1 Changes of ARIRANG

ARIRANG has two changes in explaining the step functions of ARIRANG hash functions. Following two tables will explain the changes of ARIRANG in detail.

Table 1: The first change : ARIRANG256_StepFunction (page 15).

Original version (wrong)

ARIRANG256_StepFunction($W_{\sigma(2t)}$, $W_{\sigma(2t+1)}$, a, b, c, d, e, f, g, h)
{
$T_1 = G^{(256)}(a \oplus W_{\sigma(2t)})$;
$b = a \oplus W_{\sigma(2t)}$;
$c = b \oplus T_1$;
$d = c \oplus (T_1 \lll 13)$;
$e = d \oplus (T_1 \lll 23)$;
$T_2 = G^{(256)}(e \oplus W_{\sigma(2t+1)})$;
$f = e \oplus W_{\sigma(2t+1)}$;
$g = f \oplus T_2$;
$h = g \oplus (T_2 \lll 29)$;
$a = h \oplus (T_2 \lll 7)$;
}

Changed version (right)

ARIRANG256_StepFunction($W_{\sigma(2t)}$, $W_{\sigma(2t+1)}$, a, b, c, d, e, f, g, h)
{
$a = a \oplus W_{\sigma(2t)}$;
$T_1 = G^{(256)}(a)$;
$b = b \oplus T_1$;
$c = c \oplus (T_1 \lll 13)$;
$d = d \oplus (T_1 \lll 23)$;
$e = e \oplus W_{\sigma(2t+1)}$;
$T_2 = G^{(256)}(e)$;
$f = f \oplus T_2$;
$g = g \oplus (T_2 \lll 29)$;
$h = h \oplus (T_2 \lll 7)$;
$T_1 = a$; $a = h$; $h = g$; $g = f$; $f = e$; $e = d$; $d = c$; $c = b$; $b = T_1$;
}

The reason for the change
We made a mistake in writing ARIRANG256_StepFunction in page 15. The figure 3 in page 16 is correct, there was a mistake in translating into pseudo code. So, this change doesn't affect the source code.

Table 2: The second change : ARIRANG512_StepFunction (page 25).

Original version (wrong)

ARIRANG512_StepFunction($W_{\sigma(2t)}$, $W_{\sigma(2t+1)}$, a, b, c, d, e, f, g, h)
{
$T_1 = G^{(512)}(a \oplus W_{\sigma(2t)})$;
$b = a \oplus W_{\sigma(2t)}$;
$c = b \oplus T_1$;
$d = c \oplus (T_1 \lll 29)$;
$e = d \oplus (T_1 \lll 41)$;
$T_2 = G^{(512)}(e \oplus W_{\sigma(2t+1)})$;
$f = e \oplus W_{\sigma(2t+1)}$;
$g = f \oplus T_2$;
$h = g \oplus (T_2 \lll 53)$;
$a = h \oplus (T_2 \lll 13)$;
}

Changed version (right)

ARIRANG512_StepFunction($W_{\sigma(2t)}$, $W_{\sigma(2t+1)}$, a, b, c, d, e, f, g, h)
{
$a = a \oplus W_{\sigma(2t)}$;
$T_1 = G^{(512)}(a)$;
$b = b \oplus T_1$;
$c = c \oplus (T_1 \lll 29)$;
$d = d \oplus (T_1 \lll 41)$;
$e = e \oplus W_{\sigma(2t+1)}$;
$T_2 = G^{(512)}(e)$;
$f = f \oplus T_2$;
$g = g \oplus (T_2 \lll 53)$;
$h = h \oplus (T_2 \lll 13)$;
$T_1 = a$; $a = h$; $h = g$; $g = f$; $f = e$; $e = d$; $d = c$; $c = b$; $b = T_1$;
}

The reason for the change
We made a mistake in writing ARIRANG512_StepFunction in page 25. The figure 7 in page 25 is correct, there was a mistake in translating into pseudo code. So, this change doesn't affect the source code.