**SCIENCE CHINA**
Information Sciences

• **Supplementary File** •

# Improved linear (hull) cryptanalysis of round-reduced versions of SIMON

SHI Danping[1,2,3], HU Lei[1,2*], SUN Siwei[1,2], SONG Ling[1,2], QIAO Kexin[1,2] & MA Xiaoshuang[1,2]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering,*
*Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Data Assurance and Communication Security Research Center,*
*Chinese Academy of Sciences, Beijing* 100093*, China;*
[3]*University of Chinese Academy of Sciences, Beijing* 100093*, China*

## Appendix A Introduction

The previous best linear characteristic that we are aware of for a key-recovery attack on SIMON128 is a 34-round linear characteristic with correlation $2^{-63}$, as shown in [1]. Here we present one with correlation $2^{-61}$. The 34-round linear characteristic can be used to mount a linear attack with a success rate of 99.7% with an 8-bit advantage on round-reduced SIMON by use of the method presented in [2]. In addition, the *potential* of the linear hulls we found on 13-round SIMON32, 15-round SIMON48, and 21- and 22-round SIMON64 are $2^{-28.99}$, $2^{-42.28}$, $2^{-60.72}$, and $2^{-63.83}$, respectively, while the *potential* of the previous best linear hulls for these versions are $2^{-31.69}$, $2^{-44.11}$, and $2^{-62.53}$, proposed in [1]. Using the 21-round linear hull, we present a 29-round key-recovery attack on SIMON64/128. The previous best cryptanalysis of this version was a 28-round differential cryptanalysis [1, 3].

For each linear characteristic, we obtain an accurate absolute value for the correlation of the linear approximation for each round by use of the nonsingular transform method presented in the main letter. Once the correlation in each round has been determined, the piling-up lemma is applied to obtain the absolute value of the correlation of the whole cipher, because S-boxes from different rounds can be seen as independent,given the effect of the round keys.

## Appendix A.1 Linear characteristics

We performed experiments on SIMON128. A 34-round linear characteristic with correlation $2^{-61}$ was found. The linear mask (separated into left and right parts) is presented in Tables A1 and A2. To the best of our knowledge, the previous best 34-round characteristic of SIMON128 was presented in [1], with a correlation of $2^{-63}$. A 43-round linear attack is presented with the 34-round linear characteristic in Figure A1, where 60 of the numbered subkey bits need to be guessed and the underlined ones shown in red do not..

The probability of success with an 8-bit advantage can be estimated using the method presented in [2] as follows:

$$P_s = \Phi(2\sqrt{N}\,|p - \tfrac{1}{2}| - \Phi^{-1}(1 - 2^{-8-1})), \tag{A1}$$

where $N$ is the number of known plaintexts, $|p - \frac{1}{2}| = \epsilon/2$, $\epsilon$ is the correlation, and $\Phi$ is the normal distribution. If we choose $N = 2^{127}$, the success probability is 99.7%. The previous best result achieving this probability is a 33-round characteristic with correlation $2^{-59}$ in [1].

For SIMON64, an 18-round linear characteristic with correlation $2^{-31}$ is listed in Table A3. The previous best linear characteristic with absolute value of the correlation no less than $2^{-31}$ is a 17-round linear characteristic with correlation $2^{-28}$ presented in [1]. For SIMON32 and SIMON48, similar results are found. Characteristics for SIMON32 and SIMON48 are listed in Tables A4 and A5. A comparison between our results and those of [1] is provided in Table A6. Examining the dependences among S-boxes is the primary focus of this letter.

[*] Corresponding author (email: hu@is.ac.cn)

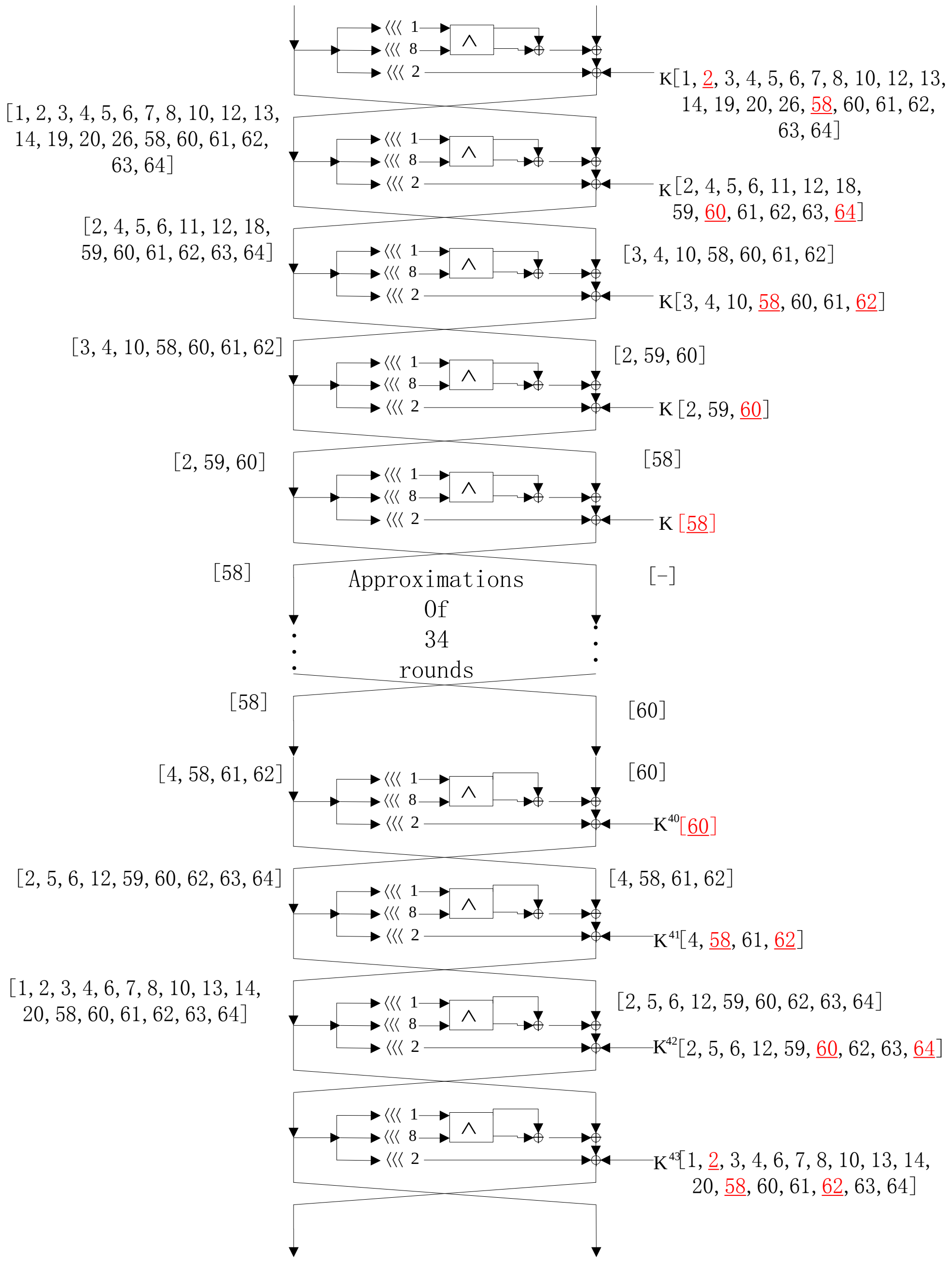

**Figure A1** Linear cryptanalysis of SIMON128/192,

**Table A1** Left mask of the 34-round linear characteristic for SIMON128

| Rounds | The input linear mask of the left half |
|---|---|
| 1 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 2 | 0000000000000000000000000000000000000000000000000000000000000000 |
| 3 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 4 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 5 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 6 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 7 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 8 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 9 | 0100110000000000000000000000000000000000000000000000000001000000 |
| 10 | 0110001000000000000000000000000000000000000000000000000000000000 |
| 11 | 0100010000000000000000000000000000000000000000000000000001000000 |
| 12 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 13 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 14 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 15 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 16 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 17 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 18 | 0000000000000000000000000000000000000000000000000000000000000000 |
| 19 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 20 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 21 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 22 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 23 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 24 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 25 | 0100010000000000000000000000000000000000000000000000000001000000 |
| 26 | 0110001000000000000000000000000000000000000000000000000000000000 |
| 27 | 0100110000000000000000000000000000000000000000000000000001000000 |
| 28 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 29 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 30 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 31 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 32 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 33 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 34 | 0000000000000000000000000000000000000000000000000000000000000000 |
| 35 | 0000000000000000000000000000000000000000000000000000000001000000 |

**Table A2** Right mask of the 34-round linear characteristic for SIMON128

| Rounds | The input linear mask of the right half |
|---|---|
| 1 | 0000000000000000000000000000000000000000000000000000000000000000 |
| 2 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 3 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 4 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 5 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 6 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 7 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 8 | 0100110000000000000000000000000000000000000000000000000001000000 |
| 9 | 0110001000000000000000000000000000000000000000000000000000000000 |
| 10 | 0100010000000000000000000000000000000000000000000000000001000000 |
| 11 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 12 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 13 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 14 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 15 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 16 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 17 | 0000000000000000000000000000000000000000000000000000000000000000 |
| 18 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 19 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 20 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 21 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 22 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 23 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 24 | 0100010000000000000000000000000000000000000000000000000001000000 |
| 25 | 0110001000000000000000000000000000000000000000000000000000000000 |
| 26 | 0100110000000000000000000000000000000000000000000000000001000000 |
| 27 | 0001000000000000000000000000000000000000000000000000000000010000 |
| 28 | 0100000000000000000000000000000000000000000000000000000001000100 |
| 29 | 0000000000000000000000000000000000000000000000000000000000000001 |
| 30 | 0000000000000000000000000000000000000000000000000000000001000100 |
| 31 | 0000000000000000000000000000000000000000000000000000000000010000 |
| 32 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 33 | 0000000000000000000000000000000000000000000000000000000000000000 |
| 34 | 0000000000000000000000000000000000000000000000000000000001000000 |
| 35 | 0000000000000000000000000000000000000000000000000000000000010000 |

**Table A3** Input mask of the 18-round linear characteristic for SIMON64

| Rounds | The left half | The right half |
|---|---|---|
| 1 | 10000000000000000000000000000000 | 00000000000000000000000000000010 |
| 2 | 00000000000000000000000000000010 | 00000000000000000000000000000000 |
| 3 | 00000000000000000000000000000000 | 00000000000000000000000000000010 |
| 4 | 00000000000000000000000000000010 | 10000000000000000000000000000000 |
| 5 | 10000000000000000000000000000000 | 00100000000000000000000000000010 |
| 6 | 00100000000000000000000000000010 | 00001000000000000000000000000000 |
| 7 | 00001000000000000000000000000000 | 00100010000000000000000000000010 |
| 8 | 00100010000000000000000000000010 | 10000000100000000000000000000000 |
| 9 | 10000000100000000000000000000000 | 00000010011000000000000000000010 |
| 10 | 00000010011000000000000000000010 | 00000011000010000000000000000000 |
| 11 | 00000011000010000000000000000000 | 00000010001000000000000000000010 |
| 12 | 00000010001000000000000000000010 | 10000000100000000000000000000000 |
| 13 | 10000000100000000000000000000000 | 00100010000000000000000000000010 |
| 14 | 00100010000000000000000000000010 | 00001000000000000000000000000000 |
| 15 | 00001000000000000000000000000000 | 00100000000000000000000000000010 |
| 16 | 00100000000000000000000000000010 | 10000000000000000000000000000000 |
| 17 | 10000000000000000000000000000000 | 00000000000000000000000000000010 |
| 18 | 00000000000000000000000000000010 | 00000000000000000000000000000000 |
| 19 | 00000000000000000000000000000000 | 00000000000000000000000000000010 |

**Table A4** Input mask of the 11-round linear characteristic for SIMON32

| Rounds | The left half | The right half |
|---|---|---|
| 1 | 0100010001000000 | 0001000000010000 |
| 2 | 0001000000010000 | 0100000001000100 |
| 3 | 0100000001000100 | 0000000000000001 |
| 4 | 0000000000000001 | 0000000001000100 |
| 5 | 0000000001000100 | 0000000000010000 |
| 6 | 0000000000010000 | 0000000001000000 |
| 7 | 0000000001000000 | 0000000000000000 |
| 8 | 0000000000000000 | 0000000001000000 |
| 9 | 0000000001000000 | 0000000000010000 |
| 10 | 0000000000010000 | 0000000001000100 |
| 11 | 0000000001000100 | 0000000000000001 |
| 12 | 0000000000000001 | 0100000001000100 |

## Appendix A.2 Linear hull

Nyberg defined the *potential* of a linear hull with the input and output masks $\alpha$ and $\beta$ for a block cipher $C = f(P, K)$ in [4] as follows:

$$\mathrm{ALH}(\alpha, \beta) = \sum_{\gamma} (\Pr(\alpha P + \beta C + \gamma K = 0) - \frac{1}{2})^2. \tag{A2}$$

By setting the input and output masks shown as in Table A7 with the added constraint $\sum_r \sum_{j=1}^{n} V^r[j] \leqslant 48$, we find a 13-round linear hull with *potential* $2^{-28.99}$ for SIMON32. To our knowledge, the best previous result for SIMON32 was a 13-round linear hull presented in [1] with *potential* $2^{-31.69}$. Our model returns 412,206 linear characteristics, of which only 196,474 have nonzero correlation; the others are zero as a result of the dependence of active S-boxes. Furthermore, this hull can be used to attack 21-round SIMON32/64, as Figure A2 shows. The number of bits needed to be guessed for the key is 32.

A 15-round linear hull with *potential* $2^{-42.28}$ for SIMON48 is obtained by setting the input and output masks as in Table A7 with the additional constraint $\sum_r \sum_{j=1}^{n} V^r[j] \leqslant 59$. The previous best linear hull for SIMON48 that we are aware of is the 15-round hull presented in [1], with *potential* $2^{-44.11}$. Our method returns, 50,432 linear characteristics, of which only 43,524 are valid. This linear hull can be used to mount an attack on 21-round SIMON48/96, as shown in Figure A3. The number of guessed bits for the key is 51.

A 21-round linear hull with *potential* $2^{-60.72}$ for SIMON64 was obtained, whereas the previous best result for this version is a 21-round linear hull with *potential* $2^{-62.53}$ [1]. Among the 115,199 linear characteristics found with the

**Table A5** Input mask of the 14-round linear characteristic for SIMON48

| Rounds | The left half | The right half |
|---|---|---|
| 1 | 000000000100000001000000000000000000000000000000 | 000000010001000100000000000000000000000000000000 |
| 2 | 000000010001000100000000000000000000000000000000 | 000000000000010000000000000000000000000000000000 |
| 3 | 000000000000010000000000000000000000000000000000 | 000000010001000000000000000000000000000000000000 |
| 4 | 000000010001000000000000000000000000000000000000 | 000000000100000000000000000000000000000000000000 |
| 5 | 000000000100000000000000000000000000000000000000 | 000000010000000000000000000000000000000000000000 |
| 6 | 000000010000000000000000000000000000000000000000 | 000000000000000000000000000000000000000000000000 |
| 7 | 000000000000000000000000000000000000000000000000 | 000000010000000000000000000000000000000000000000 |
| 8 | 000000010000000000000000000000000000000000000000 | 000000000100000000000000000000000000000000000000 |
| 9 | 000000000100000000000000000000000000000000000000 | 000000010001000000000000000000000000000000000000 |
| 10 | 000000010001000000000000000000000000000000000000 | 000000000000010000000000000000000000000000000000 |
| 11 | 000000000000010000000000000000000000000000000000 | 000000010001000100000000000000000000000000000000 |
| 12 | 000000010001000100000000000000000000000000000000 | 000000000100000001000000000000000000000000000000 |
| 13 | 000000000100000001000000000000000000000000000000 | 000000010000000100010000000000000000000000000000 |
| 14 | 000000010000000100010000000000000000000000000000 | 000000000000000000000100000000000000000000000000 |
| 15 | 000000000000000000000100000000000000000000000000 | 000000010000000100010001000000000000000000000000 |

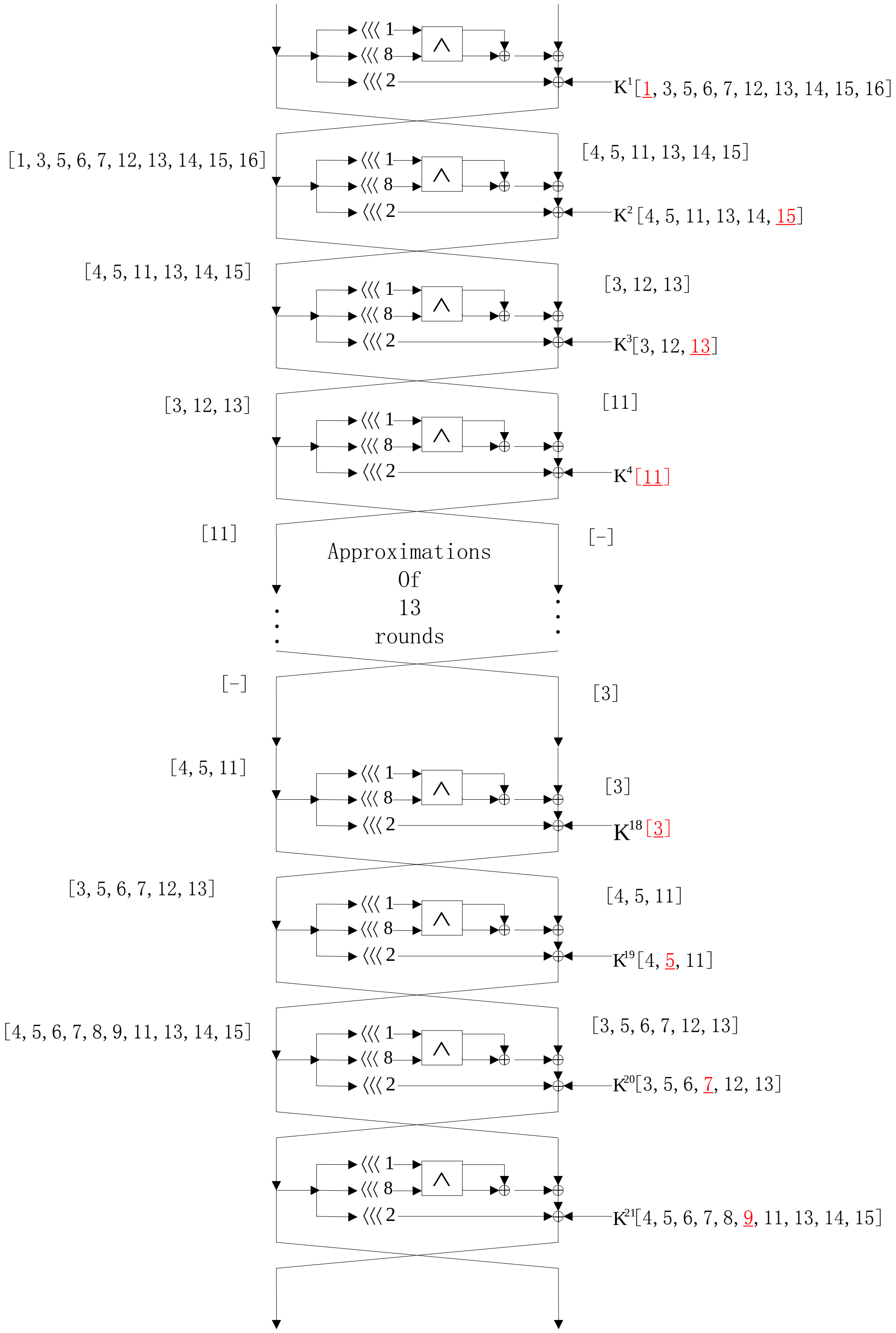

**Figure A2** Linear hull cryptanalysis of SIMON32/62

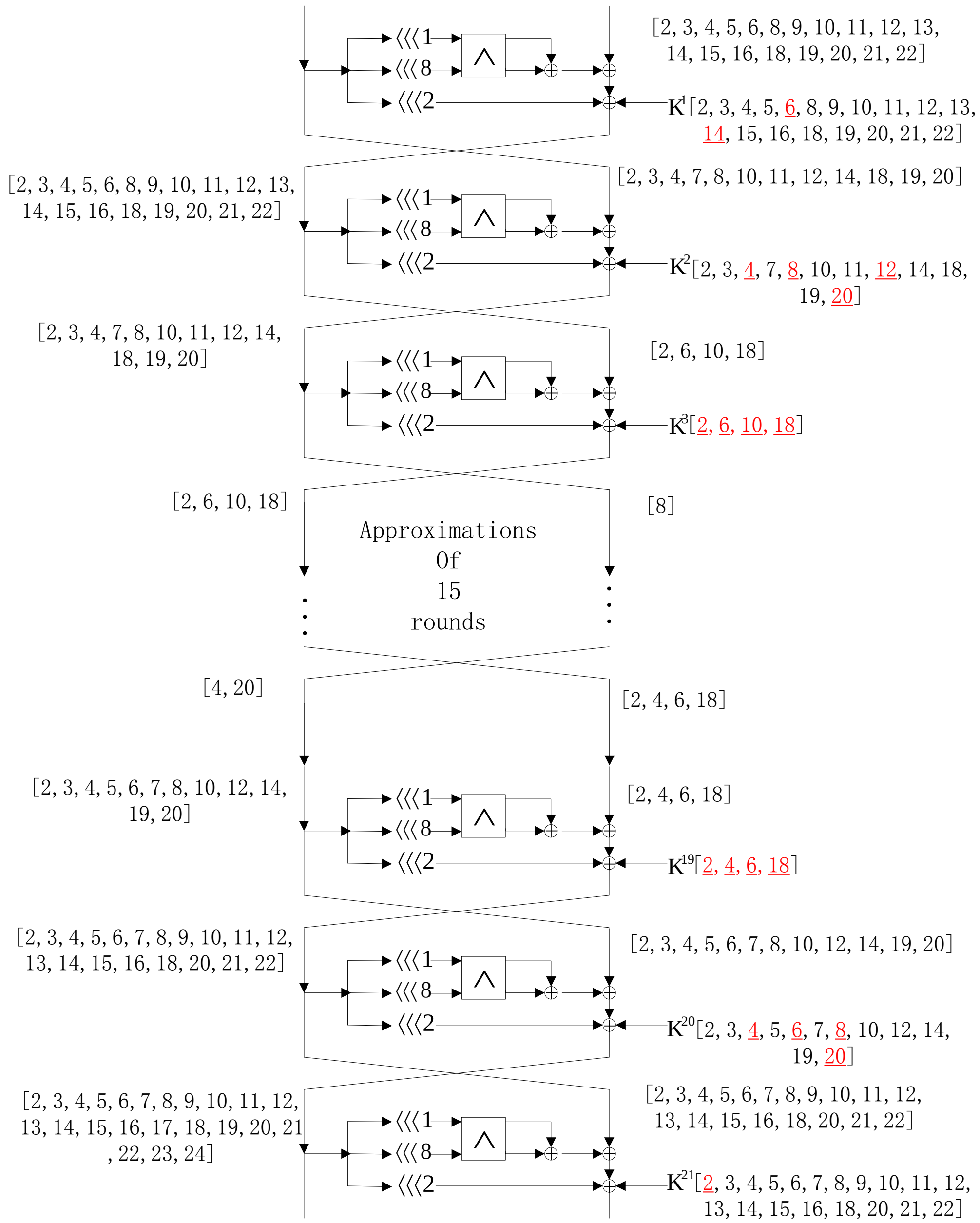

**Figure A3** Linear hull cryptanalysis of SIMON48/96

**Table A6** Comparison between our and other results

| Version | # Rounds | correlation | Reference |
|---|---|---|---|
| SIMON32 | 11 | $2^{-15}$ | [1] |
| | 11 | $2^{-15}$ | This paper |
| SIMON48 | 14 | $2^{-22}$ | [1] |
| | 14 | $2^{-22}$ | This paper |
| SIMON64 | 17 | $2^{-28}$ | [1] |
| | 18 | $2^{-31}$ | This paper |
| SIMON128 | 34 | $2^{-63}$ | [1] |
| | 34 | $2^{-61}$ | This paper |

# Rounds: Number of rounds for linear characteristic.

**Table A7** Input and output masks of the linear hulls

| Version | | The left half masks | The right half masks |
|---|---|---|---|
| SIMON32 | First-round input | 0000000000100000 | 0000000000000000 |
| | 13th round output | 0010000000000000 | 0000000000000000 |
| SIMON48 | First-round input | 010001000100000001000000 | 000000010000000000000000 |
| | 15thround output | 010101000000000001000000 | 000100000000000000010000 |
| SIMON64 | First-round input | 00000000000000000000000001000000 | 00000000000000000000000000000000 |
| | 21st-round output | 01000000000000000000000001000100 | 00000000000000000000000000000001 |
| SIMON64 | First-round input | 10001000000000000000000000001000 | 00100000000000000000000000000000 |
| | 22nd-round output | 00000000000000000000000000000110 | 00000000000000000000000000001000 |

additional constraint $\sum_r \sum_{j=1}^{n} V^r[j] \leqslant 78$, 63,996 have nonzero correlation. This linear hull can be used to mount an attack on 29-round SIMON64/128, demonstrated in Figure A4. There were 63 guessed bits for the key. In addition, a 22-round linear hull with *potential* $2^{-63.83}$ for SIMON64 was found, with input and output masks listed in Table A7 and constraint $\sum_r \sum_{j=1}^{n} V^r[j] \leqslant 80$. This hull can be used to mount an attack on 29-round SIMON64/128 with 52 guessed key bits. The guessed subkeys are shown in Table A8. The data complexity $N$ is set as $\mathrm{ALH}^{-1}$. The time complexity is $N\,2^{l_k}$, where $l_k$ is the length of the guessed key. A summary of the results for linear hulls in this paper is presented in Table A9. For SIMON128, no meaningful result was obtained, as a result of limited computational resources. These results also show that taking the dependence of S-boxes into consideration is necessary where many characteristics have correlation 0.

**Table A8** Guessed key bits for SIMON64

| | |
|---|---|
| First round | 3,4,6,7,8,10,11,13,14,15,17,21,31,32 |
| Second round | 2,5,6,9,13,30 |
| Third round | - |
| 26th round | - |
| 27th round | 6,7,31,32 |
| 28th round | 1,2,5,7,8,9,14,15,30,32 |
| 29th round | 1,2,3,4,6,7,8,9,10,11,13,15,16,17,22,23,31,32 |

**Table A9** Summary of results with linear hulls

| Version | # Rounds | *Potential* | # Returned | # Valid | # Attacked | Data | Time | Reference |
|---|---|---|---|---|---|---|---|---|
| SIMON32/64 | 13 | $2^{-31.69}$ | - | - | 20 | $2^{31.69}$ | $2^{59.69}$ | [1] |
| | 13 | $2^{-28.99}$ | 412206 | 196474 | 21 | $2^{28.99}$ | $2^{60.99}$ | This paper |
| SIMON48/96 | 15 | $2^{-44.11}$ | - | - | 20 | $2^{44.11}$ | $2^{80.11}$ | [1] |
| | 15 | $2^{-42.28}$ | 50432 | 43524 | 21 | $2^{42.28}$ | $2^{93.28}$ | This paper |
| SIMON64/128 | 21 | $2^{-62.53}$ | - | - | 28 | $2^{62.53}$ | $2^{119.53}$ | [1] |
| | 21 | $2^{-60.72}$ | 115199 | 63996 | 29 | $2^{60.72}$ | $2^{123.72}$ | This paper |
| | 22 | $2^{-63.83}$ | 52840 | 28590 | 29 | $2^{63.83}$ | $2^{115.83}$ | This paper |

# Rounds: Number of rounds for linear hull. # Returned: Number of characteristics returned by the model. # Valid: Number of characteristics with nonzero correlation. # Attacked: Number of attacked rounds.

## References

1 Alizadeh J, Alkhzaimi H A, Aref M R, et al. Improved linear cryptanalysis of round reduced SIMON. IACR Cryptology ePrint Archive, Reprot 2014/681, 2014.

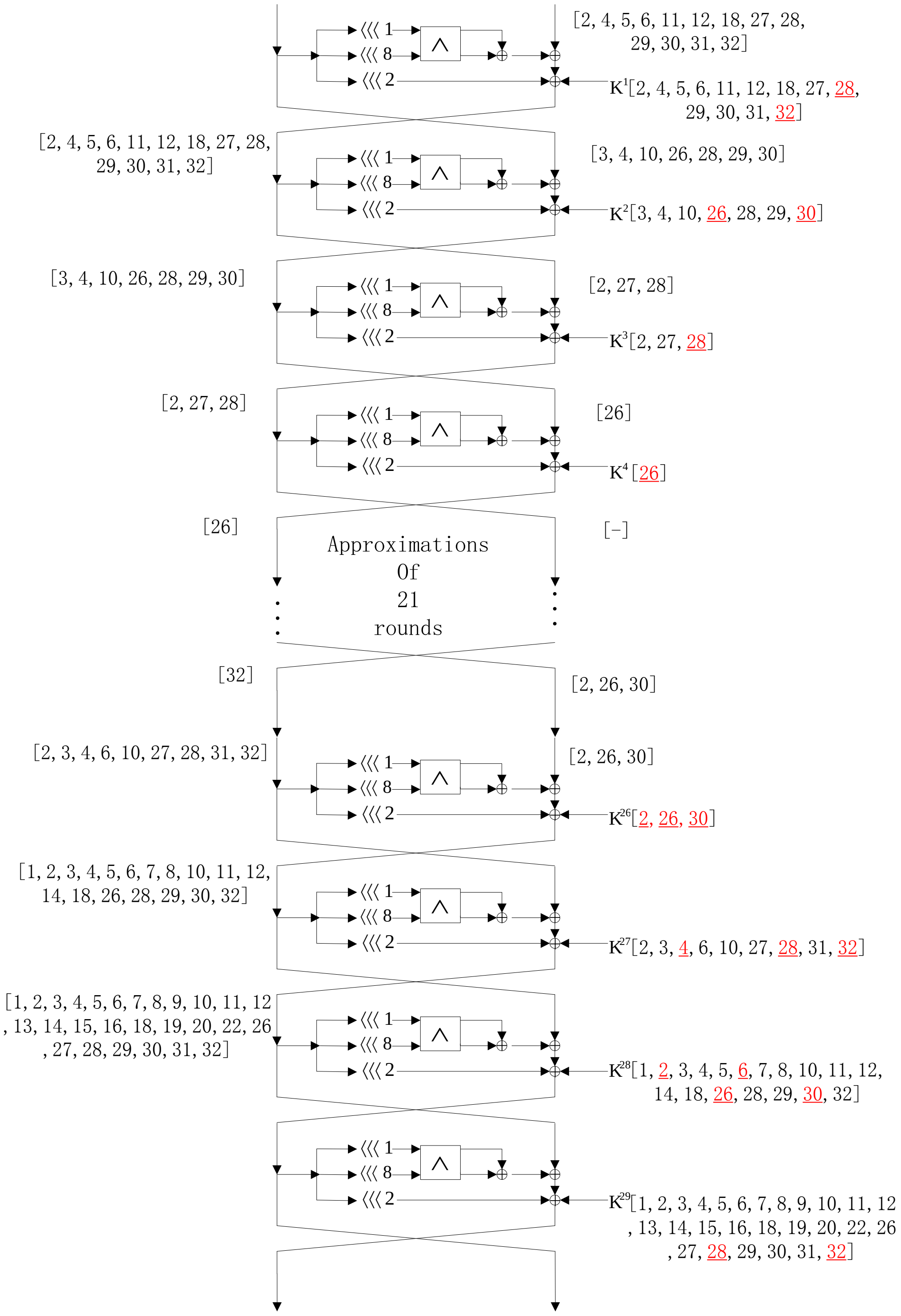

**Figure A4** Linear hull cryptanalysis of SIMON64/128

2 Selcuk A A. On probability of success in linear and differential cryptanalysis. Journal of Cryptology, 2008, 21(1): 131-147.

3 Wang N, Wang X, Jia K, et al. Improved differential attacks on reduced SIMON versions. Cryptology ePrint Archive, Report 2014/448

4 Nyberg K. Linear approximation of block ciphers. Advances in CryptologyEUROCRYPT'94. Springer Berlin Heidelberg, 1995: 439-444