PacketPortal™ IP-Lock™ Security

IP-Lock security technology is the cornerstone of PacketPortal architecture. Perhaps the most important security features in the product are related to the secure communication and authentication between SFProbes™ and the packet-routing engines (PREs) that control and configure them.

Since SFProbes and PREs may communicate with each other on unsecured subscriber networks, there is a potential opportunity for malicious users to hijack them or their communications. To prevent this, SFProbes and PREs communicate via a proprietary 128 bit Grain cipher[1] algorithm. The essential elements of IP-Lock are:

- each SFProbe has a unique serial number and a 48-bit globally unique device ID
- each SFProbe can have an optional customer-programmed 48-bit network ID (CNID)
- each SFProbe has a unique, private, licensed activation key from Viavi Solutions™
- management communication is ciphered with a 128 bit Grain algorithm
- SFProbes are not assigned a MAC or IP address

White Paper

The Grain algorithm was chosen because of its high-strength security and very small hardware footprint, making it ideal for use in an SFP form factor. The strength of the security comes from the use of both a linear feedback register and a non-linear feedback shift register. The Grain-128 cipher[2] keystream engine is shown below.

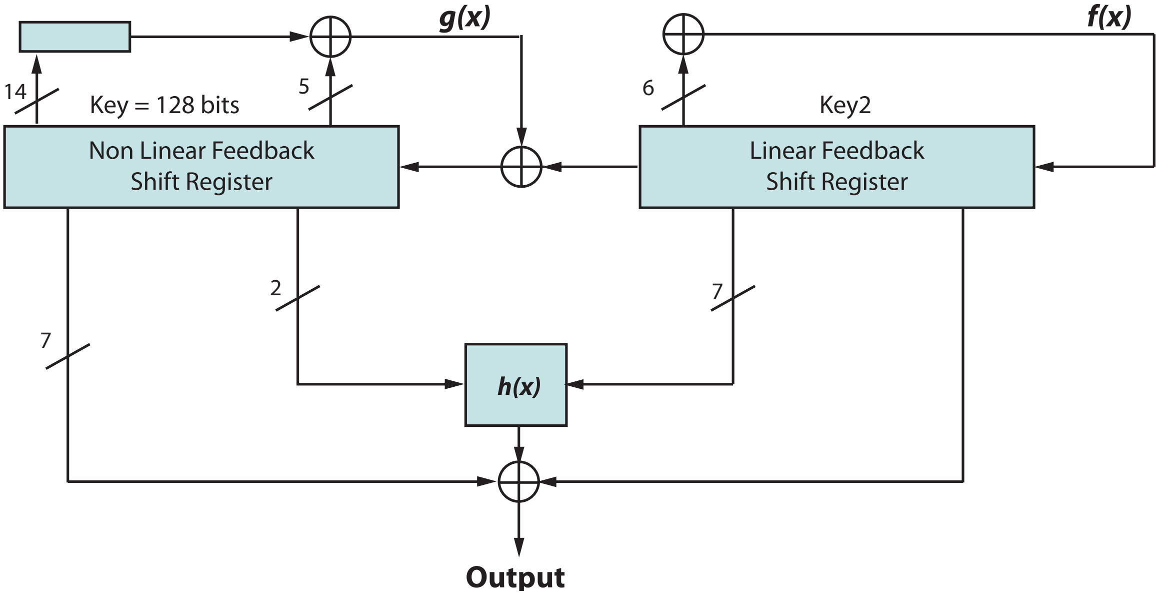
g(x)
f(x)
14
Key = 128 bits
5
6
Key2
Non Linear Feedback Shift Register
Linear Feedback Shift Register
2
7
7
h(x)
Output

Figure 1. The Grain-128 cipher keystream engine.

[1] A stream cipher consists of a pseudo-random bit stream generated by a keystream generator. The data stream to be encrypted is then typically XORed with the keystream and sent on the wire.

[2] More information on the Grain-128 cipher can be found in A Stream Cipher Proposal: Grain-128 by Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier

Another security element of the PacketPortal platform is the CNID. Its function is to link a SFProbe to a specific operator's network to prevent the possibility of accidental discovery of devices not belonging to a network operator or malicious discovery of another operator's SFProbes.

Upon being plugged into the network element, the SFProbe works like any standard SFP. When a Discovery Hello packet from a PRE flows through, the SFProbe wakes up and checks that the CNID in the discovery packet matches the CNID programmed in its EEPROM. If not, it ignores the discovery attempt and waits for another attempt. If it matches, the device responds to the PRE with its device ID. The PRE captures that ID and it is passed securely to the system manager (SM). There, the network operator passes the ID and the device serial number to the Viavi licensing center which then provides the EEPROM key that was programmed during manufacture for that specific SFProbe. This proves ownership of the SFProbe because a licensing attempt requires both physical and network access to the element. This information is then entered into the SM and fed to the PRE so the discovery and activation process can be completed.

In addition to the Grain encryption, all command and control packets are sequenced, and the SFProbe ignores any out-of-sequence packets. This protects against man-in-the-middle and replay attacks.

This Viavi IP-Lock technology ensures that PacketPortal delivers carrier-grade, multilayer security to ensure information integrity in a highly reliable and scalable deployment.

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.