



Safe Nanotechnology through Cryptography

Ralph C. Merkle, Ph.D.
Principal Fellow, Zyvex



Overview

Three historical trends in manufacturing

- More diverse
- More precise
- Less expensive



Where these trends are going: nanotechnology

- Fabricate most products consistent with physical law
- Get essentially every atom in the right place
- Reduce manufacturing costs to \$1/kilogram or less

<http://www.zyvex.com/nano>

Molecular arrangement matters

- Coal → • Diamonds
- Sand → • Computer chips
- Dirt, water & air → • Wood

There's plenty of room at the bottom

“...our ability to see what we are doing, and to do things on an atomic level, is ... a development which I think cannot be avoided.”

Nobel Laureate (physics)
Richard Feynman, 1959

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



President Clinton on the NNI

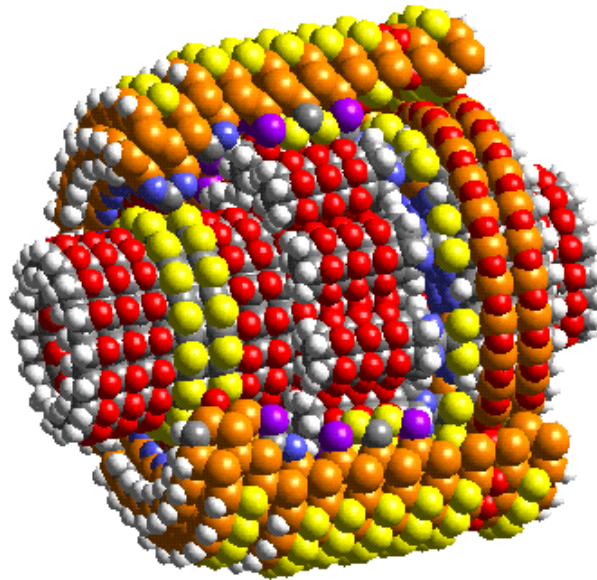
“Imagine the possibilities: materials with ten times the strength of steel and only a small fraction of the weight -- shrinking all the information housed at the Library of Congress into a device the size of a sugar cube -- detecting cancerous tumors when they are only a few cells in size.”

Time magazine on nanotechnology

“Everything in the physical world is made of atoms. Nanobots manipulate atoms. Thus nanobots could in principle make anything from apples to airplanes.”

Time, June 19th 2000

Proposal for a molecular planetary gear



Copyright 1995 IMM and Heros.
Do not reproduce without permission.

<http://www.zyvex.com/nanotech/gearAndCasing.html>

Proposal for a molecular robotic arm

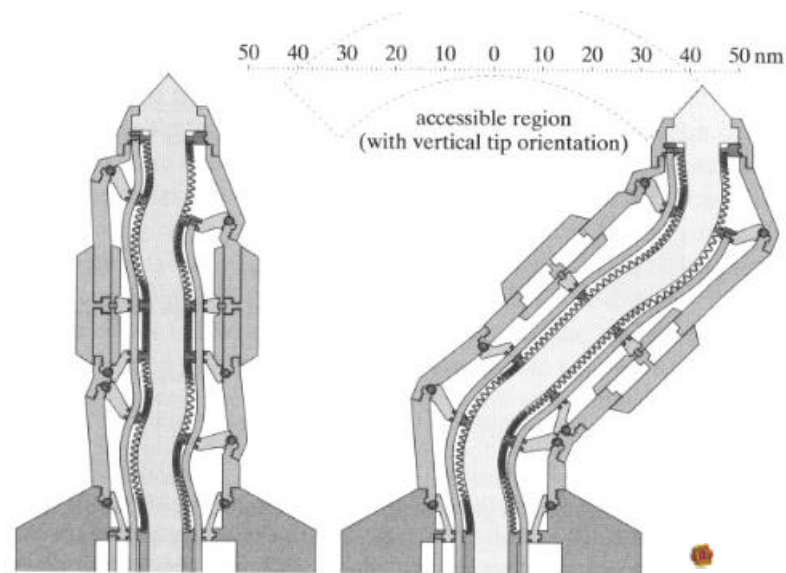
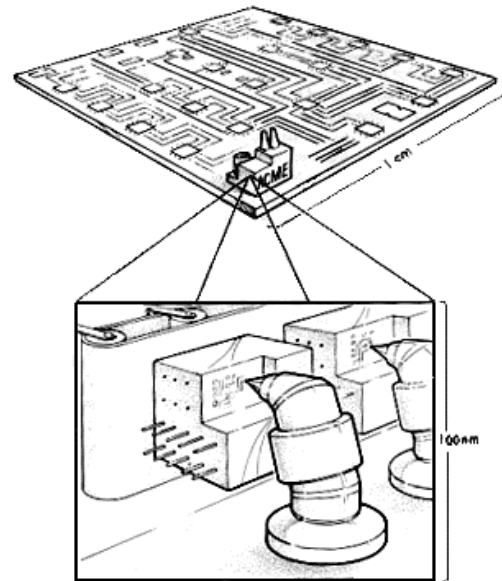


Figure 13.14. Cross section of a stiff manipulator arm, showing its range of motion (schematic).

Drexler's proposal for a nanorobotic factory



http://www.foresight.org/UTF/Unbound_LBW/chapt_3.html



The Vision

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



The Vision

Lighter, stronger, smarter, less expensive

- New, inexpensive materials with a strength-to-weight ratio over 50 times that of steel
- Critical for aerospace: airplanes, rockets, satellites...
- Useful in cars, trucks, ships, ...



The Vision

Nanomedicine

- Disease and ill health are caused largely by damage at the molecular and cellular level
- Today's surgical tools are huge and imprecise in comparison

<http://www.foresight.org/Nanomedicine>



The Vision

Molecular medical tools could

- Eliminate cancer cells, bacteria
- Remove circulatory obstructions
- Provide oxygen (artificial red blood cells)

<http://www.foresight.org/Nanomedicine>



A scenario

The Box: nanotechnology as a kitchen appliance

- An appliance in your kitchen the size of a microwave oven
- Plug in power, plug into the internet
- You pour in “nanotoner”
- It makes things
- Including copies of itself

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



A scenario

The Box: nanotechnology as a kitchen appliance

- The Box loads blueprints off the internet
- Purchased software, shareware, freeware, open source.....
- It makes the economics of everything like the economics of software
- Enforcement of intellectual property rights?



A scenario

“Military applications of molecular manufacturing have even greater potential than nuclear weapons to radically change the balance of power.”

Admiral David E. Jeremiah, USN (Ret)

Former Vice Chairman, Joint Chiefs of Staff

November 9, 1995

<http://www.zyvex.com/nanotech/nano4/jeremiahPaper.html>



A scenario

Conventional weapons

- Existing designs (tanks, bombers, destroyers, ...) but with new materials
- Reduced manufacturing cost
- Rapid buildup



A scenario

Questions, questions, questions

- Is it a problem if anyone can make anything?
- Foresight Guidelines
- *Should we* restrict the Box?
- *Who decides* what to restrict?
- *How do we* restrict the Box?

<http://www.foresight.org/guidelines/index.html>



A scenario

Cryptographic security for the Box

- The Box won't build what hasn't been approved
- What's approved is digitally signed
- The Box is tamperproof
- The usual protocols



A scenario

A side benefit: enforceable intellectual property rights

- The Box logs what it builds
- And tells someone about it
- Who bills you
- And pays the author



A scenario

**It doesn't work for software or music,
why should it work for the Box?**

- Greater incentives
- Greater penalties
- Tabula rasa



A scenario

Do we want it to work?

- Privacy
- Another regulatory agency
- Reduced rate of innovation
- Regulation of matters unrelated to global security
 - Guns, drugs, vitamins, fatty foods



Conclusion

New technologies, new challenges

- Nanotechnology raises new concerns
- Some of those concerns could be addressed by cryptographic mechanisms
- These issues will take some time to sort out
- Sorting them out before the technology is deployed might be advantageous



zyvex
assembling tomorrow...[®]