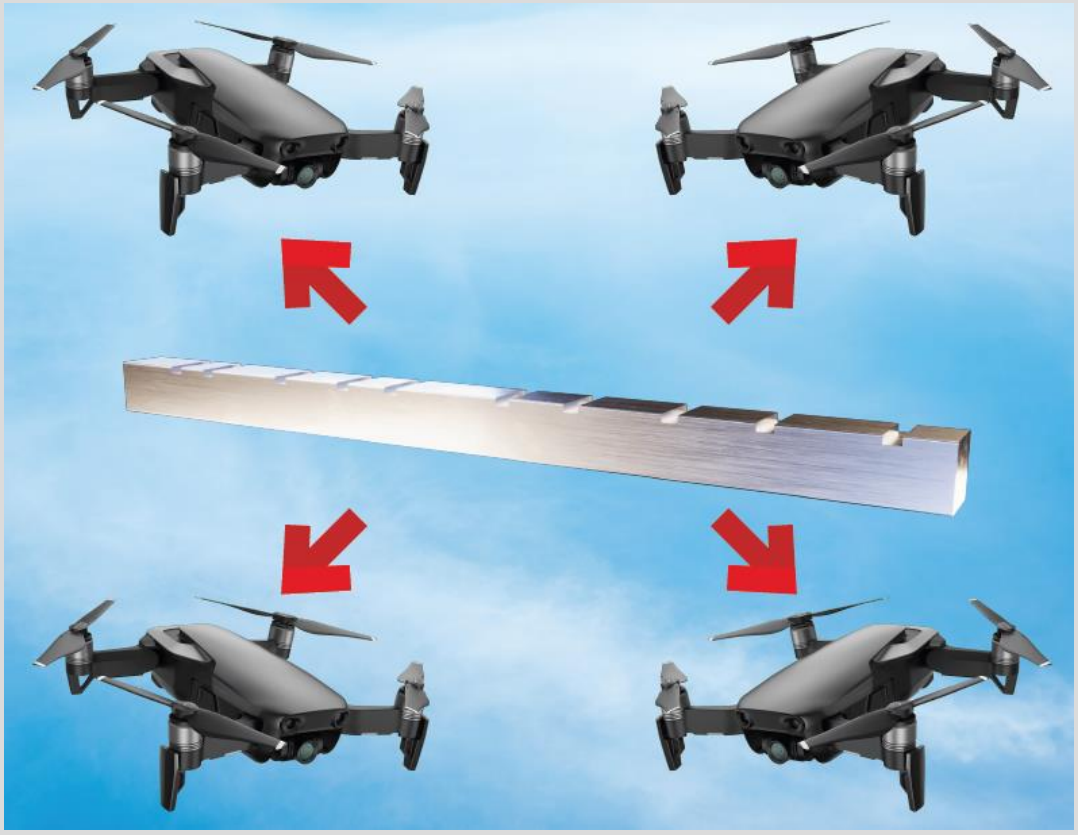
DRONE CONTROL



Our technology allows a unique encryption key to be generated for each mission even when multiple users must connect with the drone. The launching user generates a key from a combination of notches on the token and a base key. The notches used are then transmitted to everyone else who needs to use that drone, allowing them to generate the necessary key from their matching tokens. This is not limited to single small UAVs, and could be used for drone boats, ground vehicles, deployed sensors, and swarms.

The use of unique encryption keys prevents exploitation of downed or captured drones. Since the token and base key remain with the operators, the drone will only have the final encryption key onboard. Since that final key was unique to the mission and it will be easy for users to track which measurement combination was used on lost drones, it cannot be used to compromise other drones. This rapid rotation of codes also defeats more traditional codebreaking since it guarantees codes are out of service long before they can be broken.

Using tokens to indirectly communicate the encryption key minimizes the risk of a key being seized in transit if other communications are compromised. Our tokens also make it impossible for a cyberattack to fully compromise the encryption system because you can’t hack a piece of steel.