【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29年12月7日(2017.12.7)

【公開番号】特開2017-73789(P2017-73789A)
【公開日】平成29年4月13日(2017.4.13)
【年通号数】公開・登録公報2017-015
【出願番号】特願2016-211833(P2016-211833)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｇ０６Ｆ　21/32　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０６Ｆ　21/31
Ｇ０６Ｆ　21/32

【手続補正書】
【提出日】平成29年10月20日(2017.10.20)
【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】
サーバによって実行される方法であって、
端末に複数の質問を送信するステップと、
前記複数の質問に対する応答に基づいて生成された認証ハッシュを前記端末から受信するステップと、
前記認証ハッシュが秘密認証ハッシュと整合する場合には、アクセスを許可するステップと、
前記認証ハッシュが前記秘密認証ハッシュと整合しない場合には、アクセスを拒否するステップとを含み、
認証ハッシュは、ノイズのある補間アルゴリズムを使用することで、複数のハッシュの多項式補間および複数のハッシュに対する代数演算から生成されて、多項式補間のための１つ以上のエラー点、および多項式補間のための１つ以上の正しい点のうちの一方の導入を通して、ノイズのある補間アルゴリズムのしきい値が調節され、
前記認証ハッシュを格納するステップをさらに含む、方法。
【請求項２】
秘密認証ハッシュおよびしきい値に基づいて、ノイズのある補間アルゴリズムで使用するための１つ以上のエラー点および１つ以上の正しい点のうちの一方を生成して送信するステップをさらに含む、請求項１に記載の方法。
【請求項３】
送信された質問のうちの選択されたグループに基づいて、複数の秘密認証ハッシュから秘密認証ハッシュを選択するステップをさらに含み、
複数の秘密認証ハッシュの各々は、複数の質問のうちの少なくとも２つに関連付けられている、請求項１または２に記載の方法。
【請求項４】
複数の質問への応答を受信するステップをさらに含み、前記応答は、応答ハッシュと、

複数の質問のうちの１つまたは部分集合への回答とを含み、前記方法はさらに、
応答ハッシュおよび回答から認証ハッシュを構築するステップを含む、請求項１から３のいずれか１項に記載の方法。
【請求項５】
前記認証ハッシュを構築するステップは、前記応答ハッシュおよび前記回答から入れ子ハッシュを構築することによって、当該認証ハッシュを構築することを含む、請求項４に記載の方法。
【請求項６】
前記認証ハッシュを構築するステップは、応答ハッシュに回答のハッシュを乗算することによって、認証ハッシュを構築することを含む、請求項４に記載の方法。
【請求項７】
ユーザに関連付けられた装置およびユーザに関連付けられたアカウントから確認を受信後、秘密認証ハッシュを受信して、秘密認証ハッシュをメモリに格納するステップをさらに含む、請求項１から６のいずれかに記載の方法。
【請求項８】
複数の質問は、生体計測情報についての要求を含む、請求項１から７のいずれか１項に記載の方法。
【請求項９】
請求項１から８のいずれかに記載の方法をコンピュータに実行させる、プログラム。
【請求項１０】
請求項８に記載のプログラムを格納するためのメモリと、
前記プログラムを実行するためのプロセッサとを備える、装置。