from *SIAM News*, Volume 33, Number 4

Listening In on a Cryptography Seminar

FROM THE SIAM PRESIDENT
By Gilbert Strang

I don't often go to seminars on cryptography. But a few weeks ago I heard Adi Shamir, who is the S in RSA, describe his recent attack on the A5/1 cipher. This encryption scheme helps to protect billions of cell phone conversations. It is used on GSM telephones—they are dominant in Europe, and Omnipoint is one user in North America. The first step, to discover the algorithms by reverse engineering the DSP chip in an actual handset, was taken by Marc Briceno (see www.scard.org). The weaker A5/2 code was then broken immediately; A5/1 has not been so easy. A successful attack has now been simulated (to find the session key in a short piece of a specific conversation). Shamir stresses that he makes no claims about the practical security of fielded GSM systems.

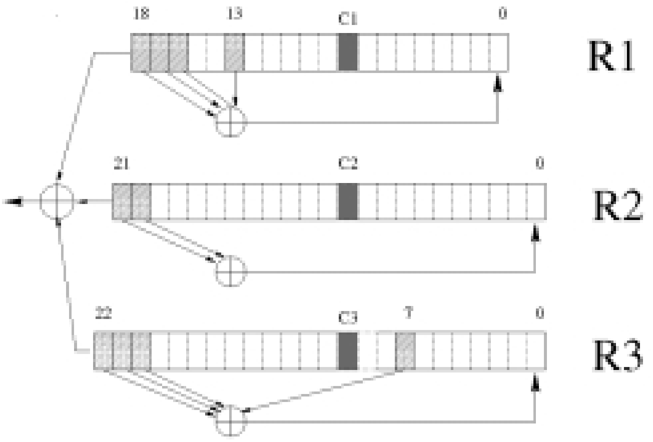
History provides good reasons to be careful. A few years ago Serge Humpich broke the algorithm selected by the French banks for smart cards. (The banks had used too few digits.) It is fascinating to see how inverting a nonlinear transformation can affect a whole banking system—well, this mathematics is *applied*. Humpich offered to show the bankers how to create a false card. At the moment when he obtained a few illegal Metro tickets, the police entered from the next room. The whole thing was a setup . . . and Humpich got a prison sentence. It was suspended by a fairly sympathetic judge, but the chill is still felt.

Back to A5/1. It is built from three short registers, containing 19, 22, and 23 bits. Each register has a clocking position near its center (see illustration, page 2). The one nonlinear step in the whole cipher is a "majority rule" that selects whichever bit appears in most (two or three) of the clocking positions. Those registers in the majority will be advanced one step. This majority function is not uniquely invertible, but it is weak enough that the tree of all possibilities can be quickly traced.

The problem is to discover the session key K. It is mixed into the registers with a known frame counter F. The bits in certain known positions determine three outputs. Each register is then shifted, or not, by the majority rule, and the outputs reenter the back of the shifted registers. They also mix with the unknown conversation to produce the ciphertext that we can hear (and try to decode).

I can't describe the whole attack on K. (Fortunately, the paper by Shamir and co-authors Alex Biryukov and David Wagner is very well written.) There are no fewer than ten key ideas, but one central idea is simple. The system has 2^{64} internal states, since the registers have $19 + 22 + 23$ bits. Make wise choices for a large set A of these states and precompute their first k output bits. Then eavesdrop on the ciphertext and extract all k-sequences. Let B contain the (unknown) states that produced them. If a common state is found in A and B, it is an actual state of the algorithm and the key K is vulnerable.

The trouble is, an intersection can be expected only if the product of the set sizes $|A|$ and $|B|$ is roughly $N = 2^{64}$. That requires excessive memory for fast random access to A, or hours of conversation to fill B. We want the key in a few minutes (seconds if possible). The high estimates assume that the N states s lie in the sets A and B with uniform probabilities $|A|/N$ and $|B|/N$. The chance of a common state is then about $\Sigma\ (|A|/N)\ (|B|/N) = 1$. It is here that a "wise choice" is needed, to fill A and B with states that have higher probability and strong correlation. An intersection can then be expected for much smaller sets (Shamir is really playing with the inner product $\Sigma\ \text{Prob}_A(s)\ \text{Prob}_B(s)$ and the Schwarz inequality).



The A5/1 stream cipher (from "Real Time Cryptanalysis of A5/1 on a PC," by Alex Biryukov, Adi Shamir, and David Wagner).

The good choice of A and B exploits specific weaknesses in A5/1. A much stronger mixing among the registers would defeat the attack. With only a majority rule to untangle, and clock-ing bits badly located within the registers, the simulated attacks have succeeded. The paper can be found at www.cryptome.org/a51-paper.htm, and www.jya.com has other cryptic news.

I would like to add two notes, one on matrices and the other on SIAM meetings. Last month I mentioned the 1,0,1 tridiagonal matrix, perturbed by an extra $A_{ij} = A_{ji} = 1$ in its interior. The top eigenvalue jumps to the square root of 5, and its eigenvector has spikes localized at i and j. Now perturb just with $A_{ij} = 1$. The top eigenvector has only a single spike, decaying geometrically away from position i. This is one tiny observation (likely not new) in the growing theory of partly random matrices.

SIAM's Annual Meeting is July 10–14 in Puerto Rico, with a terrific program (www.siam.org/meetings/an00). The timetable for the first Com-putational Science and Engineering meeting in Washington is just now set (soon to be posted; www.siam.org/meetings/cse00). There are so many contributors that we have extended the meeting from September 21–23 to include Sunday the 24th. I really hope that the attraction of computational science, and the program, and the city, will convince you to come.