[1]: Xiaoyun Wang, Hongbo Yu: How to break MD5 and Other Hash Functions, Advances in EUROCRYPT2005, LNCS 3494, pp. 19-35, Springer-Verlag, 2005.

Message Modification for MD5

Yu Sasaki

The University of Electro-Communications, Japan

(Joint work with Yusuke Naito, Noboru Kunihiro, Kazuo Ohta)

The Attack of Wang et al.

- Sufficient Conditions are constructed to generate collisions.

Conds in 1st round	Conds from 2nd round
⇩	⇩
All conds are satisfied with probability 1.	Some conds are corrected, others are not.
	We found message modification satisfying more conditions

3

Our Results

Comparison of the complexity of finding a collision

Wang et al.[1]	2^{37} (2^{31})
Klima[2]	2^{33}
Liang et al.[3]	2^{33}
Ours	$\approx 2^{29}$

Black et al.[4] : 2^{30}?

it: MD5 operations

4

Idea 1: Message Modification for Conditions in 2nd Round.

A: Total num of conds in 2R

Black et al.[4]	15	13	$15/16$?	2^{-2} ?

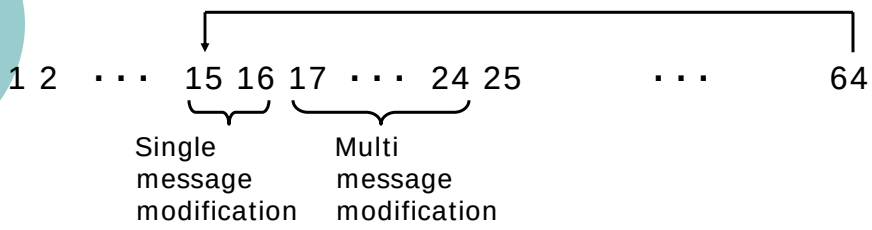
Pr_1: Success prob of [illegible]

	A	**B**	**Pr_1**	Success prob of 2R
Wang et al.[1]	15	6	≈ 1	2^{-9}
Klima[2]		10	≈ 1	2^{-5}
Liang et al.[3]		10	≈ 1	2^{-5}
Ours		**14**	**1 / 2**	**2^{-2}**

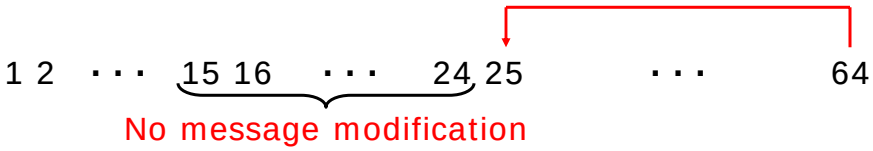
5

Idea 2: Message Modification for Quick Repetition

Original Restart Point: Step 15



Ours: Step **25**



6

Conclusion

- **MM for 2nd round**

correct 14 conds, but error rate: 1/2

Applicable to other hashs? ⟶ ***Yes!!***

- **MM for quick repetition**

save the complexity of collision search

Applicable to other hashs? ⟶ ***Yes!!***

[1]: Xiaoyun Wang, Hongbo Yu: How to break MD5 and Other Hash Functions, Advances in EUROCRYPT2005, LNCS 3494, pp. 19-35, Springer-Verlag, 2005.

[2]: Vlastimil Klima: Finding MD5 Collisions on a Notebook PC Using Multi-message Modifications, Cryptology ePrint Archive 102, 2005

[3]: Jie Liang, Xuejia Lai: Improved Collision Attack on Hash Function MD5, Cryptology ePrint Archive 425, 2005

[4]: John Black, Martin Cochran, Trevor Highland: A Study of the MD5 Attacks: Insights and Improvements, FSE 2006

Thank You!!