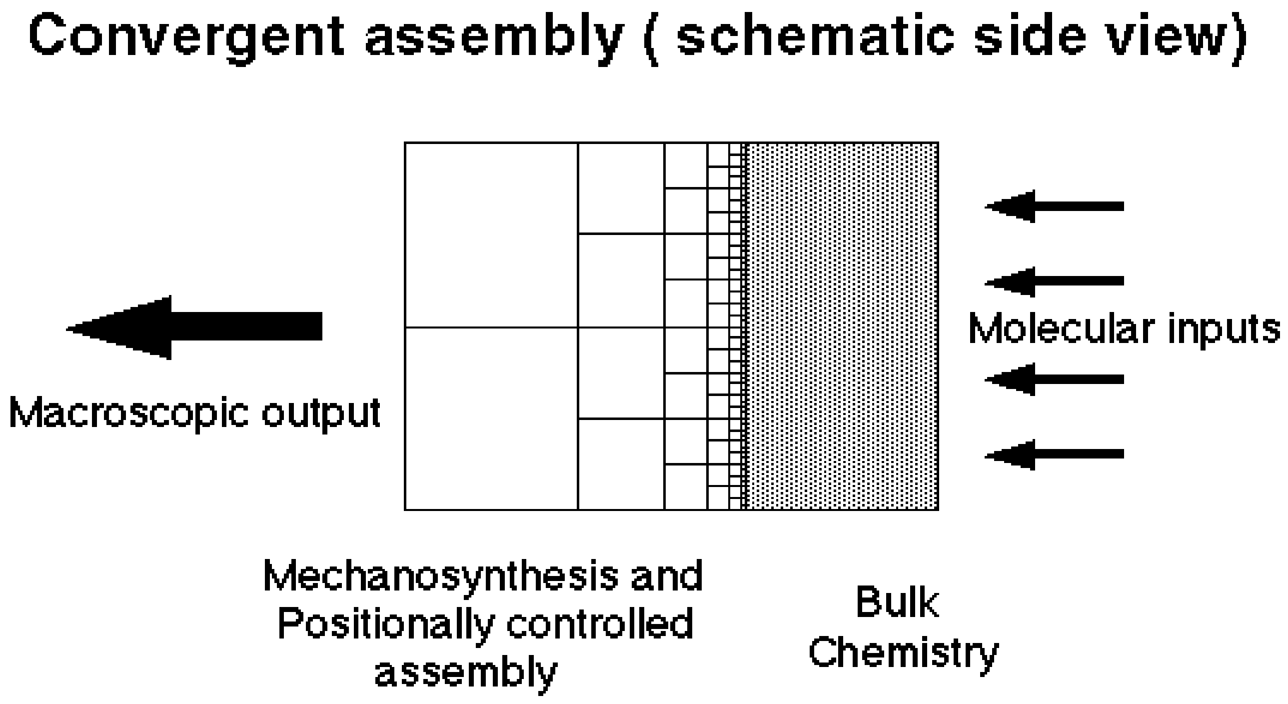
Reviews the voluminous theoretical and experimental literature about physical self-replicating systems.

www.molecularassembler.com/KSRM.htm

Exponential assembly



Convergent assembly



Convergent assembly

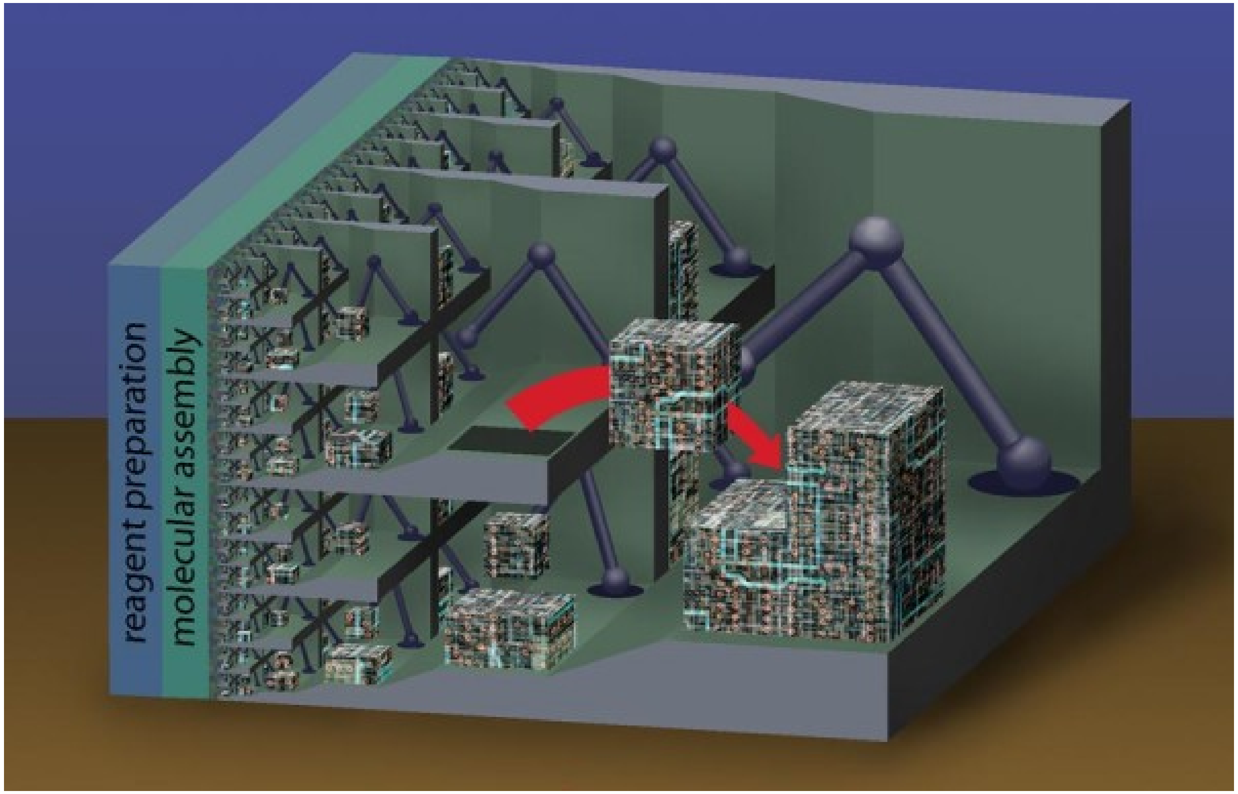


Illustration courtesy of Eric Drexler

http://www.zyvex.com/nanotech/convergent.html

Manufacturing costs per kilogram will be low

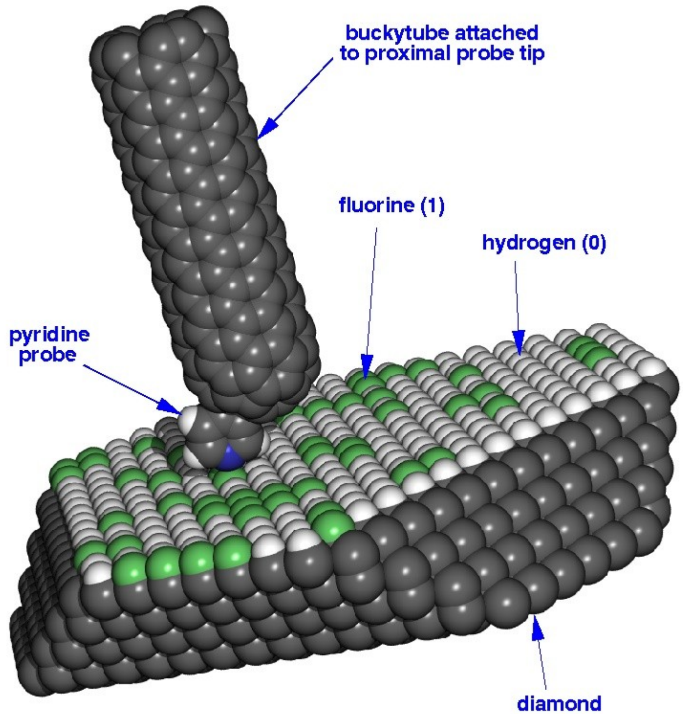
- **Today: potatoes, lumber, wheat, etc. are all about a dollar per kilogram.**
- **Tomorrow: almost *any* product will be about a dollar per kilogram or less. (Design costs, licensing costs, etc. not included)**

The impact
of a new manufacturing technology
depends on what you make

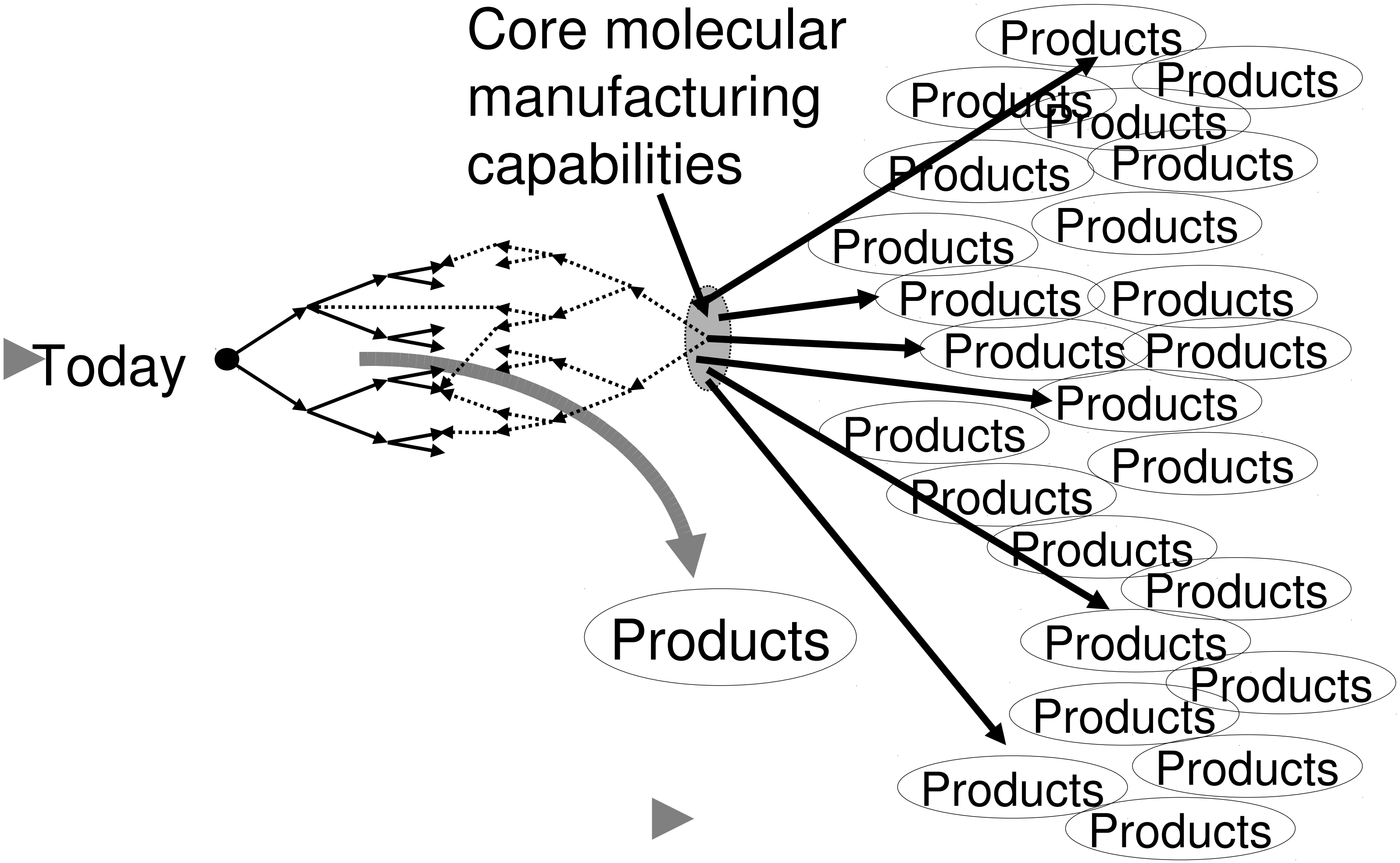
Powerful Computers

- We'll have more computing power in the volume of a sugar cube than the sum total of all the computer power that exists in the world today
- More than 10^{21} bits in the same volume
- Almost a billion Pentiums in parallel

High density memory



Overview


Today
Core molecular manufacturing capabilities
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products
Products

How long?

- Correct scientific answer: I don’t know
- Trends in computer hardware suggestive
- Beyond typical 3-5 year planning horizon
- Depends on what we do
- Babbage’s computer designed in 1830’s

Nanotechnology offers ... possibilities for health, wealth, and capabilities beyond most past imaginings.

K. Eric Drexler