Subject: OFFICIAL COMMENT: ARIRANG
From: "Seokhie Hong" <hsh@cist.korea.ac.kr>
Date: Wed, 24 Dec 2008 16:29:49 +0900
To: <hash-function@nist.gov>
CC: <hash-function@nist.gov>

I sent e-mail a few minute ago. Please ignore the previous e-mail because I sent a wrong pdf file.
The attached pdf file is right.
Sorry for annoying you.
===:
Hi.
We made two mistakes in explaining the step function of ARIRANG in page 15 and 25.
So we would like to corret the mistakes. For corrections, see the pdf file

Best regards,
Seokhie Hong.(A submitter of ARIRANG)

correction.pdf	**Content-Type:**	application/pdf
	Content-Encoding:	base64

1 Correction of ARIRANG

We made two mistakes in explaining the step functions of ARIRANG hash functions. Thus we correct the mistakes.

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

Original version (wrong)

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

Correct version

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

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

Original version (wrong)

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

Correct version

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