

✂ On behavior of Professors Ohta and Sakiyama.



Free-start preimages of round-reduced Blake compression function

Lei Wang, Kazuo Ohta and Kazuo Sakiyama

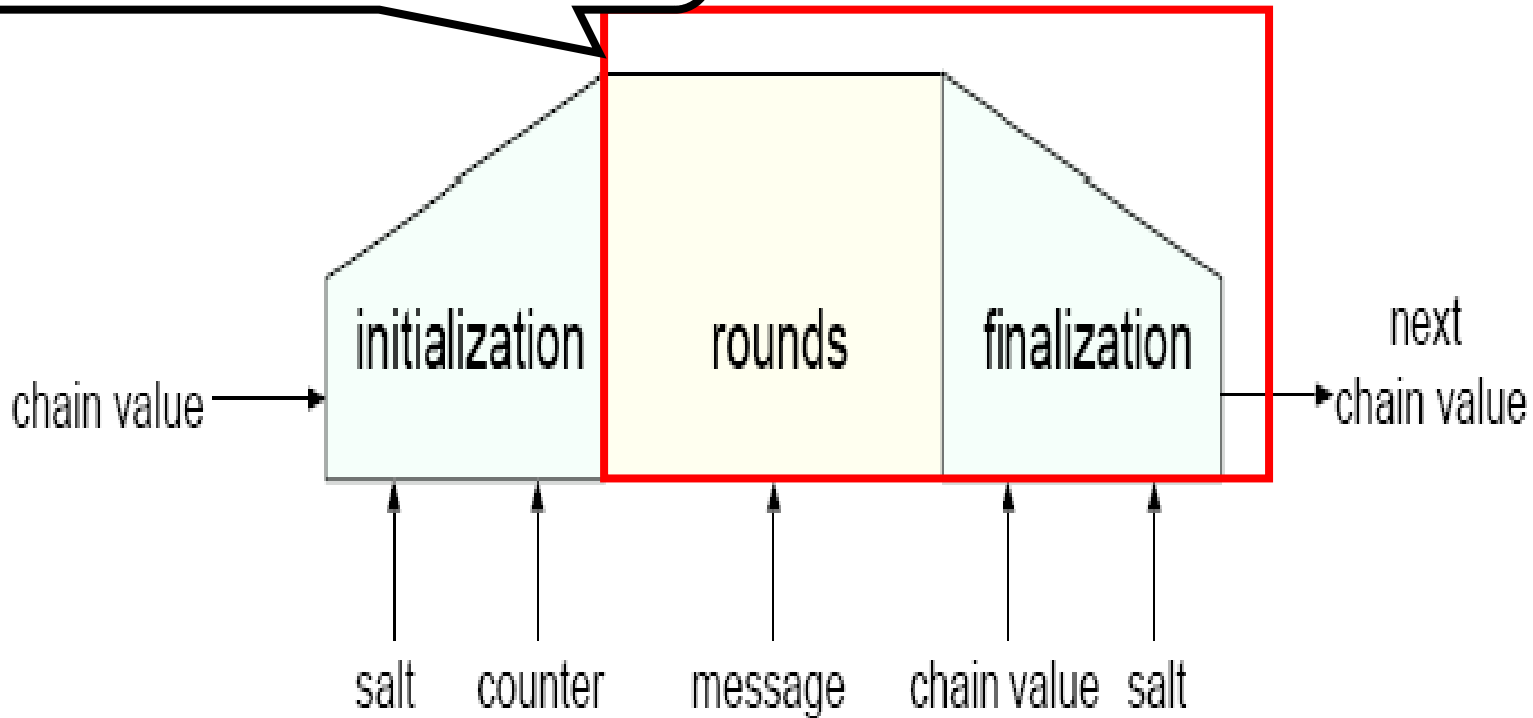
The University of Electro-Communications, Japan

Blake

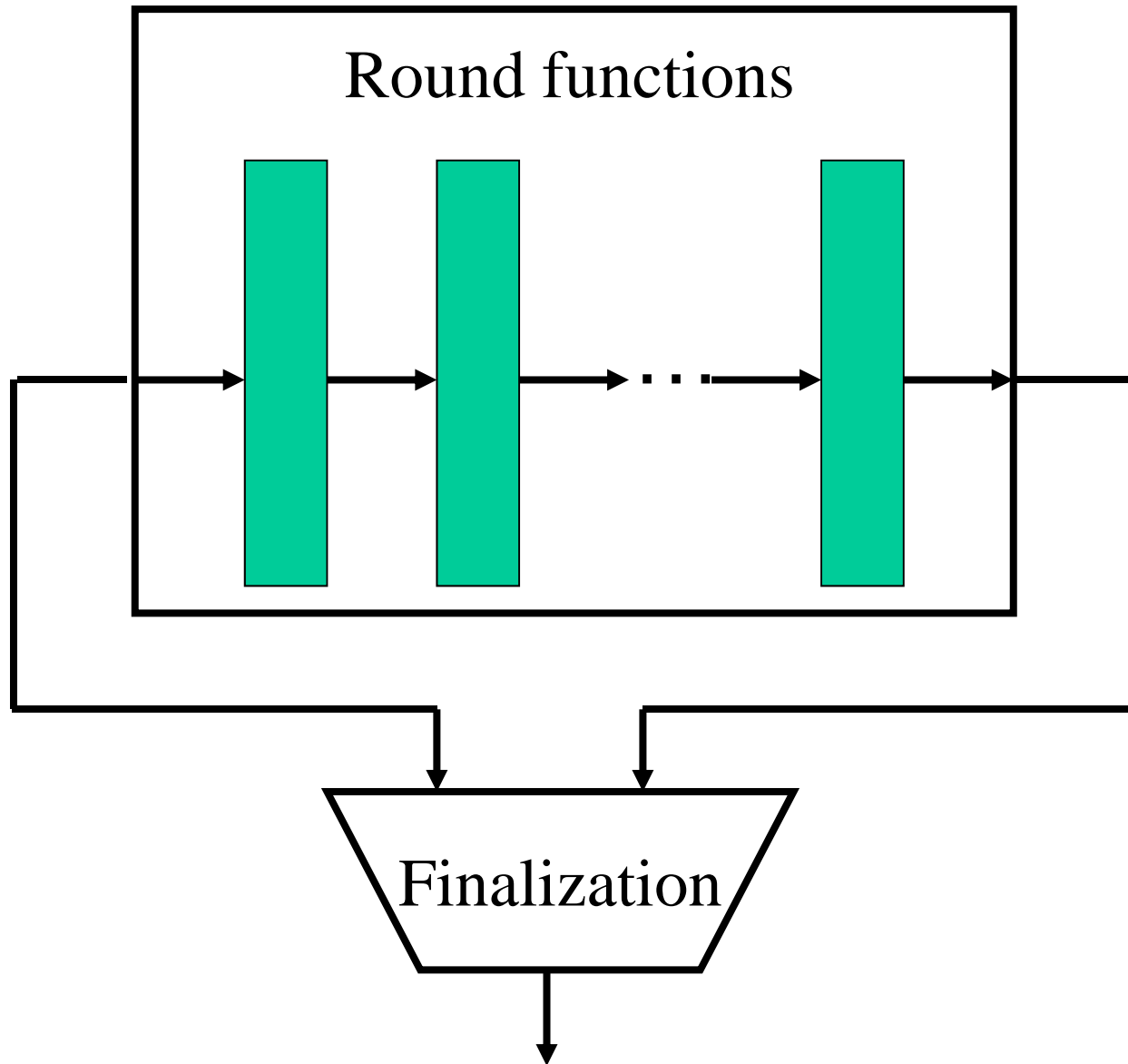
- ◆ A candidate in second round for SHA-3 competition proposed by Aumasson et al.

Specification of Black compression function

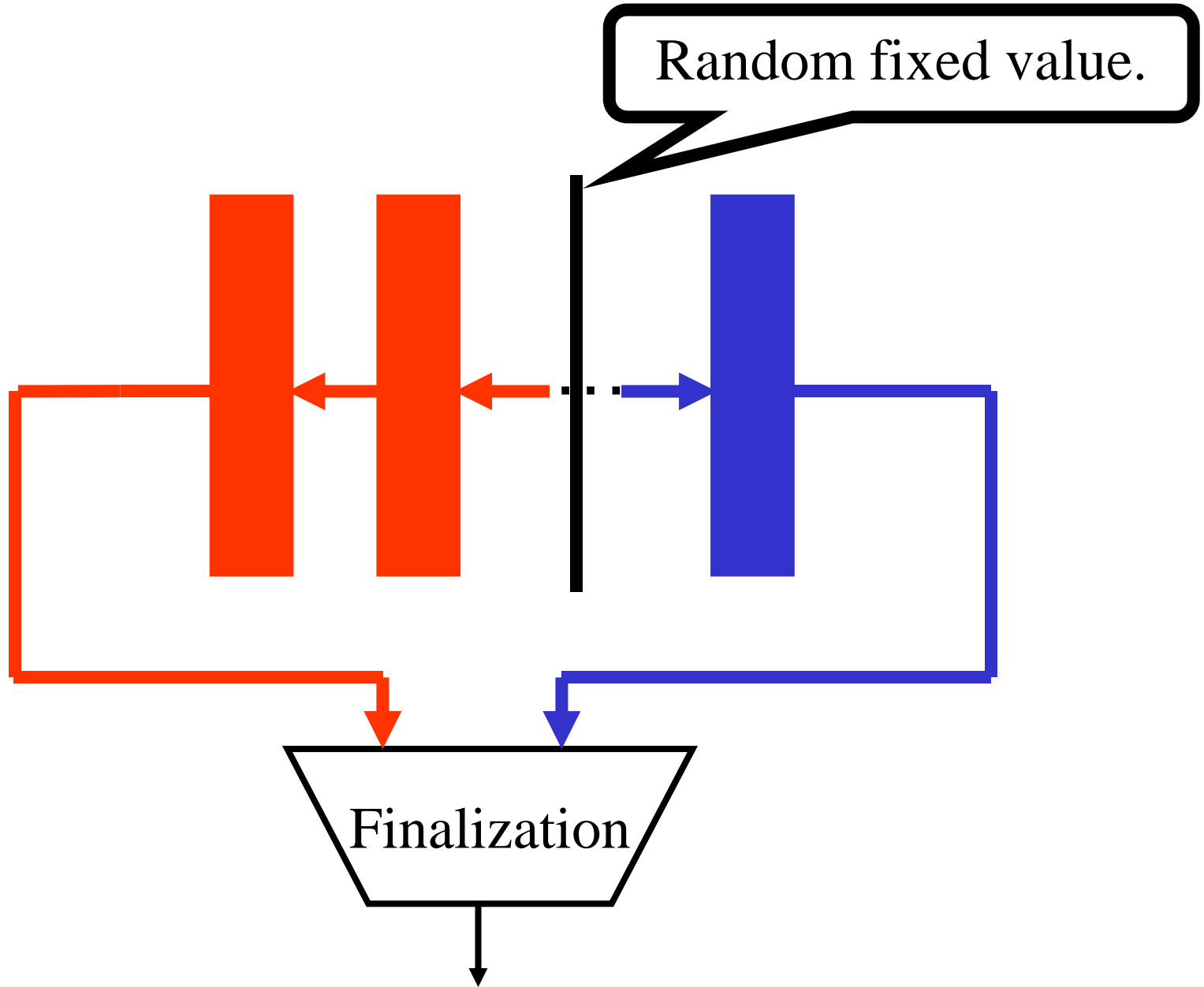
Random starting value
(free-start)



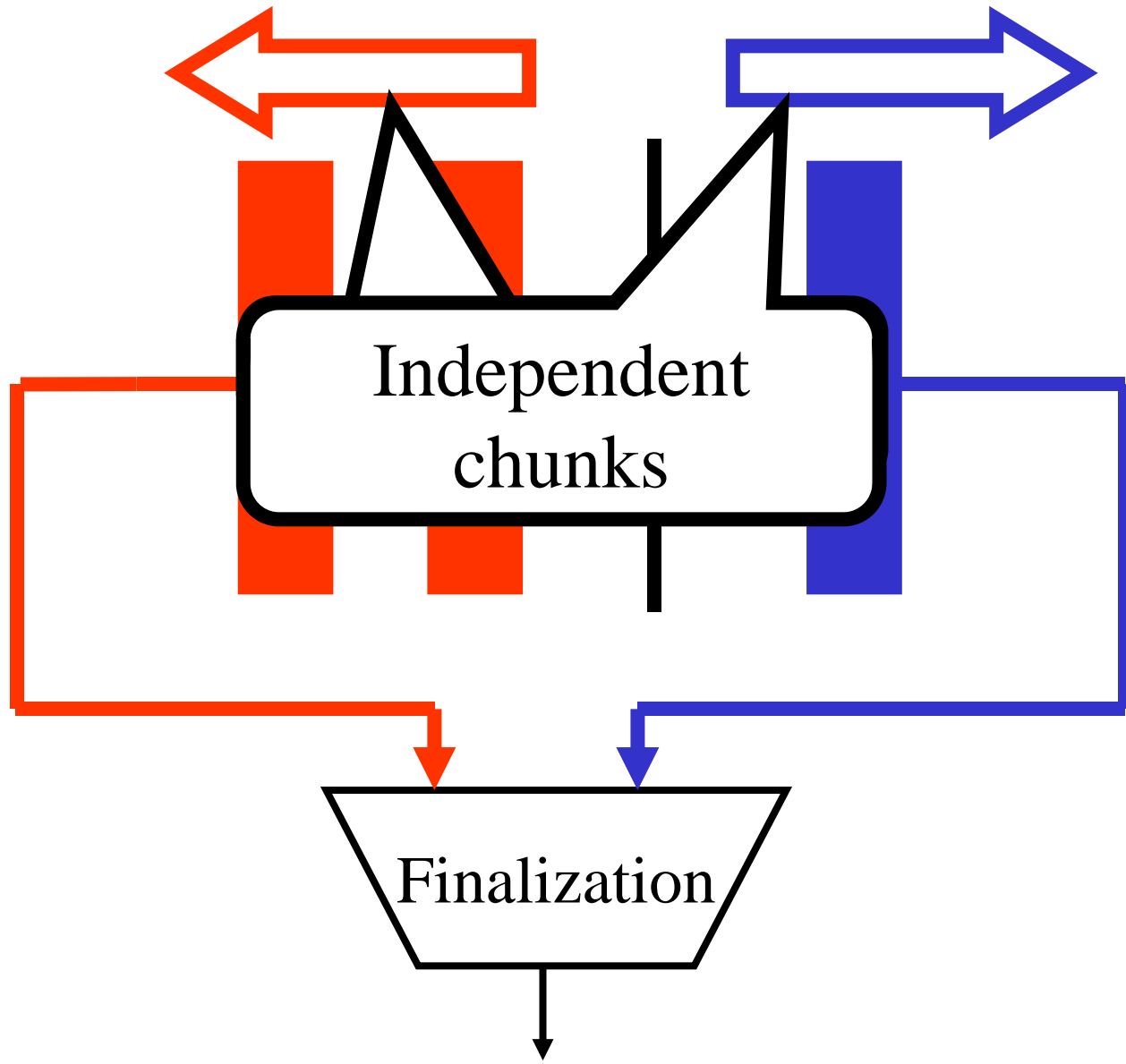
What Black compression function becomes?



Attack scenario

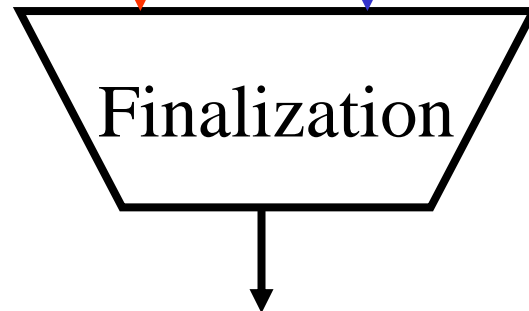


Attack scenario

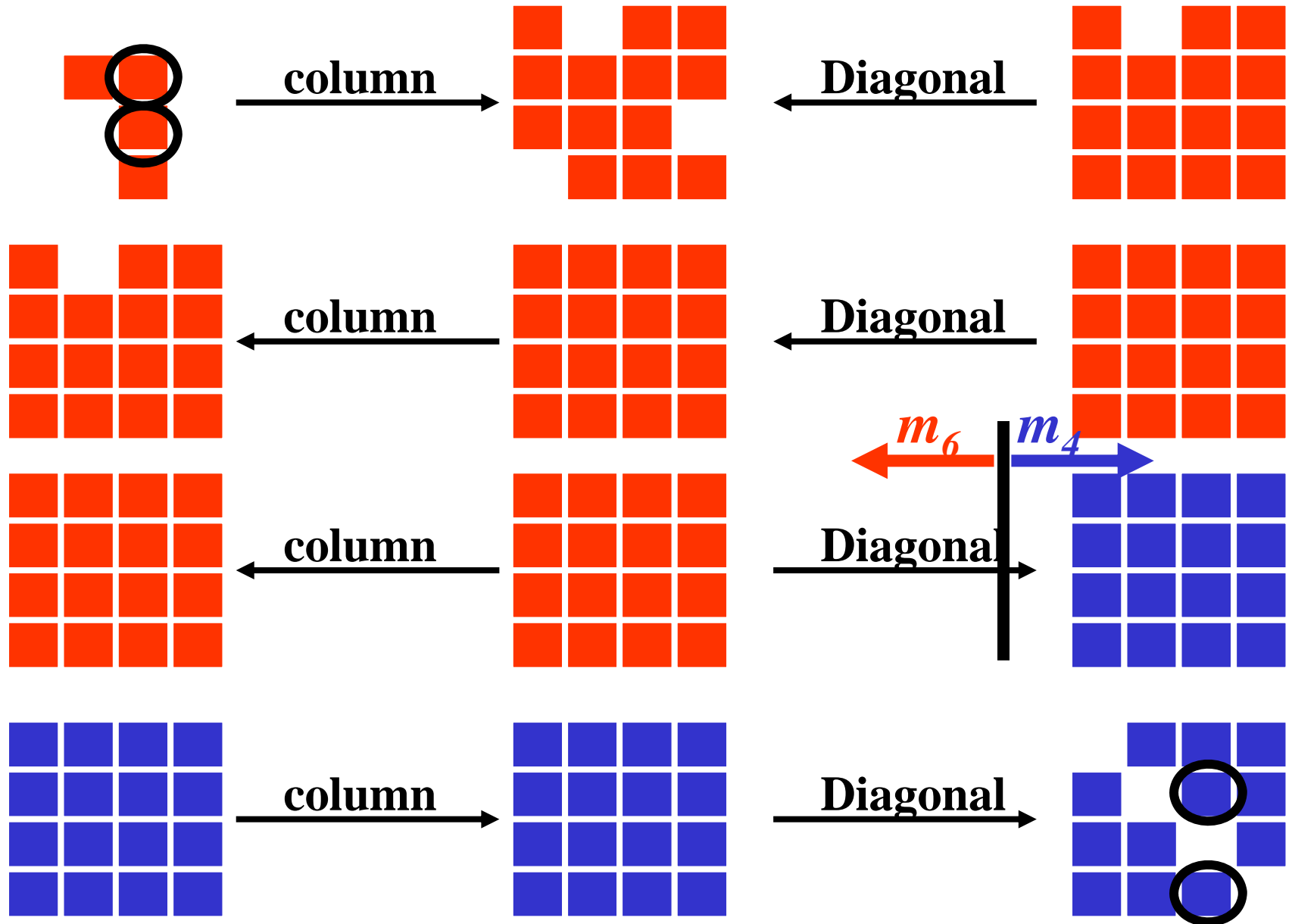


Attack scenario

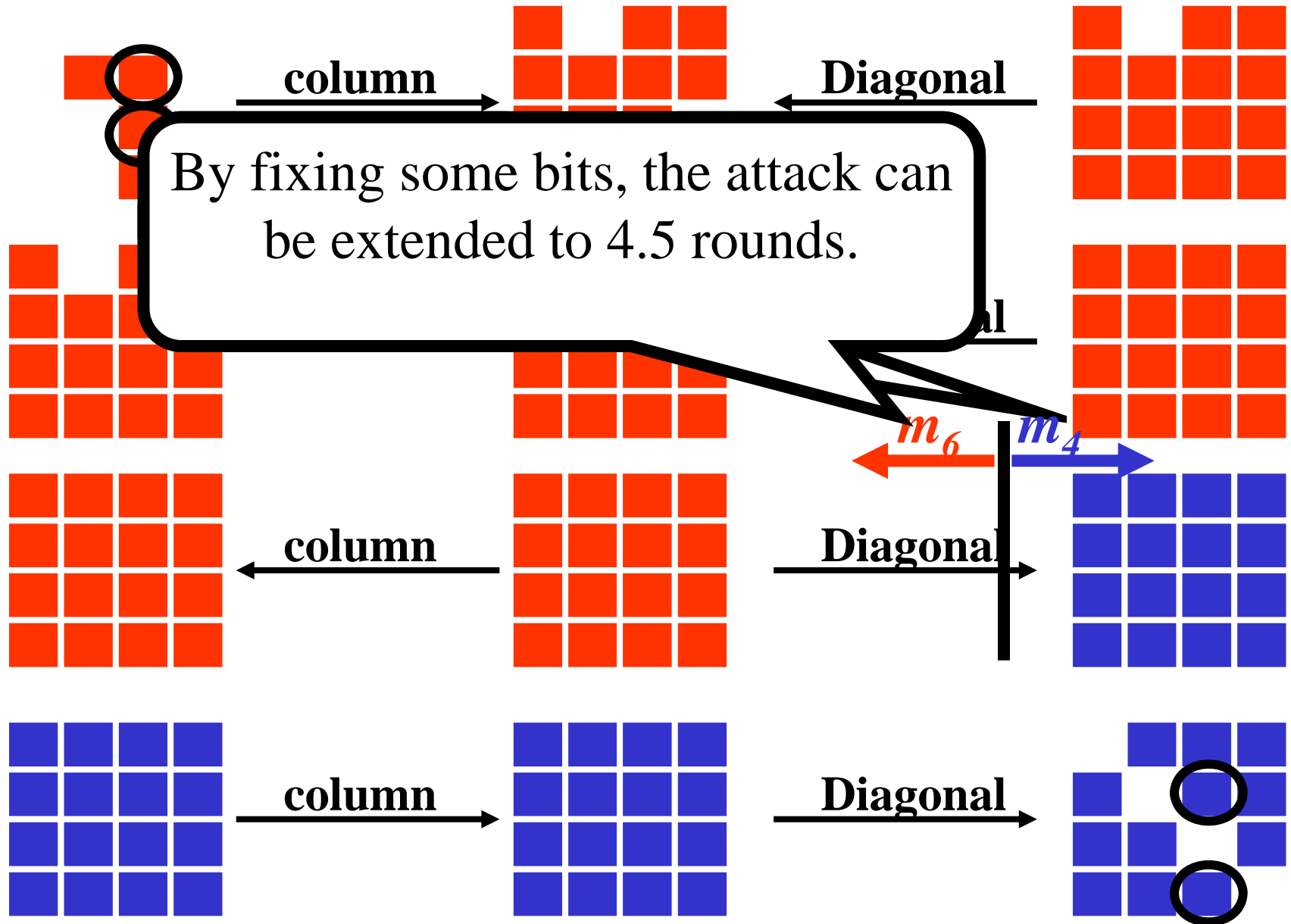
Any pair of **a hash chaining value** and **an internal state** can contribute to one output value. If each independent chunk has t -bit freedom, we obtain 2^{2t} output values, where the complexity is 2^t Blake compression function computation. Therefore, the complexity of finding a preimage will be reduced by a factor of 2^t .



Attack details on 4-round Blake






Attack details on 4-round Blake



Conclusion

◆ Applicable to all elements of (round-reduced) Blake-family.
Here pick Blake-32 as an example, which has **10** rounds.

#round	complexity	memory	technique
4	2^{224}	2^{32}	Splice-and-cut Partial-matching
4.5	2^{252}	2^8	Splice-and-cut Partial-matching Partial-fixing
			Splice-and-cut Partial-matching Partial-fixing Initial-structure New technique

Thank you!