Attacks on A5/2

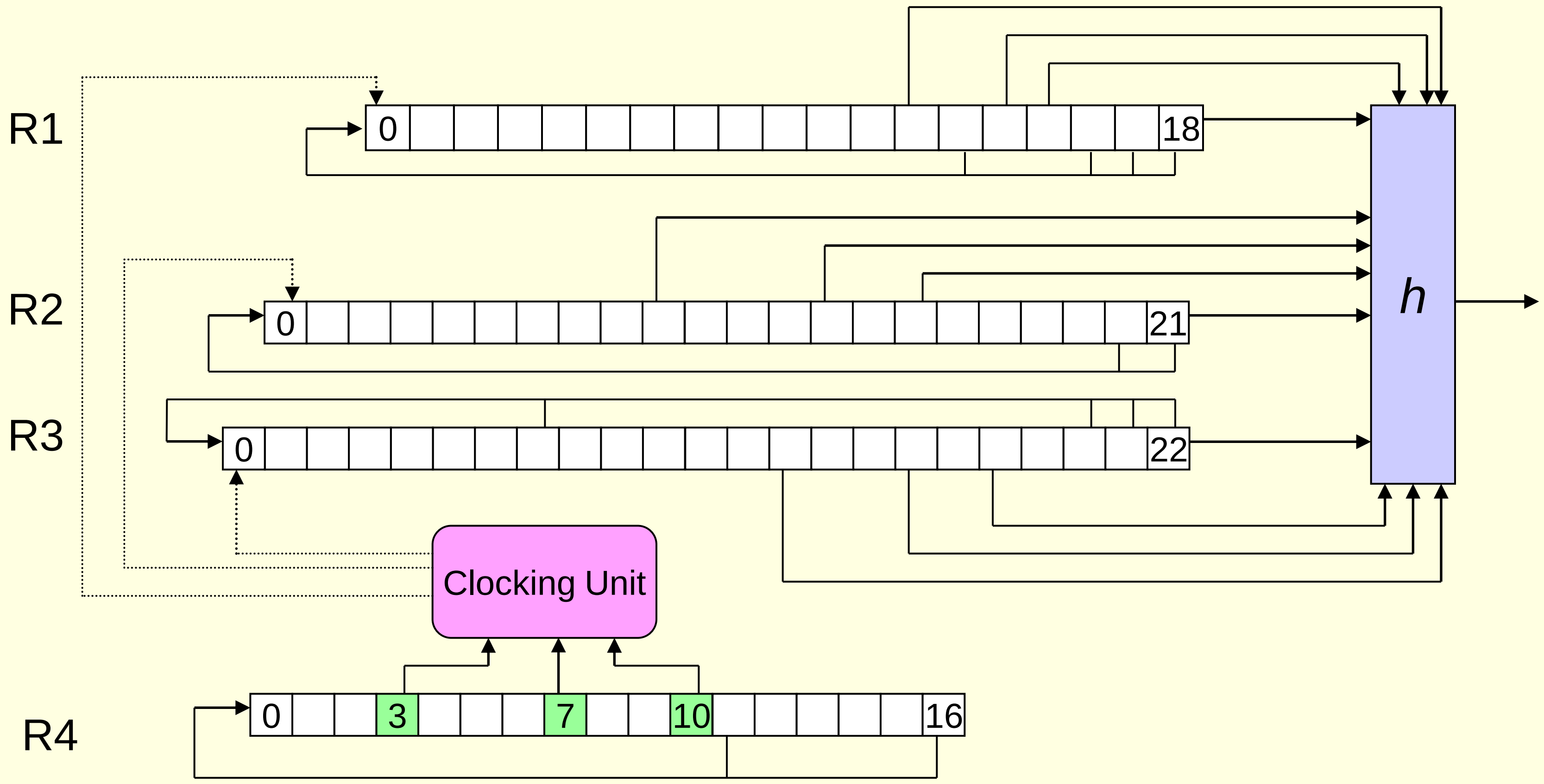
Mehdi Hassanzadeh

Selmer Center, University of Bergen, Norway

FRISC Winter School, Finse, May 6-11, 2012

Contents

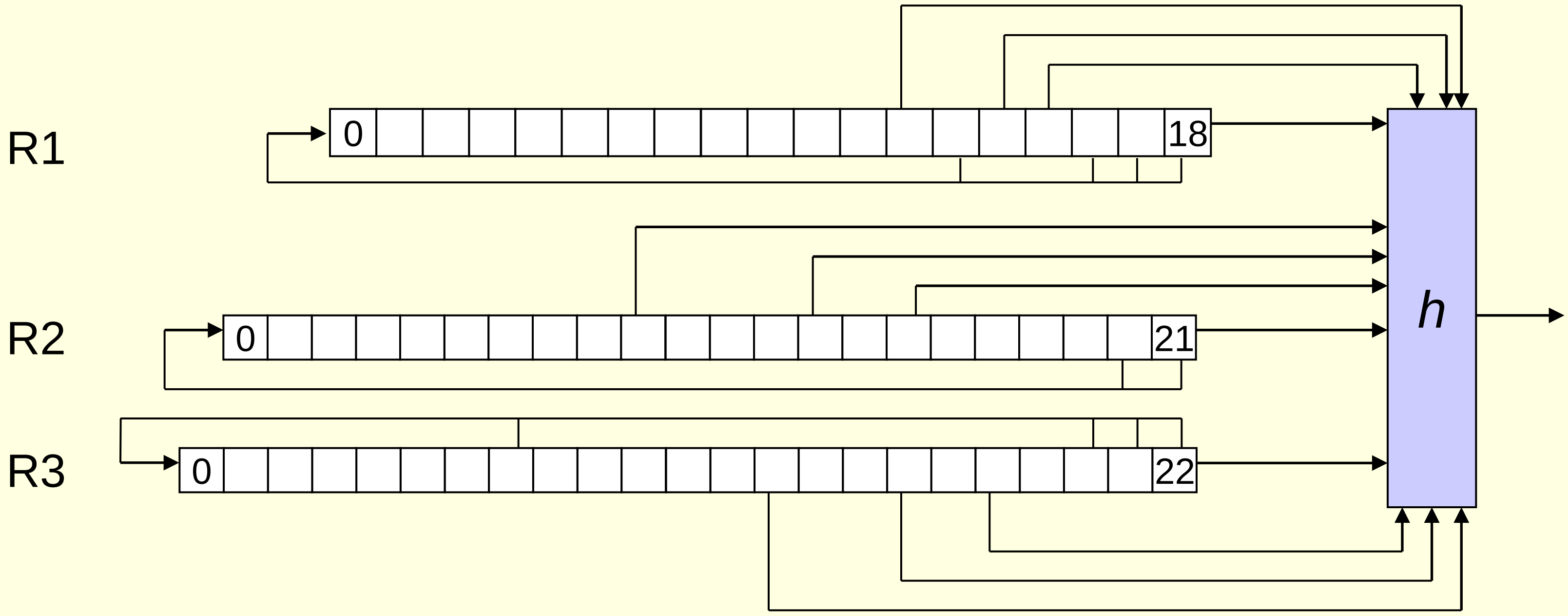
A5/2 Structure



Clocking unit

R4[10], R4[3], R4[7])	Registers that are clocked
(0,0,0) or (1,1,1)	R1 , R2 , R3
(1,0,0) or (0,1,1)	R2 , R3
(0,1,0) or (1,0,1)	R1 , R3
(0,0,1) or (1,1,0)	R1 , R2

Output Filter



$$h(x_1,x_2,\ldots,x_{12})=\sum a_{ij}x_ix_j \oplus \sum a_ix_i \oplus a_0$$

Initialization and generation

Initialization:

- Reset all 4 registers
- Load 64 bit key to registers
- Load 22 bit frame number to registers
- Force on bit of each register to be set

Generation:

- Clock A5/2 and discard output (99 times)
- Clock A5/2 and get output (228 times)

Attacks On A5/2

1. Goldberg , Green and Wagner 99
   1. Known plaintext attack
   2. Needs two frame which are exactly 2^{11} frame apart.
   3. Recovers key in:
      1. Less than one minutes
      2. Less than 1 sec with 1 min preprocessing and 28 MB memory.

Attacks On A5/2

3. Barkan , Biham and Keller 2003
   1. Known plaintext attack
   2. Needs a 4 frame information.
   3. Recovers key in:
      1. 20 min .
      2. Less than 1 sec from 16 frame.
         with 160 min precomputation and 250 MB memory.

Attacks On A5/2

4. Barkan , Biham and Keller 2003
   1. It is an ciphertext-only attack.
   2. Needs 16 frames of encrypted unknown data.
   3. Recovers key in:
      1. 20 min
      2. Less than 1 sec from 16 frame.
         with 160 min precomputation and 250 MB memory.

GGW attack

- $f \oplus f' \rightarrow R_i \oplus R'_i$
- $\therefore\ f \oplus f' = 2048 \rightarrow R_4 = R'_4$
- The output filter is a quadratic function:

  $h(x_1, x_2, \ldots, x_{12}) = \Sigma\, a_{ij} x_i x_j \oplus \Sigma\, a_i x_i \oplus a_0$

$$\therefore\ h(x_1, x_2, \ldots, x_{12}) \oplus h(x_1 \oplus d_1, x_2 \oplus d_2, \ldots, x_{12} \oplus d_{12}) = \Sigma\, c_i x_i \oplus c_0$$

GGW attack

- Suppose that we know R4
- $z_n \oplus z'_n = \Sigma c_{ni} x_i \oplus b_n$
- We can construct the linear equation set $CX = Z \oplus Z' \oplus B$
- If the equation set is consistent R4 is true initial state for 4th register, else R4 is not real initial state for 4th register.

BBK attack

- Each output bit is quadratic function of initial state of R1, R2 and R3.
- Each quadratic term $x_i x_j$ is considered as a new variable, and system equation is linearized.
- Total number of variables is 656.

$$18+\binom{18}{2}+21+\binom{21}{2}+22+\binom{22}{2}+1=656$$

BBK attack

- V is a vector with length 656 that contain all linearized variables .
- Knowing R4 and f, we can write $z_n = \Sigma\ c_n v_i$
- Consider four consecutive frame with number f, f+1, f+2, and f+3 and output Z_0, Z_1, Z_2, Z_3
- $Z = Z_0 \| Z_1 \| Z_2 \| Z_3$
- Knowing initial state of 4th register of first frame we can write Z = AV

BBK algorithm

1. Choose an initial state for R4
2. Compute A
3. $Z = Z_0 \| Z_1 \| Z_2 \| Z_3$
4. construct the linear equation set $Z = AV$.
5. If the equation set is not consistent, go to 1.

Vector V

element	#elements	index
R1	19	1-19
R2	22	20-41
R3	23	42-64
QR1	171	65-235
QR2	231	236-466
QR3	253	467-719

$$V = \begin{bmatrix} R1(1) \\ \ldots \\ R1(19) \\ R2_{22*1} \\ R3_{23*1} \\ R1(1).R1(2) \\ R1(1).R1(3) \\ \ldots \\ R1(18).R1(19) \\ QR2 \\ QR3 \end{bmatrix}$$

Transition Matrix M1

$$M1 = \begin{bmatrix} 0100000000000000000 \\ 0010000000000000000 \\ 0001000000000000000 \\ \ldots \\ 0000000000000000001 \\ 1110010000000000000 \end{bmatrix} \qquad R1 = \begin{bmatrix} R1(1) \\ R1(2) \\ . \\ . \\ . \\ R1(19) \end{bmatrix}$$

$$R1^t = M1 * R1^{t-1} = M1^t * R1^0$$

Transition Matrix G0

$$G0 = \begin{bmatrix} M1 \ 0000000000000000000 \\ 00 \ M2 \ 0000000000000000 \\ 000000 \ M3 \ 00000000000 \\ 000000000 \ QM1 \ 0000000 \\ 00000000000000 \ QM2 \ 000 \\ 0000000000000000000 \ QM3 \end{bmatrix}$$

$$V = \begin{bmatrix} R1_{19*1} \\ R2_{22*1} \\ R3_{23*1} \\ R1(1).R1(2) \\ R1(1).R1(3) \\ \ldots \\ R1(18).R1(19) \\ QR2_{231*1} \\ QR3_{253*1} \end{bmatrix}$$

R1(1).R1(2) ← R1(2).R1(3)

R1(1).R1(3) ← R1(2).R1(4)

. . .

R1(1).R1(18) ← R1(2).R1(19)

R1(1).R1(19) ←R1(2).(R1(2)+R1(3)+R1(4)+R1(7))

Transition Matrix G1,G2,G3

$$G1 = \begin{bmatrix} M1 & 0 & 0 & 0 & 0 & 0 \\ 0 & M2 & 0 & 0 & 0 & 0 \\ 0 & 0 & M3 & 0 & 0 & 0 \\ 0 & 0 & 0 & QM1 & 0 & 0 \\ 0 & 0 & 0 & 0 & QM2 & 0 \\ 0 & 0 & 0 & 0 & 0 & QM3 \end{bmatrix}$$

Linear Equation system

First Frame number give us 114 linear equations:

$$Z_i = P\prod_{k=1}^{i+99} G_k V \qquad G_k \in \{G0, G1, G2, G3\}$$

Consider difference of frame numbers and extract more linear equations:

$$Z^f{}_i = P\prod_{k=1}^{i+99} G_k V \oplus P\prod_{k=1}^{i+99} G_k \Delta F_{1,f}$$

Complexity

- 2^16 search on R4
- Solving a linear equation system with 656 variables= 656^3=2^28
- Total=2^44 bit-xor operation
- 32-bit machine=> Complexity=2^39

- But we need to find first 61 variables=partial gauss elimination=61^3=2^18
- Then Complexity=2^29

Optimization

- Pre-Computation=2^46 bit-Xor operations =160 minutes
- Complexity=2^28 bit-Xor operations
- 32-bit machine= 2^23 < 1 second
- Memory= 250 MB
- Need more data

Security of 3th generation

A5/3

A5/3

- A5/3 is a block cipher called KASUMI
- KASUMI is a modified version of the MISTY
- Developed in 2002
- Published in 2003
- 8 round Feistel structure
- 64 bit blocks
- 128 bit key lenght
- Never full round of MISTY is broken

Attack on A5/3

- Orr Dunkelman, Nathan Keller, and Adi Shamir, 2010
- Distinguisher for 7 round with prob. 2^-14
- Using
  - 4 related keys
  - 2^26 data
  - 2^30 Bytes memory
- Time Complexity=2^32 Xor operation< two hours

Thank You !