Cryptanalyse de Trivium par *Cube Attack* et *Cube Tester*

Léo Barré

Équipe CARAMBA - Inria Nancy Grand-Est
Master Cryptologie et Sécurité Informatique - Université de Bordeaux

13 Septembre 2017

Sommaire

Sommaire

Principe

Soient

- $K \in \mathbb{F}_2^n$, une clé de n bits,
- $M \in \mathbb{F}_2^m$, un message de m bits,
- $G_n^m : \mathbb{F}_2^n \to \mathbb{F}_2^m$, un générateur pseudo-aléatoire.

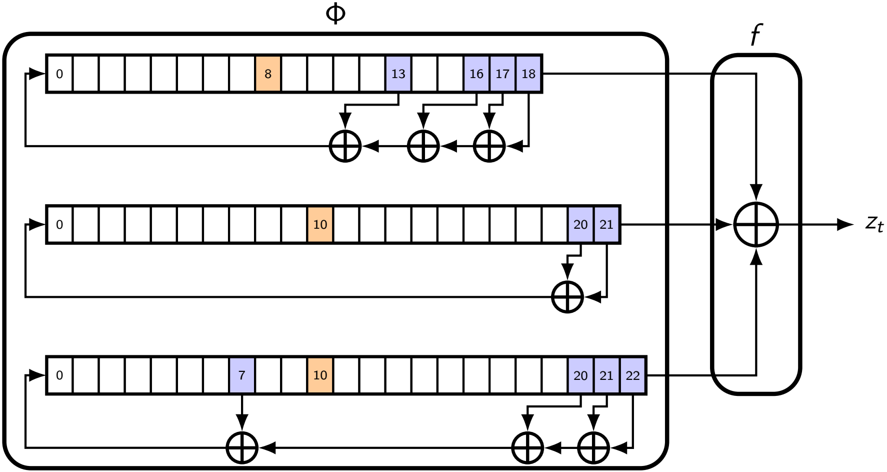
Un chiffrement à masque jetable est un chiffrement où :

- encryption : $C = M \oplus G_n^m(K)$
- decryption : $M = C \oplus G_n^m(K)$

Avantages :

- plus rapide et moins gourmand qu'un chiffrement par bloc
- si G_n^m générateur aléatoire $\Rightarrow$ chiffrement incassable (*One-Time Pad*)

Chiffrement par flot : A5/1 (crédit : Jérémie Detrey)



Sommaire

"Stream Cipher Project" (2004-2008)

a.k.a. eSTREAM

- mené par l'ECRYPT
- Objectif : rassembler de nouvelles primitives robustes de chiffrement par flot
- Deux catégories :
  - "*software*" : primitives à exécution rapide
  - "*hardware*" : primitives à faible coût en ressource
- découpé en trois phases de tests (performance, cryptanalyse, etc.)
- portfolio officiel (2012) :

"*software*"	"*hardware*"
HC	Grain
Rabbit	MICKEY
Salsa20	Trivium
SOSEMANUK	

Sommaire

Trivium

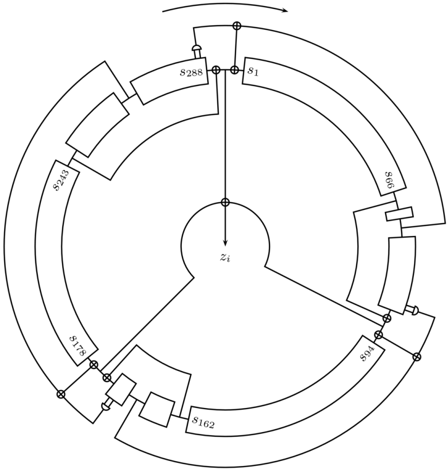


Figure – Trivium [2, Fig. 6]

- conçu par Cristophe De Cannière et Bart Preneel
- clé : $k \in \mathbb{F}_2^{80}$
- IV : $x \in \mathbb{F}_2^{80}$
- état interne : registre de 288 bits partitionné en trois (93, 84, 111)
- mise à jour du $i^{\text{ème}}$ tour $\Rightarrow$ bit de suite chiffrante z_i
- 1152 tours de *warm'up*

Algorithme

INITIALISATION

$$(S_1, \ldots, S_{93}) \leftarrow (k_1, \ldots, k_{80}, 0, \ldots, 0)$$
$$(S_{94}, \ldots, S_{177}) \leftarrow (x_1, \ldots, x_{80}, 0, 0, 0, 0)$$
$$(S_{178}, \ldots, S_{288}) \leftarrow (0, \ldots, 0, 1, 1, 1)$$

MISE À JOUR

$$t_1 \leftarrow S_{66} + S_{93}$$
$$t_2 \leftarrow S_{162} + S_{177}$$
$$t_3 \leftarrow S_{243} + S_{288}$$

$$z_i \leftarrow t_1 + t_2 + t_3$$

$$t_1 \leftarrow t_1 + S_{91} S_{92} + S_{171}$$
$$t_2 \leftarrow t_2 + S_{175} S_{176} + S_{264}$$
$$t_3 \leftarrow t_3 + S_{286} S_{287} + S_{69}$$
$$(S_1, \ldots, S_{93}) \leftarrow (t_3, S_1, \ldots, S_{92})$$
$$(S_{94}, \ldots, S_{177}) \leftarrow (t_1, S_{94}, \ldots, S_{176})$$
$$(S_{178}, \ldots, S_{288}) \leftarrow (t_2, S_{178}, \ldots, S_{287})$$

Sommaire

Attaques sur Trivium-N

(Trivium avec N tours de warm'up)

Attaques par différenciation selon les IVs :
soit $I \subseteq \{x_1, \ldots, x_{80}\}$, on considère l'ensemble des IVs $\left\{x \in \mathbb{F}_2^{80} \;\middle|\; x_i = 1 \Rightarrow i \in I,\ \forall i\right\}$ et leurs suites chiffrantes

- Englund, Johansson et Turan [4] :
  - Analyse statistique
  - $\rightarrow$ Distinction sur Trivium-736
- Vielhaber [11] :
  - AIDA (*Algebraic IV Differential Attack*)
  - $\rightarrow$ Récupération sur Trivium-576
- Fischer, Khazaei et Meier [5] :
  - AIDA + tests statistiques
  - $\rightarrow$ Récupération sur Trivium-672 (complexité : 2^{55})

Attaques sur Trivium-N

(Trivium avec N tours de warm'up)

Attaques par différenciation selon les IVs :
soit $I \subseteq \{x_1, \ldots, x_{80}\}$, on considère l'ensemble des IVs $\left\{x \in \mathbb{F}_2^{80} \;\middle|\; x_i = 1 \Rightarrow i \in I,\ \forall i\right\}$ et leurs suites chiffrantes

- Englund, Johansson et Turan [4] :
  - Analyse statistique
  - $\rightarrow$ Distinction sur Trivium-736
- Vielhaber [11] :
  - AIDA (*Algebraic IV Differential Attack*) $\Rightarrow$ cubes de Dinur-Shamir
  - $\rightarrow$ Récupération sur Trivium-576
- Fischer, Khazaei et Meier [5] :
  - AIDA + tests statistiques
  - $\rightarrow$ Récupération sur Trivium-672 (complexité : 2^{55})

Sommaire

Contexte

On considère

- $p(x_1,\ldots,x_n) \in \mathbb{B}_{x_1,\ldots,x_n} \left(= \frac{\mathbb{F}_2[x_1,\ldots,x_n]}{\left\langle x_1^2+x_1,\ldots,x_n^2+x_n \right\rangle} \right)$, un polynôme booléen
- $I \subseteq \{1,\ldots,n\}$, un ensemble d'indices d'IV
- $t_I = \prod_{i \in I} x_i$, son monôme associé

et l'exemple fil rouge suivant
Exemple :

$$\begin{aligned} p(x_1,x_2,x_3,x_4,x_5) =& x_1x_2x_3 + x_1x_2x_4 + x_2x_4x_5 \\ & + x_1x_2 + x_2 + x_3x_5 + x_5 + 1 \\ I =& \{1,2\} \\ \Rightarrow t_I =& x_1x_2 \end{aligned}$$

Definition

Le superpoly de p par I est le polynôme $p_{S_I} \in \mathbb{B}_{x_1,\dots,x_n}$ tel que :

$$p = t_I \cdot p_{S_I} + r \text{ , avec } r_{S_I} = 0.$$

Exemple :

$$\begin{aligned} p =& x_1x_2x_3 + x_1x_2x_4 + x_2x_4x_5 \\ & + x_1x_2 + x_2 + x_3x_5 + x_5 + 1 \\ t_I =& x_1x_2 \\ p =& x_1x_2(x_3 + x_4 + 1) + (x_2x_4x_5 + x_2 + x_3x_5 + x_5 + 1) \\ p_{S_I} =& x_3 + x_4 + 1 \end{aligned}$$

Definition

Un *maxterm* t_I est tel que le superpoly associé p_{S_I} est de degré 1.

Definition

Le cube de Dinur-Shamir défini par I est l'ensemble des $2^{|I|}$ polynômes $p_{|v}$, et leur somme p_I, où $v \subseteq I$ et $p_{|v}$ est le polynôme p dont chaque variable subit la substitution

$$x_i \xrightarrow{v} \begin{cases} 1 & \text{si } i \in v, \\ 0 & \text{si } i \in I \backslash v, \\ x_i & \text{sinon.} \end{cases}$$

Exemple : $p = x_1 x_2 (x_3 + x_4 + 1) + (x_2 x_4 x_5 + x_2 + x_3 x_5 + x_5 + 1)$

x_1	x_2	$p_{\|v}$
0	0	$x_3x_5 + x_5 + 1$
1	0	$x_3x_5 + x_5 + 1$
0	1	$x_4x_5 + x_3x_5 + x_5$
1	1	$x_3 + x_4 + x_4x_5 + x_3x_5 + x_5 + 1$
p_I		$x_3 + x_4 + 1$

Theorem

Pour tout p et I, $p_I = p_{S_I}$.

Sommaire

Contexte :

- On considère les polynômes booléens des bits de suite chiffrante en fonction de ceux d'IV et de clé : $z_i \in \mathbb{B}_{K,X}$

auteur(s)	ℓ	N	clés
Dinur, Shamir [3]	12	672 - 685	all
	23	735 - 747	all
	29	767 - 774	all
Fouque, Vannet [6]	30 (38)	784	all
	37 (40)	799	all

test le plus probant : **neutralité**

$$j \text{ est neutre pour } p \Leftrightarrow p(v) + p(v + e_j) = 0,\ \forall v \in \mathbb{F}_2^n$$

auteur(s)	ℓ	N	clés
Aumasson, Dinur, Meier, Shamir [1]	24	772	all
	30	790	all
Stankovski [10]	44	806	all
Knellwolf, Meier, Naya-Plasencia [7]	25	798	all
	25	868	2^{31}
	25	961	2^{26}
Liu, Lin, Wang [8]	31	812	all
	34	824	all
	37	839	all
Sarkar, Maitra, Baksi [9]	13	710	all
	20	792	all
	21	801	all
	22	810	all
	27	829	all

Sommaire

Problème SAT

Fonction boléenne :

- variables : $b_1, \ldots, b_n \in \mathbb{F}_2$
- opérateurs : $\vee, \wedge, \neg [, \oplus, \rightarrow, \ldots]$

ex : $f = (b_1 \vee b_2) \wedge (\neg b_1 \vee b_2)$

Problème SAT :

Contexte :	$f(b_1, \ldots, b_n)$ est une formule booléenne
Question :	*existe-t-il une évaluation de chaque booléen b_1 à b_n telle que la formule f soit vraie ?*

ex : f est SATisfiable pour $(b_1, b_2) \in \{(false, true), (true, true)\}$

Problème NP-complet

Trivium en SAT

Trivium (inspiré de la version de Bernstein)

$$(a_{-1}, \ldots, a_{-93}) \leftarrow (k_1, \ldots, k_{80}, 0, \ldots, 0)$$
$$(b_{-1}, \ldots, b_{-84}) \leftarrow (x_1, \ldots, x_{80}, 0, 0, 0, 0)$$
$$(c_{-1}, \ldots, c_{-111}) \leftarrow (0, \ldots, 0, 1, 1, 1)$$

$\forall i \geq 0$:

$$t_{1_i} = a_{i\text{-}66} \oplus a_{i\text{-}93}$$
$$t_{2_i} = b_{i\text{-}69} \oplus b_{i\text{-}84}$$
$$t_{3_i} = c_{i\text{-}66} \oplus c_{i\text{-}111}$$

$$\lambda_{1_i} = a_{i\text{-}92} \wedge a_{i\text{-}91}$$
$$\lambda_{2_i} = b_{i\text{-}83} \wedge b_{i\text{-}82}$$
$$\lambda_{3_i} = c_{i\text{-}110} \wedge c_{i\text{-}109}$$

$$a_i = t_{3_i} \oplus \lambda_{3_i} \oplus a_{i\text{-}69}$$
$$b_i = t_{1_i} \oplus \lambda_{1_i} \oplus b_{i\text{-}78}$$
$$c_i = t_{2_i} \oplus \lambda_{2_i} \oplus c_{i\text{-}87}$$
$$z_i = t_{1_i} \oplus t_{2_i} \oplus t_{3_i}$$

Attaques menées

- SAT-solver : **co-processeur de Riss (Donau)** $\oplus$ **Plingeling** (versions SAT competition 2016)
- Environnement : 4 cœurs, 3.20 GHz
- Plusieurs IVs (et leurs suites chiffrantes) considérés à la fois

Version	Nb d'IVs	Bits de sortie	Temps
Trivium-224	6	226	3s
Trivium-256	10	176	17s
Trivium-272	15	128	40s
Trivium-280	20	120	75s
Trivium-284	22	116	1 500s
Trivium-288	20	172	4 800s

Sommaire

Test du χ^2

- Sert à évaluer la qualité d'un biais calculé.
- Caractéristiques sur N tests [$p(v) + p(v + e_j) =?$] :
  - 2 résultats possibles pour chaque test $\Rightarrow$ 1 degré de liberté
  - comparaison avec loi uniforme $\frac{N}{2}$
  - pourcentage : $\frac{n}{N}$

  $\Rightarrow$ calcul du χ^2 ici :

$$\chi^2 = 2\frac{\left(n - \frac{N}{2}\right)^2}{\frac{N}{2}}$$

- Biais valable $\Leftrightarrow \chi^2 > \chi_\tau$, avec τ la marge d'erreur :

τ	χ_τ
10%	2.706
5%	3.841

τ	χ_τ
1%	6.635
0.1%	10.828

Notations

On considère ici des couples modèle d'IV / modèle de clé codés comme suit pour chaque bit :

$$x_i : \begin{cases} \texttt{0} & \Rightarrow x_i \text{ prend la valeur fixe } 0 \\ \texttt{1} & \Rightarrow x_i \text{ prend la valeur fixe } 1 \\ \texttt{c} & \Rightarrow x_i \text{ est dans l'ensemble du cube} \\ \texttt{n} & \Rightarrow \text{on regarde la neutralité de } x_i \end{cases}$$

$$k_i : \begin{cases} \texttt{0} & \Rightarrow k_i \text{ prend la valeur fixe } 0 \\ \texttt{1} & \Rightarrow k_i \text{ prend la valeur fixe } 1 \\ \texttt{r} & \Rightarrow k_i \text{ prend une valeur aléatoire} \end{cases}$$

Exemple : $I = \{1, 3, 10, 12, 14, 38, 45, 48, 50, 69, 75, 79\}$
test de neutralité du bit 23, clés totalement aléatoires

$$\begin{cases} x : & \texttt{c0c000000c0c0c00000000n00000000000000c00} \\ & \texttt{0000c00c0c000000000000000000c00000c000c0} \\ k : & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \\ & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \end{cases}$$

Clés faibles de Knellwolf (20 000 tests)

$$\begin{cases} x : & \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c00c} \\ & \texttt{00c00c00c00c00c00c00c00c00c00c00n00n00n0} \\ k : & \texttt{r00r00r00r00r00r00r00r00r00r00r00r00r00r} \\ & \texttt{00r00r00r00r00r00r00r00r00010r00r00r00r0} \end{cases} \Rightarrow$$

	73	76	79
953	0.00 20 000	0.00 20 000	0.00 20 000
961	100.00 20 000	50.37 1.066	0.00 20 000

Clés aléatoires (20 000 tests)

$$\begin{cases} x : & \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c00c} \\ & \texttt{00c00c00c00c00c00c00c00c00c00c00n00n00n0} \\ k : & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \\ & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \end{cases} \Rightarrow$$

	73	76	79
798	44.83 213.83	41.71 549.13	34.25 1 985.8
805	47.87 36.30	49.36 3,328	47.35 56.39
808	49.56 1.549	48.74 12.70	48.80 11.52

Cubes de Knellwolf

Clés faibles de Knellwolf régularisées (20 000 tests)

$$\begin{cases} x : & \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c} \\ & \texttt{00c00c00c00c00c00c00c00c00c00n00n00n0} \\ k : & \texttt{r00r00r00r00r00r00r00r00r00r00r00r00r} \\ & \texttt{00r00r00r00r00r00r00r00r00r00r00r00r0} \end{cases} \Rightarrow$$

	73	76	79
952	24.69 5 124.8	24.92 5 034.1	74.99 4 994.0
968	24.44 5 228.6	24.86 5 056.2	24.98 5 010.0

Cube de Knellwolf prolongé

Clés aléatoires (22 000 tests)

$$\begin{cases} x : & \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c00c} \\ & \texttt{00c00c00c00c00c00c00c00c00c00c00c00c00n0} \\ k : & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \\ & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \end{cases} \Rightarrow$$

798	20.11 7 860.1
808	39.13 1 040.3
818	48.76 13.45

Clés faibles de Knellwolf (20 000 tests)

$$\begin{cases} x : & \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c00c} \\ & \texttt{00c00c00c00c00c00c00c00c00c00c00c00c00n0} \\ k : & \texttt{r00r00r00r00r00r00r00r00r00r00r00r00r00r} \\ & \texttt{00r00r00r00r00r00r00r00r00010r00r00r00r0} \end{cases} \Rightarrow$$

961	0.00 20 000
962	0.00 20 000
977	0.00 20 000

Cube de Sarkar

Clés aléatoires (20 000 tests)

$$\begin{cases} x : \texttt{0c00c00c00c00c00c00c00c00c00c00c00c00c00} \\ \quad\;\; \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c00n} \\ k : \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \\ \quad\;\; \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \end{cases} \Rightarrow$$

808	45.62 153.48
816	47.71 41.95
818	47.71 13.21

Clés faibles de Knellwolf décalées (1 000 tests)

$$\begin{cases} x : \texttt{0c00c00c00c00c00c00c00c00c00c00c00c00c00} \\ \quad\;\; \texttt{c00c00c00c00c00c00c00c00c00c00c00c00c00n} \\ k : \texttt{0r00r00r00r00r00r00r00r00r00r00r00r00r00} \\ \quad\;\; \texttt{r00r00r00r00r00r00r00r00r00010r00r00r00r} \end{cases} \Rightarrow$$

953	0.00 1 000.0
954	0.00 1 000.0
969	0.00 1 000.0

Petit cube (taille : 13)

$I = \{2, 5, 8, 11, 14, 17, 20, 23, 26, 47, 50, 53, 65\}$

<u>Clés aléatoires</u> (100 000 tests)

$$\begin{cases} x : & \texttt{0c00n00c00c00c00c00c00c00c00000000000000} \\ & \texttt{000000c00c00c00000000000c000000000000000} \\ k : & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \\ & \texttt{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr} \end{cases} \Rightarrow$$

710	33.30 11 157
722	44.51 1 206.0
725	49.15 28.76

Mes résultats

auteur(s)	ℓ	N	clés
Knellwolf, Meier, Naya-Plasencia	25	798	all
	25	868	2^{31}
	25	961	2^{26}
Sarkar, Maitra, Baksi	13	710	all
	20	792	all
	21	801	all
	22	810	all
	27	829	all
Mon stage	13	725	all
	25	808	all
	25	968	2^{27}
	27	818	all
	27	969	2^{26}
	27	977	2^{26}

Conclusion

- principal problème : trouver des cubes
- aucune méthode polynomiale pour déterminer la qualité d'un cube
  $\Rightarrow$ SAT-solvers inutiles pour l'instant
- pour la prochaine fois :
  - $\rightarrow$ **Neutrality test $\oplus$ Möbius**
    permet de tester la neutralité de plusieurs cubes en même temps
  - $\rightarrow$ **SAT-solver poussé**
    SAT competition 2017 achevée début septembre, considérer tests plus longs

Références I

Jean-Philippe Aumasson, Itai Dinur, Willi Meier, and Adi Shamir.
Cube testers and key recovery attacks on reduced-round MD6 and trivium.
In Orr Dunkelman, editor, Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers, volume 5665 of Lecture Notes in Computer Science, pages 1–22. Springer, 2009.

Christophe De Cannière and Bart Preneel.
Trivium.
In Matthew J. B. Robshaw and Olivier Billet, editors, New Stream Cipher Designs - The eSTREAM Finalists, volume 4986 of Lecture Notes in Computer Science, pages 244–266. Springer, 2008.

Itai Dinur and Adi Shamir.
Cube attacks on tweakable black box polynomials.
In Antoine Joux, editor, Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings, volume 5479 of Lecture Notes in Computer Science, pages 278–299. Springer, 2009.

Références II

Håkan Englund, Thomas Johansson, and Meltem Sönmez Turan.
A framework for chosen IV statistical analysis of stream ciphers.
In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, Progress in Cryptology - INDOCRYPT 2007, 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007, Proceedings, volume 4859 of Lecture Notes in Computer Science, pages 268–281. Springer, 2007.

Simon Fischer, Shahram Khazaei, and Willi Meier.
Chosen IV statistical analysis for key recovery attacks on stream ciphers.
In Serge Vaudenay, editor, Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings, volume 5023 of Lecture Notes in Computer Science, pages 236–245. Springer, 2008.

Pierre-Alain Fouque and Thomas Vannet.
Improving key recovery to 784 and 799 rounds of trivium using optimized cube attacks.
In Shiho Moriai, editor, Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers, volume 8424 of Lecture Notes in Computer Science, pages 502–517. Springer, 2013.

Références III

Simon Knellwolf, Willi Meier, and María Naya-Plasencia.
Conditional differential cryptanalysis of trivium and KATAN.
In Ali Miri and Serge Vaudenay, editors, Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers, volume 7118 of Lecture Notes in Computer Science, pages 200–212. Springer, 2011.

Meicheng Liu, Dongdai Lin, and Wenhao Wang.
Searching cubes for testing boolean functions and its application to trivium.
In IEEE International Symposium on Information Theory, ISIT 2015, Hong Kong, China, June 14-19, 2015, pages 496–500. IEEE, 2015.

Santanu Sarkar, Subhamoy Maitra, and Anubhab Baksi.
Observing biases in the state : case studies with trivium and trivia-sc.
Des. Codes Cryptography, 82(1-2) :351–375, 2017.

Paul Stankovski.
Greedy distinguishers and nonrandomness detectors.
In Guang Gong and Kishan Chand Gupta, editors, Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings, volume 6498 of Lecture Notes in Computer Science, pages 210–226. Springer, 2010.

Références IV

Michael Vielhaber.
Breaking ONE.FIVIUM by AIDA an algebraic IV differential attack.
IACR Cryptology ePrint Archive, 2007 :413, 2007.