Cryptanalysis of 48-step RIPEMD-160

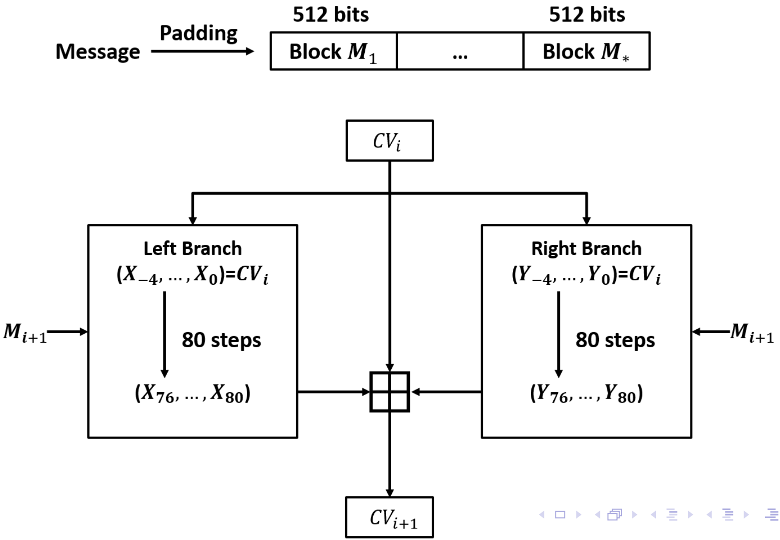
Gaoli Wang[1], Yanzhao Shen[2], Fukang Liu[1]

[1] East China Normal University
[2] Shandong University

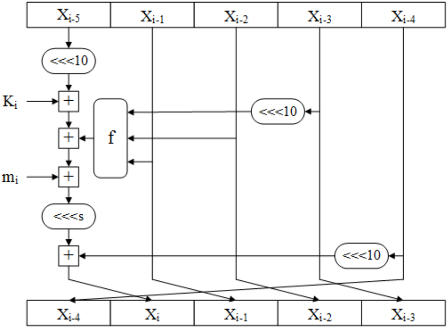
FSE 2018
6 March 2018

Outlines

Description of RIPEMD-160



The step update transformation



$$X_i = (X_{i-4} \lll 10) + \left((X_{i-5} \lll 10) + F_j\,(X_{i-1}, X_{i-2}, (X_{i-3} \lll 10)) + m_{\pi^l(i)} + k_j^l \right) \lll s_i^l,$$

$$Y_i = (Y_{i-4} \lll 10) + \left((Y_{i-5} \lll 10) + F_{6-j}\,(Y_{i-1}, Y_{i-2}, (Y_{i-3} \lll 10)) + m_{\pi^r(i)} + k_j^r \right) \lll s_i^r$$

Boolean functions:

$$
\begin{aligned}
F_1(X,Y,Z) &= X \oplus Y \oplus Z, \\
F_2(X,Y,Z) &= (X \wedge Y) \vee (\neg X \wedge Z), \\
F_3(X,Y,Z) &= (X \vee \neg Y) \oplus Z, \\
F_4(X,Y,Z) &= (X \wedge Z) \vee (Y \wedge \neg Z), \\
F_5(X,Y,Z) &= X \oplus (Y \vee \neg Z).
\end{aligned}
$$

Step i	Round j	Left Branch	Right Branch
1 to 16	1	F_1	F_5
17 to 32	2	F_2	F_4
33 to 48	3	F_3	F_3
49 to 64	4	F_4	F_2
65 to 80	5	F_5	F_1

Summary of (Semi-free-start) Collision Attacks on RIPEMD-160

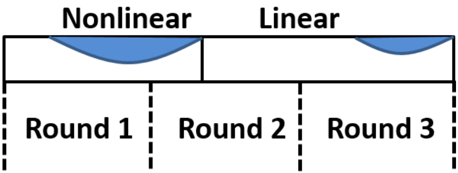
Type	Steps	Complexity	Reference
△	36*	practical	Mendel et al., ISC 2012
△	42*	$2^{75.5}$	Mendel et al., ASIACRYPT 2013
△	36	$2^{70.4}$	Mendel et al., ASIACRYPT 2013
△	36	$2^{55.1}$	Liu et al., ASIACRYPT 2017
△	48*	$2^{76.4}$	**This**
Collision	30	2^{67}	Liu et al., ASIACRYPT 2017

* The attack starts from an intermediate step.

△ The attack is semi-free-start collision.

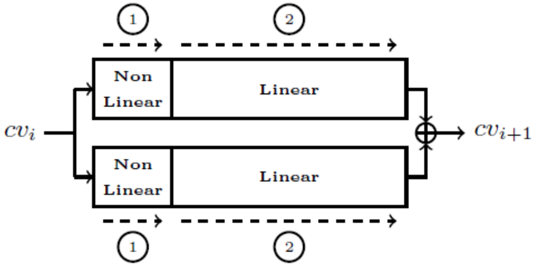
Classical approach to find a collision (MD4) [Wang05]

1. Find a message difference and a collision differential path, which holds with high probability in the linear part (i.e., the middle and the last steps).
2. Using part of the message freedom to make sure the nonlinear part hold with probability almost 1 (some techniques such as message modification). The linear part is verified probabilistically using the remaining message freedom.



Classical approach-apply to RIPEMD-128/160 directly

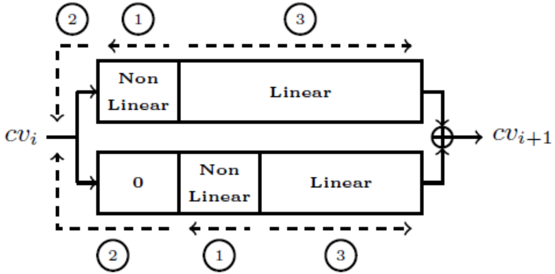
1. Choose a message difference and find two differential paths. The nonlinear parts lie in round 1 in both branches, and the differential paths without round 1 holds with high probability.
2. Derive two sets of sufficient conditions which ensure the two differential paths hold, respectively.
3. Modify the message to fulfill most of the conditions on nonlinear parts. The other conditions are fulfilled probabilistically.



New strategy to find a semi-free-start collision of RIPEMD-128 [LP13]

The non-linear part is not necessarily in the first round.

1. Ensure the non-linear parts hold with probability almost 1 using the freedom from the internal states and a few message words.
2. From this starting point, merge the two branches using some remaining free message words.
3. The linear parts in both branches are verified probabilistically.



Semi-free-start on 42-step RIPEMD-160 [MPS+13]

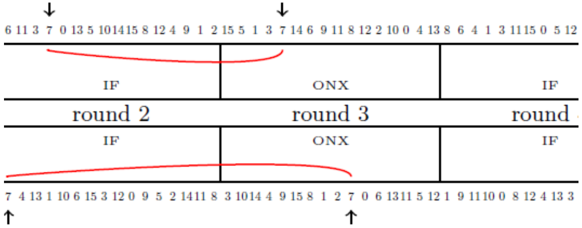
Phase 1: a 48-step differential path (in rounds 2-4), difference in m_7

Phase 2: Use the freedom of m_i $(0 \leq i \leq 15, i \neq 1, 4, 7, 13)$ and the internal states to satisfy the non-linear parts (starting point).

- The probability of the linear parts is $2^{-45.4}$.

Phase 3: Use the remaining free m_i $(i = 1, 4, 7, 13)$ to merge, 2^{-32}.

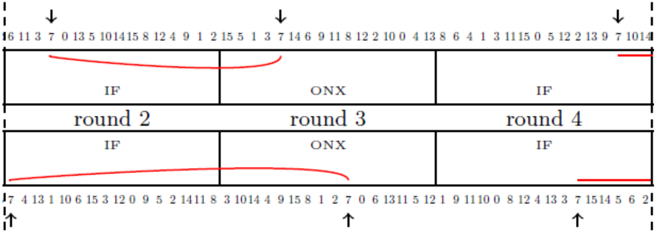
- The overall probability for collision is $2^{-77.4}$.
- We need to obtain $2^{77.4}$ starting points.



Semi-free-start on 42-step RIPEMD-160 [MPS$^+$13]

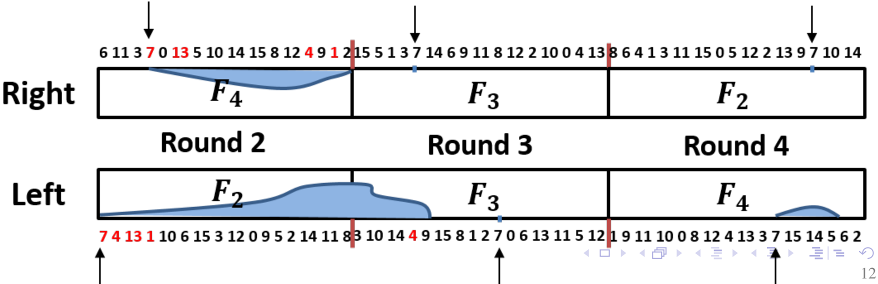
Phase 4: Handle probabilistically the linear parts.

- The probability of last steps (59-64) is about $2^{-11.3}$ by experiment.
- The overall probability will exceed 2^{80} for 48-step RIPEMD-160.



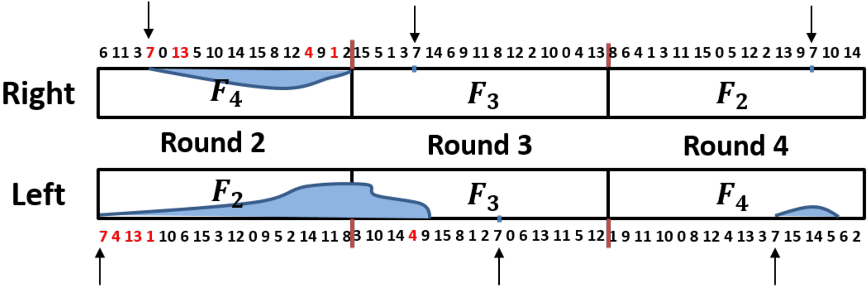
Overview of Attack on 42 steps $\longrightarrow$ 48 steps

- We use the same 48-step differential path (in rounds 2-4) as in [MPS$^+$13].
- Leave m_i $(i = 1, 4, 7, 13)$ to do merging. When satisfying the non-linear parts (Phase 2), m_i $(i = 1, 4, 7, 13)$ is unknown.
- Left: m_4 is used to compute X_{36}, so X_{36} is unknown in Phase 2.
- Right: m_4 and m_1 are used to compute Y_{29} and Y_{31}, so Y_{29} and Y_{31} are unknown in Phase 2.



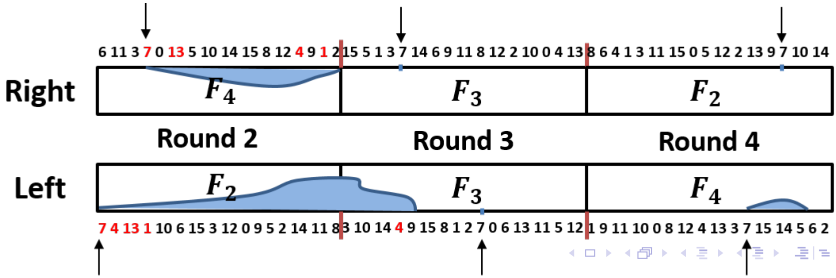
Overview of Attack on 42 steps $\longrightarrow$ 48 steps

- In order to improve the overall probability, the number of the uncontrolled conditions must decrease.
- If we can not compute X_i $(i \geq 36)$ and Y_i $(i \geq 29)$, the conditions on these variables have to be handled probabilistically.



Overview of Attack on 42 steps $\longrightarrow$ 48 steps

- In order to ensure $X_{37,i} = 0$ $(i = 2, 21)$, $X_{37,i} = 1$ $(i = 7, 17)$, $X_{38,i} = 0$ $(i = 17, 21)$ hold, the values of these bits must be computed firstly (under the condition that X_{36} is not known).
- $Y_{30,i}$ $(i = 9, 15, 21, 27, 30, 31)$ and $Y_{32,20}$ can be computed (under the condition that Y_{29} and Y_{31} are unknown).
- The conditions on X_{37}, X_{38}, Y_{30} and Y_{32} can be satisfied by message modification, once their values are calculated.



Compute some bits of X_{37}, X_{38}, Y_{30} and Y_{32} (X_{36}, Y_{29} and Y_{31} are unknown)
Example – compute $Y_{30,9}$

- In order to compute $Y_{32,20}$, we need to compute $Y_{30,9}$.

$$Y_{30} = (Y_{26} \lll 10) + \Big((Y_{25} \lll 10) + F_4\big(Y_{29}, Y_{28}, (Y_{27} \lll 10)\big) + m_9 + k_2^r\Big) \lll 15$$

- $F_4\big(Y_{29}, Y_{28}, (Y_{27} \lll 10)\big) = \big(Y_{29} \wedge (Y_{27} \lll 10)\big) \vee \big(Y_{28} \wedge \neg(Y_{27} \lll 10)\big)$
- Y_{29} is not known
- If the condition $Y_{27} = 0$ is added, then F_4 can be calculated.
- However, if all the 32-bit value of $Y_{27} = 0$ is added, it will waste too much freedom or contradict with the differential path.

$$Y_{30} = (Y_{26} \lll 10) + \Big(\big((Y_{25} \lll 10) + F_4\big(Y_{29}, Y_{28}, (Y_{27} \lll 10)\big) + m_9 + k_2^r\Big) \lll 15$$

$$F_4\big(Y_{29}, Y_{28}, (Y_{27} \lll 10)\big) = \big(Y_{29} \wedge (Y_{27} \lll 10)\big) \vee \big(Y_{28} \wedge \neg(Y_{27} \lll 10)\big)$$

Adding conditions $Y_{27,i} = 0$ $(i = 13, 14, 16) \Longrightarrow$
bits 23, 24, 26 of F_4 can be computed by $Y_{28} \wedge \texttt{0x5800000}$.
($Y_{27,15} = 1$ is a condition of the differential path)
$Y_{30,9}$ is equal to the 9-th bit of

$$(Y_{26} \lll 10) + \big((Y_{25} \lll 10) + (Y_{28} \wedge \texttt{0x5800000}) + m_9 + k_2^r\big) \lll 15$$

by adding some conditions.

$$Y_{30} = (Y_{26} \lll 10) + \Big((Y_{25} \lll 10) + F_4\big(Y_{29}, Y_{28}, (Y_{27} \lll 10)\big) + m_9 + k_2^r\Big) \lll 15$$

$$Y_{30,9}: \quad (Y_{26} \lll 10) + \big((Y_{25} \lll 10) + (Y_{28} \wedge \texttt{0x5800000}) + m_9 + k_2^r\big) \lll 15$$

Adding Conditions:

$$R_1 = (Y_{25} \lll 10) + F_4\big(Y_{29}, Y_{28}, (Y_{27} \lll 10)\big) + m_9 + k_2^r$$
$$T = (Y_{25} \lll 10) + (Y_{28} \wedge \texttt{0x5800000}) + m_9 + k_2^r$$
$$R_2 = (Y_{25} \lll 10) + m_9 + k_2^r$$
$$Q_1 = R_1 \lll 15$$

Add conditions $T_i = 0\ (i = 23, 24)$, $R_{2,i} = 0\ (i = 23, 24, 25)$, $F_{4,23} = 0$

$\Longrightarrow R_{1,i} = T_i\ (i = 24, 26)$ can be calculated correctly, because there is no carry from bit 23 to 24 and from bit 25 to 26 when computing R_1.

Thus, $Q_{1,i}\ (i = 7, 9)$ can be computed correctly and $Q_{1,7} = 0$.

Add conditions $Y_{26,i} = 0\ (i = 29, 30)$,

$\Longrightarrow$ there is no carry from bit 8 to 9 when computing $Y_{30,9}$ $(Y_{30} = (Y_{26} \lll 10) + Q_1)$.

Therefore, $Y_{30,9}$ can be calculated correctly by

$$(Y_{26} \lll 10) + \big((Y_{25} \lll 10) + (Y_{28} \wedge \texttt{0x5800000}) + m_9 + k_2^r\big) \lll 15.$$

The experiment confirms the above computation.

Existing Problem in the Sufficient Conditions of the Differential Path

We give an example to illustrate the problem. The step operation of RIPEMD-160 can be abbreviated as

$$X = a + (b + c) <<< 14,$$

$$X' = a' + (b' + c) <<< 14.$$

If $b' - b = 2^{17}, \quad b'_{17} = 1, \quad b_{17} = 0, \quad a' - a = 2^{31}, \quad$ then

$$Pr[X' = X] = 1$$

is incorrect.

Because: the difference of $(b' + c)$ and $(b + c)$ will propagate to the 18-th,... bits, the difference of $(b' + c) <<< 14$ and $(b + c) <<< 14$ is not necessarily equal to 2^{31}.

Finding a Set of Sufficient Conditions of the Differential Path

The step function of RIPEMD-160 is not a T-function (i.e., the i-th output bit depends only on the i first lower bits of all input words).

- Daum (Ph.D thesis 2005) has proposed a method to calculate the probability.
- Liu et al. (ASIACRYPT 2017) solve the problem completely, can give a set of sufficient conditions of the differential path. Then do message modification.
- When submitting this paper, we can make sure the modular difference hold when the difference of the internal variable is a power of 2.

Message Modification to Ensure the Modular Difference Hold

$$X_i = (X_{i-4} <<< 10) + ((X_{i-5} <<< 10) + f(X_{i-1}, X_{i-2}, (X_{i-3} <<< 10)) + m + k) <<< 3,$$

$$r_1 = (X_{i-5} \lll 10) + f(X_{i-1}, X_{i-2}, (X_{i-3} \lll 10)) + m + k,$$

$$r_1' = (X_{i-5} \lll 10) + f(X_{i-1}, X_{i-2}, (X_{i-3} \lll 10)) + m' + k,$$

$$r_2 = r_1 \lll 3, \qquad r_2' = r_1' \lll 3.$$

Let $m' - m = 2^{30}$, if $r_1' - r_1 = 2^{30}$, then $X_i' - X_i = 2$.
If $X_i' - X_i \neq 2$, we know that $\Delta r_1 = [-30, -31]$, i.e. $r_{1,30} = r_{1,31} = 1$, $r'_{1,30} = r'_{1,31} = 0$. One of the message modification methods is:

$$m \longleftarrow m \pm 2^{31},$$

then after this modification, the most two significant bits of r_1 and r_1' are $r_{1,30} = 1$, $r_{1,31} = 0$, $r'_{1,30} = 0$, $r'_{1,31} = 1$, which means $\Delta r_1 = [-30, 31]$, thus $\Delta r_2 = [-1, 2]$. Therefore, $X_i' - X_i = -2 + 2^2 = 2$.

Results

1. The success probability of the match of the five initial words is 2^{-32}.
2. In the left branch until step 56, the uncontrolled probability is $2^{-5.4}$.
3. In the right branch until step 59, the uncontrolled probability is $2^{-29.6}$.
4. The probability of the differential path in steps 57-64 (left branch) and in steps 60-64 (right branch) is $2^{-11.3}$.

The uncontrolled probability is $2^{-78.5}$ in total.
The complexity of the semi-free start collision attack on 48-step RIPEMD-160 is $2^{76.4}$.

Conclusion

- Compute Some Bits of X_{37}, X_{38}, Y_{30} and Y_{32} whenX_{36}, Y_{29} and Y_{31} are Unknown.
- Present some insights of the sufficient conditions or to make modular difference hold.
- Get semi-free-start collision attack on more rounds.

Thanks for your attention.