An Improved Attack on A5/1

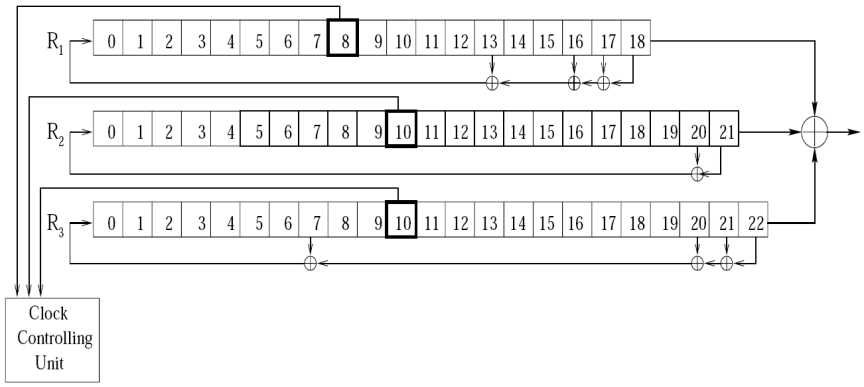
Vahid Amin Ghafari
Information and Communication Technology complex
Malek Ashtar University of Technology
Tehran, Iran
vahidaming@yahoo.com

Javad Mohajeri
Electronic Institute
Sharif University of Technology
Tehran, Iran
mohajer@sharif.ir

Outline

- A5/1 Structure
- Biham and Dunkelman's Attack
- Our Improvement
- Contradictory States
- Time Complexity of the Attack
- Decrease Data Complexity

A5/1 Structure



3

Cryptanalysis of the A5/1

- Attacks against A5/1 are divided into two categories: active and passive.
- Passive attacks can be divided into three classes:
  - guess-and-determine
  - time-memory-data tradeoff
  - correlation attacks

4

Biham and Dunkelman's Attack

- This attack is guess-and-determine that improved by exploiting a precomputed table.
- The main idea was to wait until an event which leaks a large amount of information about the internal state occurs.

5

Our Improvement

- Our improvement is identification and elimination of useless states from the precomputed table.

Attack	Precomputation complexity	Time complexity	Data complexity (known bits)	Memory Complexity	Success Rate
Biham & Dunkelman	2^38	2^39.91	2^21.1	32 GB	63%
Our improvement	2^38	2^37.89	2^21.1	≈ 16 GB	63%

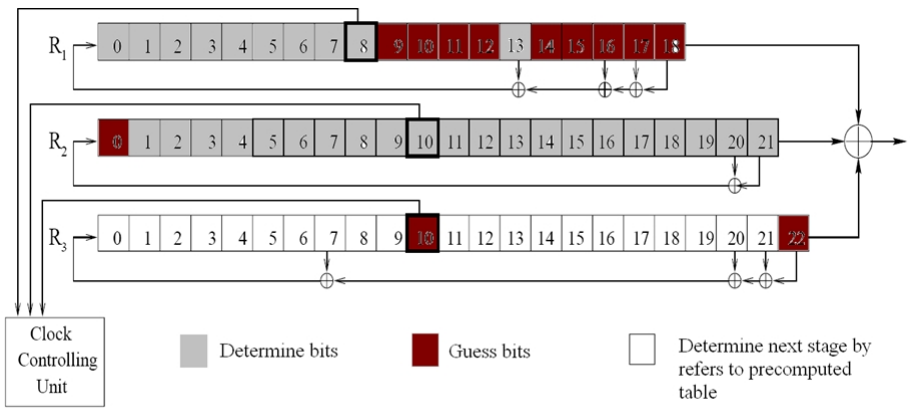
6

Biham and Dunkelman's Attack

- Suppose that for 10 consecutive clock cycles, register R_3 is not clocked.
- R_1 [9,10,11,12,14,15,16,17,18], R_2 [0] and R_3[10,22] are guessed and then all bits of R_1 and R_2 are recovered

7

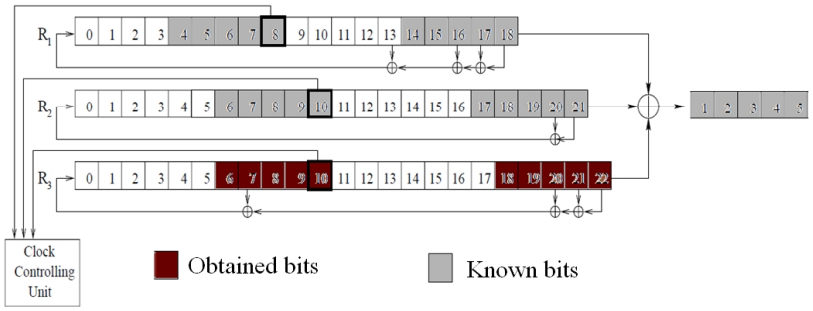
Biham and Dunkelman's Attack



8

Biham and Dunkelman's Attack

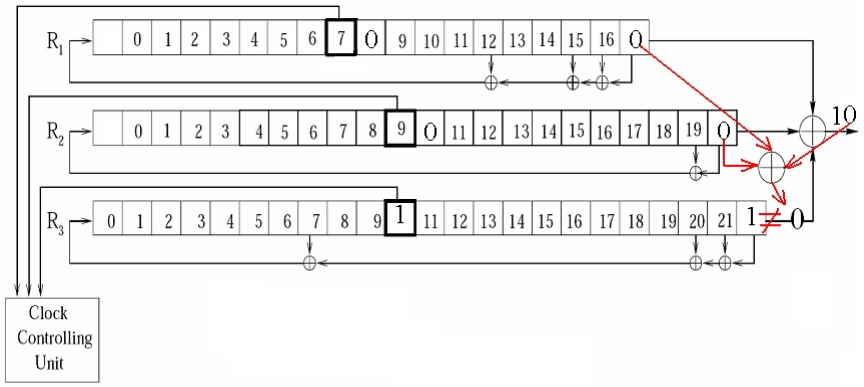
- In the second step, the attacker refers to the precomputed table and recovers remaining bits of R_3.



9

Contradictory States

- Biham and Dunkelman has not been mentioned it.



10

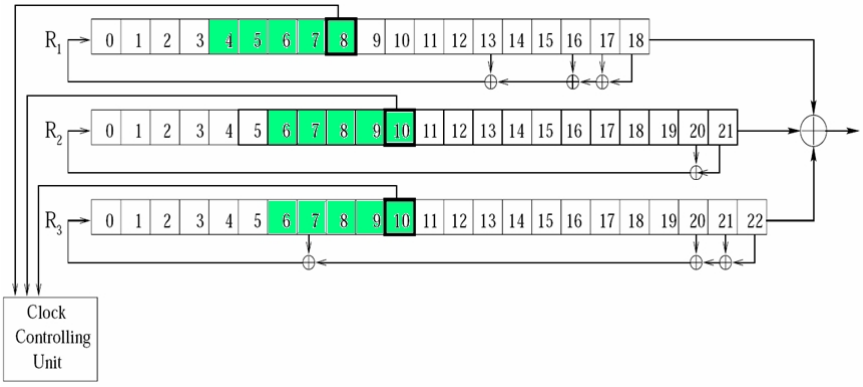
Contradictory States

- The probability of contradiction after first clock cycle is 1/4×1/2=1/8
- the probability of contradiction after n th clock cycle is (7/8)^(n-1)×1/8
- we sum the probability of contradictions in the first 5 clock cycles
- almost half of the cases in the table are contradictory, and they can be eliminated from the table.

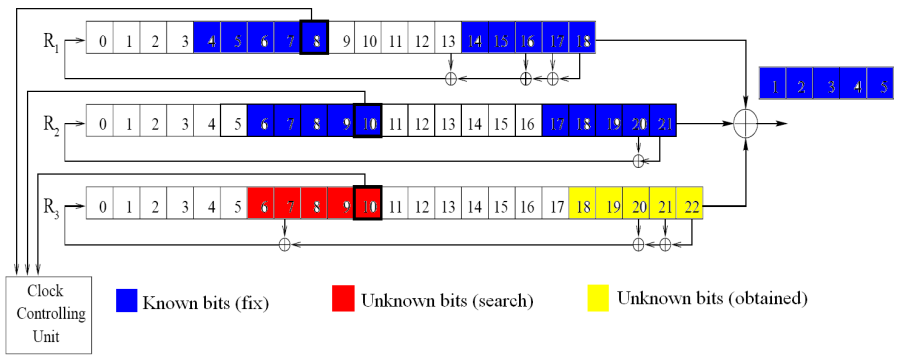
11

Contradictory States

- percentage of consistency for different lengths of output for 15 bits of clock controlling



12



	All possible cases	Output stream with length 5 bits	Output stream with length 6 bits	Output stream with length 7 bits
Number	1789394944	15968	14280	2520
Percentage of consistency	50.1%	64.3%	47%	36.2%

13

Time Complexity of the Attack

- The average number of candidates for the 20 bits of R_1 , R_2 and 5 bits of the output stream is (2^3.75≈13.52). This amount in [3] is 23.2
- 1/(2^10(15968×0.64+14280/2×0.47+2520/4×0.362)=13.52
- The result can be improved by using more bits in the table

14

Time Complexity of the Attack

- For each 2^20 strings, there are 2^12 possible cases for guessing
- in first access to the table, attacker gets 2^0.3 candidates on average
- in the second access to the table, attacker gets 2^3.3 candidates
- in the third access to another table, attacker gets 2^(-0.57)≈(0.67) candidates

15

Time Complexity of the Attack

- 2^20×2^12×2^0.3×2×2^3.3((1+1)+2×0.67)=2^38.34
- Another our improvement is using of negligible memory in the online phase of the attack, time complexity is decreased to
- 2^20×2^12×2^0.3×2×(1+2^3.3(1+2×0.67))=2^37.89

16

Decrease Data Complexity

- we can decrease the amount of the known bits by time-data tradeoffs.
- A and B attacks are based on this assumption that R_3 is not clocked for 4 and 3 clock cycles respectively.

	Precomputation complexity	Time complexity	Data complexity (frame)	Memory Complexity (GB)	Success Rate
A	2^38	2^44.19	4	16	55%
B	2^38	2^47.19	4	16	96%

17

Thank you

Any question?

18