WHAT IS CLAIMED IS:

1. A method for performing a privacy-preserving multi-party computation, the method comprising performing, by a receiver device:

storing an input value b that is to be used in executing an encrypted program;

generating a first value r_{1-b} using a first random number generator;

generating a second value a using a second random number generator;

generating a hash output using a hash function of the first value r_{1-b};

generating a first public key corresponding to the second value a using a cryptographic function;

generating a third value r_b using the first public key and the hash output;

sending the first value r_{1-b} and the third value r_b to a sender device;

receiving a second public key c from the sender device, wherein the second public key c is generated using the cryptographic function;

generating, using the second public key c and the second value a, a key value that corresponds to the input value b;

receiving the encrypted program from the sender device;

executing the encrypted program using the key value to obtain an encrypted output value; and

sending the encrypted output value to the sender device, wherein the sender device decrypts the encrypted output value using the key value.

2. The method of claim 1, wherein the input value b is an element of a set of values associated with a number of possible keys.

3. The method of claim 1, wherein the hash function is a random oracle.

4. The method of claim 1, wherein the first value r_{1-b} has a same length in bits as the first public key.

5. The method of claim 1, wherein the hash output has a same length in bits as the first public key.

6. The method of claim 1, wherein generating the key value comprises raising the second public key c to a power of the second value a.

7. The method of claim 1, wherein generating the first public key using the cryptographic function comprises raising a value g to a power of the second value a to produce the first public key.

8. The method of claim 1, wherein a private key d used to generate the second public key c is generated by using the second random number generator.

9. The method of claim 8, wherein generating the second public key c using the cryptographic function comprises raising a value g to a power of the private key d to produce the second public key c.

10. A receiver device comprising:

one or more processors; and

a computer readable medium coupled to the one or more processors and containing instructions for causing the one or more processors to perform the method of any one of claims 1-9.