(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 2 月 2 日(02.02.2012)

PCT

(10) 国際公開番号
WO 2012/014669 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/20* (2006.01)

(21) 国際出願番号: PCT/JP2011/065872

(22) 国際出願日: 2011 年 7 月 12 日(12.07.2011)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2010-171940 2010 年 7 月 30 日(30.07.2010) JP
特願 2010-224752 2010 年 10 月 4 日(04.10.2010) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社(SONY CORPORATION) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 作本 紘一(SAKUMOTO, Koichi) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 白井 太三(SHIRAI, Taizo) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 樋渡 玄良(HIWATARI, Harunaga) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 亀谷 美明, 外(KAMEYA, Yoshiaki et al.); 〒1600004 東京都新宿区四谷３－１－３ 第一冨澤ビル はづき国際特許事務所 四谷オフィス Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, IS, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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.

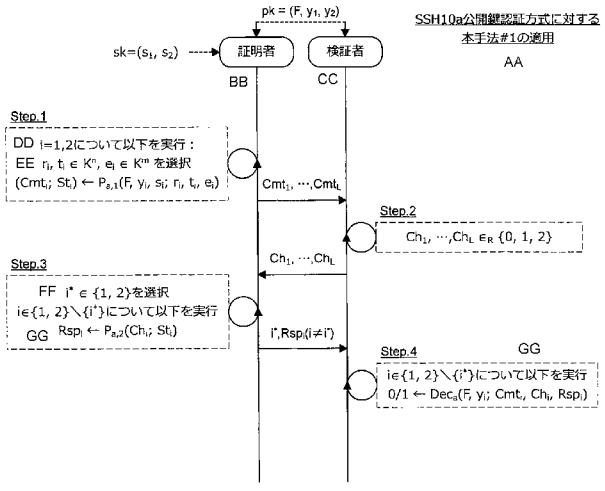
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,

[続葉有]

(54) **Title**: AUTHENTICATION DEVICE, AUTHENTICATION METHOD, AND PROGRAM

(54) 発明の名称 : 認証装置、認証方法、及びプログラム

[図9]



AA Application of disclosed technique #1 to SSH 10a public-key authentication
BB Claimant
CC Verifier
DD Perform the following for i = 1, 2
EE Select $r_i, t_i \in K^n$, and $e_i \in K^m$
FF Select $i^* \in \{1, 2\}$
GG Perform the following for $i \in \{1, 2\} \setminus \{i^*\}$

(57) **Abstract**: Disclosed is an authentication device that produces a level of security against active attacks. Said authentication device is provided with: a key storage unit that stores L ($L \geq 2$) secret keys s_i ($i = 1, \ldots, L$) and L public keys y_i that satisfy $y_i = F(s_i)$ for an nth-order ($n \geq 2$) multivariate polynomial F; and an interaction-protocol execution unit that executes an interaction protocol with a verifier to prove knowledge of L - 1 secret keys s_i satisfying $y_i = F(s_i)$. The interaction-protocol execution unit executes said interaction protocol with the verifier such that the verifier does not know which secret key s_i was used.

(57) 要約: 【課題】能動的攻撃に対する安全性レベルを実現すること。 【解決手段】Ｌ個（Ｌ≧２）の秘密鍵ｓｉ（ｉ＝１～Ｌ）、及びｎ次多変数多項式Ｆ（ｎ≧２）についてｙｉ＝Ｆ（ｓｉ）を満たすＬ個の公開鍵ｙｉを保持する鍵保持部と、（Ｌ－１）個のｙｉ＝Ｆ（ｓｉ）を満たす秘密鍵ｓｉを知っていることを証明するための対話プロトコルを検証者との間で実行する対話プロトコル実行部と、を備え、前記対話プロトコル実行部は、前記検証者との間で前記対話プロトコルを実行する際に、どの秘密鍵ｓｉを使用したかを当該検証者に知られないようにする、認証装置が提供される。

WO 2012/014669 A1

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, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）