The Impact of Carries on the Complexity of Collision Attacks on SHA-1

Florian Mendel, *Norbert Pramstaller*,
Christian Rechberger, and Vincent Rijmen

FSE 2006 – Graz, Austria

2006/03/16

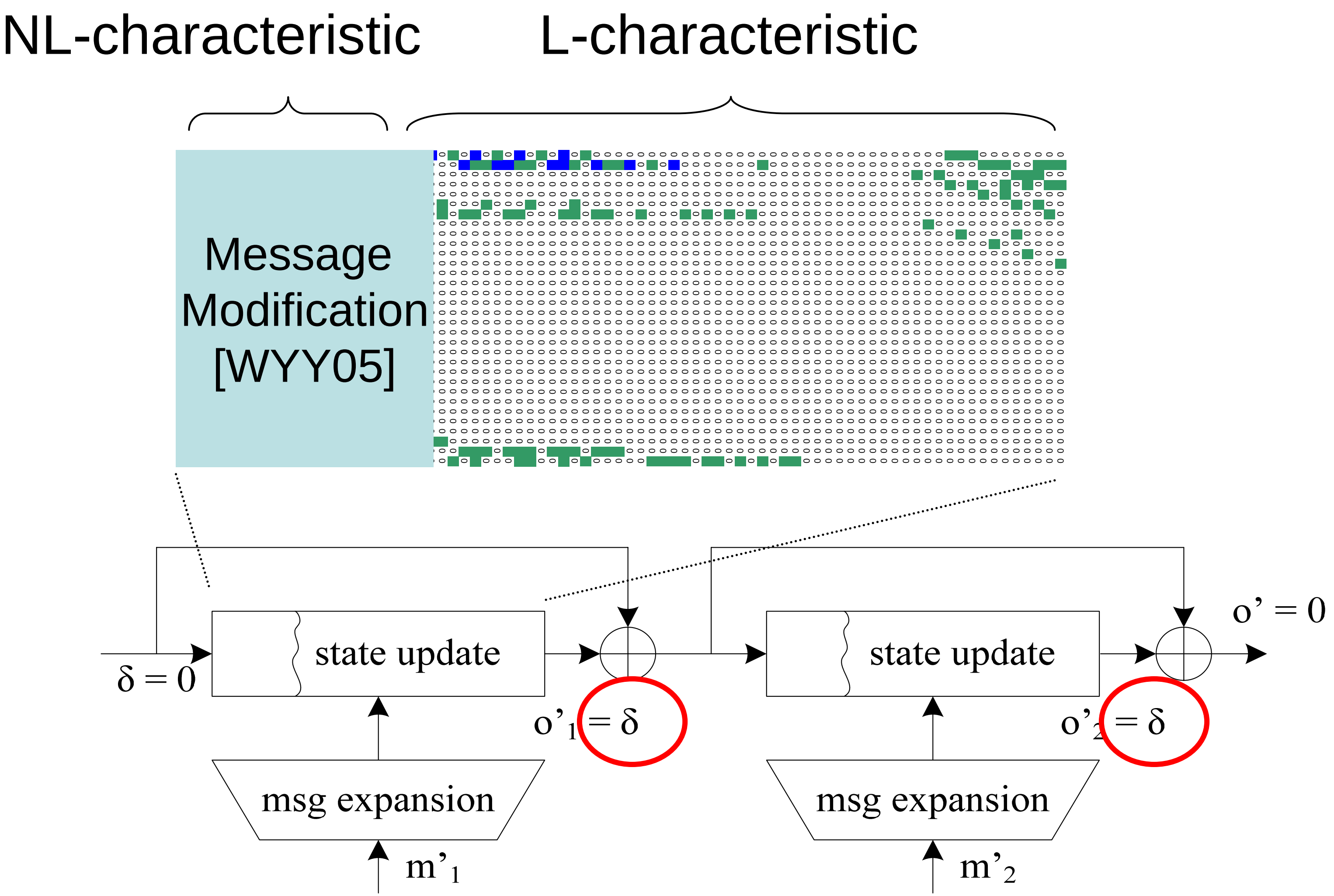
Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Outline

- Basic attack strategy on SHA-1
- Local collisions and corresponding probabilities
- Impact of carries on probability
- Update of SHA-1 complexity
- Conclusion

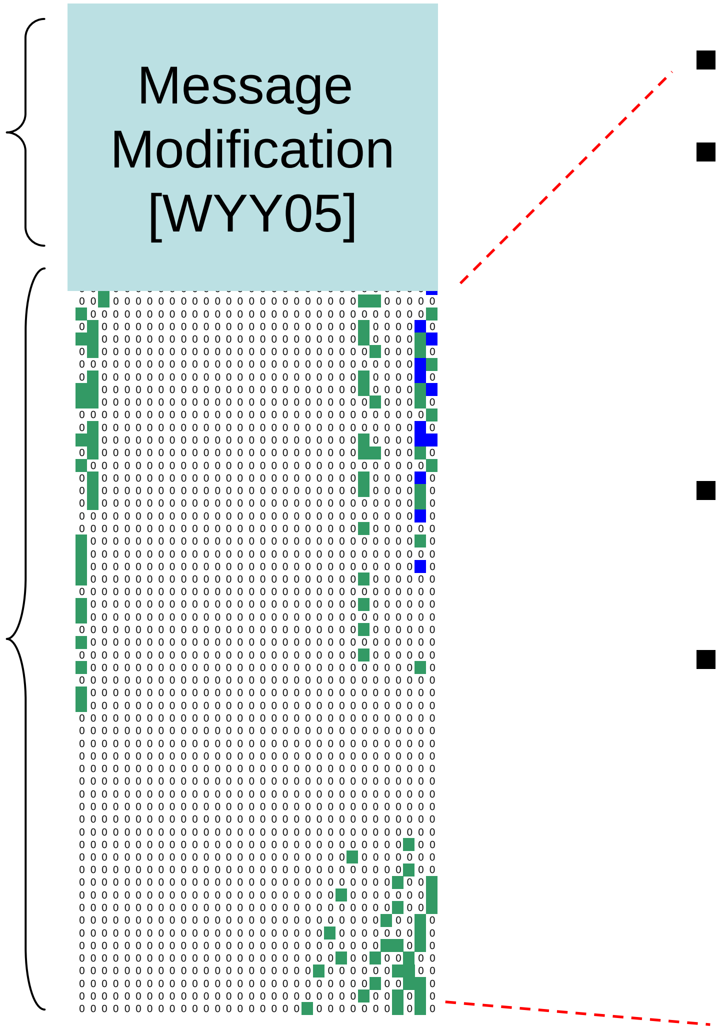
Basic attack strategy on SHA-1



Basic attack strategy on SHA-1

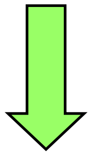
NL-characteristic

L-characteristic



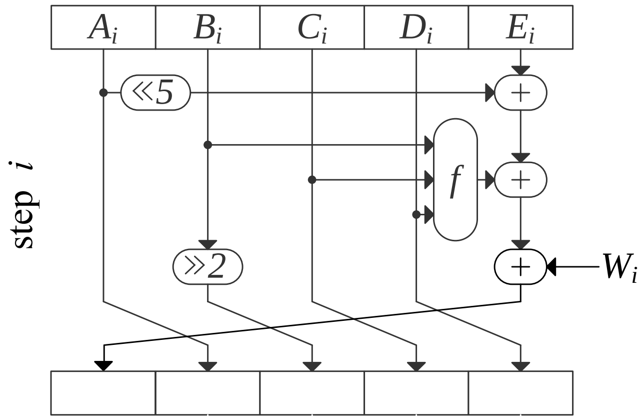
- Pseudo-near collision
- E.g. last 60 steps
  - Boolean function in first 20 steps not important

- Determines collision attack complexity
- Overlapping local collisions

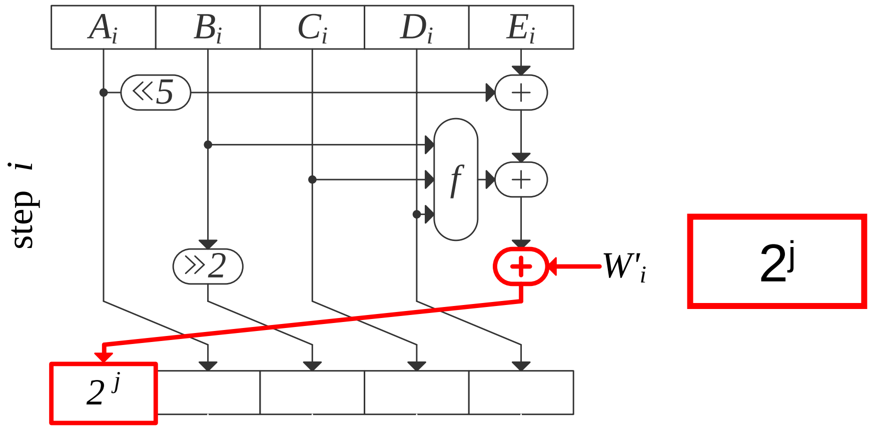


probability of local collisions?

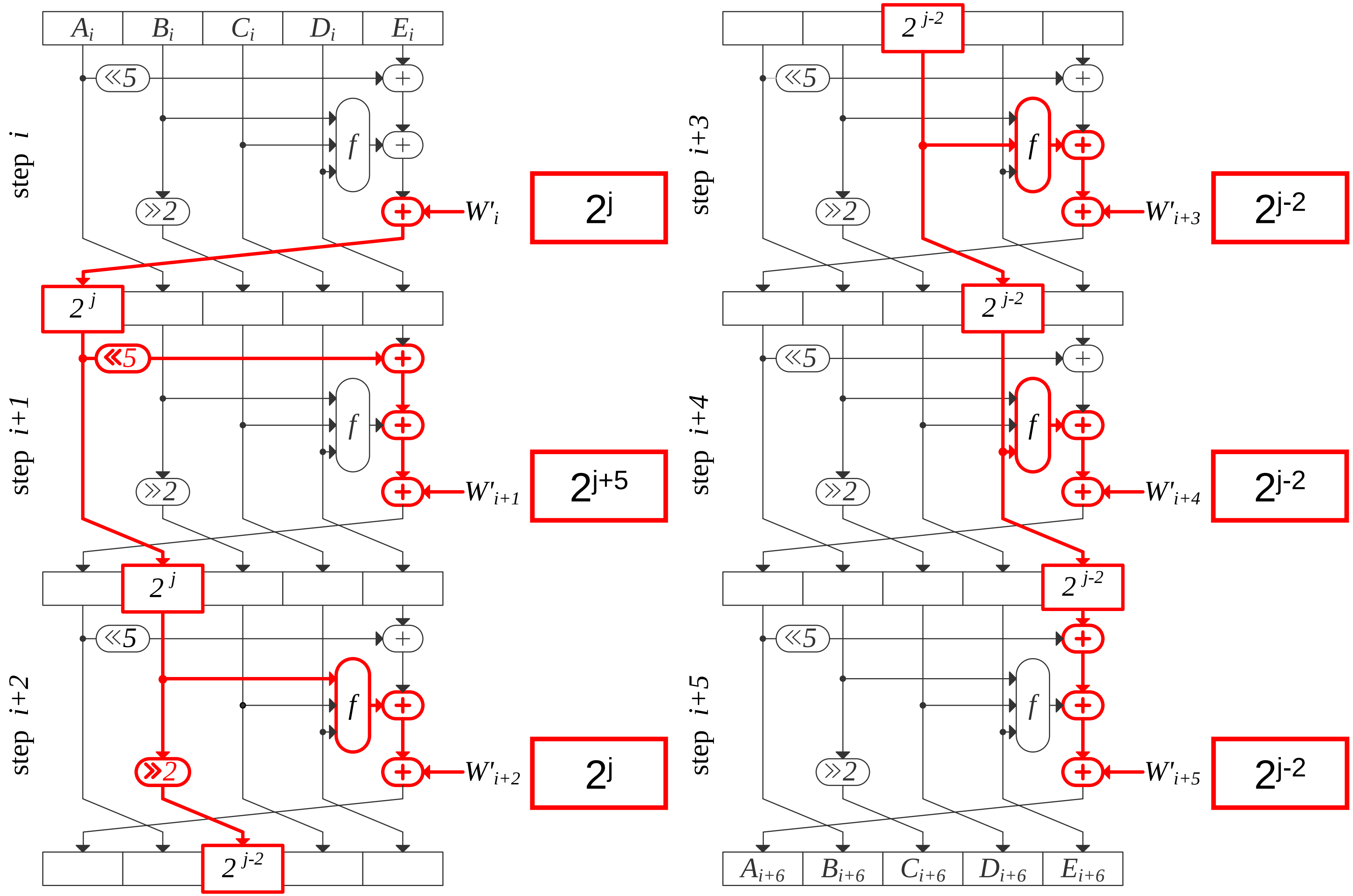
SHA-1 local collision



SHA-1 local collision



SHA-1 local collision



Signed bit differences

- We define sign of difference as $w'_j = w_j - w^*_j$

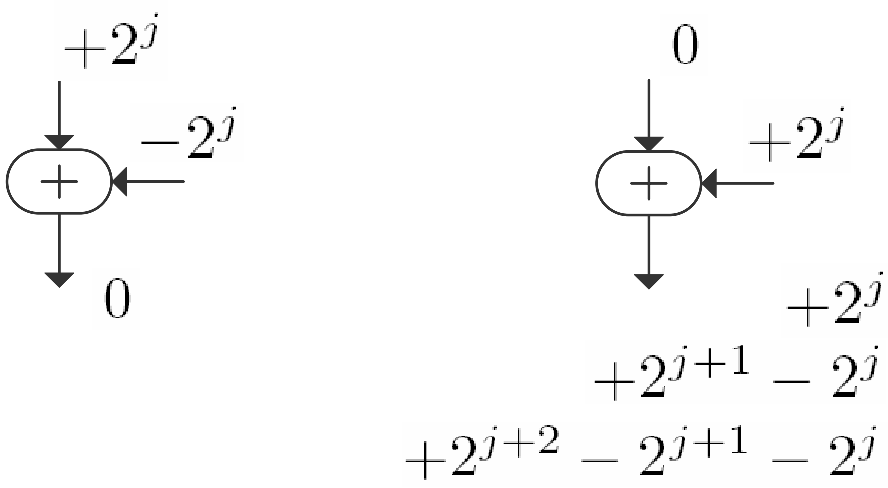
$$w_j, w^*_j \in \{0, 1\} \qquad w'_j \in \{-1, 0, +1\}$$

- Signed bit difference is defined as $W'_j = w'_j 2^j$

$$W'_j = \begin{cases} +2^j & \text{if } w_j = 1 \text{ and } w^*_j = 0 \\ 0 & \text{if } w_j = w^*_j, \\ -2^j & \text{if } w_j = 0 \text{ and } w^*_j = 1 \end{cases}$$

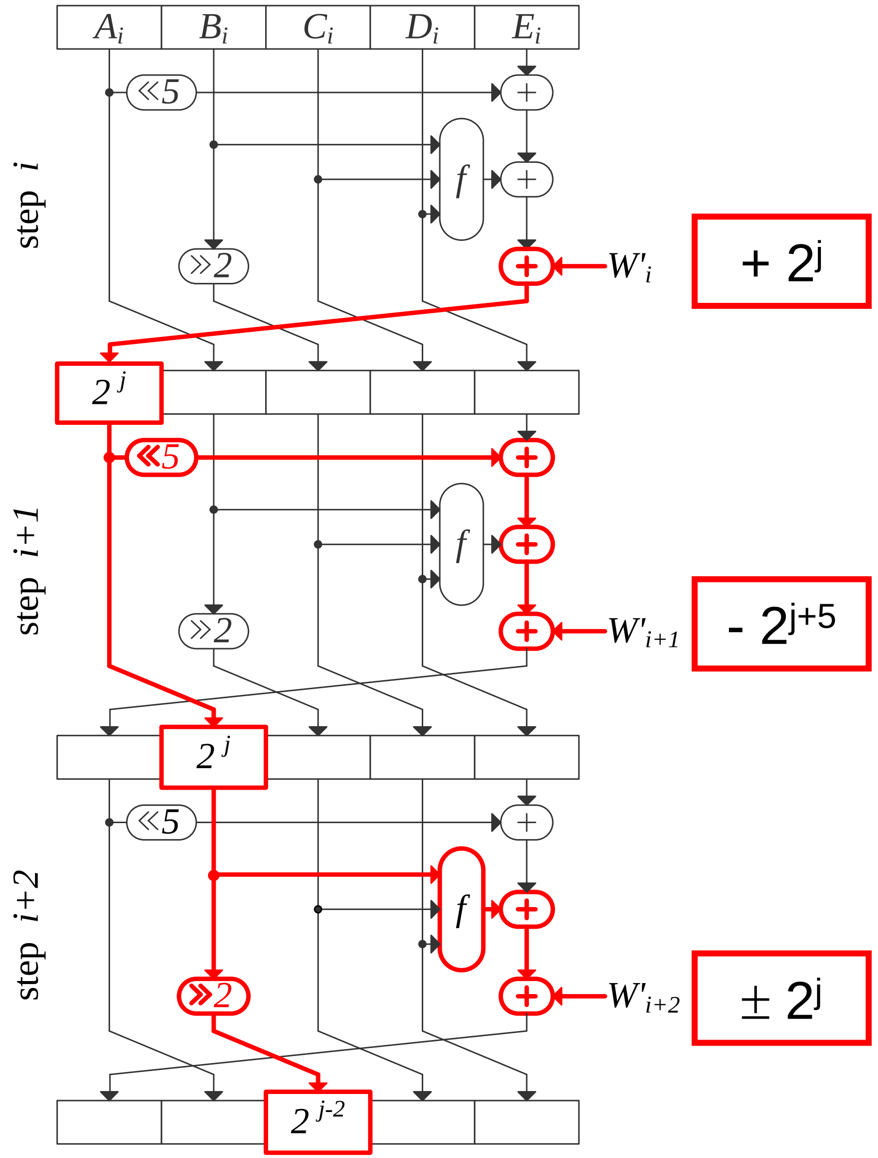
Differential properties of signed bit differences

- Addition



- f_{XOR}
  - Flips sign of input difference with p=1/2
  - Difference always propagates

Probability for local collision – f_{XOR}



- introduce disturbance
- propagates with p = ½
- if j=31 (MSB) => p=1

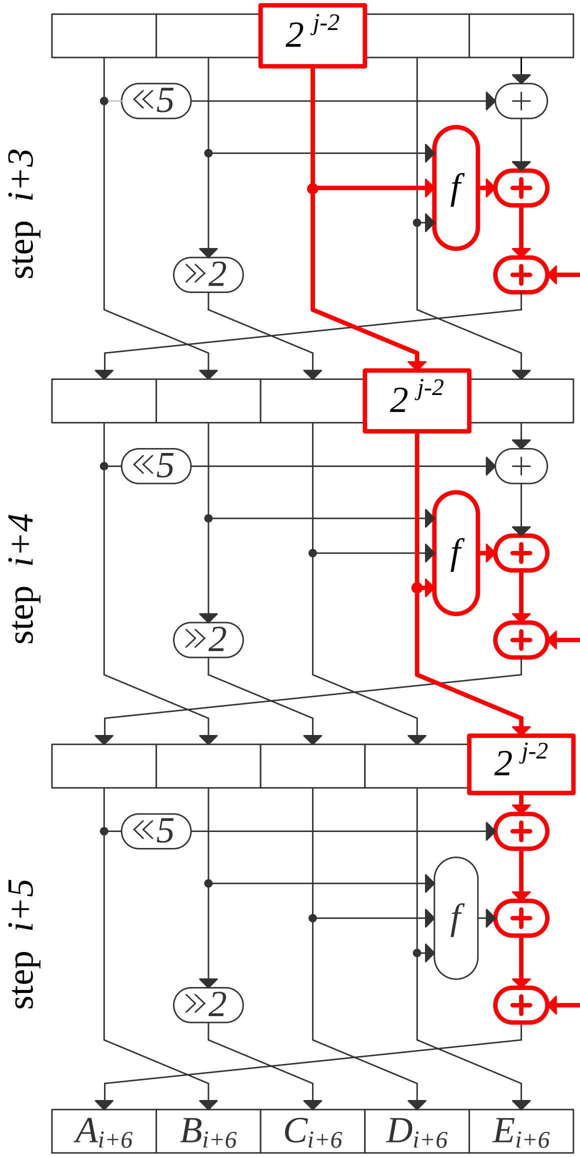
- introduce correction (opposite sign)

$$W_{i+1,j+5} \oplus W_{i,j} = 1 \quad (CW_{i+1})$$

- cancels difference with p = 1

- introduce correction
- cancels difference with p = ½
- if j=31 => p=1

Probability for local collision – f_{XOR}



$\pm 2^{j-2}$

- introduce correction
- cancels difference with p = ½
- if (j-2) mod 32=31 => p=1

$\pm 2^{j-2}$

- introduce correction
- cancels difference with p = ½
- If (j-2) mod 32 = 31 => p=1

$- 2^{j-2}$

- introduce correction (opposite sign)

$$W_{i+5,j-2} \oplus W_{i,j} = 1 \quad (CW_{i+5})$$

- cancels difference with p = 1

Probability for local collision – f_{XOR}

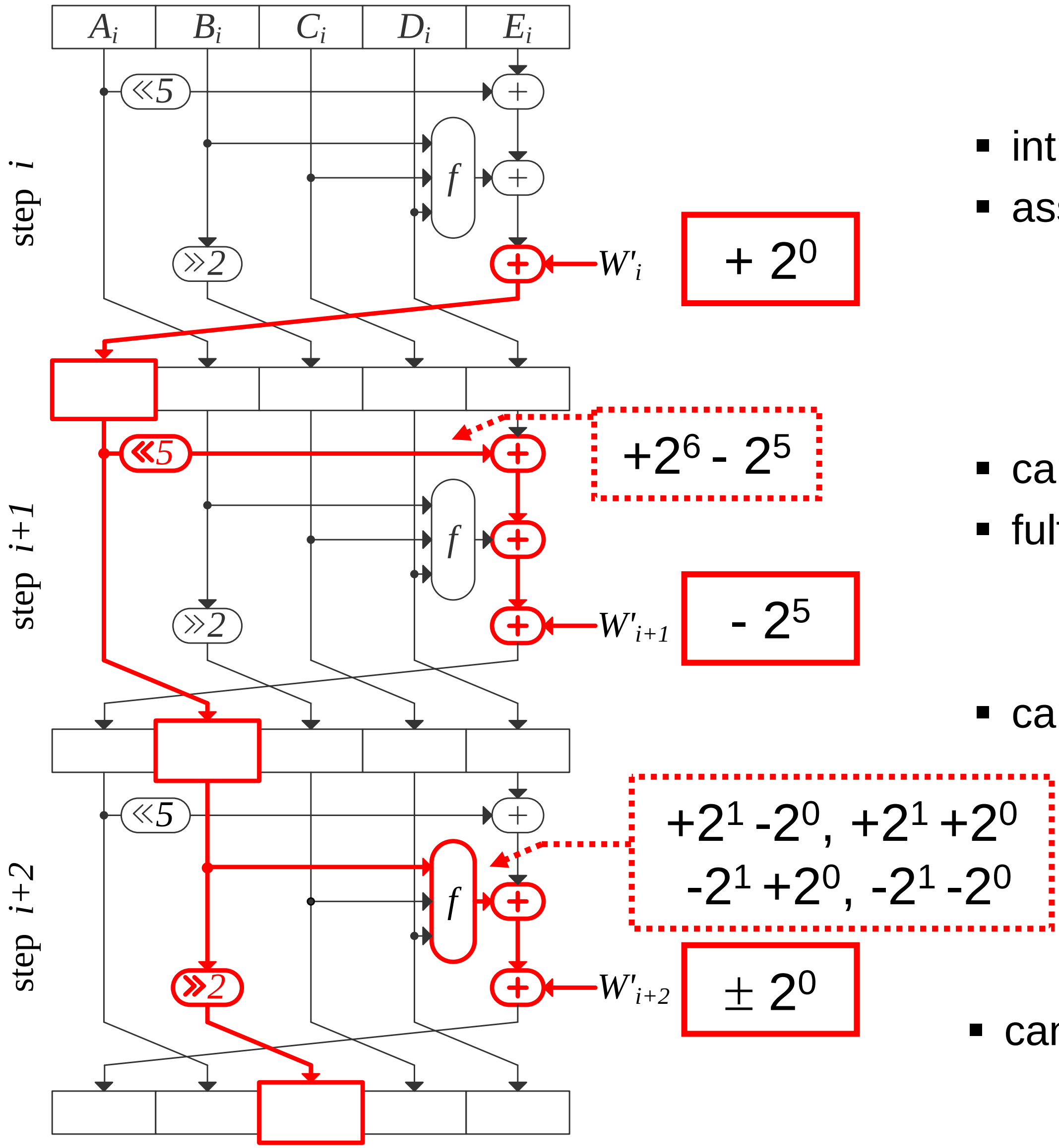
- f_{XOR}
  - Set signs of corrections
  - Then probability depends on bit position *j*
  - Best probability for *j=1*: 2^{-2} (probability 1 in step *i+3 and i+4*)

disturbance bit position	probability	set signs of corrections
j=0,2,…,25,27,…,30	2^{-4}	CW_{i+1}, CW_{i+5}
j=31	2^{-3}	CW_{i+1}, CW_{i+5}
j=26	2^{-4}	CW_{i+5}
j=1	2^{-2}	CW_{i+1}

Accurate probability computation

- So far we did not allow carry in step *i*
- Now we look at impact of carries

Accurate probability computation – f_{XOR}



- introduce disturbance j=0
- assume carry occurs (p = ¼)

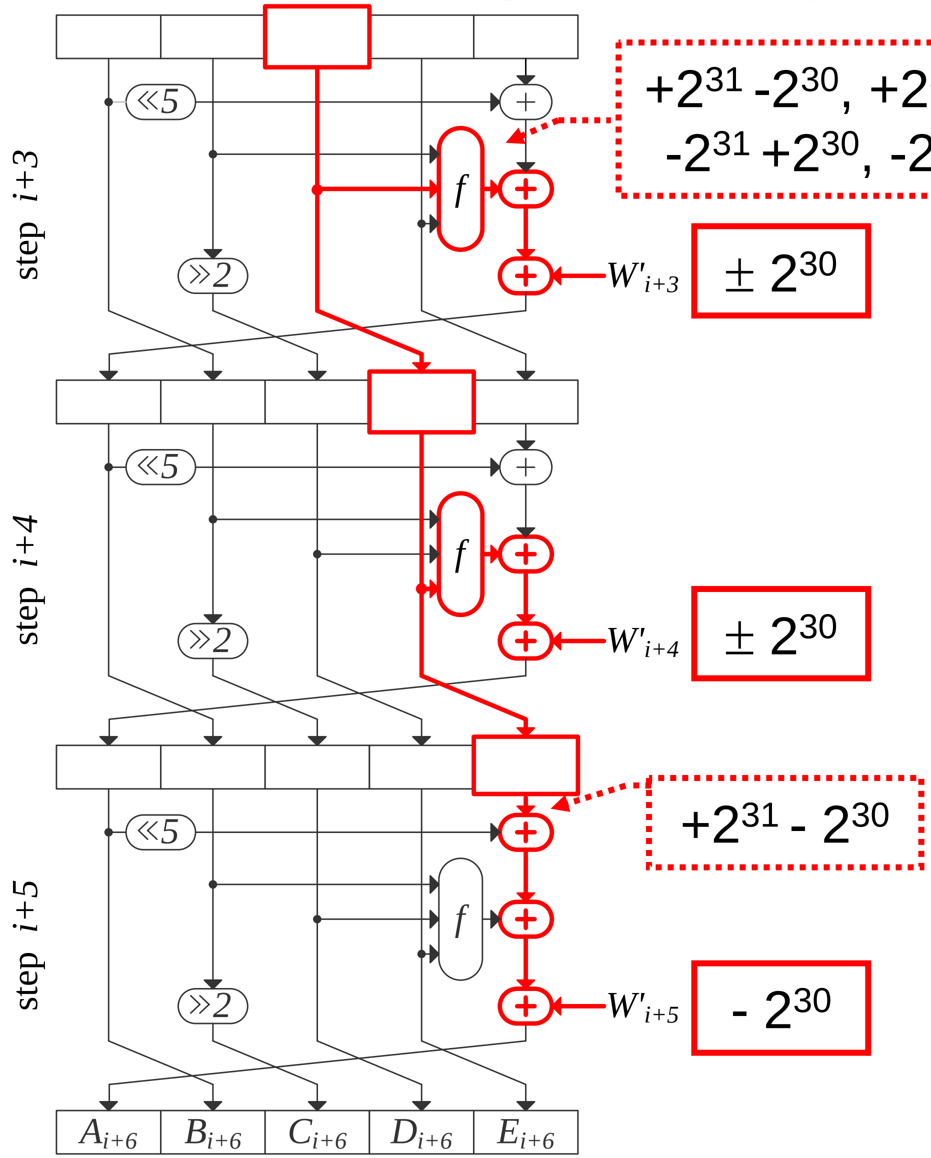
$$+2^0 \rightarrow +2^1 - 2^0$$

- carry in correction required
- fulfill

$$W_{i+1,j+5} \oplus W_{i,j} = 1 \quad (CW_{i+1})$$

- cancels difference with p = 1
- cancels difference with p = ¼

Accurate probability computation – f_{XOR}



- introduce correction
- cancels difference with p = ½

- introduce correction
- cancels difference with p = ½ (same as in step *i+3*)

- introduce correction (opposite sign)

$$W_{i+5,j-2} \oplus W_{i,j} = 1 \quad (CW_{i+5})$$

- cancels difference with p = 1

Accurate probability computation – f_{XOR}

- local collision with disturbance in j=0
  - Probability without carry

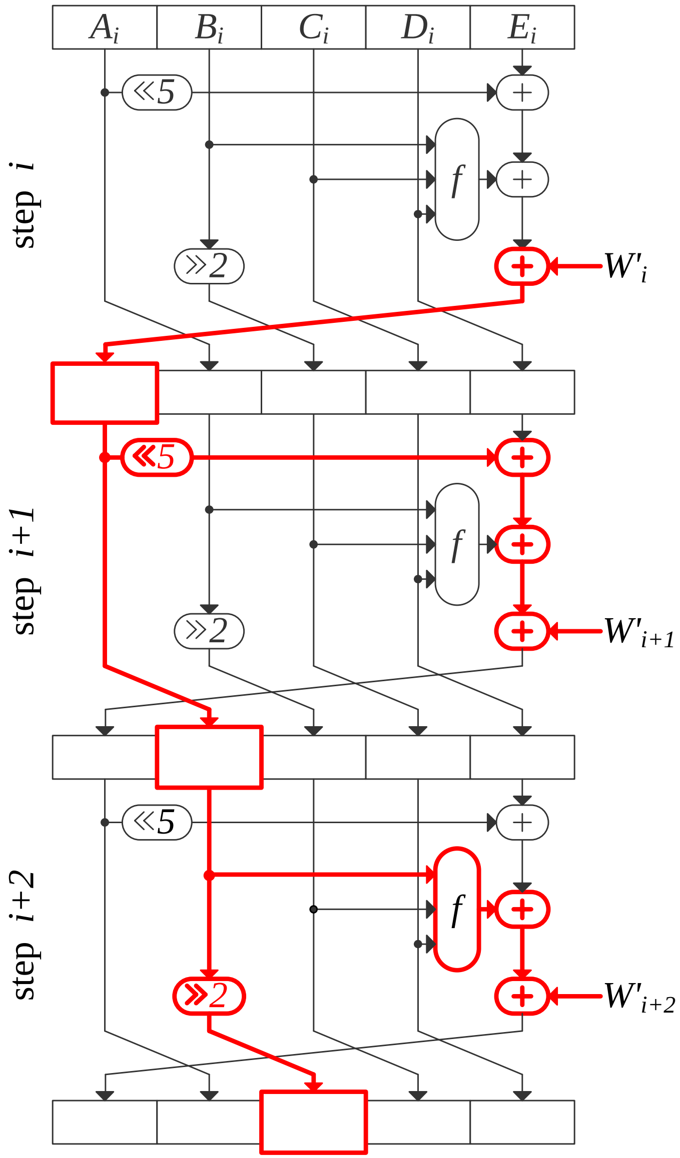
$$p(f_{XOR}, j = 0) = 2^{-4}$$

  - Probability including carry effect

$$p(f_{XOR}, j = 0) = 2^{-4} + 2^{-6} = 2^{-3.6781}$$

  - Further improvement possible?

Uncorrectable carries

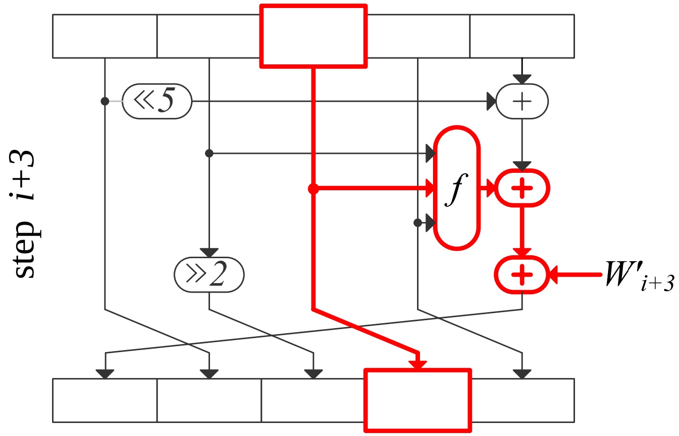


$+ 2^0$

- introduce disturbance j=0
- assume 2 carries occurs (p=1/8)

$+2^0 \rightarrow +2^2 -2^1 -2^0$

$+2^0 - 2^{31} -2^{30}$



$- 2^{30}$

Accurate probability computation

- Do analysis for all different bit positions
- Carry impact improves in general probability

$$p(f_{XOR}, j) = \begin{cases} 2^{-2} & \text{for } j = 1, \\ 2^{-4} + 2^{-6} & \text{for } j = 0, \\ \sum_{k=1}^{27-j} 2^{-4k} & \text{for } j = 2, \ldots, 26, \\ 2 \cdot 2^{-4 \cdot (32-j)} + \sum_{k=1}^{31-j} 2^{-4k} & \text{for } j = 27, \ldots, 31, \end{cases}$$

Update on complexity for SHA-1 [WYY05]

- Attack complexity slightly lower (approx. 2.7)

	disturbance bit position	# local collisions	Wang et al. probability	our work
f_{XOR}	j=1	7	2^{-14}	2^{-14}
f_{XOR}	j=0	3	2^{-12}	$2^{-11.03}$
f_{MAJ}	j=1	5	2^{-20}	2^{-20}
f_{XOR}	j=2,3,4,5,7	5	2^{-20}	$2^{-19.534}$
		total	$\mathbf{2^{-66}}$	$\mathbf{2^{-64.56}}$

- Assume local collisions are independent
- Computed probabilities were verified by performing probability measurements

Conclusion

- Accurate probability computation of local collisions
- In case of SHA-1 attack complexity is slightly lower
  - Sparse L-characteristic
  - Most of disturbances for f_{XOR} are in j=1
- If L-characteristic is more dense, carry impact is higher
  - For instance SHA1-IME [JP05]
- Looking at probabilities is more accurate than looking at conditions