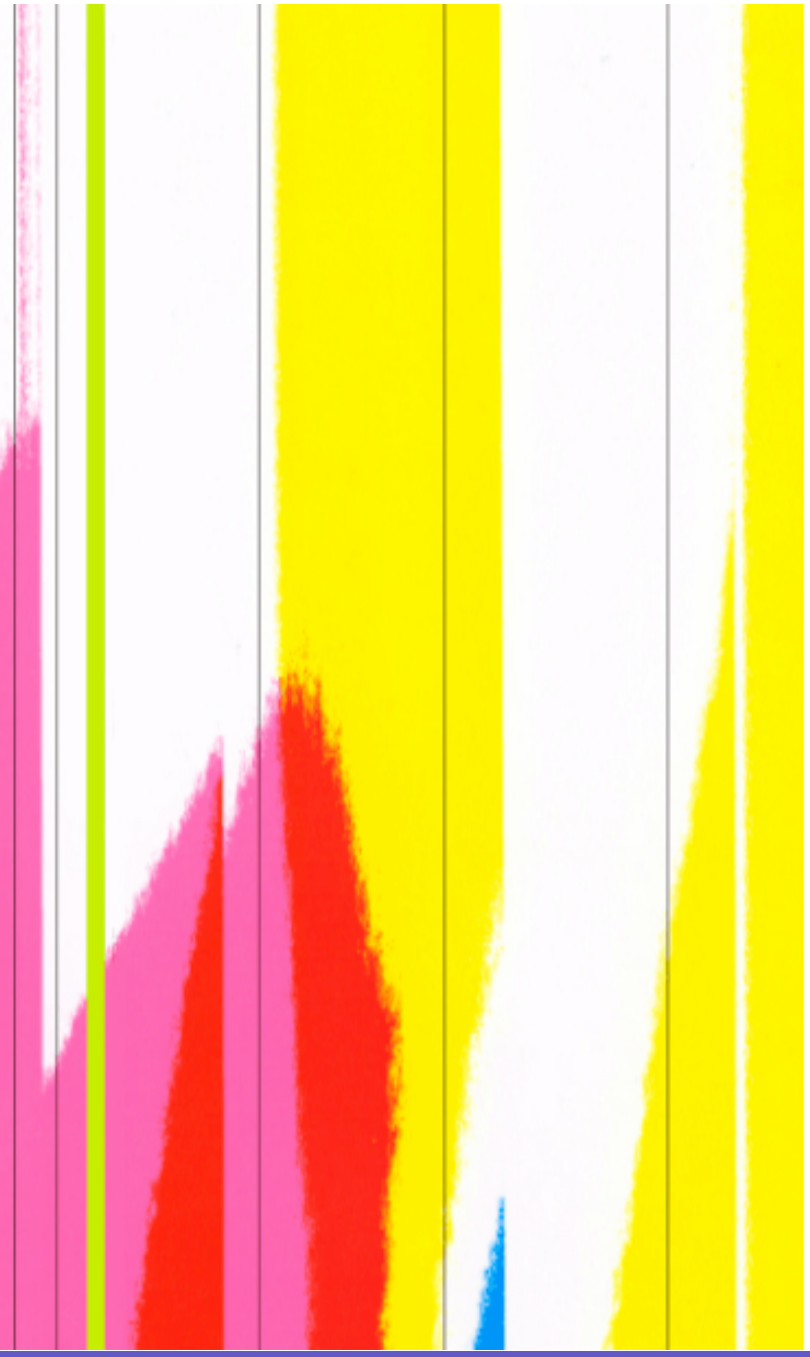


Attaques par Collision contre SHA-1

Stéphane Manuel

CRI Paris-Rocquencourt, Équipe SECRET

Journées Codage et Cryptographie
4 octobre 2009
Fréjus

Plan

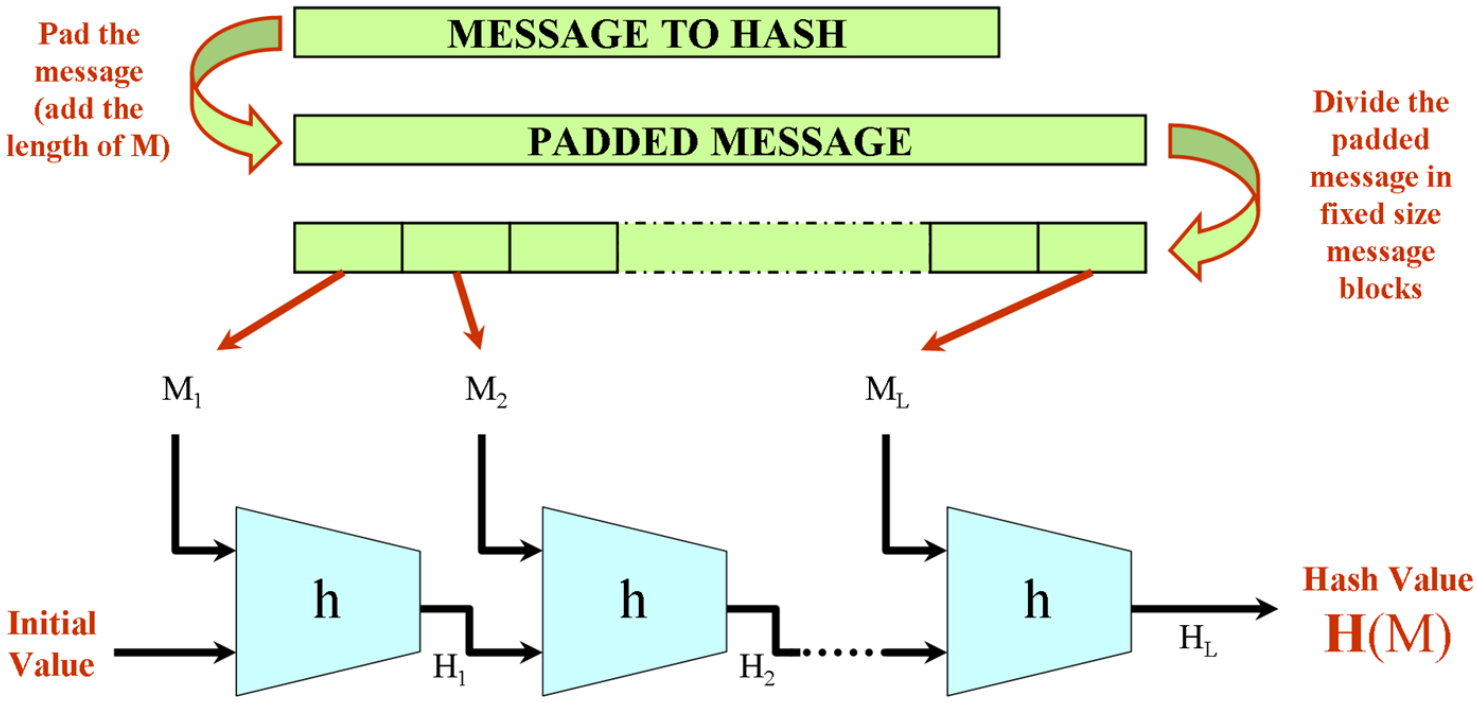
Plan

Fonction de hachage cryptographique

- Une fonction de hachage est un algorithme prenant en entrée une chaîne de bits de longueur arbitraire finie (le message) et restituant en sortie une chaîne de bits de longueur fixée (le haché).
- Propriétés cryptographiques classiques :
  - Résistance aux attaques de pre-image
  - Résistance aux attaques de seconde pre-image
  - Résistance aux attaques par collision

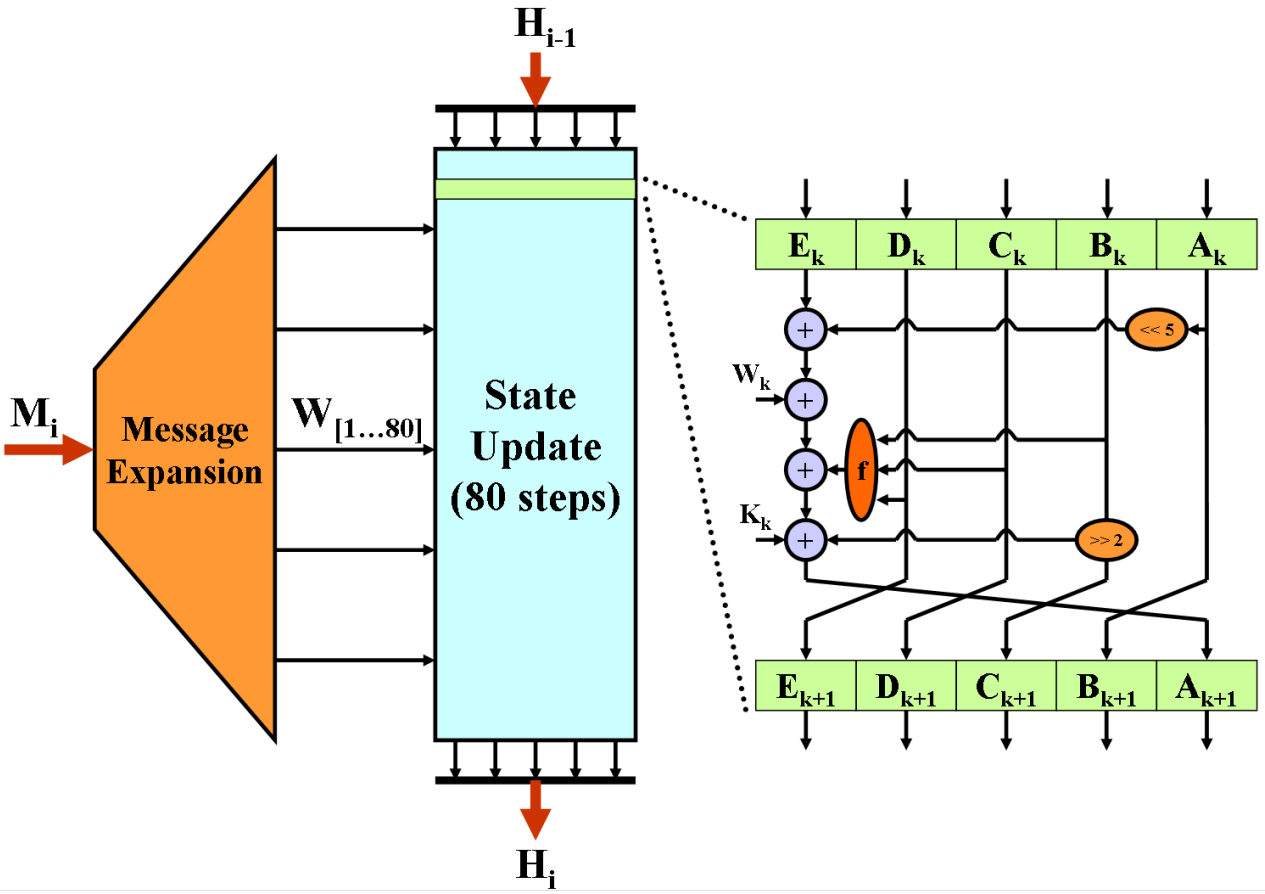
Extenseur de domaine

- L'algorithme de Merkle-Damgård renforcé :



Fonction de compression de SHA-1

- Évolution de SHA-0, proposée en 1995
- Blocs de message de 512 bits, 160 bits en sortie



Fonction de compression de SHA-1

- Expansion de message :

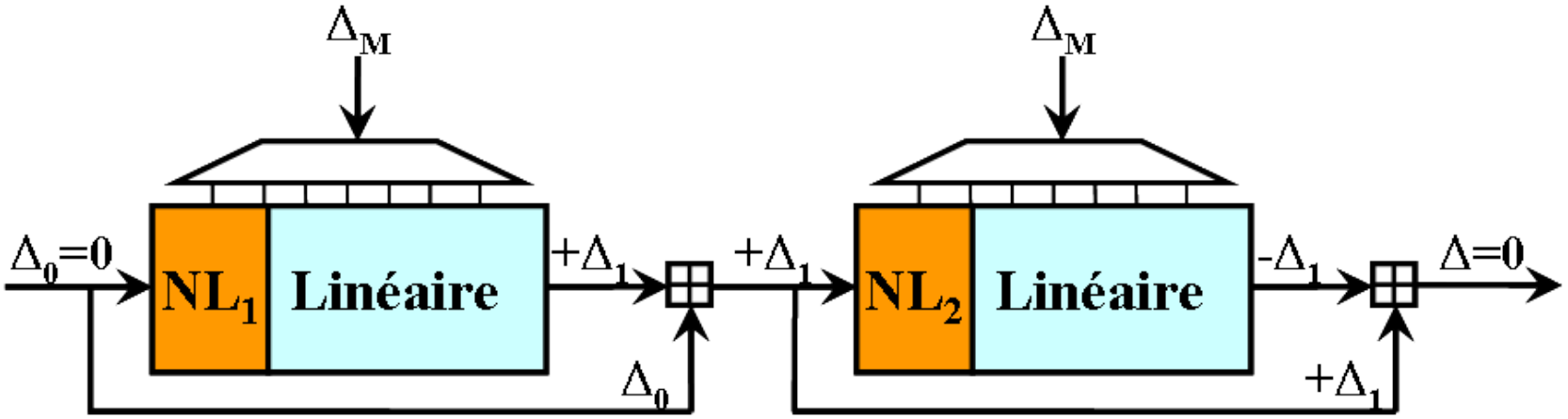
$$W_k = \begin{cases} M_k, & \text{pour } 0 \leq k \leq 15 \\ (W_{k-16} \oplus W_{k-14} \oplus W_{k-8} \oplus W_{k-3}) \lll 1, & \text{pour } 16 \leq k \leq 79 \end{cases}$$

- Fonctions booléennes et constantes :

Pas	Fonction de ronde	Constante
$1 \leq k \leq 20$	$IF = (B \wedge C) \oplus (\overline{B} \wedge D)$	0x5a827999
$21 \leq k \leq 40$	$XOR = B \oplus C \oplus D$	0x6ed6eba1
$41 \leq k \leq 60$	$MAJ = (B \wedge C) \oplus (B \wedge D) \oplus (C \wedge D)$	0x8fabbcdc
$61 \leq k \leq 80$	$XOR = B \oplus C \oplus D$	0xca62c1d6

Plan

Principe d'une attaque contre SHA-1



- Technique des blocs multiples
- 1 caractéristique linéaire
- 2 caractéristiques non-linéaires
- Techniques d'accélérations de recherche

Première étape de l'attaque

Précalcul :

- Trouver une bonne caractéristique linéaire
- Instancier le sens des collisions locales
  - fixer le signe de la différence de sortie
- Traduire l'instanciation en équations sur les bits de message
- Ajouter des boomerangs
  - équations supplémentaires
- Construire une première caractéristique non-linéaire
  - compatible avec les équations

Recherche :

- Trouver une paire de messages vérifiant la différence de sortie
  - utilisation des modifications de message et des boomerangs

Seconde étape de l'attaque

Précalcul :

- Instancier le sens des collisions locales
  - fixer le signe opposé pour la différence de sortie
- Traduire l'instanciation en équations sur les bits de message
- Ajouter des boomerangs
  - équations supplémentaires
- Construire une seconde caractéristique non-linéaire
  - compatible avec les équations et la différence en entrée

Recherche :

- Trouver une paire de messages vérifiant la différence de sortie avec un signe opposé
  - utilisation des modifications de message et des boomerangs

Plan

Vecteur de perturbations

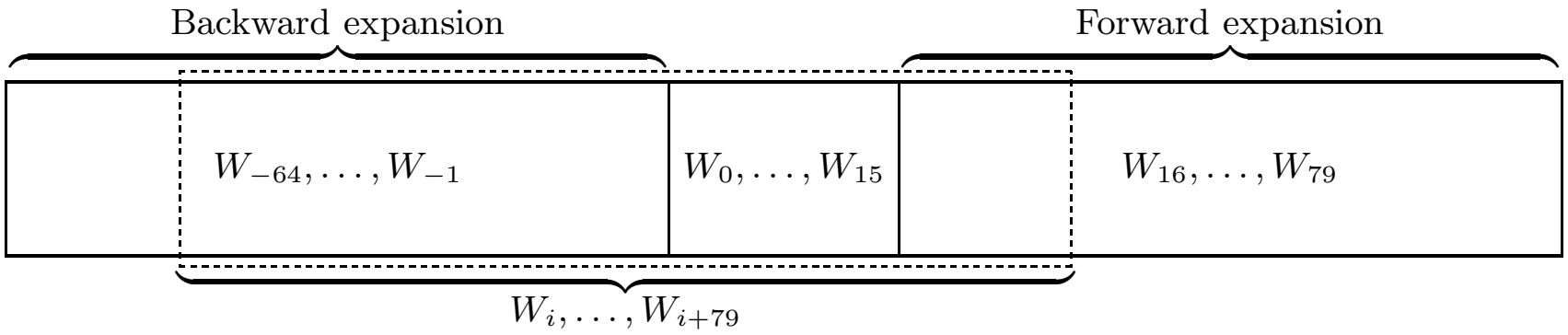
- Permet de définir la caractéristique linéaire :
  - emplacement des collisions locales
- Complexité de l'attaque liée au nombre de collisions locales :
  - vecteur de poids de Hamming faible
- Approche type théorie de l'information :
  - Matusiewicz and Pieprzyk (2004) : *"The problem of finding the best pattern is equivalent to the problem of finding minimum weight codewords in a particular linear code".*
  - Jutla and Patthak (2005) : *"The minimum weight over F2 of any non-zero codeword in the SHA-1 (linear) message expansion code, projected on the last 60 words, is at least 25".*

Rectangle Range

- Wang *et al.* (CRYPTO'05) puis Yajima *et al.* (ASIACCS'08)
  - optimiser le nombre de perturbations sur la position 1
- Définition de l'espace de recherche sous forme de rectangle
  - $\{W_i = (0, \ldots, 0, w_{i,1}, w_{i,0}) | i = t, \ldots, t+15\}$ pour $t = 0, \ldots, 64$
- Pour chaque élément du rectangle :
  - générer le vecteur $(W_0, \ldots, W_t, \ldots, W_{t+15}, \ldots, W_{79})$
  - estimer le nombre de conditions sur les 60 derniers pas
  - sélectionner le vecteur avec le moins de conditions

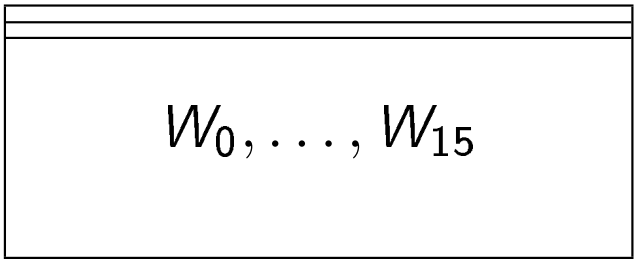
Nouvelle approche

- Fenêtre d'information : 16 mots de 32 bits $(W_0, \ldots, W_{15})$
- Expansion vers l'avant :
  $W_i = (W_{i-16} \oplus W_{i-14} \oplus W_{i-8} \oplus W_{i-3}) \lll 1$, pour $16 \leq i \leq 79$
- Expansion vers l'arrière :
  $W_i = (W_{i+16} \ggg 1) \oplus W_{i+13} \oplus W_{i+8} \oplus W_{i+2}$, pour $-64 \leq i \leq -1$

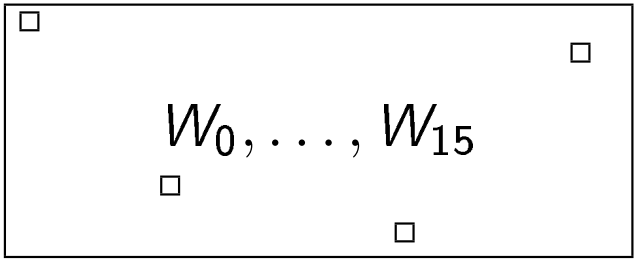


Compromis sur l'espace de recherche

- *Rectangle Range*
  - Poids de la fenêtre d'information ≤ 32
  - Perturbations autorisées sur les positions 0 et 1



- Nouvel algorithme
  - Poids de la fenêtre d'information $\leq pw$
  - Perturbations autorisées sur les positions $0, \ldots, 31$



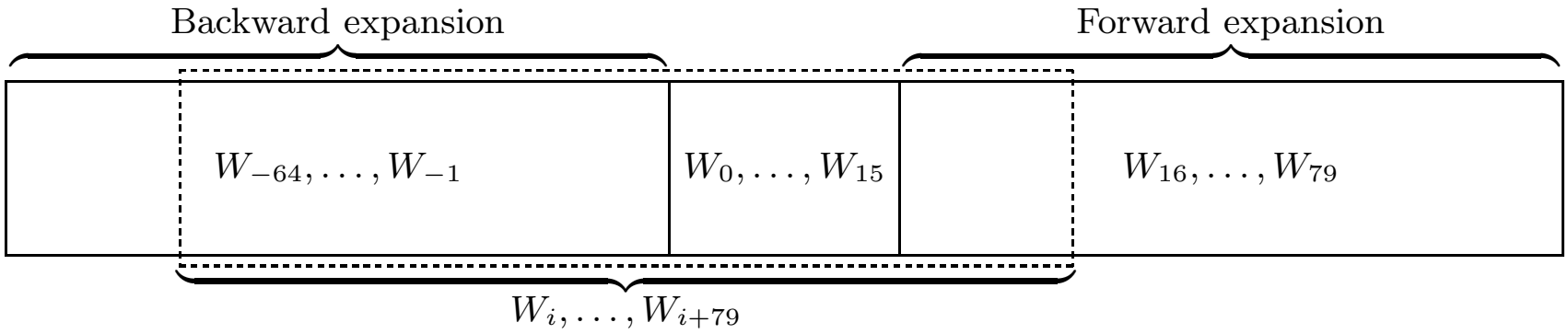
Résultats

- Recherche menée pour $pw \leq 6$
- Seulement 2 fenêtres d'information donnent les vecteurs les plus efficaces :

i	Weight 1 Information Window	Weight 3 Information Window
0	----------	----------
1	----------	o---------
2	----------	----------
3	----------	o---------
4	----------	----------
5	----------	----------
6	----------	----------
7	----------	----------
8	----------	----------
9	----------	----------
10	----------	----------
11	----------	----------
12	----------	----------
13	----------	----------
14	----------	----------
15	----------o	----------o

Relation d'équivalence

- Deux vecteurs sont équivalents si :
  - invariance par permutation circulaire des bits des mots $(W_0, \ldots, W_{79})$
  - génération à partir du même message expansé étendu



- Tous les différents vecteurs publiés réduits à 2 classes :
  - Type-I : classe du vecteur de Wang *et al.*
  - Type-II : classe du vecteur de Jutla et Patthak

Nouvelle notation

Disturbance vectors	Notation
Wang *et al.* CRYPTO 2005	
58 steps	I(43, 2)
80 steps	I(49, 2)
Rijmen & Oswald CT-RSA 2005	
*Codeword*1	I(45, 1)
*Codeword*2	I(41, 1)
*Codeword*3	I(39, 1)
Jutla & Patthak ePrint 2005	
*Codeword*1	I(52, 0)
*Codeword*2	II(52, 0)
*Codeword*3	I(51, 0)
Pramstaller *et al.* IMA 2005	I(50, 2)
De Cannière & Rechberger ASIACRYPT 2006	I(35, 2)
De Cannière *et al.* SAC 2007	II(46, 2)
Yajima *et al.* ASIACCS 2008	II(56, 2)

Plan

Probabilité de succès d'une collision locale isolée

- Moyenne de 3 expériences de 2^{20} essais

Pattern type	----------o

Bit position b	0	1	2, ..., 25	26	27,28,29	30	31
Round function	Signs	Holding probabilities $-\log_2$					
IF	+	4.87	5.00	[4.85, 4.87]	5.00	4.86	4.83	4.01
	−	4.87	5.00	[4.85, 4.87]	5.00	4.86	4.84	4.00
		(5)	(5)	(5)	(5)	(5)	(5)	(5)
XOR	+	3.68	2.00	[3.90, 3.92]	4.00	[3.90, 3.91]	3.83	3.00
	−	3.68	2.00	[3.90, 3.92]	4.00	3.91	3.83	3.00
		(4)	(2)	(4)	(4)	(4)	(4)	(3)
MAJ	+	3.91	4.00	[3.90, 3.92]	4.00	[3.90, 3.91]	3.92	4.00
	−	3.92	4.00	[3.90, 3.92]	4.00	3.91	3.91	4.00
		(4)	(4)	(4)	(4)	(4)	(4)	(3)(4)

Évaluation des vecteurs connus

Disturbance vectors	Given evaluations	Evaluation 1 $-\log_2$	Evaluation 2 $-\log_2$
Wang *et al.* CRYPTO 2005			
58 steps	2^{33} hash operations	35	35
80 steps	2^{69} hash operations	73	73
Rijmen & Oswald CT-RSA 2005			
80 steps			
*Codeword*1	-	90	90
*Codeword*2	-	97	97
*Codeword*3	-	102	102
Jutla & Patthak ePrint 2005			
80 steps			
*Codeword*1	-	70	76
*Codeword*2	-	65	69
*Codeword*3	-	71	76
Pramstaller *et al.* IMA 2005			
80 steps	-	73	73
De Cannière & Rechberger ASIACRYPT 2006			
64 steps	2^{35} hash operations	34	34
80 steps	-	94	94
De Cannière *et al.*			
70 steps	2^{44} hash operations	43	43
80 steps	-	88	88
Yajima *et al.* ASIACCS 2008			
80 steps	70 (72) CVCs	75	75

Bilan des attaques publiées

- Meilleure attaque pratique : De Cannière *et al.* SAC 2007
  - 2^{44} (70 pas) évaluations SHA-1
- Meilleure attaque théorique : Wang *et al.* CRYPTO 2005
  - $C \times 2^{69}$ évaluations SHA-1
- Évaluations théoriques fondées sur une hypothèse d'indépendance des collisions locales

Cas pathologiques connus

- Fonction de ronde IF : collision locales consécutives
  - chemin différentiel impossible
- Fonction de ronde MAJ : collision locales consécutives
  - chemin différentiel impossible sauf si directions opposées
- Compression de bit :
  - série de collisions locales réductibles à une seule collision

Collisions locales consécutives

- Moyenne de 3 expériences de 2^{24} essais

Pattern type	----------o ----------o

Bit position b	0	1	2, . . . , 24	25	26	27,28,29	30	31
Round function	Signs	Holding probabilities $-\log_2$						
XOR	$--$	5.91	4.00	[5.97, 5.98]	5.98	6.00	[5.97, 5.98]	5.91	4.00
	$-+$	5.91	4.00	[5.97, 5.98]	5.98	6.00	5.98	5.91	4.00
	$+-$	5.91	4.00	5.98	5.98	6.00	5.98	5.91	4.00
	$++$	5.91	4.00	[5.97, 5.98]	5.98	6.00	[5.97, 5.98]	5.91	4.00
		(8)	(4)	(8)	(8)	(8)	(8)	(8)	(6)
MAJ	$--$	10.01	> 24	[9.88, 9.92]	9.99	> 24	[9.91, 9.92]	9.99	> 24
	$++$	10.00	> 24	[9.88, 9.92]	10.00	> 24	[9.90, 9.91]	10.01	> 24
		(∞)	(∞)	(∞)	(∞)	(∞)	(∞)	(∞)	(∞)
	$-+$	5.98	6.00	[5.97, 5.98]	5.98	6.00	5.98	5.98	6.00
	$+-$	5.98	6.00	[5.97, 5.98]	5.98	6.00	5.98	5.98	6.00
		(8)	(8)	(8)	(8)	(8)	(8)	(8)	(8)

Collisions locales alternées

- Moyenne de 3 expériences de 2^{24} essais

Pattern type	----------o ---------- ----------o

Bit position b	0	1	2, . . . , 24	25	26	27,28,29	30	31
Round function	Signs	Holding probabilities $-\log_2$						
XOR	−−	7.36	4.00	[7.81, 7.82]	7.82	8.00	[7.81, 7.82]	7.66	6.00
	−+	7.36	4.00	[7.79, 7.80]	7.83	8.00	[7.77, 7.81]	7.66	6.00
	+−	7.35	4.00	[7.79, 7.81]	7.82	8.00	[7.78, 7.80]	7.66	6.00
	++	7.36	4.00	[7.81, 7.82]	7.82	8.00	[7.81, 7.82]	7.66	6.00
		(8)	(4)	(8)	(8)	(8)	(8)	(8)	(6)
MAJ	−−	11.88	8.00	[11.77, 11.82]	11.91	> 24	[11.80, 11.82]	11.91	> 24
	++	11.91	7.99	[11.79, 11.82]	11.90	> 24	[11.81, 11.82]	11.91	> 24
	+−	11.89	> 24	[11.58, 11.62]	11.90	> 24	[11.60, 11.63]	11.93	8.00
	−+	11.92	> 24	[11.58, 11.63]	11.90	> 24	[11.58, 11.63]	11.89	8.00
		(8)	(8)	(8)	(8)	(8)	(8)	(8)	(8)

Indépendance des collisions locales

- Collisions locales consécutives :
  - probabilités mesurées globalement meilleures
  - cas pathologique MAJ seulement sur les positions 1, 26 et 31
- Collisions locales alternées :
  - apparition de nouveaux cas pathologiques inconnus
  - probabilités mesurées légèrement meilleures pour le XOR
  - probabilités mesurées nettement moins bonnes pour le MAJ
- Hypothèse d'indépendance fausse dans de nombreux cas

Plan

Conclusion

- Nouvel algorithme :
  - fondé sur un compromis différent
  - indépendant de la fonction d'évaluation
  - nouvelle classification des vecteurs de perturbations
- Étude statistique du comportement des collisions locales
  - hypothèse d'indépendance fausse dans certains cas
  - apparition de nouveaux cas pathologiques
  - écarts entre probabilités mesurées et probabilités théoriques
- Bilan :
  - pour 70 pas : attaques pratiques inadaptées pour 80 pas
  - pour 80 pas : attaques théoriques remises en cause

Perspectives

- Mesurer les probabilités des différents patrons présents dans les 2 classes de vecteurs connus
- Évaluer les vecteurs publiés sur ces nouvelles bases
- Rechercher de nouveaux vecteurs de perturbations avec de nouveaux critères