(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2016 (28.04.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/064263 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 21/32* (2013.01)

(21) International Application Number:
PCT/MY2015/000081

(22) International Filing Date:
30 September 2015 (30.09.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2014702934 3 October 2014 (03.10.2014) MY

(71) Applicants: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY). **SUNWAY UNIVERSITY** [MY/MY]; No. 5, Jalan Universiti, Bandar Sunway, 46150 Petaling, Jaya, Selangor (MY).

(72) Inventors: **GOH, Alwyn**; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **NG, Kang Siong**; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **LEE, Kay Win**; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MAT NEN, Laifah**; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **NGO, Chek Ling, David**; c/o Sunway University, No. 5, Jalan Universiti, Bandar Sunway, 46150 Petaling Jaya, Selangor (MY).

(74) Agent: **CHEW, Kherk Ying**; Wong & Partners, Level 21, The Gardens South Tower, Mid Valley City, Lingkaran Syed Putra, Kuala Lumpur 59200 (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD OF ZERO KNOWLEDGE PROCESSING ON BIOMETRIC DATA IN DISCRETISED VECTOR REPRESENTATION

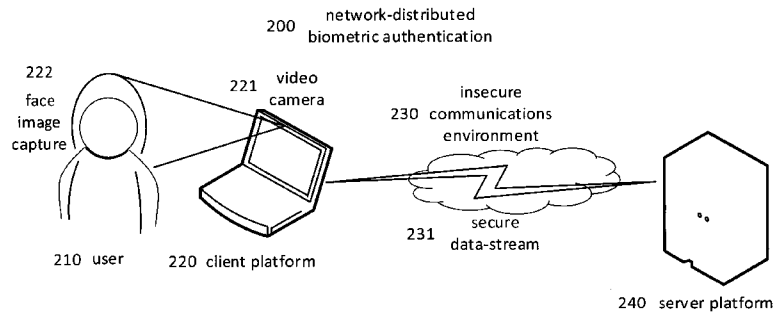

FIGURE 2A

(57) Abstract: The present invention provides a method comprising: encoding of a biometric vector-stream, as comprises a sequence of biometric vector-frames, during an authentication interaction between a client and a server sub-system, wherein encoding of any particular biometric vector-frame is different from any other biometric vector-frame in vector-stream of interest; secure transmission of such an encoded biometric vector-stream as originating from a particular user of interest operating the client to the server; and then decoding at the server of the encoded biometric vector-stream as received from the client; further comprising limitation in capability of server to undertake such decoding by subject to correct demonstration of private PKC credential corresponding to public credential stipulated by the user during the authentication interaction.

WO 2016/064263 A1

METHOD OF ZERO KNOWLEDGE PROCESSING ON BIOMETRIC DATA IN DISCRETISED VECTOR REPRESENTATION

FIELD OF INVENTION

The present invention relates generally to a method of cryptographic encoding on biometric data in discretised vector representation, more particularly a method of client-side masking of biometric data and client-side encoding and corresponding server-side decoding, wherein masking and encoding/decoding operations are based on finite field (FF) computations, as exemplified by Galois Field (GF) computations, and as applicable in cryptographic operations.

BACKGROUND ART

Authentication by means of biometric data is fundamentally different from equivalent process by means of knowledge-based or hardware-specific credentials, arising from the fact that biometric data is "attached" to a particular user, with the corresponding difficulty of revocation and refreshment in a manner equivalent to that of knowledge-based or hardware-specific credentials, resulting in necessity for exceptionally strong protection of biometric authentication data and processes.

At present, such protection is generally of extrinsic nature, as exemplified by encrypted storage of biometric reference data, or establishment of SSL/TLS secure connectivity for transport of biometric data streams.

Rather than constituting a security measure, biometric representations are generally utilized as analytic methods. Biometric authentication is regarded as a unidirectional client-to-server process, with correspondingly insufficient specification with regards to server-side credentials prior to undertaking biometric authentication, or server-side storage and management of biometric reference data.

SUMMARY OF INVENTION

The present invention provides a method of zero knowledge (ZK) encoding on biometric data in discretised vector representation. The present invention proposes client-side masking of biometric data, as protective measure against leakage of biometric data on server-side storage, and additionally client-side encoding and corresponding server-side decoding, as protective measure against interception and/or leakage of biometric data in transit from client-to-server, as predicate on client-server interaction to establish mutual trustworthiness, wherein masking and encoding/decoding operations are based on finite field (FF) computations, as exemplified by Galois Field (GF) computations.

In one aspect of the present invention is a method of cryptographic encoding on biometric data in discretised vector representation. The method comprises encoding a biometric vector-stream during an authentication interaction between a client and a server, wherein encoding the biometric vector-stream further comprises encoding a biometric vector-frame differently from another biometric vector-frame; securely transmitting an encoded biometric vector-stream from a user opearating the client to the server; verification of server by demonstrating private credential corresponding to public credential stipulated by the user during the authentication interaction; and decoding the encoded biometric vector-stream or vector-frame at the server; with both private and public credentials as aforesaid applicable in stipulated public-key cryptographic (PKC) operations.

In the preferred embodiment of the present invention, verification is undertaken after decoding if user is able to demonstrate private credential during authentication interaction as corresponding to public credential used by the server of interest to specify user to be verified.

Encoding and decoding of biometric vector-streams comprises a pair of mutually inverse trapdoor one-way functions such that correct combination of encode and decode functions on biometric vector-streams has no effect on subsequent computation of a distance measurement, with biometric vector-streams as input. Biometric authentication is then based on the aforesaid distance measurement

between test biometric vectors arising from authentication interaction, and reference biometric vectors previously established by the user with the server.

The method further comprises masking the biometric vector-stream wherein the computation of the distance measurement is independent of masking function that is identically applicable on test biometric vectors and reference biometric vectors and dependent on a valuation of masking key.

Encoding the biometric vector-stream further comprises FF encoding; as arising from finite fields of type GF (2^n) modulo irreducible polynomial of n-th degree with binary (modulo-2) coefficients, or GF (p^n) modulo irreducible polynomial of n-th degree with coefficients modulo small prime (p); wherein representational form of biometric vector-frame is of equal component-level dimensionality, or multiple thereof; and of consistent component-level structure to corresponding encoding, such that component-level discretisation is to 2^m or p possible values, as the case might be.

Encoding the biometric vector-stream further comprises FF encoding arising from GF (2^n) finite fields, wherein product of vector dimension, m and bit-length of component-level discretisation, m', resulting in 2^m possible valuations per component is equal to bit-length of valuations arising from GF (2^n) encoding or multiple thereof.

The method further comprises masking the biometric vector-stream at the client during authentication interaction between the user and the server, wherein masking is performed by means of FF addition of masking key with each element in biometric vector-stream such that a distance measurement between test biometric vectors and reference biometric vectors is specified by Hamming distance between test biometric vectors and reference biometric vectors, and is demonstrative of invariance under masking operation as specified.

The method is applicable within context of the client and the server engaging in interactive key establishment, as exemplified by the authenticated Diffie-Hellman (ADH) protocol and variations thereof, wherein both the client and the server undertake independent contribution of random key-pairs, and mutual

challenge of correct private-key demonstration by other party, as arising from computation on corresponding public-key associated with other party and resulting in independent computation for session-key as aforesaid, subject to correct execution by both the client and the server.

The client might alternatively undertake key distribution to the server, as exemplified by use of a signcryption protocol, wherein the Client undertakes computation of random key-pair and derivative session-key authentication, with the server public-key and the user private-keys as protocol inputs, subsequent to which the server undertakes recovery and verification of session-key, with the user public-key and the server private-key as protocol inputs, such that the session-key as delivered can be authenticated to be correctly received as transmitted and furthermore correctly associated with the user engaged in authentication interaction.

The session-key as independently established on the client and the server is then applicable to the client undertaking computation of key-stream of equal frame-length to stream of biometric vector-frames wherein the computation is an outcome of cryptographic key schedule function, as comprising block ciphers and keyed-hash message authentication code (HMAC) functions, with session-key as a function input; with corresponding encoding, by FF addition or multiplication, of each element in key-stream with corresponding element in vector-stream. Subsequent to this, the server undertakes Independent computation of key-stream of equal frame-length to received stream of encoded vector-frames wherein the computation is an outcome of cryptographic key schedule function with independently established session-key as a function input; enabling computation of stream of key inverses, by FF multiplicative inversion of each element in said key-stream; and then decoding, by FF addition or multiplication, of each element in stream of key inverses to corresponding element in encoded vector-stream of interest. Therefore the server is able to establish that vector-stream is correctly received as transmitted, and furthermore correctly associated with the user engaged in authentication interaction.

In another aspect of the present invention is a method of user authentication of a client by a server. The method comprises the user presenting biometric to a capture apparatus attached to the client. The client generates test vector-stream resulting from the user presentation, establishes session-key specific to a particular authentication interaction, computes an applicable key-stream, and then computes encoded vector-stream for transmission to the server. The server then independently establishes session-key specific to the said particular authentication interaction; computes applicable key-stream; computes inversion of each element thereof; computes decoded vector-stream; and then computes distance measures between elements of test vector-stream as presently received from user of interest, against set of reference vector-frames as previously received from the user; and lastly undertakes assessment of authentication outcome based on distance measures between set of test and reference vector-frames.

The client further undertakes application of masking function on biometric vector-stream, resulting in computation of masked vector-stream from corresponding vector-stream, as arising from masking key unique and specific to combination of user and server of interest, such that valuation of masking key is presumed secret and exclusive to user of interest.

The server further undertakes assessment of authentication outcome based on distance measures between set of test and reference vector-frames, such that distance measurements are not affected by application of same mask function on both test and reference vector-frames, as is predicated on use of identical masking key during masking of both test and reference vector-frames.

The correctness of key establishment interaction as aforesaid is dependent on correct prior demonstration by the user to the client of knowledge-based credential, as presumed secret and exclusive to the user; and which is inclusive of but not limited to textual sequence with input via keyboard or keypad, or geometric sequence with input via touch-sensitive screen.

The correctness of key establishment interaction as aforesaid is optionally additionally dependent on correct determination by the client of platform-specific identifier, corresponding to singular particular platform from plurality of platforms previously designated by the user and as presumed unique and specific to the particular platform.

The private-key particular to user of interest, as applicable in aforesaid key establishment, is obtained from output of one-way computation, with input inclusive of knowledge-based credential as aforesaid.

The private-key particular to user and associated platform of interest, as applicable in aforesaid key establishment, is obtained from output of computation to interpolate for constant coefficient of random credential-encoding polynomial of linear degree, as defined on finite field of interest, from coordinates comprising: first-ordinate as output of one-way computation, with inputs inclusive of knowledge and platform-specific credentials as applicable; and second-ordinate as output of said polynomial as evaluated upon input of corresponding first-ordinate, with such particular valuation of polynomial retained on the client.

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it is being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated, in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

FIGURE 1 illustrates a method of zero knowledge (ZK) processing of biometric data in discretised vector representation.

FIGURE 2A illustrates a security framework for biometric authentication according to the present invention.

FIGURE 2B illustrates an assertion of multiple factors contributing to user identity.

FIGURE 3 illustrates the process flow of Zero Knowledge (ZK) processing of biometric data, by means of session-specific key, concluding in biometric authentication.

FIGURE 4A illustrates the process flow of interactive client-server establishment of session key, as subsequently used in ZK processing of biometric data.

FIGURE 4B illustrates the process flow of client-to-server session key delivery, as subsequently used in ZK processing of biometric data.

FIGURE 5 illustrates the process flow for generation of key-stream, and subsequent use thereof for encoding of biometric vector stream.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a method and system to undertake zero knowledge (ZK) masking and encoding of biometric data, so as to enable biometric authentication while also ensuring strong protection of biometric data . Hereinafter, this specification will describe the present invention according to the preferred embodiments of the present invention. However, it is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned that those skilled in the art may devise various modifications and equivalents without departing from the scope of the appended claims.

Reference is first being made to FIGURE 2A. FIGURE 2A illustrates a security framework for biometric authentication according to the present invention. The present invention proposes a method (200) for client-side masking of biometric

data, as protective measure against leakage of biometric data on server-side storage, and additionally client-side encoding and corresponding server-side decoding, as protective measure against interception or leakage of biometric data in transit from client-to-server, with application of such protective measures predicated on client-server interaction to establish mutual trustworthiness, wherein masking and encoding/decoding operations are based on finite field (FF) computations, as exemplified by Galois Field (GF) computations commonly used in cryptographic protocols.

The present invention allows for a client (220), acting on behalf of a user (210), to verify server (240) credentials as authentic, and reciprocally the server (240) to verify user credentials as similarly authentic. Thereafter both client and server engage into mutual establishment of secure network (231) over an insecure communications environment (230), in preparation for capture (221) of the user biometric data (222), encoding of such biometric data into a stream of biometric frames, and subsequently transmission of such stream to the server. The server is then able to verify each and every frame in any particular stream as being correctly received as transmitted, and furthermore correctly associated with the user identity as asserted.

Reference is now being made to FIGURE 2B. FIGURE 2B illustrates a process flow for the assertion of user identity (250). Assertion of user identity is undertaken on the basis of demonstration of knowledge-based credential (251), as presumed secret and exclusive to the user of interest; or alternatively demonstration of such knowledge-based credential, in addition to demonstration of at least one credential (252, 253) arising from previously specified client platform associated with the user, as similarly presumed unique and specific to platform of interest. Demonstration of credential is by means of FF polynomial interpolation (280), from coordinates (271) constituted (270) from; ZK hashing (260) of credential inputs as first ordinate, in combination with previously computed second ordinate corresponding to credential of interest, and resulting in computation of secret or private-key (281) previously associated with user of interest..

Overall process flow

Reference is now being made to FIGURE 1. FIGURE 1 illustrates a method of ZK processing on biometric data in discretised vector representation according to the present invention.

The process flow according to the present invention begins with biometric capture (110) on apparatus attached to the client sub-system (115), followed by biometric detection on applicable frames of apparatus data stream (115) and biometric signal enhancement (120), to correct for variability of the user behavior and capture environment, on such frames of apparatus data stream. Thereafter, biometric processing (100) applies with biometric vector extraction (125) on applicable frames of apparatus data stream; resulting in computation, preferentially on the client, of biometric vector stream in floating-point representation; and is followed by biometric vector discretisation (130) of vector stream into elements of bitstring representation. According to the various embodiments of the present invention, the process flow is enhanced at this juncture to include masking of biometric vector stream (140), to protect against leakage of biometric information, and to ensure revocability of aforesaid biometric vectors by user of interest. Thereafter, it is followed by encoding of masked or unmasked vector stream (150), as the case might be, to protect against leakage of biometric information during transit, and to ensure privacy. The process continues, on the biometric server (106), with corresponding decoding (160) of the previously encoded vector stream, to enable verification, by the server; that vector stream is correctly received as sent, and furthermore correctly associated with user of interest. This is followed by error correction on vector stream (165), to compensate for some specified degree of variability, as specified in the error correction encoding scheme of interest, in the discretised vector stream. The authentication process concludes with measurement of some specified distance metric (170) between test and reference vector streams, as the basis for assessment of authentication outcome, with said distance measurement being unaffected by application of aforesaid masking, encoding and decoding operations.

The process flow is, in successive steps, applicable on:

Image arising from video capture apparatus of interest results in colour image $C^{M \cdot M'}$ of pixel dimensionality M×M', with typical values of M×M' = 640×480 for VGA-grade cameras; and colour depth $2^{M''}$.

Biometric, as exemplified by face image, arising from detection and extraction from image captured into smaller region of interest (ROI) image $G^{N \cdot N'}$ of reduced pixel dimensionality N×N', with typical values of (N,N') significantly smaller than the preceding (M,M'); and greyscale depth $2^{M''}$, with typical value of M"=8 for 8-bit greyscale images.

Biometric vector, arising from feature vector extraction from ROI image into vector F^m of dimensionality m, as significantly smaller than corresponding N×N' of ROI image; and as comprising vector components, as represented in computations by means of floating-point number valuations; as representations of real of complex number valuations of the particular vector extraction methodology.

Biometric vectors are subsequently subject to various signal enhancement operations which do not affect the dimensionality of the biometric vector representation.

Masking, encoding and decoding operations are by means of FF and Elliptical Curve (EC) cryptography for session-level secure biometric transport; and FF and cryptographic hashing for stream-level biometric encoding and decoding.

Detailed description

Reference is being made to FIGURE 3. FIGURE 3 illustrates a flow for ZK processing of biometric data (300), concluding in biometric authentication (390).

Biometric data (311) of a user (302) is captured on client platform (301) by means of camera activation (310), followed by image-level processing (315), vector-level processing (320), vector-stream discretisation (325), and then

vector stream masking (330), by means of FF and cryptographic computations which accept as input user secret-key a' (331).

Establishment of secure connectivity between user (302) and server (303) is then undertaken; on presumption of prior establishment of user EC key-pair (a,A) (342, 346) with which to undertake interaction with server; and corresponding secret-key a' (331) as aforesaid with which to mask outgoing biometric vector stream (330); and reciprocally server EC key-pair (b,B) (341, 346); and furthermore that each of user and server is in possession of the other party's public-key (341, 346) prior to undertaking such cryptographic interaction for establishment of such secure connectivity.

User (302) on client platform (301) and server (303) of interest engage in their respective roles in cryptographic interaction (340, 345) of interest, resulting in independent computation of session-key k (350, 355) with which to establish secure connectivity; and subsequently independent computation by client, on behalf of user, and server of encoding key-stream [k_i] (360); and correspondingly computation by server of decoding key-stream [k'_i] (370) as inversion of encoding key-stream. This is followed by encoding by client of biometric vector stream by means of encoding key-stream; and subsequently transmission of encoded vector stream from client to server; and following that decoding by server of encoded vector stream by means of decoding key-stream. The biometric vector stream as received is then subject of error correction (380), and finally biometric authentication (390) on the basis of distance measurements between test vectors as received and reference vectors as previously associated with user of interest.

Reference is being made to FIGURE 4A. FIGURE 4A illustrates a process flow of interactive client-server establishment of session-specific key, as subsequently used in ZK processing of biometric data.

Independent establishment (400) of session-key k (440. 445) by the respective interacting parties is implemented by means of client-server key negotiation, as exemplified without limitation by the authenticated Diffie-Hellman (ADH)

protocol. Client (401) and server (406) commence interaction by undertaking independent generation of session-specific key-pairs (410, 415), and following that by executing random challenges (411, 416) on the public-key of other party, necessitating correct demonstration (420, 430) by each party of their respective corresponding private-keys; and resulting in independent computation (440, 445) of session-key k by both parties, provided both parties are able to correctly undertake all required computations.

Reference is being made to FIGURE 4B. FIGURE 4B illustrates a process flow of client-to-server delivery of session-specific key (450), as subsequently used in ZK processing of biometric data.

Alternatively, establishment of session-key k is implemented by means of client-to-server key transport or delivery, as exemplified without limitation by the signcryption protocol.

This requires the client (451) to undertake challenge on public-key of server in the process of generating random session-key (460), while additionally applying authentication (461), by application of user private-key, on such random challenge. This in turns allows the server (456) to undertake recovery (462) and verification (463) of such session-key, by means of use of user public-key, and correct demonstration of server private-key.

Reference is being made to FIGURE 5. FIGURE 5 illustrates a process flow for the generation of a key-stream, and subsequent use thereof for encoding of the biometric vector stream (500).

Establishment of session-key k as aforesaid concludes with both client and server in possession of session-key k (502), enabling independent computation by means of ZK key-scheduling function (510) by both parties of particular element of encoding key-stream k_i (511), of index value i (501). This process is exemplified without limitation by output of hash computation H(k,i), with session-key and stream index values as inputs; resulting in computation by client of encoding key-stream element k_i (511), and furthermore independent computation by server of decoding key-stream element k'_i, as exemplified

without limitation by FF multiplicative or additive inversion. This is such that client can compute encoding (521) of particular element of outgoing biometric stream (512), via use of k_i and additionally that server can compute corresponding decoding on particular element of incoming biometric stream, via use of k'_i, with both encoding and decoding operations undertaken by means of FF computations.

Operational sequence of biometric post-processing

The post-processing process flow according to the present invention is subsequently applicable on:

Biometric vector discretisation, arising from preceding floating-point representation into binary vector $D^m = (2^{m'})^m$, as represented by means of bitstring of length n = m×m′, such that each valuation in range of $[-2^{m'-1}, \cdots, 0, \cdots, 2^{m'-1} - 1]$ has equal probability of occurrence; and subsequent to that

Biometric vector in such 2^n bitstring representation $a = a_{k-1} \cdots a_1 a_0$, represented as element in specified finite field (FF); as exemplified by GF(2^n), modulo previously specified irreducible polynomial $P_n = \sum_{k=n}^{0} p_k x^k$, with coefficients p_k mod 2 in range [0,1].

Biometric test vector a is subsequently subject to FF multiplication with cryptographic element k, such that product of form x = a • k is suitable for secure transmission from biometric client to server, even if intervening communications network is presumed to be insecure, such that only intended recipient server can compute FF multiplicative inverse k^{-1}, as required for recovery of biometric vector a by means of computation $x \bullet k^{-1}$.

Biometric vector is alternatively subject to FF addition with cryptographic element as aforesaid, such that recovery of biometric vector by intended recipient is predicated on correct computation of FF additive inverse.

Cryptographic element k may arise from various interactions undertaken between client A, with corresponding elliptic curve (EC) key-pair (α,A) associated with user of interest, private-key of which is presumed to be secret and exclusive; and server B, with corresponding EC key-pair (b,B) associated with authentication server of interest, private-key of which is similarly presumed to be secret and exclusive.

Cryptographic element k can be obtained from engagement in ADH key-establishment protocol, in which both client and server both contribute random session-specific key-pairs, and undertake mutual challenges on each others public-keys; such that correct completion of said protocol requires demonstration by both parties of their respective private-keys corresponding to public-keys previously challenged, prior to mutual and independent establishment of random session-key k.

Cryptographic element k can alternatively be obtained from engagement in signcryption protocol from client to server; in which client contributes random session-specific key-pair, user private-key a and server public-key B as stipulated input elements; and in which server undertakes reciprocal unsigncryption protocol, which requires demonstration of private-key b corresponding to previously stipulated public-key B, prior to

correct recovery of random session-key k, and additionally verification of association with user of interest, by mean of public-key A corresponding to previously applied private-key a.

Singular cryptographic element k established as aforesaid is then subject to expansion into key-stream of random elements $[k_1, k_2, \cdots, k_i, \cdots]$, such that no singular element k_i of key-stream can be used to deduce the value of any other element in said key-stream.

Each element k_i of key-stream is subject to FF multiplication with corresponding biometric vector element a_i in vector-stream $[a_1, a_2, \cdots, a_i, \cdots]$, to compute FF-encoded element $x_i = a_i \bullet k_i$ in encoded-stream $[x_1, x_2, \cdots, x_i, \cdots]$ on client for transmission to server; such that only intended recipient server is able to

compute FF multiplicative inverse k_i^{-1}, with which to decode corresponding encoded element x_i, for recovery of corresponding vector element a_i, by means of computation $x_i \bullet k_i^{-1}$, and additionally undertake verification that said vector element is associated with user of interest.

Each element of key-stream k_i is alternatively subject to FF addition with corresponding biometric vector element a_i, to compute FF-encoded element $x_i = a_i \oplus k_i$, such that corresponding decoding and recovery is by means of FF additive inversion $x_i \oplus k_i$, with equivalent verification as aforesaid.

Each received test vector is subsequently subject to error correction as previously established subsequent to computation of reference vectors.

Each test vector element a_i is then subject to comparison against previously established reference vectors, via computation of distance measure $d(a_i, \alpha_j)$, where α_j is an element of the set of reference vectors, and subsequently assessment of authentication outcome based on singular or plural valuations of said distance measure.

Operational sequence of key-masked biometric post-processing

Biometric vector is optionally subject to additional key-masking operation at instance of initial registration, such that masking operation is specific to user and additionally server of interest, and that masking key k', as exemplified without limitation by hash output H(B,α) of server public-key and user private-key, is furthermore presumed secret and exclusive to user of interest.

Masking key k' established as aforesaid is then subject to FF addition with corresponding biometric element in vector-stream $[a_1, a_2, \cdots, a_i, \cdots]$, to compute FF-masked element $x'_i = a_i \oplus k'$ in masked-stream $[a'_1, a'_2, \cdots, a'_i, \cdots]$, with stipulation that said masking operation preserves distance measures $d(a'_i, \alpha'_j) = d(a_i, \alpha_j)$ between biometric vectors subject to masking by means of same masking key, as would arise exclusively for

combination of particular user of interest undertaking authentication interaction with particular server of interest.

Operational sequence of user credential processing

User of interest, as associated with identity i and key-pair (α,A), is able to compute particular private-key by means of one-way computation with input of password α' or equivalent knowledge-based credential, as presumed secret and exclusive to user, as exemplified without limitation by hash output α = H(i,α').

User of interest, may alternatively be associated with multiple credentials of plurality n, as exemplified without limitation by password or equivalent knowledge-based credential; and one or more identifiers unique to client-side platform of interest; such that correct demonstration of at least k credentials, as specified threshold for authentication, is required for correct computation of private-key.

Private-key α in this alternative association is encoded by means of (k-1)-th degree polynomial in FF of interest, as output value of encoding polynomial $y(x) = \sum_{i=0}^{k-1} \alpha_i \bullet x^i$, modulo irreducible polynomial previously specified, at input value of x = 0, such that private-key is encoded as constant coefficient of encoding polynomial $y(0) = \alpha_0 = \alpha$.

Each credential is subsequently associated with (x,y) point on polynomial y(x) such that first-ordinate x results from outcome of one-way computation, with credential of interest as input, as subject to correct demonstration at point of credential demonstration; with corresponding applicable second-ordinate y = y(x), as are stored on client platform of interest, in anticipation of combination with said first-ordinate.

Correct computation for private-key at point of credential demonstration is then obtained by means of polynomial interpolation $\prod_{i \in S}(x_i, y_i)$ comprising any k coordinates (x,y), as predicated on correct demonstration of coordinates to plurality of previously specified threshold k.

The present invention supports a basic and a hardened embodiment.

Basic embodiment

User of interest presents biometric, as exemplified by face visage, to capture apparatus, as exemplified by video camera, attached to client platform deemed trustworthy; for purpose of registration by service provider of interest as being associated with particular user.

Client computes of vector-stream $[a_1, a_2, \cdots, a_i, \cdots]$ resulting from user presentation preferably encompassing range of illumination, pose and expression variations under environmental conditions as deemed representative of realistic operational conditions; and as possibly subject to refreshment by user on periodic basis, or as deemed necessary by service provider of interest.

Client establishes key specific to registration interaction as aforesaid,

computes applicable key-stream $[k_1, k_2, \cdots, k_i, \cdots]$, and then encodes vector-stream resulting in $[x_1, x_2, \cdots, x_i, \cdots]$.

Client transmits encoded vector-stream to registration server operated by service provider, such that any interception does not result in disclosure of biometric information.

Registration server computes key-stream as aforesaid, inverts each element in key-stream resulting in $[k_1^{-1}, k_2^{-1}, \cdots, k_i^{-1}, \cdots]$, and then decodes vector-stream to recover vector-stream $[a_1, a_2, \cdots, a_i, \cdots]$.

Server stores one or more vectors in presented vector-stream to as reference vectors for use in subsequent authentication interactions by user.

Subsequent to aforesaid registration, user of interest presents biometric to capture apparatus attached to client platform, for purpose of authentication. Client then computes vector-stream $[a_1, a_2, \cdots, a_i, \cdots]$ resulting from user presentation. Client furthermore establishes key specific to authentication interaction of interest, computes applicable key-stream, and then encodes vector stream. Client transmits encoded vector-stream to authentication server

operated by service provider, such that any interception does not result in disclosure of biometric information. Authentication server subsequently computes key-stream as aforesaid, inverts each element in key-stream, and then decodes vector-stream to recover vector-stream $[\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_i, \cdots]$. Registration server finally computes distance measures $d(\mathbf{a}_i, \alpha_j)$ to assess outcome of authentication interaction.

Basic embodiment presumes user authentication based on correct demonstration of one or more credentials, inclusive of without limitation, password or equivalent knowledge-based credential, or optionally identifiers unique to client-side platform. During registration, user of interest presents applicable credential or credentials to client sub-system on platform deemed to be trustworthy. Client computes private-key α as one-way computation with inputs inclusive of credential as aforesaid; and then corresponding public-key A = G • α by means of EC scalar multiplication. Client transmits said public-key to server on channel with security previously established.

During authentication subsequent aforesaid registration, user of interest presents applicable credential or credentials of interest to client sub-system. Client undertakes computation of private-key as one-way computation with inputs inclusive of credential as aforesaid; and then engagement into key-establishment interaction with inputs inclusive of corresponding private-key; with correct outcome predicated on correct demonstration of said singular credential.

Hardened embodiment

Hardened embodiment requires additional operations pertaining to computation of masking key, and subsequently masking of test biometric vector-stream.

User of interest presents information and credentials necessary to undertake computation of masking key. Client computes masking key as outcome of one-way function with inputs provided by user as aforesaid; and then undertakes masking of vector-stream arising from user biometric demonstration as aforesaid.

Hardened embodiment presumes user authentication based on correct demonstration of aggregate of credentials, inclusive of without limitation, password or equivalent knowledge-based credential, and optionally one of plurality of credentials arising from platform-specific identifier. During registration, user of interest presents; to client sub-system, on platform deemed to be trustworthy; applicable credential or credentials; such that authentication threshold is specified to be aggregate of knowledge-based credential, and optionally at least one such platform-specific identifier.

Client computes random coefficients of interpolating polynomial y(x) of linear degree in FF of interest, such that coordinate (x,y) on said polynomial is associated with each credential as aforesaid; with first-ordinate x as one-way computation with inputs inclusive of credential, and second-ordinate y = y(x) corresponding to each respective credential; and furthermore with corresponding public-key A = G • y(0). Client then transmits said public-key to server on channel with security previously established in registration interaction. Client retains set of second-ordinate values $[y_1, y_2, \cdots, y_n]$, as respectively corresponds to set of previously established credentials.

During authentication, user of interest presents knowledge-based credential of interest to client sub-system on platform of interest. Client concurrently undertakes determination of platform-specific identifier as presently applicable; and then computation of first-ordinates from one-way computation with inputs inclusive of respective credentials; formulation of interpolating coordinates from retrieval of second-ordinates corresponding to said first-ordinates; computation of private-key as interpolation from said coordinates; and then engagement into key-establishment interaction with inputs inclusive of corresponding private-key; with correct outcome predicated on correct demonstration of said plurality of credentials.

CLAIMS

1. A method of cryptographic encoding on biometric data in discretised vector representation, comprising

Zero knowledge (ZK) encoding (150) at a client sub-system (220) of a biometric vector-stream, as comprised of a sequence of biometric vector-frames, during an authentication interaction between a client (220) and a server sub-system (240), further comprising such encoding as different from particular biometric vector-frame in aforesaid vector-stream to any other biometric vector-frame in such vector-stream;

securely transmission of an encoded biometric vector-stream from a particular user (210) operating the client (220) to the server (240); and

decoding (160) at the server (240) of the encoded biometric vector-stream as received from the client (220); further comprising

limitation in capability of server (240) to undertake such decoding subject to correct demonstration of private PKC credential corresponding to public credential stipulated by the user (210) during the authentication interaction.

2. A method according to claim 1, wherein server undertakes verification, subsequent to decoding of biometric vector-stream received from client in authentication interaction of interest; such that each and every biometric vector-frame in aforesaid vector-stream is correctly received as transmitted from client; and furthermore subject to user of interest undertaking correct demonstration of private PKC credential during authentication interaction, as corresponds to public PKC credential used by the server to perform verification.

3. A method according to claim 1, wherein encoding and decoding functions acting on the biometric vector-streams comprises a pair of mutually

inverse trapdoor one-way functions such that correct combination of encode and decode functions on biometric vector-streams has no effect on subsequent computation of a distance measurement (170), as undertaken with biometric vector-streams as input, with subsequent biometric authentication based on the distance measurement between test biometric vectors arising from present authentication interaction, and reference biometric vectors previously established by the user with the server.

4. A method according to claim 3, wherein the method further comprises masking (140) of the biometric vector-stream such as to have no effect on subsequent computation of the distance measurement; and further comprising masking function that is identically applicable on test biometric vectors and reference biometric vectors and dependent on a valuation of masking key, such valuation as presumed secret and exclusive to user of interest, and as further arises from output of one-way function acting on inputs inclusive, without limitation, of public credentials of server, and private credentials of user.

5. A method according to claim 4, wherein masking and encoding of the biometric vector-stream further comprises computations arising from finite fields (FF) of type

Galois Fields (GF) (2^n) modulo irreducible polynomial of n-th degree with binary (modulo-2) coefficients, and

Galois Fields (GF) (p^n) modulo irreducible polynomial of n-th degree with coefficients modulo small prime (p); wherein

representational form of biometric vector-frame is of

equal component-level dimensionality, or multiple thereof; and furthermore of

consistent component-level structure to corresponding encoding, such that component-level discretisation is to 2^m

or p possible values, as the case might be for applicable finite field.

6. A method according to claim 5, wherein masking (140) and encoding (150) of the biometric vector-stream further comprises FF computations arising from the Galois Fields (GF) (2^n) representational form; wherein product of biometric vector dimension m and bit-length of component-level discretisation m', as resulting in 2^m possible valuations per component, is equal to bit-length of Galois Fields (GF) (2^n) representation or multiple thereof.

7. A method according to claim 5, wherein the method further comprises masking (140) of the biometric vector-stream at the client during authentication interaction between the user and the server, and wherein masking is undertaken by means of FF computation, with inputs of masking key and any particular element in biometric vector-stream, such that a distance measurement between test biometric vector and reference biometric vector is specified by Hamming distance between test biometric vector and reference biometric vector, and as furthermore invariant under masking computation as aforesaid.

8. A method according to claim 3, wherein the client, as representative of a particular user, and the server engage in interactive key establishment, inclusive of without limitation the authenticated Diffie-Hellman (ADH) protocol and variations thereof, wherein both the client and the server undertake independent contribution of random key-pairs, mutual challenge of correct private-key demonstration by other party, resulting from computation on corresponding public-key associated with other party and concluding in independent computation for session-key as aforesaid, subject to correct execution by both the client and the server.

9. A method according to claim 3, wherein the client, as representative of a particular user, undertakes key distribution to the server, inclusive of

without limitation the signcryption protocol, wherein the client undertakes computation of random key-pair and derivative session-key authentication, with the server public-key and the user private-keys as protocol inputs; subsequent to which the server undertakes recovery and verification of session-key, with the user public-key and the server private-key as protocol inputs; such that the session-key as delivered can be authenticated to be correctly received as transmitted, and furthermore correctly associated with the user engaged in authentication interaction.

10. A method according to claim 3, wherein the session-key as established on the client, as representative of user, and the server wherein

client undertakes computation of key-stream of equal frame-length to stream of biometric vector-frames wherein said computation is an outcome of

cryptographic key schedule function, inclusive of without limitation, block ciphers and keyed-hash message authentication code (HMAC) functions, with applicable established session-key as function input; and then

encoding, by Galois Field (GF) computation, of each element in key-stream with corresponding element in vector-stream; subsequent to which

server undertakes independent computation of key-stream of equal frame-length to received stream of encoded vector-frames wherein the computation is an outcome of

cryptographic key schedule function with independently established session-key as function input;

computation of stream of key inverses, by applicable Galois Field (GF) inversion, of computation previously undertaken at encoding, of each element in said key-stream; and then

decoding, by aforesaid Galois Field (GF) inversion, of each element in stream of key inverses with corresponding element in encoded vector-stream of interest; such that

server is able to establish that vector-stream is correctly received as transmitted, and furthermore correctly associated with the user engaged in authentication interaction.

11. A method of user authentication of a client by a server, the method comprising

user presenting biometric to a capture apparatus attached to the client;

client undertaking

generation of test vector-stream resulting from the user presentation,

establishment of session-key specific to particular authentication interaction;

computation of applicable key-stream, and resulting encoded vector-stream for transmission to the server;

and subsequently server undertaking

independent establishment of said session-key specific to particular authentication interaction;

computation of applicable key-stream, inversion thereof and resulting decoded vector-stream;

computation of distance measures between elements of test vector-stream, as presently received from user of interest during authentication, against set of reference vector-frames as previously received from the user during registration; and

assessment of authentication outcome based on distance measures between set of test and reference vector-frames.

12. A method according to claim 11, wherein the client further undertakes

application of masking function on biometric vector-stream, resulting in computation of masked vector-stream from corresponding vector-stream, as arising from masking key unique and specific to combination of user and server of interest, such that valuation of masking key is presumed secret and exclusive to user of interest.

13. A method according to claim 12, wherein the server further undertakes

assessment of authentication outcome based on distance measures between set of test and reference vector-frames, such that distance measurements are unaffected by application of same mask function on both test and reference vector-frames, as subject to use of identical masking key on both test and reference vector-frames.

14. A method according to claim 11, wherein the correctness of key establishment interaction as aforesaid is dependent on correct prior demonstration by the user to the client of knowledge-based credential, as presumed secret and exclusive to the user; and which comprises inputs inclusive of but not limited to textual sequence with input via keyboard or keypad, or geometric sequence with input via touch-sensitive screen.

15. A method according to claim 14, wherein the correctness of key establishment interaction as aforesaid is additionally dependent on correct determination by the client sub-system of particular platform-specific identifier from plurality thereof, corresponding to singular particular platform from plurality thereof previously designated by the user and as presumed unique and specific to the particular platform.

16. A method according to claim 14, wherein the private-key is obtained from output of one-way computation, with input inclusive of knowledge-based credential as aforesaid.

17. A method according to claim 15, wherein the private-key is obtained from output of computation to interpolate for constant coefficient of random credential-encoding polynomial of linear degree, as defined on FF finite field of interest, from coordinates comprising:

first-ordinate as output of one-way computation, with inputs inclusive of knowledge, and optionally platform-specific credentials as applicable; and

second-ordinate as output of said polynomial as evaluated at input of corresponding first-ordinate, with such particular valuation of polynomial; as generated during registration interaction, and as retained on the client thereafter.

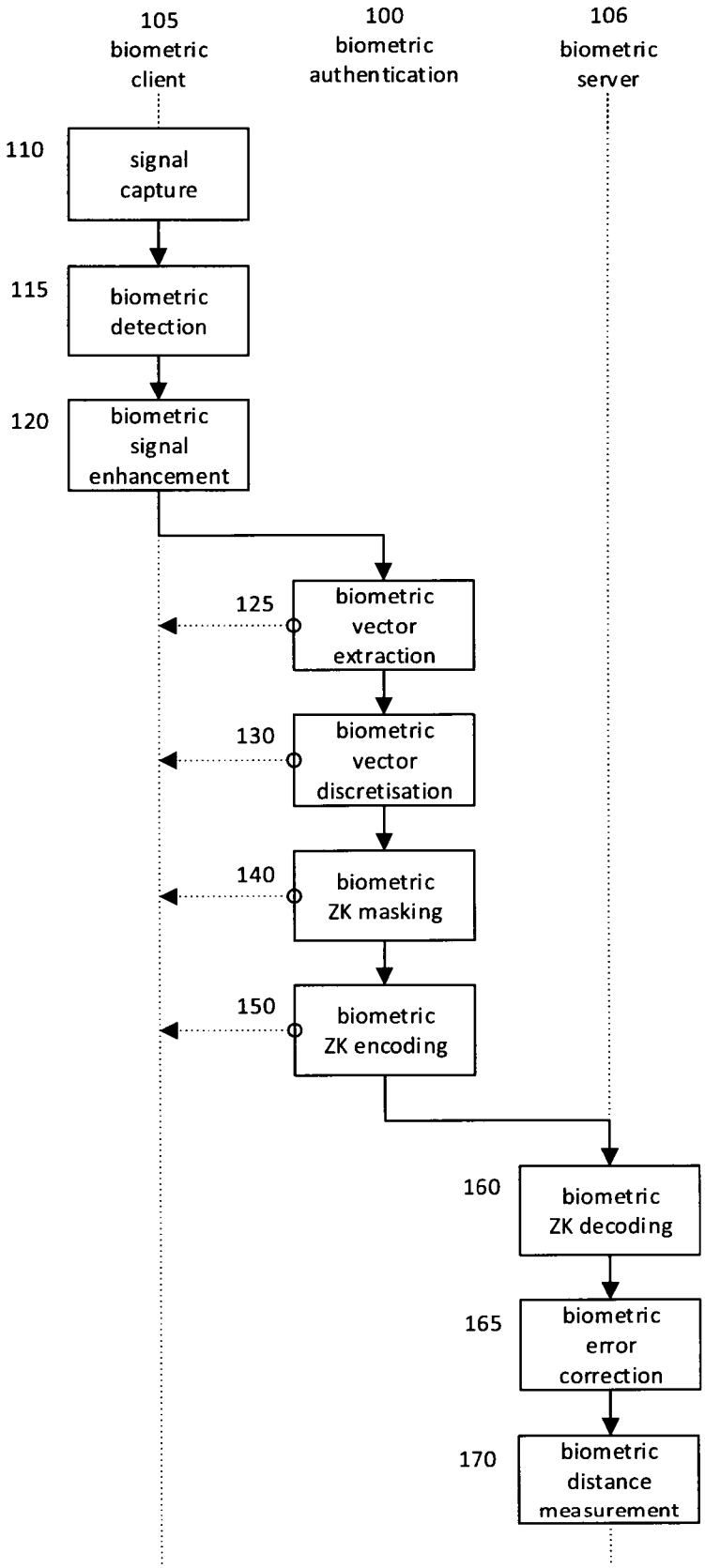
105
biometric
client
100
biometric
authentication
106
biometric
server
110
signal
capture
115
biometric
detection
120
biometric
signal
enhancement
125
biometric
vector
extraction
130
biometric
vector
discretisation
140
biometric
ZK masking
150
biometric
ZK encoding
160
biometric
ZK decoding
165
biometric
error
correction
170
biometric
distance
measurement

FIGURE 1

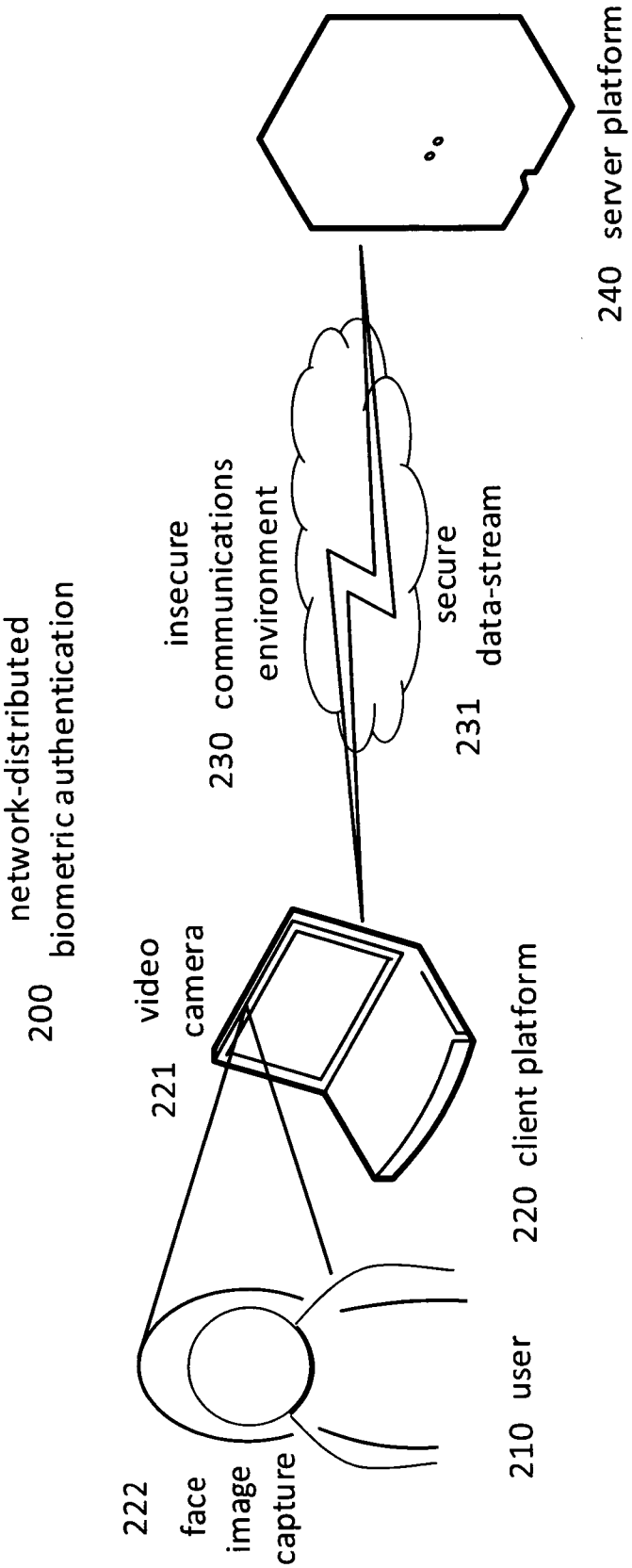
200 network-distributed biometric authentication
221 video camera
222 face image capture
210 user
220 client platform
230 insecure communications environment
231 secure data-stream
240 server platform

FIGURE 2A

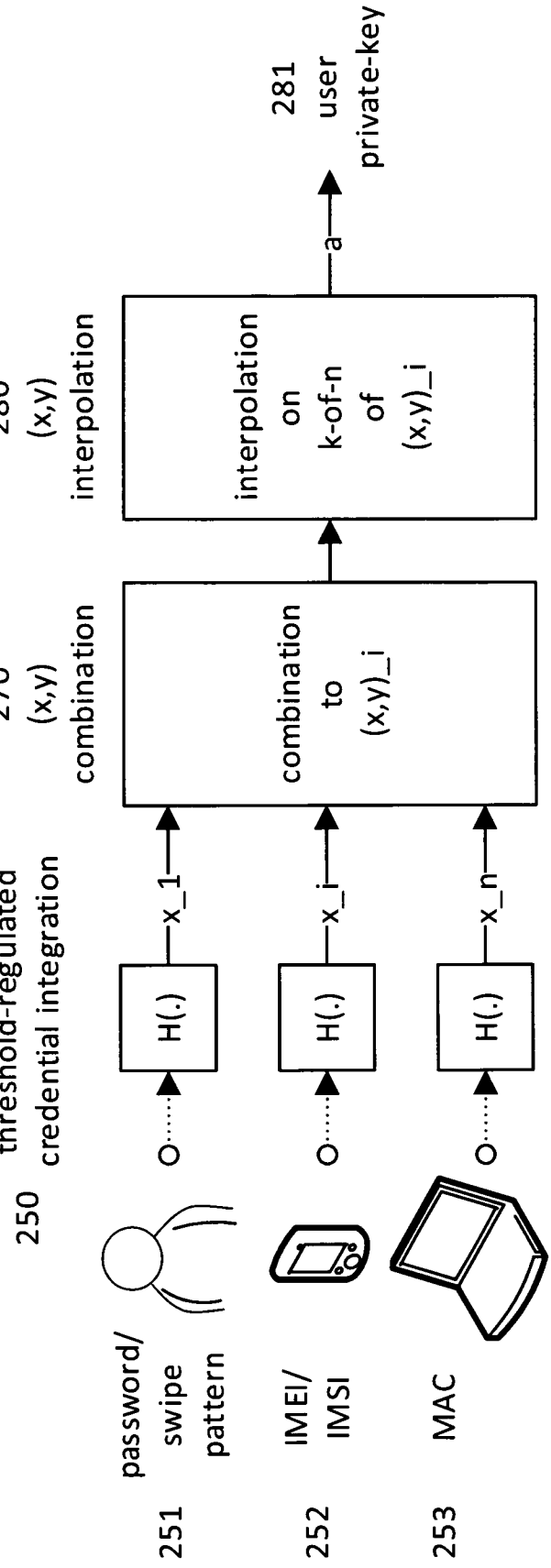
250
threshold-regulated credential integration
270
(x,y) combination
280
(x,y) interpolation
281
user private-key
password/ swipe pattern
IMEI/ IMSI
MAC
251
252
253
H(.)
H(.)
H(.)
x_1
x_i
x_n
combination to (x,y)_i
interpolation on k-of-n of (x,y)_i
a
ZK function
260
x-ordinate
261
(x,y) coordinate
271

FIGURE 2B

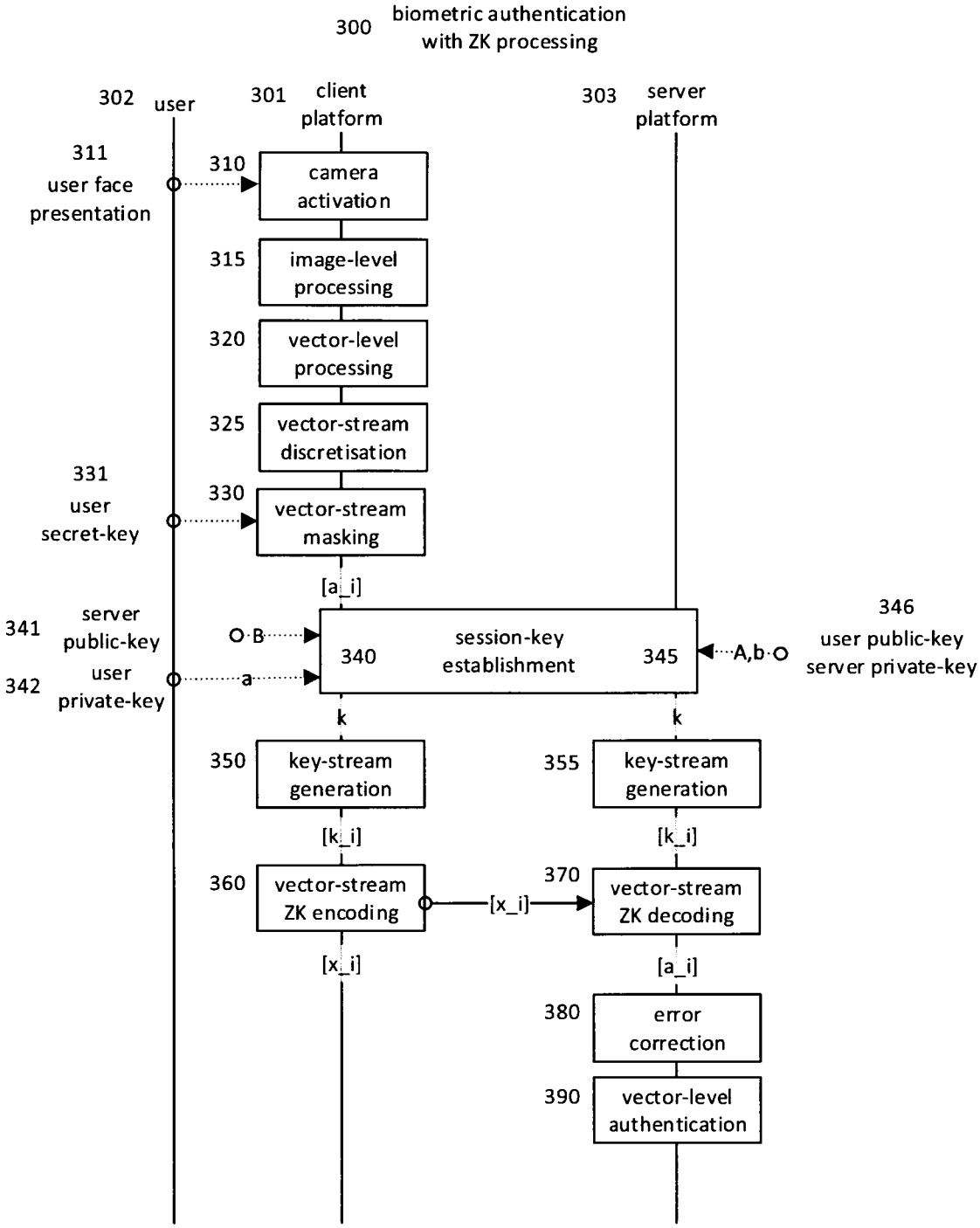
300 biometric authentication with ZK processing
302 user
301 client platform
303 server platform
311 user face presentation
310 camera activation
315 image-level processing
320 vector-level processing
325 vector-stream discretisation
331 user secret-key
330 vector-stream masking
[a_i]
341 server public-key
342 user private-key
B
a
340 session-key establishment
345
A,b
346 user public-key server private-key
k
k
350 key-stream generation
355 key-stream generation
[k_i]
[k_i]
360 vector-stream ZK encoding
[x_i]
370 vector-stream ZK decoding
[x_i]
[a_i]
380 error correction
390 vector-level authentication

FIGURE 3

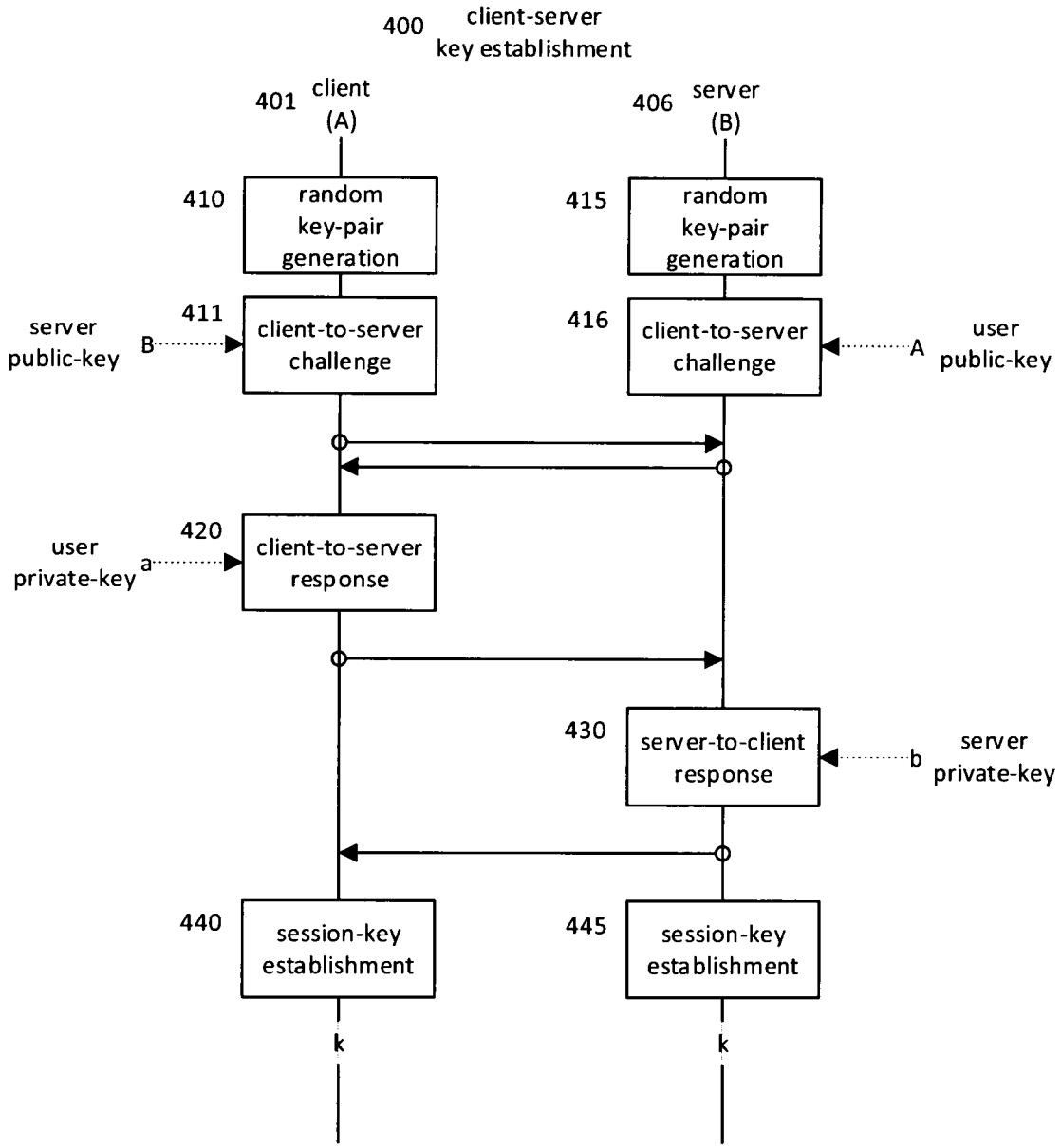
400
client-server
key establishment
401
client
(A)
406
server
(B)
410
random
key-pair
generation
415
random
key-pair
generation
411
server
public-key
B
client-to-server
challenge
416
client-to-server
challenge
A
user
public-key
420
user
private-key
a
client-to-server
response
430
server-to-client
response
b
server
private-key
440
session-key
establishment
445
session-key
establishment
k
k

FIGURE 4A

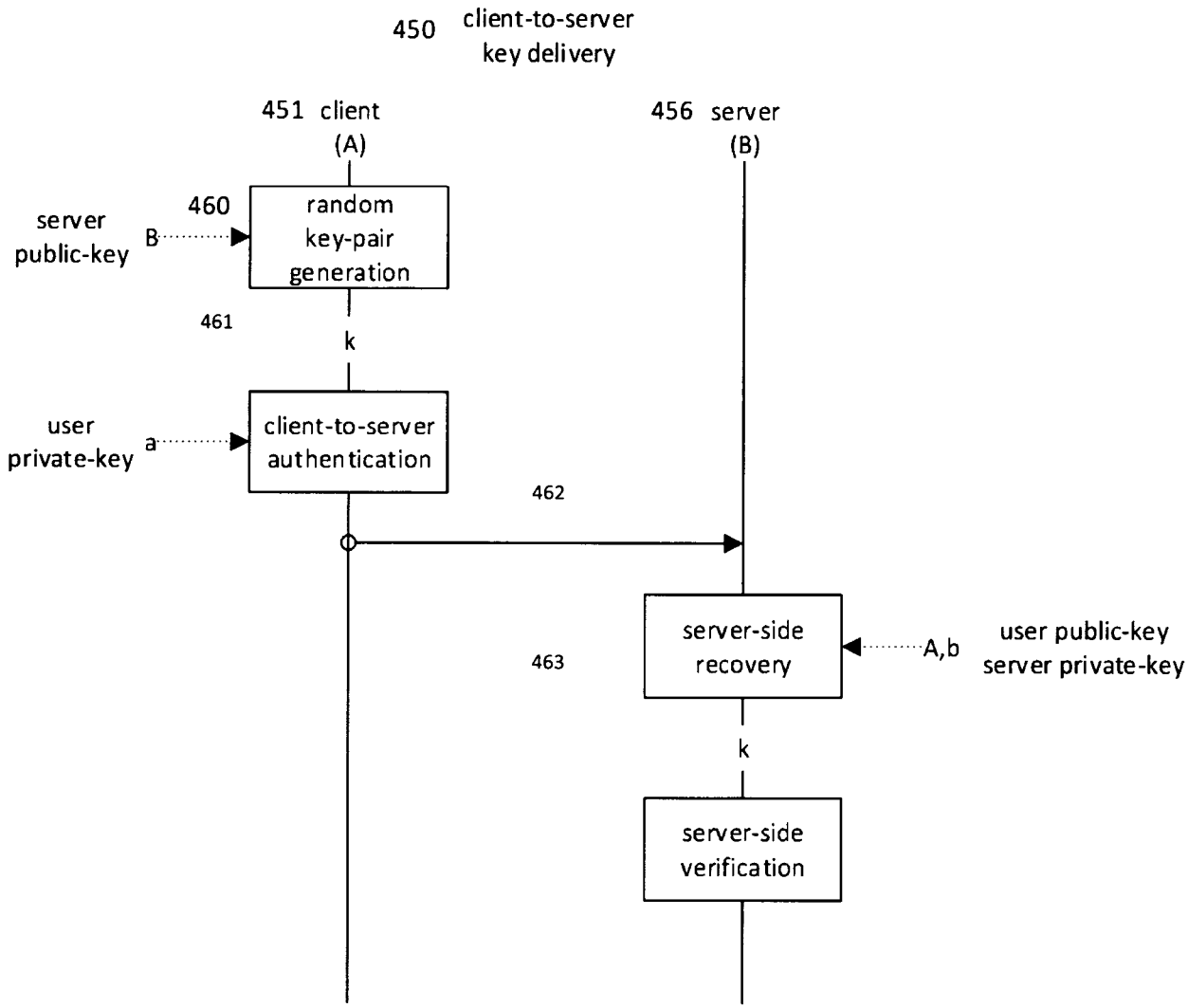
450 client-to-server key delivery
451 client (A)
456 server (B)
server public-key
B
460
random key-pair generation
461
k
user private-key
a
client-to-server authentication
462
server-side recovery
A,b
user public-key
server private-key
463
k
server-side verification

FIGURE 4B

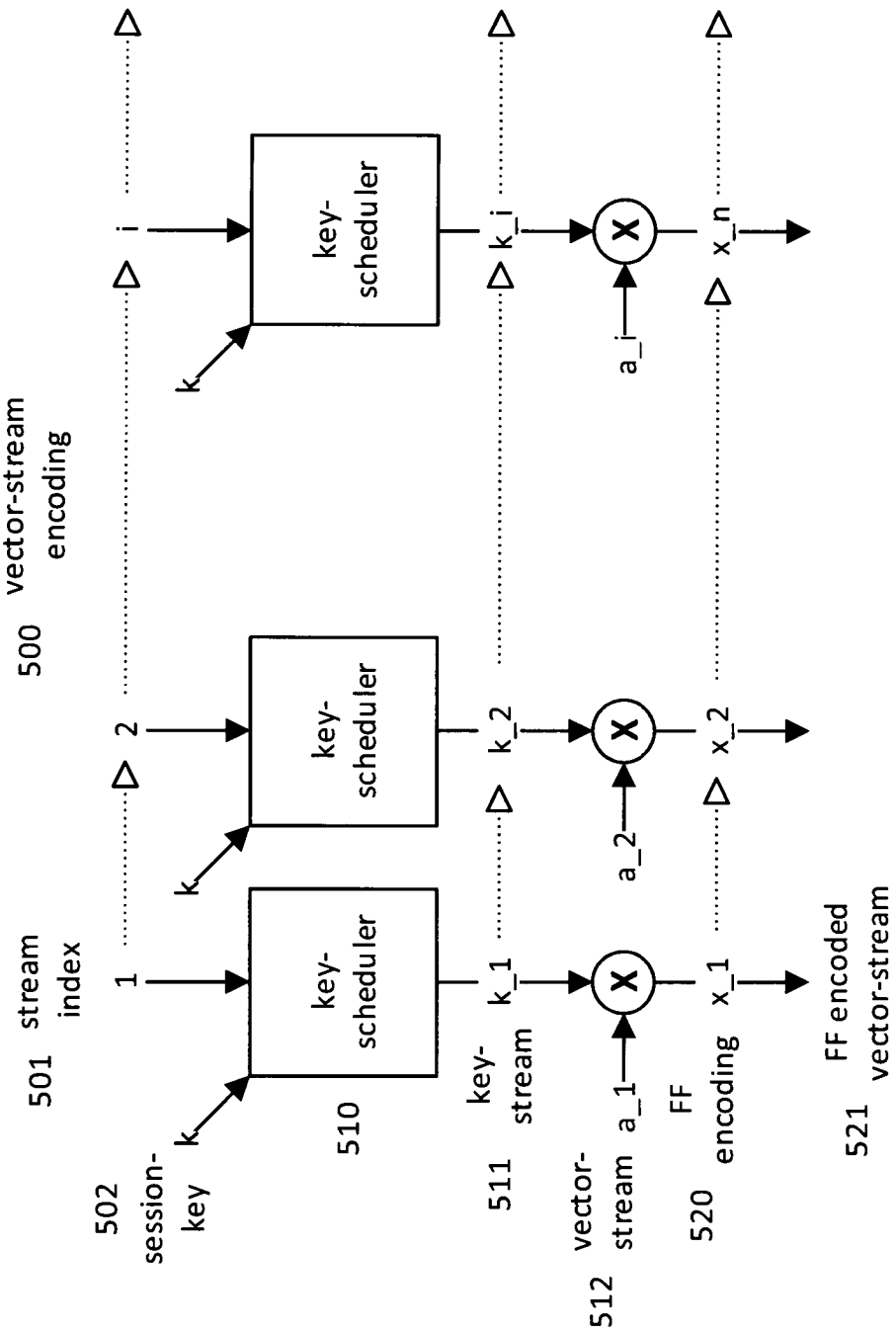
500 vector-stream encoding
501 stream index
1
2
i
key-scheduler
key-scheduler
key-scheduler
510
k
k
k
502 session-key
key-stream
511
k_1
k_2
k_i
vector-stream
512
a_1
a_2
a_i
FF encoding
520
x_1
x_2
x_n
FF encoded vector-stream
521

FIGURE 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2015/000081

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L9/32(2006.01)i, G06F21/32(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. H04L9/32, G06F21/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2016
Registered utility model specifications of Japan 1996-2016
Published registered utility model applications of Japan 1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2007/108397 A1 (SHARP KABUSHIKI KAISHA) 2007.09.27, pars.[0056]-[0085], Figs.1-5	1-17
Y	JP 2011-203822 A (SONY CORPORATION) 2011.10.13, pars.[0089]-[0105]	1-17
Y	MENEZES, A. J. et al., HANDBOOK of APPLIED CRYPTOGRAPHY, CRC Press, 1997, pp.228-233, 507-512, 524-526	1-17
A	US 2002/0056043 A1 (SENSAR, INC.) 2002.05.09, pars.[0077]-[0082], Fig.13	1-17
A	US 2004/0193893 A1 (BRAITHWAITE, M. et al.) 2004.09.30, pars.[0020]-[0068]	1-17

☑ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29.01.2016	09.02.2016

Name and mailing address of the ISA/JP	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	NAKAZATO, Hiromasa Telephone No. +81-3-3581-1101 Ext. 3546

5S 9364

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2015/000081

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014/0006290 A1 (NATURAL SECURITY SAS) 2014.01.02, pars.[0053]-[0113]	1-17

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/MY2015/000081

WO 2007/108397 A1	2007.09.27	None	
JP 2011-203822 A	2011.10.13	None	
US 2002/0056043 A1	2002.05.09	JP 2005-513641 A	2005.05.12
		WO 2003/053123 A2	2003.07.03
		EP 1449086 A2	2004.08.25
		CA 2465227 A1	2003.07.03
		KR 10-2004-0053253 A	2004.06.23
		AU 2002365086 A1	2003.07.09
		IL 144331 A	2006.04.10
US 2004/0193893 A1	2004.09.30	JP 2004-537103 A	2004.12.09
		WO 2002/095657 A2	2002.11.28
		EP 1402681 A2	2004.03.31
		CA 2447578 A1	2002.11.28
		KR 10-2004-0000477 A	2004.01.03
US 2014/0006290 A1	2014.01.02	JP 2014-503159 A	2014.02.06
		WO 2012/098306 A1	2012.07.26
		EP 2666255 A1	2013.11.27
		FR 2970612 A1	2012.07.20
		AU 2011356179 A1	2013.08.15
		CA 2825050 A1	2012.07.26
		CN 103477585 A	2013.12.25
		EA 201391054 A1	2013.12.30
		NZ 613485 A	2015.06.26