7 ESCROWED ENCRYPTION STANDARD EES

The Escrowed Encryption Standard (EES) defines a US Government family of cryptographic processors, popularly known as "Clipper" chips, intended to protect unclassified government and private-sector communications and data. A basic feature of key setup between pairs of EES processors involves the exchange of a "Law Enforcement Access Field" (LEAF) that contains an encrypted copy of the current session key. The LEAF is intended to facilitate government access to the cleartext of data encrypted under the system. Several aspects of the design of the EES, which employs a classified cipher algorithm and tamper-resistant hardware, attempt to make it infeasible to deploy the system without transmitting the LEAF. We evaluated the publicly released aspects of the EES protocols as well as a prototype version of a PCMCIA-based EES device. This paper outlines various techniques that enable cryptographic communication among EES processors without transmission of the valid LEAF. We identify two classes of techniques. The simplest allow communication only between pairs of "rogue" parties. The second, more complex methods permit rogue applications to take unilateral action to interoperate with legal EES users. We conclude with techniques that could make the fielded EES architecture more robust against these failures.

The structure of the EES is shown in Figure.

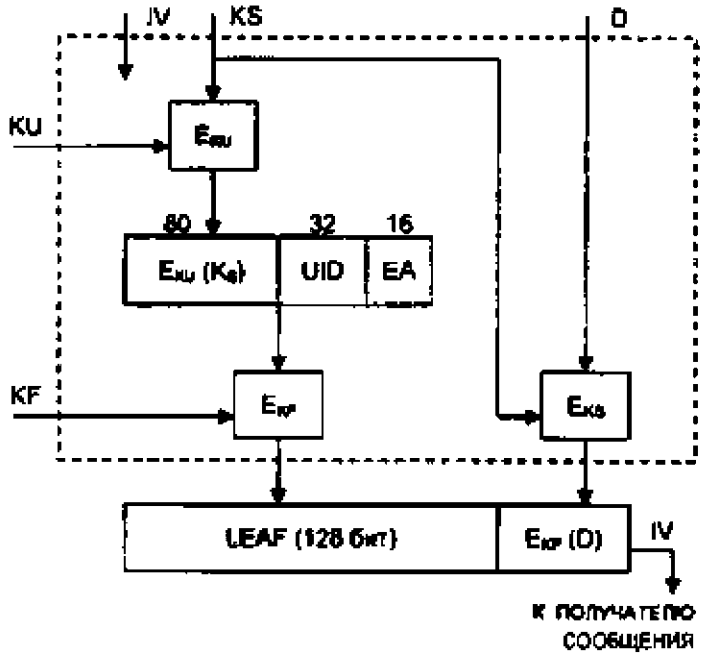

Figure – Block diagram of the Calculating LEAF

LEAF can be expressed by the equations:

$$LEAF = E_{KF}\left(E_{KU}(KS), UID, EA\right). \qquad (1)$$

The scheme of protecting telephone conversations is shown in the Figure.

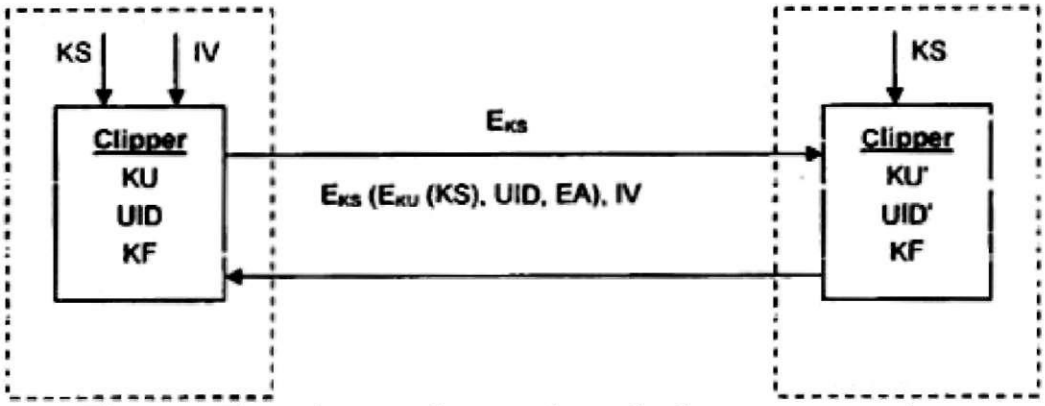

Figure – The scheme of protecting telephone conversations