Biometrics: Application in Cryptographic Signatures

Eugene Phan Hin Min
<hpha013@ec.auckland.cs.nz>
University of Auckland
20 October 2006

Abstract. There has always been the use of cryptographic techniques by governments and corporations to keep secrets. However, in recent years cryptographic solutions have become available to individuals, e.g. Pretty Good Privacy (PGP). With the increasing use of cryptography, the key management process particularly for public key systems has become complicated. In an attempt to simplify this, a suggested solution is the identity-based encryption (IBE) scheme. This is a public key cryptosystem that utilizes a publicly available string to encrypt the message. This arbitrary string should uniquely identify the intended receiver, e.g. an email address, etc. Would biometrics be able to provide a unique non-repudiatable identity in such a scheme?

This paper begins with introduction cryptography, what it is, and briefly explains how it operates. This paper further describes the cryptographic systems available and focuses on one of them. Next, the IBE scheme is introduce as a means of simplifying the public-key cryptosystem. A current work is presented on the incorporation of biometrics into an IBE signature (IBS) scheme including a proposed implementation. This paper will conclude as to whether the applicability of biometrics in an IBS scheme.

Acknowledgment. With thanks to Dr Clark Thomborson (University of Auckland) for advice on research topic and materials and feedback on research paper.

1. Introduction

The world in the 21st century is more integrated and fast-pace than ever and shows no signs of slowing down. The global economies have become more inter-dependent, commerce more competitive, and so are political interests. Communication and the movement of information take minutes rather than days and weeks of 100 years ago due thanks to electronic networks that span the globe. Yet the requirement for information secrecy remains: confidential, reliable, and accessible only to the intended person[1]. The protection of the information before, during, and after transmission becomes a prime concern. A secured transmission over an unsecured channel requires the information be packaged such that to any interceptor the package is useless but remains intelligible to the intended recipient. Such protection requires special techniques and systems to be used - this is the realm of cryptology.

Cryptology studies the secure means by which the information can be securely transmitted over unsecured communication. This encompasses cryptography, which is the process of designing such a system, and crypto-analysis, which studies the means by which the designed system may be compromised[5].

In this paper we will focus our attention on public-key cryptographic system.

2. Cryptology

A typical secure transmission can be described in this way. Alan has important and confidential information, in plaintext, for Becky. He does not want anyone else to know what the information is, least of all Caine. Alan converts his plaintext into ciphertext with an encryption key and method agreed beforehand with Becky. Becky, on receiving the ciphertext, retrieves the plaintext with a decryption key. Caine, not knowing the keys will not be able to know what the plaintext is, even though he may be knowledgeable about the encryption method e.g. DES (Data Encryption Standard).

The security in a cryptographic system depends on the secrecy of the keys rather than the knowledge of how the algorithms. The algorithms themselves are public knowledge but do not compromise the secrecy of the information being protected. Kerckhoff's principle is an assumption in cryptology - that the opponent is knowledgeable about the methods used[5].

A perfect cryptographic system is difficult and costly to create as well as maintain. Yet secrets are required to be kept safe and prevented from falling into the hands of hackers. A secure cryptographic system discourages hackers from breaking in because it is too costly in terms of time, effort, and material. In addition, if they (the hackers) get caught a hefty penalty would be expected. On the other hand, an extremely secure cryptographic system to protect trivial information does not justify the expenditure in the creation and maintenance of the system. There is a need to balance between the costs of losing the protected secret and of protecting the same secret[1].

In the scenario of Alan, Becky, and Caine described above, we assumes that Caine is more interested in obtaining knowledge of the decryption key rather than preventing Becky from receiving the ciphertext. The ability to obtain the decryption key would allow Caine to monitor the messages between Alan and Becky without being noticed.

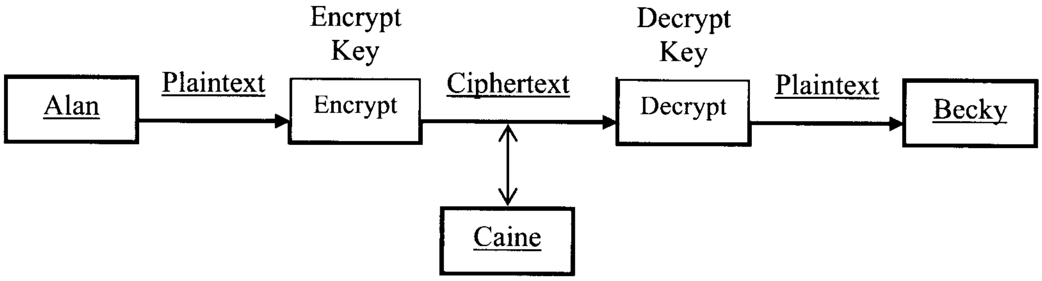

Fig 1: Cryptography Communication Scenario[5]

Caine could attempt to deduce the decryption key by the following methods[5]:
(a) Caine intercepts a copy of the ciphertext.
(b) Caine obtains both the ciphertext and plaintext. This could also be in the form of some fragments of the ciphertext with the corresponding plaintext.
(c) Caine gets temporary access to the encryption program or machine but the encryption key is not accessible. By encrypting a large number of carefully chosen plaintext Caine can attempt to deduce the decryption key from the resulting ciphertext.
(d) Conversely if Caine could get access to the decryption program or machine he could decrypt strings of symbols or even previously obtained ciphertext and attempt to deduce the decryption key from there.

3. Cryptographic Systems

The algorithms used for encryption/decryption fall generally in to groups - symmetric and public key algorithms[5].

In symmetric key algorithms the encryption key would be shared to the communicating parties in a secure manner. The decryption key would then be easily derived from the encryption key although typically both keys are identical. Symmetric algorithms include Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

In public key algorithms only the encryption key is made known to the public, hence the term "public key". The decryption key is kept secret, i.e. privately, by the owner and cannot be easily derived from the public key. This pairing of public-private keys is commonly known as a key-pair and only a corresponding private key can decrypt a message encrypted by the respective public key.

A public key cryptosystem is implemented in a framework that defines the rules and procedures under which the system would operate. Such a framework is called the public key infrastructure (PKI). Within the PKI are one or more secure sites belonging to publishers that are 'trusted' by users - even though the users may not trust each other. A PKI can be located in the public domain or within a corporate local or global network, and may include several CAs working together.

The trusted publishers, called certificate authority (CA), generate keys on behalf of users and publish the public keys in the form of digital certificates. A user requesting a CA to generate one or more key-pairs would need to provide some form of identification e.g. email address, phone number, etc. The CA will validate this information and will be bind it to the public key in the certificate.

Suppose Becky uses a CA to generate and publish her public key. When Alan wants to send a message to Becky, he will need to obtain Becky's latest certificate from the CA. What would happen if the CA was down at that particular time and unable to issue certificates?

Becky could generate and manage her own keys but that would include having to distribute the certificates every time someone wants to encrypt a message for her. In addition, if she has multiple certificates for different groups of people - one for her office, another for family members, yet another for friends, etc. In addition, Becky would have to handle certificate revocation as well. The certificate management is not an easy process and could be time consuming.

In 1984, Adi Shamir floated an idea to simplify the certificate management process[2] for the email system.

4. Identity-Based Encryption (IBE) Scheme[3]

In an IBE scheme, if Alan wants to send an encrypted message to Becky, all he needs as an encryption key is an arbitrary string that uniquely identifies Becky. Alan does not need to go to a CA to obtain Becky's certificate. This arbitrary string could be an email address, phone number, or home address. For example, Alan uses Becky's email, "Becky@beckymail.com", as the public key. Becky goes to a third party called the Private Key Generator (PKG), authenticates herself in a similar way as a CA, provides her email address, and obtains her private key. With the private key Becky can read her email from Alan.

An IBE scheme consists of three algorithms:
(a) Setup: creates the global system parameters and master key when Becky initially registers and authenticates herself.
(b) Extract: generates the private key for Becky given the arbitrary string used as encryption key, in the example above it would be "Becky@beckymail.com".
(c) Encrypt: used by others like Alan to encrypt messages to Becky.
(d) Decrypt: used by Becky to decrypt messages from others like Alan.

With an IBE scheme, Alan's message is independent of whether Becky has setup her master/private keys with the PKG. Also the PKG acts key escrow for Becky's master key.

The IBE scheme main advantage is the simplification of managing a large number of public keys. In particular, the IBE email scheme presented in [3] highlights two advantages: revocation of public keys and self-delegation of private keys.

Each time Alan sends Becky a message, he appends the current year to the encryption key. Becky would not be able to decrypt a message that has a new year appended to the arbitrary string and she would have to get a new private key from PKG. This approach requires that everyone, including those external to the corporate system, follow this format.

Delegation of private keys entails Becky generating the system parameters (param) and master key herself. Becky can use 'param' as a public key by obtaining a certificate from a CA for it. Alan will encrypt with 'param' from Becky's public certificate. When Becky goes on a business trip, she can generate private keys according to the dates of her trip. Anyone who sends her an email would use the appropriate date as the encryption key. At the same time Becky may delegate some responsibilities when she's away on that business trip. In this case, Becky generate private keys according to fixed subject line, e.g. purchasing, delivery, etc., to the assistants who can only read Becky's email that uses the appropriate subject line as encryption key.

The ability to delegate implies that the IBE scheme could be implemented without the need for a key escrow.

5. Biometrics in IBE Signature Scheme

Biometrics technology is gaining attention in recent years mainly due to security concerns. We see cameras and fingerprint capture devices in airports and to a limited extent in commercial field e.g. fingerprint sensors on laptops and video stores using fingerprint as authentication methods. We see biometrics used in law and order; handwriting and fingerprinting in forensics and in recent years, DNA, or Deoxyribonucleic acid[7], has become admissible evidence in US courts.

Biometrics attempts to differential individual from each other based on some physical and/or behavioral traits. These traits include but not limited to fingerprint patterns, facial features, iris patterns, speech behavior, and handwriting. Each person differs in these traits and that uniqueness is non-repudiatable and would be useful for identification and verification. Unfortunately, a major drawback is that the same biometric measurement cannot be reproducible with any consistently as it changes with time, wear, and tear[6].

In an IBE scheme, the public key is the identity, an arbitrary string that identifies the person e.g. email address. In their proposal, Andrew Burnett, et al, describes a biometric identity-based signature (BIO-IBS) scheme whereby a biometric measurement as the arbitrary identifying string in an IBE scheme[4]. The specific application is in the electronic signing of binding documents/contracts, where non-repudiation is of utmost importance, with digital signatures. Andrew Burnett, et al, describe the method of extracting a biometric feature, deriving a key-pair, and applying this key-pair in digital signature and subsequent verification.

5.1 Biometric String Extraction, Key-Pair Generation, Digital Signing

Work from Y. Dodis et al,[8] and Wattenberg et al,[9, 10] form the basis of Burnett's method of extracting a viable 'string' from a biometric input, with the Hamming Distance metric space applied to ensure a "uniform level of randomness"[8] from the biometric input so that subsequent input from the same biometric feature having a certain amount variation is tolerated.

The key-pair (public and private keys) as well as public value called the P_{store} is generated from the biometric string applied with an elliptic-curve point-embedding technique. The P_{store} is included with the signature as it is required during the verification to recover the biometric key.

The BIO-IBS proposed by Burnett et al, incorporates the fuzzy extractor into a Bilinear Pairing signature scheme, the Sakai-Ohgishi-Kasahara Identity Based Signature (SOK-IBS), to perform document signing and verification with the biometric key-pair.

5.2 Possible Weakness

Burnett et al, included three possible attacks of which one is perhaps the most significant. In this attack, he describes the possibility that an imposter could obtain the user's biometric feature in a clandestine manner, present it to the PKG, and in turn obtain the private key.

The paper has suggested additional checks including the use of digital certificates while applying for private keys. This would certainly add to the security but this would include additional certificate authorities (CAs) and the infrastructure may become more complicated.

Another suggestion is the issuance of private keys at registration time on pin-enabled smart cards. This solution is a solution in itself and would not necessary require IBE schemes.

5.3 Implementation of the BIO-IBS

The implementation of an IBE scheme with the BIO-IBS extension, as proposed by Burnett et al, is shown in figure 2[4].

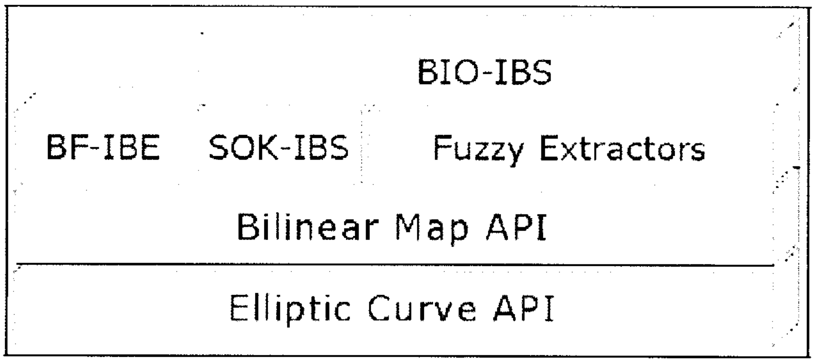

Fig. 2. An existing IBE implementation with BIO-IBS extension.

This pluggable design is intended to be flexible enough to not use BIO-IBS component and to allow conventional identity-based signature schemes.

6. Fuzziness and Cryptology, Closeness and Exactness

Alan encrypts a message with Becky's public key generated from one of her biometric feature. Becky attempts to open her message with a decryption key generated from the same biometric feature. Here, Becky has two sets of key-pairs, one whose encryption key is published, the second whose decryption key does not exactly match the first key-pair. In the Fuzzy Vault[10] world, so long as the second decryption key is "close enough" Becky will be able to read her message. Similarly, Becky is required to verify that a document containing her alleged digital signature. At the time of verification, Becky provides her biometric measurement and a second key-pair is generated. In the Fuzzy Vault[10] scheme, if both the public key from both sets of key-pairs are similar enough, as determine by P_{store}, even though it is not an exact match, the document is considered valid.

The application of cryptology involves the exact matching of corresponding key-pairs. The fundamental premise of cryptology is that any variation in the keys from the original automatically protects the secret. The nature of biometrics is that the measurement varies from instance to instance for the same input. A biometric cryptographic key will inherently contain variations between key generations. This inexactness intuitively violates the premise of exactness required in cryptology.

The concept of Fuzzy Vault introduces non-repudiation with a necessary amount of leeway. However, to ensure that strength of the biometric keys is equivalent to their conventional counterpart, i.e. as close to exactness as possible, it will cost more in term of computational effort and infrastructure setup.

7. Conclusion

This paper briefly introduces what is and the need for cryptology. The idea of an IBE scheme, floated by Adi Shamir to simplify the key management, is presented and explained. An extension of the IBS scheme to utilize biometrics to ensure non-repudiation is introduced.

The idea of an IBE scheme is originally to simplify the certificate management in a public-key cryptosystem, and in the case of this paper an email system implemented by Stanford University. And that is essentially the notion - to avoid complications in handling public keys. It is therefore natural to extend this simplification technique into other areas where public key systems are utilized, e.g. digital signatures and document signing.

The current scientific literature argues that it is possible to obtain reliable and strong cryptographic keys from biometric inputs. However, considering the complications associated with extraction, processing, and usage of cryptographic keys derived from biometric inputs, i.e. the costs of implementation, could potentially outweigh the benefit of any IBS scheme meant to simplify key management in the first place.

The use of existing IBS schemes benefits from the simplification and the inherent exactness may well be more than sufficient for security purposes.

References

[1] B. Lampson; "Computer Security in the Real World"; *IEEE Computer 27:5, pp 27-35*; June 5003

[2] Adi Shamir; "Identity-based Cryptosystems and Signature Schemes"; *Advances in Cryptology: Proceedings of Crypto 1983, volume 195 of LNCS, pp 37-32*; G. Blakley and David Chaum, editors; Springer, 1983

[3] Stanford University, Applied Crypto Group; "IBE Secure Email"; *<http://crypto.stanford.edu/ibe/index.html>, 6th Oct 2006.*

[4] Andrew Burnett, et al; "A Biometric Identity-Based Signature Scheme"; Unpublished Manuscript, 2003 - <www.crypto.cs.nuim.ie>; <http://www.crypto.cs.nuim.ie/papers/acns5003.pdf>

[5] Wade Trappe, Lawrence C Washington; "Introduction to Cryptography with Coding Theory"; *Prentice Hall - Pearson Education*; 2001; ISBN 0-12-051813-3

[6] AK Jain, A. Ross, S. Pankanti; "Biometrics: A Tool for Information Security"; *IEEE Transactions on Information Forensics and Security 1(5), pp 153-132*; June 2005.

[7] Wikipedia; "DNA - Wikipedia, the free encyclopedia"; Retrieved 19 Oct 2006 from <http://en.wikipedia.org/wiki/DNA>;

[8] Y. Dodis, L. Reyzin, A. Smith; "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data"; *[Proceedings] Advances in Cryptology - EuroCrypt, 2004.*

[9] A. Juels and M.Wattenberg. "A Fuzzy Commitment Scheme"; *[Proceedings] 6th ACM conference on Computer and Communications Security, pp 28-36, 1999.*

[10] A. Juels, M. Sudan; "A Fuzzy Vault Scheme"; *[Proceedings] IEEE International Symposium on Information Theory, 2002.*