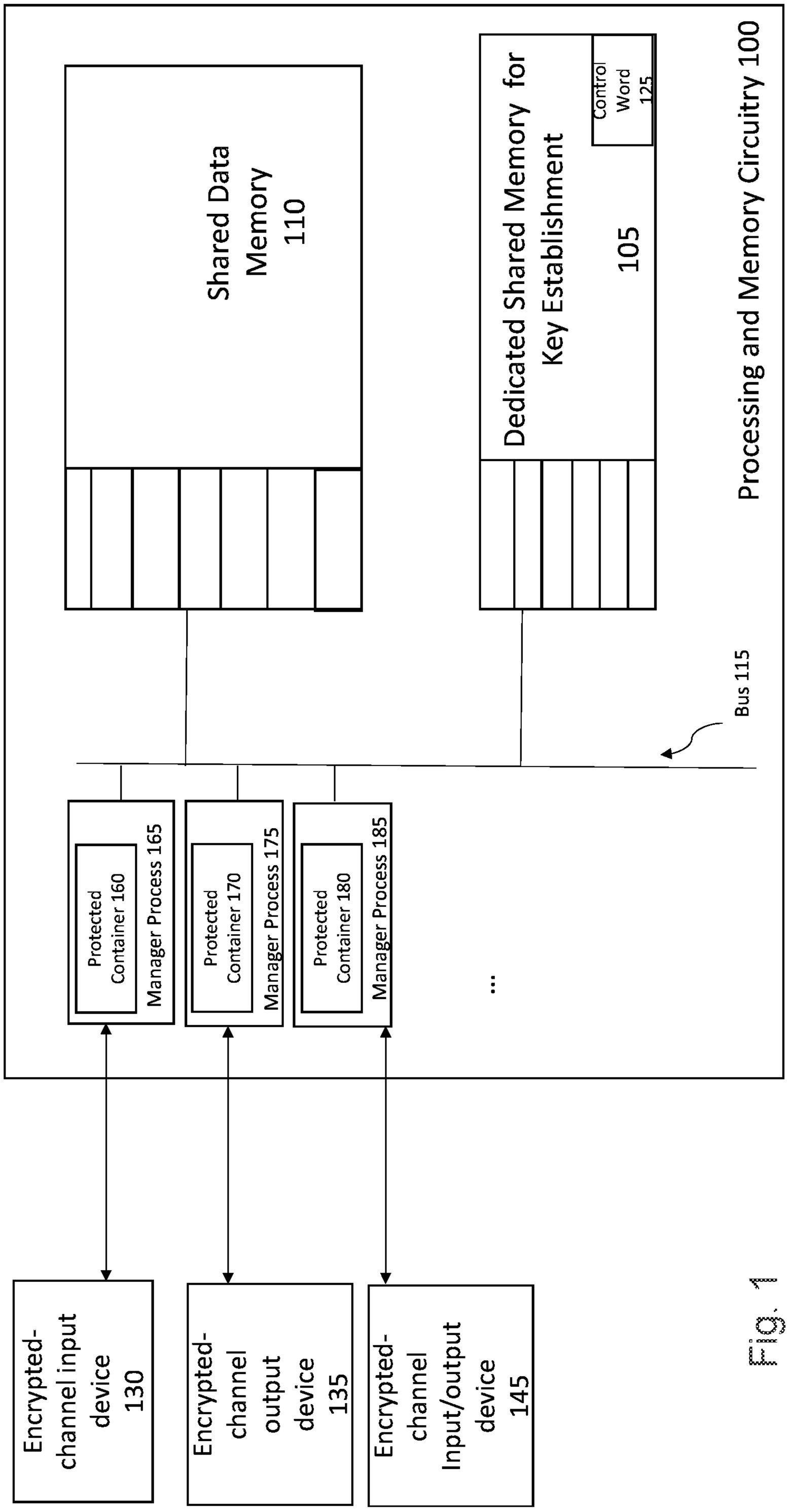

Processing and Memory Circuitry 100
Shared Data Memory 110
Dedicated Shared Memory for Key Establishment
105
Control Word 125
Bus 115
Protected Container 160
Manager Process 165
Protected Container 170
Manager Process 175
Protected Container 180
Manager Process 185
...
Encrypted-channel input device 130
Encrypted-channel output device 135
Encrypted-channel Input/output device 145

Fig. 1

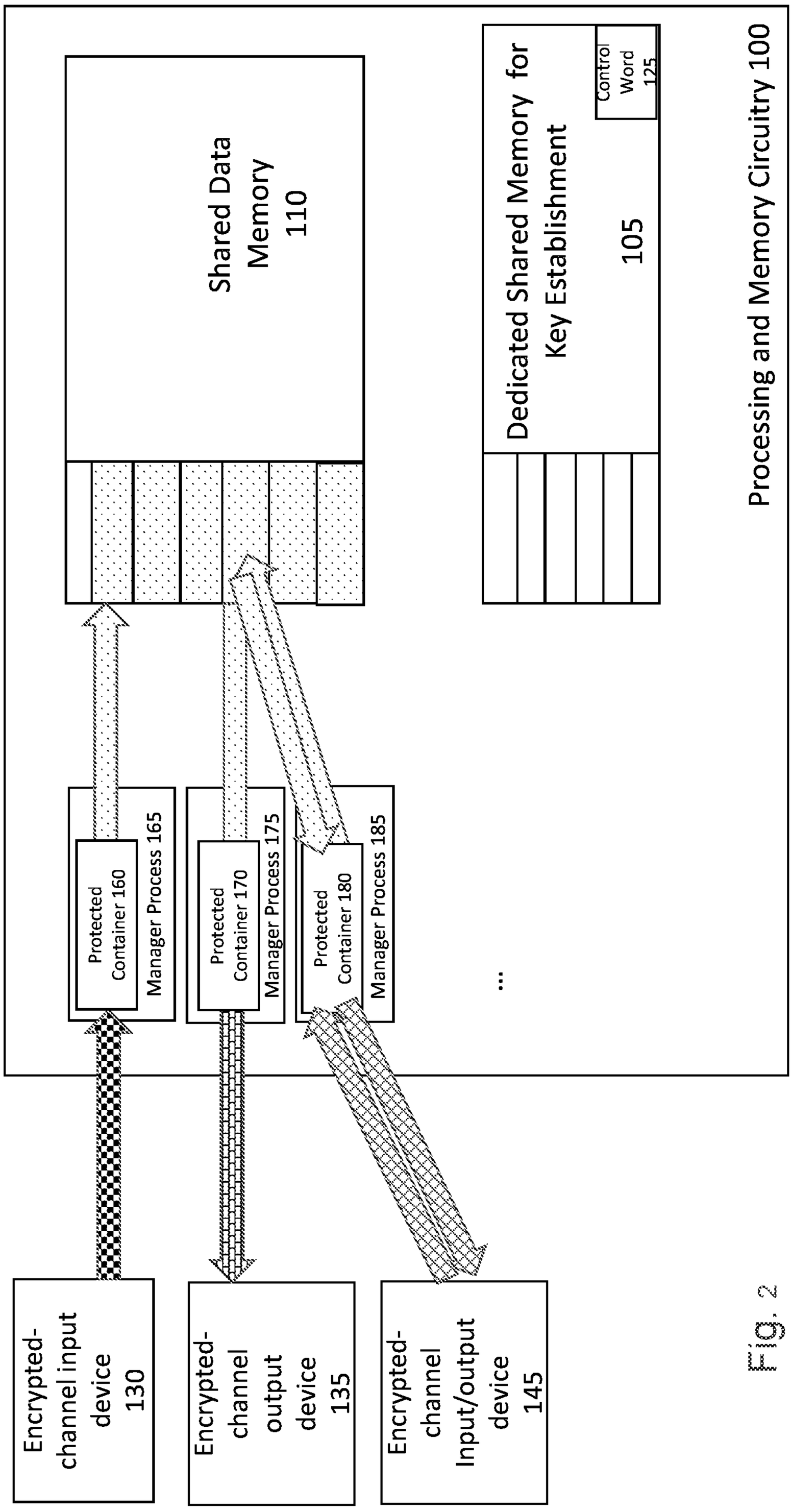

Processing and Memory Circuitry 100
Shared Data Memory 110
Dedicated Shared Memory for Key Establishment 105
Control Word 125
Protected Container 160
Manager Process 165
Protected Container 170
Manager Process 175
Protected Container 180
Manager Process 185
...
Encrypted-channel input device 130
Encrypted-channel output device 135
Encrypted-channel Input/output device 145

Fig. 2

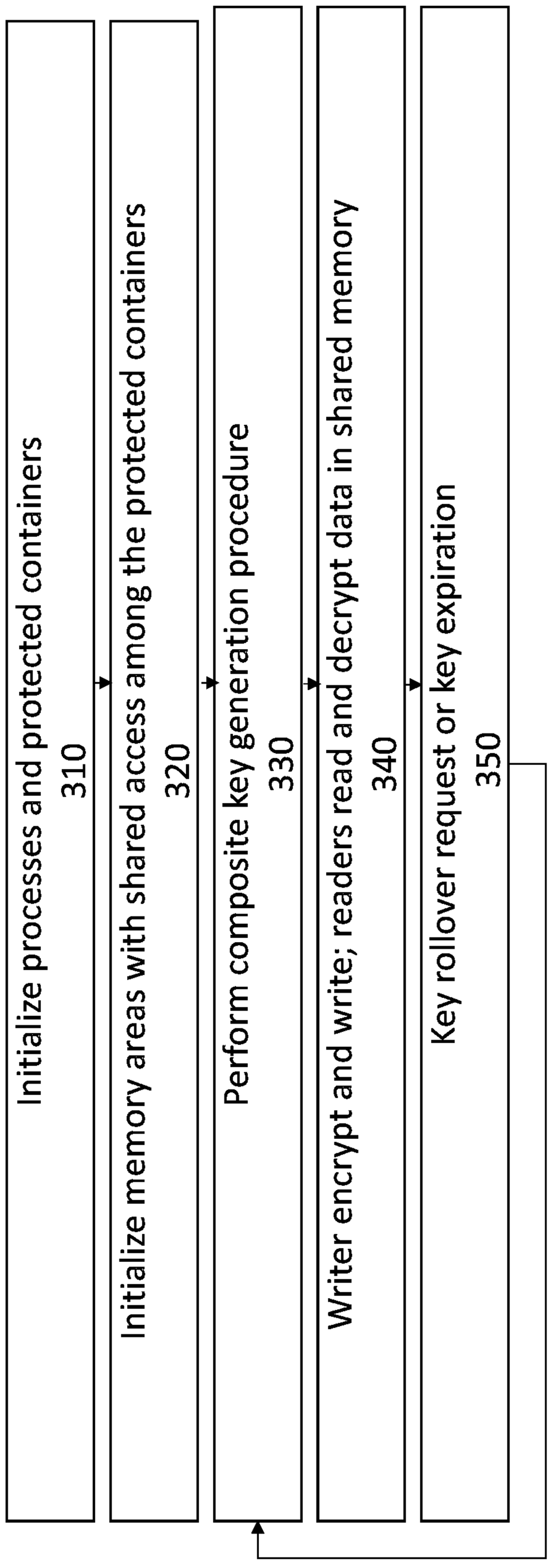

Initialize processes and protected containers
310
Initialize memory areas with shared access among the protected containers
320
Perform composite key generation procedure
330
Writer encrypt and write; readers read and decrypt data in shared memory
340
Key rollover request or key expiration
350

Fig. 3

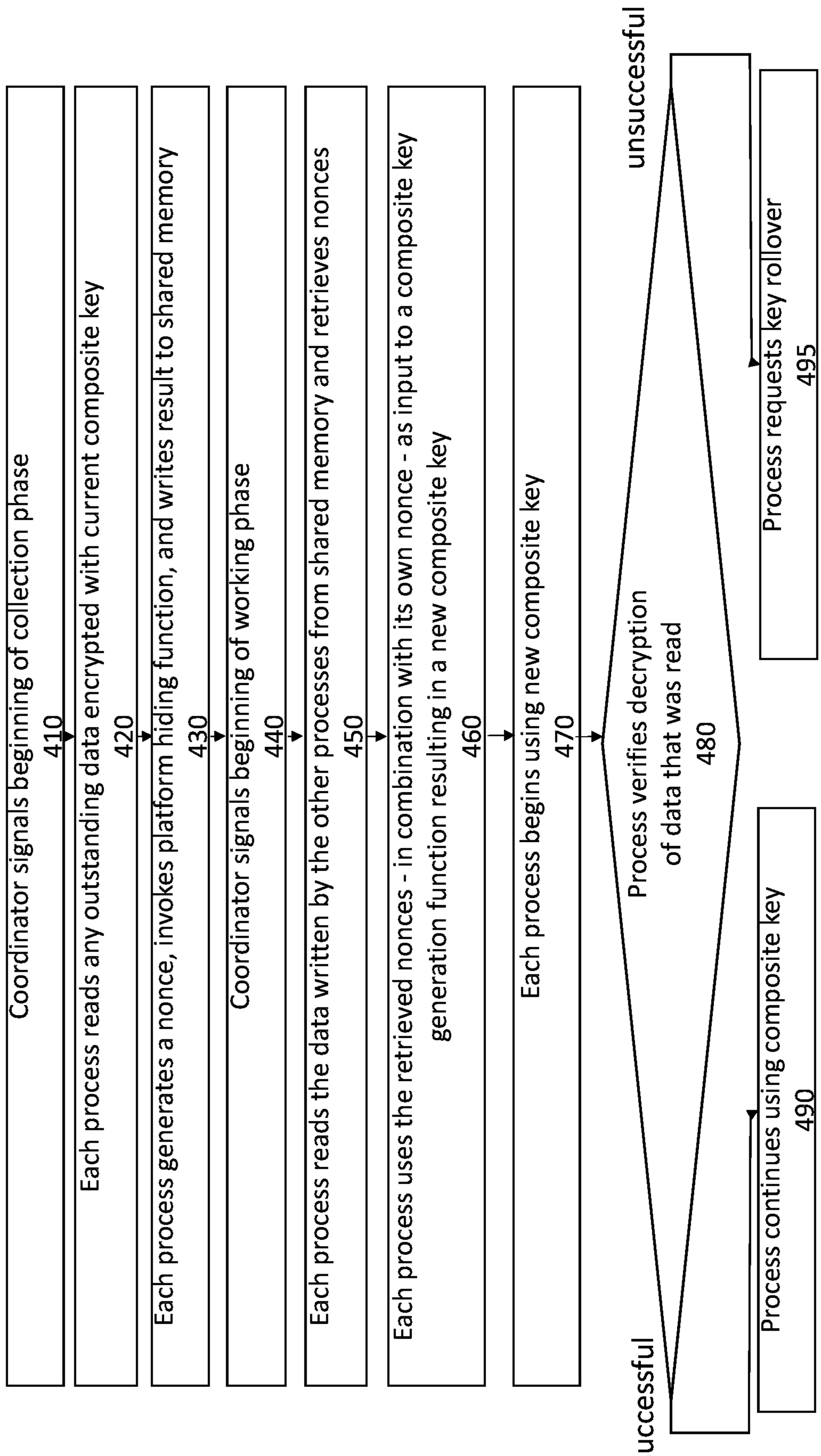

Coordinator signals beginning of collection phase
410
Each process reads any outstanding data encrypted with current composite key
420
Each process generates a nonce, invokes platform hiding function, and writes result to shared memory
430
Coordinator signals beginning of working phase
440
Each process reads the data written by the other processes from shared memory and retrieves nonces
450
Each process uses the retrieved nonces - in combination with its own nonce - as input to a composite key generation function resulting in a new composite key
460
Each process begins using new composite key
470
Process verifies decryption of data that was read
480
unsuccessful
Process requests key rollover
495
successful
Process continues using composite key
490

Fig. 4