

WHAT IS CLAIMED IS:

- 1                   1.       A method for performing secure communication, the method  
2   comprising performing by a computer system:  
3                   generating a verification matrix **A** comprising a first plurality of elements, the  
4   first plurality of elements sampled from a uniform distribution;  
5                   generating a secret matrix **S** comprising a second plurality of elements, the  
6   second plurality of elements sampled from the uniform distribution;  
7                   generating an error matrix **E** comprising a third plurality of elements, the third  
8   plurality of elements sampled from a non-uniform distribution;  
9                   generating a public matrix **Y** using a modulus  $q$  as  $\mathbf{Y} = \mathbf{SA} + \mathbf{E} \bmod q$ ;  
10                  generating a public key comprising the verification matrix **A** and the public  
11   matrix **Y**;  
12                  generating a private key comprising the secret matrix **S** and the error matrix **E**;  
13   and  
14                  transmitting the public key to a verifying device.
- 1                   2.       The method of claim 1, further comprising transmitting the public key  
2   and the private key to a signing device.
- 1                   3.       The method of claim 1, wherein the uniform distribution is  
2   implemented using a ring.
- 1                   4.       The method of claim 1, wherein the uniform distribution is bound by  
2   the modulus  $q$ , such that each element of the first plurality of elements and the second  
3   plurality of elements is less than or equal to the modulus  $q$ .
- 1                   5.       The method of claim 1, wherein each element of the first plurality of  
2   elements and the second plurality of elements is an integer greater than or equal to 0 and less  
3   than or equal to  $q-1$ .
- 1                   6.       The method of claim 1, wherein the non-uniform distribution  
2   comprises a Gaussian distribution.
- 1                   7.       The method of claim 1, wherein:  
2   the verification matrix **A** is an  $n$  by  $m$  matrix;

3                   the secret matrix  $\mathbf{S}$  is an  $h$  by  $n$  matrix;  
4                   the error matrix  $\mathbf{E}$  is an  $h$  by  $m$  matrix;  
5                    $h$  is less than or equal to  $n$ ; and  
6                    $m$  is greater than  $n$ .

1                   8.       The method of claim 1, wherein the computer system comprising a  
2   signing device, wherein the method further comprises generating a digital signature for a  
3   message  $m$ , including:  
4                   (1) generating a random vector  $\mathbf{r}$  by sampling from the uniform distribution;  
5                   (2) generating a product vector  $\mathbf{rA}$  by calculating a product of the random  
6   vector  $\mathbf{r}$  and the verification matrix  $\mathbf{A}$ ;  
7                   (3) generating a rounded product vector by discarding one or more least  
8   significant bits from each element of the product vector  $\mathbf{rA}$ ;  
9                   (4) generating an intermediate vector using the rounded product vector  
10   modulus  $q$ ;  
11                   (5) generating a challenge vector  $\mathbf{c}$  by hashing the message  $m$  and the  
12   intermediate vector;  
13                   (6) calculating a verification vector  $\mathbf{v}$  based on the product vector  $\mathbf{rA}$ , the  
14   challenge vector  $\mathbf{c}$ , and the error matrix  $\mathbf{E}$ ;  
15                   (7) verifying that a plurality of elements of the verification vector  $\mathbf{v}$  are within  
16   a predetermined interval of values;  
17                   (8) generating a signature vector  $\mathbf{z}$  based on the random vector  $\mathbf{r}$ , the challenge  
18   vector  $\mathbf{c}$ , and the secret matrix  $\mathbf{S}$ , wherein the digital signature includes the signature vector  $\mathbf{z}$   
19   and the challenge vector  $\mathbf{c}$ ; and  
20                   (9) sending the digital signature and the message  $m$  to the verifying device.

1                   9.       The method of claim 8, further comprising:  
2                   if the plurality of elements of the verification vector  $\mathbf{v}$  are not within the  
3   predetermined interval of values, repeating steps (1) through (7) until the plurality of  
4   elements of the verification vector  $\mathbf{v}$  are within the predetermined interval of values.

1                   10.      The method of claim 8, wherein (6) calculating the verification vector  
2    $\mathbf{v}$  comprises calculating  $\mathbf{rA} - \mathbf{cE}$ .

- 1                   11.     The method of claim 8, wherein generating the signature vector  $\mathbf{z}$   
2     comprises calculating  $\mathbf{r} + \mathbf{cS}$ .
- 1                   12.     The method of claim 8, wherein step (7) comprises:  
2                   determining a plurality of least significant bits of the verification vector  $\mathbf{v}$ ;  
3                   calculating a norm of the plurality of least significant bits; and  
4                   verifying that the norm is within the predetermined interval of values.
- 1                   13.     The method of claim 8, wherein the predetermined interval of values is  
2     determined based on a parameter  $\beta$ , wherein the parameter  $\beta$  is greater than or equal to a  
3     norm of a product of the challenge vector  $\mathbf{c}$  and the error matrix  $\mathbf{E}$  with a specified  
4     probability.
- 1                   14.     The method of claim 13, wherein the specified probability comprises a  
2     probability greater than 99.99%.
- 1                   15.     The method of claim 8, wherein the signing device comprises an  
2     authorization computer, and wherein the message  $m$  comprises an authorization response  
3     message, the authorization response message indicating to the verifying device an  
4     authorization status of an interaction between the verifying device and a user device or a user  
5     of the user device.
- 1                   16.     A method for performing secure communication, the method  
2     comprising performing, by a verifying device:  
3                   storing a public key comprising a verification matrix  $\mathbf{A}$  and a public matrix  $\mathbf{Y}$ ;  
4                   receiving, from a signing device, a message  $m$  and a digital signature including  
5     a signature vector  $\mathbf{z}$  and a first challenge vector  $\mathbf{c}$ ;  
6                   generating a first verification vector  $\mathbf{v}$  based on the verification matrix  $\mathbf{A}$ , the  
7     public matrix  $\mathbf{Y}$ , the signing vector  $\mathbf{z}$ , and the first challenge vector  $\mathbf{c}$ ;  
8                   generating a rounded verification vector  $\mathbf{w}$  by discarding one or more least  
9     significant bits from the verification vector  $\mathbf{v}$ ;  
10                  generating a second challenge vector by hashing the message  $m$  and the  
11     rounded verification vector  $\mathbf{w}$ ;  
12                  comparing the first challenge vector  $\mathbf{c}$  to the second challenge vector; and

13                    verifying the signing device in response to the first challenge vector  $\mathbf{c}$   
14   matching the second challenge vector.

1                    17.    The method of claim 16, wherein the rounded verification vector  $\mathbf{w}$  is  
2   equal to an intermediate vector generated by the signing device, wherein the intermediate  
3   vector is equal to a rounded product vector  $\mathbf{rA}$  modulus  $q$ .

1                    18.    The method of claim 16, wherein the first verification vector  $\mathbf{v} = \mathbf{zA} -$   
2    $\mathbf{cY}$ .

1                    19.    The method of claim 16, wherein the verifying device comprises a  
2   resource provider computer, wherein the signing device comprises an authorization computer,  
3   wherein the message  $m$  comprises an authorization response message, and wherein the  
4   method further comprises:  
5                      evaluating the authorization response message; and  
6                      after verifying the signing device and evaluating the authorization response  
7   message, performing an interaction with a user device or a user of the user device.

1                    20.    A computer system comprising:  
2                      a processor; and  
3                      a non-transitory computer readable medium coupled to the processor, the non-  
4   transitory computer readable medium comprising code, executable by the processor for  
5   implementing the method of any one of claims 1-19.

1