EXEMPLARY DESIGNS FROM THE GOLDEN AGE OF SHIFT REGISTER CRYPTOGRAPHY

NTACC 2010

Eric Bach
Computer Sciences Department
University of Wisconsin
Madison, WI 53706
USA

Three Eras of Cryptography

Cryptography is embedded in communication technology and follows its development.

By Hand: $-\infty$ to 1920

Electromechanical: 1920 to 1970

All Electronic: 1970 to present

Major Electronic-Era Events

Microprocessor ($\sim$ 1974) – allowed the use of complicated algorithms

Public Cryptography Research (1975) – DES competition, public key papers led to wider communication

Telecommunications Then and Now

- 1950: Telephone and teletype links
  - Phones: totally analog, circuit switched
  - TTY: Electromechanical transmit/receive units, using primitive ASCII code (Baudot).
  - Links controlled by large organizations, so authentication not an issue.
  - Stream ciphering *was* encryption.
- 2010: Convergence of media
  - Internet-style links (digital, packet switched) used for everything.
  - No authentication: On the Internet, no one can tell you're a dog.
  - Public key, private key block ciphers, stream ciphers all coexist.

What was cryptography like in the "early" electronic era?

> Not widely known (outside full-time professional circles). One of the early evaluators of DES says:
>
> > It rapidly became clear during the first morning that most of the individuals involved in the "assessment" of the algorithm (including one of the authors) knew so little about cryptography and cryptanalysis that the task at hand could not be performed at all... It was if a group of scientists versed in Aristotelian physics were asked to check the solution of a quantum mechanical problem. [Deavours and Kruh, 1985]
>
> Rumors abounded
>
> > Nonlinear feedback shift registers seem to have been used extensively for military cryptography, but despite persistent rumors the details of what was done continue to be secret. [Wolfram 2001]

As well as good advice

> It is common belief among engineers that a pseudo-random sequence, obtained from a linear feedback shift register, can be used as a key-stream to obtain cryptologic secrecy. Communications engineers are advised that this method is fallacious. [Geffe 1967]

and bad

> Besides their obvious applications as ... noise sources, pseudo-random bit sequences [LFSRs] ... can be used for encipherment of messages or data, since an identical PRBS generator at the receiving end provides the key [Horowitz and Hill 1980]

Who Were the Players?

- Professional Specialists
  - In government or large companies
- Academics
  - Rare before 1975: Hill, Levine, ...
- Amateurs
  - A few authors, e.g. Gaines

Why This Project?

As a teacher of cryptography, I have always wondered what happened between Enigma and DES.

Realized that part of the story is documented in America's electronics patents.

Scope of this Project

Examine U.S. patents on encryption, digital communication, random number generation, etc.

Filing dates (roughly) 1960 to 1980

Filing date more important than issue date

After 1980, more and more research in public domain

This lecture will not cover everything! The focus is on a few designs that illustrate interesting ideas.

Some Specific Questions for Study:

Did anyone use straight LFSRs for encryption? (No.)

We can now recognize Geffe as an "insider" who helped prevent this.

How did system designers think about and achive nonlinearity? (As we do it today.)

Where did today's "operation modes" come from? (It's complicated.)

Why Patents?

There is nothing else to read! (No academic literature.)

Long file-to-release time allows ideas to be "time stamped" even if revealed later.

Longest known delay: William Friedman's rotor machine patent was filed 1933, issued 2000 (!).

Learn about designers that did *not* publish academic research.

Why Shift Registers?

- Electronics was built out of individual components
- Can get huge periods with very small hardware investment
- Some theory for their behavior (especially if linear)
- Interesting math involved in their analysis

History vs. Archaeology

History: examine oral and written records by participants in the events studied.

Archaeology: examine artifacts left behind by their users.

We don't have the artifacts, but patents are a pretty good substitute (enough info to reproduce the device).

Caveat: We do not have information on how (or even if) these systems got used.

Why Study the Past?

Ideas are constantly recycled (technical knowledge as a spare parts bin).

We can appreciate human ingenuity in the face of different constraints

Some prehistory.

In 1945, Hans Rohrbach (Germany) wrote a report on what the Axis powers knew of cryptology during WWII. [English trans. Cryptologia, 1978.]

The Fibonacci-style recurrence

$$X_n = X_{n-10} + X_{n-9} \pmod{10}$$

is mentioned as a key stream generator.

Discusses finding the period (analyze mod 2 and mod 10), and how to avoid "bad" seeds.

Sequence prediction not mentioned.

In 1955, Golomb (Martin Co.) studied shift register sequences for applications to missile control.

Algebraic theory for linear sequences

Linear sequences could be easily acquired by an "intelligent jammer," so initiated the study of nonlinear recurrences.

Understood the relevance of correlation to cryptanalysis of combined sequences, but didn't write about this application.

Other Work:

Error-correcting code implementations based on LFSRs

Spread spectrum communications (another use for long-period pseudorandom sequences)

We conclude that the basics of shift register theory were well known to insiders by 1960.

> My cryptanalytic approach involved multi-dimensional correlations, and I developed a theory of "correlation immunity" based on a set of *invariants* for boolean functions of n binary variables. In 1957-1959 this was of course classified, even though the flow of information between me and NSA was always one way (me to them). However, I presented a talk ... in 1959 ... I just didn't mention the application, explicitly, that motivated it. [Golomb 2006]

I. Combining Pseudorandom Streams

Laurence Safford (1890-1973): one of the principal U.S. cryptographers during WWII.

With Rowlett, developed U.S. SIGABA rotor machine

Bit part in Pearl Harbor story (tried to warn higher-ups).

Filed 1962, issued 1980. Suggests some of the ideas were in use.

Generated a pseudo-random bit stream to be XOR'd with (TTY) plaintext.

4 LFSRs, but could use only 2 if necessary (reliability or backward compatibility?)

$$\underbrace{\text{LFSR}_1\ \text{LFSR}_2\ \text{LFSR}_3\ \text{LFSR}_4}$$

$$\downarrow$$

[nonlinear combiner F]

$$\downarrow$$

keystream

Combiner inputs:

4 max-period LFSRs, lengths 11, 13, 17, 19. Feedback function is

$$f(x, y, z, w) = 1 \text{ iff 3 out of 4 bits agree}$$
$$= x \oplus y \oplus z \oplus w$$

Eldest bit required, others settable by the user.

Theorem: if m, n relatively prime, so are $2^m - 1, 2^n - 1$. So 4-tuples of bits repeat with period

$$115220689749526732 9 \approx 1.1 \times 10^{18}.$$

Hard Wired Combiner

$$F(A,B,C,D) = AB \vee CD \vee \overline{A \vee B \vee C \vee D}$$

with truth table

		00	01	10	11	CD
AB	00	1	0	0	1	
	01	0	0	0	1	
	10	0	0	0	1	
	11	1	1	1	1	

Symmetric under $AB \leftrightarrow CD$

Balanced

Not correlation immune!

Why was this chosen?

There are 333 4-variable balanced CI functions, so plenty to choose from

This may have been the best "easy to implement" function, as its correlation table is not too bad.

A Few Engineering Details

Memory (shift registers) used magnetic core technology, driven by silicon power transistors.

Alarm sounded if PT = CT for too long.

Previous machines used key tapes.

Claims unbiased key stream, but it isn't (max length LFSRs are biased toward 1)

Intended data rate: a few kbits/sec.

II. Nonlinear Feedback for Bit Ciphering

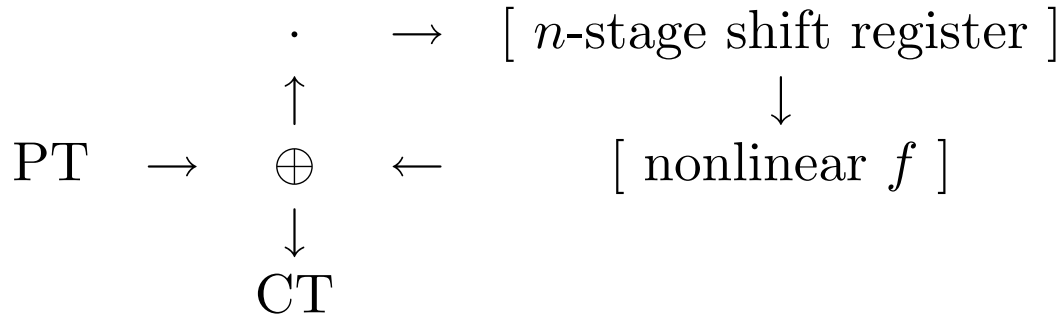
Ferrel design for Racal/Milgo (Miami)

Filed 1965 (abandoned), re-filed 1981, issued 1982

In the style of a research article (not a complete design)

Claims on encryption AND message integrity, synchronization, hardware testing.

Nonlinear SR used for cipher feedback mode



Design details?

Level of detail more like an academic research article than a patent.

Register length unspecified, no effort to make the iteration reversible (eldest bit not special).

Claim covers "arbitrary" feedback logic

Variable Feedback

Nonlinear logic not specified, except for one short example

4 bit register with x_0, x_1, x_2, x_3

Six switches can select various quadratic/cubic terms:

$$x_0x_1,\ x_0x_2,\ x_0x_3,\ x_0x_1x_2,\ x_0x_2x_3.$$

By itself this is not enough! (00..00 is fixed pt)

Claim on periodic change of logic to enhance difficulty of analysis

III. A Complete Design With Nonlinear Feedback

Ivar Mo, et al. (Norway)

Filed 1966 in Norway, U.S. patent issued 1970.

Intended for TTY traffic, so works on 5-bit (Baudot) blocks

Key Generator

$$\underbrace{\text{NLFSR}_1\ \text{NLFSR}_2}$$
$$\downarrow$$
$$[\ \text{combiner } F\ ]$$
$$\downarrow$$
$$\text{keystream}$$

Two-Stage Encryption Cycle

PT is first put into a short LFSR and stepped a pseudorandom number of times:

$$X \to \cdots \to X_P$$

(the LFSR control logic counts down from the 5-bit integer P)

Added to pseudorandom key as usual:

$$X_P \to X_P \oplus K = \text{ CT block}$$

Decryption is the reverse process.

Shift Registers for Keystream Generator

2 registers, each 15 bits long (to permit cycle length testing?)

Galois configuration (so not a Golomb-style nonlinear shift register)

Why? Perhaps availability of flip-flop units.

Small example (length 4):

$$\begin{pmatrix} z_1' \\ z_2' \\ z_3' \\ z_4' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} + \begin{pmatrix} f(z_i\text{'s}) \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Feedback function is a variation on 2-1 multiplexer:

$$f(x, y, z, w) = \begin{cases} z, & \text{if } x + y = 0; \\ w, & \text{if } x + y = 1. \end{cases}$$

This f satisfies

$$f(\bar{x}, \bar{y}, \bar{z}, \bar{w}) = \overline{f(x, y, z, w)}$$

and has 4 inputs, so nonlinear.

Users selected 4 of 15 taps to be the inputs to f.

Are There Any Branches?

Abbreviate the iteration as

$$z' = Mz + (f(z)\ 0 \cdots\ 0)^T.$$

Sum all equations to get $\sum z'_i = f(z)$.

So

$$(\sum_{i \neq 1} z'_i\ z'_2\ \cdots\ z'_n)^T = M(z_1\ z_2\ \cdots\ z_n)^T$$

Theorem: The iteration is reversible.

Proof: Rank of M is $n - 1$, so its nullity is 2. The kernel is exactly the constant vectors.

So a state can have at most 2 predecessors; if distinct they are complements.

Could there be 2 predecessors, i.e.

$Mz + (f(z)\ 0 \cdots\ 0)^T = M\bar{z} + (f(\bar{z})\ 0\ \cdots\ 0)^T$?

No, since $f(\bar{z}) \neq f(z)$.

The iteration graph must be all cycles, since any non-cyclic state would lead to a branch.

How General is This?

Patent does not mention reversibility.

It holds as long as the feedback function f is changed by complementation.

We can pick such f in $2^{2^{n-1}}$ ways.

Same number as the count of "eldest bit added" functions given by Golomb.

We now have a Galois configuration analog to Golomb's well known reversibility criterion for Fibonacci configurations.

How was the Shift Register Output Used?

Two streams combined using XOR

5 bits taken to determine P, the number of clocks for the short LFSR

These 5 bits get re-used and are XORd with the superencrypted PT block.

Engineering Details

TTY circuits have forbidden characters, so these must be prevented in ciphertext

Complete specification (ICs with several gates per chip) suggests the device was built and used.

User supplied feedback connections. Exhaustive search cryptanalysis would have been possible IF these connections were known.

The Lion's Paw

This design reflects sophisticated analysis, but by whom?

Ernst Selmer (CRYPTO 93 talk) cites work with two of the inventors (Abrahamsen and Meisingset) on an earlier (?) TTY crypto machine.

This machine was similar to Safford's: LFSR streams combined nonlinearly.

IV. A Machine with a Shift Register Ladder

Inventor Bohman of Ericsson (Stockholm).

Filed 1967, issued 1972

This used 17 (!) short linear shift registers

Lengths mostly (but not always) prime, largest 29.

8 used as ring counters, 9 as hard wired max period LFSRs.

Patent addresses keystream generator only.

High-level description

Cascade of LFSR-based stages (the "ladder")

Ladder output switches streams from two standard LFSRs

Very similar to Geffe's 1973 generator (no ladder, just a third LFSR).

Affine Ladders (my term)

$n + 1$ ring counters produce streams $x_0, a_1, \ldots, a_n$.

n max-length LFSRs produce streams $b_1, \ldots, b_n$.

If x_i is the i-th stage output, the next stage produces

$$x_{i+1} = ax_i + b$$

Output of the entire ladder is

$$\begin{aligned} x_n = {} & a_1 a_2 \ldots a_n x_0 \\ & + b_1 a_2 \ldots a_n \\ & + b_2 a_3 \ldots a_n \\ & + \cdots \\ & + b_{n-1} a_n \\ & + b_n \end{aligned}$$

How Did Correlation Influence the Design?

As a Boolean function, the combiner is

$$F = LA + \bar{L}B$$

(L is ladder output, A, B output from two LFSRs)

Here is its correlation table

	F	$\bar{F}$
L	4	4
A	3	1
B	3	1

This suggests that the ladder was considered the weak point, but we now know (Siegenthaler) that A and B actually are.

Examination of the Boolean Fourier transform reveals that we can't do better than the 2-1 mux, if we want balance between A and B, and low correlations.

Ladder output is immune with respect to the ring counters. A cryptanalyst attacking the ladder would be forced to work on the longer period sequences, not the ring counters.

V. A DeBruijn Sequence Generator

Perlman (NASA), filed 1974 and issued 1975.

Goal: produce a sequence of length 2^n from an n-cell shift register

Claims application to straight stream ciphers

Use deBruijn sequence for key stream, XOR with plaintext

Good substitute for LFSRs in Safford-type combining systems, removes bias over full period. (They don't mention this.)

Algorithm involves "cycle patching:"

Run a max-length or nearly so LFSR

Use AND gates to detect patterns in register

When one trips, stuff a 0 or 1 into the output and make the device switch cycles.

Cryptographically Secure?

Not as claimed.

Most of the cycle is the same as for a max length LFSR.

VI. A Cipher for Banking

Harold Richard, et al. of NCR (Dayton)

Filed 1975, Issued 1977

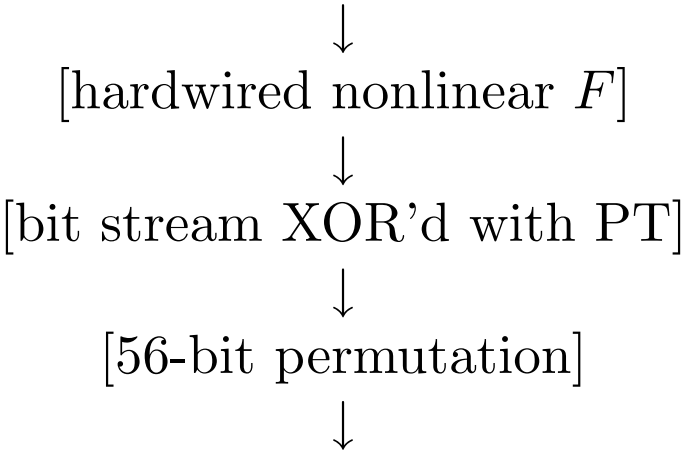
Design goal: encryption for ATMs

Now done with DES or 3-DES

Previously patented methods were weak: transposition of letters/numbers + shifting up by 1 (!).

This design was much stronger.

Additive stream cipher based on nonlinear transformation of 16 bit LFSR sequence:



Hard wired shift register: period $2^{16} - 1 = 65536$. (Too short for security.)

Nonlinear Transformation (Cont'd.)

User selects 14 SR cells to pass to nonlinear logic

Permutations allowed, so

$$\binom{16}{2} \times 14! \approx 10^{13}$$

possible connections

Nonlinear F:

The outputs of 7 copies of

$$f(x, y) = \text{NAND}(x, \sim y).$$

feed into a parity function (1 iff an even number of inputs are 1).

Why these choices? Perhaps commercially available.

F is symmetric, so we must divide the 10^{13} possible connections by $7! = 5040$ to get

$$2 \times 10^{10}.$$

Weakness: f is biased ($\Pr[1] = 3/4$), so the key stream has

$$\Pr[0] = \sum_{k=0,2,4,6} \binom{7}{k} (\frac{3}{4})^k (\frac{1}{4})^{7-k} = 0.496...$$

Final stage: User-selected permutation of 56 wires

Permutation is product of 28 disjoint 2-cycles

Similar to Enigma plugboard, but not as strong (some 1-cycles should have been allowed).

VII. Irregularly Clocked Linear Shift Registers

Inventor Barrie Morgan of Datotek (Dallas TX). Filed 1976, issued 1978.

This patent covers the pseudorandom bit generator. Others deal with the complete device.

> Desktop-size unit, to go between TTY keyboard and modem. Design goals of flexibility (can store multiple keys, several data rates), plus short issue time suggests a commercial unit?

Main Components:

> 2 LFSRs to generate clocking signals
>
> 3 more to generate pseudorandom bits
>
> User-selectable permutation for LFSR outputs
>
> Tree of 5 multiplexers (4, then 1)

Master Clock Registers

Lengths not specified but nicely drawn circuit suggests 11 and 15; note

$$\gcd(2^{11} - 1, 2^{15} - 1) = 1$$

Stepped a fixed number of steps per key cycle

Why? It's equivalent to stepping 2 other LFSRs one clock tick.

This fixed number is rel prime to both periods, to guarantee maximum period

Master clock period is about $2^{11+15} = 6.7 \times 10^{11}$.

Slave Shift Registers

Claim that all can be same length (15?).

Each has a "menu" of two step lengths (e.g. 11 and 13). Signal from the master registers indicates which is used.

All menu choices must be relatively prime.

Claim (dubious!) that this guarantees a long period.

Multiplexer Tree

Outputs of the master LFSRs (some permuted if user wishes) and the slave LFSRs are inputs to four 4:1 multiplexers

Outputs of these are similarly boiled down to one key bit

Anti-Spoofing Feedback

Claim is to prevent key recovery by subtracting PT from CT

Equivalent to a final (short) nonlinear SR, fed by a nonlinear bit generator, with cipher feedback.

Engineered by making some cipher bits feed into multiplexer inputs.

Some Conclusions

All the popular nonlinearity tricks (combining, nonlinear and/or time-varying feedback, irregular timing) were known to insiders a decade or more before their appearance in academic literature.

Evidence for cryptanalytic expertise is less strong.

- Security arguments based on number of combinations
- Some evidence of correlation arguments
- Caveat: Patents must only argue that the device fulfills its intended function, not that it is best.

We can't understand what happened by reading only academic journal and conference papers. Patents may be unreadable, but we must read them.

Is This the Whole Story?

Certainly not. (What remains to be issued in the future?)

National and corporate archives should be examined, where possible.