**Subject:** OFFICIAL COMMENT: Tangle
**From:** "Yaser Esmaeili" <yaser.esmaeili@gmail.com>
**Date:** Tue, 16 Dec 2008 10:20:06 +0330
**To:** "hash-function@nist.gov" <hash-function@nist.gov>
**CC:** "hash-forum@nist.gov" <hash-forum@nist.gov>

Hi,

I've had some observations on Tangle which can be utilized in the future.

Best regards,
Yaser Esmaeili
Sharif University of Technology, Iran

| | | |
|---|---|---|
| **Tangle_Observation.pdf** | **Content-Type:** | application/pdf |
| | **Content-Encoding:** | base64 |

# Some observations on Tangle

Yaser Esmaeili Salehani
yaser.esmaeili@gmail.com

## 1. Introduction

Tangle is a hash function proposed by Alvarez, McGuire and Zamora [AMZ08] at the NIST Hash Competition3. No attack or weakness has been reported so far. In this paper, we give some observations on Tangle which can be utilized in the future.

## 2. Some observations on Tangle

We do not bring Tangle description and use the same notations and symbols as mentioned in [AMZ08].

**Notations:** $X(i,j) = X^i_j$ [e.g. $M(i,127) = M^i_{127}$]

**Assumption:** Let $M'(i,127) - M(i,127) = M(i,119) – M'(i,119) = \Delta$ or $M'(i,127) + M'(i,119) = M(i,127) + M(i,119) = \Delta'$

With considering the Generator Seeding (GS) process and the above assumption, we investigate two chaining variables (e.g. X' and X) (also the middle variables) as following:

$j=0$; $g'_1= g_1, \ldots,g'_6 = g_6$ , $X'(0,0) = X(0,0)$,

.

.

.

$j=7$; $g'_1= g_1, \ldots,g'_5 = g_5$ , $g'_6 = M (i,103) + M (i,111) + M'(i,119) + M'(i,127) = g_6$, $X'(0,7) = FR_1(g_1+ g_2+ g_3) + FR_2(g_4+ g_5+ g'_6) = X(0,7)$

So, all of $X'(0,j) = X(0,j)$ $(j=0,1,\ldots,7)$.

In the next step, we consider the Iteration and Extraction (I&E) and Round Function (RF) processes together and apply them on the previous variables as following:

**Note:** Let R=72 if Tangle-224.

k=1 to R/2 (=36) and r=0 to R-1 (=71)

(I&E) **k=1**; $X'(1,0) = X(1,0), \ldots , X'(1,7) = X(1,7)$, $t=0$, $W'_1 = W_1, \ldots, W'_3 = W_3$

(RF**) r=0**; $C'=C$, $s'=s$, $p'=p$, $q'=q$; $A'=A$, $B'=B$, $h'_0=h_0$, $h'_{16}=h_{16}$ **; r=1**; $C'=C$, $s'=s$, $p'=p$, $q'=q$; $A'=A$, $B'=B$, $h'_1=h_1$, $h'_{17}=h_{17}$.

(I&E) **k=2**; $X'(2,0) = X(2,0), \ldots , X'(2,7) = X(2,7)$, $t=4$, $W'_4 = W_4, \ldots, W'_7 = W_7$

(RF) **r=2**; $C'=C$, $s'=s$, $p'=p$, $q'=q$; $A'=A$, $B'=B$, $h'_2=h_2$, $h'_{18}=h_{18}$ ; **r=3**; $C'=C$, $s'=s$, $p'=p$, $q'=q$; $A'=A$, $B'=B$, $h'_3=h_3$, $h'_{18}=h_{18}$.

.

.

.

(I&E) **k=30**; $X'(30,0) = X(30,0), \ldots , X'(30,7) = X(30,7)$, $t=116$, $W'_{116} = W_{116}, \ldots,$ $W'_{119} = F_2(X'(30,6), X'(30,7),K_{119}) + M'(i,119) = W_{119} – \Delta$.

(RF) **r=58**; $C' = W'_{116} + W'_{117} = C$, $s'=s$, $p'=p$, $q'=q$; $A'=A$, $B'=B$, $h'_0=h_0$, $h'_{16}=h_{16}$ ;
**r=59**; $C' = W'_{118} + W'_{119} = C - \Delta$, $s' = s \oplus Sbox(C' \oplus (C'>>8) \oplus (C'>>16) \oplus (C'>>24))$
it can be showed that $s'=s$ by choosing the appropriate $(-\Delta)$ (e.g. let $-\Delta = \Delta_3\Delta_2\Delta_1\Delta_0$, and $\Delta_0 = \Delta_1 = 0$, $\Delta_3 = \Delta_2 = 0x80$.), then, $p'=p$, $q'=q$; $A'=A$,
$B' = F_2(h_{q'}, h_3, FR_2(h_{p'+16}) + W'_{119} = B - \Delta$, $h'_{27} = h_{27} + B' = h_{27} - \Delta$,
$h'_{11} = h_{11} \oplus (A+B') = h_{11} \oplus (A+B-\Delta)$.

(I&E) **k=31**; $X'(31,0) = X(31,0)$, … , $X'(31,7) = X(31,7)$, $t=120$, $W'_{120} = W_{120}$, …, $W'_{123} = W_{123}$.
(RF) **r=60**; $C' = C$, $s'=s$, $p'=p$, $q'=q$; here, some conditions might be risen: for example: if $p' = p = 11$, then $h'_{11} \neq h_{11}$ and/or $h'_{11+16} \neq h_{11+16}$ and finally,
$A' = F_1(h_{p'}, h_{28}, FR_1(h_{q'+16})) + W'_{120} + K_{s'} \neq (?)\ A$, $B' = F_1(h_{q'}, h_4, FR_2(h_{p'+16})) + W'_{121} \neq (?)\ B$, otherwise: $h'_{28} = (?)\ h_{28}$, $h'_{12} = (?)\ h_{12}$ ;
**r=61**; $C' = C$, $s'=s$, $p'=p$, $q'=q$; similar to the previous explanations, if again $p' = p = 11$ and/or 12, then $h'_{11} \neq h_{11}$ and/or $h'_{11+16} \neq h_{11+16}$, also it is possible that $h'_{12} \neq h_{12}$ and/or $h'_{28} \neq h_{28}$, then $A' \neq (?)\ A$, $B' \neq (?)\ B$, otherwise: $h'_{29} = (?)\ h_{29}$, $h'_{13} = (?)\ h_{13}$.

(I&E) **k=32**; $X'(32,0) = X(32,0)$, … , $X'(32,7) = X(32,7)$, $t=124$, $W'_{124} = W_{124}$, …, $W'_{127} = F_2(X'(32,6), X'(32,7), K_{127}) + M'(i,127) = W_{127} + \Delta$.
(RF) **r=62**; $C' = C$, $s'=s$, $p'=p$, $q'=q$; similar to the previous section, if $p' = p = 11$ and/or 12 and/or 13 , then $h'_{11} \neq h_{11}$ and/or $h'_{11+16} \neq h_{11+16}$, also it is possible that $h'_{12} \neq h_{12}$ and/or $h'_{28} \neq h_{28}$, $h'_{13} \neq h_{13}$ and/or $h'_{29} \neq h_{29}$ then $A' \neq (?)\ A$, $B' \neq (?)\ B$, otherwise: $h'_{30} = (?)\ h_{30}$, $h'_{14} = (?)\ h_{14}$;
**r=63**; $C' = W'_{126} + W'_{127} = C + \Delta$, $s' = s \oplus Sbox(C' \oplus (C'>>8) \oplus (C'>>16) \oplus (C'>>24))$, again, it can be showed that $s'=s$ by choosing the appropriate $(\Delta)$ (e.g. let $\Delta = \Delta_3\Delta_2\Delta_1\Delta_0$, and $\Delta_0 = \Delta_1 = 0$, $\Delta_3 = \Delta_2 = 0x80$ or the other options.), then, $p'=p$, $q'=q$; similar to the previous section, if $p' = p = 11$ and/or 12 and/or 13 and/or 14, then $h'_{11} \neq h_{11}$ and/or $h'_{11+16} \neq h_{11+16}$, also it is possible that $h'_{12} \neq h_{12}$ and/or $h'_{28} \neq h_{28}$, $h'_{13} \neq h_{13}$ and/or $h'_{29} \neq h_{29}$, $h'_{14} \neq h_{14}$ and/or $h'_{30} \neq h_{30}$ then $A' \neq (?)\ A$, $B' \neq (?)\ B$, otherwise: $h'_{31} = (?)\ h_{31}$, $h'_{15} = (?)\ h_{15}$.
.
.
.
(I&E) **k=36**; $X'(36,0) = X(36,0)$, … , $X'(36,7) = X(36,7)$, $t=140$, $W'_{141} = W_{141}$, …, $W'_{144} = W_{144}$.
(RF) **r=70**; $C' = C$, $s'=s$, $p'=p$, $q'=q$; similar to the previous section, if $p' = p = 11$ and/or 12 ... and/or 21, then $h'_{11} \neq h_{11}$ and/or $h'_{11+16} \neq h_{11+16}$, also it is possible that $h'_{12} \neq h_{12}$ and/or $h'_{28} \neq h_{28}$, ... , $h'_{21} \neq h_{21}$ and/or $h'_6 \neq h_6$ then $A' \neq (?)\ A$, $B' \neq (?)\ B$, otherwise: $h'_6 = (?)\ h_6$, $h'_{22} = (?)\ h_{22}$;
**r=71**; $C' = C$, $s' = s$, $p'=p$, $q'=q$; similar to the previous section, if $p' = p = 11$ and/or 12 ... and/or 22, then $h'_{11} \neq h_{11}$ and/or $h'_{11+16} \neq h_{11+16}$, also it is possible that $h'_{12} \neq h_{12}$ and/or $h'_{28} \neq h_{28}$, ... , $h'_{22} \neq h_{22}$ and/or $h'_7 \neq h_7$ then $A' \neq (?)\ A$, $B' \neq (?)\ B$, otherwise: $h'_7 = (?)\ h_7$, $h'_{23} = (?)\ h_{23}$.
Although the output hash values are depended on the first seven words of $h_i$ ($i=0,1,\ldots,6$), it is clear that some output words do not change at all such as: $h_8$ , $h_9$ , $h_{10}$ , $h_{24}$ , $h_{25}$ , $h_{26}$.

Obviously, we can not say that a direct attack has been proposed, but an attack might be found to exploit this weakness. In future, we will give more details our observations.

Also, it can be continued for the upper rounds of Tangle (e.g. for R=80 (Tangle-256)).

## 3. References

[AMZ08] Rafael Alvarez, Gary McGuire and Antonio Zamora, "The Tangle Hash Function", Submission to NIST, 2008. http://ehash.iaik.tugraz.at/wiki/Tangle.

**Subject:** OFFICIAL COMMENT: Tangle
**From:** Søren Steffen Thomsen <ssth@win.dtu.dk>
**Date:** Tue, 16 Dec 2008 15:38:49 +0100
**To:** <hash-function@nist.gov>
**CC:** <hash-forum@nist.gov>

Hi,
I have found practical collisions in Tangle-n for all supported digest sizes n.

As an example, the following is a collision in Tangle-256 (messages are written byte-by-byte, without padding):

```
Message 1:
c8190000000000000000000000000000000000000000000000000000000000000000000000000000
Hash of message 1:
f710be651ab67737a58ac452056bbf13e62abed071943617dadbf25c2dea710b
Message 2:
c819008000000080000000000000000000000000000000000000000000000000000000008000000080
Hash of message 2:
f710be651ab67737a58ac452056bbf13e62abed071943617dadbf25c2dea710b
XOR of hashes:
0000000000000000000000000000000000000000000000000000000000000000
```

A description of the attack can be downloaded from
http://www.mat.dtu.dk/people/S.Thomsen/tangle/tangle-coll.pdf.

Best regards,
Søren Thomsen.

--
Søren Steffen Thomsen
PH.D. student
DTU Mathematics
-------------------------------
Technical University of Denmark
Department of Mathematics
Matematiktorvet 303S
Building 303S
2800 Kgs. Lyngby
Direct +45 4525 3010
Mobile +45 2290 5443
S.Thomsen@mat.dtu.dk
www.mat.dtu.dk/