

(51) International Patent Classification:
H04L 9/08 (2006.01)(21) International Application Number:
PCT/US2009/043533(22) International Filing Date:
12 May 2009 (12.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/052,333 12 May 2008 (12.05.2008) US(71) Applicant (for all designated States except US): **INTER-DIGITAL PATENT HOLDINGS, INC.** [US/US]; 3411 Silverside Road, Concord Plaza, Suite 105, Hagley Building, Wilmington, DE 19810 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **YE, Chunxuan** [CN/US]; 1021 Penn Circle, Apt. E502, King Of Prussia, PA 19406 (US). **REZNIK, Alexander** [US/US]; 1212 River Road, Titusville, NJ 08560 (US).(74) Agent: **KLINE, Adam, D.**; Volpe And Koenig, P.c., United Plaza, Suite 1600, 30 South 17th Street, Philadelphia, PA 19103 (US).

(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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: INFORMATION-THEORETICALLY SECURE SECRECY GENERATION

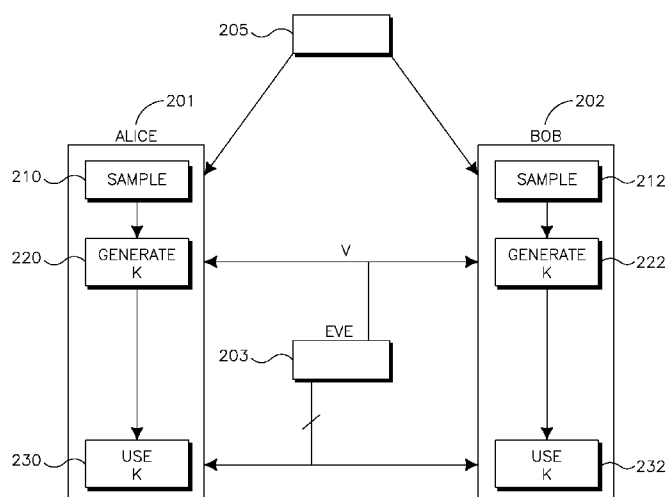


FIG. 2

210, 212 ECHANTILLON
220, 222 GENERATION DE LA CLE
230, 232 UTILISATION DE LA CLE

200

(57) Abstract: A method and apparatus are provided for performing information-theoretically secure cryptography using joint randomness not shared by others. Two valid communicating entities independently generate samples of a shared source that is not available to an illegitimate entity. The shared source may be a satellite signal, and each legitimate entity may generate uniformly distributed samples from a binary phase-shift keying signal received on an independent channel. Alternatively, the shared source may be a channel between the two legitimate entities, such that each legitimate entity generates samples of unknown distribution based on the channel impulse response of the channel. One legitimate entity generates an encryption key, a quantization error, and a syndrome from its samples. The quantization error and the syndrome are reported to the other legitimate entity. The other legitimate entity generates a matching encryption key using its samples, the quantization error, and the syndrome.

[0001] INFORMATION-THEORETICALLY SECURE
 SECRECY GENERATION

[0002] FIELD OF INVENTION

[0003] This application is related to wireless communications.

[0004] BACKGROUND

[0005] In a typical wireless communication scenario two wireless transmit/receive units (WTRUs), Alice and Bob, communicate with each other on a channel. To exclude an eavesdropper, Eve, Alice and Bob cryptographically protect their communications. However, traditional cryptographic techniques, which rely on computational difficulty, are increasingly ineffective as the availability of computing power increases. Therefore, it would be advantageous to provide a cryptographic technique that is information-theoretically secure, rather than one based on computational difficulty.

[0006] SUMMARY

[0007] A method and apparatus are provided for performing information-theoretically secure cryptography using joint randomness not shared by others. Two valid communicating entities independently generate samples of a shared source that is not available to an illegitimate entity. The shared source may be a satellite signal, and each legitimate entity may generate uniformly distributed samples from a binary phase-shift keying signal received on an independent channel. Alternatively, the shared source may be a channel between the two legitimate entities, such that each legitimate entity generates samples of unknown distribution based on the channel impulse response of the channel. One legitimate entity generates an encryption key, a quantization error, and a syndrome from its samples. The quantization error and the syndrome are reported to the other legitimate entity. The other legitimate entity generates a matching encryption key using its samples, the quantization error, and the syndrome.

[0008] BRIEF DESCRIPTION OF THE DRAWINGS

[0009] A more detailed understanding may be had from the following description, given by way of example in conjunction with the accompanying drawings, wherein:

[0010] Figure 1 shows an example block diagram of a wireless transmit/receive unit for performing wireless communications using joint randomness not shared by others;

[0011] Figure 2 shows an example block diagram of a network for performing wireless communications using joint randomness not shared by others with a source of uniformly distributed correlated random values;

[0012] Figure 3 shows an example of a method for shared secret key generation by Alice using uniformly distributed input samples;

[0013] Figure 4 shows an example of a method for shared secret key generation by Bob using uniformly distributed input samples;

[0014] Figure 5 shows an example block diagram of a network for performing wireless communications using joint randomness not shared by others using a reciprocal wireless channel;

[0015] Figure 6 shows an example of a method for universal shared secret key generation by Alice;

[0016] Figure 7 shows an example of a method for universal shared secret key generation by Bob;

[0017] Figure 8 shows an example of a rate-matching method;

[0018] Figure 9 shows an example of a method for converting input samples of unknown distribution to uniformly distributed samples;

[0019] Figure 10 shows an example of a method for generating uniformly distributed samples; and

[0020] Figure 11 shows an example of a method for computing a log-likelihood ratio.

[0021] DETAILED DESCRIPTION

[0022] When referred to hereafter, the term “wireless transmit/receive unit (WTRU)” includes but is not limited to a user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a cellular telephone, a personal digital assistant (PDA), a computer, or any other type of user device capable of operating in a wireless environment. When referred to hereafter, the terminology “base station” includes but is not limited to a Node-B, a site controller, an access point (AP), or any other type of interfacing device capable of operating in a wireless environment. When referred to hereafter, the term “Alice” includes a WTRU or a base station that is a legitimate communicating entity. When referred to hereafter, the term “Bob” includes a WTRU or a base station that is a legitimate communicating entity. When referred to hereafter, the term “information-theoretically secure” includes but is not limited to perfectly secure, unconditionally secure, and nearly information-theoretically secure.

[0023] Figure 1 is an example block diagram of a wireless transmit/receive unit (WTRU) 100 for performing wireless communications using joint randomness not shared by others (JRNSO). The WTRU 100 includes a processor 110, an antenna 120, a user interface 125, a display 130, and a transceiver 135. Optionally, the transceiver may include a transmitter, a receiver, or a satellite receiver. The WTRU 100 also includes a channel estimator 140, a post processing unit 145, a data conversion unit 150, a quantization unit 155, a source coding unit 160, a channel coding unit 165, a decoding unit 170, and a privacy amplification (PA) processor 175. The configuration shown is for illustrative purposes. A WTRU may include only a subset of the elements described herein. For example, a particular embodiment of a WTRU 100 may only include a channel estimator 140, a post processing unit 145, a decoding unit 165, and a PA processor 170. The processor 110 is shown as including the channel estimator 140, the post processing unit 145, the data conversion unit 150, the quantization unit 155, the source coding unit 160, the channel coding unit 165, the decoding unit 170, and the privacy amplification (PA) processor 175 for illustration; however, one or more of these elements may be a separate unit.

[0024] Figure 2 shows an example block diagram of a network 200 for performing wireless communications using joint randomness not shared by others (JRNSO) with a source of uniformly distributed correlated random values. The network 200 includes two legitimate WTRUs, Alice 201 and Bob 202, and an illegitimate eavesdropper, Eve 203. The network 200 also includes a source of uniformly distributed correlated random values 205. For example, the source may be a binary phase-shift keying (BPSK) satellite signal that is received by Alice 201 and Bob 202 through independent channels. Although Alice 201, Bob 202, and Eve 203 are shown individually, the communications may involve multiple legitimate and illegitimate entities.

[0025] Alice 201 and Bob 202 each generate input samples at 210, 212. The input samples are based on contemporaneous estimates of the source of uniformly distributed correlated random values 205 and is not available to Eve 203. Although Alice's channel is independent from Bob's, their estimates are highly correlated. The input samples taken by Alice 201 and Bob 202 may be expressed as X^n and Y^n respectively, where X^n and Y^n include n independent and identically distributed repetitions of the correlated random values X and Y , such that $X^n = (X_1, \dots, X_n)$ and $Y^n = (Y_1, \dots, Y_n)$. Where the distribution of the discrete random variable U is such that the probability that $U = 1$ is equal to the probability that $U = -1$, and the distribution of the random values Z_A and Z_B is Gaussian, such that $N(0, N_A)$ and $N(0, N_B)$, the correlation between the random values X and Y may be expressed as $X = U + Z_A$ and $Y = U + Z_B$. The random values U , Z_A , and Z_B are mutually independent. Although equal values of N_A and N_B , and a signal to noise ratio (SNR) of $\frac{1}{N}$, are used for simplicity herein, other values are applicable.

[0026] Alice 201 and Bob 202 communicate with each other over a public channel and each generates a shared secret key K , at 220, 222. The public keys are based on their respective input samples X^n , Y^n and their public communications V . Alice 201 generates the bit string K_A based on (X^n, V) , and Bob 202 generates the bit string K_B based on (Y^n, V) . Where $\epsilon > 0$ and κ is the

finite range of the shared secret key K , the shared secret key K is uniformly distributed, such that $\frac{1}{n} H(K) \geq \frac{1}{n} \log |\mathcal{K}| - \epsilon$, nearly statistically independent of V , such that $\frac{1}{n} I(K;V) \leq \epsilon$, and is almost the same at Alice 201 and Bob 202, such that $\Pr(K=K_A=K_B) \geq 1 - \epsilon$. Alice 201 and Bob 202 use the shared secret key K to perform information-theoretically secure communications, at 230, 232.

[0027] Although Eve 203 may observe the public communications V , Eve 203 does not observe the signal 205 and cannot decrypt the information-theoretically secure communications between Alice 201 and Bob 202. For example, where Eve 203 does not have a receiver capable of receiving the signal, is out of range of the signal, does not know which signal to sample, or does not know the sampling time period, Eve 203 cannot receive the signal.

[0028] Figure 3 shows an example of a method for shared secret key generation 220 by Alice 201 using uniformly distributed input samples. The input samples X^n are quantized, at 310. The quantization produces quantization values X_b^n , and quantization errors E^n . The quantization values X_b^n are channel coded to generate syndrome bits S , in terms of a given block error correction code, at 320. The syndrome bits S and the quantization errors E^n are transmitted through an error-free public channel to Bob 202, at 330. The publicly transmitted syndrome bits S include $|S|$ bits of information, and the publicly transmitted quantization errors E^n are independent of X_b^n .

[0029] Privacy amplification is performed on the quantization values X_b^n , at 340. The publicly revealed information is hashed out of the quantization values X_b^n , leaving perfectly secret bits for the shared secret key K_A . The probability density function (PDF) of X is an even function and the quantized values X_b^n are a full entropy sequence, such that $H(X_b^n) = |X_b^n|$. Therefore, X_b^n includes n bits of information and at least $n - |S|$ perfectly secret bits are generated for the shared secret key K_A .

[0030] Quantization 310 includes identifying a partition, corresponding quanta, and quantization errors. Quantization produces quantization values X_b^n ,

and quantization errors E^n . Each quantized value $X_{b,i}$ includes the v bits corresponding to the v most significant values of the input, and the corresponding quantization error E_i includes $A-v$ bits corresponding to the remaining $A-v$ least significant values of the input. Although equiprobable quantization is shown, any suitable quantization method may be applied.

[0031] The partition includes a set of disjoint intervals $Q_1...Q_v$, which cover the sample range. The quantization boundaries of each interval Q_i is determined based on the samples. The corresponding quanta, which represent the quantized values, include a set of numbers $q_1...q_v$, such that $q_i \in Q_i$. Where a quantization level v which indicates the number of bits per quantization value and $0 \leq i \leq 2^v$, the determination of quantization boundaries may be expressed as $q_i = \frac{i}{2^v}$. The quantization error E^n may be expressed as $(E_i, \dots, E_n) = (|X_i|, \dots, |X_n|)$, and the generation of a quantized value uses a binary (single bit) quantizer and may be expressed as:

$$X_{b,i} = \begin{cases} 0, & X_i \leq 0; \\ 1, & X_i > 0; \end{cases}$$

Equation (1)

[0032] Figure 4 shows an example of a method for shared secret key generation 222 by Bob 202 using uniformly distributed input samples. The syndrome bits S and the quantization errors E^n are received from Alice 201, at 410. The input samples Y^n are decoded using the syndrome bits S and the quantization errors E^n to produce the decoded samples X_b^n , at 420. Privacy amplification is performed on the decoded samples X_b^n at 430.

[0033] Decoding 420 includes performing a modified belief-propagation algorithm to produce the decoded samples X_b^n . The modified belief-propagation algorithm includes calculating a per-bit log-likelihood ratio (LLR). The LLR is a logarithm of a ratio between the probability that $X_{b,i}$ is 0 and the probability that $X_{b,i}$ is 1. More generally, the LLR is related to the distances from V to the possible U values that cause $X_{b,i}$ to be 0 and that cause $X_{b,i}$ to be 1.

[0034] Where the inputs are based on a uniformly distributed binary signal, such as a BPSK modulated satellite signal, N is the noise power, $1 \leq i \leq n$, $E_i = e$, and $Y_i = y$, the LLR (the uniform distribution LLR algorithm) may be expressed as:

$$X_{b,i} = \ln \frac{\exp\left(-\frac{(-e-1)^2}{2N} - \frac{(y-1)^2}{2N}\right) + \exp\left(-\frac{(-e+1)^2}{2N} - \frac{(y+1)^2}{2N}\right)}{\exp\left(-\frac{(e-1)^2}{2N} - \frac{(y-1)^2}{2N}\right) + \exp\left(-\frac{(e+1)^2}{2N} - \frac{(y+1)^2}{2N}\right)}.$$

Equation (2)

[0035] During privacy amplification 430 publicly revealed information is hashed out of the decoded samples X_{b^n} , leaving the perfectly secret bits for the shared secret key K_B . The PDF of X is an even function and the decoded samples X_{b^n} are a full entropy sequence, such that $H(X_{b^n}) = |X_{b^n}|$. Therefore, the decoded samples X_{b^n} include n bits of information and at least $n - |S|$ perfectly secret bits are generated for the shared secret key K_B .

[0036] Figure 5 shows an example block diagram of a network 500 for performing wireless communications using JRNSO performed on a reciprocal wireless channel. The network 500 includes two legitimate WTRUs, Alice 501 and Bob 502, and an illegitimate eavesdropper, Eve 503. Although Alice 501, Bob 502, and Eve 503 are shown individually, the communications may involve multiple legitimate and illegitimate entities.

[0037] Alice 501 and Bob 502 each generate input samples, at 510, 512. The input samples are based on contemporaneous channel impulse response (CIR) measurements of their reciprocal wireless channel 505, which is not available to Eve 503. Due to channel reciprocity, the CIR estimates are composed of highly correlated samples of unknown distribution. Any two consecutive observations, at either Alice 501 or Bob 502, are independent if the time between observations is larger than the channel coherence time. The input samples taken by Alice 501 and Bob 502 may be expressed as X^n and Y^n respectively, where X^n and Y^n include n independent and identically distributed repetitions of the correlated random values X and Y , such that $X^n = (X_1, \dots, X_n)$ and $Y^n = (Y_1, \dots, Y_n)$.

[0038] Alice 501 and Bob 502 communicate with each other over a public channel and each generates a shared secret key K , at 520, 522. The shared secret keys K are based on their respective input samples X^n , Y^n and their public communications V . Alice 501 generates the bit string K_A based on (X^n, V) , and Bob 502 generates the bit string K_B based on (Y^n, V) . Where $\varepsilon > 0$ and $\mathcal{K}$ is the finite range of the shared secret key K , the shared secret key K is uniformly distributed, such that $\frac{1}{n} H(K) \geq \frac{1}{n} \log |\mathcal{K}| - \varepsilon$, nearly statistically independent of V , such that $\frac{1}{n} I(K; V) \leq \varepsilon$, and is almost the same at Alice 201 and Bob 202, such that $\Pr(K=K_A=K_B) \geq 1 - \varepsilon$. Alice 501 and Bob 502 use the shared secret key K to perform information-theoretically secure communications, at 530, 532.

[0039] Although Eve 503 may observe the public communications V , Eve 503 does not observe the shared reciprocal wireless channel 505 between Alice 501 and Bob 502, and cannot decrypt the information-theoretically secure communications between Alice 501 and Bob 502. For example, where Eve 503 is at least a few wavelengths away from Alice 501 and Bob 502, Eve's CIR measurements are not correlated with Alice's or Bob's.

[0040] Figure 6 shows an example of a method for universal shared secret key generation 520 by Alice 501. The input samples X^n are converted to uniformly distributed samples U^n , such that each uniformly distributed sample $U_i \in [0, 1)$, at 605. Each uniformly distributed sample U_i has a sample size of A , indicating A bits per sample. The uniformly distributed samples U^n are quantized, at 610. The quantization produces quantization values X_q^n , and quantization errors E^n .

[0041] Quantization 410 includes identifying a partition, corresponding quanta, and quantization errors. Quantization produces quantization values X_q^n , and quantization errors E^n . Each quantized value $X_{q,i}$ includes the v bits corresponding to the v most significant values of the input, and the corresponding quantization error E_i includes $A-v$ bits corresponding to the remaining $A-v$ least significant values of the input. Although equiprobable quantization is shown, any suitable quantization method may be applied.

[0042] The partition includes a set of disjoint intervals $Q_1 \dots Q_v$, which cover the sample range. The quantization boundaries of each interval Q_i is determined based on the samples. The corresponding quanta, which represent the quantized values, include a set of numbers $q_1 \dots q_v$, such that $q_i \in Q_i$. Where a quantization level v which indicates the number of bits per quantization value and $0 \leq v \leq 2^v$, the determination of quantization boundaries may be expressed as $q_i = \frac{i}{2^v}$.

[0043] Where the inputs are fixed point inputs, such as the uniformly distributed samples U^n , and v is less than A , the quantized value $X_{q,i}$ is the v most significant bits in U_i , and the quantization error E_i is the remaining $A-v$ least significant bits in U_i .

[0044] The quantization values X_q^n are source coded into bit strings X_b^n , at 615. For example, gray coding may be used to convert X_q^n to X_b^n . The source coded bit strings X_b^n are channel coded to generate syndrome bits S . Block Error Correction Coding is applied X_b^n to generate syndrome bits S , in terms of a given low density parity code (LDPC), at 620. The syndrome bits S and the quantization errors E^n are transmitted through an error-free public channel to Bob 502, at 630. The publicly transmitted syndrome bits S include $|S|$ bits of information, and the publicly transmitted quantization errors E^n are independent of X_b^n . The publicly revealed information is hashed out of the common bit string X_b^n , leaving perfectly secret bits for the shared secret key K_A , at 640.

[0045] Figure 7 shows an example of a method for universal shared secret key generation 522 by Bob 502. The input samples Y^n are converted to uniformly distributed samples V^n , such that each uniformly distributed sample $V_i \in [0,1)$, at 705. The syndrome bits S and the quantization errors E^n are received from Alice 501, at 710. The uniformly distributed samples V^n are decoded using the syndrome bits S and the quantization errors E^n to produce the decoded samples X_b^n , at 720. The publicly revealed information is hashed out of the decoded samples X_b^n , leaving the perfectly secret bits for the shared secret key K_B , at 730.

[0046] Decoding 720 includes performing a modified belief-propagation algorithm to produce the decoded samples X_b^n . The modified belief-propagation

algorithm includes calculating a per-bit log-likelihood ratio (LLR). The LLR is a logarithm of a ratio between the probability that $X_{b,i}$ is 0 and the probability that $X_{b,i}$ is 1. More generally, the LLR is related to the distances from V to the possible U values that cause $X_{b,i}$ to be 0 and that cause $X_{b,i}$ to be 1.

[0047] Where $1 \leq i \leq v$, the LLR L_i for $X_{b,i}$ may be computed using an unknown distribution LLR algorithm as shown in Figure 8. For example, where the quantization error E_i is 0.2 and the number of bits per quantized value v is 1, either U is 0.2 and $X_{b,1}$ is 0 or U is 0.7 and $X_{b,1}$ is 1. The value of U that is closer to V represents the more likely value of $X_{b,1}$. Where V is 0.3, $X_{b,1}$ is 0 and the LLR for $X_{b,1}$ is positive. Similarly, where V is 0.5, $X_{b,1}$ is 1 and the LLR for $X_{b,1}$ is negative. Therefore, the LLR L_1 is -0.1. Optionally, L_i may be scaled to the operational range of the modified belief-propagation algorithm by multiplying L_i with a constant.

[0048] Figure 9 shows an example of a method for converting input samples of unknown distribution to uniformly distributed samples. For simplicity, the conversion is described in reference to Alice's input samples X^n ; however, one skilled in the art would recognize that the method may be applied to Bob's input samples Y^n .

[0049] The input samples X^n are sorted according to the observed value of each input sample X_i , at 910. For example, the values X_i may be sorted in ascending order such that $\tilde{X}_1 \leq \dots \leq \tilde{X}_n$. Each sorted sample $\tilde{X}_i$ retains an association with the pre-sort index of the corresponding input sample X_i . The sorted samples $\tilde{X}^n$ are converted (transformed) into sorted uniformly distributed samples $\tilde{U}^n$, at 920. The sorted uniformly distributed samples $\tilde{U}^n$ are sorted into uniformly distributed samples U^n by sorting each sorted uniformly distributed sample $\tilde{U}_i$ according to the index of the corresponding input samples X_i , at 930. The resultant uniformly distributed samples U^n are inherently fixed-point values.

[0050] The conversion, which is based on an empirical distribution of the input samples, associates the sorted sample $\tilde{X}_i$ with the sorted uniformly distributed sample $\tilde{U}_i$. For example, the conversion is performed using a rate-

matching method as shown in Figure 10. Where X_i indicates the i^{th} sample of the input samples X^n , $F(X_i)$ indicates the number of samples in X^n that are less than the input sample X_i added to the number of samples in the input samples X^n that are equal to X_i and have an index less than i . The corresponding uniformly distributed sample U_i may be expressed as:

$$U_i = \frac{F(X_i)}{n} \quad \text{Equation (3)}$$

[0051] Where $0 \leq j \leq 2^A - 1$, the value of a uniformly distributed sample U_i may be expressed as $\frac{j}{2^A}$. Where $0 \leq j \leq 2^A$, the $C(j)$ uniformly distributed samples have a value of $\frac{j-1}{2^A}$.

[0052] Where $\lfloor x \rfloor$ is the largest integer less than x , the uniformly distributed samples U_i in $C(j)$ may be generated as shown in Figure 10. Thus, the uniformly distributed sample U_i corresponding to an input sample X_i may be expressed as $\frac{k}{2^A}$ where the input sample X_i may be expressed as:

$$\sum_{j=0}^k C(j) \leq F(X_i) < \sum_{j=0}^{k+1} C(j) \quad \text{Equation (4)}$$

[0053] Although conversion has been shown in terms of 2^A for simplicity, any integer number of values may be converted such that the unit interval $[0,1)$ is partitioned into equal sub-intervals with the data distributed among them as uniformly as possible.

[0054] Although features and elements are described above in particular combinations, each feature or element can be used alone without the other features and elements or in various combinations with or without other features and elements. The methods or flow charts provided herein may be implemented in a computer program, software, or firmware incorporated in a computer-

readable storage medium for execution by a general purpose computer or a processor. Examples of computer-readable storage mediums include a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs).

[0055] Suitable processors include, by way of example, a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) circuits, any other type of integrated circuit (IC), and/or a state machine.

[0056] EMBODIMENTS

1. A method of performing information-theoretically secure wireless communication.
2. A method as in any one of the preceding embodiments, including deriving an information-theoretically secure cryptographic key.
3. A method as in any one of the preceding embodiments, wherein the deriving includes using a plurality of input samples.
4. A method as in any one of the preceding embodiments, wherein the deriving is performed at a first wireless transmit/receive unit (WTRU).
5. A method as in any one of the preceding embodiments, including communicating with a second WTRU.

6. A method as in any one of the preceding embodiments, wherein communicating includes using the cryptographic key.
7. A method as in any one of the preceding embodiments, wherein the deriving includes privacy amplification.
8. A method as in any one of the preceding embodiments, wherein the deriving includes conversion.
9. A method as in any one of the preceding embodiments, wherein the conversion includes uniformly distributing the plurality of input samples.
10. A method as in any one of the preceding embodiments, wherein the conversion is based on an empirical distribution of the plurality of input samples.
11. A method as in any one of the preceding embodiments, wherein the conversion includes sorting the plurality of input samples.
12. A method as in any one of the preceding embodiments, wherein the sorting produces a plurality of plurality of ordered samples.
13. A method as in any one of the preceding embodiments, wherein each ordered sample includes an index of a corresponding input sample.
14. A method as in any one of the preceding embodiments, wherein the conversion includes transforming the plurality of ordered samples.
15. A method as in any one of the preceding embodiments, wherein transforming produces a plurality of uniformly distributed ordered samples.

16. A method as in any one of the preceding embodiments, wherein the conversion includes re-sorting the plurality of uniformly distributed ordered samples.

17. A method as in any one of the preceding embodiments, wherein the re-sorting produces a plurality of uniformly distributed samples.

18. A method as in any one of the preceding embodiments, wherein the re-sorting is based on the index of the corresponding input sample.

19. A method as in any one of the preceding embodiments, wherein the transforming includes rate-matching.

20. A method as in any one of the preceding embodiments, wherein the deriving includes decoding.

21. A method as in any one of the preceding embodiments, wherein the decoding includes receiving a public component of the plurality of input samples.

22. A method as in any one of the preceding embodiments, wherein the public component is received from the second WTRU.

23. A method as in any one of the preceding embodiments, wherein the public component is received on a public channel.

24. A method as in any one of the preceding embodiments, wherein the decoding includes applying a modified belief-propagation algorithm on the plurality of input samples.

25. A method as in any one of the preceding embodiments, wherein applying the modified belief-propagation algorithm includes calculating a log-likelihood ratio (LLR) of the plurality of input samples.

26. A method as in any one of the preceding embodiments, wherein calculating the LLR includes performing a uniform-distribution LLR algorithm.

27. A method as in any one of the preceding embodiments, wherein calculating the LLR includes performing an unknown-distribution LLR algorithm.

28. A method as in any one of the preceding embodiments, wherein the deriving includes encoding.

29. A method as in any one of the preceding embodiments, reporting a public component of the plurality of input samples.

30. A method as in any one of the preceding embodiments, wherein the reporting includes reporting to the second WTRU.

31. A method as in any one of the preceding embodiments, wherein the reporting is performed on a public channel.

32. A method as in any one of the preceding embodiments, wherein the encoding includes quantization

33. A method as in any one of the preceding embodiments, wherein the encoding includes channel coding.

34. A method as in any one of the preceding embodiments, wherein the quantization includes producing a quantization value.

35. A method as in any one of the preceding embodiments, wherein the quantization includes producing a quantization error.

36. A method as in any one of the preceding embodiments, wherein the producing a quantization value includes using a binary quantizer.

37. A method as in any one of the preceding embodiments, wherein the producing a quantization error includes calculating an absolute value.

38. A method as in any one of the preceding embodiments, wherein the absolute value is calculated based on a corresponding random value.

39. A method as in any one of the preceding embodiments, wherein the producing a quantization value includes selecting a predetermined number of most significant bits.

40. A method as in any one of the preceding embodiments, wherein the most significant bits are based on a corresponding random value.

41. A method as in any one of the preceding embodiments, wherein the producing a quantization error includes selecting a predetermined number of least significant bits.

42. A method as in any one of the preceding embodiments, wherein the least significant bits are based on a corresponding random value.

43. A method as in any one of the preceding embodiments, wherein the reporting a public component includes transmitting the quantization error.

44. A method as in any one of the preceding embodiments, wherein the channel coding includes generating a syndrome.

45. A method as in any one of the preceding embodiments, wherein the reporting a public component includes transmitting the syndrome.

46. A method as in any one of the preceding embodiments, wherein the encoding includes source coding.

47. A method as in any one of the preceding embodiments, wherein the source coding includes grey coding.

48. A wireless transmit/receive unit (WTRU) configured to perform at least part of any one of the preceding embodiments.

49. A base station configured to perform at least part of any one of the preceding embodiments.

50. An integrated circuit configured to perform at least part of any one of the preceding embodiments.

[0057] A processor in association with software may be used to implement a radio frequency transceiver for use in a wireless transmit receive unit (WTRU), user equipment (UE), terminal, base station, radio network controller (RNC), or any host computer. The WTRU may be used in conjunction with modules, implemented in hardware and/or software, such as a camera, a video camera module, a videophone, a speakerphone, a vibration device, a speaker, a microphone, a television transceiver, a hands free headset, a keyboard, a Bluetooth® module, a frequency modulated (FM) radio unit, a liquid crystal display (LCD) display unit, an organic light-emitting diode (OLED) display unit, a digital music player, a media player, a video game player module, an Internet

browser, and/or any wireless local area network (WLAN) or Ultra Wide Band (UWB) module.

*

*

*

CLAIMS

What is claimed is:

1. A method of performing information-theoretically secure wireless communication, the method comprising:
deriving an information-theoretically secure cryptographic key using a plurality of input samples at a first wireless transmit/receive unit (WTRU);
communicating with a second WTRU using the cryptographic key.
2. The method of claim 1, wherein the deriving includes privacy amplification.
3. The method of claim 1, wherein the deriving includes conversion.
4. The method of claim 3, wherein the conversion includes uniformly distributing the plurality of input samples.
5. The method of claim 3, wherein the conversion is based on an empirical distribution of the plurality of input samples.
6. The method of claim 3, wherein the conversion includes:
sorting the plurality of input samples to produce a plurality of ordered samples such that each ordered sample includes an index of a corresponding input sample;
transforming the plurality of ordered samples to produce a plurality of uniformly distributed ordered samples; and
resorting the plurality of uniformly distributed ordered samples to produce a plurality of uniformly distributed samples based on the index of the corresponding input sample.
7. The method of claim 6, wherein the transforming includes rate-matching.

8. The method of claim 1, wherein the deriving includes decoding.
9. The method of claim 8, wherein the decoding includes:
receiving a public component of the plurality of input samples from the second WTRU on a public channel; and
applying a modified belief-propagation algorithm on the plurality of input samples.
10. The method of claim 9, wherein applying the modified belief-propagation algorithm includes calculating a log-likelihood ratio (LLR) of the plurality of input samples.
11. The method of claim 10, wherein calculating the LLR includes performing a uniform-distribution LLR algorithm.
12. The method of claim 10, wherein calculating the LLR includes performing an unknown-distribution LLR algorithm.
13. The method of claim 1, wherein the deriving includes encoding.
14. The method of claim 13, wherein encoding includes:
reporting a public component of the plurality of input samples to the second WTRU on a public channel.
15. The method of claim 14, wherein the encoding includes:
quantization; and
channel coding.
16. The method of claim 15, wherein the quantization includes:
producing a quantization value; and

producing a quantization error.

17. The method of claim 16, wherein the producing a quantization value includes using a binary quantizer.

18. The method of claim 16, wherein the producing a quantization error includes calculating an absolute value of a corresponding random value.

19. The method of claim 16, wherein the producing a quantization value includes selecting a predetermined number of most significant bits of a corresponding random value.

20. The method of claim 16, wherein the producing a quantization error includes selecting a predetermined number of least significant bits of a corresponding random value.

21. The method of claim 16, wherein the reporting a public component includes transmitting the quantization error.

22. The method of claim 16, wherein the channel coding includes generating a syndrome.

23. The method of claim 22, wherein the reporting a public component includes transmitting the syndrome.

24. The method of claim 23, wherein the encoding includes source coding.

25. The method of claim 24, wherein the source coding includes grey coding.

26. A wireless transmit/receive unit (WTRU), the WTRU comprising:
a processor configured to derive an information-theoretically secure cryptographic key using a plurality of input samples; and
a transceiver configured to communicate with a second WTRU using the information-theoretically secure cryptographic key.

27. The WTRU of claim 26, wherein the processor includes a privacy amplification processor configured to remove a public component from the plurality of input samples.

28. The WTRU of claim 26, wherein the processor includes a data conversion unit configured to uniformly distribute the plurality of input samples.

29. The WTRU of claim 28, wherein the data conversion unit is configured to use an empirical distribution of the plurality of input samples.

30. The WTRU of claim 28, wherein the data conversion unit is configured to uniformly distribute the plurality of input samples by:

sorting the plurality of input samples to produce a plurality of ordered samples such that each ordered sample includes an index of a corresponding input sample;

transforming the plurality of ordered samples to produce a plurality of uniformly distributed ordered samples; and

resorting the plurality of uniformly distributed ordered samples to produce a plurality of uniformly distributed samples based on the index of the corresponding input sample.

31. The WTRU of claim 30, wherein the data conversion unit is configured to transform using rate-matching.

32. The WTRU of claim 26, wherein the processor includes a decoding unit configured to:

receive a public component of the plurality of input samples from the WTRU on a public channel; and

apply a modified belief-propagation algorithm to the plurality of input samples.

33. The WTRU of claim 32, wherein the decoding unit is configured to calculate a log-likelihood ratio (LLR) of the plurality of input samples for use in the modified belief-propagation algorithm.

34. The WTRU of claim 33, wherein the decoding unit is configured to calculate the LLR using a uniform-distribution LLR.

35. The WTRU of claim 33, wherein the decoding unit is configured to calculate the LLR using an unknown-distribution LLR.

36. The WTRU of claim 26, wherein the processor includes:
a quantization unit configured to produce a quantization value and a quantization error; and
a channel coding unit configured to generate a syndrome.

37. The WTRU of claim 36, wherein the transceiver is configured to report the quantization error and the syndrome to the second WTRU on a public channel.

38. The WTRU of claim 36, wherein the quantization unit is configured to produce a quantization value using a binary quantizer.

39. The WTRU of claim 36, wherein the quantization unit is configured to produce a quantization error by calculating an absolute value of a corresponding random value.

40. The WTRU of claim 36, wherein the quantization unit is configured to produce a quantization value by selecting a predetermined number of most significant bits of a corresponding random value.

41. The WTRU of claim 36, wherein the quantization unit is configured to produce a quantization error by selecting a predetermined number of least significant bits of a corresponding random value.

42. The WTRU of claim 36, wherein the processor includes a source coding unit configured to convert the quantization value to a bit string.

43. The WTRU of claim 42, wherein the source coding unit is configured to convert using grey coding.

1/7

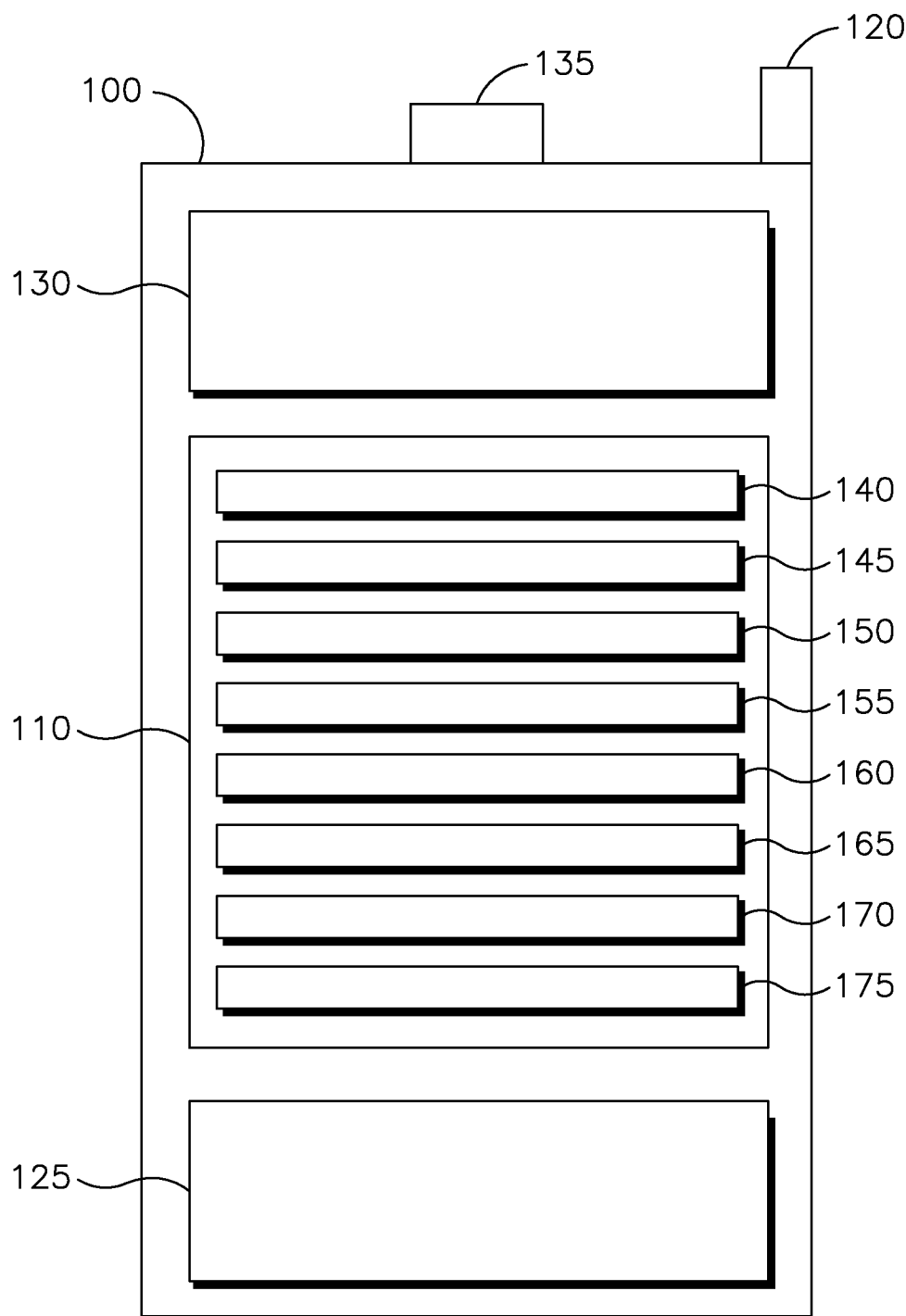


FIG. 1

200

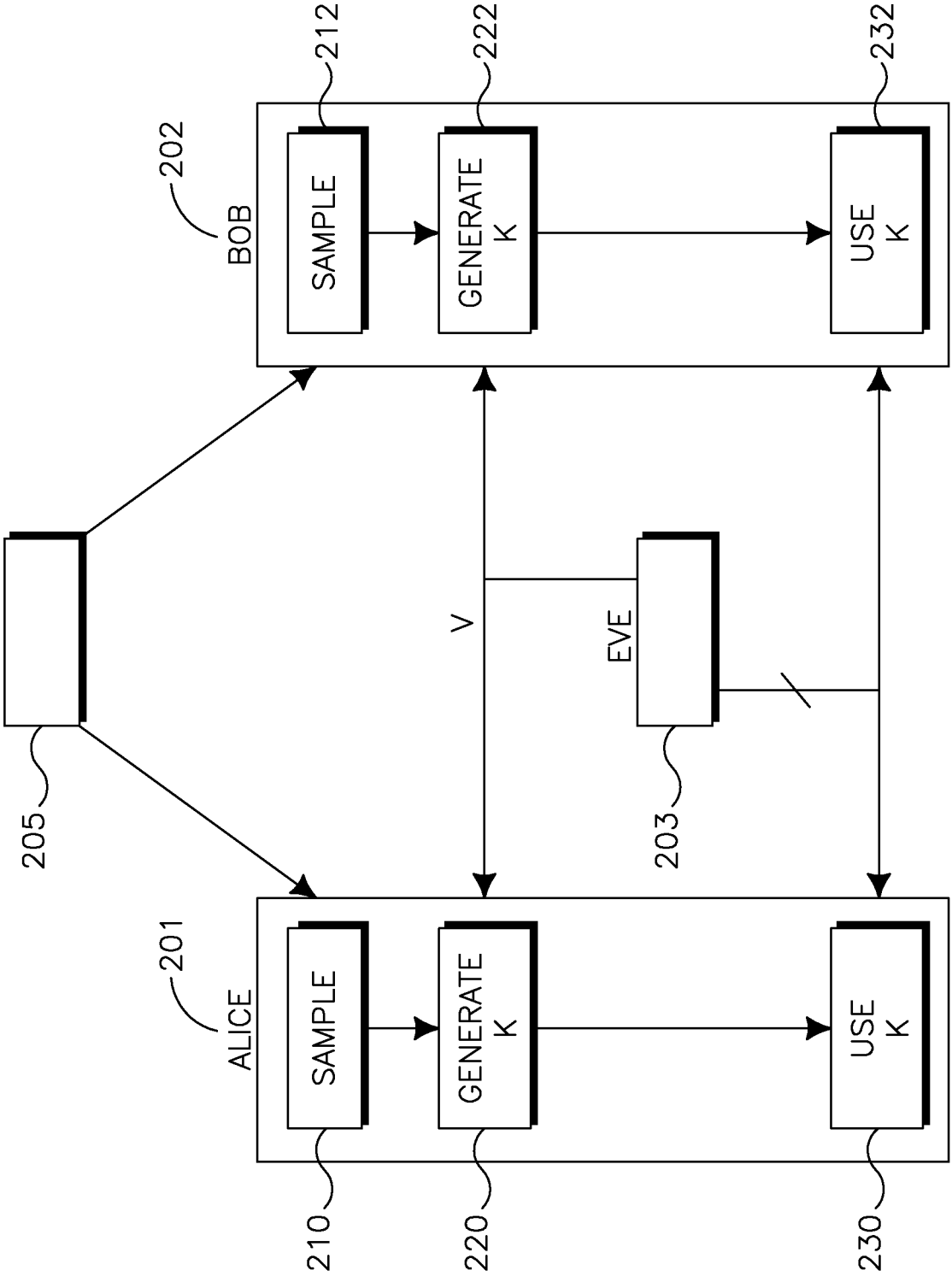


FIG. 2

220

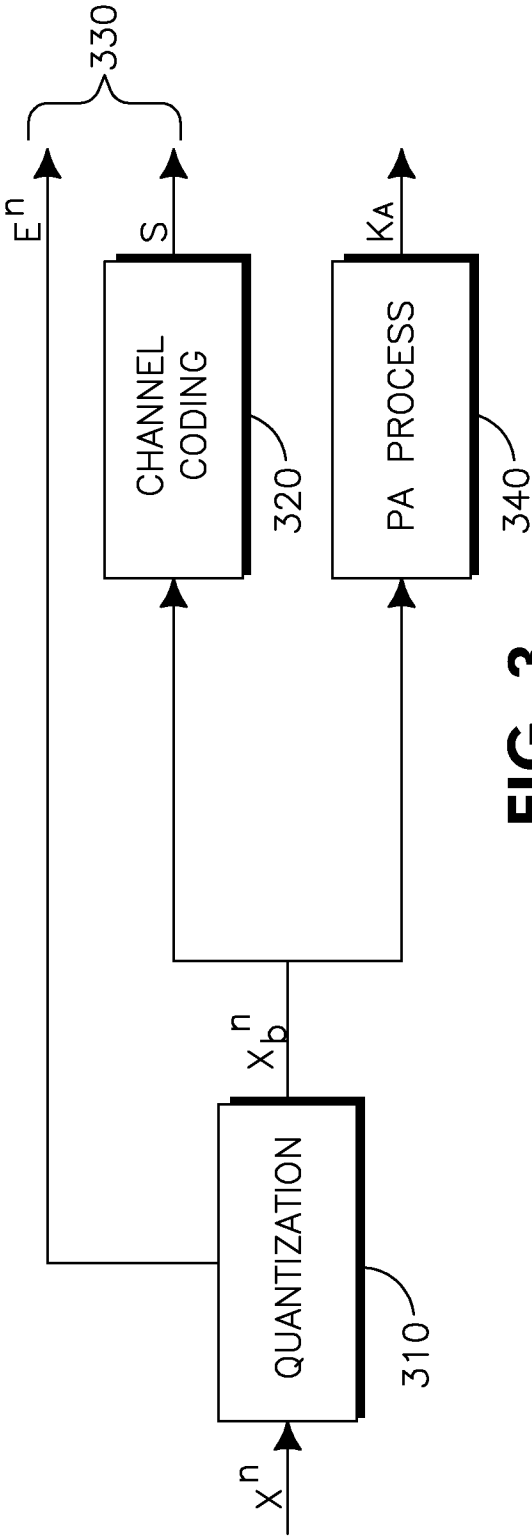


FIG. 3

222

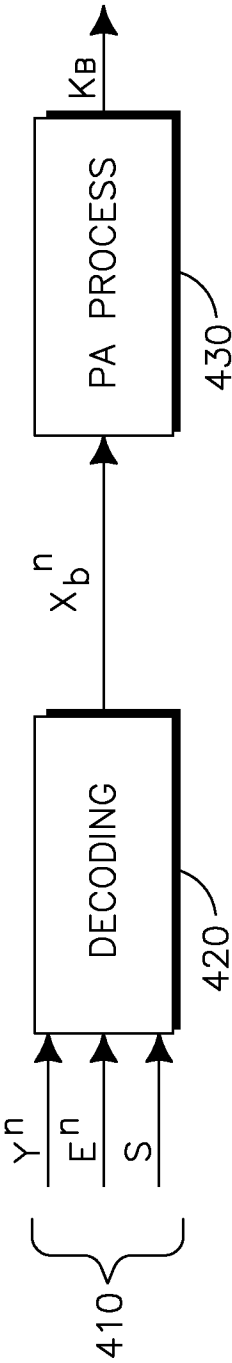


FIG. 4

500

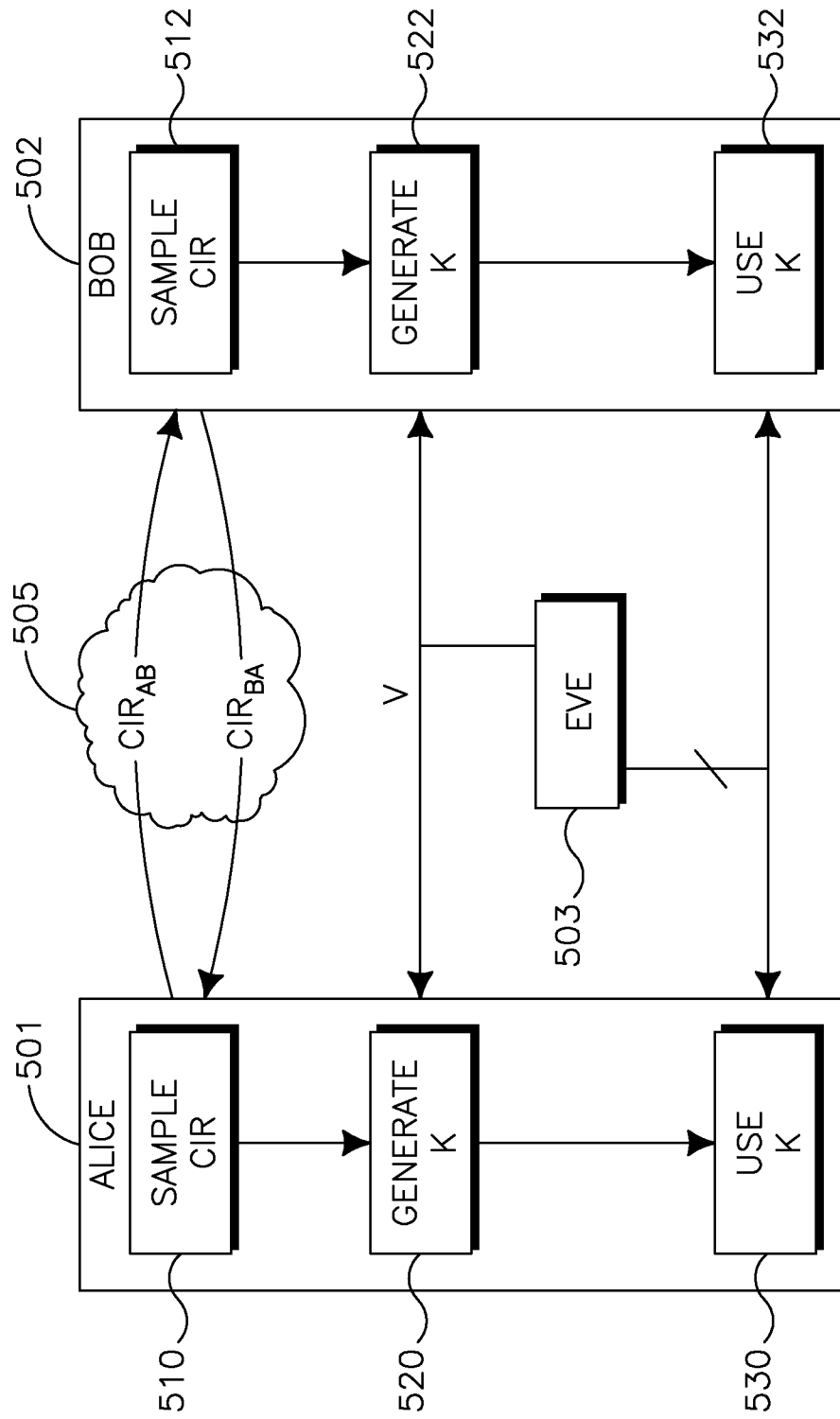


FIG. 5

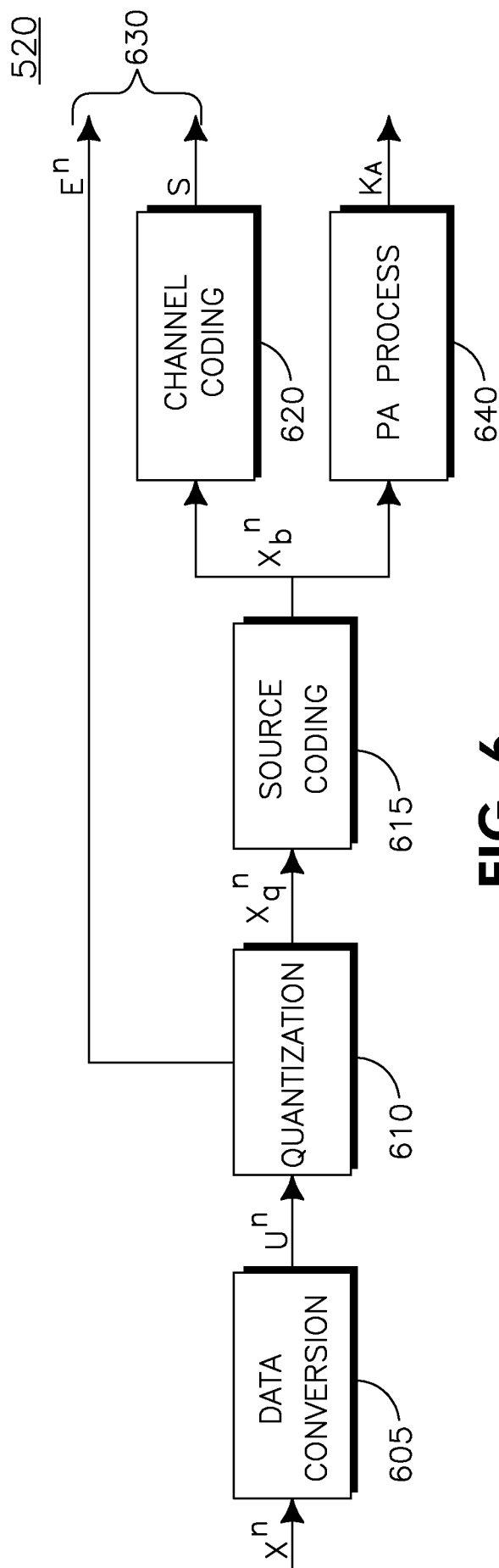
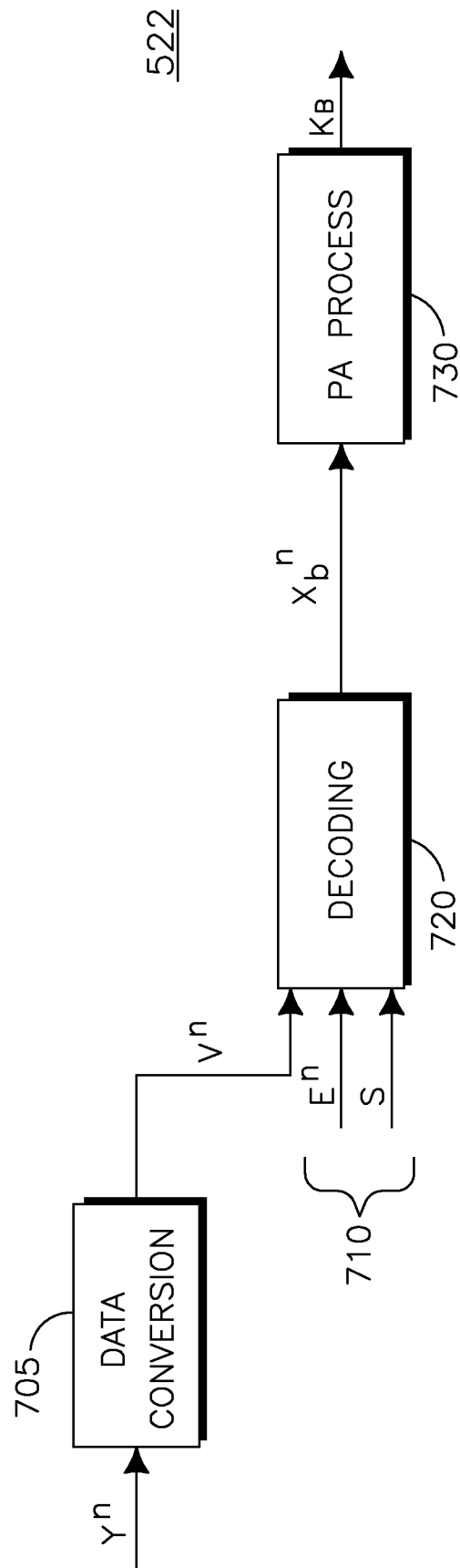


FIG. 6

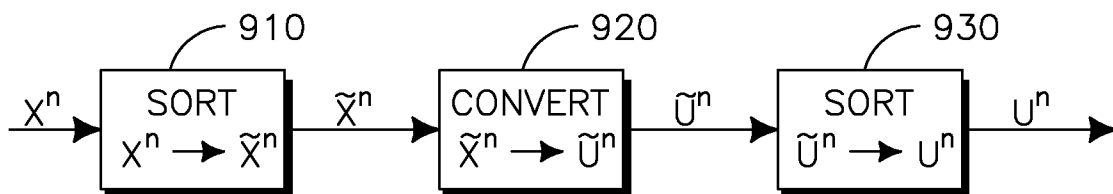


6/7

```

FOR i = 1 TO v
   $L_i \leftarrow 2E - 2V + 1 - 2^{-(v-i+1)}$ ;
  IF  $V < 0.5$ 
     $V \leftarrow 2V$ ;
     $E \leftarrow 2E$ ;
  ELSE
     $V \leftarrow 1 - 2V$ ;
     $E \leftarrow 2^{-(v-i)} - 2E$ ;
  END
END
END

```

FIG. 8**FIG. 9**

7/7

```

c ← 0;    k ← 0;    j ← 1;
WHILE (j ≤ n)
    c ← c +  $\frac{n}{2^A}$ ;
    WHILE (c ≥ 1)
         $\tilde{U}_j \leftarrow \frac{k}{2^A}$ ;  j ← j + 1;  c ← c - 1;
    END
    k ← k + 1;
END

```

FIG. 10

```

C(0) ← 0;
FOR j = 1 TO  $2^A$ 
    C(j) ←  $\left\lfloor \frac{j \cdot n}{2^A} \right\rfloor - \sum_{k=0}^{j-1} C(k)$ ;
END

```

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/043533

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/08

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)

H04L

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96/23376 A2 (ERICSSON GE MOBILE INC [US]) 1 August 1996 (1996-08-01)	1,26
Y	page 23, line 9 - page 24, line 17; figures 4,7	2-25, 27-43
Y	WO 2008/010838 A2 (INTERDIGITAL TECH CORP [US]; YE CHUNXUAN [US]; REZNIK ALEXANDER [US];) 24 January 2008 (2008-01-24) paragraphs [0057], [0061], [0135]; figure 2 paragraphs [0070], [0076], [0089], [0105], [0110]; figures 2,8,11-13	2-25, 27-43

☐ 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 document 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

17 September 2009

Date of mailing of the international search report

01/10/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5318 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Horbach, Christian

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2009/043533

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9623376	A2	01-08-1996	AU 702129 B2	11-02-1999
			AU 5414896 A	14-08-1996
			CA 2210714 A1	01-08-1996
			CN 1179248 A	15-04-1998
			EP 0804840 A2	05-11-1997
			FI 973067 A	19-09-1997
			JP 10513317 T	15-12-1998
WO 2008010838	A2	24-01-2008	EP 1969760 A2	17-09-2008
			JP 2009521188 T	28-05-2009
			KR 20080083174 A	16-09-2008
			KR 20080083176 A	16-09-2008
			US 2007165845 A1	19-07-2007