

[0012a]

According to a first aspect, there is provided an authentication device comprising:

a key holding unit for holding L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$); and

an interactive protocol execution unit for performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$,

wherein the interactive protocol execution unit includes

a challenge reception unit for receiving L challenges Ch_i from the verifier,

a challenge selection unit for arbitrarily selecting $(L-1)$ challenges Ch_i from the L challenges Ch_i received by the challenge reception unit,

a response generation unit for generating, by using the secret keys s_i , $(L-1)$ responses Rsp_i respectively for the $(L-1)$ challenges Ch_i selected by the challenge selection unit, and

a response transmission unit for transmitting the $(L-1)$ responses Rsp_i generated by the response generation unit to the verifier.

[0012b]

According to a second aspect, there is provided an authentication device comprising:

a key holding unit for holding L secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$);

a challenge reception unit for receiving Q sets ($Q \geq 2$) of L challenges $Ch_i^{(j)}$ ($i = 1$ to L) from a verifier;

a challenge selection unit for arbitrarily selecting one set of L challenges $Ch_i^{(j)}$ from the Q sets of L challenges $Ch_i^{(j)}$ received by the challenge reception unit;

a response generation unit for generating, by using the secret keys s_i , L responses Rsp_i respectively for the L challenges $Ch_i^{(j)}$ selected by the challenge selection unit; and

a response transmission unit for transmitting the L responses Rsp_i generated by the response generation unit to the verifier.

[0012c]

According to a third aspect, there is provided an authentication method comprising:

generating L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$); and

performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$,

wherein the performing includes receiving L challenges Ch_i from the verifier, arbitrarily selecting $(L-1)$ challenges Ch_i from the L challenges Ch_i that have been received, generating, by using the secret keys s_i , $(L-1)$ responses Rsp_i respectively for the $(L-1)$ challenges Ch_i that have been selected, and transmitting the $(L-1)$ responses Rsp_i that have been generated to the verifier.

[0012d]

According to a fourth aspect, there is provided a program for causing a computer to realize:

a key holding function of holding L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$); and

an interactive protocol execution function of performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$,

wherein the interactive protocol execution function includes

a challenge reception function of receiving L challenges Ch_i from the verifier,

a challenge selection function of arbitrarily selecting $(L-1)$ challenges Ch_i from the L challenges Ch_i received by the challenge reception function,

a response generation function of generating, by using the secret keys s_i , $(L-1)$ responses Rsp_i respectively for the $(L-1)$ challenges Ch_i selected by the challenge selection function, and

a response transmission function of transmitting the $(L-1)$ responses Rsp_i generated by the response generation function to the verifier.

[0012e]

According to a fifth aspect, there is provided an authentication method comprising:

generating L secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$);

receiving Q sets ($Q \geq 2$) of L challenges $Ch_i^{(j)}$ ($j = 1$ to Q) for a verifier;

arbitrarily selecting one set of L challenges $Ch_i^{(j)}$ from the Q sets of L challenges $Ch_i^{(j)}$ that have been received;

generating, by using the secret keys s_i , L responses Rsp_i respectively for the L challenges $Ch_i^{(j)}$ that have been selected; and

transmitting the L responses Rsp_i that have been generated to the verifier.

[0012f]

According to a sixth aspect, there is provided a program for causing a computer to realize:

a key holding function of holding L secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to multivariate polynomials F of n-th order ($n \geq 2$);

a challenge reception function of receiving Q sets ($Q \geq 2$) of L challenges $Ch_i^{(j)}$ ($j = 1$ to Q) from a verifier;

a challenge selection function of arbitrarily selecting one set of L challenges $Ch_i^{(j)}$ from the Q sets of L challenges $Ch_i^{(j)}$ received by the challenge reception function;

a response generation function of generating, by using the secret keys s_i , L responses Rsp_i respectively for the L challenges $Ch_i^{(j)}$ selected by the challenge selection function; and

a response transmission function of transmitting the L responses Rsp_i generated by the response generation function to the verifier.

[0012g]

According to a seventh aspect, there is provided an authentication device comprising:

a key setting unit for setting $s \in K^n$ to a secret key, and setting multi-order polynomials on a ring K, $f_i(x_1, \dots, x_n)$ ($i=1 \sim m$) and $y_i=f_i(s)$ to a public key;

a message transmission unit for transmitting message c to a verifier;

a verification pattern reception unit for receiving information on one verification pattern selected from k ($k \geq 3$) verification patterns by the verifier according to one piece of the message c; and

a response transmission unit for transmitting response information corresponding to the information on the verification pattern received by the verification pattern reception unit from k ways of response information to the verifier,

wherein the response information is calculated using information $z \in K^n$ in which the secret key s is masked by $r \in K^n$, $t' \in K^n$ in which the r is masked by $t \in K^n$, polynomial $f_i'(x)$ in which multi-order polynomials $f_i(x+r)$ related to x is masked by polynomial $f_i'(x)$.

[0012h]

According to an eighth aspect, there is provided an authentication device comprising:
circuitry configured to:

set $s \in K^n$ to a secret key;

set a multi-order multi-variable polynomial $f_i(x_1, \dots, x_n)$ ($i = 1$ to m) on a ring K to a public key or a system parameter;

set $y_i = f_i(s)$ to the public key;

transmit a message c to a verifier, wherein a prover attempts to prove a legitimacy to the verifier;

receive information on one verification pattern selected by the verifier from a plurality of verification patterns for one message c ; and

transmit, to the verifier, response information, among a plurality of the verification patterns of response information, corresponding to the information on the verification pattern.

[0012i]

According to a ninth aspect, there is provided an authentication method comprising:

setting $s \in K^n$ to a secret key, and setting second-order polynomials on a ring K , $f_i(x_1, \dots, x_n)$ ($i=1 \sim m$) and $y_i=f_i(s)$ to a public key;

transmitting message c to a verifier;

receiving information on one verification pattern selected from k ($k \geq 3$) verification patterns by the verifier according to one piece of the message c ; and

transmitting response information corresponding to the information on the verification pattern received by the verification pattern reception unit from k ways of response information to the verifier,

wherein the response information is calculated using information $z \in K^n$ in which the secret key s is masked by $r \in K^n$, $t' \in K^n$ in which the r is masked by $t \in K^n$, $e_i' \in K$ in which $f_i(r)$ substituted by the r for the second-order polynomials f_i is masked by $e_i \in K$.

[0012j]

According to a tenth aspect, there is provided a program causing a computer to realize:

setting $s \in K^n$ to a secret key, and setting second-order polynomials on a ring K , $f_i(x_1, \dots, x_n) (i=1 \sim m)$ and $y_i = f_i(s)$ to a public key;

transmitting message c to a verifier;

receiving information on one verification pattern selected from k ($k \geq 3$) verification patterns by the verifier according to one piece of the message c ; and

transmitting response information corresponding to the information on the verification pattern received by the verification pattern reception unit from k ways of response information to the verifier,

wherein the response information is calculated using information $z \in K^n$ in which the secret key s is masked by $r \in K^n$, $t' \in K^n$ in which the r is masked by $t \in K^n$, $e_i' \in K$ in which $f_i(r)$ substituted by the r for the second-order polynomials f_i is masked by $e_i \in K$.

[0013]

According to an embodiment aspect of the present invention ~~disclosure in order to achieve the above-mentioned object~~, there is provided an authentication device which includes a key holding unit for holding L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$), and an interactive protocol execution unit for performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$. The interactive protocol execution unit prevents, at the time of performing the interactive protocol with the verifier, the verifier from knowing which secret key s_i was used.

[0014]

Further, the interactive protocol execution unit may include a challenge reception unit for receiving L challenges Ch_i from the verifier, a challenge selection unit for arbitrarily selecting $(L-1)$ challenges Ch_i from the L challenges Ch_i received by the challenge reception unit, a response generation unit for generating, by using the secret keys s_i , $(L-1)$ responses Rsp_i respectively for the $(L-1)$ challenges Ch_i selected by the challenge selection unit, and a response transmission unit for transmitting the $(L-1)$ responses Rsp_i generated by the response generation unit to the verifier.

[0015]

Further, the interactive protocol execution unit may further include a message transmission unit for transmitting, to the verifier, messages Cmt_i each corresponding to each of the L secret keys s_i . In this case, the challenge reception unit receives a challenge Ch_i indicating a verification pattern selected from k ($k \geq 2$) verification patterns by the verifier according to each message Cmt_i transmitted by the message transmission unit.

[0016]

Further, in a case of the message $Cmt_i = (c_{i,1}, \dots, c_{i,N})$, the message transmission unit may calculate a new message $Cmt' = H(Cmt_1, \dots, Cmt_L)$ using a one-way function H and transmits this message Cmt' to the verifier, and the response transmission unit may transmit, together with the response Rsp_i , an element of the

message Cmt_i that the verifier is not able to restore even when using this response Rsp_i .

[0017]

Further, the key holding unit may not have to hold one secret key s_{i_0} ($1 \leq i_0 \leq L$) among the L secret keys s_i . In this case, the interactive protocol execution unit performs, based on a falsification algorithm, processing related to the secret key s_{i_0} that is to be performed in the interactive protocol.

[0018]

Further, according to another ~~embodiment~~ aspect of the present ~~invention~~ disclosure in order to achieve the above-mentioned object, there is provided an authentication device which includes a key holding unit for holding L secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$), a challenge reception unit for receiving Q sets ($Q \geq 2$) of L challenges $Ch_i^{(j)}$ ($j = 1$ to Q) from a verifier, a challenge selection unit for arbitrarily selecting one set of L challenges $Ch_i^{(j)}$ from the Q sets of L challenges $Ch_i^{(j)}$ received by the challenge reception unit, a response generation unit for generating, by using the secret keys s_i , L responses Rsp_i respectively for the L challenges $Ch_i^{(j)}$ selected by the challenge selection unit, and a response transmission unit for transmitting the L responses Rsp_i generated by the response generation unit to the verifier.

[0019]

Further, the interactive protocol execution unit may further include a message transmission unit for transmitting, to the verifier, messages Cmt_i respectively corresponding to the L secret keys s_i . In this case, the challenge reception unit receives a challenge $Ch_i^{(j)}$ indicating a verification pattern selected from k ($k \geq 2$) verification patterns by the verifier according to each message Cmt_i transmitted by the message transmission unit.

[0020]

Further, in a case of the message $Cmt_i = (c_{i,1}, \dots, c_{i,N})$, the message transmission unit may calculate a new message $Cmt' = H(Cmt_1, \dots, Cmt_L)$ using a one-way function H and transmits this message Cmt' to the verifier, and the response

transmission unit may transmit, together with the response Rsp_i , an element of the message Cmt_i that the verifier is not able to restore even when using this response Rsp_i .

[0021]

Further, according to another embodiment ~~aspect of the present invention~~ ~~disclosure in order to achieve the above-mentioned object~~, there is provided an authentication method which includes a key generating step for generating L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$), and an interactive protocol performing step for performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$. The interactive protocol execution step prevents, at the time of performing the interactive protocol with the verifier, the verifier from knowing which secret key s_i was used.

[0022]

Further, according to another embodiment ~~aspect of the present invention~~ ~~disclosure in order to achieve the above-mentioned object~~, there is provided a program for causing a computer to realize a key holding function of holding L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$), and an interactive protocol execution function of performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$. The interactive protocol execution function prevents, at the time of performing the interactive protocol with the verifier, the verifier from knowing which secret key s_i was used.

[0023]

Further, according to another embodiment ~~aspect of the present invention~~ ~~disclosure in order to achieve the above-mentioned object~~, there is provided an authentication method which includes a key generating step for generating L secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$), a challenge receiving step for receiving Q sets ($Q \geq 2$) of L challenges $Ch_i^{(j)}$ ($j = 1$ to Q) for a verifier, a challenge selecting step arbitrarily selecting one set of L challenges $Ch_i^{(j)}$ from the Q sets of L challenges

$Ch_i^{(j)}$ that have been received in the challenge receiving step, a response generating step for generating, by using the secret keys s_i , L responses Rsp_i respectively for the L challenges $Ch_i^{(j)}$ that have been selected in the challenge selecting step, and a response transmitting step for transmitting the L responses Rsp_i that have been generated in the response generating step to the verifier.

[0024]

Further, according to another ~~embodiment~~ aspect of the present ~~invention~~ disclosure in order to achieve the above-mentioned object, there is provided a program for causing a computer to realize a key holding function of holding L secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to multivariate polynomials F of n -th order ($n \geq 2$), a challenge reception function of receiving Q sets ($Q \geq 2$) of L challenges $Ch_i^{(j)}$ ($j = 1$ to Q) from a verifier, a challenge selection function of arbitrarily selecting one set of L challenges $Ch_i^{(j)}$ from the Q sets of L challenges $Ch_i^{(j)}$ received by the challenge reception function, a response generation function of generating, by using the secret keys s_i , L responses Rsp_i respectively for the L challenges $Ch_i^{(j)}$ selected by the challenge selection function, and a response transmission function of transmitting the L responses Rsp_i generated by the response generation function to the verifier. According to another embodiment of the present disclosure, there is provided a computer-readable recording medium in which the program is recorded.

Advantageous Effects of Invention

[0025]

According to the embodiments of the present ~~invention~~ disclosure described above, it is possible to guarantee a security level sufficient for an active attack even if an interactive protocol is repeatedly performed in parallel.

Brief Description of Drawings

[0026]

[Fig. 1] FIG. 1 is an explanatory diagram for describing an algorithm structure of a public key authentication scheme;

[Fig. 2] FIG. 2 is an explanatory diagram for describing an n -pass public key

19. The authentication device according to claim 18,

wherein the multi-order multi-variable polynomial f_i is a second-order multi-variable polynomial.

~~2023~~. An authentication method comprising:

setting $s \in K^n$ to a secret key, and setting second-order polynomials on a ring K , $f_i(x_1, \dots, x_n) (i=1 \sim m)$ and $y_i=f_i(s)$ to a public key;

transmitting message c to a verifier;

receiving information on one verification pattern selected from k ($k \geq 3$) verification patterns by the verifier according to one piece of the message c ; and

transmitting response information corresponding to the information on the verification pattern received by the verification pattern reception unit from k ways of response information to the verifier,

wherein the response information is calculated using information $z \in K^n$ in which the secret key s is masked by $r \in K^n$, $t' \in K^n$ in which the r is masked by $t \in K^n$,

$e_i' \in K$ in which $f_i(r)$ substituted by the r for the second-order polynomials f_i is masked by $e_i \in K$.

2124. A program causing a computer to realize:

setting $s \in K^n$ to a secret key, and setting second-order polynomials on a ring K , $f_i(x_1, \dots, x_n) (i=1 \sim m)$ and $y_i = f_i(s)$ to a public key;

transmitting message c to a verifier;

receiving information on one verification pattern selected from k ($k \geq 3$) verification patterns by the verifier according to one piece of the message c ; and

transmitting response information corresponding to the information on the verification pattern received by the verification pattern reception unit from k ways of response information to the verifier,

wherein the response information is calculated using information $z \in K^n$ in which the secret key s is masked by $r \in K^n$, $t' \in K^n$ in which the r is masked by $t \in K^n$, $e_i' \in K$ in which $f_i(r)$ substituted by the r for the second-order polynomials f_i is

masked by $e_i \in K$.

2220. An authentication device comprising:

circuitry configured to:

receive a message c from a prover, wherein the prover attempts to prove a legitimacy to a verifier;

select one verification pattern from a plurality of verification patterns for one message c ;

transmit information on the verification pattern selected by the verification pattern selection unit to the prover;

receive, from the prover, response information, among a plurality of the verification patterns of response information, corresponding to the information on the verification pattern transmitted; and

verify a legitimacy of the prover by using the received message c and the received response information,

wherein $s \in K^n$ is set to a secret key, a multi-order multi-variable polynomial $f_i(x_1, \dots, x_n)$ ($i = 1$ to m) on a ring K is set to a public key or a system parameter, and $y_i = f_i(s)$ is set to the public key.

2324. A signature generation device comprising:

circuitry configured to:

set $s \in K^n$ to a secret key;

set a multi-order multi-variable polynomial $f_i(x_1, \dots, x_n)$ ($i = 1$ to m) on a ring K to a public key or a system parameter;

set $y_i = f_i(s)$ to the public key;

generate N messages c based on the multi-order multi-variable polynomial $f_i(x_1, \dots, x_n)$ and the secret key s ;

select a verification pattern from a plurality of verification patterns based on information obtained by applying a document M and the message c to a one-way hash function; and

generate, according to the selected verification pattern, a digital signature σ

that will pass verification that uses the message c and the document M .

2422. A signature verification device comprising:

circuitry configured to:

receive N messages c based on a multi-order multi-variable polynomial $f_i(x_1, \dots, x_n)$ and a secret key s ;

select a verification pattern from a plurality of verification patterns based on information obtained by applying a document M and the N messages c to a one-way hash function ;

transmit a challenge $Ch \in \{0, 1\}$ indicating the selected verification pattern to a prover;

generate a response Rsp to be sent back to the prover in response to the challenge $Ch \in \{0, 1\}$ received from the prover;

perform verification based on the response Rsp and the secret key s by executing the one way hash function; and

verify the legitimacy of the verification by performing an operation to obtain a value 0 or 1 based on the executed hash values, wherein 0 indicates a verification failure and 1 indicates a verification success;

wherein $s \in K^n$ is set to the secret key s and the multi-order multi-variable polynomial $f_i(x_1, \dots, x_n)$ ($i = 1$ to m) on a ring K is set to a public key or a system parameter.