

# Fast Software-Based Attacks on SecurID

Scott Contini<sup>1</sup> and Yiqun Lisa Yinini



## 2 The SecurID Hash Function

W

Every time 4 bits are removed from the original data array, the size shrinks by 4. Indexes within that array are always modulo the bmo

possible. According to their simulations, one only needs to do up to  $N = 12$  to  
ha



Hence, the expected number of final candidates is:

$$\text{table size} = 2^{64} \cdot \frac{1}{64}$$

full hash operations, where  $s$  is the speedup factor that can be obtained by taking advantage of the redundancy in the key with respect to the permutation. The value of  $s$  is  $\frac{96}{256}$  for  $N = 1$ ,



The combined speedups give the run times in Table 2. In all cases, phase 2, step 1 has become faster than the time for testing the nal

We programmed all iterating steps of both phases and the three main iterating speedups. In addition, we programmed an extra "table lookup" speedup that would improve the running time by a factor of 8 for  $N = 1$ . The extra speedup



## 7.2 Multiple Vanishing Derivatives with Different Derivatives

Given two v

Assume a vanishing differential occurred at times  $t$  and  $t^0$ , but no vanishing differential occurred among the time pairs  $(t$

Table 4. Assuming no more vanishing differentials occur within 2.8 days b

5. Tips on Reassigning SecurID Cards and Requesting New SecurID Cards, AMS Newsletter, March 2002, Issue No. 117. Available at <http://www.utoronto.ca/ams/news/117/html/117-5.htm> .
6. The Magma Computer Algebra Package. Information available at <http://magma.maths.usyd.edu.au/magma/> .

## **A Analysing Precomputed Tables**

Using computer experiments, we were able to exhaustively search for

{ If  $B_4$   $B_4^0 = 2^4 - (i)Tj / R, 3 9.6.5996(B)Tj / R$  then  $3 9.23.0276B222B9 9.96264 Tf 10.31083.8356B$

**Table 5. Example of 16 vanishing differentials that happened within 1.3 days, using key b5 a9 f4 8c 16 23 a6 1a.**