International Journal of Internet, Broadcasting and Communication Vol.9 No.3 35-43 (2017)
https://doi.org/10.7236/IJIBC.2017.9.3.35

IJIBC 17-3-5

An Improved Smart Card-based User Authentication Scheme with Session Key Agreement for Telecare Medicine Information System

Hyungkyu Yang

Computer Media Information Engineering, Kangnam University,
111, Gugal-dong, Giheung-gu, Yongin-si, Gyounggi-do, 446-702, Korea
hkyang@kangnam.ac.kr

Abstract

In 2013, Lee-Lie proposed secure smart card based authentication scheme of Zhu's authentication for TMIS which is secure against the various attacks and efficient password change. In this paper, we discuss the security of Lee-Lie's smart card-based authentication scheme, and we have shown that Lee-Lie's authentication scheme is still insecure against the various attacks. Also, we proposed the improved scheme to overcome these security problems of Lee-Lie's authentication scheme, even if the secret information stored in the smart card is revealed. As a result, we can see that the improved smart card based user authentication scheme for TMIS is secure against the insider attack, the password guessing attack, the user impersonation attack, the server masquerading attack, the session key generation attack and provides mutual authentication between the user and the telecare system.

Keywords: *Authentication, Smart Card, Session Key Agreement, Telecare Medicine Information System*

1. Introduction

With rapid development of the Internet technology, user authentication scheme for telecare medicine information system (TMIS) has been becoming one of important security issues. Telecare medicine information system (TMIS) provides certain healthcare services, which become a feasible solution to the continuously rising demand in medical and healthcare sector. Since Lamport [1], in 1987, first proposed a remote password authentication protocol with the insecure communication, many researchers have proposed smart card-based authentication protocols [2-12] to improve security issues.

In 2012, Zhu [7] proposed an effective authentication scheme for telecare medicine information system which can withstand the security drawbacks of Wei et al.'s scheme [6]. They claimed that their scheme resists insider attack, password guessing attack, impersonation attack, replay attack etc. But Lee-Liu [8], in 2013, pointed out that Zhu's scheme fails to resist parallel session attack. Also, Lee-Liu showed that Zhu's authentication scheme cannot execute correctly. Then, Lee-Liu proposed secure smart card based authentication scheme for TMIS to remove the security drawbacks of Zhu's scheme. And they claimed that their scheme resists parallel session attack, password guessing attack, session key generation attack etc. and provides user's anonymity.

Manuscript Received: June. 15, 2017 / Revised: June. 28, 2017 / Accepted: July. 10, 2017
*Corresponding Author: *hkyang@kangnam.ac.kr*
Tel:+82-31-280-3760
Computer Media Information Engineering, Kangnam University. Korea

In this paper, we briefly discuss the security of Lee-Liu's smart card-based authentication scheme for TMIS [8] and we have shown that Lee-Liu's authentication scheme is still vulnerable to several attacks. Also, we propose the improved scheme to remove these security drawbacks of Lee-Liu's smart card-based authentication scheme, even if the secret information stored in the smart card (such as mobile device) is revealed to an attacker. To analyze Lee-Liu's smart card-based authentication scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [13-14] and intercept messages communicating between the user and the telecare system. Also, we assume that an attacker may possess the following capabilities to thwart the security schemes.

•An attacker has total control over the communication channel between the user and the server in the login and authentication phase. That is, the attacker may intercept, insert, delete, or modify any message across the communication procedures.

•An attacker may (i) either steal a user's smart card and then extract the secret values stored in the smart card, (ii) or steal a user's password, but cannot commit both of (i) and (ii) at a time.

Obviously, if both of the user's smart card and password was stolen at the same time, then there is no way to prevent an attacker from impersonating as the user. Therefore, a remote user authentication scheme should be secure if only one case out of (i) and (ii) is happening.

This paper is organized as follows. In section 2, we briefly review Lee-Liu's authentication scheme. In section 3, we describe the security analysis of Lee-Liu's authentication scheme. An improved smart card-based authentication scheme for TMIS is presented in section 4, and its security analysis is given in section 5. Finally, conclusions are presented in section 6.

2. Reviews of Lee-Liu' Scheme

In 2013, Lee-Liu [8] proposed a secure smartcard-based authentication scheme for telecare medicine information systems (TMIS). This scheme is composed of four phases: initial phase, registration phase, login phase, and authentication phase. The notations used in this paper are as follows.

Table 1. Notations Used in This Paper

Notation	Description
U_i	User/Patient
S	Telecare system (TMIS)
ID_i	Unique identity of U_i
PW_i	Unique password of U_i
x	Master key of S
(e, d)	System public/private key pair
h()	A secure hash function
a ‖ b	Concatenates of a and b
a⊕b	XOR operation of a and b

2.1 Initial Phase

The telecare system S performs the following steps before performing the registration phase.

I1. S generates two large number p and q, and computes n=p*q.
I2. S chooses the system public/private key pair (e, d).

2.2 Registration Phase

Before logging in the telecare system S, a user U_i initially has to register to the telecare system S as the following steps.

R1. U_i generates a random number N_i, and chooses his identity ID_i and password PW_i.

R2. U_i computes $pw_i^*=h(PW_i // N_i)$, and then sends the registration request information ID_i, pw_i^* to S via a secure channel.

R3. Upon receiving the registration request information, S computes $B_i=h(ID_i \oplus d) \oplus pw_i^*$. Then, S stores $\{n, e, ID_i, B_i\}$ into the smart card, and issues the smart card to U_i via a secure channel.

R4. After receiving the smart card, U_i inserts N_i and a serial number $SN_i=0$ into it.

2.3 Login Phase

When a user U_i wants to login the telecare system, U_i has to perform the following steps.

L1. U_i first inserts his smart card into a card reader and then inputs his password PW_i.

L2. U_i generates a random number w_i, and computes $pw_i^*=h(PW_i \| N_i)$, $SN_i=SN_{i+1}$, $B_i^*=B_i \oplus pw_i^*$, $h_i=h(B_i^* \| w_i \| SN_i)$, and $X_i=(ID_i \| h_i \| w_i \| SN_i)^e \bmod n$.

L3. Finally, U_i sends the login message $M_1=\{X_i\}$ to the telecare system S.

2.4 Authentication Phase

Upon receiving the login message M_1, the telecare system S has to perform the following steps to authenticate each other.

A1. S computes $(X_i)^d \bmod n=(ID_i^* \| h_i^* \| w_i^* \| SN_i^*)$, and then checks the validity of ID_i^*, SN_i^* and $h_i^*=?h(h(ID_i^* \oplus d) \| w_i^* \| SN_i^*)$. If verification holds, U_i is authenticated by S.

A2. S generates a random number w_s, and computes $h_2=h(ID_i^* \| w_i^* \| w_s \| SN_i^*)$, and then sends the mutual authentication message $M_2=\{h_2, w_s \oplus w_i^*\}$ to U_i. Beside, S updates SN_i for U_i and keeps it until this session completed.

A3. Upon receiving the message M_2, U_i computes $w_s^*=(w_s \oplus w_i^*) \oplus w_i$, and checks $h_2=?h(ID_i \| w_i \| w_s^* \| SN_i)$. If verification holds, S is authenticated by U.

A4. For session key agreement, U computes a session key $SK=h(ID_i \| w_s^* \| w_i \| SN_i)$, $h_3=h(SK)$, and then sends $M_3=\{h_3\}$ to S.

A5. Upon receiving the message M_3, S computes $SK^*=h(ID_i^* \| w_s \| w_i^* \| SN_i^*)$, and checks $h_3=?h(SK^*)$. If verification holds, S and U_i have a common session key $SK(=SK^*)$ for later secure communication.

3. Attacks against of Lee-Liu' Scheme

In this section, we will analyze Lee-Liu's smart card-based authentication scheme for telecare medicine information system (TMIS). To analyze the security weaknesses, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [13-14] and intercept messages communicating between the user and the telecare system. Under this assumption, we will show that Lee-Liu's scheme is vulnerable to the various attacks, such as the insider attack, the off-line password guessing attack, the user impersonation attack, the session key generation attack etc. and cannot provide mutual authentication between the user and the telecare system.

3.1 Insider Attack

A malicious insider in the telecare system may try to get user's secret information, such as the user's password. In the registration phase, since the user's password information pw_i^* is revealed to an insider in the

telecare system, the insider as an attacker can perform the off-line password guessing attack and the user impersonation attack etc. with user's secret information.

3.2 Off-Line Password Guessing Attack

If an attacker is a malicious insider in the telecare system, and can extract the secret value (N_i) illegally from the legal user's smart card by some means [13-14], the attacker can easily find out PW_i by performing the off-line password guessing attack, in which each guess PW_i^* for PW_i can be verified by the following steps.

PA1. The attacker computes secret parameter $h(PW_i^* \,//\, N_i)$ with the secret value (N_i) extracted.
PA2. The attacker verifies the correctness of PW_i^* by checking $pw_i^* =? h(PW_i^* \,//\, N_i)$.
PA3. The attacker repeats the above steps until a correct password PW_i^* is found.

3.3 User Impersonation Attack

With the security information pw_i^* as described in subsection 3.1 and the secret values (B_i, N_i, SN_i) extracted from smart card, the attacker can perform the user impersonation attack as the following steps.

UA1. The attacker computes the following equations.

$B_i^* = B_i \oplus pw_i^*$
$h_i^* = h(B_i^* \,//\, r_i \,//\, SN_i)$
$X_i^* = (ID_i \,//\, h_i^* \,//\, r_i \,//\, SN_i)^e \bmod n$

where r_i is a random number chosen by the attacker.
UA2. Then, the attacker sends the forged login message $M1=\{X_i^*\}$ to S.
UA3. Upon receiving the forged login message, S computes $(X_i^*)^d \bmod n = (ID_i \,//\, h_i^* \,//\, r_i \,//\, SN_i)$, and then checks ID_i, SN_i, and $h_i^* =? h(h(ID_i \oplus d) \,//\, r_i \,//\, SN_i)$. If verification holds, the attacker as the legitimate user is authenticated by S.

3.4 Session Key Generation Attack

If the attacker can receive the mutual authentication message $M_2(=\{h_2, w_s \oplus r_i\})$ from the telecare system after performing the user impersonation attack as described in subsection 3.3, the attacker and the telecare system can generate a common session key $SK(=SK^*)$ each other as the following steps.

SKG1. The attacker computes the following equations.

$w_s^* = (w_s \oplus r_i) \oplus r_i$
$SK = h(ID_i \,||\, w_s^* \,||\, r_i \,||\, SN_i)$

where r_i is an random number chosen by the attacker in the user impersonation attack phase and the secret values (ID_i, SNi) extracted from smart card.
SKG 2. Then, the attacker sends the session key message $h_3=h(SK)$ to the telecare system.
SKG 3. Upon receiving the session key message, the telecare system computes a common session key $SK^* = h(ID_i^* \,||\, w_s \,||\, r_i \,||\, SN_i^*)$, and checks $h_3 =? h(SK^*)$. If verification holds, S and the attacker have a common session key SK(=SK') each other between the attacker and the telecare system.

3.5 Mutual Authentication

Generally, if a user authentication scheme is insecure against the user impersonation attack as described in

subsection 3.3, the user authentication scheme cannot provide mutual authentication between the user and the telecare system for secure communication. Therefore, Lee-Liu's smart card-based user authentication scheme for TMIS fails to provide mutual authentication.

4. The Improved Scheme

In this section, we propose an improved smart card-based user authentication scheme for telecare medicine information system (TMIS) that improved Lee-Liu's scheme which cannot withstand the various attacks. The improved scheme is divided into four phases: initial phase, registration phase, login phase and authentication phase.

4.1 Initial Phase

In order to initialize the improved smart card-based user authentication scheme for TMIS, the telecare system S performs the following steps.

I1. A user U_i selects large prime number p and q, and computes $n=p \cdot q$.
I2. U_i chooses a prime e, and then computes an integer d, such that $e \cdot d \bmod (p-1)(q-1)=1$, where e is the user's public key, and d is the user's private key.

4.2 Registration Phase

Before logging in the telecare medicine information system S, a user U_i initially has to register to the telecare system as the following steps. The registration phase is illustrated in figure 1.

R1. U_i selects his identity ID_i and password PW_i.
R2. U_i computes $h(PW_i \oplus d)$ and then submits the registration request information with ID_i, $h(PW_i \oplus d)$ to S via secure channel.
R3. Upon receiving the registration request information, S computes the following equations.

$A_i=(h(PW_i \oplus d))^e$

$B_i=(A_i \oplus h(ID_i \oplus x))^e$

R4. S stores these personalized security parameters $\{ID_i, A_i, B_i, h()\}$ in the user's smart card, and issues the smart card to U via secure channel.

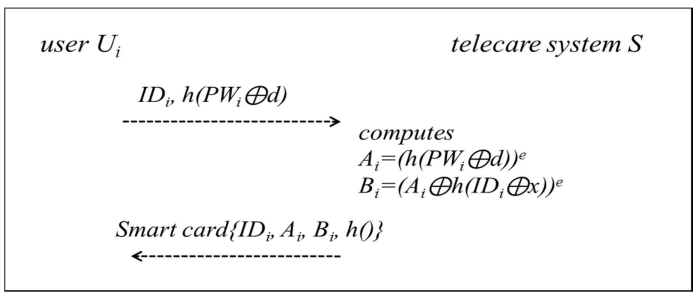

Figure1. Registration Phase of the Improved Authentication Scheme

4.3 Login Phase

When the user U_i wants to login the telecare system, U_i has to perform the following steps. The registration and authentication phase is illustrated in figure 2.

L1. U_i first inserts his smart card into a card reader and then inputs his password PW_i.

L2. Smart card computes $h(PW_i \oplus d)$ and then verifies whether the computed value equals A_i^d or not. If the verification holds, the smart card (or mobile device) computes the following equations. Otherwise, it terminates the registration phase.

$C_i=B_i^d \oplus A_i$
$D_i=h(C_i) \oplus N_U$
$M_U=h(ID_i \,//\, C_i \,//\, N_U \,//\, T_U)$

where N_U is a random number generated by U_i and T_U is a current timestamp of the smart card.

L3. Finally, U_i sends the login message $\{ID_i, D_i, M_U, T_U\}$ to the telecare system S.

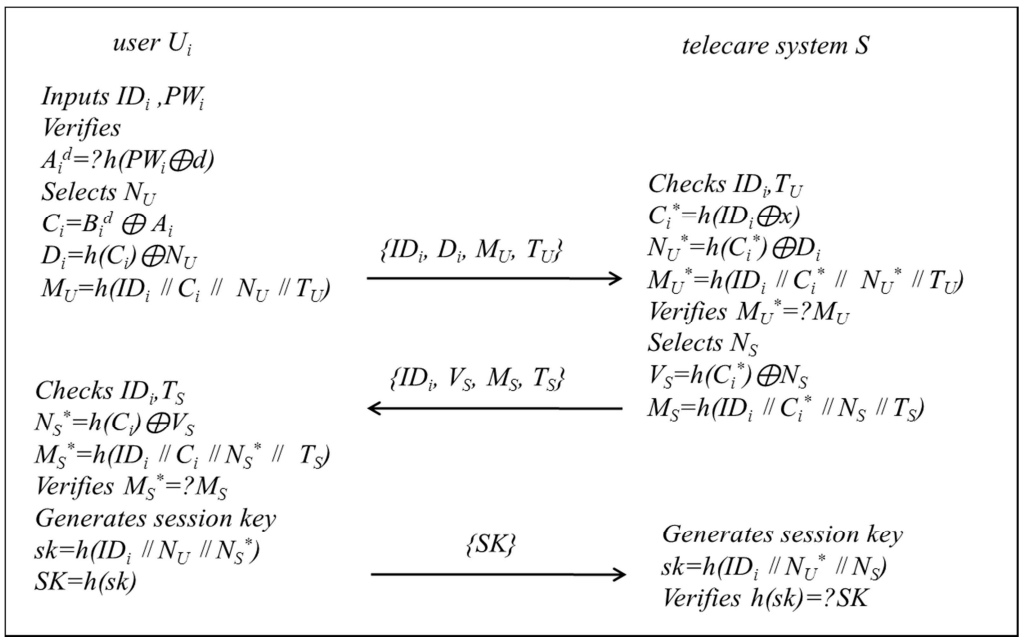

Figure 2. Login Phase and Authentication Phase of the Improved Authentication Scheme

4.4 Authentication Phase

After receiving the login message, the telecare system S has to perform the following steps.

A1. S verifies the freshness of timestamp, $T_U' - T_U \le \Delta T$, where ΔT is the valid time delay. If the condition holds, the telecare system S computes $C_i^*=h(ID_i \oplus x)$, $N_U^*=h(C_i^*) \oplus D_i$, and then verifies whether M_U equals $h(ID_i \,//\, C_i^* \,//\, N_U^* \,//\, T_U)$ or not. If verification holds, U_i is authenticated by S.

A2. S computes the following equations.

$V_S= h(C_i^*) \oplus N_S$
$M_S=h(ID_i \,//\, C_i^* \,//\, N_S \,//\, T_S)$

where N_S is a random number generated by S and T_S is a current timestamp of the telecare system. Then, S sends the mutual authentication message $\{ID_i, V_S, M_S, T_S\}$ to U.

A3. Upon receiving the mutual authentication message, U_i verifies the freshness of timestamp, $T_S' - T_S \le \Delta T$, where ΔT is the valid time delay. If the condition holds, U_i computes $N_S^* =h(C_i) \oplus V_S$, and then verifies whether M_S equals $h(ID_i \,//\, C_i \,//\, N_S^* \,//\, T_S)$ or not. If verification holds, S is authenticated by U_i.

A4. For session key agreement between the user and the telecare system, U_i computes a session key

$sk=h(ID_i \| N_U \| N_S^*)$, $SK=h(sk)$, and then sends SK to S.

A5. Upon receiving the message SK, S computes $sk=h(ID_i \| N_U^* \| N_S)$, and checks SK=?h(sk). If verification holds, S and U_i have a common session key sk for later secrecy communication.

5. Security Analysis of the Improved Scheme

In this section, we analyze the improved smart card-based user authentication scheme for telecare medicine information system (TMIS) proposed. To analyze the scheme, we assume that an attacker as the insider could obtain the secret values stored in the smart card by monitoring the power consumption [13-14] and intercept messages communicating between the user and the telecare medicine information system. Under this assumption, we will show that the improved scheme is not vulnerable to the various attacks, such as the insider attack, the off-line password guessing attack, the user impersonation attack, the server masquerading attack, the session key generation attack etc. and provide mutual authentication between the user and the telecare system.

5.1 Insider Attack

In the registration phase, if user's password information is revealed to the malicious insider as an attacker, the malicious insider has no way to get the related secret information without knowing the secret decryption key d kept by the user. Because a user submits $h(PW_i \oplus d)$ instead of PW_i.

5.2 Off-Line Password Guessing Attack

After the attacker as malicious insider in the telecare system extract the secret values (A_i, B_i) illegally from the legal user's smart card by some means, the attacker attempts to derive the user's password PW_i using $A_i=(h(PW_i \oplus d))^e$ in the registration phase. However, the attacker cannot guess the user's password PW_i using the secret values extracted from the legitimate user's smart card, because the attacker cannot compute the secret values without knowing the secret decryption key d kept by the user.

5.3 User Impersonation Attack

To impersonate as the legitimate user, an attacker attempts to make a forged login message which can be authenticated to the server. However, the attacker cannot impersonate as the legitimate user by forging the login massage even if the attacker can extract the secret values (A_i, B_i) stored in the legal user's smart card, because the attacker cannot compute the login message (D_i, M_U) sending to the telecare system without knowing the secret value x kept by the telecare system and the secret encryption key d kept by the user. Therefore, the attacker has no chance to login to the improved authentication scheme by launching the user impersonation attack.

5.4 Server Masquerading Attack

To masquerade as the legitimate telecare system, an attacker attempts to make the forged mutual authentication message when receiving the user's login request message. However, the attacker cannot masquerade as the telecare system by forging the mutual authentication massage, because the attacker cannot compute (V_S, M_S) without knowing the secret value x kept by the telecare system. Hence, the attacker cannot masquerade as the legitimate telecare system to the user by launching the server masquerading attack.

5.5 Mutual Authentication

As described in subsection 5.3 and 5.4, we can say that the improved scheme provides mutual authentication between the user and the telecare system because the improved scheme can withstand to the user impersonation attack and the server masquerading attack. Namely, even if an attacker can extract the secret values (A_i, B_i) stored in a user's smart card, the improved scheme can perform the mutual

authentication. In addition, after achieving the mutual authentication, the user and the telecare system can compute the shared session key $sk=h(ID_i \,//\, N_U \,//\, N_S)$ each other for later secrecy communication.

5.6 Functionality Comparisons between the Improved Scheme and the Related Scheme

The functionality comparisons between the related scheme and the improved scheme are summarized in Table 2. As a result, the improved scheme is relatively more secure than the related schemes. In addition, the improved scheme provides mutual authentication between the user and the telecare system.

Table 2. Security Comparison of the Related Scheme and the Improved Scheme

security features	Zhu's scheme [7]	Lee-Liu's scheme [8]	Improved scheme
insider attack	possible	possible	impossible
password guessing attack	possible	possible	impossible
user impersonation attack	possible	possible	impossible
sever masquerading attack	impossible	impossible	impossible
session key generation attack	possible	possible	impossible
mutual authentication	not provided	not provided	provided

6. Conclusions

In this paper, we have shown that Lee-Liu's smart card-based user authentication scheme is not secure against the various attacks, such as insider attack, off-line password guessing attack, user impersonation attack, session key generation attack and fails to provide mutual authentication between the user and the telecare system. Also, we proposed the improved smart card-based user authentication scheme for the telecare medical information system (TMIS) to overcome these various attacks, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result, the improved smart card-based user authentication scheme is relatively more secure than the related schemes.

Acknowledgement

This work was supported by Kangnam University Research Grants.

References

[1] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1987.
[2] M.S. Hwang and L.H. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Transactions on Consumer Electronics, vol. 46, pp. 28-30, 2000.
[3] C.W. Lin, C.S. Tsai and M.S. Hwang, "A New Strong-Password Authentication Scheme Using One-Way Hash Functions," Journal of Computer and Systems Sciences International, vol.45, no.4, pp. 623-626, 2006.
[4] C.T. Li and M.S. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards," Journal of Network and Computer Applications, vol. 33, pp. 1-5, 2010.
[5] A.K. Das, "Analysis and Improvement on an Efficient Biometric-based Remote User Authentication Scheme Using Smart Cards," IET Information Security, vol.5, Iss. 3, pp. 541-552, 2011.
[6] J. Wei, X. Hu, and W. Lie, "An Improved Authentication Scheme for Telecare Medicine Information Systems," Journal of Medicine Systems, vol. 36, no. 6, pp. 3597-3604, 2012.
[7] Z. Zhu, "An Efficient Authentication Scheme for Telecare Medicine Information Systems," Journal of Medicine Systems, vol. 36, no. 6, pp. 3833-3838, 2012.

[8] T.F. Lee, C.M. Lie, "A Secure Smart-Card Based Authentication and Key Agreement Scheme for Telecare Medicine Information Systems," Journal of Medicine Systems, 37:9933, 2013.
[9] A.K. Awasthi, K. Srivastava, "A Biometrics Authentication Scheme for Telecare Medicine Information Systems with Nonce," Journal of Medicine Systems, vol. 37(5), pp. 1-4, 2013.
[10] D. Mishra, S. Mukhopadhyay, S. Kumar, M.K. Kyan, A.Chaturvedi, "Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce," Journal of Medicine Systems, vol. 38(41), pp. 1-11, 2014.
[11] Y. An, "A Strong Biometric-based Remote User Authentication Scheme for Telecare Medicine Information Systems with Session Key Agreement," International Journal of Internet, Broadcasting and Communication, vol. 8(3), pp. 41-49, 2016.
[12] H. Yang, "An Improved Biometric-based Password Authentication Scheme with Session Key Agreement," International Journal of Internet, Broadcasting and Communication, vol. 8(3), pp. 50-57, 2016.
[13] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," Proceedings of Advances in Cryptology, pp. 388-397, 1999.
[14] T. S. Messerges, E. A. Dabbish and R.H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552, 2002.