【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成26年1月9日(2014.1.9)

【公開番号】特開2012-163917(P2012-163917A)
【公開日】平成24年8月30日(2012.8.30)
【年通号数】公開・登録公報2012-034
【出願番号】特願2011-26216(P2011-26216)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６２０Ｚ
Ｇ０９Ｃ　1/00　６６０Ｇ

【手続補正書】
【提出日】平成25年11月14日(2013.11.14)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項５
【補正方法】変更
【補正の内容】
【請求項５】
前記暗号処理システムは、
少なくとも基底ベクトル$b_{0,i}$（$i=1,...,1+n_0,1+n_0+1,...,1+n_0+1+u_0,...,1+n_0+1+u_0+w_0,...,1+n_0+1+u_0+w_0+z_0$）（$n_0$, u_0, w_0, z_0は１以上の整数）を有する基底B_0と、
少なくとも基底ベクトル$b^*_{0,i}$（$i=1,...,1+n_0,1+n_0+1,...,1+n_0+1+u_0,...,1+n_0+1+u_0+w_0,...,1+n_0+1+u_0+w_0+z_0$）（$n_0$, u_0, w_0, z_0は１以上の整数）を有する基底B^*_0と、
少なくとも基底ベクトル$b_{t,i}$（$i=1,...,n_t,...,n_t+u_t,...,n_t+u_t+w_t,...,n_t+u_t+w_t+z_t$）（$u_t$, w_t, z_tは１以上の整数）を有する基底B_t（$t=1,...,L+1$）と、
少なくとも基底ベクトル$b^*_{t,i}$（$i=1,...,n_t,...,n_t+u_t,...,n_t+u_t+w_t,...,n_t+u_t+w_t+z_t$）を有する基底$B^*_t$（$t=1,...,L+1$）と
を用いて暗号処理を行い、
前記復号要素生成部は、ｔ＝０，．．．，Ｌの各整数ｔについての乱数$\vec{\eta}_{dec,t}:=(\eta_{dec,t,i})$（$i=1,...,w_t$）に基づき、数２に示す復号要素$k^*_{L,dec}$を生成し、
前記暗号化データｃ１生成部は、ｔ＝０，．．．，Ｌの各整数ｔについての乱数$\vec{\phi}_t:=(\phi_{t,i})$（$i=1,...,z_t$）に基づき、数３に示す暗号化データ$c_1$を生成する
ことを特徴とする請求項４に記載の暗号処理システム。
【数２】

$$k^*_{L,\mathsf{dec}} := \big((-s_{\mathsf{dec},0}, 0^{u_0}, \Delta, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{dec},t}\,\vec{e}_{t,1} + \theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,...,L\big)$$

【数３】

$$c_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega \vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1, ..., L)$$

【手続補正２】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項７
【補正方法】変更
【補正の内容】
【請求項７】
前記委譲装置は、さらに、
ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’について、第１下位ランダム化要素ｋ＊$_{L+1,ran,j'}$を生成するとともに、τ＝Ｌ＋２，．．．，ｄ（ｄはＬ＋２以上の整数）の各整数τと、各整数τに関してι＝１，．．．，ｎ$_{\tau}$の各整数ιについて、第２下位ランダム化要素ｋ＊$_{L+1,ran,(\tau,\iota)}$を生成する下位ランダム化要素生成部であって、
前記述語情報ｖ$^{\rightarrow}_{L+1}$と、前記復号鍵ｓｋ$_{L}$と、ｊ＝１，．．．，２Ｌの各整数ｊとｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’とについての乱数α$_{ran,j',j}$と、ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’についての乱数σ$_{ran,j'}$と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，ｗ$_{t}$の各整数ｉとについての乱数η$_{ran,j',(t,i)}$とに基づき、数８に示す第１下位ランダム化要素ｋ＊$_{L+1,ran,j'}$を生成し、
前記述語情報ｖ$^{\rightarrow}_{L+1}$と、前記復号鍵ｓｋ$_{L}$と、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数α$_{ran,(\tau,\iota),j}$と、乱数σ$_{ran,(\tau,\iota)}$と、乱数φ$_{ran,(\tau,\iota)}$と、ｔ＝０，．．．，Ｌ＋１，τの各整数ｔとｉ＝１，．．．，ｗ$_{t}$の各整数ｉとについてのの乱数η$_{ran,(\tau,\iota),(t,i)}$とに基づき、数９に示す第２下位ランダム化要素ｋ＊$_{L+1,ran,(\tau,\iota)}$を生成する下位ランダム化要素生成部と、
τ＝Ｌ＋２，．．．，ｄ（ｄはＬ＋２以上の整数）の各整数τと、各整数τに関してι＝１，．．．，ｎ$_{\tau}$の各整数ιについて、下位委譲要素ｋ＊$_{L+1,del,(\tau,\iota)}$を生成する下位委譲要素生成部であって、前記述語情報ｖ$^{\rightarrow}_{L+1}$と、前記復号鍵ｓｋ$_{L}$と、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数α$_{del,(\tau,\iota),j}$と、乱数σ$_{del,(\tau,\iota)}$と、乱数ψ’と、乱数φ$_{del,(\tau,\iota)}$と、ｔ＝０，．．．，Ｌ＋１，τの各整数ｔとｉ＝１，．．．，ｗ$_{t}$の各整数ｉとについてのの乱数η$_{del,(\tau,\iota),(t,i)}$とに基づき、数１０に示す下位委譲要素ｋ＊$_{L+1,del,(\tau,\iota)}$を生成する下位委譲要素生成部と
を備え、
前記委譲鍵送信部は、前記下位復号要素生成部が生成した下位復号要素ｋ＊$_{L+1,dec}$と、前記下位ランダム化要素生成部が生成した第１下位ランダム化要素ｋ＊$_{L+1,ran,j'}$及び第２下位ランダム化要素ｋ＊$_{L+1,ran,(\tau,\iota)}$と、前記下位委譲要素生成部が生成した下位委譲要素ｋ＊$_{L+1,del,(\tau,\iota)}$とを含む下位の復号鍵ｓｋ$_{L+1}$を下位の委譲装置へ送信する
ことを特徴とする請求項６に記載の暗号処理システム。

【数８】

$$k^{*}_{L+1,\mathrm{ran},j'} \coloneqq \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},j',j} k^{*}_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},j'} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i)} \right) + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^{*}_{t,n_t+u_t+i}$$

【数９】

$$k^{*}_{L+1,\mathrm{ran},(\tau,\iota)} \coloneqq \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},(\tau,\iota),j} k^{*}_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i)} \right) + \phi_{\mathrm{ran},(\tau,\iota)} k^{*}_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

【数１０】

$$k^{*}_{L+1,\mathrm{del},(\tau,\iota)} \coloneqq \sum_{j=1}^{2L+1} \alpha_{\mathrm{del},(\tau,\iota),j} k^{*}_{L,\mathrm{ran},j} + \sigma_{\mathrm{del},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i)} \right) + \psi' k^{*}_{L,\mathrm{del},(\tau,\iota)} + \phi_{\mathrm{del},(\tau,\iota)} k^{*}_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i},$$

【手続補正３】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１０
【補正方法】変更
【補正の内容】
【請求項１０】
前記暗号処理システムは、
少なくとも基底ベクトル$b_{0,i}$（$i=1,\ldots,1+n_0,1+n_0+1,\ldots,1+n_0+1+u_0,\ldots,1+n_0+1+u_0+w_0,\ldots,1+n_0+1+u$

$_0$＋w$_0$＋z$_0$）（n$_0$，u$_0$，w$_0$，z$_0$は１以上の整数）を有する基底Ｂ$_0$と、
少なくとも基底ベクトルｂ＊$_{0,i}$（ｉ＝１，．．．，１＋n$_0$，１＋n$_0$＋１，．．，１＋n$_0$＋１＋u$_0$，．．．，１＋n$_0$＋１＋u$_0$＋w$_0$，．．．，１＋n$_0$＋１＋u$_0$＋w$_0$＋z$_0$）（n$_0$，u$_0$，w$_0$，z$_0$は１以上の整数）を有する基底Ｂ＊$_0$と、
少なくとも基底ベクトルｂ$_{t,i}$（ｉ＝１，．．．，n$_t$，．．．，n$_t$＋u$_t$，．．，n$_t$＋u$_t$＋w$_t$，．．．，n$_t$＋u$_t$＋w$_t$＋z$_t$）（u$_t$，w$_t$，z$_t$は１以上の整数）を有する基底Ｂ$_t$（ｔ＝１，．．．，Ｌ＋１）と、
少なくとも基底ベクトルｂ＊$_{t,i}$（ｉ＝１，．．．，n$_t$，．．．，n$_t$＋u$_t$，．．，n$_t$＋u$_t$＋w$_t$，．．．，n$_t$＋u$_t$＋w$_t$＋z$_t$）を有する基底Ｂ＊$_t$（ｔ＝１，．．．，Ｌ＋１）と
を用いて暗号処理を行い、
前記復号要素生成部は、ｔ＝０，．．．，Ｌの各整数ｔについての乱数η$^{\rightarrow}_{dec,t}$：＝（η$_{dec,t,i}$）（ｉ＝１，．．．，w$_t$）に基づき、数１２に示す復号要素k＊$_{L,dec}$を生成し、
前記暗号化データｃ１生成部は、ｔ＝０，．．．，Ｌの各整数ｔについての乱数φ$^{\rightarrow}_t$：＝（φ$_{t,i}$）（ｉ＝１，．．．，z$_t$）に基づき、数１３に示す暗号化データｃ$_1$を生成する
ことを特徴とする請求項９に記載の暗号処理システム。
【数１２】

$$k^*_{L,\mathsf{dec}} := \Big((-s_{\mathsf{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}^*_0}, \left\{ \begin{array}{ll} (s_{\mathsf{dec},t}\vec{e}_{t,1} + \theta_{\mathsf{dec},t}, \vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{dec},t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\} : t = 1, \ldots, L \Big)$$

【数１３】

$$c_1 := \Big((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1, \ldots, L \Big)$$

【手続補正４】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１５
【補正方法】変更
【補正の内容】
【請求項１５】
ｔ＝１，．．．，Ｌ（Ｌは１以上の整数）の各整数ｔについての基底Ｂ$_t$と基底Ｂ＊$_t$とを用いて暗号処理を行う暗号処理システムにおいて、暗号化データｃ$_1$を復号鍵ｓｋ$_L$により復号する復号装置であり、
属性情報ｘ$^{\rightarrow}_t$：＝（ｘ$_{t,i}$）（ｉ＝１，．．．，n$_t$）と、所定の値ω，ζとを用いて、基底Ｂ$_0$の基底ベクトルｂ$_{0,p}$（ｐは所定の値）の係数として前記ωを設定し、基底Ｂ$_0$の基底ベクトルｂ$_{0,q}$（ｑは所定の値）の係数として前記ζを設定し、少なくとも一部の整数ｔについての基底Ｂ$_t$の基底ベクトルｂ$_{t,i}$（ｉ＝１，．．．，n$_t$）の係数としてωｘ$_{t,i}$（ｉ＝１，．．．，n$_t$）を設定した暗号化データｃ$_1$を暗号化装置から受信するデータ受信部と、

述語情報$\vec{v}_t$：＝（$v_{t,i}$）（ｉ＝１，．．．，n_t）と、所定の値Δと、ｔ＝１，．．．，Ｌの各整数ｔについての所定の値$\theta_{dec,t}$と、$s_{dec,0}=\Sigma_{t=1}^{L} s_{dec,t}$であるようなｔ＝０，．．．，Ｌの各整数ｔについての所定の値$s_{dec,t}$とを用いて、基底B^*_0の基底ベクトル$b^*_{0,p}$（ｐは所定の値）の係数として$-s_{dec,0}$を設定し、基底B^*_0の基底ベクトル$b^*_{0,q}$（ｑは所定の値）の係数として前記Δを設定し、ｔ＝１，．．．，Ｌの各整数ｔについての基底B^*_tの基底ベクトル$b^*_{t,i}$（ｉ＝１，．．．，n_t）の係数として$s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$（ｉ＝１，．．．，$n_t$）を設定した復号要素$k^*_{L,dec}$を含む復号鍵$sk_L$を鍵生成装置から取得する復号鍵取得部と、

前記データ受信部が受信した暗号化データc_1と、前記復号鍵取得部が取得した前記復号鍵sk_Lに含まれる復号要素$k^*_{L,dec}$とについて、ペアリング演算$e(c_1, k^*_{L,dec})$を行い、前記暗号化データc_1を復号するペアリング演算部と

を備えることを特徴とする復号装置。

【手続補正５】

【補正対象書類名】特許請求の範囲

【補正対象項目名】請求項１８

【補正方法】変更

【補正の内容】

【請求項１８】

ｔ＝１，．．．，Ｌ＋１（Ｌは１以上の整数）の各整数ｔについての基底B_tと基底B^*_tとを用いて暗号処理を実行する暗号処理プログラムであり、

ｔ＝１，．．．，Ｌのうち少なくとも一部の整数ｔについての基底B_tの基底ベクトルに属性情報$\vec{x}_t$を埋め込んだベクトルを暗号化データｃｔとして生成する暗号化処理と、

ｔ＝１，．．．，Ｌの各整数ｔについての基底B^*_tの基底ベクトルに述語情報$\vec{v}_t$を埋め込んだベクトルを復号鍵sk_Lとして、前記暗号化処理で生成した暗号化データｃｔと前記復号鍵sk_Lとについて、ペアリング演算を行い前記暗号化データｃｔを復号する復号処理と、

基底B^*_{L+1}の基底ベクトルに述語情報を埋め込んだベクトル$\vec{v}_{L+1}$と、前記復号処理で使用した復号鍵sk_Lとに基づき、前記復号鍵sk_Lの下位の復号鍵sk_{L+1}を生成する鍵委譲処理と

を備えることを特徴とする暗号処理プログラム。