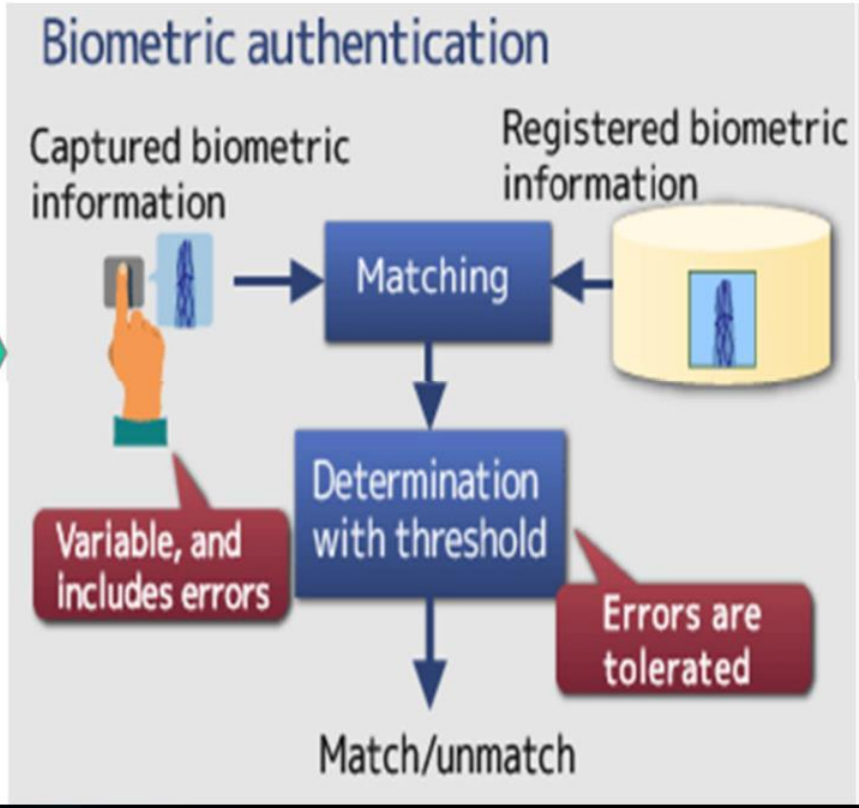
О ПРИМЕНЕНИИ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В ПРОЦЕДУРАХ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

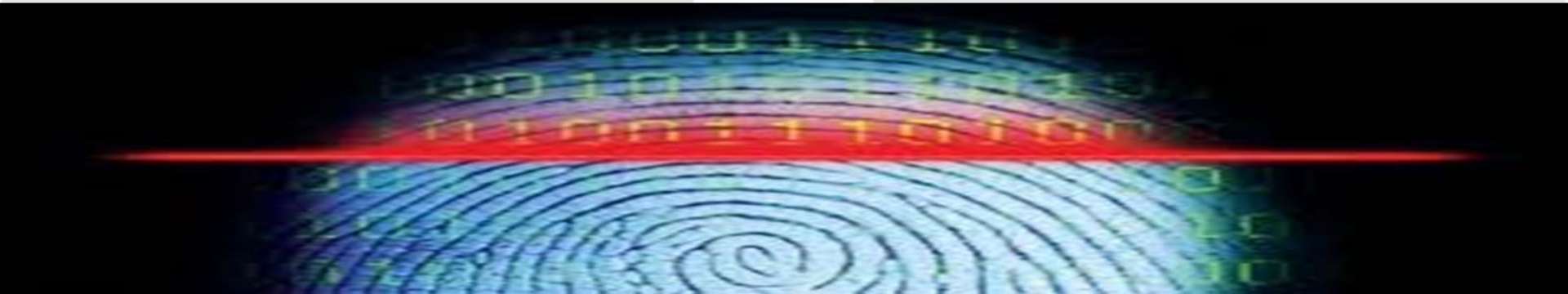
КОМИСАРЕНКО В.В.
директор по развитию
ЗАО «БЕЛТИМ СБ»
Республика Беларусь

Введение

Примеры практического применения «биометрической подписи»

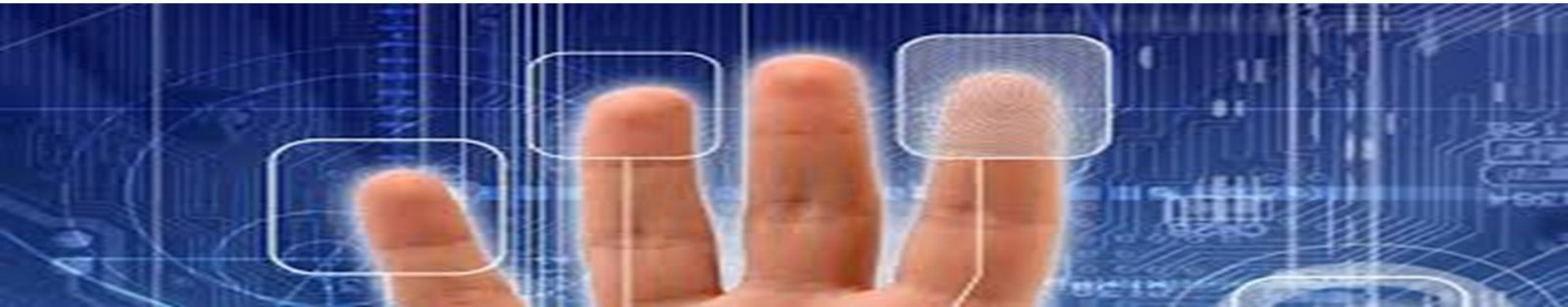
Классические методы



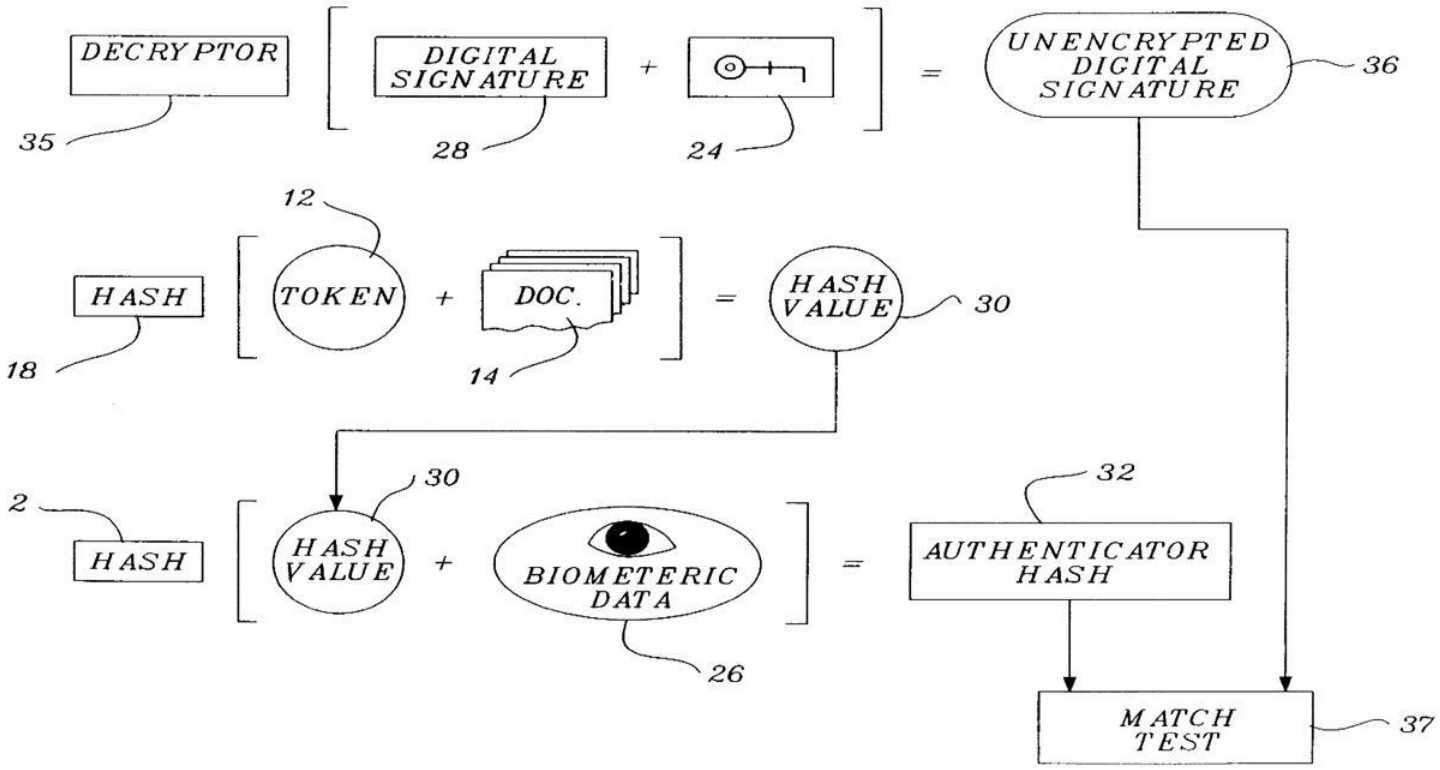


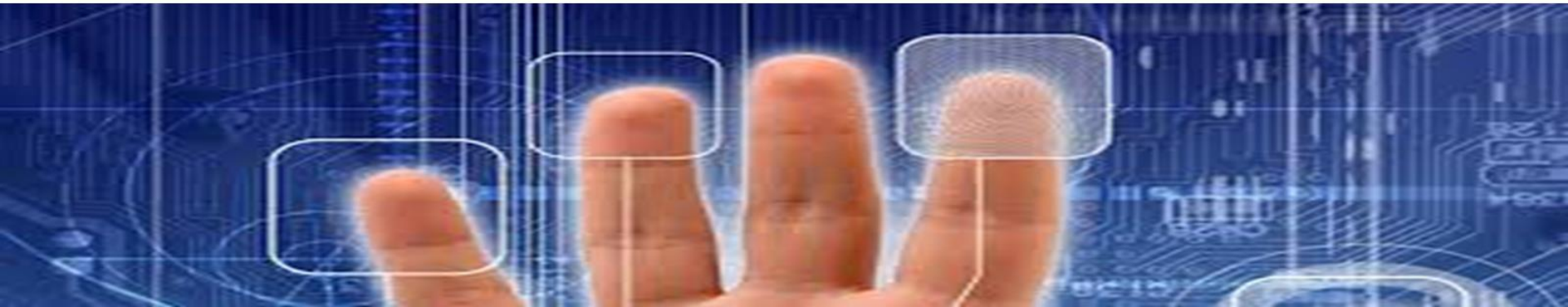
Один из методов применения биометрических данных в процедурах электронной подписи

Method and apparatus for applying and verifying a biometric-based digital signature to an electronic document , 1999
US 6553494 B1

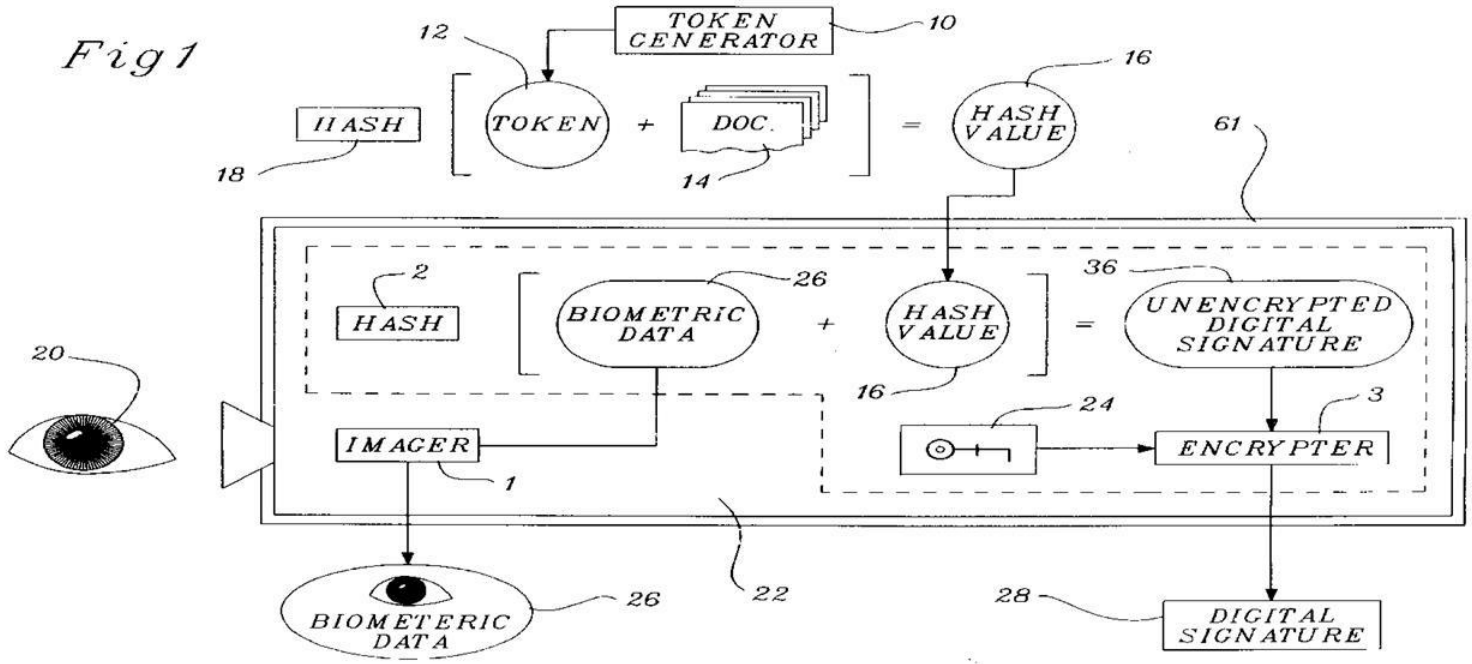


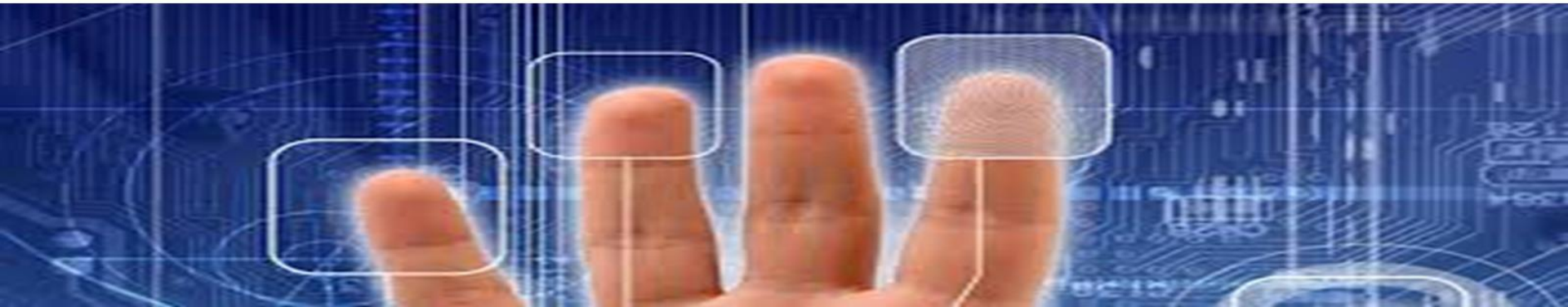
Общая схема метода



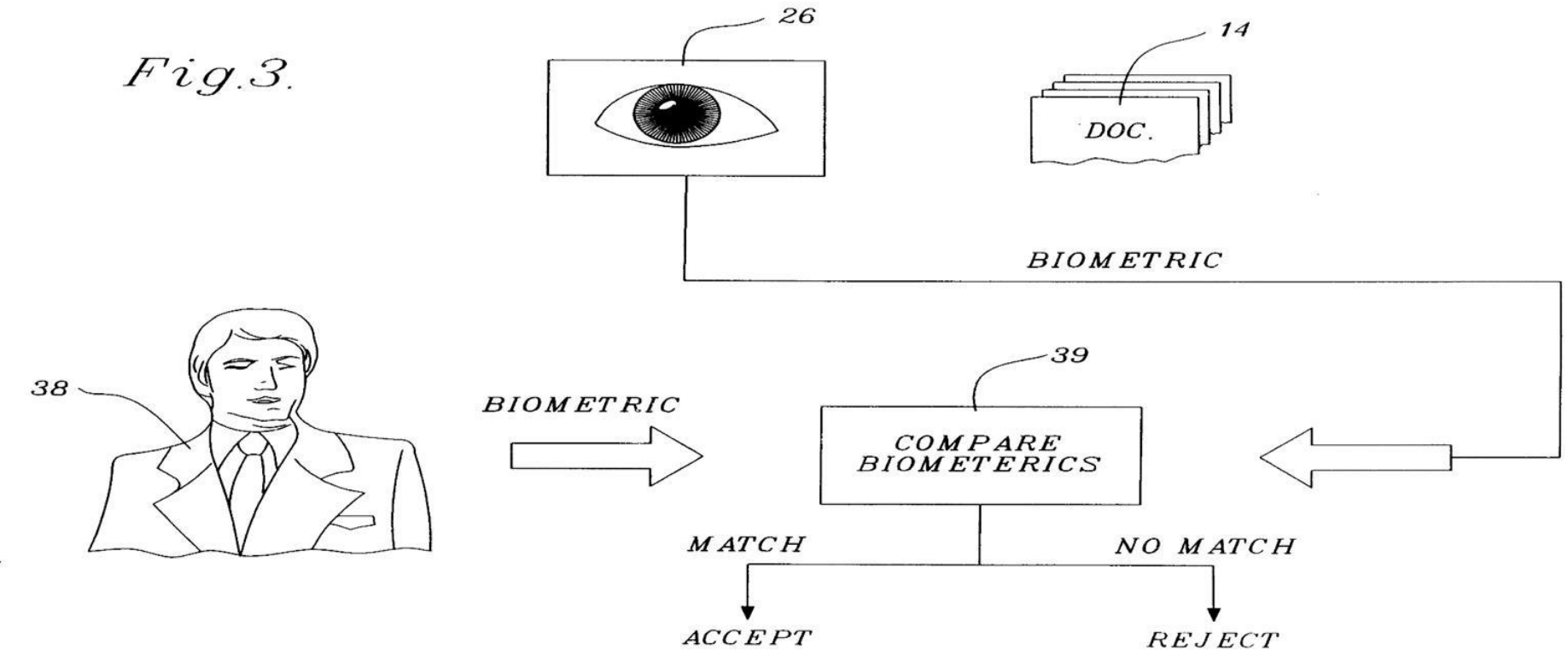


Техническая реализация метода





Проверка подписи



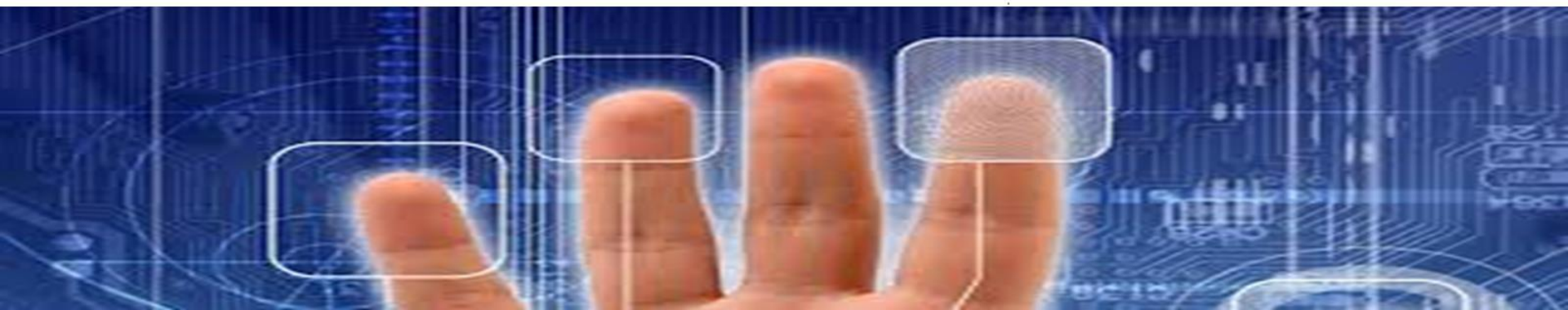


Схема подписи Вотерса. Новая схема подписи без использования случайного оракула

Efficient Identity-Based Encryption Without Random Oracles

Brent Waters

Abstract

We present the first efficient Identity-Based Encryption (IBE) scheme that is fully secure without random oracles. We first present our IBE construction and reduce the security of our scheme to the decisional Bilinear Diffie-Hellman (BDH) problem. Additionally, we show that our techniques can be used to build a new signature scheme that is secure under the computational Diffie-Hellman assumption without random oracles.

Практически удобный метод выработки электронной подписи

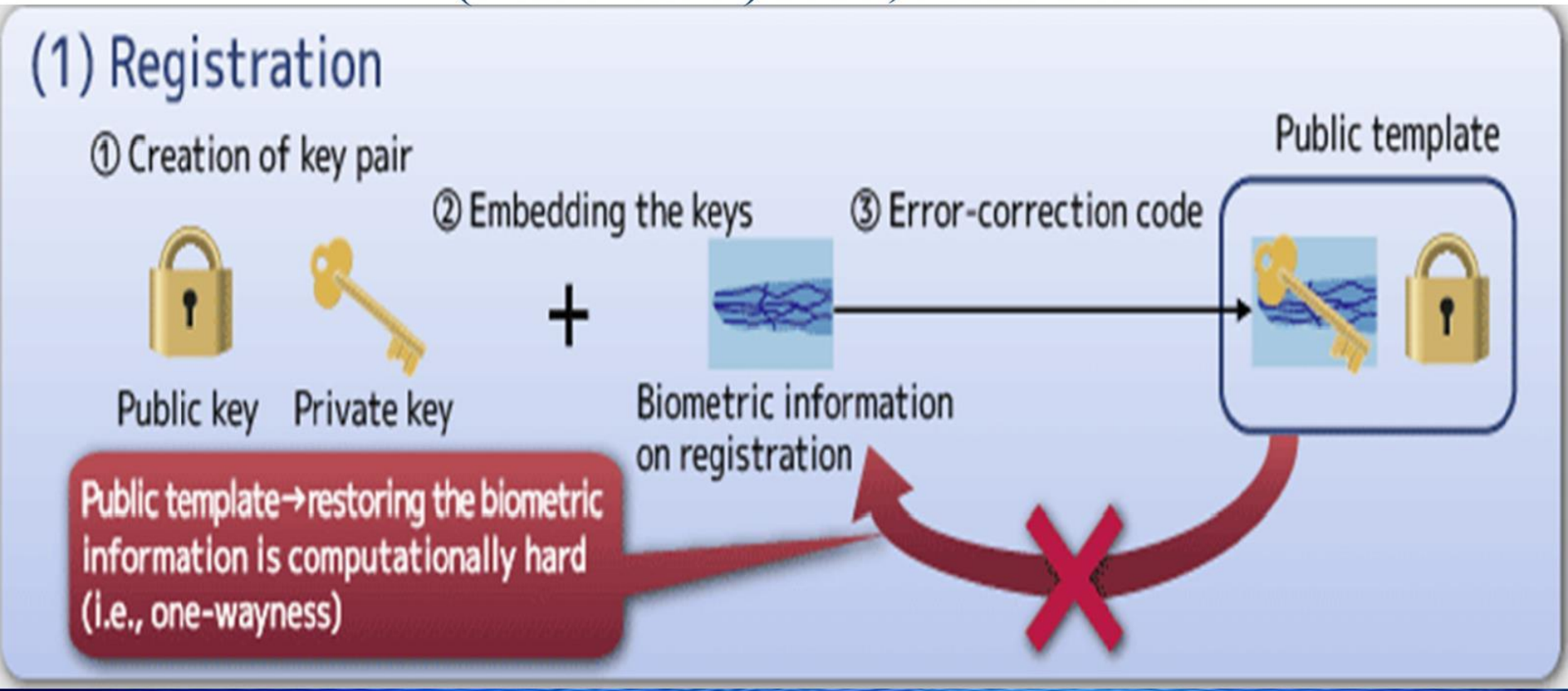
Practical Digital Signature Generation using Biometrics

Taekyoung Kwon[1] and Jae-il Lee[2]

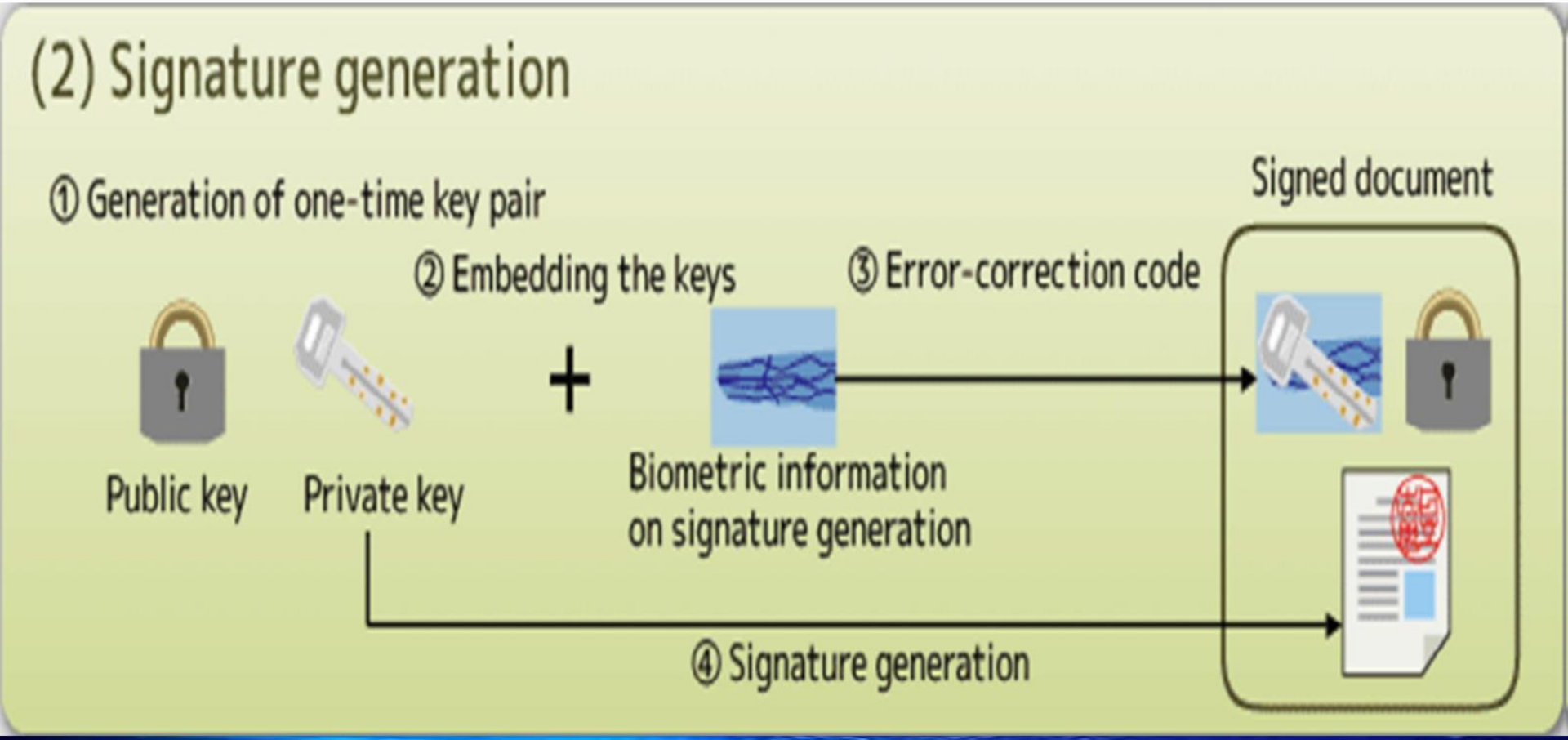
[1] Sejong University, Seoul 143-747, Korea
[2] Korea Information Security Agency, Seoul 138-803, Korea
tkwon@sejong.ac.kr

Abstract. It is desirable to generate a digital signature using biometrics but not practicable because of its inaccurate measuring and potential hill-climbing attacks, without using specific hardware devices that hold signature keys or biometric templates securely. We study a simple practical method for biometrics based digital signature generation without such restriction, by exploiting the existing tools in software in our proposed model where a general digital signature such as RSA can be applied without losing its security.

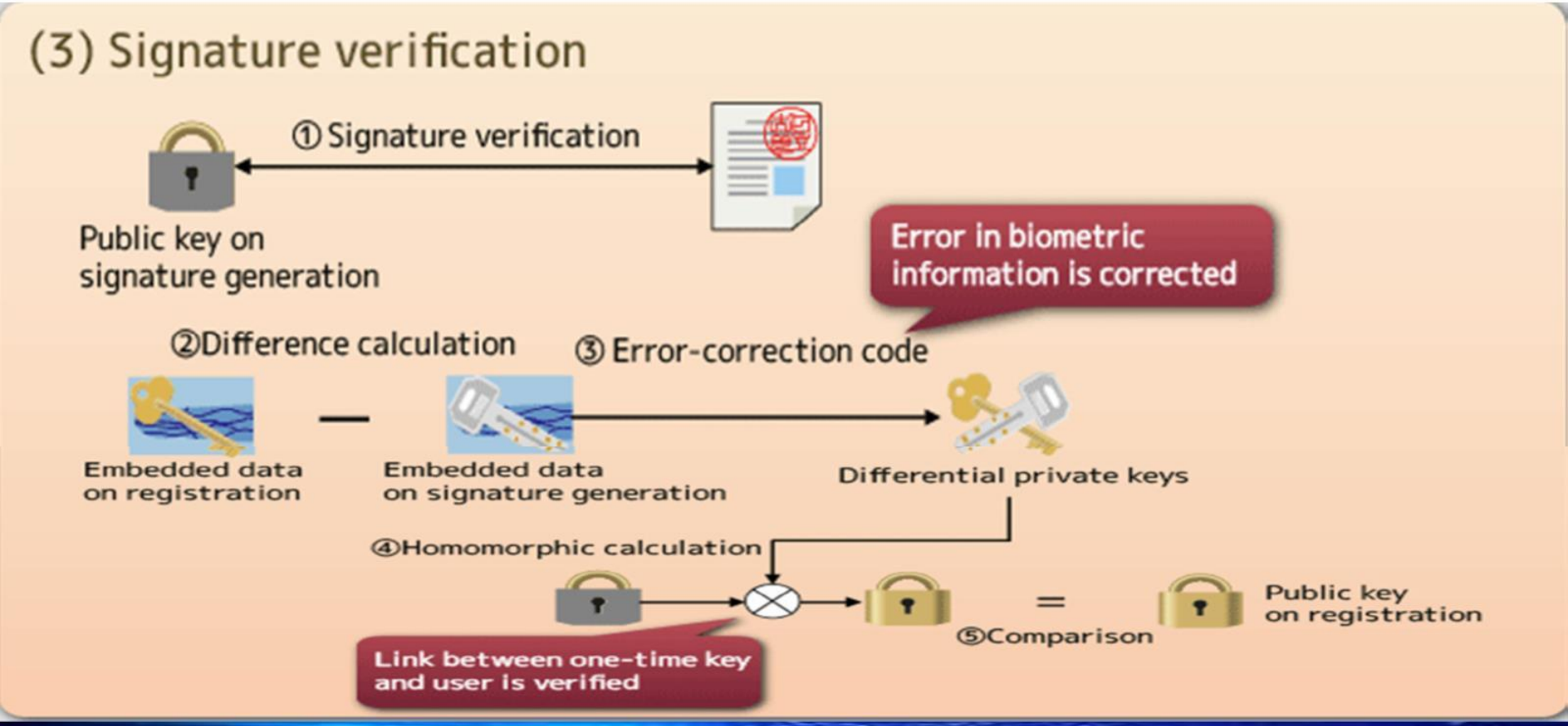
Метод биометрической подписи, применяемый компанией Hitachi Asia (Thailand) Co., Ltd. 2014



Метод биометрической подписи, применяемый компанией Hitachi Asia (Thailand) Co., Ltd. 2014
Процедура подписи



Метод биометрической подписи, применяемый компанией Hitachi Asia (Thailand) Co., Ltd. 2014
Процедура проверки подписи



О ПРИМЕНЕНИИ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В ПРОЦЕДУРАХ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

КОМИСАРЕНКО В.В.
директор по развитию
ЗАО «БЕЛТИМ СБ»
Республика Беларусь