The Cryptography of John Nash

Ron Rivest and Adi Shamir

(Along with our students)

John Nash and the NSA

- In 1955, John Nash wrote a series of secret letters to the NSA, proposing a new type of encryption/decryption machine.

- This correspondence had just been declassified, and can be viewed at http://www.nsa.gov/public_info/press_room/2012/nash_exhibit.shtml

- In his letters, Nash anticipated the birth of complexity theory a decade later, and the birth of modern cryptography two decades later.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

CAMBRIDGE 39, MASS.

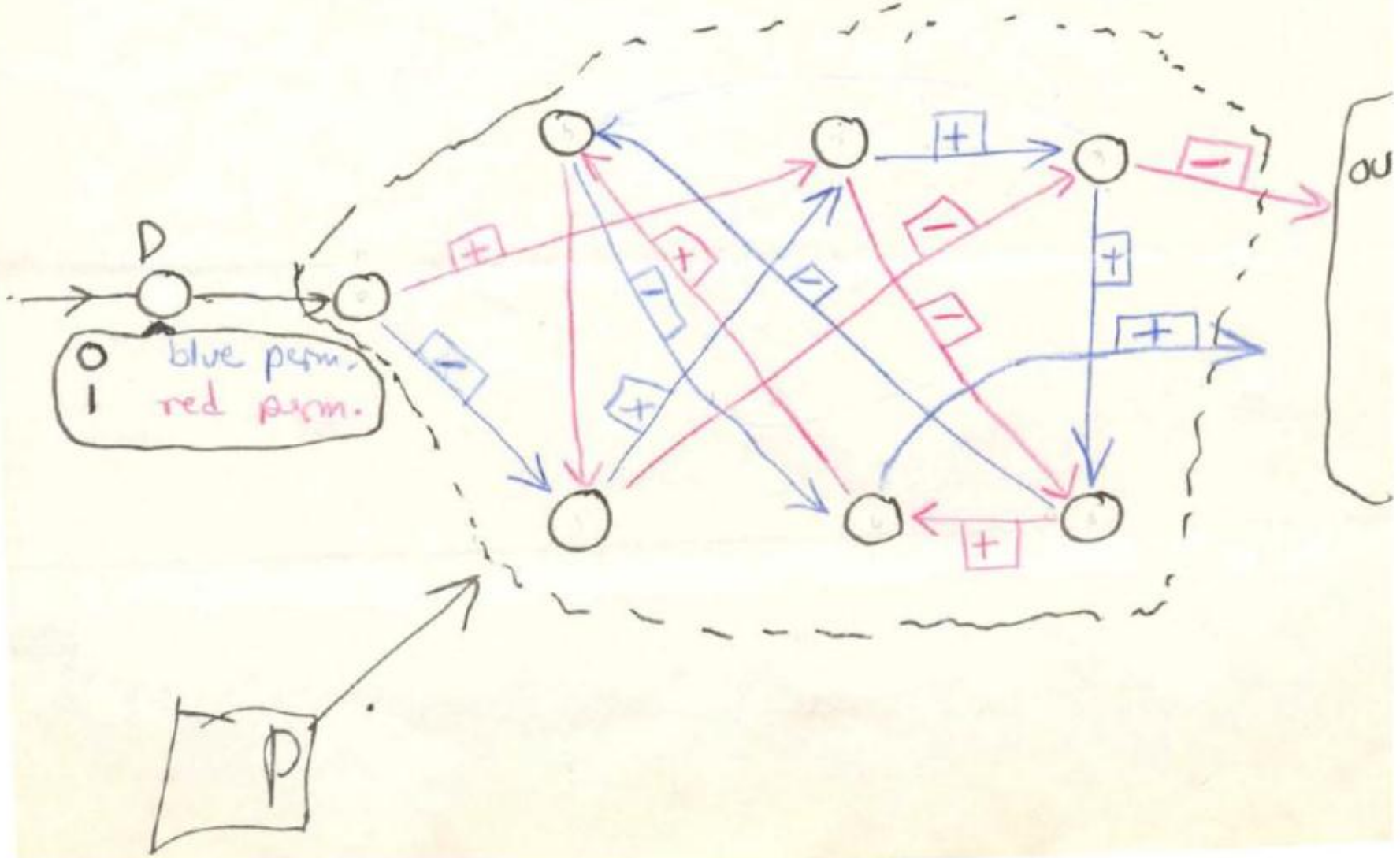
DEPARTMENT OF MATHEMATICS

letter concerns ENCIPHERING

Dear Sirs:

An enciphering-deciphering machine (in general outline) of my invention has been sent to your organization by way of the RAND corporation. In this letter I make some remarks on a general principle relevant to enciphering in general and to my machine in particular. This principle seems quite important to me, and I have some reason to believe you may not be fully aware of it.

the permuter, P, and "decider", D, work as follows, illustrated by example:



The "key" for the enciphering machine is the choice of the permutations. If there are n storage points in P, not counting the first one, which receives the digit from 0, then there are

$$[n!\, 2^{n+1}]^2$$ possible keys.

I guess I can rely on your people to check on the possession of this machine of the various properties I claimed for it

Mr. John Nash
Department of Mathematics
Massachusetts Institute of Technology
Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your letter received in this Agency on 17 February 1955.

The system which you describe has been very carefully examined for possible application to military and other government use. It has been found that the cryptographic principles involved in your system, although ingenious, do not meet the necessary security requirements for official application.

Unfortunately it is impossible to discuss any details in this letter. Perhaps in the future another opportunity will arise for discussion of your ideas on the subject of cryptography.

Although your system cannot be adopted, its presentation for appraisal and your generosity in offering it for official use are very much appreciated.

It is regretted that a more favorable reply cannot be given.

Sincerely,

E. M. Gibson
Lt. Col., AGC
Assistant Adj. Gen.

The Claimed Security Level:

- The secret key consists of two permutations over n bit positions and two strings of n-bits
- For n=256, this gives a huge key size of almost 4000 bits

The Real Security Level:

- Ron Rivest and his students (primarily Ansel) worked on a chosen plaintext attack
- The best attack in this model requires polynomial time and data of just O(n^2)

The Real Security Level:

- Adi Shamir and his students (primarily Zinger) worked on a known plaintext attack
- The best attack found so far in this model requires subexponential time and data of $2^{O(\sqrt{n})}$

An interesting observation:

- If we ignore the constants, 2^(sqrt(n)) is actually smaller than n^2 for all the practically significant choices of n between 2 and 256 (for example, for n=100, 2^(sqrt(100))=1024 whereas 100^2=10,000
- Even if we include the constants, both algorithms are likely to have practical time complexities
- It is still an interesting open problem whether a fully polynomial known message attack exists

Concluding Remarks:

- This exchange of letters is a fascinating piece of cryptographic history
- John Nash foresaw in 1955 many theoretical developments which would appear in complexity theory and cryptography decades later
- However, he was a much better game theorist than a cryptographer…