TRIVIUM's output partially autocancels

Michael Vielhaber vielhaber@gmail.com September, 2nd 2008
Hochschule Bremerhaven, An der Karlstadt 8, D–27568 Bremerhaven, Germany and
Instituto de Matemáticas, Universidad Austral de Chile, Casilla 567, Valdivia, Chile

ABSTRACT The eStream cipher proposal TRIVIUM outputs an XOR sum of six internal state bits. These in turn are obtained from 18 bits linearly, plus six ANDings of two bits each.

We show that 4 of the 18 linear terms cancel between themselves.

Keywords: Trivium, eStream, Algebraic IV differential attack, AIDA.

The eStream cipher proposal TRIVIUM [1] has a 288 bit register with bits $s_1, \ldots s_{288}$.
After 1152 cycles of setting up the system, each new cycle outputs the combination

$$OUT(t) = s_{66}(t) \oplus s_{93}(t) \oplus s_{162}(t) \oplus s_{177}(t) \oplus s_{243}(t) \oplus s_{288}(t).$$

We have $s_{66}(t) = s_1(t-65)$, except at sites 1, 94, and 178, (only shifts). In turn

$$s_1(t-65) = s_{243}(t-66) \oplus s_{288}(t-66) \oplus \underline{s_{69}(t-66)} \oplus (s_{286}(t-66) \wedge s_{287}(t-66)),$$

similarly

$$s_{93}(t) = s_1(t-92) = \cdots \oplus \underline{s_{69}(t-93)} \ldots.$$

Finally, we need $s_{162}(t) = s_{94}(t-68)$ by shifting and then

$$s_{162}(t) = s_{94}(t-68) = \underline{s_{66}(t-69)} \oplus \underline{s_{93}(t-69)} \oplus s_{171}(t-69) \oplus (s_{91}(t-69) \wedge s_{92}(t-69)).$$

Notice now that

$$s_{69}(t-66) = s_1(t-135) = s_{66}(t-69)$$

as well as

$$s_{69}(t-93) = s_1(t-162) = s_{93}(t-69),$$

in other words, 4 of the 18 linear terms (22%) cancel out between themselves.

The annoying equalities are $162-(94-66) = 66-(1-69)$ and $93-(1-69) = 162-(94-93)$, where the leading term is the output site, and the parentheses cover the feedback taps. Both simplify to $69 - 1 = 162 - 94 = \mathbf{68}$.

"Never use a distance twice."

ADVERTISEMENT This might be one reason, why the AIDA attack (see [2]) is successful at least up to 640 bits into the setup length of TRIVIUM.

References

[1] Christophe de Cannière, Bart Preneel, "TRIVIUM Specifications"
http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf

[2] M. Vielhaber, "Breaking ONE.FIVIUM by AIDA, an Algebraic IV Differential Attack", eprint.iacr.org/2007/413.pdf