WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

generating, with a payment network, a first value (a) and a second value (g^a), the second value (g^a) generated based on the first value (a) and a generator value (g);

generating, with the payment network, a plurality of random merchant numbers (m_i) for a respective plurality of merchant banks;

determining, with the payment network, a merchant product (M) based on a product of the plurality of random merchant numbers (m_i) for the respective plurality of merchant banks;

generating, with the payment network, a public key (pk_i) based on the second value (g^a), the merchant product (M), and the random merchant number (m_i) and a random key (rk_i) based on the merchant product (M) and the random merchant number (m_i) for each respective merchant bank of the plurality of merchant banks; and

communicating, with the payment network, the public key (pk_i) and the random key (rk_i) to at least one respective merchant bank;

generating, with the merchant bank, a plurality of random payment gateway numbers (p_i) for a respective plurality of payment gateways;

generating, with the merchant bank, a payment gateway public key based on the second value (g^a), the merchant product (M), and the random payment gateway number (p_i) and a payment gateway random key based on the random payment gateway number (p_i) for each respective payment gateway of the plurality of payment gateways;

generating, with the merchant bank, a plurality of terminal numbers (t_i) for a respective plurality of point-of-sale (POS) terminals;

generating, with the merchant bank, a terminal public key based on the second value (g^a), the merchant product (M), the random payment gateway number (p_i), and the terminal number (t_i) and a terminal random key based on the random payment gateway number (p_i) and the terminal number (t_i) for each respective POS terminal of the plurality of POS terminals;

generating, with the at least one POS terminal, a random number (r) for a transaction message (m) associated with a transaction;

generating, with the at least one POS terminal, a first ciphertext associated with the transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with the transaction message (m), the first ciphertext value encrypted based on the random number (r), the generator value (g), and the transaction message (m); and

ii) a second ciphertext value associated with the random number (r), the second ciphertext value encrypted based on the random number (r) and the terminal public key; and

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

~~2. The computer-implemented method of claim 1, further comprising:~~

~~generating, with the merchant bank, a plurality of random payment gateway numbers (p_i) for a respective plurality of payment gateways; and~~

~~generating, with the merchant bank, a payment gateway public key based on the second value (g^a), the merchant product (M), and the random payment gateway number (p_i) and a payment gateway random key based on the random payment gateway number (p_i) for each respective payment gateway of the plurality of payment gateways.~~

~~3. The computer-implemented method of claim 2, further comprising:~~

~~generating, with the merchant bank, a plurality of terminal numbers (t_i) for a respective plurality of point-of-sale (POS) terminals; and~~

~~generating, with the merchant bank, a terminal public key based on the second value (g^a), the merchant product (M), the random payment gateway number (p_i), and the terminal number (t_i) and a terminal random key based on the random payment gateway number (p_i) and the terminal number (t_i) for each respective POS terminal of the plurality of POS terminals.~~

4~~3~~2. The computer-implemented method of claim 1~~3~~, further comprising:

communicating, with the merchant bank, the terminal public key and the terminal random key to at least one payment gateway; and

communicating, with the at least one payment gateway, the terminal public key to at least one POS terminal.

~~5. The computer-implemented method of claim 4, further comprising:~~

~~generating, with the at least one POS terminal, a random number (r) for a transaction message (m) associated with a transaction;~~

~~generating, with the at least one POS terminal, a first ciphertext associated with the transaction, the first ciphertext comprising:~~

~~(i) a first ciphertext value associated with the transaction message (m), the first ciphertext value encrypted based on the random number (r), a generator value (g), and the transaction message (m); and~~

~~ii) a second ciphertext value associated with the random number (r), the second ciphertext value encrypted based on the random number (r) and the terminal public key; and~~

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

~~6~~3. The computer-implemented method of claim ~~5~~1, further comprising:

re-encrypting, with the at least one payment gateway, the second ciphertext value based on the terminal random key to transform the second ciphertext value to a re-encrypted second ciphertext value based on the second value (g^a), the merchant product (M), and the random number (r); and

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

~~7~~4. The computer-implemented method of claim ~~6~~3, further comprising:

re-encrypting, with the at least one merchant bank, the re-encrypted second ciphertext value based on the random key (rk_i) to transform the re-encrypted second ciphertext value to a second re-encrypted second ciphertext value based on the second value (g^a), the merchant product (M), the ~~merchant~~ random merchant number (m_i), and the random number (r); and

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

~~8~~5. The computer-implemented method of claim ~~7~~4, further comprising:

decrypting, with the payment network, the first ciphertext value based on the second re-encrypted second ciphertext value, the merchant product (M), the ~~merchant~~ random merchant number (m_i), and the first ciphertext value.

~~9~~6. A system, comprising:

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

generate a first value (a) and a second value (g^a), the second value (g^a) generated based on the first value (a) and a generator value (g);

generate a plurality of random merchant numbers (m_i) for a respective plurality of merchant banks;

determine a merchant product (M) based on a product of the plurality of random merchant numbers (m_i) for the respective plurality of merchant banks;

generate a public key (pk_i) based on the second value (g^a), the merchant product (M), and the random merchant number (m_i) and a random key (rk_i) based on the merchant product (M) and the random merchant number (m_i) for each respective merchant bank of the plurality of merchant banks; and

communicate the public key (pk_i) and the random key (rk_i) to at least one respective merchant bank,

wherein the merchant bank includes one or more processors,

wherein the merchant bank is programmed and/or configured to:

generate a plurality of random payment gateway numbers (p_i) for a respective plurality of payment gateways;

generate a payment gateway public key based on the second value (g^a), the merchant product (M), and the random payment gateway number (p_i) and a payment gateway random key based on the random payment gateway number (p_i) for each respective payment gateway of the plurality of payment gateways,

generate a plurality of terminal numbers (t_i) for a respective plurality of point-of-sale (POS) terminals; and

generate a terminal public key based on the second value (g^a), the merchant product (M), the random payment gateway number (p_i), and the

terminal number (t_i) and a terminal random key based on the random payment gateway number (p_i) and the terminal number (t_i) for each respective POS terminal of the plurality of POS terminals,

wherein the at least one POS terminal includes one or more processors, and

wherein the at least one POS terminal is programmed and/or configured to:

generate a random number (r) for a transaction message (m) associated with a transaction;

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

(i) a first ciphertext value associated with the transaction message (m), the first ciphertext value encrypted based on the random number (r), the generator value (g), and the transaction message (m); and

ii) a second ciphertext value associated with the random number (r), the second ciphertext value encrypted based on the random number (r) and the terminal public key; and

communicate the first ciphertext to the at least one payment gateway.

~~10. The system of claim 9, wherein the merchant bank includes one or more processors, and~~

~~wherein the merchant bank is programmed and/or configured to:~~

~~generate a plurality of random payment gateway numbers (p_i) for a respective plurality of payment gateways; and~~

~~generate a payment gateway public key based on the second value (g^a), the merchant product (M), and the random payment gateway number (p_i) and a payment gateway random key based on the random payment gateway number (p_i) for each respective payment gateway of the plurality of payment gateways.~~

~~11. The system of claim 10, wherein the merchant bank is further programmed and/or configured to:~~

~~generate a plurality of terminal numbers (t_i) for a respective plurality of point-of-sale (POS) terminals; and~~

~~generate a terminal public key based on the second value (g^a), the merchant product (M), the random payment gateway number (p_i), and the terminal number (t_i) and a terminal random key based on the random payment gateway number (p_i) and the terminal number (t_i) for each respective POS terminal of the plurality of POS terminals.~~

~~12~~7. The system of claim ~~11~~6, wherein the merchant bank is further programmed and/or configured to:

communicate the terminal public key and the terminal random key to at least one payment gateway,

wherein the at least one payment gateway includes one or more processors, and

wherein the at least one payment gateway is programmed and/or configured to:

communicate the terminal public key to at least one POS terminal.

~~13. The computer-implemented method of claim 12, wherein the at least one POS terminal includes one or more processors, and~~

~~wherein the at least one POS terminal is programmed and/or configured to:~~

~~generate a random number (r) for a transaction message (m) associated with a transaction;~~

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

~~(i) a first ciphertext value associated with the transaction message (m), the first ciphertext value encrypted based on the random number (r), a generator value (g), and the transaction message (m); and~~

~~ii) a second ciphertext value associated with the random number (r), the second ciphertext value encrypted based on the random number (r) and the terminal public key; and~~

~~communicate the first ciphertext to the at least one payment gateway.~~

~~14~~8. The ~~computer-implemented method~~ system of claim ~~13~~6, wherein the at least one payment gateway is further programmed and/or configured to:

re-encrypt the second ciphertext value based on the terminal random key to transform the second ciphertext value to a re-encrypted second ciphertext value based on the second value (g^a), the merchant product (M), and the random number (r); and

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

wherein the at least one merchant bank is further programmed and/or configured to:

re-encrypt the re-encrypted second ciphertext value based on the random key (rk_i) to transform the re-encrypted second ciphertext value to a second re-encrypted second ciphertext value based on the second value (g^a), the merchant product (M), the ~~merchant~~ random merchant number (m_i), and the random number (r); and

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

wherein the payment network is further programmed and/or configured to:

decrypt the first ciphertext value based on the second re-encrypted second ciphertext value, the merchant product (M), the ~~merchant~~ random merchant number (m_i), and the first ciphertext value.

~~15~~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 payment network, a first value (a) and a second value (g^a), the second value (g^a) generated based on the first value (a) and a generator value (g);

generate, with the payment network, a plurality of random merchant numbers (m_i) for a respective plurality of merchant banks;

determine, with the payment network, a merchant product (M) based on a product of the plurality of random merchant numbers (m_i) for the respective plurality of merchant banks;

generate, with the payment network, a public key (pk_i) based on the second value (g^a), the merchant product (M), and the random merchant number (m_i) and a random key (rk_i) based on the merchant product (M) and the random merchant number (m_i) for each respective merchant bank of the plurality of merchant banks; and

communicate, with the payment network, the public key (pk_i) and the random key (rk_i) to at least one respective merchant bank;

generate, with the merchant bank, a plurality of random payment gateway numbers (p_i) for a respective plurality of payment gateways;

generate, with the merchant bank, a payment gateway public key based on the second value (g^a), the merchant product (M), and the random payment gateway number (p_i) and a payment gateway random key based on the random payment gateway number (p_i) for each respective payment gateway of the plurality of payment gateways;

generate, with the merchant bank, a plurality of terminal numbers (t_i) for a respective plurality of point-of-sale (POS) terminals;

generate, with the merchant bank, a terminal public key based on the second value (g^a), the merchant product (M), the random payment gateway number (p_i), and the terminal number (t_i) and a terminal random key based on the random payment gateway number (p_i) and the terminal number (t_i) for each respective POS terminal of the plurality of POS terminals;

generate, with the at least one POS terminal, a random number (r) for a transaction message (m) associated with a transaction;

generate, with the at least one POS terminal, a first ciphertext associated with the transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with the transaction message (m), the first ciphertext value encrypted based on the random number (r), the generator value (g), and the transaction message (m); and

ii) a second ciphertext value associated with the random number (r), the second ciphertext value encrypted based on the random number (r) and the terminal public key; and

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

~~16. The computer program product of claim 15, wherein the instructions further cause the at least one processor to:~~

~~generate, with the merchant bank, a plurality of random payment gateway numbers (p_i) for a respective plurality of payment gateways; and~~

~~generate, with the merchant bank, a payment gateway public key based on the second value (g^a), the merchant product (M), and the random payment gateway number (p_i) and a payment gateway random key based on the random payment gateway number (p_i) for each respective payment gateway of the plurality of payment gateways.~~

~~17. The computer program product of claim 16, wherein the instructions further cause the at least one processor to:~~

~~generate, with the merchant bank, a plurality of terminal numbers (t_i) for a respective plurality of point-of-sale (POS) terminals; and~~

~~generate, with the merchant bank, a terminal public key based on the second value (g^a), the merchant product (M), the random payment gateway number (p_i), and the terminal number (t_i) and a terminal random key based on the random payment gateway number (p_i) and the terminal number (t_i) for each respective POS terminal of the plurality of POS terminals.~~

~~18~~10. The computer program product of claim ~~17~~9, wherein the instructions further cause the at least one processor to:

communicate, with the merchant bank, the terminal public key and the terminal random key to at least one payment gateway; and

communicate, with the at least one payment gateway, the terminal public key to at least one POS terminal.

~~19. The computer program product of claim 18, wherein the instructions further cause the at least one processor to:~~

~~generate, with the at least one POS terminal, a random number (r) for a transaction message (m) associated with a transaction;~~

~~generate, with the at least one POS terminal, a first ciphertext associated with the transaction, the first ciphertext comprising:~~

~~(i) a first ciphertext value associated with the transaction message (m), the first ciphertext value encrypted based on the random number (r), a generator value (g), and the transaction message (m); and~~

~~ii) a second ciphertext value associated with the random number (r), the second ciphertext value encrypted based on the random number (r) and the terminal public key; and~~

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

~~20~~11. The computer program product of claim ~~19~~, wherein the instructions further cause the at least one processor to:

re-encrypt, with the at least one payment gateway, the second ciphertext value based on the terminal random key to transform the second ciphertext value to a re-encrypted second ciphertext value based on the second value (g^a), the merchant product (M), and the random number (r); and

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

wherein the instructions further cause the at least one processor to:

re-encrypt, with the at least one merchant bank, the re-encrypted second ciphertext value based on the random key (rk_i) to transform the re-encrypted second ciphertext value to a second re-encrypted second ciphertext value based on the second value (g^a), the merchant product (M), the ~~merchant~~ random merchant number (m_i), and the random number (r); and

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

wherein the instructions further cause the at least one processor to:

decrypt, with the payment network, the first ciphertext value based on the second re-encrypted second ciphertext value, the merchant product (M), the ~~merchant~~ random merchant number (m_i), and the first ciphertext value.