【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７部門第３区分
【発行日】平成28年7月21日(2016.7.21)

【公表番号】特表2015-522998(P2015-522998A)
【公表日】平成27年8月6日(2015.8.6)
【年通号数】公開・登録公報2015-050
【出願番号】特願2015-513272(P2015-513272)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/12　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６３１

【手続補正書】
【提出日】平成28年5月23日(2016.5.23)
【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】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
第１当事者と第２当事者とが、共有秘密情報を得ることを可能にするための方法であって、
Ｘが、１つの数値列であり、N^{A}が、前記第１当事者にかかわるランダム列であるとしたときに、数値列Ａ＝Ｘ＋N^{A}が、前記第１当事者によって得られるステップと、
N^{B}が、前記第２当事者にかかわるランダム列であるとしたときに、数値列Ｂ＝Ｘ＋N^{B}が、前記第２当事者によって得られるステップと、
ＡおよびＢが、それぞれ前記数値列ＡおよびＢに等しいか、または前記数値列ＡおよびＢから導出される、または前記数値列ＡおよびＢを用いて導出される、離散数値から成る数値列であるとしたときに、該数値列ＡおよびＢ中の対応し合う数値a_iおよびb_iのうちの一致し合う数値から成る数値対を識別するためのデータ一致処理が、前記第１当事者および第２当事者によって遂行されるステップとを含む方法において、
前記共有秘密情報は、前記数値列ＡおよびＢ中の前記一致し合う数値と等しいか、または前記一致し合う数値から導出されるか、または前記一致し合う数値を用いて導出される方法。
【請求項２】
前記データ一致処理は、
前記第１当事者と第２当事者とのうちの少なくとも一方が、１つ以上の数値を取得するように、前記第１当事者と第２当事者との間で１つ以上のメッセージを交換するステップであって、前記取得される数値のうちの少なくとも１つは、前記数値a_iに等しいか、または前記数値a_iから導出され、前記取得される数値のうちの少なくとも１つは、前記数値b_iに等しいか、または前記数値b_iから導出されるステップと、
比較演算を含む１つ以上の数学操作が、前記第１当事者と第２当事者とのうちの少なくとも一方によって遂行されるステップであって、前記数値a_iとb_iとの一致は、前記比較演算の比較結果から特定されるステップとを
含んでいる、請求項１に記載の方法。
【請求項３】

前記データ一致処理は、
ｐが、前記第１当事者と第２当事者とのうちの一方であるＰ当事者の数値列中の１つの数値であり、f_1が、あらかじめ定められた関数であるとしたときに、数値$T_1 = f_1$（ｐ）が、前記Ｐ当事者から、前記第１当事者と第２当事者とのうちの他方であるＱ当事者に送信されるステップと、
ｑが、前記Ｑ当事者の数値列中の、数値列中の位置において前記数値ｐに対応する数値であるとしたときに、前記数値T_1、または前記数値T_1から導出される数値と、前記数値ｑ、または前記数値ｑから導出される数値とが、前記Ｑ当事者によって比較される比較ステップとが、
前記Ｐ当事者およびＱ当事者によって遂行されるステップを含んでいる、請求項１または２に記載の方法。
【請求項４】
f^{-1}_1が、前記関数f_1の逆関数であるとしたときに、前記比較ステップは、前記数値T_1と数値f_1（ｑ）とを比較するステップと、数値f^{-1}_1（T_1）と前記数値ｑとを比較するステップとのうちの少なくとも一方を含んでいる、請求項３に記載の方法。
【請求項５】
前記データ一致処理は、
ｐが、前記第１当事者と第２当事者とのうちの一方であるＰ当事者の数値列中の１つの数値であり、f_1が、あらかじめ定められた関数であるとしたときに、数値$T_1 = f_1$（ｐ）が、前記Ｐ当事者から、前記第１当事者と第２当事者とのうちの他方であるＱ当事者に送信されるステップと、
f_2が、あらかじめ定められた関数であり、ｑが、前記Ｑ当事者の数値列中の、数値列中の位置において前記数値ｐに対応する数値であるとしたときに、数値$T_2 = f_2$（T_1, ｑ）が、前記Ｑ当事者によって計算されるステップとが、
前記Ｐ当事者およびＱ当事者によって遂行されるステップを含んでおり、
前記比較ステップは、前記数値T_2とあらかじめ定められた数値とが、前記Ｐ当事者とＱ当事者とのうちの少なくともどちらかによって比較されるステップを含んでいる、請求項１または２に記載の方法。
【請求項６】
ｒがランダムな数値であり、数１がモジュロ２加算を意味するとしたときに、前記数値f_1（ｐ）は、数２で与えられる、請求項５に記載の方法。
【数１】

【数２】
$f_1(p)=p \oplus r$

【請求項７】
f_3が、あらかじめ定められた関数であるとしたときに、前記方法は、さらに、数値$T_3 = f_3$（ｒ）が、前記Ｐ当事者から前記Ｑ当事者に送信されるステップを含んでおり、
前記数値T_2は、数３で与えられ、前記比較ステップは、前記数値T_3とハッシュ値Ｈ（T_2）とが、前記Ｑ当事者によって比較されるステップを含んでいる、請求項６に記載の方法。
【数３】
$T_2=T_1 \oplus q$

【請求項８】
f_3が、あらかじめ定められた関数であるとしたときに、前記方法は、さらに、数値（数４）が、前記Ｑ当事者から前記Ｐ当事者に送信されるステップを含んでおり、
前記比較ステップは、前記数値f_3（ｒ）と前記数値T_2とが、前記Ｐ当事者によって

比較されるステップを含んでいる、請求項６に記載の方法。
【数４】
$T_2=f_3(T_1 \oplus q)$.

【請求項９】
前記データ一致処理は、
p_1が、前記第１当事者と第２当事者とのうちの一方であるＰ当事者の数値列中の１つの数値ｐの第１のビットであり、ｒがランダムビットであり、数１がモジュロ２加算を表すとしたときに、ビット値（数５）が、前記Ｐ当事者によって計算されるステップと、
p_2が、前記数値ｐの第２のビットであるとしたときに、ビット値（数６）が、前記Ｐ当事者によって計算されるステップと、
前記ビット値m_1およびm_2が、前記Ｐ当事者から、前記第１当事者と第２当事者とのうちの他方であるＱ当事者に送信されるステップと、
q_1が、前記Ｑ当事者の数値列中の、数値列中の位置において前記数値ｐに対応する数値ｑの、ビット位置において前記第１のビットp_1に対応する第１のビットであるとしたときに、ビット値（数７）が、前記Ｑ当事者によって計算されるステップと、
q_2が、前記数値ｑの、ビット位置において前記第２のビットp_2に対応する第２のビットであるとしたときに、ビット値（数８）が、前記Ｑ当事者によって計算されるステップと、
数値（数９）と数値０とが比較されるステップとが、
前記Ｐ当事者およびＱ当事者によって遂行されるステップを含んでいる、請求項１または２に記載の方法。
【数５】
$m_1=p_1 \oplus r$

【数６】
$m_2=p_2 \oplus r$

【数７】
$m'_1=m_1 \oplus q_1$

【数８】
$m'_2=m_2 \oplus q_2$

【数９】
$m'_1 \oplus m'_2$

【請求項１０】
前記データ一致処理は、前記数値列ＡおよびBのそれぞれの数値a_iおよびb_iから成る数値対の各々に対応するランダムな数値r_iを用い、前記共有秘密情報は、前記数値列ＡおよびBのそれぞれの数値a_iおよびb_iのうちの一致し合う数値に対応する前記ランダムな数値r_iに基づいて導出される、請求項１～９のいずれか１つに記載の方法。
【請求項１１】
前記数値列Ｘを、ある信号中に符号化するステップ、および数値列Ｘの符号化が行われた該信号を送信するステップを、さらに含み、
前記数値列Ｘ中の各数値が、前記第１当事者によって送信される前記信号の量子状態中に符号化され、
前記数値列Ｘ中の各数値が、前記信号の振幅と位相とのうちの少なくとも一方の中に符号化される、請求項１～１０のいずれか１つに記載の方法。
【請求項１２】

前記信号は、前記第１当事者、および前記第１当事者および第２当事者以外の当事者のうちの１人の当事者によって、前記数値列Ｘの符号化に用いられて、送信される、請求項１１に記載の方法。
【請求項１３】
数値列Ｂが第２当事者によって得られる前記ステップは、前記数値列Ｘの符号化に用いられている前記信号が、前記第２当事者によって受信されるステップ、および符号化されている前記数値列Ｘの各数値が、前記第２当事者によって検出されるステップを含み、
数値列Ａが第１当事者によって得られる前記ステップは、前記数値列Ｘの符号化に用いられている前記信号が、前記第１当事者によって受信されるステップ、および符号化されている前記数値列Ｘの各数値が、前記第１当事者によって検出されるステップを含んでいる、請求項１１に記載の方法。
【請求項１４】
前記数値列Ｘは、ランダムな数値列、ガウス分布値から成る数値列およびあらかじめ定められた数値列を含んでいる、請求項１～１３のいずれか１つに記載の方法。
【請求項１５】
前記第１当事者および第２当事者によって、それぞれ前記数値列ＡおよびＢが、対応する離散値の数値列Ａおよび Ｂに変換されるステップを、さらに含んでいる、請求項１～１４のいずれか１つに記載の方法。
【請求項１６】
数値列ＡおよびＢが、対応する離散値の数値列Ａおよび Ｂに変換される前記ステップは、前記離散値の数値列Ａおよび Ｂ中の二進数値を得るために、前記数値列ＡおよびＢ中の、連続値である各数値a_iおよびb_iに、あらかじめ定められた離散化操作を適用することによって、前記数値列ＡおよびＢにそれぞれ対応する、二進数値から成る数値列Ａおよび Ｂが、それぞれ前記第１当事者および第２当事者によって得られるステップを含んでおり、前記離散化操作によって、前記連続値である各数値a_iおよびb_iの範囲が、対応する二進数値にマッピングされる、請求項１５に記載の方法。
【請求項１７】
前記数値列Ａと Ｂとの間の相関を高めるために、誤り訂正処理は、前記第１当事者および第２当事者によって遂行されるステップを、さらに含んでいる、請求項１～１６のいずれか１つに記載の方法。
【請求項１８】
誤り訂正処理が遂行される前記ステップは、前記数値列Ａおよび Ｂ中の対応し合う数値a_iとb_iとの間で、前記誤り訂正処理は、前記第１当事者および第２当事者によって遂行されるステップを含んでおり、前記誤り訂正処理は、あらかじめ定められた量までの誤りを訂正することが可能である、請求項１７に記載の方法。
【請求項１９】
前記誤り訂正処理は、
前記第１当事者および第２当事者のうちの一方の当事者に対応する数値列Ａ／Ｂ中の数値a_i／b_iに基づく誤り訂正情報が、該一方の当事者によって生成されるサブステップと、該誤り訂正情報が、前記第１当事者および第２当事者のうちの他方の当事者に送信されるサブステップと、
前記誤り訂正情報が、前記他方の当事者によって、前記他方の当事者に対応する数値列Ｂ／Ａ中の、前記数値a_i／b_iに対応する数値b_i／a_iに適用されるサブステップとが、
前記対応し合う数値a_iおよびb_iから成る数値対の各々に対して遂行されるステップを含んでいる、請求項１７または１８に記載の方法。
【請求項２０】
前記数値列Ａおよび Ｂ中の各数値a_iおよびb_iにおいて、あらかじめ定められた１つ以上のビット位置のビットが保持され続け、残りのビットが破棄されるステップを、さらに含んでいる、請求項１～１９のいずれか１つに記載の方法。

【請求項２１】
保持され続けたビットを有する数値a_i、b_iを用いて、前記データ一致処理が繰り返されるステップを、さらに含んでいる、請求項２０に記載の方法。
【請求項２２】
前記数値列Ａおよび Ｂ中の各数値a_iおよびb_iを、該数値a_iおよびb_iから導出されるパリティ値で置き換えるステップを、さらに含んでいる、請求項２１に記載の方法。
【請求項２３】
新しい数値a_i、b_iを形成するために、前記数値列Ａおよび Ｂの各々のパリティビットを、一連の、ｐビットの集まりに分割するステップと、
請求項２０～２２のいずれか１つに記載のステップを繰り返すステップとを、
さらに含んでいる、請求項２２に記載の方法。
【請求項２４】
第１当事者および第２当事者が共有秘密情報を得ることを可能にするための、該第１当事者に対する方法であって、
Ｘは、１つの数値列であり、N^Aは、前記第１当事者にかかわるランダム列であるとしたときに、数値列Ａ＝Ｘ＋N^Aが、前記第１当事者によって得られるステップと、
Ｂは、前記第２当事者によって得られる数値列Ｂ＝Ｘ＋N^Bであり、N^Bは、前記第２当事者にかかわるランダム列であり、Ａおよび Ｂは、それぞれ前記数値列Ａおよび Ｂに等しい、または前記数値列Ａおよび Ｂから導出されるか、または前記数値列Ａおよび Ｂを用いて導出される、離散数値から成る数値列であるとしたときに、前記第１当事者と第２当事者との間のメッセージの交換によって、前記数値列Ａおよび Ｂ中の対応し合う数値a_iおよびb_iのうちの一致し合う数値から成る数値対を識別するためのデータ一致処理が、前記第１当事者によって遂行されるステップとを含む方法において、
前記共有秘密情報は、前記数値列Ａおよび Ｂ中の前記一致し合う数値に等しいか、または前記一致し合う数値から導出されるか、または前記一致し合う数値を用いて導出される方法。
【請求項２５】
第１当事者および第２当事者が共有秘密情報を得ることを可能にするための、該第２当事者に対する方法であって、
Ｘは、１つの数値列であり、N^Bは、前記第２当事者にかかわるランダム列であるとしたときに、数値列Ｂ＝Ｘ＋N^Bが、前記第２当事者によって得られるステップと、
Ａは、前記第１当事者によって得られる数値列Ａ＝Ｘ＋N^Aであり、N^Aは、前記第１当事者にかかわるランダム列であり、Ａおよび Ｂは、それぞれ前記数値列Ａおよび Ｂに等しい、または前記数値列Ａおよび Ｂから導出されるか、または前記数値列Ａおよび Ｂを用いて導出される、離散数値から成る数値列であるとしたときに、前記第１当事者と第２当事者との間のメッセージの交換によって、前記数値列Ａおよび Ｂ中の対応し合う数値a_iおよびb_iのうちの一致し合う数値から成る数値対を識別するためのデータ一致処理が、前記第２当事者によって遂行されるステップとを含んでいる方法において、
前記共有秘密情報は、前記数値列Ａおよび Ｂ中の前記一致し合う数値に等しいか、または前記一致し合う数値から導出されるか、または前記一致し合う数値を用いて導出される方法。