WHAT IS CLAIMED IS:

1. A method for securely transmitting and extracting information from encrypted data without fully decrypting the data, comprising:

receiving a data request, with at least a portion of the data request encrypted according to a homomorphic encryption scheme, and the encrypted portion of the data request comprising at least a set of confidential data;

retrieving one or more sets of encrypted comparison data from a database, each set of encrypted comparison data encrypted according to a homomorphic encryption scheme;

comparing the encrypted set of confidential data from the data request with each set of encrypted comparison data using one or more homomorphic operations to determine which set of encrypted comparison data matches the encrypted set of confidential data and validating the set of confidential data upon a match;

generating an encrypted indicator indicating success or failure of validating the set of confidential data; and

forwarding the encrypted indicator to a party associated with the data request,

wherein the set of confidential data is never decrypted during the method.

2. The method of claim 1, wherein the set of confidential data is from one of: an identity card, a passport, a driver's license, a security card, a bank card, a credit card, and a health card.

3. The method of claim 1, wherein the encrypted indicator is sent to a party different from the party the data request was received from.

4. A data system comprising:

a network interface for connecting to a network to receive homomorphically encrypted data from a plurality of remote data devices, wherein the homomorphically encrypted data is associated with users associated with the remote data devices; and

a calculation engine connected to the network interface, the calculation engine configured to perform homomorphic calculations on the data to obtain calculation results that can be selectively decrypted.

5. The system of claim 4, wherein the calculation engine is configured to perform a relational operation.

6. A device for performing homomorphic calculations, the device comprising a memory and at least one processor, the device configured to model a homomorphic calculation as a polynomial series and to compute a value of the polynomial series using encrypted data to obtain an encrypted result, the encrypted data being encrypted according to an encryption scheme, the device further configured to perform a homomorphic relational operation to compare the encrypted result with an encrypted condition, the encrypted condition being encrypted according to the encryption scheme, the device further configured to output a result of the comparison.

7. The device of claim 6, comprising at least one graphics processing unit (GPU).

8. The device of claim 6, configured to implement Chinese Remainder Theorem (CRT), Number Theoretic Transform (NTT), one or more memory blocks, one or more memory interfaces, matrix multiplications, matrix additions, or a combination of such.

9. A method of processing a secure financial transaction, comprising:

receiving an at least partially homomorphically encrypted request to complete a financial transaction, which is homomorphically encrypted according to a lattice-based Fully Homomorphic Encryption (FHE) scheme, and the transaction request comprising confidential cardholder data including an account number, non-confidential cardholder data and transaction data;

retrieving one or more sets of homomorphically encrypted comparison cardholder data encrypted according to a lattice-based FHE scheme;

comparing the confidential cardholder data to each set of the comparison cardholder data using one or more homomorphic operations to determine which set of comparison cardholder data matches the confidential cardholder data and validating the confidential cardholder data;

generating and encrypting an indicator indicating authorization or rejection of the request to complete the financial transaction based upon at least the validation of the confidential cardholder data; and

forwarding the encrypted indicator indicating authorization or rejection of the request to complete the financial transaction to a party seeking authorization to complete the financial transaction,

wherein the confidential cardholder data is never decrypted during the method.

10. The method of claim 9, wherein the confidential cardholder data includes one or more of: a portion of the account number, the account number, an expiry date and a Card Verification Value (CVV) number.

11. The method of claim 9, wherein the non-confidential cardholder data includes one or more of: a bank name, a cardholder name, a Bank Identification Number (BIN) and the last four digits of the account number.

12. The method of claim 9, wherein the transaction data includes one or more of: a transaction amount, a transaction date and a merchant identifier.

13. The method of claim 9, further including executing a step of retrieving the transaction data and executing the step of comparing the transaction data using one or more homomorphic operations to determine whether the transaction amount can be authorized.

14. The method of claim 9, wherein the non-confidential cardholder data is encrypted using a public key wherein the public key is held by a party making the request to complete the financial transaction, and a private key is held by a party receiving the request to complete the financial transaction.

15. The method of claim 9, wherein the financial transaction is a credit card transaction.

16. The method of claim 9, wherein the request to complete the financial transaction is received by one or more of: a bank, a credit card company, a card issuer or a payment processor.

17. A method of performing a comparison with encrypted data, the method comprising:

modeling a calculation as a polynomial series;

computing a value of the polynomial series using encrypted data to obtain an encrypted result, the encrypted data being encrypted according to an encryption scheme;

performing a homomorphic relational operation to compare the encrypted result with an encrypted/non-encrypted condition, the encrypted condition being encrypted according to the encryption scheme; and

outputting a result of the comparison.

18. The method of claim 17, wherein the calculation is a medical calculation and the encrypted data is representative of measured physiological data of patients.

19. A system configured to perform the method of claim 17.

20. A medical data system comprising:

a network interface for connecting to a network to receive homomorphically encrypted data from a plurality of remote medical devices, wherein the homomorphically encrypted data is representative of measured physiological data of patients associated with the remote medical devices; and

a calculation engine connected to the network interface, the calculation engine configured to perform homomorphic calculations on the data to obtain calculation results that can be selectively decrypted.