

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 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 that functions
9 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 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 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 a smallest powers of the base
4 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 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 claims 1 to 9.

1 11. A system comprising:
2 the computer product of claim 10; and
3 one or more processors for executing instructions stored on the computer
4 readable medium.