

WHAT IS CLAIMED IS:

1 1. A method for use in verifying digital signatures, the method
2 comprising performing, by a generating device:
3 generating a gadget matrix G , wherein ~~the~~ columns of the gadget matrix G
4 comprise ascending powers of a base b ;
5 generating a reduced gadget matrix F , wherein the reduced gadget matrix F is
6 generated by dropping l columns of the gadget matrix G , wherein a value of l is
7 determined based on a desired level of security and a key size;
8 sampling a probability distribution to form a trapdoor matrix R , ~~wherein the~~
9 ~~trapdoor matrix that~~ functions as a secret key for generating a digital signature;
10 generating a verification matrix A using the reduced gadget matrix F and the
11 trapdoor matrix R ; and
12 transmitting, to a verification device, the verification matrix A , causing the
13 verification device to verify the digital signature generated by a sending device, using
14 ~~the trapdoor matrix R~~ verification matrix A .

1 2. The method of claim 1, wherein the base b of the gadget matrix G is 2.

1 3. The method of claim 1, wherein the trapdoor matrix R is sampled from
2 a Gaussian distribution.

1 4. The method of claim 1, wherein generating the verification matrix A
2 comprises:

3 sampling a uniform distribution to form a uniform matrix $\hat{A}$;
4 forming a generation matrix $\bar{A}$ by concatenating an identity matrix I and the
5 uniform matrix $\hat{A}$, wherein $\bar{A} = [I \mid \hat{A}]$; and
6 forming the verification matrix A , wherein $A = [\bar{A} \mid F\bar{A}R]$.

7 5. The method of claim 1, wherein l is in ~~the~~ a range 0 to $(\log_b q)/2$ for a
8 modulus q , and wherein the modulus q is between 2^{16} and 2^{24} .

1 6. The method of claim 1, wherein the gadget matrix G comprises n
2 repeats of k columns with ascending powers of the base b , and where generating the reduced
3 gadget matrix F further comprises dropping the l columns with ~~the~~ a smallest powers of the
4 base b from each group of k columns of the gadget matrix G .

1 7. The method of claim 1, wherein the probability distribution is a
2 Gaussian distribution.

1 8. The method of claim 1, wherein the verification matrix A is transmitted
2 to the sending device.

1 9. The method of claim 1, wherein the verification matrix A is made
2 public.

1 10.——A method comprising performing by a sending device:
2 receiving a message m ;
3 storing a verification matrix A and a trapdoor matrix R , wherein the trapdoor
4 matrix is generated by sampling a probability distribution;
5 generating a signature vector x by (1) using the verification matrix A to form a
6 lattice vector v , (2) sampling an intermediate vector z from a distribution based on the
7 lattice vector v , and (3) forming the signature vector x from a product of the
8 intermediate vector z and the trapdoor matrix R such that the signature vector x
9 satisfies a relationship $Ax \equiv h(m) + e \pmod{q}$ for a hash $h(m)$ of the message m , a
10 modulus q , and an error vector e ; and
11 transmitting, to a verification device, the message m and the signature vector
12 x , wherein the verification device stores the verification matrix A for verifying that the
13 signature vector x was generated by the sending device.

1 11.——The method of claim 10, wherein generating the signature vector x
2 comprises:
3 sampling a perturbation p from a probability distribution;
4 forming the lattice vector v using the message m , the verification matrix A , and
5 the perturbation p as inputs to a function defined by $v = m - Ap$;
6 sampling an intermediate vector z from a lattice Gaussian distribution, wherein
7 the lattice Gaussian distribution is based on a lattice formed from the lattice vector v ; and
8 forming the signature vector x by inputting the trapdoor matrix R , the
9 perturbation p , an identity matrix I , and the intermediate vector z into a function defined by

10
$$x = p + \begin{bmatrix} R \\ I \end{bmatrix} z.$$

12. — The method of claim 11, wherein the probability distribution is a Gaussian distribution.

13. — The method of claim 10, wherein the modulus q is between 2^{16} and 2^{24} .

14. — The method of claim 10, wherein the signature vector x is verified based on a size of the error vector e being less than a threshold.

15. — The method of claim 14, wherein the threshold is the dimension of the hash $h(m)$.

16. — The method of claim 15, wherein the threshold is $q/4$ for the modulus q .

17. — The method of claim 14, wherein the size of the error vector e is a Euclidean length of the error vector e .

18. — The method of claim 10, wherein the sending device receives the verification matrix A from a generating device.

19. — The method of claim 10, wherein the sending device transmits the hash $h(m)$ to the verification device.

20. — A method for authenticating a sending device, the method comprising performing by a verification device:

storing a verification matrix A ;

receiving from the sending device, a message m and a signature vector x ;

computing an error vector e by solving an equation $Ax = h(m) + e \bmod q$ for a hash $h(m)$ of the message m and a modulus q ;

quantifying a size of the error vector e ;

comparing the size to a threshold; and

verifying the signature vector x based on the size of the error vector e being less than the threshold.

21. — The method of claim 20, wherein the threshold is a dimension of the hash $h(m)$.

1 22. ~~—The method of claim 20, wherein the threshold is $q/4$ for the modulus~~
2 ~~q .~~

1 23. ~~—The method of claim 20, wherein the modulus q is between 2^{16} and 2^{24} .~~

1 24. ~~—The method of claim 20, further comprising receiving the hash $h(m)$~~
2 ~~from the sending device.~~

1 25. ~~—The method of claim 20, further comprising generating the hash $h(m)$~~
2 ~~by applying a hashing function to the message m .~~

1 26. ~~—The method of claim 20, wherein the verification matrix A is received~~
2 ~~from the sending device.~~

1 27. ~~—The method of claim 20, wherein the verification matrix A is received~~
2 ~~from a generating device, and wherein the generating device generates the verification matrix~~
3 ~~A .~~

1 28. ~~—The method of claim 20, wherein quantifying the size of the error~~
2 ~~vector e comprises computing a Euclidean length of the error vector e .~~

1 1029. A computer product comprising a computer readable medium storing a
2 plurality of instructions for controlling a computer system to perform the method of any one
3 of the preceding claims 1 to 9.

1 1130. A system comprising:
2 the computer product of claim 1029; and
3 one or more processors for executing instructions stored on the computer
4 readable medium.

1 31. ~~—A system comprising means for performing any of the above methods.~~

1 32. ~~—A system comprising one or more processors configured to perform~~
2 ~~any of the above methods.~~

1 33. ~~—A system comprising modules that respectively perform the steps of~~
2 ~~any of the above methods.~~