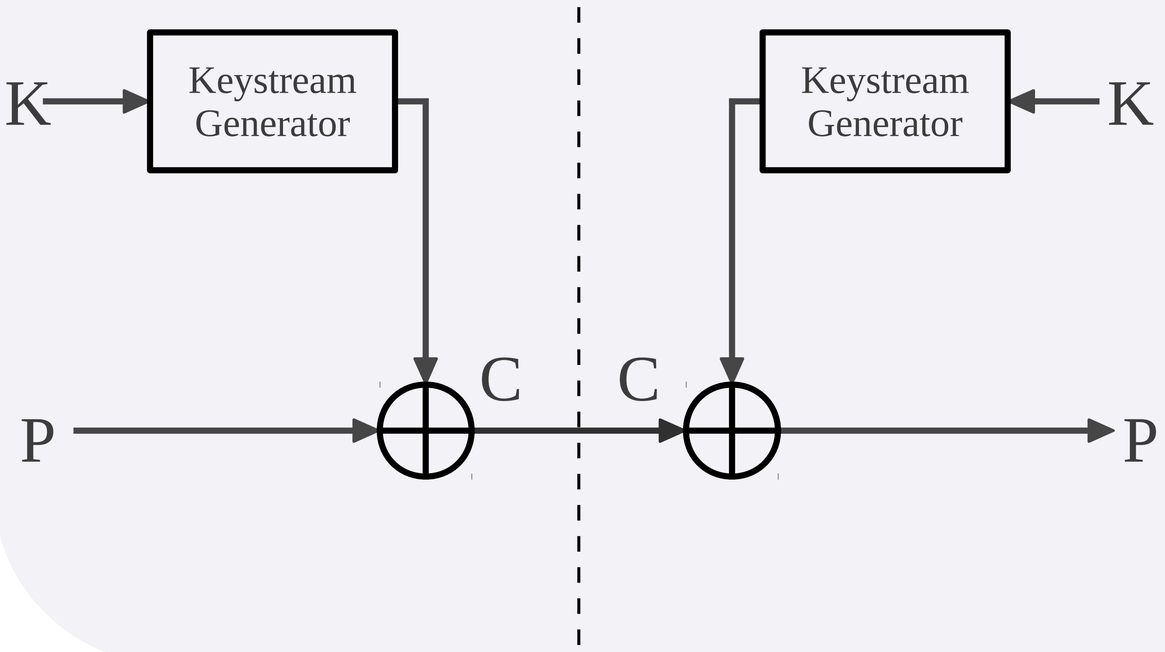
A Fast Correlation Attack Implementation

Encryption



Decryption

Stream Ciphers

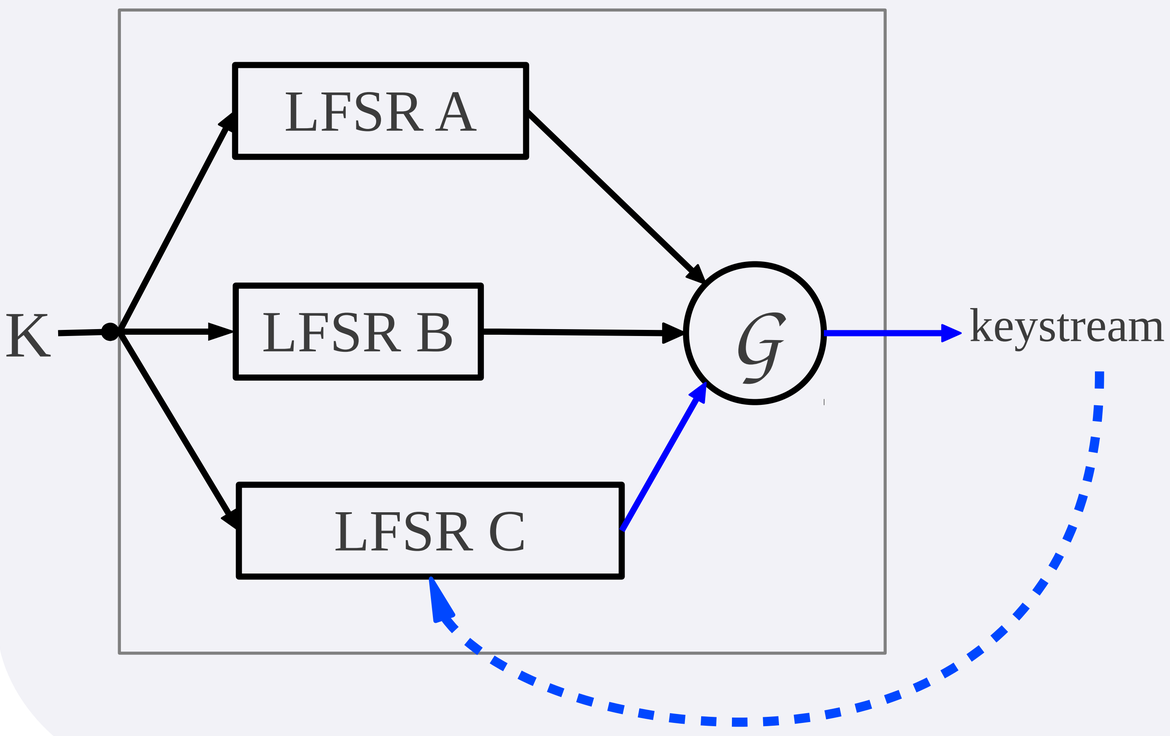
Stream ciphers are used for encryption where limited computational power. Examples include A5/1 which GSM for cellphone communications and E0, the stream cipher used in the Bluetooth protocol.

Two parties, a sender and receiver, both know some shared key, K, which is, for our purposes, a finite binary string. They exchange confidentially as follows:.

The sender first uses K to generate a keystream as long as the plaintext message P. Then the bitwise XOR of P and the keystream is computed to get the ciphertext C. This is sent to the receiver

The receiver can generate the same keystream using K and then XOR it with the ciphertext to get the plaintext back.

Combination (Keystream) Generator



Fast Correlation Attacks

A certain type of keystream generator is called a combination generator. These use components called Linear Feedback Shift Registers (LFSR). The LFSR are each initialised with a part of a key, and produce a sequence with good statistical properties. Each bit of the keystream is produced by combining a bit from each LFSR sequence with a boolean function G..

If G is chosen poorly, the sequence of one LFSR is correlated to the keystream. This project implements a fast correlation attack, which exploits the correlation, to find out the initial sate of the correlated LFSR from the keystream hence gaining partial knowledge of the key.

Parameters for a successful attack

	d = N/L				
t	10	10^2	10^3	10^4	10^5
2					
4					
6					
8					

The blue blocks indicate a successful recoveries of the LFSR sequence.

Implementation

A fast correlation attack is implemented in C and tested against the Geffe generator. This combination generator has 3 input LFSR sequences (a_t, b_t, c_t). The boolean function is G(a,b,c) = ab + bc +c which means the keystream is correlated to both inputs a and c.

The implementation successfully recovers the whole correlated LFSR sequence under the range of parameters indicated on the left. In doing so, knowledge of part of the key used to initialise to correlated LFSR is gained.

Azhar Desai
adesai@cs.uct.ac.za

Honours Project 2011
University of Cape Town

Supervisors

Dr Anne Kayem
Department of Computer Science

Dr Christine Swart
Department of Mathematics and Applied Mathematics