Galois Extension Field Block Cipher

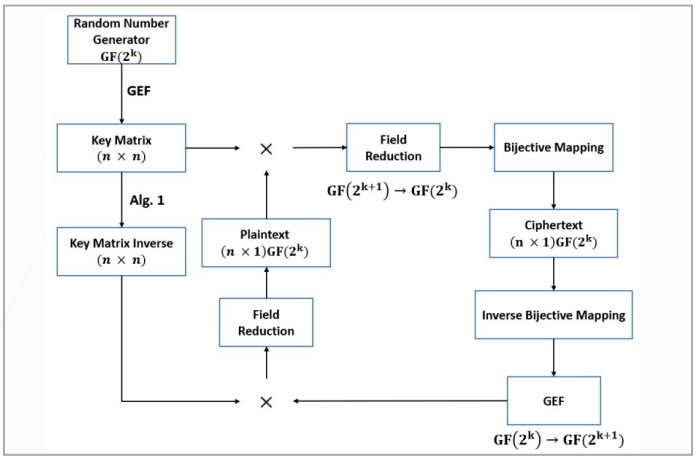
VTIP 21-097: "Galois Extension Field Block Cipher"

THE CHALLENGE

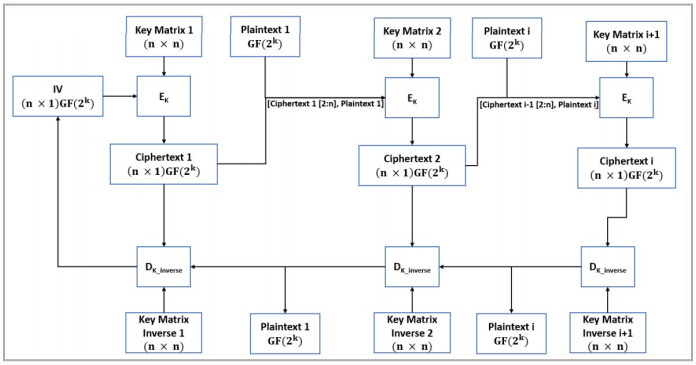
Many parts of the Internet of Things (IoT) have little to say, perhaps as little as periodic status indicators representing on/off or open/close. As a result, many designers forget that these elements still have security needs and represent a vector into the larger network. When these nodes are (1) too size, weight, and power (SWaP) constrained to implement AES and related commercial protocols, or (2) transmit so little at a given time to justify large crypto block sizes, an alternative cryptographic approach is needed. Key design requirements to fill this need include lightweight processing and small, variable-length block sizes that can adjust to any application.

OUR SOLUTION

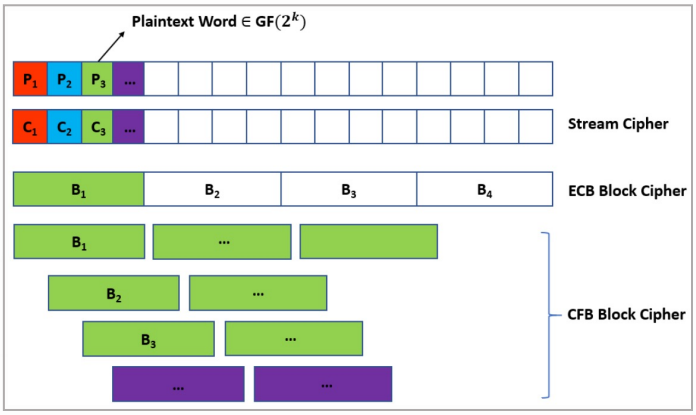
Alan Michaels and his team at Virginia Tech have developed an algorithm that can be used to efficiently encrypt small data transfers for power-constrained IoT-caliber devices. The algorithm extends prior work using Galois extension field (GEF) arithmetic as a sequence combination technique, which also supports stream-based ciphers. This modification works as a block cipher in both electronic code book (ECB) and cipher feedback (CFB) modes. Encryption takes less time than decryption (which must compute the inverse of the key matrix), opening the potential of asymmetric processing loads (access points bearing the brunt of the load), yet all steps are more efficient and cost effective than the Advanced Encryption Standard (AES) when dealing with small amounts of information. This modified cipher has numerous applications in the IoT, including the automotive; unmanned vehicle; robotics; telemetry, tracking, and control (TT&C); and wireless avionics industries.



Galois Extension Field (GEF) Electronic Code Book (ECB) mode for streaming data encryption/decryption.



Cipher Feedback (CFB) mode for the cryptographic algorithm.



Diffusion expansion for CFB modes in the cryptosystem.

CONTACT:

Rozzy Finn

rozzy@vt.edu

540-231-1566