ԳՅՈՒՄՐՈՒ Մ. ՆԱԼԲԱՆԴՅԱՆԻ ԱՆՎԱՆ ՊԵՏԱԿԱՆ ՄԱՆԿԱՎԱՐԺԱԿԱՆ ԻՆՍՏԻՏՈՒՏ
ГЮМРИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ ИМ. М. НАЛБАНДЯНА
GYUMRI STATE PEDAGOGICAL INSTITUTE AFTER M. NALBANDYAN
УЧЕНЫЕ ЗАПИСКИ ԳԻՏԱԿԱՆ ՏԵՂԵԿԱԳԻՐ SCIENTIFIC PROCEEDINGS

Պրակ Ա
Выпуск А
Issue A

2014 № 1

INFORMATICS AND COMPUTING MACHINERY

UDC 004.3

M. E. Harutunyan, N. S. Pahlevanyan

TECHNICAL ASPECTS OF BIOMETRIC SECRET SHARING SYSTEM CONSTRUCTION

Keywords: biometric secret sharing system, “raspberry pi”, biometric sensor, generated secret, helping data, configurable reliability.

Ключевые слова: биометрическая система распределения секрета, “raspberry pi”, биометрический сенсор, генерируемый секрет, вспомогательные данные, конфигурируемая надежность.

Բանալի բառեր՝ կենսաչափական գաղտնիք բաշխող համակարգ, «raspberry pi», կենսաչափական սենսոր, գեներացվող գաղտնիք, օգնող տվյալներ, կոնֆիգուրացվող հուսալիություն:

In this paper we present technical details of construction of biometric secret sharing system with configurable parameters. The system provides possibilities to change secret rate and secret length for required reliability.

Introduction. In last years the traditional passwords are being widely used, even though they have a lot of security related issues.

Biometric secrecy systems can solve many problems that traditional passwords have [1]. Biometric secrecy systems are based on human physical or behavioral features, like fingerprints, irises, faces, voices et al [2]. The measurement results of these features are known as biometric data. Biometric data are unique identifiers of human beings, therefore biometric secrecy systems have huge advantage against the traditional passwords.

However, the usage of biometric secrecy systems has its own limitations. For example, because of biometric data are gathered from individuals under environmental conditions and the channels are exposed to noise biometric secrecy system may accept an impostor or reject an authorized individual. Also biometric secrecy systems are mostly being used for identification and authentication purposes, for that reason biometric data needs to be kept inside some storage (database) and the database might be attacked from inside, which will allow an owner of a database to abuse biometric information. People

have limited biometric resources, so "identity theft" has much more serious impacts than a "simple" theft of credit card.

As mentioned in [3] biometric secrecy systems are grouped around two classes: cancelable biometrics and "fuzzy encryption". Cancelable biometrics has known limitations, so in this paper we will concentrate on "fuzzy encryption" approach, which focuses on generation and binding of secret keys from/to biometric data. Biometric secret sharing systems are based on "fuzzy encryption" approach and can solve above mentioned limitations. Building a biometric secret sharing system, that is secure and allows security configuration to users based on users needs, has a lot of potential in sphere of biometric secrecy systems.

In this paper we present technical details of building mini biometric secret sharing system that will be based on human fingerprint. It will allow an option for setting configurations and user will be able to adjust the reliability of the system, based on his needs. The core of the system will be *Raspberry Pi* single-board mini computer, that will be attached to DigitalPersona's TCS4K swipe sensor.

Devices. The biometric secret sharing system that will generate secret key from biometric data will be built on *Raspberry Pi* single-board mini computer. First versions of Raspberry Pi were built in 2006 by Eben Upton, these versions were based on Atmel ATmega644 microcontroller. Nowadays Raspberry Pi has a Broadcom BCM2835 system on a chip, which includes an ARM1176JZF-S 700 MHz processor, VideoCore IV GPU and was originally shipped with 256 megabytes of RAM, later upgraded (Model B & Model B+) to 512 MB. It does not include a built-in hard disk or solid-state drive, but it uses an SD card for booting and persistent storage, with the Model B+ using a MicroSD [4].

Raspberry Pi has big advantages against other boards, such as high performance, small power consumption, less noise, expansion capabilities, overclocking capabilities, huge community support and small sizes. It is capable to do everything you would expect a desktop computer to do, from browsing the internet and playing high-definition video, making spreadsheets, word-processing, and playing games. Raspberry Pi is designed to run GNU Linux operating system, there are Debian and Arch Linux ARM distributions available for downloading and installation on it. However, we will use Raspbian OS, which is based on Debian kernel, as it comes with over 35000 packages and already optimized for best performance on the Raspberry Pi. Python is the main programming language for Raspberry Pi, but it also supports other languages – Java, C/C++ and others, basically every language that can run on Debian Linux can also be usable on Raspberry Pi.

TCS4K is a sensor for scanning fingerprints, created by DigitalPersona. It is an enterprise-friendly solution for PC makers looking for versatility, including a wide imaging area. It's minutia matching algorithms include support for ISO 19794-2 & ANSI/INCITS 378 compatible minutia templates. The solution also supports additional security features including image data signing, encryption and anti-spoofing. DigitalPersona provides rich

SDK (Software development kit) for TCS4K sensor, which later will be used for creating software part under Raspberry Pi.

Biometric secret sharing model. We consider construct biometric secret sharing system based on generated secret key sharing model (Figure 1). Later chosen secret key model will be added to the system.

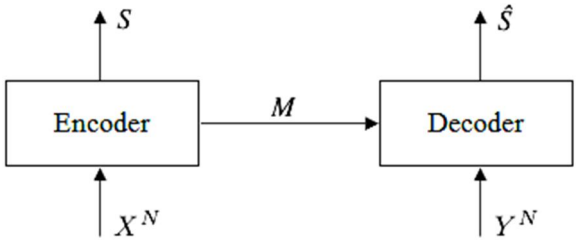

Figure 1. – Generated secret key model

Here X^N is the fingerprint binary sequence at enrolment phase, N is the biometric sequence length, which will be adjustable. S is generated secret from X^N. M is the helper-message (helper data) that is being generated during enrolment phase and later being used in authentication phase for building estimated secret.

Y^N is the noisy version of X^N, also known as authentication sequence. $\hat{S}$ is the reconstructed secret key from helper data and authentication sequence, also known as estimated secret key. More detailed version of the model is available at [3].

When $S = \hat{S}$ system will grant an access to the user, otherwise user will be rejected. From information-theoretical point of view biometric secrecy systems were investigated by O'Sullivan and Schmid [5] and Willems et al [6]. Willems [6] studied the fundamental properties of biometric identification system. It has been shown that it is impossible to reliably identify more persons than capacity which is an inherent characteristic of any identification system. In [7] authors investigated biometric secret sharing models and provided linking between secret key rate, secret length and reliability E.

System construction. System has client-server architecture. Client part is Raspberry Pi + TCS4K sensor. Server part is dedicated machine with database management system, either locally or in the cloud, running GNU Linux or Windows. Client part will get fingerprint binary sequences from individuals and send to server, server part will keep those biometric sequences inside database and will handle "decision making" process during authentication phase for either granting access or rejecting.

The important quantitative measures of a biometric secrecy system are reliability *E,* secret key rate, size of secret key and the information that the helper data leak on the biometric observation. That leak of biometric information is called privacy leakage. The privacy leakage should be small, to avoid the biometric data of an individual to become compromised. Moreover, the secret key length should be large to minimize the probability that the secret key is guessed or is "protected" against brute force attacks.

Client part will include R language inside Raspbian and provide to owner of system the interface inside it, where system owner can adjust *E*-achievable secret key rate and size of secret key, so allowing system to have configurable reliability. R is a language and platform for statistical computing, data manipulation, data mining, calculations and graphics [8]. System model is represented in Figure 2.

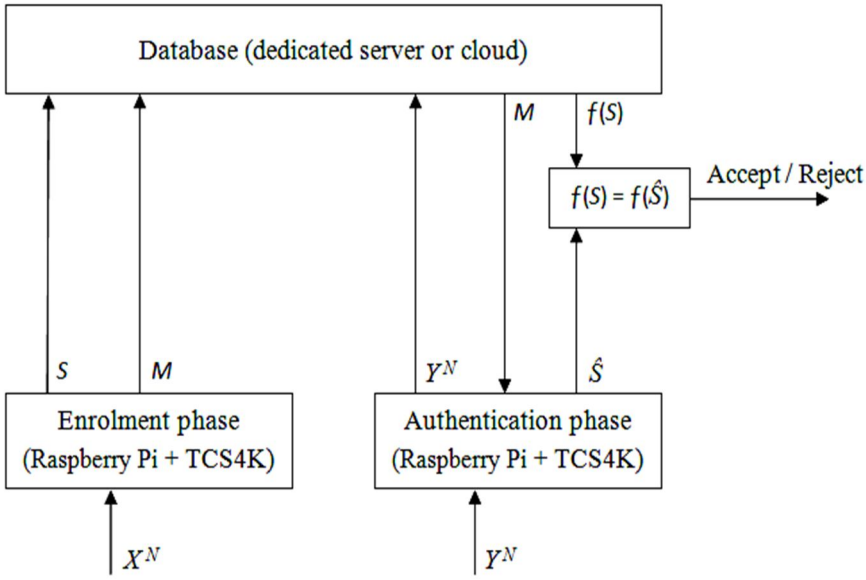

Figure 2. – Biometric generated secret sharing system

At enrolment phase user's biometric data (fingerprint) is being captured and analyzed. A secret key is being generated. Then enrolment sequence is being linked with secret key via helper message. The generated secret key is encrypted using one-way function and stored in the database with helper message.

During authentication phase user's biometric data is being analyzed again and sent to database, then database sends helper messages of users bake to autentication . Using brute-force method system gets the best match of helper message for provided biometric data and estimates secret key. Then one-way function is being applied to estimated secret key and compared with hash version of secret key in the database. If hash values match access is granted, otherwise rejected.

Conclusion. We presented construction details of biometric generated secret sharing system. It allows system owner to adjust *E*-achievable secret key rate and size of secret key, in such way providing system to have configurable reliability. The mentioned system belongs to "fuzzy encryption" biometric secrecy systems group and focuses on generation and binding of secret keys from/to biometric data. It has big advantage against traditional passwords and also solves some limitations that standard biometric secrecy systems have. For example individuals "pure" biometric data are not being kept inside database, rather hash of secret keys and helper data are being kept. As well as an individual can use same

biometric feature multiple times and every time have different records inside database, because each time a new secret will be generated.

Մ. Ե. Հարությունյան, Ն. Ս. Փահլևանյան
Գաղտնիք բաշխող կենսաչափական համակարգի կառուցման տեխնիկական ասպեկտները

Հոդվածում ներկայացվում են կոնֆիգուրացվող պարամետրերով գաղտնիք բաշխող կենսաչափական համակարգի կառուցման տեխնիկական մանրամասները: Համակարգը ապահովում է գաղտնիքի երկարության և արագության փոփոխման հնարավորություններ պահանջվող հուսալիության համար:

М.Е. Арутюнян, Н.С. Пайлеванян
Технические аспекты строительства биометрической системы распределения секрета

В статье рассматриваются технические детали строительства биометрической системы распределения секрета с конфигурируемыми параметрами. Система обеспечивает возможности для изменения скорости и длины секрета для требуемой надежности.

References

1. U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, “Biometric cryptosystems: Issues and Challenges”, Proc. of the IEEE.92(6), pp. 948-960, 2004.
2. Y. Chen and A. H. Vinck, “From password to biometrics: How far can we go”, 7th Asia-Europe Workshop on Concepts in Information theory, Boppard, Germany, pp. 1–8, 2011.
3. T. Ignatenko and F. M. Willems, “Biometric security from an information-theoretical perspective”, Foundations and Trends in Communicationsand Information Theory, vol. 7, no. 23, pp. 135–316, 2012.
4. E. Upton and Gareth Halfacree, “Raspberry Pi User Guide”, first edition, John Wiley & Sons, London, Great Britain, pp. 18-38, 2014.
5. J. A. OSullivan and N. A. Schmid, “Large deviations performance analysis for biometrics recognition.”, Proc. 40th Annual Allerton Conf. on Communication, Control, and Computing, pp. 1–10, 2002.
6. F. Willems, T. Kalker, J. Goseling, and J.-P. Linnartz, “On the capacity of a biometrical identification system,” in Information Theory, 2003. Proceedings.

IEEE International Symposium on Information Theory, Yokohama, Japan, p. 82, 2003.
7. M. Haroutunian, N. Pahlevanyan, “Information Theoretical Analysis of Biometric Secret Key Sharing Model”, Transactions of IIAP of NAS of RA, Mathematical Problems of Computer Science,Vol. 42, pp 17-27, 2014.
8. W. N. Venables, D. M. Smith and the R Core Team. "An Introduction to R", version 3.1.1, pp. 51-77, 2014.

Information about the authors:

Haroutunian Mariam E. - *Professor,* Doctor of Physical and Mathematical Sciences, *Leading Researcher and Head of department for Information Theory and Cognitive Models at Institute for Informatics and Automation Problems, National Academy of Sciences of Armenia, E-mail: armar@ipia.sci.am*

Pahlevanyan Narek S. - *Ph.D student at Gyumri State Pedagogical Institute, E-mail: narek@ravcap.com*

Received 11.09.2014