

Antoon Bosselaers Bart Preneel (Eds.)

# Integrity Primitives for Secure Information Systems

Final Report of  
RACE Integrity Primitives Evaluation  
RIPE-RACE 1040



Springer

# Table of Contents

<b>I Introduction and Background</b>	<b>1</b>
<b>II Integrity Concepts</b>	<b>9</b>
<b>III Recommended Integrity Primitives</b>	<b>23</b>
1 Introduction to Part III . . . . .	25
2 MDC-4 . . . . .	31
3 RIPEMD . . . . .	69
4 RIPE-MAC . . . . .	113
5 IBC-Hash . . . . .	145
6 SKID . . . . .	169
7 RSA . . . . .	179
8 COMSET . . . . .	199
9 RSA Key Generation . . . . .	213
10 Implementation Guidelines for Arithmetic Computation . . . . .	233