Table 2 lists the IGLOO2 design requirements.

Table 2 • **IGLOO2 Design Requirements**

Design Requirements and Details	Description
Hardware Requirements	
IGLOO2 Evaluation Kit (M2GL-EVAL-KIT): • 12 V adapter (provided along with the kit) • FlashPro4 programmer (provided along with the kit) • M2GL090TS-1FGG484	Rev D
Host PC or Laptop	Any 64-bit Windows Operating System
Software Requirements	
Libero SoC	v11.7
Note: The IGLOO2 design uses M2GL090TS-1FGG484 device in the IGLOO2 Evaluation Kit. However, the official IGLOO2 Evaluation Kit uses the M2GL010T-1FGG484 device. If you want to run the application note design in M2GL010T-1FGG484, refer to the KB5659 for migrating M2GL090TS-1FGG484 to M2GL010T-1FGG484.	

Overview

SHA is a cryptographic hash function designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST - FIPS. This Standard specifies several secure hash algorithms, including SHA-256. SHA-256 is a one-way hash function that can process a message to produce a message digest. In this application note, the term message digest and hashed output are used interchangeably. The input data is a message and hash value is a message digest.

In the SmartFusion2 and IGLOO2 devices, the SHA-256 accelerator block is part of the Cryptographic Services block that resides in the system controller. The SHA-256 accelerator block implements the SHA-256 function.

The SHA-256 algorithm determines the integrity of the message—any change to the message, with a very high probability, results in a different message digest. This property is widely used in security applications and protocol, generation and verification of digital signatures and message authentication codes, and so on. Following are the basic properties of the SHA-256 algorithm:

- Message size: < 2^{64} bits
- Block size: 512 bits
- Word size: 32 bits
- Message digest size: 256 bits

Figure 1 shows the basic SHA-256 operation.

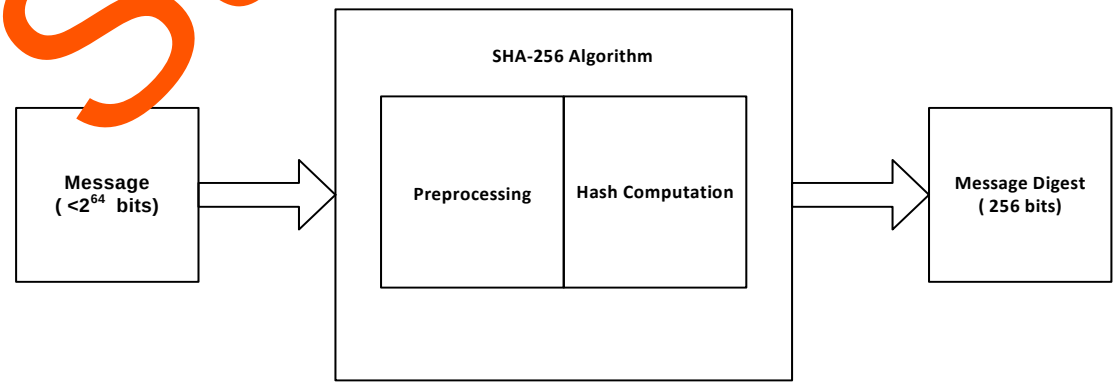

Figure 1 • **SHA-256 Operation**

Superseded