

funds for each user involved in the split-payment transaction (e.g., amounts of funds to be credited and/or debited from an account of the respective user, if approved by the respective user).

[0096] In some non-limiting embodiments or aspects, transaction service provider system 102 may receive a split-payment request message that is encrypted with the secret key (e.g., the message itself is encrypted with the secret key and/or the message includes data that is encrypted with the secret key). For example, transaction service provider system 102 may receive the split-payment request message from user device 106 and/or user device 108, where the split-payment message is encrypted by user device 106 or user device 108 using the secret key, respectively. In another example, transaction service provider system 102 may receive the split-payment request message from user device 106 and/or user device 108, where encrypted data included in the split-payment request message is encrypted by user device 106 and/or user device 108 using the secret key, respectively. In such an example, the encrypted data encrypted by user device 106 and/or user device 108 may be associated with one or more values (e.g., a value of an amount of funds associated with the user of user device 106 and/or user device 108, the values of one or more other users involved in the split-payment transactions, and/or the like).

[0097] As shown in FIG. 2, at step 206, process 200 may include generating an encrypted balance. For example, transaction service provider system 102 may generate an encrypted balance. In such an example, transaction service provider system 102 may generate the encrypted balance for a requesting user (e.g., a first user and/or a second user) associated with user device 106 and/or a responding user (e.g., a second user and/or a first user) associated with user device 108. In some non-limiting embodiments or aspects, transaction service provider system 102 may generate the encrypted balance based on the split-payment request message. For example, transaction service provider system 102 may generate the encrypted balance based on the split-payment request message and/or the encrypted data included in the split payment request message.

[0098] In some non-limiting embodiments or aspects, transaction service provider system 102 may generate the encrypted balance without transaction service provider system 102 having access to the secret key. For example, transaction service provider system 102 may generate the encrypted balance based on the split-payment request message, the encrypted data included in the split-payment request message. For

whether the communication from the other of user device 106 or user device 108 and/or transaction service provider system 102 is genuine or malicious).

[0111] Referring now to FIG. 3, illustrated is a diagram of an implementation 300 of a process for maintaining user privacy in group transactions according to a non-limiting embodiment or aspect. As illustrated in FIG. 3, implementation 300 may include transaction service provider system 302, user device 306, and user device 308. Transaction service provider system 302 may be the same as, or similar to, transaction service provider system 102, user device 306 may be the same as, or similar to, user device 106, and/or user device 308 may be the same as, or similar to, user device 108 (see FIG. 1).

[0112] As shown by reference number 310 in FIG. 3, user device 306 may communicate with transaction service provider system 302 to establish a secret key. For example, user device 306 may communicate with transaction service provider system 302 to establish a secret key with user device 308. In such an example, user device 306 may receive and encrypt data with a public key of user device 308. As a result, security may be maintained in that transaction service provider system 302 does not have access to the private key of user device 308 to decrypt communications between user device 306 and user device 308. A secret symmetric key inaccessible to the transaction service provider system 302 may also be established and shared. A secret key may be established by being generated for each group, transaction, or user, and/or may be identified from a key exchange.

[0113] As shown by reference number 312 in FIG. 3, user device 308 may communicate with transaction service provider system 302 to establish a secret key. For example, user device 308 may communicate with transaction service provider system 302 to establish a secret key with user device 306. In such an example, user device 308 may receive and encrypt data with a public key of user device 306.

[0114] As shown by reference number 314 in FIG. 3, user device 306 may transmit a split-payment request message to transaction service provider system 302. For example, user device 306 may transmit a split-payment request message to transaction service provider system 302, the split-payment request message including encrypted data associated with a split-payment transaction. In such an example, the split-payment transaction may represent a request that a responding user associated with user device 308 agrees to transmit an amount of funds from an account

unit (APU), etc.), a microprocessor, a digital signal processor (DSP), and/or any processing component (e.g., a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), etc.) that can be programmed to perform a function. Memory 606 may include random access memory (RAM), read-only memory (ROM), and/or another type of dynamic or static storage device (e.g., flash memory, magnetic memory, optical memory, etc.) that stores information and/or instructions for use by processor 604.

[0167] Storage component 608 may store information and/or software related to the operation and use of device 600. For example, storage component 608 may include a hard disk (e.g., a magnetic disk, an optical disk, a magneto-optic disk, a solid state disk, etc.), a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a cartridge, a magnetic tape, and/or another type of computer-readable medium, along with a corresponding drive.

[0168] Input component 610 may include a component that permits device 600 to receive information, such as via user input (e.g., a touchscreen display, a keyboard, a keypad, a mouse, a button, a switch, a microphone, a camera, etc.). Additionally or alternatively, input component 610 may include a sensor for sensing information (e.g., a global positioning system (GPS) component, an accelerometer, a gyroscope, an actuator, etc.). Output component 612 may include a component that provides output information from device 600 (e.g., a display, a speaker, one or more light-emitting diodes (LEDs), etc.).

[0169] Communication interface 614 may include a transceiver-like component (e.g., a transceiver, a separate receiver and transmitter, etc.) that enables device 600 to communicate with other devices, such as via a wired connection, a wireless connection, or a combination of wired and wireless connections. Communication interface 614 may permit device 600 to receive information from another device and/or provide information to another device. For example, communication interface 614 may include an Ethernet interface, an optical interface, a coaxial interface, an infrared interface, a radio frequency (RF) interface, a universal serial bus (USB) interface, a Wi-Fi® interface, a cellular network interface, and/or the like.

[0170] Device 600 may perform one or more processes described herein. Device 600 may perform these processes based on processor 604 executing software instructions stored by a computer-readable medium, such as memory 606 and/or storage component 608. A computer-readable medium (e.g., a non-transitory