Mitigating Vulnerabilities in 3-Factor Based Authentication

Yogita Borse
University of Mumbai
K J Somaiya College of Engineering
Mumbai

Irfan Siddavatam
University of Mumbai
K J Somaiya College of Engineering
Mumbai

ABSTRACT

Remote user authentication schemes are use to identify a user in the distributed environment. There are three different factors commonly use for authentication purpose named as password, smart card and biometric. It is been observed that authentication protocols designed till date are based on password. Normally, password is used as a first authentication factor, where as other two factors are included according to the level of security requirements. In this paper, analysis of 3-factor based protocols is done on the basis of wrong password input and stolen smart card vulnerabilities. Paper also suggest the improvements to control these vulnerabilities.

General Terms:

security, authentication protocol flaws.

Keywords:

password vulnerability, authentication, biometrics, smart cards, 3-factor authentication.

1. INTRODUCTION

Now a days every one is depending on the internet to fulfill their daily needs. Many organizations, institutions and government sectors are shifting from traditional storage (which includes confidential and sensitive data) and services to cloud computing. This growth and population is demanding higher level of security over the internet. In such environment remote user authentication plays a vital role.

In early days, authentication protocols were using only passwords to identifying the user [1, 2]. These protocols are very simple, fast and easy to use. But these are weak against many attacks including dictionary attacks. Also, it requires server side storage of user passwords and identity information, which is difficult to maintain. To overcome these weaknesses, smart card based protocols [3, 4, 5, 6] were designed where user credentials are stored on smart card instead of server. To add extra level of security, the third factor was added to this protocol called as biometric. The biometric feature of the person are unique and considered as useful to identify the user correctly. Based on this many 3-factor based protocol are proposed [7, 8, 9]

It is clear that the main purpose of including more authentication factors is to improve the security level. Since, password is very basic factor in the authentication it has been given very little attention. This fact leads to failure in achieving the said level of security. The purpose of this paper is to analyze such 3-factor based protocol design and point out the vulnerabilities which can be exploited by entering wrong password may be by intentionally or unintentionally. Improved scheme try to overcome such vulnerabilities.

Rest of the paper is organized as follows- section (2) is about the related work in which 3-factors based protocols brief review is given. Section (3) gives the in-site of Lin-Lai's scheme to understand their protocol design. Section (4) is about the cryptanalysis of the Lin-Lai's scheme. Here vulnerabilities in their scheme and possible attacks are explained. The proposed improved scheme is explained in Section (5). In Section (6) security of proposed scheme is given. Finally, Section (7) gives the overall conclusion of the paper.

2. RELATED WORK

In 2002, Lee-Ryu-Yoo [7] proposed a fingerprint based remote user authentication scheme using smart card. Their scheme is based on ElGamal's cryptosystem with two secrete keys and a smart card owner's fingerprint. In 2004, Lin-Lai [8] pointed out that Lee-Ryu-Yoo scheme is vulnerable to masquerade attack as well as it does not allow user to choose their password and/or fingerprint flexibly. So, Lin-Lai suggested a solution with the improved scheme to enhance the security. Lin-Lai's scheme is also uses ElGamal's cryptosystem, but with only one secrete key and user's fingerprint, without any verification tables. They proved that their scheme prevents the masquerading attack and allows the user to flexibly change their password as well as fingerprint. However, in 2007, Khan-Zhang [9] proved that Lin-Lai's scheme is vulnerable to server spoofing attack and suggested an improvement through a security patch. However, Khan-Zhang proposed security patch protects the protocol from server spoofing attack but still vulnerable to many attacks like DoS, Man-in-the-middle etc.

In 2010, Li-Hwang proposed an efficient biometric based remote user authentication scheme [3]. In this scheme, random number are used to avoid replay attack and hash value of users fingerprint is used to login and authenticate the user along with the secrete password. However,their scheme fails to provide strong login-authentication. Also, password change phase dose not verify the old password of the user before replace it with new one [10]. However, the proposed scheme of A. K. Das is vulnerable to stolen smart card attacks etc.

In the next section, review of Lin-Lai scheme is given. based on that the detail analysis of Lin-Lai scheme is done from the design point of view of the protocol.

Table 1. Notations used in Lin-Lai's scheme

Notation	Description
Ui	Client
IDi	User's identity
PWi	Ui User's password
Si	Ui User's finger print minutiae
Xs	a secrete maintained by the server
r	random number generated from the Ui's finger print
A$\oplus$B	XOR operation on A and B
A$\|\|$B	concatenation of A and B
T	current time stamp of the login device
DT	expected valid time interval for transmission delay

3. REVIEW OF LIN-LAI'S SCHEME

This section reviews Lin-Lai's a flexible biometrics remote user authentication scheme [8]. For describing the Lin-Lia's scheme [8], proposed scheme use the notations shown in Table 1. The security of Lin-Lai's scheme is based on the ElGamal's public key crypto system with one server secrete key (Xs), kept securely in the system. User's identity IDi comprises of user's name, phone number, date of birth etc. Password PWi is assumed as a securely selected password by the user at the time of registration, and his/her finger print minutiae template Si. $\oplus$ denotes XOR operation, which is reversible. Random number 'r' which is generated from the user's finger print taken during login. It is used to achieve freshness; it also helps to protect replay attacks. P is a large prime number selected by the server at the time of new user registration. They secure one-way hash function. A one-way hash function h(.) takes an arbitrary-length input and produces a fixed-length (say, n-bits) output, called the message digest. In Lin-Lai's scheme exponential operations used many times, which are known as time consuming mathematical operations. Lin-Lai's scheme comprises of following four phases, namely registration phase, login phase, authentication phase and change password phase. Details of each phase are given in the following sub-sections.

3.1 Registration phase

Every new user has to register at the registration center to login to the system. For registration, new user, Ui first selects his/her password PWi and IDi information. Then he/she provides his/her finger print Si on a specific device at the registration center. Then registration center performs following operations:
Computes PWi' = h(PWi$\oplus$Si) mod P and
Yi=(IDi^{Xs} mod P)$\oplus$PWi'.
Then, the registration center issues user Ui a smart card, with h, P, Yi, Si, IDi stored on the card.

3.2 Login phase

When a user Ui wants to login to the remote server, he/she needs to perform the following steps. Ui first inserts his/her smart card into the card reader and provides his/her finger print Si' on a specific device to verify the user's biometrics by checking whether Si' matches with the Si stored on the smart card. If this does not match, the remote user authentication terminates.
Otherwise, Ui inputs his/her password PWi and then the smart card does the following computations:
Generates a random number 'r' using the minutiae extracted from the Si' and computes
PWi" = h(PWi $\oplus$ Si') mod P
Yi' = Yi $\oplus$ PWi"
C1=(IDi)^{r} mod P
M= h(Yi' $\oplus$ T) mod P
C2=(Yi')^{r} M mod P.
Finally, sends a message C=(IDi,C1,C2,T) to the remote server.

3.3 Authentication phase

After transmission delay, the server receives the message C at T', where T' is the receiving time stamp of the server system. The server then performs the following operations. The server checks whether the format of IDi is correct. If the format is incorrect, the server rejects the login request. Otherwise, verifies whether (T'-T)$\geq$DT, if it holds, the server rejects the login request. If user ID is valid and transmission delay is acceptable, server computes and verifies whether C2 (C1^{Xs})$^{-1}$ mod P ?= h((IDi^{Xs} mod P)$\oplus$T) mod P, if it holds, the server accepts the login request. Otherwise, rejects the login request.

3.4 Change password

To freely change the password PWi of a user Ui to a new password PWi*, the user Ui does the following steps. Ui first inserts his/her smart card into the card reader and provides his/her finger print Si' on a specific device to verify the user's biometrics by checking whether Si' matches with the Si on the smart card. If this verification passes, the user Ui inputs his/her old password PWi' and the new password PWi*. After receiving this, the client device performs following computations:
PWi" = h(PWi' $\oplus$ Si') mod P
Yi'= Yi$\oplus$PWi" =IDi^{Xs} mod P and then computes new
Yi*= Yi'$\oplus$h(PWi*$\oplus$Si'). Finally, replaces the old Yi with the new Yi* on the smart card.

4. VULNERABILITIES IN LIN-LAI'S SCHEME

This section show the flaws in the Lin-Lai's scheme [8].

4.1 Vulnerabilities in login and authentication phases

It is seen from login phase of the Lin-Lai's scheme that the user Ui first enters his/her finger print on a specific device to verify whether his/her biometric passes. If this verification passes, then Ui enters his/her password PWi. But, client device does not verify the user's password in the login phase. Thus, even if user Ui enters his/her password incorrectly by mistake, both the login and authentication phases still continue, and finally, at the end of authentication phase, server rejects Ui's login request. This results in causing unnecessarily extra communication and computational overheads during login and authentication phases. From security point of view, any user Ui keeps different passwords for different purposes. Assume that the user Ui enters his/her password wrongly and let the entered password be PWi'($\neq$ PWi). Then from login phase, following is noted
The client device generates a random number 'r' using the minutiae extracted from the Ui's fingerprint and computes followings

PWi" =h(PWi' $\oplus$ Si) mod p
$\neq$ h(PWi $\oplus$ Si) mod p

Yi’ = Yi $\oplus$ PWi”
= h((IDi)^{Xs} mod p) $\oplus$ h(PWi $\oplus$ Si) mod p $\oplus$ h(PWi’ $\oplus$ Si) mod p
$\neq$ h(IDi)^{Xs} mod p

C1 = (IDi)^{r} mod p

M = h(Yi’ $\oplus$ T) mod p

C2 =(Yi’)^{r}M mod p

C =(IDi,C1,C2,T)
After sending C to the remote server, server computes

C2(C1^{Xs})$^{-1}$ mod p
$\neq$ h((IDi)^{Xs} mod p) $\oplus$ T) mod p

As a result, on receiving user’s message C when server compares, there will be a mismatch. Thus, server will reject user’s login request message. Here the user is totally unaware of the fact that he/she has entered his/her password incorrectly in login phase. Thus, note that if the user password verification takes place at the very beginning of th login phase, this situation will never occur and will not result in unnecessarily extra communication and computational overheads during both login and authentication phases.

4.2 Vulnerable Smart card data

In Lin-Lai’s scheme, Ui’s smart card stores fingerprint data Si in plain form. Here, assume that the attacker has got the Ui’s smart card. Then from Ui’s smart card attacker can easily extract Si ([11, 12]) and use it for login purpose.

Based on the above vulnerabilities (4.1) and (4.2), Denial of service attack on the server is also possible. It is explained as follows.

4.2.1 Denial of service attack. The above scenario results in more serious problem, when attacker uses this vulnerability to launch Denial of service(DoS) attack. In DoS attack, attacker simply wants to overload the server so that it can not provide the services to the legal users. In the extreme case, server may crash. Here, assume that the attacker has got the Ui’s smart card and successful in extracting the data from it. In Lin-Lai’s scheme, as seen from the login phase, user requires only Si for verification. Since, attacker has got Si, he/she can easily pass the login phase. Then even if attacker enters wrong password, the client device does not verify the user’s password and both the login phase and authentication phase are still continued as shown above. So, attacker can send such multiple login-authentication requests to the server to keep the server busy in authenticating the false user and this cause the legal users to wait.

4.3 Vulnerabilities in change password phase

In the Lin-Lai’s biometric-based remote user authentication scheme, any user Ui can freely change his/her old password by the new password without contacting the registration center. In their scheme, only after the successful verification of biometrics of user, Ui is allowed to enter his/ her old password PWi and the new password PWi*. Since there is no verification of old password in their scheme, the updation of new password will take place incorrectly if the user Ui enters his/her old password PWi wrongly by mistake. Now, due to this problem, when the user logins later in the system providing his/her biometrics as well as new password, the login request of the user is rejected by the server even if the user enters new password correctly at that time.

In order to update the new password, the Lin-Lia’s scheme does the following steps after successful verification of user’s biometrics. Assume that the user Ui enters his/ her old password PWi’ incorrectly so that PWi’ $\neq$ PWi. Then,

PWi”= h(PWi’ $\oplus$ Si) mod p
$\neq$ h(PWi $\oplus$ Si) mod p

Yi’ = Yi $\oplus$ PWi”
= h(IDi)^{Xs} mod p $\oplus$ h(PWi $\oplus$ Si) mod p
$\oplus$ h(PWi’ $\oplus$ Si) mod p
$\neq$ h(IDi)^{Xs} mod p (since PWi’ is incorrect password)

As a result,
Yi*=Yi’ $\oplus$ h(PWi* $\oplus$ Si)
$\neq$ h(IDi)^{Xs} mod p $\oplus$ h(PWi* $\oplus$ Si)

The smart card will replace Yi with Yi* into its memory. Hence, in such scenario the new password of the user is not correctly updated in the smart card. As a consequence, when the same user will login later in the system, user’s biometrics verification will be successful. But, the login request request will be always rejected by the server even if the user enters the correct new password in that time. This effect will continue in subsequent password change phases by that user. To overcome such serious problem, the user will not have other options except to issue another new smart card providing the necessary information such as his/ her fresh identity, biometrics and password securely to the registration center.

4.4 Outsider attack

In the outsider attack, the attacker can use the password change phase to make the Ui’s smart card un-usable. This can be done as follows. Assume that, the attacker has got the Ui’s smart card and successful in extracting the finger print data Si from it. Since, Si is in plain form, attacker can use it to pass the login phase(as it required only Si). After this attacker can enter any thing as a Ui’s password. Since, the client device does not verifies the Ui’s password, it asks the attacker to enter the new password. This ends with update in smart card data. Now, even if legal user Ui get back his/her smart card, he/she will fail to authenticate because of changed password. So, the card will be useless for him/her.

4.5 Server spoofing attack

In the server spoofing attack, an adversary can use the sensitive data of legitimate users by setting up fake servers. Therefore, in many applications, such as e-commerce or e-banking, mutual authentication is required; Where, server as well as client authenticates each other before starting secure communication.
LinLai’s scheme performs one directional authentication i.e. only client authentication and there is no authenticity of the remote server. Their scheme has risk of manipulating user’s data by setting up fake server by an adversary. Since, client has no way to authenticate the server, it cannot make trust on the originality of the remote server. Hence, their scheme is susceptible to the server spoofing attack.

4.6 Man-in-the-Middle attack

In Man-in-the-Middle attack, the attacker successfully sits in between the user and remote server, whereupon all the messages between the user and the remote server goes through the attacker. In this situation attacker can block the messages, or can modify the messages according to his convenience. The main reason behind the possibility of Man-in-the-Middle attack is insecure session. During authentication process, protocol is suppose to generate a session key so that the user and the remote server can perform the secure communication using session key. Here, Lin-Lai's scheme fails to generate a session key because of which it is vulnerable to Man-in-the-Middle attack.

5. IMPROVED 3-FACTORS BASED REMOTE USER AUTHENTICATION SCHEME

This section include an improvement of the Lin-Lai's a flexible biometrics remote user authentication scheme using smart cards in order to withstand the vulnerabilities discussed in Section 4. Proposed scheme use the same notations as used in the Lin-Lai's scheme shown in Table 1. Basically, Lin-Lai's scheme fails to support following features.

- Mutual Authentication
- Session key generation
- Effective use of all authentication factors
- Proper way to change authentication factor

In order to overcome serious problem that arises because of lack of above features in Lin-Lai's scheme, following improvements are suggested. Improved scheme consists of the following phases.

5.1 Registration Phase

Before login to the system, a remote user Ui needs to register using following steps.

Step 1: The user inputs his/her finger print Si on a specific device and offers his/her password PWi and the identity IDi of the user to the registration center in person.

Step 2: The registration center then computes the followings

Ki = [h(PWi $\oplus$ IDi)] mod p $\oplus$ h(Si)
Yi = h(IDi^{Xs} mod p) $\oplus$ h(PWi $\oplus$ IDi)
(Note : While doing XOR operation on PWi and IDi, size of PWi and IDi can be made equal by taking it's hash value or by using padding.)

Step 3: Finally, registration center stores h(.), p, Yi, Ki, h(Si) on the smart card and issues it to the user Ui.
Note that Ki is an extra parameter used, which is not there in Lin-Lai's scheme.

5.2 Login Phase

In this phase, if a registered user Ui wants to login to the server, he/she needs to perform the following steps.

Step 1: Ui first inserts his/her smart card into the smart card reader of a terminal and offers his/her finger print Si' on the specific device to verify his/her biometric.

Step 2: Then this h(Si') is matched against the h(Si) stored on the Ui's smart card.

Step 3: If the above verification does not hold, then Ui does not pass the biometric verification and as a result, the remote user authentication terminates. Otherwise, if the above mentioned verification holds, Ui passes the biometric verification and Ui then inputs his/her identity IDi password PWi' to perform the next step.

Step 4: The smart card verifies [h(PWi' $\oplus$ IDi)] mod p ?= Ki$\oplus$h(Si), if this verification does not hold then password verification fails, and the client terminates the session. Otherwise, Ui passes the login phase. Then, smart card computes following authentication parameters:
Generates a random number 'r' using the minutiae extracted from the Si' and computes
PWi" = h(PWi' $\oplus$ IDi)
Yi' = Yi $\oplus$ PWi"
C1=(IDi)^r mod P
M= h(Yi' $\oplus$Tc) mod P, where Tc is client's current system time stamp
C2=(Yi')^r M mod P.

Step 5: Finally, client sends message C=(IDi,C1,C2,Tc) to the remote server.

Note that, in this phase Ui's finger print as well as password is getting verified before next phase.

5.3 Authentication Phase

After transmission delay, the server receives the message C at T', where T' is the receiving time stamp of the server system. The server then performs the following operations:

Step 1: The server checks whether the format of IDi is correct or not. If the format is incorrect, the server rejects the login request. Otherwise, verifies whether (T'-Tc)$\geq$DT, if it holds, the server rejects the login request.

Step 2: If user identity is valid and transmission delay is acceptable, server computes and verifies whether
C2 (C1^{Xs})$^{-1}$ mod P ?= h(h(IDi^{Xs} mod P)$\oplus$Tc) mod P, if it holds true, the server accepts the login request. Otherwise, rejects the login request.

Step 3: On successful client authentication, server computes mutual authentication message for the client as following
C3=[h(IDi^{Xs} mod P)$\oplus$Ts)] mod P, where Ts is server's current system time stamp and sends R=(C3,Ts) to the client

Step 4: On the client side, after transmission delay, the client receives the message R at T", where T" is the receiving time-stamp of the client system. The client then verifies whether (T"-Ts)$\geq$DT, if it holds, the client terminates the session.

Step 5: Otherwise, verifies whether C3 ?= [Yi'$\oplus$Ts] mod P. if this verification dose not hold, client rejects mutual authentication request and terminates the session.

Step 6: Otherwise, both client and server generates session key as follows:
SK=h(IDi^{Xs} mod P)$\oplus$Tc$\oplus$Ts

Note that, SK is a session key which both client and server generates after the successful mutual authentication.

5.4 Change Password Phase

Whenever, a registered user Ui decides to change his/her old password, he/she needs to first pass the login phase, then the system asks for the new password and updates the smart card accordingly. The required steps are as shown below.

Step 1: Ui first inserts his/her smart card into the smart card reader of a terminal and offers his/her finger print Si' on the specific device to verify his/her biometric.

Step 2: Then this h(Si') is matched against the h(Si) stored on the Ui's smart card.

Step 3: If the above verification does not hold, then Ui does not pass the biometric verification and as a result, the change password terminates. Otherwise, if the above mentioned verification holds then Ui inputs his/her identity IDi' and password PWi' to perform the next step.

Step 4: The smart card verifies the correctness of the old password PWi' using [h(PWi' $\oplus$ IDi')] mod p ?= Ki$\oplus$h(Si), if this verification does not hold then password verification fails, and the client terminates the session. Otherwise, Ui passes the login phase.

Step 5: Then, client system asks user Ui to enter new password, let's say it is PWi*. Then it compute new Ki* and new Yi* as follows. PWi"=h(PWi* $\oplus$ IDi') Ki* = PWi" mod p $\oplus$ h(Si)

$Yi' = Yi \oplus h(PWi' \oplus IDi')$ $Yi^* = Yi' \oplus PWi''$
Finally, it replace Yi by Yi* and Ki by Ki* on the smart card.

6. SECURITY ANALYSIS OF THE IMPROVED SCHEME

This section presents the security analysis of proposed scheme. The security analysis of proposed scheme is based on the vulnerabilities mentioned in section 4

1. Since proposed scheme is based on ElGamal's cryptosystem as Lin-Lai's scheme, the complexity of computing Xs from Yi is a discrete logarithm problem. It is also difficult for the intruder to obtain the Ui's password PWi and fingerprint Si from the user Ui's smart card data, because it is masked with one-way hash function.
2. The main reason behind the vulnerability in login and authentication phases in Lin-Lai's scheme is lack of user Ui's password verification in login phase before contacting to the server. In improved login phase of proposed scheme, user Ui's proceeds to authentication phase only after successful verification of finger print Si as well as password PWi.
3. Denial of Service attack - The reason behind this attack on Lin-Lai's scheme is login based on verification of Si, which is available on the user Ui's smart card in plain form. In proposed scheme, stored secret information on the smart card is as secure as the password. Assume that a legal user Ui lost his/her smart card. Now, for any attacker it is impossible to extract Si or PWi from the Ui's smart card data. However, for successful login, attacker should know the PWi as well as Si, which is a computationally infeasible problem due to the property of one-way hash function. Therefore proposed scheme protected from Denial of Service attack
4. Outsider attack - For any attacker, it is difficult to derive or change the password because the attacker has to pass the biometric verification. However, the attacker is unable to pass the biometric verification due to the properties of the biometrics and hash function. Since, there will be a mismatch between the attacker's biometric template and the biometric template stored in the smart card of the original user.

   Also, in proposed scheme for changing the password the attacker has to enter the correct old password. Thus, the attacker has to guess the old password before updating the new password chosen by him/her. This avoids the outsider attackand vulnerability in change password phaseof Lin-Lai's scheme.
5. Server spoofing attack - One attack may be that an illegal user can intercept the message (IDi, C1, C2, Tc) from Ui or any message from the previous sessions between Ui and server and try to masquerade as the remote server. It is impossible for the illegal user to compute C3 in order to convince Ui unless he/she knows the secret information Xs.
6. Man-in-the-Middle attack - As mentioned in vulnerability, this happens because of insecure sessions. In proposed scheme, at the end of authentication phase client and server generates a session key SK which helps in protecting the system from Man-in-the-Middle attack.

7. CONCLUSION

On analyzing Lin-Lai's scheme, it is observed that their scheme fails to provide mutual authentication, session key generation, effective use of all authentication factors, and proper way to change password. Therefore, their protocol is vulnerable to attacks like denial of service, man-in-the-middle, server spoofing and outsider attacks. To overcome these vulnerabilities, this paper proposes an improvement of the Lin-Lai's scheme. This scheme provides features like mutual authentication, session key generation, flexible change of password, low computation and communication costs and less burden on server. Unlike Lin-Lai's scheme, proposed scheme provides strong authentication and non-repudiation with the help of biometrics and password verification.

8. REFERENCES

[1] Leslie Lamport. Password authentication with insecure communication. *Commun. ACM*, 24(11):770–772, November 1981.

[2] Seung Wook Jung and Souhwan Jung. Secure password authentication for distributed computing. In *Computational Intelligence and Security, 2006 International Conference on*, volume 2, pages 1345–1350, 2006.

[3] Chun-Ta Li and Min-Shiang Hwang. An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.*, 33(1):1–5, January 2010.

[4] Narn-Yih Lee and Yu-Chung Chiu. Improved remote authentication scheme with smart card. *Computer Standards & Interfaces*, 27(2):177–180, 2005.

[5] Jing Xu, Wen-Tao Zhu, and Deng-Guo Feng. An improved smart card based password authentication scheme with provable security. *Comput. Stand. Interfaces*, 31(4):723–728, June 2009.

[6] Ronggong Song. Advanced smart card based password authentication protocol. *Comput. Stand. Interfaces*, 32(5-6):321–325, October 2010.

[7] J.K. Lee, S. R. Ryu, and K.Y. Yoo. Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters*, 38(12):554–555, 2002.

[8] Chu-Hsing Lin and Yi-Yi Lai. A flexible biometrics remote user authentication scheme. *Computer Standards & Interfaces*, 27(1):19–23, 2004.

[9] Muhammad Khurram Khan and Jiashu Zhang. Improving the security of 'a flexible biometrics remote user authentication scheme'. *Computer Standards and Interfaces*, pages 82–85, 2007.

[10] A.K. Das. Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *Information Security, IET*, 5(3):145–151, 2011.

[11] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 388–397, London, UK, UK, 1999. Springer-Verlag.

[12] Thomas S. Messerges, Ezzat A. Dabbish, and Robert H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.*, 51(5):541–552, May 2002.