WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, by a remote data storage service, a request for data stored as encrypted data by the remote data storage service, the request initiated by a first entity;

transmitting, to a first multi-party computation (MPC) server controlled by the first entity, an MPC request;

receiving an MPC response from the first MPC server including a secret generated by a secure cryptoprocessor; [[and]]

decrypting, by the remote data storage service, the stored encrypted data based at least partially on the MPC response from the first entity, wherein decrypting the stored encrypted data further comprises:

determining a derived key associated with the first entity, the remote data storage service, and the secret; and

determining a master key by decrypting the stored encrypted data in the remote data storage service with the derived key, wherein decryption of the stored encrypted data is based on receiving the secret generated by the secure cryptoprocessor, and

decrypting, by the remote data storage service with the master key, data hosted by the remote data storage service associated with the first entity.

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

receiving, from a second MPC server controlled by the remote data storage service, a second MPC response, wherein the stored encrypted data is decrypted based at least partially on the second MPC response.

3. The computer-implemented method of claim 2, wherein the MPC request is transmitted to the first MPC server in response to receiving the second MPC response.

4. The computer-implemented method of claim 3, wherein the MPC request is transmitted by the second MPC server to the first MPC server.

5. The computer-implemented method of claim 1, wherein the stored encrypted data is decrypted within a predetermined period without revealing any information about the MPC request or the MPC response, and wherein the MPC response is configured to remain active for a period not exceeding the predetermined period to minimize exposure.

6. The computer-implemented method of claim 1, wherein the secret includes a key, a code, a token, a pin, a computation, or a password, and the method further comprises receiving, from a second MPC server controlled by one of a transaction terminal, an issuer bank, or an acquirer bank, a second MPC response, wherein the stored encrypted data is decrypted based at least partially on the second MPC response.

7. The computer-implemented method of claim 1, wherein the remote data storage service is configured to decrypt based on a predetermined number of MPC responses of the first entity, wherein the method further comprises:

transmitting one or more MPC requests to a plurality of MPC servers associated with the first entity; and

determining an MPC after receiving one or more MPC responses from the plurality of MPC servers, wherein the stored encrypted data is decrypted based on the received MPC responses satisfying the predetermined number of MPC responses.

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

determining, by the first entity, whether to prevent the remote data storage service from decrypting the stored encrypted data of the first entity; and

blocking at least one of a subsequent MPC request from the remote data storage service, a subsequent MPC response to the remote data storage service, or a connection between the remote data storage service and an MPC server of the first entity to prevent decryption.

9. The computer-implemented method of claim 1, wherein the secret is wrapped with a transient layer of encryption based on a transient key while being generated by the secure cryptoprocessor.

10. A system for secure key management, comprising:

at least one processor programmed or configured to:

receive, by a remote data storage service, a request for data stored as encrypted data by the remote data storage service, the request initiated by a first entity;

transmit, to a first multi-party computation (MPC) server controlled by the first entity, an MPC request;

receive an MPC response from the first MPC server including at least a secret generated by a secure cryptoprocessor; and

decrypt, by the remote data storage service, the stored encrypted data based at least partially on the MPC response, wherein the remote data storage service decrypts the stored encrypted data by:

determining a derived key associated with the first entity, the remote data storage service, and the secret; and

determining a master key by decrypting the stored encrypted data in the remote data storage service with the derived key, wherein decryption of the stored encrypted data is based on receiving the secret generated by the secure cryptoprocessor, and

decrypt, by the remote data storage service with the master key, data hosted by the remote data storage service associated with the first entity.

11. The system for secure key management of claim 10, wherein the at least one processor is further programmed or configured to:

receive, from a second MPC server controlled by the remote data storage service, a second MPC response, wherein the stored encrypted data is decrypted based at least partially on the second MPC response.

12. The system for secure key management of claim 11, wherein the MPC request is transmitted to the first MPC server in response to receiving the second MPC response.

13. The system for secure key management of claim 12, wherein the MPC request is transmitted by the second MPC server to the first MPC server.

14. The system for secure key management of claim 10, wherein the stored encrypted data is decrypted within a predetermined period without revealing any information about the MPC request or the MPC response, and wherein the MPC response is configured to remain active for a period not exceeding the predetermined period to minimize exposure.

15. The system for secure key management of claim 10, wherein the secret includes a key, a code, a token, a pin, a computation, or a password, and the system is further configured to receive, from a second MPC server controlled by one of a transaction terminal, an issuer bank, or an acquirer bank, a second MPC response, wherein the stored encrypted data is decrypted based at least partially on the second MPC response.

16. The system for secure key management of claim 10, further comprising the first MPC server, the first MPC server comprising a hardware security module configured to generate the MPC response in a secure cryptoprocessor.

17. The system for secure key management of claim 10, wherein the remote data storage service is configured to decrypt based on a predetermined number of MPC responses of the first entity, wherein the at least one processor is further programmed or configured to:

transmit one or more MPC requests to a plurality of MPC servers associated with the first entity; and

determine an MPC after receiving one or more MPC responses from the plurality of MPC servers, wherein the stored encrypted data is decrypted based on the received MPC responses satisfying the predetermined number of MPC responses.

18. A computer program product for secure key management comprising at least one non-transitory computer-readable medium including one or

more instructions that, when executed by at least one processor, cause the at least one processor to:

receive, by a remote data storage service, a request for data stored as encrypted data by the remote data storage service, the request initiated by a first entity;

transmit, to a first multi-party computation (MPC) server controlled by the first entity, an MPC request;

receive an MPC response from the first MPC server including a secret that is generated by a secure cryptoprocessor; and

decrypt, by the remote data storage service, the stored encrypted data based at least partially on the MPC response, wherein the at least one server computer decrypts the stored encrypted data by:

determining a derived key associated with a first entity, a second entity, and the secret generated by the secure cryptoprocessor; and

determining a master key by decrypting the stored encrypted data in the at least one server computer with the derived key, wherein decryption of the stored encrypted data is based on receiving the secret generated by the secure cryptoprocessor, and

decrypt, with the master key, data hosted by the at least one server computer associated with the first entity.

19. The computer program product for secure key management of claim 18, wherein the at least one processor is further programmed or configured to:

receive, from a second MPC server controlled by the remote data storage service, a second MPC response, wherein the stored encrypted data is decrypted based at least partially on the second MPC response.

20. The computer program product for secure key management of claim 19, wherein the MPC request is transmitted to the first MPC server in response to receiving the second MPC response.

21. The computer program product for secure key management of claim 20, wherein the MPC request is transmitted by the second MPC server to the first MPC server.

22. The computer program product for secure key management of claim 19 wherein the stored encrypted data includes a master key determined by the at least one processor decrypting the stored encrypted data with a derived key based on the MPC response and the second MPC response to determine a master key associated with the first entity in the remote data storage service.

23. The computer program product for secure key management of claim 18, wherein the stored encrypted data is decrypted within a predetermined period without revealing any information about the MPC request or the MPC response, and wherein the MPC response is configured to remain active for a period not exceeding the predetermined period to minimize exposure.

24. The computer program product for secure key management of claim 18, wherein the secret includes a key, a code, a token, a pin, a computation, or a password, and the computer program product is further configured to receive, from a second MPC server controlled by one of a transaction terminal, an issuer bank, or an acquirer bank, a second MPC response, wherein the stored encrypted data is decrypted based at least partially on the second MPC response.

25. The computer program product for secure key management of claim 18, further comprising the first MPC server, the first MPC server comprising a hardware security module configured to generate the MPC response in a secure cryptoprocessor.

26. The computer program product for secure key management of claim 18, wherein the remote data storage service is configured to decrypt based on a predetermined number of MPC responses of the first entity, wherein the at least one processor is further programmed or configured to:

transmit one or more MPC requests to a plurality of MPC servers associated with the first entity; and

determine an MPC after receiving one or more MPC responses from the plurality of MPC servers, wherein the stored encrypted data is decrypted based on the received MPC responses satisfying the predetermined number of MPC responses.

27. The computer program product for secure key management of claim 18, wherein the at least one processor is further programmed or configured to:

determine, by the first entity, whether to prevent the remote data storage service from decrypting the stored encrypted data by the first entity; and

block at least one of a subsequent MPC request from the remote data storage service, a subsequent MPC response to the remote data storage service, or a connection between the remote data storage service and an MPC server of the first entity.

28. The computer program product for secure key management of claim 18, wherein the secret is wrapped with a transient layer of encryption based on a transient key while being generated by the secure cryptoprocessor.

29. The computer program product for secure key management of claim 18, wherein the remote data storage service is configured to decrypt based on a predetermined number of MPC responses from an MPC server of a point-of-sale (POS) terminal, an MPC server of an issuer bank, an MPC server of a transaction handler, or an MPC server of an acquirer bank.