US006035398A

United States Patent [19]

Bjorn

[11] Patent Number: 6,035,398

[45] Date of Patent: Mar. 7, 2000

[54] **CRYPTOGRAPHIC KEY GENERATION USING BIOMETRIC DATA**

[75] Inventor: **Vance Bjorn**, San Carlos, Calif.

[73] Assignee: **DigitalPersona, Inc.**, Redwood City, Calif.

[21] Appl. No.: **08/970,304**

[22] Filed: **Nov. 14, 1997**

[51] **Int. Cl.**[7] **H04L 9/32**

[52] **U.S. Cl.** **713/186**; 713/185

[58] **Field of Search** 382/181, 199, 382/203, 206, 209; 380/23

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,419,287	12/1968	Rudie	283/7
3,872,438	3/1975	Cuttill et al.	340/149 A
3,959,884	6/1976	Jordan et al.	340/146.3
4,047,154	9/1977	Vitols et al.	340/146.3
4,151,512	4/1979	Riganati et al.	340/146.3
4,156,230	5/1979	Riganati et al.	340/146.3
4,185,270	1/1980	Fischer, II et al.	340/146.3
4,208,651	6/1980	McMahon	340/146.3
4,210,899	7/1980	Swonger et al.	340/146.3
4,225,850	9/1980	Chang et al.	340/146.3
4,253,086	2/1981	Szwarcbier	340/146.3
4,260,979	4/1981	Smith	340/146.3
4,414,684	11/1983	Blonder	382/4
4,449,189	5/1984	Feix et al.	364/513.5
4,454,610	6/1984	Sziklai	382/3
4,525,859	7/1985	Bowles et al.	382/5
4,581,760	4/1986	Schiller et al.	382/4
4,607,384	8/1986	Brooks	382/4
4,618,988	10/1986	Schiller	382/5
4,636,622	1/1987	Clark	235/380
4,641,350	2/1987	Bunn	382/4
4,646,352	2/1987	Asai et al.	382/5
4,685,145	8/1987	Schiller	382/52
4,696,046	9/1987	Schiller	382/5
4,698,751	10/1987	Parvin	364/200
4,723,298	2/1988	Schiller	382/56
4,747,147	5/1988	Sparrow	382/4
4,752,966	6/1988	Schiller	382/5
4,777,651	10/1988	McCann et al.	382/21
4,787,742	11/1988	Schiller et al.	356/71
4,790,564	12/1988	Larcher et al.	283/69
4,805,223	2/1989	Denyer	382/4
4,811,414	3/1989	Fishbine et al.	382/52

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0159037	10/1985	European Pat. Off.	G07C 9/00
4125198	5/1992	Germany	G06K 19/073
5089324	8/1993	Japan	G07D 9/00
1283748	8/1972	United Kingdom	G07D 9/00
8203286	9/1982	WIPO	G07C 11/00
9107728	5/1991	WIPO	G06K 9/00

Primary Examiner—Tod R. Swann
Assistant Examiner—Todd Jack
Attorney, Agent, or Firm—Blakely, Sokoloff, Taylor & Zafman LLP

[57] **ABSTRACT**

A method and apparatus for generating a cryptographic key using biometric data is provided. A fingerprint is received, and features are extracted from the fingerprint. These features may include one or more of the following: A message is created based on the features of the fingerprint. For one embodiment, the message is a template including the features. For another embodiment, the message is a subset of features not included in a template. For another embodiment, the message is ghost points not corresponding to the features in the template. A message digest function is applied to the message to create a cryptographic key.

Another embodiment of the present invention uses features of the fingerprint image to generate a digital certificate. The public key used for the digital certificate is based on a fingerprint image. In one embodiment, the digital certificate contains a template including the fingerprint image or the features extracted from the fingerprint image. Verification of this template provides additional security to the validity of the digital certificate.

26 Claims, 9 Drawing Sheets