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.
Keywords: Authentication, digital signature, biometrics, public key infrastructure.

1 Introduction

A digital signature is a term used to describe a data string which associates a digital message with an assigned person only. It has various applications in information security such as authentication, data integrity, and non-repudiation. One of the most significant advances in digital signature technologies is the development of the first practical cryptographic scheme called RSA [21], while it still remains as one of the most practical and versatile digital signature techniques available today [2].

One inevitable drawback of the cryptographic schemes is that the signer must carefully hold and possess a signing key which is not memorable at all. It is desirable occasionally to derive the signing key from a human source, say biometrics, rather than keeping it in an external hardware device. Biometrics is actually the science of using digital technologies to identify a human being based on the individual's unique measurable biological (say physiological or behavioral) characteristic such as fingerprint, voice pattern, iris pattern, face, retina, handwriting, thermal image, or hand print. It is widely recognized that (automatic) identification is the most suitable application for biometrics [14, 16]. In some sense, the digital signature can be compared to a biometric signature that is verified by capturing a real hand-written signature. However, it is technically hard to apply biometrics directly to the digital signature because of its inaccurate measuring and potential hill-climbing attacks [22].

Recently several studies have been done in the subject of using biometrics for generating a digital signature. However, some of them are far from practice due to

their inadequate assumption on acquiring deterministic biometrics [15, 18], while some results eventually use biometrics as only a means to access the signing key stored in some hardware devices [8, 20]. This is a seminal paper to study a simple practical method for generating digital signatures using biometrics by exploiting the existing tools in software in our proposed model where a general signature scheme (including an RSA scheme that requires a large signing key) can be applied without losing its security.

The rest of this paper is organized as follows. Section 2 describes preliminaries of this paper. Section 3 introduces the basics of our scheme including the formal model while Section 4 describes more details of the proposed scheme. Section 5 will conclude this paper.

2 Preliminaries

2.1 Related Work

In 2001, P. Janbandhu and M. Siyal studied a method for generating biometric digital signatures for Internet-based applications [15]. Their scheme was actually focused on using a 512-byte iris code invented by J. Daugman [9, 10], and deriving a singature key from the iris code. Though the equal error rate (ERR) of the iris code is only one in a 1.2 million, it does not imply that the same (or even almost the same) sample can be captured from varying biometrics. In 2002, R. Nagpal and S. Nagpal proposed a similar method except that they used a multi modal technique combining iris pattern, retina, and fingerprint in order to derive RSA parameters [18]. However, those schemes fail and are far from practice because of their inadequate assumption that the same biometric samples are always extracted. For example, it is recognized that about 15 percent of the bits in two iris codes captured from the same eye are always different.

In 2002, P. Orvos proposed a method for deriving a signing key from a biometric sample and a master secret kept securely in a smart card [20]. Actually his scheme was only abstract and did not manipulate the detailed method. In the commercial fields, several products that generate a digital signature only by accessing the server or smart card through biometric authentication, are being announced [8]. However, those schemes eventually assume the existence of hardware devices which hold a private key (or semantically equivalent value) or a biometric templates securely.

2.2 This Work

The main goal (or contribution) of this paper is to study a simple method for generating digital signatures using biometrics (from a practical perspective) by exploiting the existing tools in software that can release a human being from hardware devices storing a signing key or a biometric template. The digital signature should be generated in the way that it can be verified by the existing cryptographic algorithm such as RSA without changing its infrastructure. So we carefully define a formal model, explore such tools satisfying our model, and then present our scheme by exploiting them in the following sections.

2.3 Definitions

Security Parameters. Let κ and ℓ denote security parameters where κ is a general one (say 160 bits) and ℓ is a special one for public keys (say 1024 bits).

Digital Signature Scheme. Formally a digital signature scheme is denoted by $\Sigma = (\mathcal{G}_\Sigma(1^\ell), \mathcal{S}, \mathcal{V})$ where $\mathcal{G}_\Sigma$ is a probabilistic algorithm returning a public-private key pair from input 1^ℓ, and $\mathcal{S}$ and $\mathcal{V}$ are respectively signing and verifying algorithms, which run in polynomial time [13].

Public Key Infrastructure. For an authorized assertion about a public key, we use digital certificates issued by a trusted entity called the certificate authority (CA) in the existing public key infrastructure (PKI) [6].

3 Basics of Our Scheme

3.1 Basic Concept

Threats and Requirements. Some drawbacks of deriving a unique deterministic value such as a private key from one's biometrics only (even if it is possible) are that 1) the derived value is to be obsolete once the biometric template is compromised, 2) the possible number of keys are limited exactly by the number of biomentrics enrolled by the user, and 3) the compromise of biometric template eventually implies the permanent corrupt of the user's corresponding biometrics. As for the compromise, we should be aware of a potential biometric vulnerability known as a *hill-climbing attack*. This attack could occur when an attacker has access to the biometric system and the user's template upon which (s)he wishes to mount a masquerade attack [22]. The attacker could exploit the compromised biometric template to produce a new image that exceeds the threshold of the biometric system and use that image again as input to the system to which the original template belongs. The private key (i.e., the signing key) can be derived so easily

As a result, we are given two critical requirements for generating a digital signature using biometrics. They are 1) to randomize the signing key derived from biometrics and 2) to keep the biometric template from hill-climbing attackers. However, we have already postulated that the secure hardware storage is not provided for users. So we need to explore a different model where user's biometrics are acquired but randomized for deriving a signing key and user's biometric templates are resistant to their exposure, without any provision of the secure hardware storage devices.

Formal Model. In order to generate a digital signature using biometrics without smart-card like devices, we postulate that the human users can be scanned with regard to their biometrics and some personal possession that is not protected directly by hardware. So a user is defined formally as $\mathcal{U} = \{\mathcal{B}, \mathcal{P}\}$ where

$\mathcal{B}$ and $\mathcal{P}$ mean respectively user's biometrics and possession. We can regard $\mathcal{B}$ as a probabilistic algorithm returning user's biometrics while $\mathcal{P}$ is deterministic.

Given a signature scheme Σ, we have to manipulate the key returned by $\mathcal{G}_\Sigma$ to be linked with both the user's biometrics and possession. So we define the following transformation:

- $\mathcal{T}_1 : \langle \mathcal{G}_\Sigma(1^\ell), \mathcal{G}_R(1^\kappa), \mathcal{B} \rangle \rightarrow \langle \mathcal{B}_\mathcal{T}, \mathcal{P}_\mathcal{T} \rangle$ and
- $\mathcal{T}_2 : \langle \mathcal{B}, \mathcal{B}_\mathcal{T}, \mathcal{P}_\mathcal{T} \rangle \rightarrow \mathcal{G}_\Sigma$,

where $\mathcal{G}_R$ is a probabilistic algorithm returning a random integer from input 1^κ, and $\mathcal{B}_\mathcal{T}$ and $\mathcal{P}_\mathcal{T}$ are respective transformed values. We then define $\mathcal{P} = \{\mathcal{B}_\mathcal{T}, \mathcal{P}_\mathcal{T}\}$. As a result, $\mathcal{T}_2$ implies that both $\mathcal{B}$ and $\mathcal{P}$, say only a user, can derive the corresponding key generated in $\mathcal{T}_1$. From the perspective of biometrics, $\mathcal{T}_1$ is for enrollment while $\mathcal{T}_2$ is for verification. Similarly, from that of digital signature, $\mathcal{T}_1$ is for initial key generation and key hiding while $\mathcal{T}_2$ is for key recovery and signature generation. Note that it is required that both transformation should be easy to compute but respective inverse transformation must be computationally infeasible. So, it is impractical for our transformation to measure $\mathcal{B}$ by feature extraction which cannot guarantee enough entropy.

In this formal model, $\mathcal{U}$ can be interpreted as an oracle that returns an output $\mathcal{B}$ probabilistically to query $\mathcal{Q}_\mathcal{B}$, and an output $\mathcal{P}$ deterministically to query $\mathcal{Q}_\mathcal{P}$. So we could model the attacker $\mathcal{A}$ who is capable of asking $\mathcal{Q}_\mathcal{P}$ only to $\mathcal{U}$ with regard to the hill-climbing attack. It is obvious that $\mathcal{P}$ can be released from a hardware device and the hill-climbing attack is still defeated in our model if $\mathcal{B}$ is only acquired in a legitimate phase. Similarly an attacker who acquired a sample of $\mathcal{B}$ cannot proceed with generating a digital signature without obtaining $\mathcal{P}$. This could be a standard consideration of two-factor security. Then all we have to do is exploring suitable techniques or tools that satisfy our model.

Practice. As for using biometrics, a fingerprint scanner and a VGA level PC camera are the most widely spread scanning devices available today. So we consider a fingerprint in practice in spite that any biometrics can be applied if only they can be measured with guaranteeing enough entropy.

3.2 Basic Tools

Biometric Encryption. Since it is not easy to derive a cryptographic key from varying biometrics, much work have been done in practice to use an independent, two-stage process to first authenticate the user through biometrics and then release the key from hardware storage [8]. However, very recently, an innovative technique that links the key with the biometric at a more fundamental level during enrollment and then retrieve it using the biometric during verification, has been developed by C. Soutar et al [23].

It is interesting to process the entire fingerprint image rather than doing feature extraction, in the way that seemingly our transformation can be satisfied. So we carefully investigated their scheme and concluded that the so-called biometric

encryption scheme satisfies our formal model in implementing transformation $\mathcal{T}_1$ and $\mathcal{T}_2$. The main reason is that it provides 1) distortion tolerance to accommodate the day-to-day distortion of the fingerprint image, 2) discrimination to distinguish the aimed one clearly from other fingerprints, and 3) security to extract independently neither the cryptographic key nor the legitimate fingerprint from the stored data that can be queried by $\mathcal{Q}_{\mathcal{P}}$ in our formal model. During enrollment, a secure block of data called a Bioscrypt is generated by $\mathcal{T}_1$, while it can be combined with the biometric image sample for $\mathcal{T}_2$ during verification.

2D Bar Codes. In order to make a user possess $\mathcal{P}$ without any hardware device, we consider to print it out on a small size paper that can be kept in a wallet and read easily by the PC camera available in today's computing environment. A bar code is the dominant automatic identification technology that fits our purpose [19]. Especially two-dimensional codes provide much higher information density than conventional ones. For example, a 2D bar code symbol can hold up to about 4,300 alphanumeric characters or 3,000 bytes of binary data in a small area [12]. With the immense storage capacity, the development of 2D bar codes enables the data exchange under off-line condition [19]. The 2D bar code may work as a portable data file because the information can be received without access to a database. The 2D bar codes also have an excellent data restoration capability for a damaged symbol. There are four widely used 2D bar codes that are ISO standard: PDF417, DataMatrix, QRcode and Maxicode. QRcode(Quick Response code) is particularly developed for high data capacity, reduced printing space, and high speed reading [12]. We have chosen the 2D bar codes as a means to manipulate the external source of deterministic information, $\mathcal{P}$.

4 Practical Biometric Digital Signature Generation

4.1 Assumption

We suppose to use a simple hash-and-sign RSA primitive in a probabilistic manner (with κ_Σ-bit random numbers). The public-private keys are respectively $\langle e, N\rangle$ and $\langle d, N\rangle$ where N is the product of two distinct large primes p and q, and $ed \equiv 1 \bmod \phi(N)$ for the Euler totient function $\phi(N) = (p-1)(q-1)$ [21]. The public key is postulated to be certified by the CA. We assume $\mathcal{S}$ returns signature on a message m; $\langle s, r\rangle$ where $s \leftarrow H(m,r)^d \bmod N$ and $r \leftarrow_R \{0,1\}^{\kappa_\Sigma}$. The two-party RSA is the case that the private key is split into two shares such that $d \equiv d_1 d_2 \bmod \phi(N)$ [1, 5]. For our manipulation, a drawback of RSA is the huge size of private key. Though we have chosen RSA for wide acceptance, it is considerable to use a different signature scheme in a GDH (Gap Diffie-Hellman) group over E/F_{3^l} [4] or an elliptic curve group for more spatial efficiency and easier manipulation on a short private key.

As for acquiring fingerprint images, the mechanism of correlation is the basis for it [23]. Let $f(x)$ denote a two-dimensional input image array and $F(u)$ its corresponding Fourier Transform (FT) mate, where x denotes the space domain

and u the spatial frequency domain. Then correlation is normally used to provide a single scalar value which indicates the degree of similarity between one image, $f_1(x)$, obtained during verification and another obtained during enrollment, $f_0(x)$, that is represented by the filter function, $H(u)$, derived from a set of $T(\geq 1)$ training images $\langle f_0^1(x), f_0^2(x), ..., f_0^T(x)\rangle$. The correlation function is formally defined as

$$c(x) = \int_{-\infty}^{\infty} f_1(v) f_0^*(x+v) dv$$

where $*$ implies the complex conjugate. In practice, it is obtained by computing the inverse Fourier Transform (FT^{-1}) such that $c(x) = \mathrm{FT}^{-1}\{F_1(u)F_0^*(u)\}$, where $F_0^*(u)$ is represented by $H(u)$ that must be the biometric template tolerant to distortion in correlation-based biometric systems [23]. The stored filter function is defined as

$$H_s(u) = e^{-i\varphi_{A_0}(u)} e^{i\varphi_R(u)}$$

where the phase of the complex conjugate of the training set images, $e^{-i\varphi_{A_0}(u)}$, and the random phase-only function, $e^{i\varphi_R(u)}$, are only multiplied. The magnitude terms of the optimal filter can be calculated on-the-fly during either enrollment or verification and are denoted by $|\cdot|$.

4.2 Key Generation ($\mathcal{T}_1$ Transformation)

Input. A user $\mathcal{U}$ provides a series of fingerprint images $\langle f_0^1(x), f_0^2(x), ..., f_0^T(x)\rangle$ as input $\mathcal{B}$. A conventional fingerprint scanner or high quality PC camera can be deployed for acquiring those images.

Key Split. $\mathcal{G}_\Sigma(1^\ell)$ outputs an RSA public-private key pair, $\langle e, N\rangle$ and $\langle d, N\rangle$. As for the private exponent, an t-bit integer d_1 is chosen at random to be relatively prime to $\phi(N)$ and d_2 is computed for a large integer k as follows:

$$d_2 = dd_1^{-1} \bmod \phi(N) + k\phi(N)$$

Note that d_2 is to be huge, for example, about $\log k + \ell$ bits, while d_1 is small, for example, only 128 bits. Our manipulation has considered Wiener's attack to be defeated [24]. Readers are referred to Section 4.4 with regard to security.

Image Processing. A series of input images are combined with a random phase array to create two output arrays, $H_s(u)$ and $c_0(x)$, where $H_s(u) = e^{-i\varphi_{A_0}(u)} e^{i\varphi_R(u)}$ and $c_0(x) = \mathrm{FT}^{-1}\{A_0(u) \cdot |H_0(u)| \cdot H_s(u)\}$ [23].

Encoding. Given the partial key d_1, the central $\frac{t}{2} \times \frac{t}{2}$ portion of $c_0(x)$ must be extracted and binarized for marority-encoding d_1. A complex element $a + bi$ at position (x, y) of the $\frac{t}{2} \times \frac{t}{2}$ portion of $c_0(x)$ will be fragmented in the way that a will appear at (x, y) and b at $(x + \frac{t}{2}, y)$ in the $t \times \frac{t}{2}$ binarized template [23]. Now the binarized template, bt, contains $\frac{t^2}{2}$ real values that can be binarized

with respect to 0.0, i.e., set as 1 if they are equal to or greater than 0.0, and otherwise 0. From bt, we can compose a lookup table, L, which may encode d_1 in the way that a number of locations whose element values are equal to each bit of d_1 are stored in each corresponding column.

Possession. Finally the user's possession $\mathcal{P}$ is defined as $\mathcal{B}_{\mathcal{T}} = \{H_s(u), L\}$ and $\mathcal{P}_{\mathcal{T}} = \{d_2, N\}$. In other words, $\langle \mathcal{B}_{\mathcal{T}}, \mathcal{P}_{\mathcal{T}} \rangle$ is encoded and printed by an arbitrary 2D bar code such as PDF417 or QRcode.

4.3 Signature Generation ($\mathcal{T}_2$ Transformation)

Input. A user $\mathcal{U}$ provides a series of fingerprint images $\langle f_1^1(x), f_1^2(x), ..., f_1^T(x) \rangle$ as input $\mathcal{B}$ along with his or her possession $\langle \mathcal{B}_{\mathcal{T}}, \mathcal{P}_{\mathcal{T}} \rangle$, say $\langle H_s(u), L, d_2, N \rangle$, in 2D bar codes that are readable by a PC camera.

Image Processing. A series of input images are combined with $H_s(u)$ to create a new output array, $c_1(x)$ where $c_0(x) = \mathrm{FT}^{-1}\{A_1(u) \cdot |H_1(u)| \cdot H_s(u)\}$.

Majority Decoding. Given the lookup table L, the central $\frac{t}{2} \times \frac{t}{2}$ portion of $c_1(x)$ must be extracted and binarized for majority-decoding d_1. A method to obtain the new binarized template, bt', is exactly the same to that of key generation process. From bt' and L, we can compose a new table L' which may majority-decodes d_1 in the way that a majority bit in each column is derived to each location in d_1.

Signature Generation. Given an arbitrary message M, $\mathcal{S}$ raises it to the power of d_1 and subsequently the result to the power of d_2 for obtaining the corresponding signature $M^d \equiv (M^{d_1})^{d_2} \pmod{N}$. This is obvious because $d \equiv d_1 d_2 \equiv d_1\{dd_1^{-1} \mod \phi(N) + k\phi(N)\} \pmod{\phi(N)}$.

4.4 Analysis

Security against Wiener's Attack. In 1990, M. Wiener first showed that instances of the RSA cryptosystem using low secret exponents are insecure [24]. Here "low" implies that the length of d must not exceed approximately one-quarter of the length of N. The so-called Wiener's attack is based on the continued fraction algorithm that if $|x - \frac{a}{b}| < \frac{1}{2b^2}$ holds for a (known) rational x and two (unknown) co-prime integers a and b, the value $\frac{a}{b}$ is a convergent of the continued fraction expansion of x and can be obtained in polynomial time. As for RSA, Wiener set $x = \frac{e}{N}$, $a = c$, and $b = d$ where $ed - c\lambda(N) = 1$ and $\lambda(N) = \mathrm{lcm}(p-1, q-1)$. Note that $\lambda(N)$ can preferably be used instead of $\phi(N)$. So, d can be recovered in polynomial time unless c is sufficiently large. In order to make c large, Wiener proposed to use $e' = e + k\lambda(N)$ without exposing

e where k is set to have $e' > N^{1.5}$. Also, Boneh and Durfee improved the related attack and showed the higher boundary for e' [3].

In the proposed system, the parameter t for obtaining a portion of $c_0(x)$ might be set as 128 bits, so that the partial secret exponent d_1 should have 128 bits only while d_2 is not protected by any secure device. Recall that $ed_1d_2 \equiv 1 \mod \lambda(N)$ in our system. So, an adversary who obtained $\mathcal{P}$ can set $x = \frac{ed_2}{N}$, $a = c$, and $b = d_1$ where $ed_1d_2 - c\lambda(N) = 1$. However, recall that we defined $d_2 = dd_1^{-1} \mod \lambda(N) + k\lambda(N)$ when we preferably use $\lambda(N)$ instead of $\phi(N)$. So, we have

$$x = \frac{ed_2}{N} = \frac{e(dd_1^{-1} \bmod \lambda(N) + k\lambda(N))}{N} = \frac{d_1^{-1} \bmod \lambda(N) + ek\lambda(N)}{N}$$

for d_1. This equation gives

$$\begin{aligned}\left|\frac{ed_2}{N} - \frac{c}{d_1}\right| &= \left|\frac{d_1(e'' + k'\lambda(N)) - c\lambda(N) - cN + c\lambda(N)}{d_1N}\right| \\ &= \left|\frac{1 - c(N - \lambda(N)) + d_1k'\lambda(N)}{d_1N}\right| \\ &= \left|\frac{1 - c(N - \lambda(N))}{d_1N} + \frac{k'\lambda(N)}{N}\right| \\ &< \left|\frac{1 - c(N - \lambda(N))}{d_1N} + k'\right| \not< \frac{1}{2d_1^2}\end{aligned}$$

where $e'' = d^{-1} \mod \lambda(N)$ and $k' = ek$. So we can see obviously that the large integer k can prevent our system from Wiener's attack launched on the small partial secret exponent d_1. Say, the adversary cannot obtain d_1 and subsequent signature even if she acquired $\mathcal{P}$ including d_2.

On Practicality. In our system, we postulated $\mathcal{B}$ is a secret value while it is only measured by image processing. Also, the size of d_2 was assumed about $k+\ell$ bits where k is less than ℓ. So the liveness check for $\mathcal{B}$ is additionally necessary while its minimized template can be stored in $\mathcal{P}$, say exactly $\mathcal{P}_\mathcal{T}$, under the easy consideration of the hill-climbing attack. Note that a human user can possess $\mathcal{P}$ in his (or her) wallet, mobile phone, pda, wristwatch, or even a remote server (such as a home server when we consider an advanced digital home network). As for the length of d_2, the digital signature is eventually generated on an arbitrary computing machine equipped with the necessary scanners. When we consider the number of the most expensive modular N multiplications [17], our RSA signature generation using the repeated square-and-multiply algorithm will take $t + k + \ell$ (approximately 2ℓ) modular squarings and expected $\frac{t+k+\ell}{2}$ (approximately ℓ) modular multiplications. This means only the double of the usual RSA signature generation time. Note that we could apply discrete logarithm based digital signature schemes using smaller private exponents in much easier ways. So we believe that our scheme is practical in the real world and is the first practical scheme considering biometrics based digital signature generation.

5 Conclusion

We have studied a simple practical method for biometrics-based digital signature generation, in which biometric encryption, fingerprint verification, and bar code technology are combined to generate a digital signature by satisfying our formal model. The proposed method allows a human user to generate a digital signature on an arbitrary message off-line by being scanned biometrics and 2D bar codes without having any hardware device securely storing a signing key. We believe our scheme is the first practical scheme considering biometrics based digital signature generation.

Acknowledgement

This research was supported in part by University IT Research Center Project.

References

1. M. Bellare and R. Sandhu, "The security of practical two-party RSA signature schemes," Manuscript, 2001.
2. D. Boneh, "Twenty years of attacks on the RSA cryptosystem," Notices of the American Mathematical Society (AMS), vol. 46, no. 2, pp.203-213, 1999.
3. D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," Eurocrypt '99, Lecture Notes in Computer Science vol. 1592, Springer-Verlag, pp.1-11, 1999, and IEEE Trans. on Information Theory, vol. 46, no. 4, 2000.
4. D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the weil pairing," Asiacrypt '01, Lecture Notes in Computer Science vol. 2139, Springer-Verlag, pp.514-532, 2001.
5. C. Boyd, "Digital multisignatures," *Cryptography and Coding*, Oxford University Press, pp.241-246, 1989.
6. S. Brands, *Rethinking public key infrastructures and digital certificates*, The MIT Press, p.11 and pp.219-224, 2000.
7. H. E. Burke, "Handbook of bar Coding Systems," *Van Nostrand Reinhold*, New York, N.Y., 1984.
8. Daon Inc., "Biometric Authentication & Digital Signatures for the Pharmaceutical Industry," White paper available at `http://www.daon.com/downloads/publications/esignature.pdf`
9. J. Daugman, "High confidence personal identifications by rapid video analysis of iris texture," IEEE International Carnahan Conference on Security Technologies, pp.50-60, 1992.
10. J. Daugman, "High confidence personal identifications by a test of statistical independence," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.15, no.11, pp.648-656, November 1993.
11. G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," IEEE Symposium on Security and Privacy, pp.148-159, 1998.
12. Denso Inc., "QRmaker: User's Manual," *Denso Corporation*, Aichi, Japan, 1998.

13. S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal of Computing*, vol.17, no.2, pp.281-308, Apr. 1988.
14. A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, February 2000.
15. P. Janbandhu and M. Siyal, "Novel biometric digital signatures for Internet-based applications," Information Management & Computer Security, vol.9, no.5, pp.205-212, 2001.
16. V. Matyáš and Z. Říha, "Biometric authentication - security and usability", Manuscrypt available at `http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf`
17. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, pp.287-291, pp.312-315, 1997.
18. R. Nagpal and S. Nagpal, "Biometric based digital signature scheme", Internet-Draft, draft-nagpal-biometric-digital-signature-00.txt, May 2002.
19. Roger. C. Palmer, "The Bar Code Book," *Helmers Publishing*, Peterborough, N.H., 3rd Ed., 1995.
20. P. Orvos, "Towards biometric digital signatures," Networkshop, Eszterhazy College, Eger, pp.26-28. March 2002.
21. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol.21, pp.120-126, 1978.
22. C. Soutar, "Biometric system performance and security," Manuscrypt available at `http://www.bioscrypt.com/assets/bio_paper.pdf`, 2002.
23. C. Soutar, D. Roberge, A. Stoianov, R. Golroy, and B. Vijaya Kumar, "Biometric Encryption," ICSA Guide to Cryptography, McGraw-Hill, 1999, also available at `http://www.bioscrypt.com/assets/Biometric_Encryption.pdf`
24. M. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, vol.36, no.3, May 1990.