<u>Base</u>	SIMD&FP	<u>SVE</u>	<u>SME</u>	<u>Index by</u>
<u>Instructions</u>	<u>Instructions</u>	<u>Instructions</u>	<u>Instructions</u>	<b>Encoding</b>

#### SHA1H

SHA1 fixed rotate.

# Advanced SIMD (FEAT\_SHA1)

```
shalh <sd>, <sn>
integer d = UInt(Rd);
integer n = UInt(Rn);
if !IsFeatureImplemented(FEAT_SHA1) then UNDEFINED;
```

#### **Assembler Symbols**

<Sd> Is the 32-bit name of the SIMD&FP destination register,

encoded in the "Rd" field.

<Sn> Is the 32-bit name of the SIMD&FP source register,

encoded in the "Rn" field.

## **Operation**

```
<u>AArch64.CheckFPAdvSIMDEnabled();</u>
bits(32) operand = \underline{V}[n, 32]; // read element [0] only, [1-3] zeroed \underline{V}[d, 32] = \underline{ROL}(operand, 30);
```

### **Operational information**

If PSTATE.DIT is 1:

- The execution time of this instruction is independent of:
  - The values of the data supplied in any of its registers.
  - The values of the NZCV flags.
- The response of this instruction to asynchronous exceptions does not vary based on:
  - The values of the data supplied in any of its registers.
  - The values of the NZCV flags.

<u>Base</u> <u>SIMD&FP</u> <u>SVE</u> <u>SME</u> <u>Index by</u> Instructions Instructions Instructions Encoding

Internal version only: isa v33.64, AdvSIMD v29.12, pseudocode no diffs 2023 09 RC2, sve v2023-06 rel ; Build timestamp: 2023-09-18T17:56

Sh Pseu

Pseu

Copyright © 2010-2023 Arm Limited or it	s affiliates. All rights reserved. This document is Non-Confidential.