**CLAIMS**

1. A method comprising:

initializing a storage space of a secure storage device into a plurality of portions;

copying an update program to a first portion in the portions and copying update data to a second portion of the portions;

generating a first golden measurement for the first portion using one or more cryptographic functions, wherein the first golden measurement is a first value that securely identifies the first portion;

generating a second golden measurement for the second portion using the one or more cryptographic functions, wherein the second golden measurement is a second value that securely identifies the second portion;

measuring the first portion;

updating or rolling back an update to the secure device in response to determining that the measuring of the first portion does not match the first golden measurement of the first portion, the updating or rolling back the update to the secure device comprising:

executing a first-stage bootloader (FSBL) and transferring control of the secure device to the update program;

reading contents of one or more status registers, the status registers storing the state of the secure device; and

updating the secure device upon determining that the status registers indicate either an update should be initiated or an update is currently executing;

verifying an update operation upon determining that the measuring of the first portion matches the first golden measurement of the first portion; and

modifying a recovery block of the storage space to point to the FSBL, the FSBL configured to transfer control to the first portion.

2. The method of claim 1, the initializing the storage space performed in response to receiving a software update.

3. The method of claim 1, further comprising rebooting the secure storage device after generating the first and second golden measurements.

4. The method of claim 1, the updating comprising successively writing data from the second portion to an active storage space.

5. The method of claim 4, the successively writing data further comprising simultaneously updating the status registers after each write.

6. The method of claim 1, the verifying an update operation comprising:

measuring the second portion; and

comparing the measurement of the second portion to the second golden measurement.

7. The method of claim 6, further comprising one or more of:

restarting an update sequence upon determining that the measurement of the second portion does not match the first or second golden measurements and a number of retries has not been exceeded;

canceling the update sequence upon determining that the measurement of the second portion does not match the first or second golden measurements and a number of retries has been exceeded;

restoring the secure device upon determining that the measurement of the second portion does not match the second golden measurement and does not match the previously stored second golden measurement; and

completing the update sequence if the measurement of the second portion equals the second golden measurement.

8. The method of claim 7, the completing the update sequence comprising measuring an active storage space of the secure device and confirming the measurement matches an expected value.

9. The method of any one of claims 1 to 8, wherein the one or more cryptographic functions include at least one of a hash and a hash tree.

10. The method of claim 9, wherein the hash includes a secret key stored in the device or a hash-based message authentication code (HMAC).

11. A non-transitory computer readable storage medium for tangibly storing computer program instructions capable of being executed by a computer processor, the computer program instructions defining the steps of the method of any one of claims 1 to 10.

12. A device comprising

a processor; and

a storage medium for tangibly storing thereon program logic for execution by the processor, the stored program logic comprising instructions causing the processor to perform the operations of the method of any one of claims 1 to 10.