Study the function of building blocks in SHA Family

A.Arun Lawrence selvakumar, Dr.R.S.Ratastogi, Member IAENG

Abstract: In this paper we analyse the role of some of the building blocks in SHA-256. We show that the disturbance correction strategy is applicable to the SHA-256 architecture and we prove that functions Σ, σ are vital for the security of SHA-256 by showing that for a variant without them it is possible to find collisions with complexity $2^n$ hash operations. As a step towards an analysis of the full function, we present the results of our experiments on Hamming weights of expanded messages for different variants of the message expansion and show that there exist low-weight expanded messages for XOR-linearised variants.

I. INTRODUCTION

Recent results on the practical cryptanalysis of many hash functions from the MD family, including MD4, MD5 [WLF05, WY05] as well as SHA-0 and SHA-1 [BCJ05, RO05, WY05b, WY05a], drew a considerable attention to the security of hash functions and raised some questions about the security of the latest function in this family, namely SHA-256. The first published independent analysis of the members of the SHA-2 family was done by Gilbert and Handschuh [GH03]. They showed how to increase the probability to $2^{-66}$ Later on, this result has been improved by Hawkes, Paddon and Rose [HPR04]. They showed how to increase the probability to $2^{-39}$ using modular differences.

In this paper we investigate the limits of applying the disturbance-correction strategy that was introduced by Chabaud and Joux [CJ98] to cryptanalyse SHA-0. We demonstrate the importance of the S-boxes applied in SHA-256. Throughout this paper, we use different linearisation models, namely a linearisation with respect to the XOR-operation (XOR-linear) and a linearisation with respect to modular addition (ADD-linear). We start from the analysis of an ADD-linear variant of SHA-256 and derive a differential characteristic that produces collisions for that linear model. Next, we present a zero-output differential characteristic with probability $2^{-64}$ for the hash function with the Boolean functions. This proves that the application of the functions $\Sigma_0$, $\Sigma_1$, $\sigma_0$, and $\sigma_1$ is crucial for the security of the original hash function, since they are replaced by the identity function in this analysis. In parallel to this work, a different variant of SHA-256 was analysed by Yoshida and Biryukov [YB05].

A better understanding of the impact of these functions on the whole design is the next step in the analysis of SHA-256. While the influence of $\Sigma_0$ and $\Sigma_1$ on the probability of single correction has been studied well by Hawkes et al. [HPR04], as far as [GH03]

They know, there has been no analysis of the message expansion involving $\sigma_0$ and $\sigma_1$. In this paper we discuss some properties of the message expansion and present our results of the search for low-weight message differences for various (XOR-linear) variants of the message expansion.

II. DESCRIPTION OF SHA-256

SHA-256 [Nat02] is an iterated cryptographic hash function based on a compression function that updates the state of eight 32-bit chaining variables $A...H$ according to the values of 16 32-bit words $M_i...M_{i+512}$ of the message. The compression function consists of 64 identical steps presented in Figure 1. The step transformation employs bitwise Boolean functions

$$Maj (A,B,C) = (A\&B)\lor (A\&C)\lor (B\&C)$$

$$Ch (E,F,G) = (E\&F)\lor (\neg E\&G),$$

and two S-boxes

$$\Sigma_0(x) = ROT R^\Sigma_0(x) \oplus ROT R^{\Sigma_1}(x) \oplus ROT R^{-\Sigma_2}(x),$$

$$\Sigma_1(x) = ROT R^\Sigma_0(x) \oplus ROT R^{\Sigma_1}(x) \oplus ROT R^{\Sigma_2}(x),$$

built from word rotations to the right (ROT R) and bitwise XORs denoted by $\oplus$. The $i$-th step uses a fixed constant $K_i$ and the $i$-th word $W_i$ of the expanded message.

The message expansion works as follows. An input message is split into 512-bit message blocks (after padding). A single message block will be denoted either as a row vector $m \in Z_2^{32}$ or as a vector $M_i \in Z_2^{512}$. The words $W_i$ are generated from the initial message $M$ according to the following formula:

$$W_i = \begin{cases} M_i & \text{for } 0 \leq i < 16 \\ \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16} & \text{for } 16 \leq i < N \end{cases}$$

Figure 1: One step of the SHA-256 compression function
If we set \( N = 64 \), we get standard SHA-256, taking a different value of \( N \) results in a reduced (or extended) variant of it. The functions \( \sigma_i(x) = \text{ROTR}_7^i(x) \oplus \text{ROTR}^{17}_i(x) \oplus \text{SHR}^{10}_i(x) \) and \( \sigma_i(x) = \text{ROTR}^{13}_i(x) \oplus \text{ROTR}^{0}_i(x) \oplus \text{SHR}^{10}_i(x) \) are S-boxes defined using word rotations to the right (\text{ROTR}) and shifts to the right (\text{SHR}).

III. COMPUTING COLLISIONS FOR AN ADD-LINEAR VARIANT OF SHA-256

In order to analyse the usefulness of a disturbance-correction strategy applied to the SHA-2 architecture, we investigate an DD-linear variant of SHA-256, where S-boxes are replaced with the identity function, act which will be used later on.

Let us denote by \( \text{Delay}^a \) the next 8 words the following sequence of corrections with respect to the modular addition. If we introduce a difference \( \Delta \) to the part of a sequence following the recurrence relation, also follows the relation.

Let \( W \in \mathbb{Z}^{32} \). If \( \Delta_i \) is a result of the expansion using the recursive formula (1) with \( N = 64 + a \), then all the vectors \( \Delta_i \) are also results of the expansion process (1).

PROOF: Each vector \( \Delta_i \) consists of elements of the part of a sequence following the recurrence relation, also follows the relation.

Where \( I \), stands for the identity matrix and \( A \) denotes a matrix of the linear transformation producing 16 new words out of 16 old ones according to the recurrence relation (1). The following theorem fully characterises disturbance patterns for an ADD-linear variant of SHA-256.

THEOREM III.B

Let \( \Delta_i = M \cdot \Delta \) be a message difference. The expanded difference \( \Delta = E(\Delta_i) \) is a valid disturbance vector for an ADD–linear variant of SHA-256 if the following conditions are satisfied:

\[
0 = \Lambda \cdot \Delta, \\
0 = \Lambda \cdot \Delta = E(\Delta_i),
\]

where \( M[a::b] \) means a matrix consisting of rows of the matrix \( M \) from the a-th row to the b-th row inclusive.

PROOF. The fundamental observation is that each single word \( \Delta_i \) of the disturbance vector has to be corrected by adding to the next 8 words the following differences defined by Equation (4),

\[
\{ -4\Delta, 2\Delta, 2\Delta, 4\Delta, 2\Delta, 0, -\Delta \}
\]

This shows that the last non-zero disturbance word may appear in position 55, because we need eight steps 56,...,63 to correct it. Thus, the last 8 words of the expanded difference \( E(\Delta_i) \) have to be zero. Since \( E \) is defined by (5), this condition can be written as (6).

Now, let us consider the following linear combination of \( \Delta_i \) and its delayed versions

\[
\text{C} = \Delta_i - 4 \text{Delay}_i(\Delta) + 2 \text{Delay}_i(\Delta) + 2 \text{Delay}_i(\Delta) + 4 \text{Delay}_i(\Delta) + 2 \text{Delay}_i(\Delta) + \text{Delay}_i(\Delta) - \text{Delay}_i(\Delta)
\]

It is easy to see that each disturbance word \( \Delta_i \) in \( C \) is corrected by its appropriate multiplicities appearing in the next eight positions and coming from the delayed vectors.
Since the message expansion is linear, C is the result of the expansion if and only if all the delayed and truncated vectors Delay \(\Delta(\Lambda)\), \(0 \leq b \leq 8\) are results of the expansion process.

**LEMMA3.1**

Assures that it is true if Delay \(\Delta(\Lambda)\) is the result of the (extended, \(N=68\)) expansion process. We can achieve this by taking the first 16 words and expanding them forward according to Equation (1), but also by taking any 16 consecutive words and expanding partly forward and partly backward. In our case we select elements 8–23 for the expansion.

If we index elements of Delay \(\Delta(\Lambda)\) starting from -8 and split the vector into two parts: one having negative and the other one having non-negative indices, we can express this requirement equivalently by the following two conditions:

\[
\begin{align*}
&\text{If we multiply the basic pattern (9) by 8 \(\left(\text{so shift it left by 3 bit positions}\right)\), we get a disturbance pattern} \\
&\text{that not only follows the (extended, \(N=68\)) expansion process. We can} \\
&\text{achieve this by taking the first 16 words and expanding them} \\
&\text{partly forward and partly backward, but with both Boolean} \\
&\text{functions M} \text{aj and Ch in place. If we} \\
&\text{delay delayed disturbance patterns multiplied by corresponding coefficients of Equation (11), i.e.} \\
&\{0,0,\Delta,\Delta,0,0,0,\Delta\}, \\
&\text{we use this approximation and trace how a single bit disturbance} \\
&\text{\(\Delta_8\), introduced in step} \text{i \text{propagates through the} \\
&\text{next 8 steps, we get the following sequence of corrections:} \\
&\{0,0,\Delta,\Delta,0,0,0,\Delta\}. \\
&\text{We can approximate both Boolean functions with probability at least} \frac{1}{2} \text{assuming that the function produces an output difference} \\
each time the input difference is non-zero. This approximation is shown in Table 2.}
\end{align*}
\]

**Table 2: Probabilities of non-zero output differences for the Boolean functions Ch and M aj**

| Input difference | Ch function | Maj function | Conditions | Prob | Conditions | Prob |
|------------------|-------------|--------------|------------|------|------------|------|
| \((c_1,\delta_y,\theta_1)\) | \(y + z = 1\) | \(y + z = 1\) | \(1/2\) | \(y + z = 1\) | \(1/2\) |
| \((0,0,1)\) | \(x = 1\) | \(x + z = 1\) | \(1/2\) | \(x + y = 1\) | \(1/2\) |
| \((0,1,0)\) | \(x = 0\) | \(y + z = 0\) | \(1/2\) | \(x + y = 0\) | \(1/2\) |
| \((1,0,0)\) | \(x + y = 0\) | \(x + z = 0\) | \(1/2\) | \(x + z = 1\) | \(1/2\) |
| \((0,1,1)\) | \(y + z = 0\) | \(-\) | \(1/2\) | \(-\) | \(1/2\) |

This time however, correction process is probabilistic as each active Boolean function almost always (except for input differences \(0,1,1\) for Ch and \((1,1,1)\) for M aj) introduces a factor of \(1/2\). A detailed analysis of these probabilities is presented in Table 3.

After multiplication of all factors, we obtain a probability for a successful correction equal to \(2^{-84}\). Further optimisation are also possible as we can choose messages in such a way that conditions for successful correction will be always satisfied for the first 16 steps, what could increase the probability to around \(2^{-64}\). This shows that the use of substitution boxes \(\sigma_0, \sigma_1, \Sigma_0, \Sigma_1\) is essential for the security of SHA-256 and also demonstrates that mixing only modular additions with Boolean functions is not enough for constructing a secure hash function.
V. The role of S-boxes

The substitution boxes $\Sigma_0$ and $\Sigma_1$ constitute the essential part of the hash function and fulfil two tasks: they add bit diffusion and destroy the ADD-linearity of the function.

There are modular differentials for $\Sigma_0$ and $\Sigma_1$ that hold for one bit input difference $e$ with probability $2^{-3}$ (necessary for S-boxes used in steps $i$ and $i + 5$ and with probability around $2^{-10}$ for input difference equal to $\Sigma_0(e)$ (used for $\Sigma_1$ at step $i + 2$), using the approach of modular differences it is possible to obtain a corrective pattern for the complete round structure with probability around $2^{-42}$. A better result of $2^{-39}$ was obtained by Hawkes et al. [HPR04] by explicit computation of modular differences for $\Sigma_0$ and $\Sigma_1$, rather than approximating them with a constant differential.

The S-boxes $\sigma_0$ and $\sigma_1$ play a similar role: they provide non-linearity and better diffusion for the message expansion.

These two properties of the message expansion constitute the foundation of the security of the full SHA-256, as in order to apply corrective patterns in a straightforward way, one would need at least $37$ expanded words equal to zero (since at most three corrective patterns can be applied). Although this seems to be unlikely, further research is needed in this direction. In the rest of this section, we concentrate on the message expansion and list some interesting properties of it:

- $\sigma_0$ and $\sigma_1$ have both the property to increase the hamming weight of low-weight inputs. This increase is upper bounded by a factor of 3. The average increase if Hamming weight for low-weight inputs is even higher if three rotations are used instead of two rotations and one bit-shift. However, a reason for this bit-shift is given by the next observation.

- In contrast to all other members of the MD4-family including SHA-1, rotating expanded message words to get new expanded message words is not possible anymore (even in the XOR-linearised case). This is due to the bit-shift being used in $\sigma_0$ and $\sigma_1$.

VI. Finding low-weight code words in the code describing the XOR-linearised SHA-256 message expansion

In the first attempt to get an idea about the effect of all the changes between the SHA-1 message expansion and the SHA-256 message expansion, we consider single bit differences. Table 4 illustrates this comparison. We consider variants reduced to 40 steps as well as full variants (80 steps for SHA-1 variants and 64 steps for SHA-256 variants).

By the modified SHA-1 message expansion we refer to a variant where every XOR is replaced by an addition modulo 2. By the modified SHA-256 message expansion, we refer to a variant where every addition is replaced by an XOR. We observe that both the introduction of modular additions and the replacement of a single bit-shift by a structure

|    | orig SHA-1 | mod. SHA-1 | mod. SHA-256 | orig. SHA-256 |
|----|------------|------------|--------------|--------------|
| min (40 steps) | 28 | 18 | 10 | 13 |
| max (40 steps) | 30 | 41 | 297 | 307 |
| min (full) | 107 | 247 | 467 | 507 |
| max (full) | 174 | 354 | 694 | 709 |

Table 4: Comparison of the number of affected bits for a single bit difference in various message expansions. In variants using modular addition, we used the all-zero vector as a starting point. Using $\sigma_0$ and $\sigma_1$ heavily increases the number of affected bits in the expanded message.

When talking about the SHA-1 message expansion, it was already observed in the works [MP05, RO05] that weights much smaller than 107 (as given in Table 4) can be found. The minimum weight found for the message expansion of SHA-1 is 44. A more recent treatment of low-weight disturbance patterns in SHA-1 can be found in [JP05].

Due to the nonlinear behaviour of the modular addition, no linear code can describe the SHA-256 message expansion. However, if the modular addition is replaced by XOR, a linear code over $\mathbb{Z}_2$ can be constructed. If we consider SHA-256 with $N$ steps, this code can be represented by a $512 \times 32N$ generator matrix $G$.

Due to the XOR-linearisation, every possible difference of two expanded words is also a valid word in this code. Therefore, probabilistic algorithms from coding theory [Leo88, Ste89, CC98] can be used to find low-weight differences for the XOR-linearised SHA-256 message expansion. Some results of this codeword search are depicted in Figure 2. All minimum weights found for variants of the message expansion up to the full 64 steps are shown in the figure. Until the 42-step variant, our algorithms found reasonable low weights. This is depicted by the solid line. Considering the 40-step variant, the weight of 26 is low compared to a minimal weight of 110 for single-bit differences given in Table 4. The 40-step expanded message is given in Table 5.

For variants with more than 42 steps, the running time of our algorithms is currently too high to return reasonable low weights. The sudden jump after step 42 is not an intrinsic property of the SHA-256 message expansion, but rather the result of the limited running time of our algorithms.

To show that there indeed are low-weight words for $N > 42$, we proceed as follows. After obtaining a low-weight word for 42 steps we use the expansion process to extend it to the full length word. Weights obtained in this way are depicted by the dashed line.

A 42-step word of weight 35 is used there as a starting point. Expanding it to 64 steps gives us a weight of 356. This is considerable lower than 467, which is the minimal weight given for a single bit difference in Table 4.

However, there is room for improvements.
In contrast to the words found for the SHA-1 message expansion, there are no zero bands \cite{RO05} any more. Note that the given expanded message is not necessarily a valid difference in case of the real message expansion since we approximate the modular addition by the bitwise XOR operation. Also note that the given vector cannot directly be used as a collision-producing disturbance pattern as described by Chabaud and Joux in their original attack on SHA-0 \cite{CJ98}. The reason is that there are \textit{truncated local collisions} \cite{CJ98} generated by non-zero words in the backward expansion. These local collisions start before step 0 and would cause additional difficulties for constructing a collision-producing differential characteristic. However, we expect to find input words for reduced variants of the message expansion that can be used to build a collision-producing difference.

A number of conditions on chaining variables need to be satisfied in order to ensure that the concatenation of local collisions (which hold with a probability between $2^{-39}$ and $2^{-42}$, results in a collision of the output of the compression function. If we do not assume any pre-fulfilled conditions, the maximal weight we allow for a perturbation pattern is 3 (since $2^{-39} \times 2^{-128}$. Considering the weights in Figure 2, this would mean a maximum of 24 steps.

VII CONCLUSIONS

In this paper we presented methods for finding collisions for two simplified variants of SHA-256, one fully linearised with respect to the modular addition and the other one with all the S-Boxes replaced by the identity function. These results show that the presence of S-Boxes is essential for the security of SHA-256. We studied properties of the message expansion and presented expanded messages with low Hamming weights for the XOR-linearised message expansion of SHA-256. The general ideas of all these results apply also to other members of the SHA-2 family.

REFERENCES

1. [BCJ05] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby. Collisions of SHA-0 and Reduced SHA-1. In Ronald Cramer, editor, \textit{Advances in Cryptology– EUROCRYPT’05}, volume 3494, pages 36–57. Springer, 2005.
2. [CC98] Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to McEliece’s cryptosystem and to narrow-sense BCH codes of length 511. \textit{IEEE Transactions on Information Theory}, 44(1):367–378, 1998.
3. [CJ98] Florent Chabaud and Antoine Joux. Differential Collisions in SHA-0. In Hugo Krawczyk, editor, \textit{Advances in Cryptology-CRYPTO’98}, volume 1462 of LNCS, pages 56–71. Springer, 1998.
4. [GH03] Henri Gilbert, Helena Handschuh. Security Analysis of SHA-256 and Sisters. In Mitsuru Matsumi and Robert Zuccherato, editors, \textit{Selected Areas in Cryptography, 10th Annual International Workshop, SAC 2003, Ottawa, Canada, August 14-15, 2003. Revised Papers}, volume 3006 of \textit{Lecture Notes in Computer Science}, pages 175–193. Springer, 2003.
5. [HPR04] Philip Hawkes, Michael Paddon, and Gregory G. Rose. On Corrective Patterns for the SHA-2 Family. Cryptology ePrint Archive, Report 2004/207, August 2004. http://eprint.iacr.org/.
6. [JP05] Charanjit S. Jutla and Anindya C. Patthak. A Matching Lower Bound on the Minimum Weight of SHA-1 Expansion Code. Cryptology ePrint Archive, Report 2005/266, 2005 http://eprint.iacr.org/.
7. [Leo88] Jeffrey S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. \textit{IEEE Transactions on Information Theory}, 34(5):1354–1359, 1988.
8. [MP05] Krystian Matusiewicz and Josef Pieprzyk. Finding Good Differential Patterns for Attacks on SHA-1. In \textit{Proc. International Workshop on Coding and Cryptography, WCC’2005, LNCS, 2005}. To appear.
9. [Nat02] National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS 180-2, August 2002.
10. [PRR05] Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen. Exploiting Coding Theory for Collision Attacks on SHA-1. In Nigel P. Smart, editor, \textit{Cryptography and Coding, 10th IMA International Conference, Cirencester UK, December 19-21, 2005 Proceedings}, volume 3796 of LNCS, pages 78–95. Springer, 2005.
[11] [RO05] Vincent Rijmen and Elisabeth Oswald. Update on SHA-1. In Alfred Menezes, editor, *Topics in Cryptology CT RSA 2005*, volume 3376 of *LNCS*, pages 58–71. Springer, Feb 2005.

[12] [Ste89] Jacques Stern. A method for finding codewords of small weight. In G. Cohen and J. Wolfmann, editors, *Coding Theory and Applications, 3rd International Colloquium*, volume 388 of *Lecture Notes in Computer Science*, pages 106–113. Springer, 1989.

[13] [WLF05] Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu. Cryptanalysis of the Hash Functions MD4 and RIPEMD. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT'05*, volume 3494 of *LNCS*, pages 1–18. Springer, 2005.

[14] [WY05] Xiaoyun Wang and Hongbo Yu. How to break MD5 and other hash functions. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT'05*, volume 3494 of *LNCS*, pages 19–35. Springer, 2005.

[15] [WYY05a] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding Collisions in the Full SHA-1. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *LNCS*, pages 17–36. Springer, 2005.

[16] [WYY05b] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient Collision Search Attacks on SHA-0. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *LNCS*, pages 1–16. Springer, 2005.

[17] [YB05] Hirotaka Yoshida and Alex Biryukov. Analysis of a SHA-256 variant. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography, 12th Annual International Workshop, SAC 2005, Kingston, Ontario, Canada, August 11-12, 2005, Proceedings to appear, LNCS*. Springer, 2005.

A. Arul Lawrence Selvakumar received the M.E., M.S. degrees in Computer Science & Engineering from Bharathidasan University, INDIA and pursuing his Ph.D., in cryptography. He is currently working as a Professor in the Dept / CSE at Royal College of Engineering & Technology, Thrissur, Kerala, India. He is member of various professional societies like CSTA, IAENG, and IACSIT. He has published more than 26 papers in international journals and conference and also published 2 books in network security. He has attended more than 9 workshops, symposia, seminars and short-term training programmes. His research interest includes network security, cryptography and client server computing.