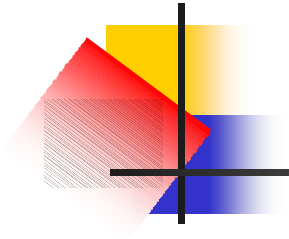
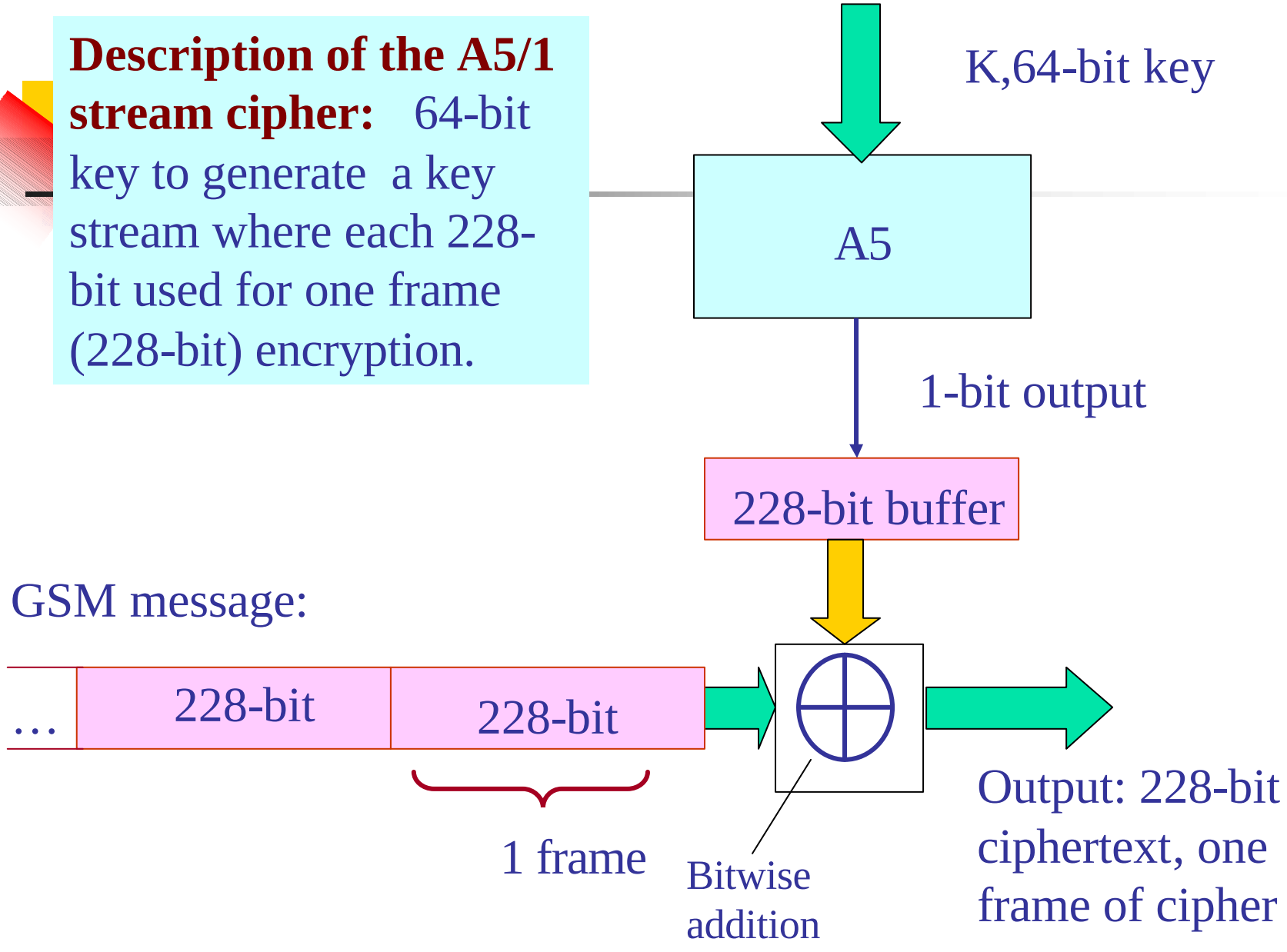


6.6 Case Study: A5 Stream Cipher

A. A5/1 stream cipher key generator for secure GSM conversations

Note. A GSM conversation is sent as a sequence of frames per 4.6 millisecond, and each frame contains 228 bits.

Description of the A5/1 stream cipher: 64-bit key to generate a key stream where each 228-bit used for one frame (228-bit) encryption.



Construction of A5/1 Generator:

Parameters:

(a) Three LSFRs which generate *m*-sequences with periods $2^{19} - 1$, $2^{22} - 1$, $2^{23} - 1$, respectively.

1. LFSR 1: $f_1(x) = x^{19} + x^5 + x^2 + x + 1$ generates $\underline{\mathbf{a}} = \{a(t)\}$.

2. LFSR 2: $f_2(x) = x^{22} + x + 1$ generates $\underline{\mathbf{b}} = \{b(t)\}$.

3. LFSR 3: $f_3(x) = x^{23} + x^{16} + x^2 + x + 1$ generates $\underline{\mathbf{c}} = \{c(t)\}$.

4. Tap positions: $d_1 = 11$, $d_2 = 12$ and $d_3 = 13$.

(b) Majority function $f(x_1, x_2, x_3) = (y_1, y_2, y_3)$ is defined by

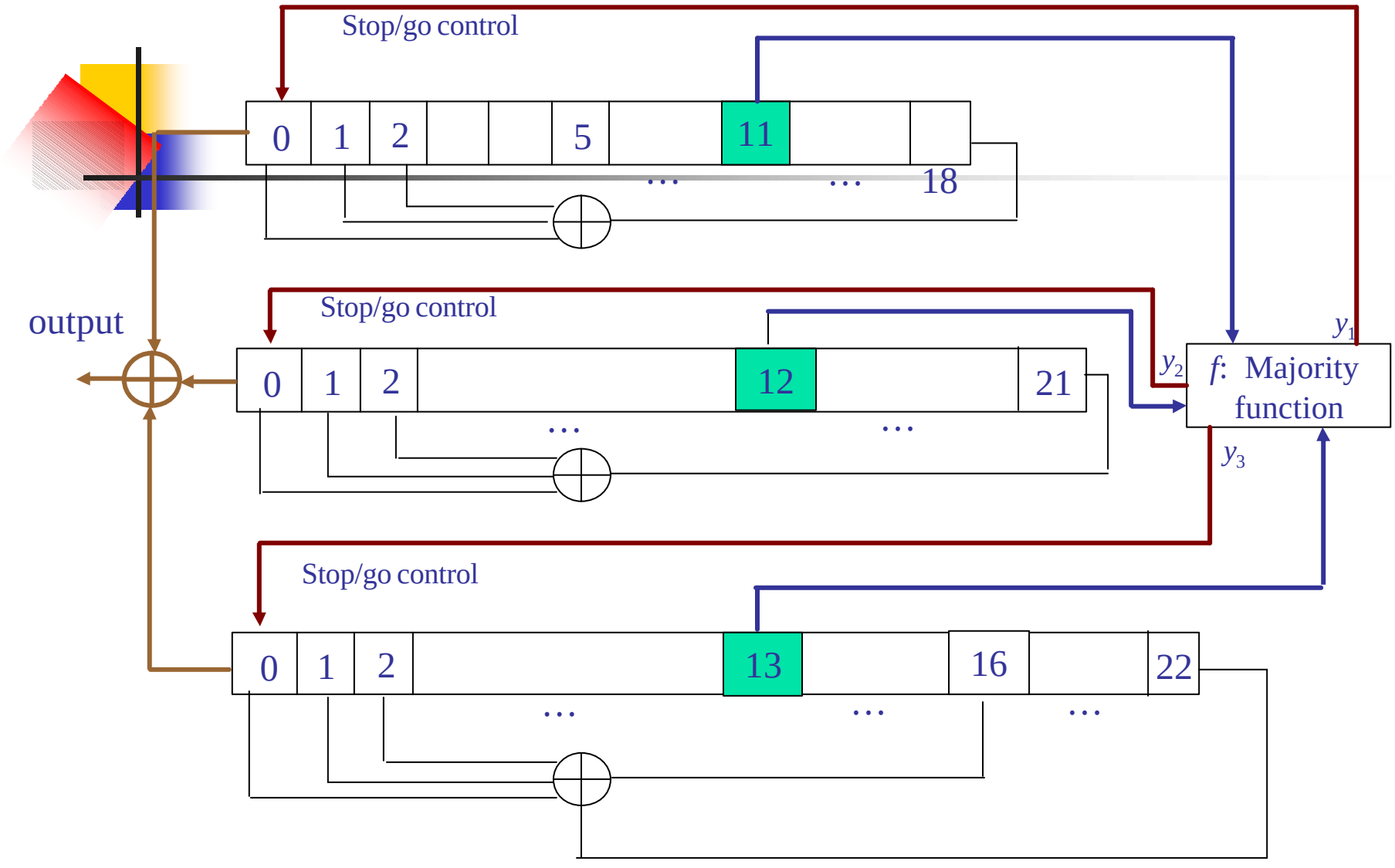
$f(a(t+11), b(t+12), c(t+13)) = (y_1, y_2, y_3)$	$a(t+11)$	$b(t+12)$	$c(t+13)$
(1,1,1)	0 1	0 1	0 1
(1,1,0)	0 1	0 1	1 0
(0,1,1)	0 1	1 0	1 0
(1,0,1)	1 0	0 1	1 0

Output:

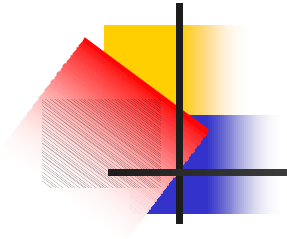
The output sequence $\underline{\mathbf{u}} = \{u(t)\}$ which performs at time t,

$$u(t) = a(i_1) + b(i_2) + c(i_3),\ t = 0, 1, \ldots$$

where i_1, i_2, and i_3 are determined in a stop-and-go clock controlled model by the majority function f.



A5/1 Key Stream Generator

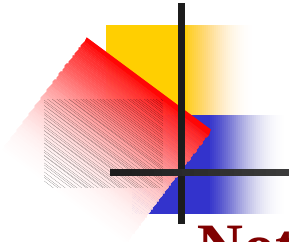


For example, at time t, if

$f(a(t+11), b(t+12), c(t+13)) = (1, 1, 0)$

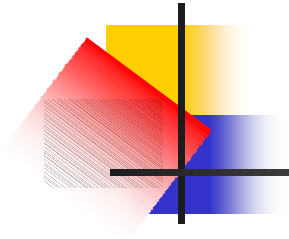
i.e., $(y_1, y_2, y_3) = (1, 1, 0)$, then LFSR 1 and LFSR 2 are clocked and LFSR 3 has no clock pulse.

Session key or seed: initial states for three LFSRs, a total of 64 bits.



Note 2. The first 'original' A5 algorithm was renamed A5/1. Other algorithms include A5/0, which means no encryption at all, and A5/2, a weaker over-the-air privacy algorithm. Generally, the A5 algorithms after A5/1 have been named A5/x. Most of the A5/x algorithms are considerably weaker than the A5/1, which has the time complexity of 254 at most as, shown above. The estimated time complexity of A5/2 is as low as 216. A5/3 is available in the work group of wireless communications

What does A5/1 suffer ?



• It can be broken with few hours by a PC.

• Short period problem: Without stop/go operation, the period of sum of the three LFSRs is given by

$$(2^{19}-1)(2^{22}-1)(2^{23}-1).$$

However, the experiement shows that the period of A5/1 is arround

$$(4/3)(2^{23}-1).$$

• Collision problem: different seeds (i.e., different initial states of three LFSRs) may result in the same key stream (our new results shows that only 70% seeds produce different key streams.)

• The maority function is the worst function in terms of correlation with all affine functions.

Possible Attacks on A5/1

- **Brute-Force Attack against A5**

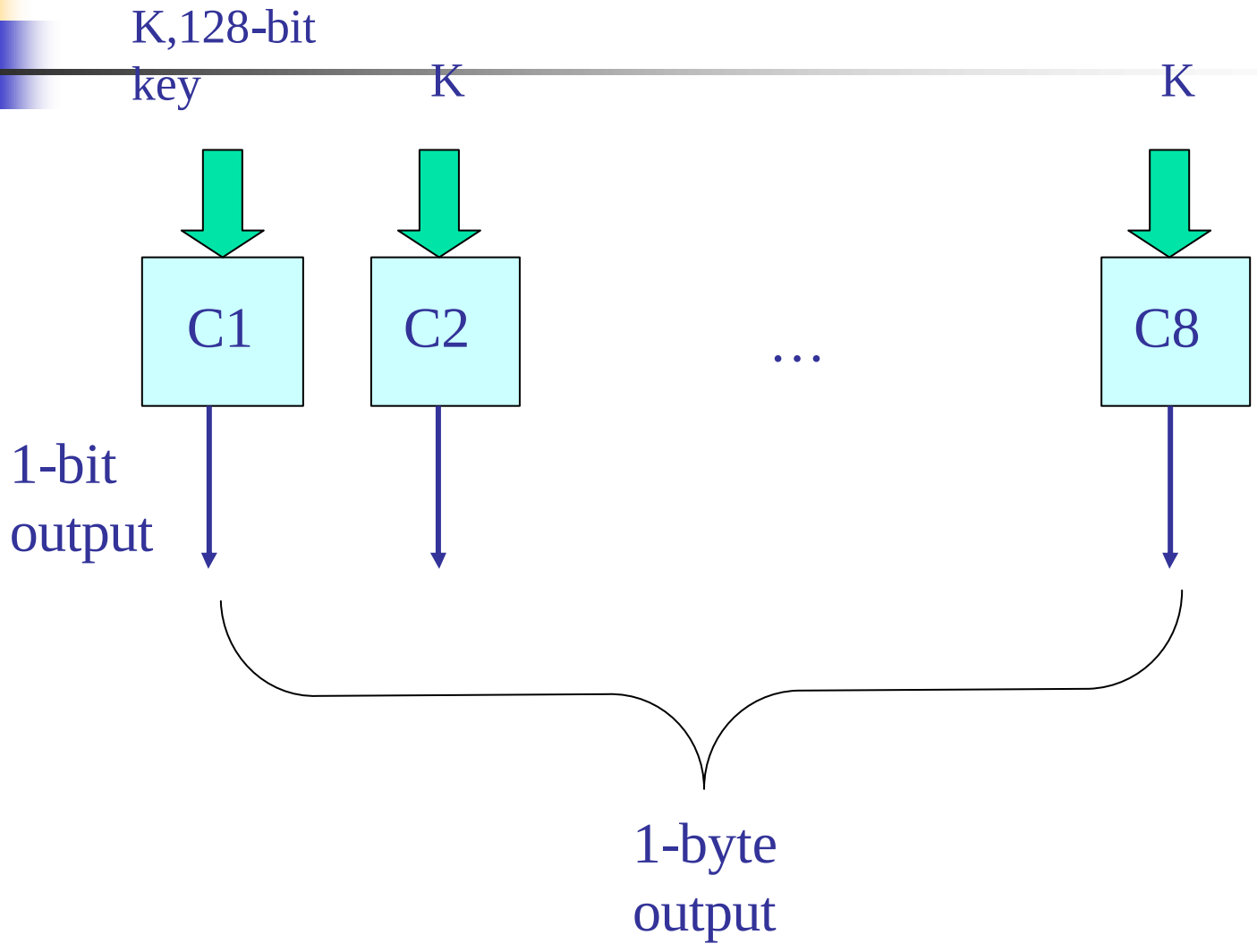
  If we have a Pentium III class chip with approximately 20 million transistors and the implementation of one set of LSFRs (A5/1) would require about 2000 transistors, we would have a set of 10,000 parallel A5/1 implementations on one chip. If the chip was clocked to 600 MHz, we could try approximately 2M keys per second per A5/1 implementation. A key space of 2^{54} keys would thus require about 900,000 seconds, 250 hours, with one chip.

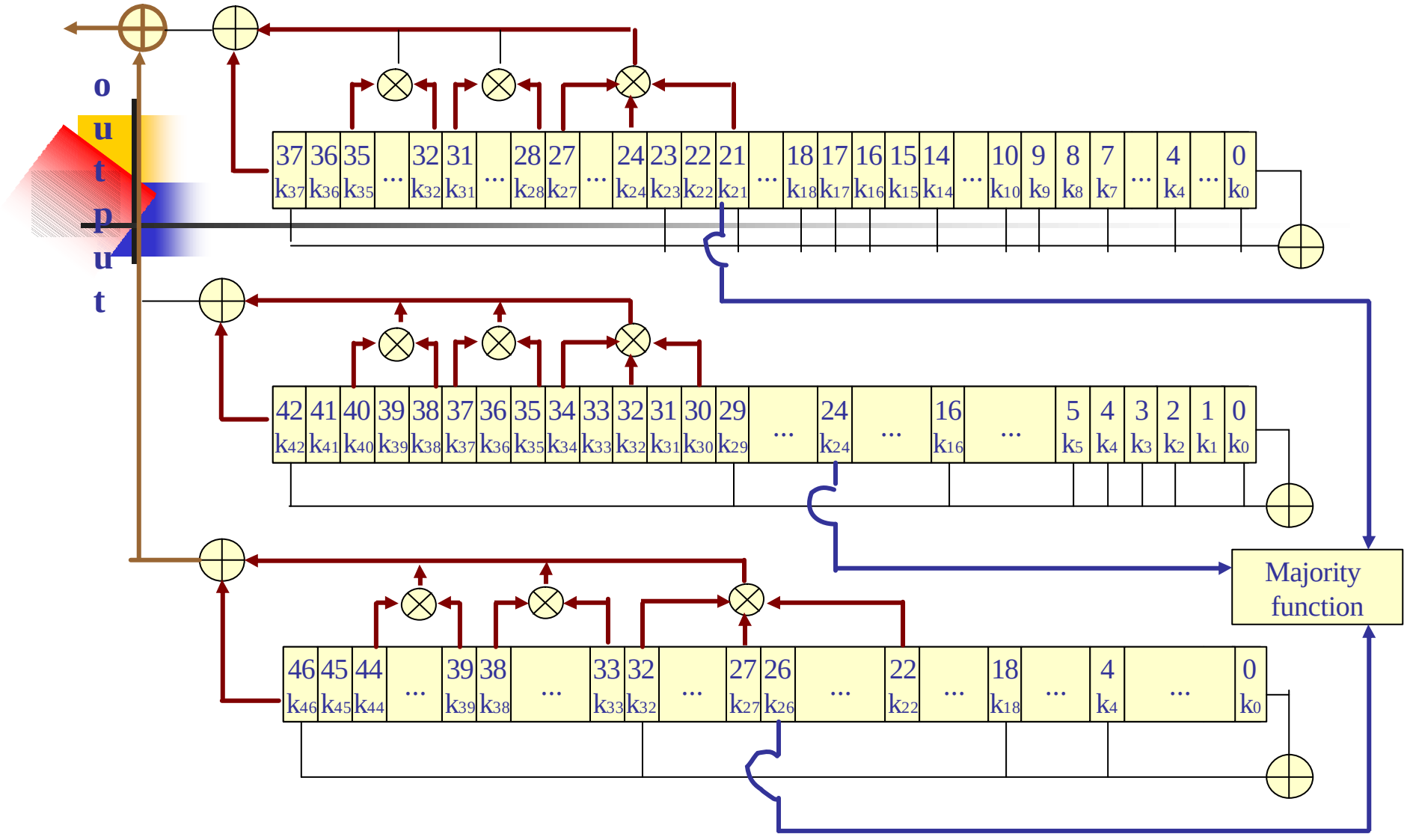
- Alex Biryukov and Adi Shamir (co-inventor of the RSA) claim to be able to penetrate the security of a A5/1 ciphered GSM call in less than one second using a PC with 128 MB RAM and large hard drives.

6.7. w7 -- an Analogue Cipher of A5

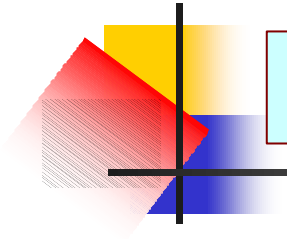
w7 stream cipher algorithm is proposed by S. Thomas, D. Anthony, T. Berson , and G. Gong published as an INTERNET DRAFT, April 2002.

Description of w7: The w7 algorithm is a byte-wide, synchronous stream cipher optimized for efficient hardware implementation at very high data rates. It is a symmetric key algorithm supporting key lengths of 128 bits. It contains eight similar models, C1, C2, …, C8 where C2 is illustrated as follows.


K,128-bit
key
K
K
C1
C2
…
C8
1-bit
output
1-byte
output



The W7 Cipher Algorithm



6.8. Correlation Attack to Stream Ciphers

Self reading.

References

1. "GSM (and PCN) security and encryption", at *Brookson*http://www.brookson.com/gsm/gsmdoc.htm
2. "GSM interception" , at http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-9900/a5/Netsec/netsec.html
3. "Wireless security", http://www.compaq.ch/ins_wpwirelesssecurity.pdf
4. "Security of mobile systems from user's point of view", at http://www.hut.fi/~hansen/papers/user-secu/