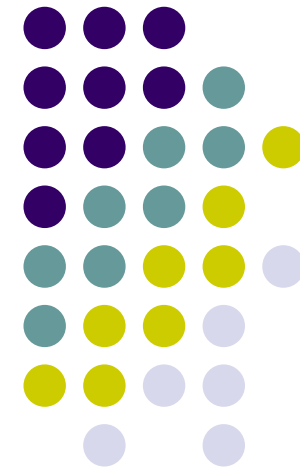


*The Second International Conference on Emerging Security  
Information, Systems and Technologies*

**SECURWARE 2008**  
August 25-31, 2008  
Cap Esterel, France



## ***Family of Parameterized Hash Algorithms***



 **Przemysław RODWALD**, Military Communication Institute, Poland

 **Janusz STOKŁOSA**, Poznań University of Technology, Poland



# Agenda



- Introduction
- Hash functions
  - Definition, properties
  - State of art in cryptanalysis
- Family of Parameterized Hash ALgorithms - PHAL
  - Iteration schema
  - Compression function
  - Security analysis
  - Efficiency
- Summary

# *Introduction*

## *Why new hash functions?*



- Great progress in cryptanalysis of hash functions
- Several flaws in Merkle-Damgård's construction
- NIST call for SHA-3 (AHS)

<http://www.nist.gov/hash-competition>

**NIST** - National Institute of Standards and Technology

**SHA** - Secure Hash Algorithm

**AHS** - Advanced Hash Standard



## ***Definition***

### **Hash function $h$ -**

computationally efficient function mapping an input (message  $m$ ) of arbitrary finite bitlength, to an output of fixed bitlength  $n$ .

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

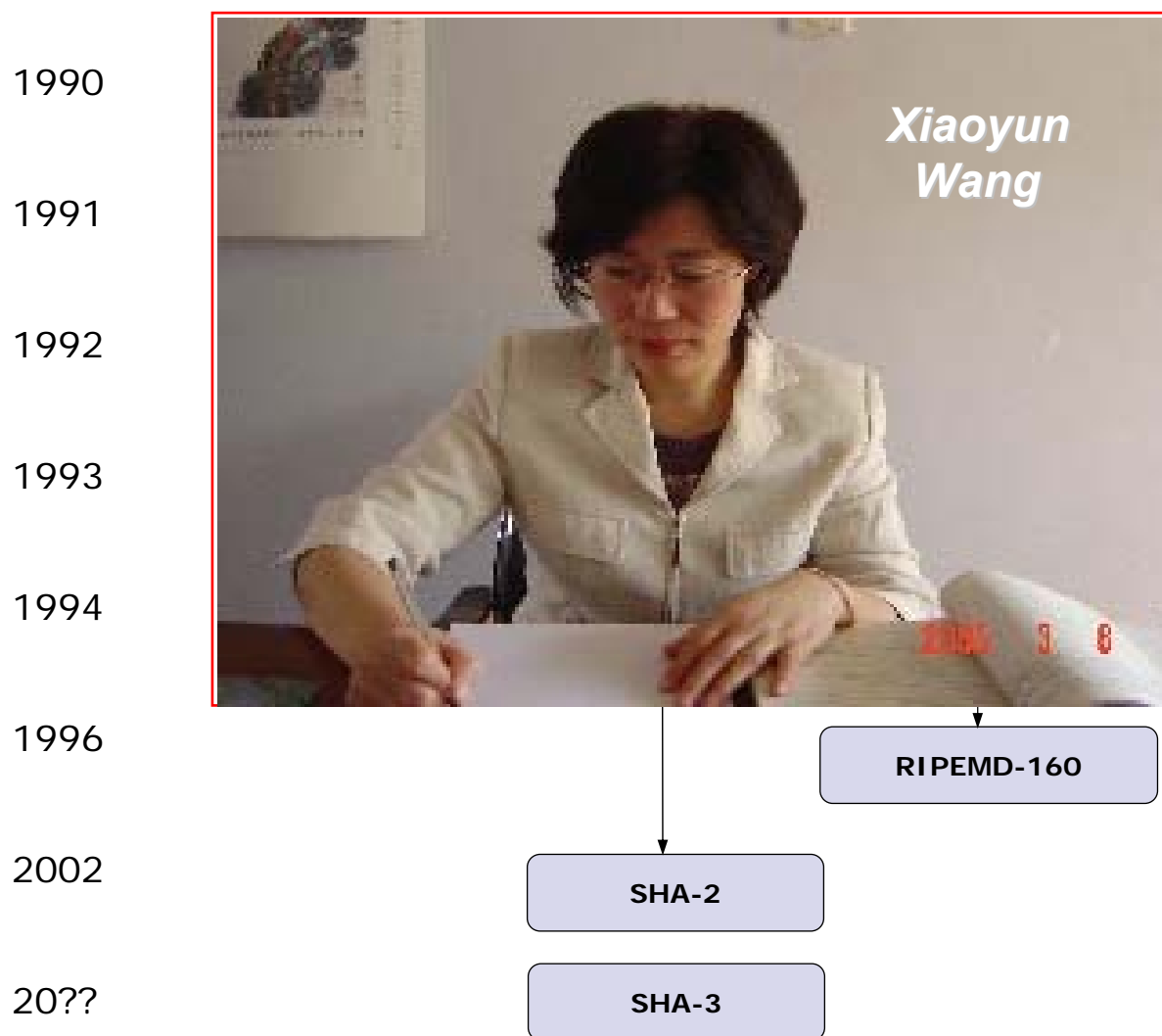


# *Properties of hashes*

- ***Preimage resistance (non-invertibility):***  
it is computationally infeasible to find any input which hashes to that output
- ***2nd preimage resistance (weak collision resistance):***  
it is computationally infeasible to find any second input ( $m'$ ) which has the same output as any specified input ( $m$ )
- ***Collision resistance (strong collision resistance):***  
*it is computationally infeasible to find any two distinct inputs  $m$  and  $m'$  which hash to the same output  $h(m) = h(m')$*



# Cryptanalysis



# *Family of PHAL*



- Message Padding
- Iteration Schema
- Message Modification
- Constants and Initial value
- Compression Function
- Statistical Tests
- Efficiency

# Family of PHAL

## Message Padding



$m$  : length of the message block (512 or 1024 bits)

$d$  : length of the digest (224, 256, 384 or 512 bits)

$w$  : length of a word (32 or 64 bits)

# Family of PHAL

## Iteration Schema



Hash function is designed using the compression function

$$\varphi: \{0,1\}^n \times \{0,1\}^m \times \{0,1\}^c \times \{0,1\}^s \times \{0,1\}^{rs} \rightarrow \{0,1\}^n$$

where:

- $n$  : length of the chaining variable (256 or 512 bits),
- $m$  : length of the message block (512 or 1024 bits),
- $c$  : the size of counter (number of bits hashed so far) modulo  $2^{64}$  (64 bits)
- $s$  : length of the *salt* (128 or 256 bits),
- $rs$  : the size of number of *rounds* (4 bits),
- *rounds* and *salt* are values defined by the user.

The process of hashing looks as follows::

$$CV_0 = IV,$$

$$CV_{i+1} = \varphi(CV_i, m_i, counter, salt, rounds), \quad i = 0, 1, \dots, k-1,$$

$$h(m) = CV_k.$$

# Family of PHAL

## Message Modification



$$\begin{aligned}w_i^x[0] &:= w_i^x[0] \oplus w_i^x[15] \oplus \text{MMConst}_1 \\w_i^x[1] &:= w_i^x[1] \oplus w_i^x[0] \\w_i^x[2] &:= w_i^x[2] \oplus w_i^x[1] \\w_i^x[3] &:= w_i^x[3] \oplus w_i^x[2] \oplus (\neg w_i^x[1] \lll \text{MMLR}_1) \\w_i^x[4] &:= w_i^x[4] \oplus w_i^x[3] \\w_i^x[5] &:= w_i^x[5] \oplus w_i^x[4] \\w_i^x[6] &:= w_i^x[6] \oplus w_i^x[5] \\w_i^x[7] &:= w_i^x[7] \oplus w_i^x[6] \oplus (\neg w_i^x[5] \ggg \text{MMRR}_1) \\w_i^x[8] &:= w_i^x[8] \oplus w_i^x[7] \oplus \text{MMConst}_2 \\w_i^x[9] &:= w_i^x[9] \oplus w_i^x[8] \\w_i^x[10] &:= w_i^x[10] \oplus w_i^x[9] \\w_i^x[11] &:= w_i^x[11] \oplus w_i^x[10] \oplus (\neg w_i^x[9] \lll \text{MMLR}_2) \\w_i^x[12] &:= w_i^x[12] \oplus w_i^x[11] \\w_i^x[13] &:= w_i^x[13] \oplus w_i^x[12] \\w_i^x[14] &:= w_i^x[14] \oplus w_i^x[13] \\w_i^x[15] &:= w_i^x[15] \oplus w_i^x[14] \oplus (\neg w_i^x[13] \ggg \text{MMRR}_2)\end{aligned}$$

where:

- MMConst1 and MMConst2 are two  $w$ -bit message modification constants.
- MMLR1 and MMLR2 are two message modification left rotation values.
- MMRR1 and MMRR2 are two message modification right rotation values.

# Family of PHAL

## Constants and Initial Value



$\Omega[0] = \text{salt}[0], \Omega[4] = \text{salt}[1] \oplus \text{counter}[0],$   
 $\Omega[8] = \text{salt}[2], \Omega[12] = \text{salt}[3] + \text{counter}[1].$

*Table. Constants word ordering*

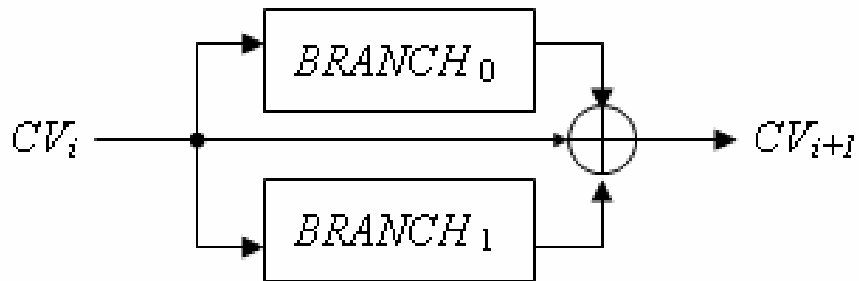
$t$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\rho_0(t)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\rho_1(t)$	13	8	12	9	15	14	10	11	6	0	2	4	1	5	7	3

*Table. Hamming Weight of Initial Value ~~BHA12356~~*

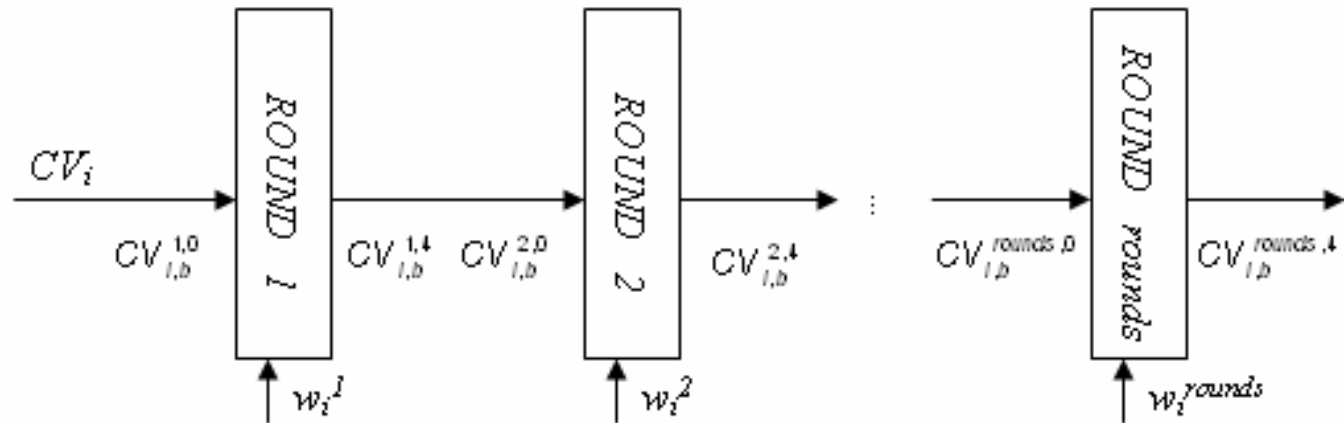
<b>c9b4361d</b>	11001001	10110100	00110110	00011101	4+4+4+4=16
<b>b14ed478</b>	10110001	01001110	11010100	01111000	4+4+4+4=16
<b>635a65c6</b>	01100011	01011010	01100101	11000110	4+4+4+4=16
<b>9c271eac</b>	10011100	00100111	00011110	10101100	4+4+4+4=16
<b>e455a927</b>	11100100	01010101	10101001	00100111	4+4+4+4=16
<b>1ed84be2</b>	00011110	11011000	01001011	11100010	4+4+4+4=16
<b>53a3ca59</b>	01010011	10100011	11001010	01011001	4+4+4+4=16
<b>2ea9b193</b>	00101110	10101001	10110001	10010011	4+4+4+4=16
	44444444	44444444	44444444	44444444	<i>hw</i>

# Family of PHAL

## Compression Function



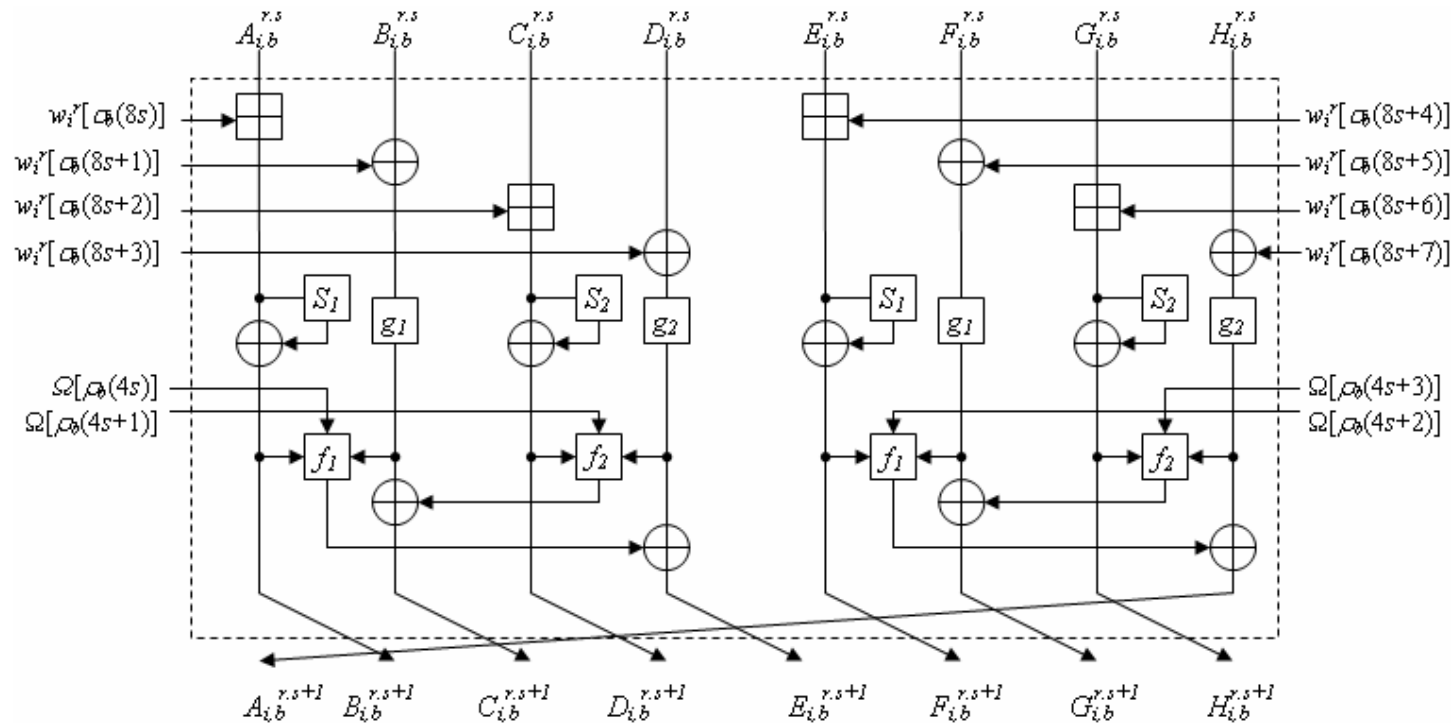
Picture. Compression Function



Picture. Branch Function (BRANCH)

# Family of PHAL

## Step Function



Picture. Step Function.

- $g_1(x) = x \oplus (x \lll G1L1) \oplus (x \lll G1L2),$
- $g_2(x) = x \oplus (x \lll G2L1) \oplus (x \lll G2L2),$
- $f_1(x,y,z) = xy \oplus (-x)z,$
- $f_2(x,y,z) = xy \oplus xz \oplus yz,$
- $S_1(x) = SBox1(x \gg 2(w/4)) \oplus SBox0(x \gg 3(w/4)),$
- $S_2(x) = SBox1(x) \oplus SBox0(x \gg (w/4)),$

# Family of PHAL

## Statistical Tests



NIST statistical tests suite for random and pseudorandom number generators for cryptographic applications

<http://csrc.nist.gov/groups/ST/toolkit/rng/>

### Tested messages:

- different number of rounds ( $rounds \in \{1,2,3,4\}$ )
- different salt values
- random messages
- sparse messages (Hamming weight  $\in \{1,2,3,m-3,m-2,m-1\}$ )

$m$  : length of the message block (512 or 1024 bits)

# Family of PHAL

## Efficiency



	PHAL-256			SHA-256
	1 round	2 rounds	3 rounds	
Message expansion or modification	$\boxplus$ : 0 $\oplus$ : 0 $\ll$ : 0	$\boxplus$ : 36 $\oplus$ : 54 $\ll$ : 24	$\boxplus$ : 72 $\oplus$ : 108 $\ll$ : 48	$\boxplus$ : 144 $\oplus$ : 384 $\ll$ : 480
Compression function	$\boxplus$ : 32 $\oplus$ : 304 $\ll$ : 128 $\wedge$ : 80	$\boxplus$ : 64 $\oplus$ : 608 $\ll$ : 256 $\wedge$ : 160	$\boxplus$ : 96 $\oplus$ : 912 $\ll$ : 384 $\wedge$ : 240	$\boxplus$ : 448 $\oplus$ : 832 $\ll$ : 768 $\wedge$ : 320
Output transformation	$\oplus$ : 16	$\oplus$ : 16	$\oplus$ : 16	$\boxplus$ : 8

Hash function	Average Speed [Mbps]
MD5	355
PHAL-256 (3 rounds)	88
SHA-256	84
PHAL-256 (4 rounds)	66

# Summary



## Family of PHAL :

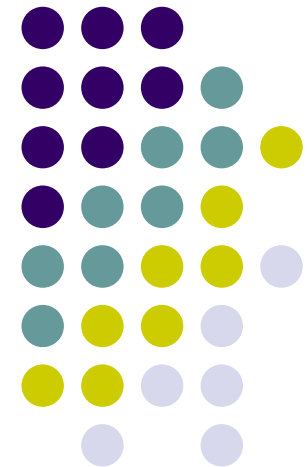
- flexibility
- increased resistance to attacks against MD-type structure
- two parallel branches
- efficiency comparable with SHA
  
- good candidate for SHA-3 ?

*Even in cryptology, silence is golden.*

Laurence D.Smith

***Thank you for your attention***

***Any questions?***



**Contact**

*p.rodwald@wil.waw.pl*

*janusz.stoklosa@put.poznan.pl*