US 20230231710A1

(54) **KEY DIVERSIFICATION IN A TRACKING DEVICE ENVIRONMENT**

(71) Applicant: **Tile, Inc.**, San Mateo, CA (US)

(72) Inventors: **Steven R. Klinkner**, Palo Alto, CA (US); **Josselin de la Broise**, Mountain View, CA (US); **Ian Thomas Meyer**, San Francisco, CA (US)

(57) **ABSTRACT**

A tracking device can use a permanent encryption key pair to encrypt a temporary private key that corresponds to a set of diversified temporary public keys. When a community mobile device subsequently detects the tracking device, the central tracking system provides a diversified temporary public key to the community mobile device. The community mobile device uses the diversified temporary public key to encrypt location data representative of a location of the community mobile device, and provides the encrypted location data to the central tracking system. When a user subsequently requests a location of the tracking device from the central tracking system, the central tracking system provides the encrypted temporary private key and the encrypted location data to a device of the user, and the device can decrypt the encrypted temporary private key using the permanent encryption key pair, and decrypt the encrypted location data using the decrypted temporary private key.