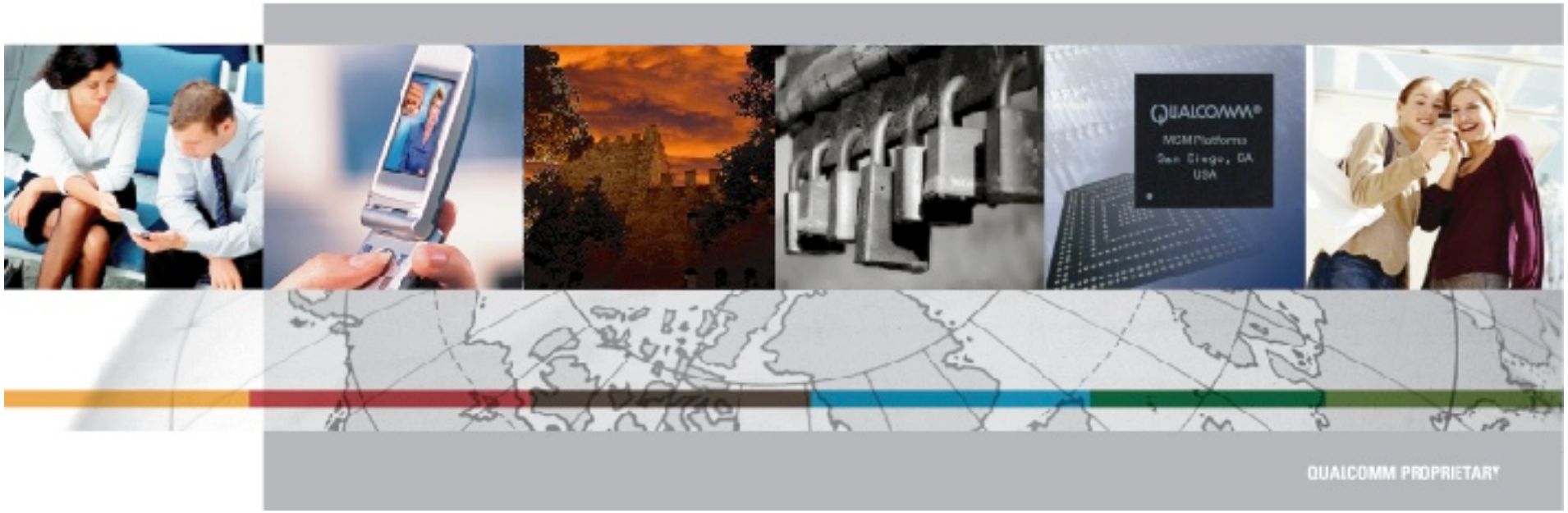
PRODUCT SECURITY INITIATIVE

QUALCOMM

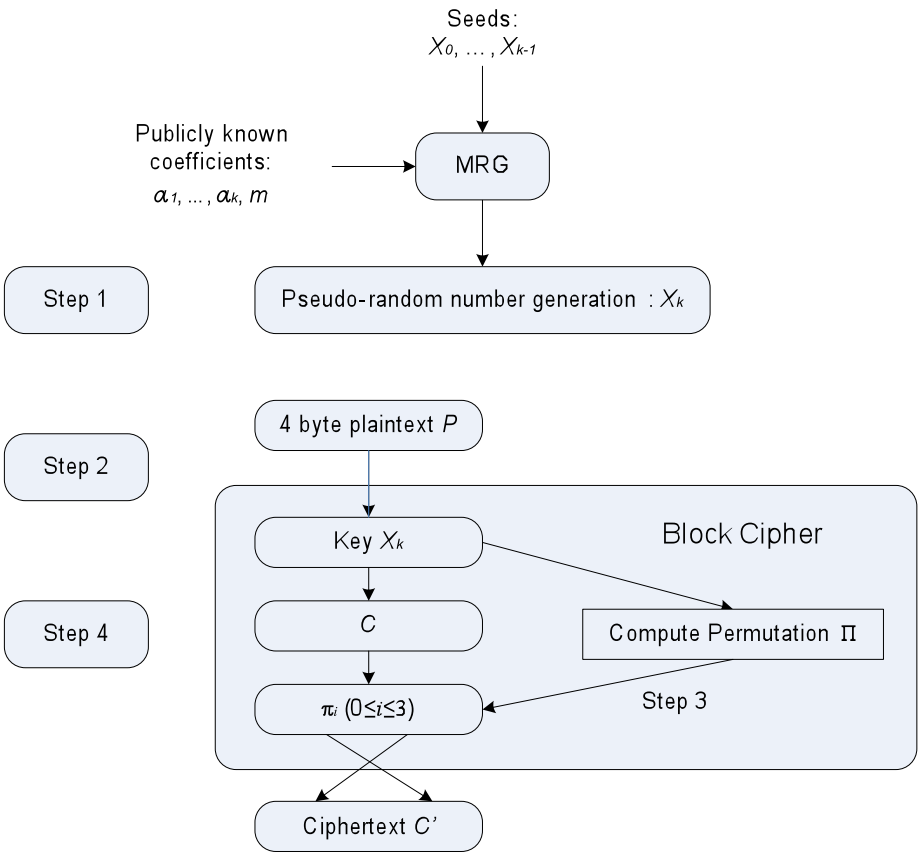


Attack on Ciphers based on Multiple Recursive Generators

Lu Xiao and Greg Rose

Eurocrypt'09 Rump Session

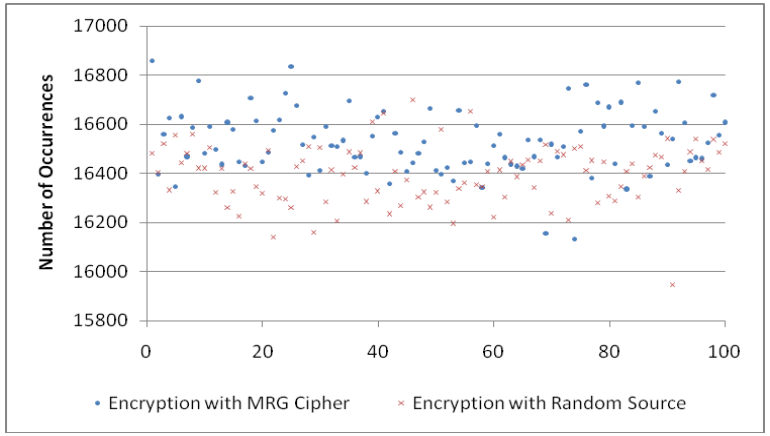
What is an MRG cipher?



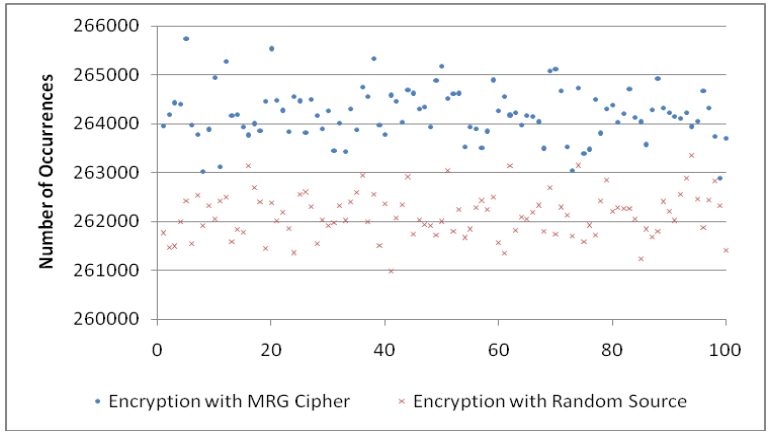
- Proposed by A. Olteanu *et al.* at IEEE GLOBECOM 2008
- A lightweight block cipher based on a multiple recursive generator (really LFSR mod P)
- Any MRG with order k >47 is extremely slow and impractical
- "*They achieve enhanced security while consuming less resource!*" – last sentence of the paper.

A Distinguishing Attack

- Observed bias: the MSBs of a ciphertext word's 4 bytes all match the corresponding plaintext word's MSB with probability $(1/16)+2^{-11}$.



Distributions with 2^{18} Samples



Distributions with 2^{22} Samples

A Known-Plaintext Attack

- Observed vulnerability: the key mixture and permutation are poorly designed , which enables effective subkey space reduction.
  - The specific cipher suggested by its inventors: the key can be derived using **94** plaintext words and negligible computation.
  - More importantly, we prove that there is an upper bound of workload to successfully attack all ciphers designed in this method => All are easy to break.
  - Be vigilant when Multiple Recursive Generators are proposed for either a cipher or a random number generator ☺.

Attack Summary

- Attack complexity

	Distinguishing attack	Known PT attack on efficient MRG ciphers	Known PT attack on any MRG cipher $k \le 47$
Space (magnitude of words)	2^{18}	$2k$ (94 words when $k=47$)	≤ 4686 (about 2^{12})
Time (encryptions)	trivial	$48k$ (2256 when $k=47$)	$\le 2^{24}$ MRG ops + 2^{12} encryptions

- More details: eprint.iacr.org/2009/128, to be submitted to SAC 2009.