7TUNNELS
ENCRYPTION BEYOND MATHEMATICS

7TUNNELS, INC.

RANDOM CIPHER PAD REPLACEMENT

v.6.2.2020

This discussion of RCP Replacement will use the Random Cipher Pad (RCP) idea as follows:

Message Keys (MK) are assembled from True Random Numbers (TRN) taken from one or more RCPs. Any given MK may be smaller, the same size, or larger, than the one or more RCPs used to form the MK. Therefore, a single RCP may be sampled multiple times for several small messages, or several RCPs can be used up for a single MK.

The initial pair (endpoints) of 7Tunnels system installations are pre-provisioned with large matching RCP pools. The RCPs in each pool are addressed using modular math thus forming a ring. RCP sampling starts at zero proceeding around the ring, thus the concept of "next available."

Encrypting/Decrypting causes the next available pointer to advance to the next higher (modular) address. There is also a "next replaceable" pointer which also started at 0. This pointer follows along behind the next available pointer, showing the RCP manager where to overwrite used RCPs.

With this method, you end up with a *slice of pie* that can never be allowed to occupy the entire *pie*. As RCPs are used up, the next available pointer is advanced. As the RCP manager brings in new keys, the next replaceable pointer is advanced. The size of the *slice* tells the RCP manager the urgency of key replacement.

RCPs in this pool may only originate from the TRN Generator (TRNG) and these RCPs are called the DataRCPs (DRCP).

A second pool of RCPs is described in the same way, but replacements may be generated algorithmically, as described later. These RCPs are called KeyRCPs.

SEND MESSAGE:

- **Sender**

➢ Uses the next available DRCP to encrypt the plain text
➢ The cipher is sent to the recipient
➢ The DRCP pointer is advanced
➢ If the DRPC is used up it is stored if needed later and deleted from the DRCP pool

- **Recipient**

➢ Uses the next available DRCP to decrypt the cipher
➢ Sends the plain text on to the user
➢ The DRCP pointer is advanced

- ➢ If the DRPC is used up it is stored if needed later and deleted from the DRCP pool

REPLACE DRCP:

The RCP Manager monitors both the next replaceable pointer and the next available pointer, and when triggered at preset thresholds, an RCP Manager would be able to handle many user pairs:

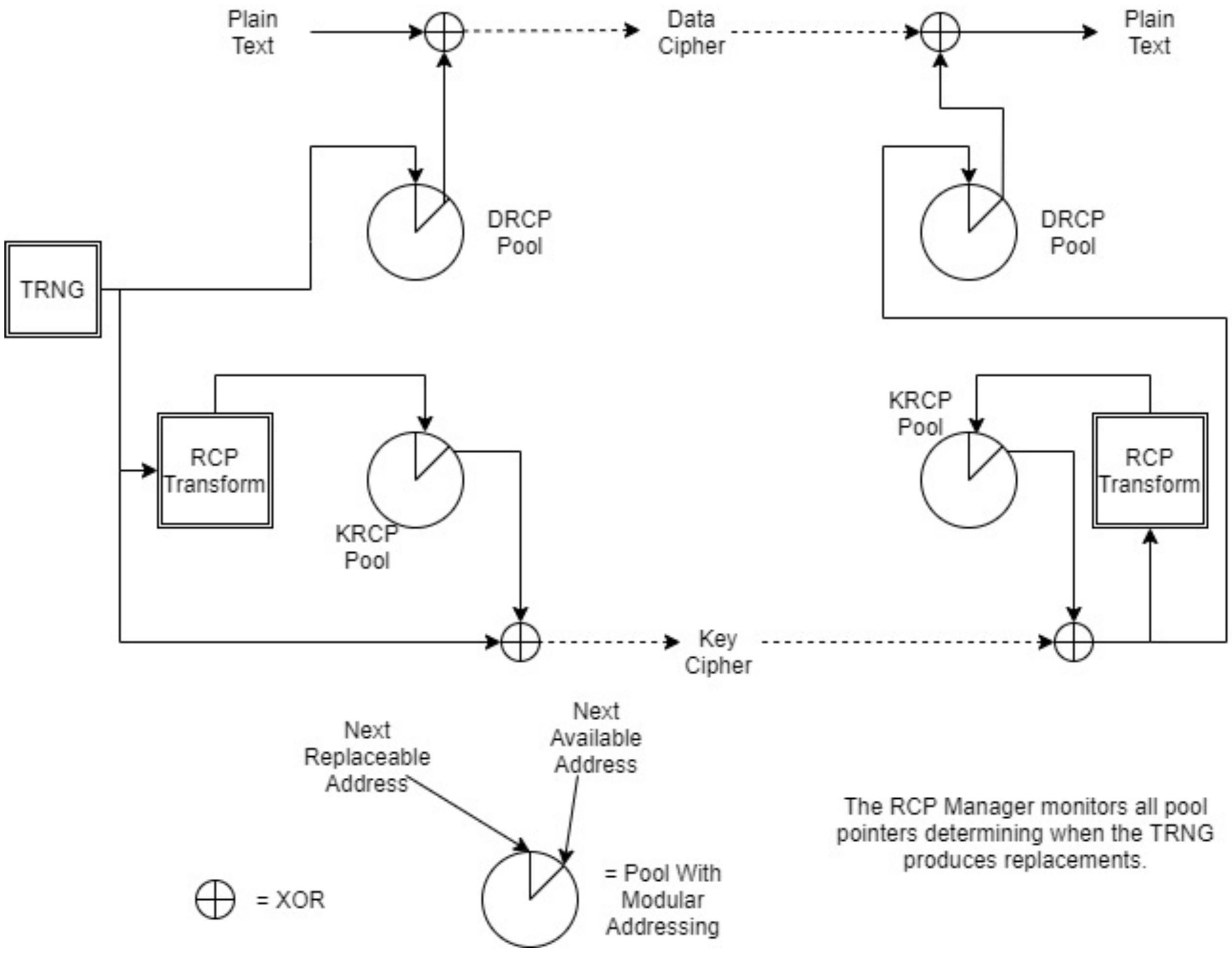
- **RCP Manager**
- ➢ Generate the replacement RCP with the TRNG
- ➢ Overwrite the next replaceable DRCP with the replacement RCP
- ➢ Advance the next replaceable DRCP pointer
- ➢ Encrypt the replacement RCP with the next available KRCP
- ➢ The cipher is sent to the recipient
- ➢ The replacement RCP is transformed into a new KRCP (see notes below)
- ➢ The replacement RCP is deleted
- ➢ The next replaceable KRCP is overwritten by the new KRCP
- ➢ The next replaceable KRCP pointer is advanced

- **Recipient**
- ➢ Decode the cipher using the next available KRCP - The plain text is the replacement DRCP
- ➢ Overwrite the next replaceable DRPC with the replacement
- ➢ Advance the next replaceable DRPC pointer
- ➢ Transform the replacement DRCP into a new KRCP (see notes below)
- ➢ Overwrite the next replaceable KRCP with the new KRCP
- ➢ Advance the next replaceable KRCP pointer

NOTES:

1. RCP Transform: The goal here is to transform the RCP into a second RCP that is uncorrelated and independent from the first. This is accomplished by bit-reversing the incoming RCP then using the result as the basis for the random selection of bytes from a large TRNG generated pool of random bytes.
2. Communication of data ciphers and key ciphers may use the same or separate channels or even be multiplexed together.
3. The above describes one direction. A full duplex design would be two pairs of users as described above.

DIAGRAM



The RCP Manager monitors all pool pointers determining when the TRNG produces replacements.

CONTACT INFORMATION

For additional information on 7Tunnels, please see our website:

www.7Tunnels.com

For **DuPont Use Case Report**, technical and operational documentation, you can request access to the 7Tunnels VDR (under NDA).

For additional information on 7Tunnels, Inc., please contact:
David Wiener, Chairman & CEO
d.wiener@7Tunnels.com 1.435.640.1650
P.O. Box 982470 Park City, Utah 84098 USA

7TUNNELS
ENCRYPTION BEYOND MATHEMATICS