WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

generating, with a point-of-sale (POS) terminal, a first ciphertext associated with a transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with a randomly selected key (r), the first ciphertext value encrypted based on the randomly selected key (r) and a generator value (g); and

(ii) a second ciphertext value associated with a first public key (pk_1) of a first pair of keys comprising ~~a~~the first public key (pk_1) and a first secret key (sk_1), the first public key (pk_1) generated based on the first secret key (sk_1) and the generator value (g), the second ciphertext value encrypted based on transaction data associated with the transaction and a symmetric key (K) generated based on the first public key (pk_1) and the randomly selected key (r);

communicating, with the POS terminal, the first ciphertext to at least one payment gateway;

re-encrypting, with the at least one payment gateway, the first ciphertext value with a first re-encryption key to transform the first ciphertext value ~~encrypted under the first public key (pk_1)~~ to a re-encrypted first ciphertext value encrypted under a second public key (pk_2) associated with the at least one payment gateway;

communicating, with the at least one payment gateway, the re-encrypted first ciphertext value and the second ciphertext value to at least one merchant bank;

re-encrypting, with the at least one merchant bank, the re-encrypted first ciphertext value encrypted with a second re-encryption key to transform the re-encrypted first ciphertext value encrypted under the second public key (pk_2) of the at least one payment gateway to a second re-encrypted first ciphertext value under a third public key (pk_3) of the at least one merchant bank;

communicating, with the at least one merchant bank, the second re-encrypted first ciphertext value and the second ciphertext value to a payment network;

re-encrypting, with the payment network, the second re-encrypted first ciphertext value encrypted with a third re-encryption key to transform the second re-encrypted first ciphertext value encrypted under the third public key (pk_3) of the at least one merchant bank to a third re-encrypted first ciphertext value under a fourth public key (pk_4) of the payment network;

communicating, with the payment network, the third re-encrypted first ciphertext value and the second ciphertext value to at least one consumer bank;

determining, with the at least one consumer bank, the symmetric key (K) based on the third re-encrypted first ciphertext value and a secret key of the consumer bank; and

decrypting, with the at least one consumer bank, the second ciphertext value based on the symmetric key (K) to obtain the transaction data.

2. The computer-implemented method of claim 1, wherein an intermediary server translates between multiple different parties by decrypting the second ciphertext value and using a portion of the transaction data to determine routing and a corresponding re-encryption key for a subsequent communication.

3. The computer-implemented method of claim 1, wherein the transaction data includes at least one of a mobile personal identification number (PIN), a card verification number, or a card number associated therewith.

4. The computer-implemented method of claim 1, wherein the second ciphertext value is used to encrypt a personal identification number (PIN) under the randomly selected key (r) protected by the first ciphertext value, and wherein a re-encryption generates a new ciphertext value while the second ciphertext value is unchanged.

5. A system comprising:

a point-of-sale (POS) terminal including one or more processors, wherein the POS terminal is programmed and/or configured to:

generate a first ciphertext associated with a transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with a randomly selected key (r), the first ciphertext value encrypted based on the randomly selected key (r) and a generator value (g); and

(ii) a second ciphertext value associated with a first public key (pk_1) of a first pair of keys comprising ~~a~~the first public key (pk_1) and a first secret key (sk_1), the first public key (pk_1) generated based on the

first secret key (sk_1) and the generator value (g), the second ciphertext value encrypted based on transaction data associated with the transaction and a symmetric key (K) generated based on the first public key (pk_1) and the randomly selected key (r); and

communicate the first ciphertext to at least one payment gateway;

the at least one payment gateway including one or more processors, wherein the at least one payment gateway is programmed and/or configured to:

re-encrypt the first ciphertext value with a first re-encryption key to transform the first ciphertext value ~~encrypted under the first public key (pk_1)~~ to a re-encrypted first ciphertext value encrypted under a second public key (pk_2) associated with the at least one payment gateway; and

communicate the re-encrypted first ciphertext value and the second ciphertext value to at least one merchant bank;

the at least one merchant bank including one or more processors, wherein the at least one merchant bank is programmed and/or configured to:

re-encrypt the re-encrypted first ciphertext value encrypted with a second re-encryption key to transform the re-encrypted first ciphertext value encrypted under the second public key (pk_2) of the at least one payment gateway to a second re-encrypted first ciphertext value under a third public key (pk_3) of the at least one merchant bank; and

communicate the second re-encrypted first ciphertext value and the second ciphertext value to a payment network;

the payment network including one or more processors, wherein the payment network is programmed and/or configured to:

re-encrypt the second re-encrypted first ciphertext value encrypted with a third re-encryption key to transform the second re-encrypted first ciphertext value encrypted under the third public key (pk_3) of the at least one merchant bank to a third re-encrypted first ciphertext value under a fourth public key (pk_4) of the payment network; and

communicate the third re-encrypted first ciphertext value and the second ciphertext value to at least one consumer bank; and

the at least one consumer bank including one or more processors, wherein the at least one consumer bank is programmed and/or configured to:

determine the symmetric key (K) based on the third re-encrypted first ciphertext value and a secret key of the consumer bank; and

decrypt the second ciphertext value based on the symmetric key (K) to obtain the transaction data.

6. The system of claim 5, further comprising:

an intermediary server programmed and/or configured to translate between multiple different parties by decrypting the second ciphertext value and using a portion of the transaction data to determine routing and a corresponding re-encryption key for a subsequent communication.

7. The system of claim 5, wherein the transaction data includes at least one of a mobile personal identification number (PIN), a card verification number, or a card number associated therewith.

8. The system of claim 5, wherein the second ciphertext value is used to encrypt a personal identification number (PIN) under the randomly selected key (r) protected by the first ciphertext value, and wherein a re-encryption generates a new ciphertext value while the second ciphertext value is unchanged.

9. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

generate, with a point-of-sale (POS) terminal, a first ciphertext associated with a transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with a randomly selected key (r), the first ciphertext value encrypted based on the randomly selected key (r) and a generator value (g); and

(ii) a second ciphertext value associated with a first public key (pk_1) of a first pair of keys comprising ~~a~~the first public key (pk_1) and a first secret key (sk_1), the first public key (pk_1) generated based on the first secret key (sk_1) and the generator value (g), the second ciphertext value encrypted based on transaction data associated with the transaction and a symmetric key (K) generated based on the first public key (pk_1) and the randomly selected key (r);

communicate, with the POS terminal, the first ciphertext to at least one payment gateway;

re-encrypt, with the at least one payment gateway, the first ciphertext value with a first re-encryption key to transform the first ciphertext value ~~encrypted under the first public key (pk_1)~~ to a re-encrypted first ciphertext value encrypted under a second public key (pk_2) associated with the at least one payment gateway;

communicate, with the at least one payment gateway, the re-encrypted first ciphertext value and the second ciphertext value to at least one merchant bank;

re-encrypt, with the at least one merchant bank, the re-encrypted first ciphertext value encrypted with a second re-encryption key to transform the re-encrypted first ciphertext value encrypted under the second public key (pk_2) of the at least one payment gateway to a second re-encrypted first ciphertext value under a third public key (pk_3) of the at least one merchant bank;

communicate, with the at least one merchant bank, the second re-encrypted first ciphertext value and the second ciphertext value to a payment network;

re-encrypt, with the payment network, the second re-encrypted first ciphertext value encrypted with a third re-encryption key to transform the second re-encrypted first ciphertext value encrypted under the third public key (pk_3) of the at least one merchant bank to a third re-encrypted first ciphertext value under a fourth public key (pk_4) of the payment network;

communicate, with the payment network, the third re-encrypted first ciphertext value and the second ciphertext value to at least one consumer bank;

determine, with the at least one consumer bank, the symmetric key (K) based on the third re-encrypted first ciphertext value and a secret key of the consumer bank; and

decrypt, with the at least one consumer bank, the second ciphertext value based on the symmetric key (K) to obtain the transaction data.

10. The computer program product of claim 9, wherein an intermediary server translates between multiple different parties by decrypting the second ciphertext value and using a portion of the transaction data to determine routing and a corresponding re-encryption key for a subsequent communication.

11. The computer program product of claim 9, wherein the transaction data includes at least one of a mobile personal identification number (PIN), a card verification number, or a card number associated therewith.

12. The computer program product of claim 9, wherein the second ciphertext value is used to encrypt a personal identification number (PIN) under the randomly selected key (r) protected by the first ciphertext value, and wherein a re-encryption generates a new ciphertext value while the second ciphertext value is unchanged.