

WHAT IS CLAIMED IS:

- 1                   1.       A method for performing a privacy-preserving multi-party computation,  
2       the method comprising performing, by a receiver device:  
3           storing an input value  $b$  that is to be used in executing an encrypted program;  
4           generating a first value  $r_{1-b}$  using a random number generator;  
5           generating a key pair comprising a private key and a public key, using a cryptographic  
6       function;  
7           generating a hash output using a hash function that corresponds to the cryptographic  
8       function;  
9           generating a second value  $r_b$  using the public key and the hash output;  
10          sending the first value  $r_{1-b}$  and the second value  $r_b$  to a sender device;  
11          receiving a cryptographic value  $c$  from the sender device, wherein the cryptographic  
12       value  $c$  is generated using the cryptographic function;  
13          generating, using the private key and the cryptographic function, a key value that  
14       corresponds to input value  $b$ ;  
15          receiving the encrypted program from the sender device;  
16          executing the encrypted program using the key value to obtain an encrypted output  
17       value; and  
18          sending the encrypted output value to the sender device, wherein the sender device  
19       decrypts the encrypted output value using the key value.
- 1                   2.       The method of claim 1, wherein the cryptographic value  $c$  is generated  
2       in parallel with the generation of the first value  $r_{1-b}$  and the second value  $r_b$ .
- 1                   3.       The method of claim 1, wherein the input value  $b$  is an element of a set  
2       of values associated with a number of possible keys.
- 1                   4.       The method of claim 1, wherein the hash function is a random oracle.
- 1                   5.       The method of claim 1, wherein the first value  $r_{1-b}$  has a same length in  
2       bits as the public key.

1                   6.       The method of claim 1, wherein generating the hash output using the  
2 hash function that corresponds to the cryptographic function comprises: executing the hash  
3 function on the first value  $r_{1-b}$ .

1                   7.       The method of claim 1, wherein generating, using the private key and  
2 the cryptographic function, the key value that corresponds to input value  $b$  comprises: using  
3 the cryptographic function and the private key to decrypt the cryptographic value  $c$  to  
4 produce the key value.

1                   8.       A method for performing a privacy-preserving multi-party  
2 computation, the method comprising performing, by a sender device:  
3       storing a first key  $k_0$  and a second key  $k_1$ ;  
4       receiving a first value  $r_0$  and a second value  $r_1$  from a receiver device;  
5       generating a first public key using the first value  $r_0$  and a first hash output by operating  
6 a hash function  $H$  on the second value  $r_1$ , wherein the hash function  $H$  correspond to a  
7 cryptographic function used by the receiver device to generate the first value  $r_0$  and the second  
8 value  $r_1$ ;  
9       generating a second public key using the second value  $r_1$  and a second hash output by  
10 operating the hash function  $H$  on the first value  $r_0$ ;  
11       generating a first cryptographic value  $c_0$  by operating the cryptographic function on the  
12 first public key and the first key  $k_0$ ;  
13       generating a second cryptographic value  $c_1$  by operating the cryptographic function on  
14 the second public key and the second key  $k_1$ ;  
15       sending the first cryptographic value  $c_0$  and the second cryptographic value  $c_1$  to the  
16 receiver device;  
17       sending an encrypted program to the receiver device, wherein the receiver device  
18 executes the encrypted program to generate an encrypted output value;  
19       receiving the encrypted output value; and  
20       decrypting the encrypted output value using a corresponding key.

1

1                   9.       The method of claim 8, wherein the first value  $r_0$  is randomly generated  
2 by the receiver device and the second value  $r_1$  is generated by the receiver device using a  
3 public key and a hash output of executing the hash function H on the first value  $r_0$ .

1                   10.      The method of claim 8, wherein the receiver device is only able to  
2 decrypt one of the first cryptographic value  $c_0$  or the second cryptographic value  $c_1$ , based on  
3 a secret key stored on the receiver device.

1                   11.      The method of claim 8, wherein the encrypted program is generated by  
2 the sender device.

1                   12.      The method of claim 11, wherein the encrypted program is keyed to  
2 either the first key  $k_0$  or the second key  $k_1$ .

1                   13.      The method of claim 8, wherein the encrypted program is a garbled  
2 circuit.

1                   14.      A method for performing a privacy-preserving multi-party  
2 computation, the method comprising performing, by a sender device:  
3       generating a first private key  $d$  using a random number generator;  
4       generating a first public key  $c$  using a cryptographic function;  
5       sending the first public key  $c$  to a receiver device;  
6       receiving a first value  $r_0$  and a second value  $r_1$  from the receiver device;  
7       generating a first key  $k_0$  using the first value  $r_0$  and a first hash output by operating a  
8 hash function H on the second value  $r_1$  to obtain a first intermediate result, wherein the  
9 cryptographic function operates on the first intermediate result using the first private key  $d$  to  
10 generate the first key  $k_0$ , wherein the hash function H corresponds to the cryptographic  
11 function;  
12       generating a second key  $k_1$  using the second value  $r_1$  and a second hash output by  
13 operating the hash function H on the first value  $r_0$  to obtain a second intermediate result,  
14 wherein the cryptographic function operates on the second intermediate result using the first  
15 private key  $d$  to generate the second key  $k_1$ ;  
16       sending an encrypted program to the receiver device, wherein the receiver device  
17 executes the encrypted program to generate an encrypted output value;

18 receiving the encrypted output value; and  
19 decrypting the encrypted output value using a corresponding key.

1 15. The method of claim 14, wherein generating the first public key  $c$   
2 using the cryptographic function comprises: raising a value  $g$  to a power of  $d$  to produce the  
3 first public key  $c$ .

1 16. The method of claim 14, wherein the first value  $r_0$  is randomly  
2 generated by the receiver device using a random number generator.

1 17. The method of claim 16, wherein the second value  $r_1$  is generated by  
2 the receiver device, by subtracting a hash output of executing the hash function  $H$  on the first  
3 value  $r_0$  from a value  $g$  raised to a power of a randomly generated number  $\alpha$ .

1 18. The method of claim 14, wherein the encrypted program is keyed to  
2 either the first value  $r_0$  or the second value  $r_1$ .

1 19. The method of claim 14, wherein the public key  $c$  raised to a power of  
2 a randomly generated number  $\alpha$  is equal to one of the first key  $k_0$  or the second key  $k_1$ .

1 20. The method of claim 14, wherein the hash function  $H$  is a random  
2 oracle.

1 21. A receiver device comprising:  
2 one or more processors; and  
3 a computer readable medium coupled to the one or more processor and  
4 containing instructions for causing the one or more processors to perform the method of any  
5 one of claims 1-7.

1 22. A sender device comprising:  
2 one or more processors; and  
3 a computer readable medium coupled to the one or more processors and  
4 containing instructions for causing the one or more processors to perform the method of any  
5 one of claims 8-20.

- 1                   23.    A computer readable medium containing instructions for causing the  
2    processor to perform the method of any one of claims 1-20.