International Journal of Cryptology Research 5(1): 28-44 (2015)

Generic Construction for Attribute-Based Identification Schemes Secure against Reset Attacks

[1]Ji-Jian Chin, [2]Hiroaki Anada, [3]Seiko Arita, [2,4]Kouichi Sakurai, [5]Swee-Huay Heng and [1]Raphael Phan

[1]Faculty of Engineering, Multimedia University
[2]Institute of Systems, Information Technologies and Nanotechnologies, Japan
[3]Institute of Information Security, Japan.
[4]Faculty of Information Science and Electrical Engineering, Kyushu University
[5]Faculty of Information Science and Technology, Multimedia University
Email: [1]jjchin@mmu.edu.my, [2]anada@isit.or.jp

ABSTRACT

Identification schemes are a common one-way authentication technique for a user to prove himself securely to a verifier. However, it is known that identification schemes based on the sigma-protocol are basically insecure against reset attacks. On the other-hand, attribute-based cryptography is a technique which allows for the secure implementation of access policies within a cryptosystem. In this paper, we provide report on the developments in the area of reset attacks for identification schemes as well as for attribute-based identification schemes. Then we put together a new idea to construct attribute-based identification schemes secure against reset attacks.

1. INTRODUCTION

An identification scheme is a cryptographic primitive that allows one party, the prover, to prove himself convincingly to another party, a verifier, without revealing any knowledge about his private key. First proposed by Fiat and Shamir (1983), this primitive is usually used to facilitate access control to allow legitimate users to access resources upon being able to prove themselves securely to a verifying mechanism.

Identification schemes are generally categorized into two-move challenge-response and three-move sigma protocols. Three-move challenge-response protocols basically utilize revolves around the capability of the prover to decrypt a challenge ciphertext or sign a verifiable message, given that he has a valid private key. However, in general, two-move protocols are more expensive operationally.

For three-move sigma protocols the prover and verifier engage in a three-step canonical interaction every time a prover wishes to prove itself. The prover begins by sending a commitment. The verifier follows by selecting a random challenge from a predefined challenge set. Then the prover provides a response using a combination of his private key,

commitment as well as the challenge. The verifier will then decide to accept or reject a prover's session based on the response.

Sigma-protocols have the following properties:

i) Completeness – provers with valid private keys should be given an accept except with negligible probability.

ii) Soundness – provers with invalid private keys should be given a reject decision except with negligible probability.

iii) Zero-knowledge – certain sigma protocols have a zero-knowledge property, where the verifier upon completing the interaction with the prover learns nothing about the user's private key. This is proven by a simulator that is able to produce a valid interaction transcript with or without a prover's participation. However, since it is hard to prove security against concurrent-active attacks for protocols with zero-knowledge properties, sometimes the requirement is relaxed to just satisfying a witness indistinguishability requirement (Fiege and Shamir, 1990), where a verifier cannot distinguish between the two witnesses used in the protocol.

Reset Attacks on Identification Schemes

While generally two-move challenge-response protocols are secure against reset attacks, unfortunately sigma protocols have an inherent weakness against reset attacks, where an adversary is allowed to reset the prover to where he first sent commitments for the prover to send the same commitment. Then due to the soundness property, with two different challenges, the adversary is able to extract a user's private key from the different responses and challenges but using the same commitment.

Reset attacks can be performed if an adversary has access to the verifying machine, for example a smart card reader that is able to tamper with the internal state of the smart card. Thus the adversary with access to this smart card reader will be able to extract an honest user's private key if the user interacts with it.

The reset attack was first addressed for identification schemes by Bellare et al. (2001). In their seminal paper, they tackled the problem of adversaries with the resetting capability and proposed several methods of overcoming this problem. We provide a more comprehensive review of these methods in a later section of this paper.

The power of reset attacks can be seen by the following scenarios given by Bellare et al. (2001), describing how a reset-attack can be mounted practically. Firstly, if an adversary captures a prover device such as a smart card, the adversary can disconnect ad reinsert the battery to reset the card's secret internal state to its initial state. This can be done multiple times.

Secondly if an adversary is able to crash the prover device, such as a causing a stack/heap overflow, upon reinitializing the device will resume computation after the crash, forcing the device to reset itself.

Thus, reset-secure identification schemes are desirable due to the existence of these threats.

Identification Schemes without Certificates

In traditional public key cryptography, certificates are required to bind a user to his public key, which could otherwise be replaced by a malicious party. These certificates are issued by certificate authorities, and include a wide-array of information ranging from the public key to validity period. Any doubtful parties can verify a user's public key actually belongs to a particular user by checking on the Certificate Authority's digital signature on the certificate.

The certificate management issue occurs when the users of the cryptosystem grow large and a large overhead is required to issue, validate, manage and revoke these certificates. To circumvent this issue, Adi Shamir first proposed identity-based cryptography (Shamir,1984), where users can implicitly certify themselves using a publicly known identity-string. Identity-based cryptography only kicked off in 2001 when (Boneh and Franklin, 2001) proposed the first identity-based encryption scheme. In 2004, the first identity-based identification schemes were proposed by Bellare et al. (2004) and Kurosawa and Heng, (2004) independently.

Since then, many identity-based identification schemes have been proposed, but none of them secure against reset attacks. The first identity-based identification scheme secure against reset attacks was first proposed by Thorncharoensri et al. (2009).

In addition to identity-based cryptography, other extensions for identification schemes that operate without the requirement of certificates have surfaced in the recent decade. Certificateless cryptography was proposed by Alriyami and Paterson (2001) to provide circumvent the key escrow issue, where the central key generation center has access to every user's private key. In certificateless cryptography, the key generation center creates a partial private key, which the user combines with his component of

the private key to create the full private key, thus without the user's component the key generation center does not have complete access to the full private key. For the identification primitive, certificateless identification was first defined and proposed by Dehkordi and Alimoradi (2013) and Chin et al. (2013) independently. However, subsequently Chin et al. (2014) pointed out flaws in Dehkordi and Alimoradi (2013)'s design, therefore it is insecure against impersonation attacks.

Another new area of identification schemes without certificates is the attribute-based identification scheme. Attribute-based identification was introduced by Anada et al. (2013). In an ABID scheme, each entity has credentials called attributes. On the other hand, an access policy is written as a boolean formula over those attributes. Then, a verifier can identify that a prover possesses a certain set of attributes that satisfies the verifier's access policy. Hence, ABID schemes can be considered as an expansion of the usual ID schemes. In Anada et al. (2013)'s seminal paper, a two-move generic (and concrete) construction was presented. That is, by employing an attribute-based key encapsulation mechanism (Sahai and Waters 2005, Waters 2011), a challenge-and-response protocol was proposed. Theirs scheme was claimed to be secure against reset attacks, but only a brief sketch of security proof was denoted. After their two-move construction, a three-move construction was presented by Anada et al., (Jan. 2014, Jun. 2014, Jan. 2015).

In contrast to the construction by Anada et al. (2013), the three-move construction was based on the (traditional) sigma protocol (Cramer et al., 2001). Enhancing the technique of OR-proof (Damgard, 2004), they succeeded to provide a three-move generic ABID scheme that can be concretely realized without pairings. Hence Anada et al., (2014)'s three-move protocol can be said to be more efficient than the two-move protocol (Anada et al., 2013). But their three-move protocol is not secure against reset attacks because its security is based on the Reset-Lemma (Bellare and Palacio, 2002).

Chronology of Research For Attribute-Based Resettable Identification

We provide the chronology of all related work and their contributions toward our generic construction, as summarized in Table 1 below:

Paper	Year	Description
Canetti et al.	2000	Introduced resettable zero-knowledge transformation techniques.
Bellare et al.	2001	Adapted Canetti's techniques to construct

		reset-secure identification schemes.
Stinson and Wu	2006	Proposed a simple 2-move reset-secure identification scheme.
Thorncharoensri et al.	2009	Proposed first reset-secure identity-based identification scheme.
Anada et al.	2013	Introduced attribute-based identification schemes.

Table 1: Summary of Related Research

Motivations and Contributions

Since its conception in 2004, identification schemes without certificates have received much attention, particularly attribute-based identification. Secondly, the notion of reset attacks has not yet been examined in depth, particularly with regards for identification schemes without certificates.

In this paper, we introduce the reader to the security notions of reset-secure identification schemes as well as attribute-based identification (ABID). In specific, we examine the two-move ABID scheme by Anada et al (2013) along with the proof of security on access policies. After that, we combine the two notions to provide the first generic construction to modify a three-move attribute-based identification scheme to be secure against reset attacks.

The rest of the paper is organized as follows: In Section 2 we begin review the definitions and security model of reset-secure identification schemes and ABID schemes. In Section 3 we review the two-move ABID scheme by Anada et al. (2013) along with the proof of security. In Section 4, we introduce the first generic construction to modify three-move ABID schemes to be reset-secure. We conclude in Section 5 with some closing remarks.

PRELIMINARIES AND DEFINITIONS

We begin by first defining the components required, namely the trapdoor commitment scheme TDC and the pseudorandom function PRF. Then, we review the formal definitions and security notions for reset-secure identification schemes as well as ABID schemes.

Trapdoor Commitment Scheme

A commitment scheme TDC is defined by a key generation algorithm $TDC_{keygen}(1^k) \rightarrow (PK_{TDC}, SK_{TDC})$ that sets up the key, a commit algorithm $TDC_{CMT}(PK_{TDC}, m) \rightarrow c$ which on input of public key PK_{TDC} and message m outputs a commitment c, as well as a decommit algorithm $TDC_{VF}(PK_{TDC}, m, c) \rightarrow b: b \in \{0,1\}$ which upon input of the public key PK_{TDC}, message m and commitment c outputs 1 if the commitment is true to the message and 0 otherwise.

Commitment schemes need to satisfy two requirements: hiding and binding. Hiding is the requirement that anybody observing c will not be able to gather any information about m. Binding binds the commitment to the original message, meaning the sender cannot find another $m' \neq m$ that corresponds to the same commitment, i.e. $TDC_{CMT}(PK_{TDC}, m') \rightarrow c$.

A trapdoor commitment scheme requires an additional property called equivocability which on input of the secret key SK_{TDC}, $TDC_{equi}(SK_{TDC}, m, r, m') \rightarrow (m', r')$ outputs an arbitrary separate message m' with its corresponding salt r'. This means with the secret key as a trapdoor, a sender can alter the original message to correspond to the same commitment.

We require the use of the binding property in our security analysis. The following experiment is defined to capture this security requirement. An adversary A is given access to the public key PK_{TDC} as well as commitment and decommitment oracles O_{CMT} and $O_{VRF}$and is allowed up to q queries. At the end of the training phase, A outputs a message-commitment pair m^*, c^* such that c^* was queried before but m^* was not. This means A manages to find a different message that corresponds to a similar commitment, therefore winning the game.

Let k denote the security parameter. The advantage of A described above is given in the probability the following experiment returns 1:

$$\begin{aligned} \mathrm{Adv}_A^{TDC}(\mathrm{k}) = \Pr[(PK_{TDC}, SK_{TDC}) \leftarrow TDC_{keygen}(1^k); \\ (m^*, c^*) \leftarrow A^{O_{CMT}(m_1,\ldots,m_q), O_{VRF}(m_1,c_1,\ldots,m_q,c_q)}(PK_{TDC}): \\ m^* \neq m_i \wedge c^* = c_i: i \in \{1, \ldots, q\} \wedge \\ TDC_{VRF}(PK_{TDC}, m^*, c^*) \rightarrow 1 \,] \end{aligned}$$

Pseudorandom Functions

A family of pseudorandom functions PRF is a group of functions that takes an input and maps it to an independent random output using a security parameter. The output needs to be indistinguishable from that of a truly random function $RAND$. However, the running time needs to be polynomial (and therefore efficient), whereas truly random functions usually have exponential description complexity.

The security for pseudorandom functions is considered using two experiments and a distinguisher algorithm D. In experiment 0, D has access to a PRF function for oracle queries while in experiment 1, D is given access to a $RAND$ function instead. D is allowed to query these oracles adaptively. Let $EXP(0)$ be the event that D outputs a 1 if it is in experiment 0, and let $EXP(1)$ be the event that D outputs a 1 if it is in experiment 1. The advantage of D would then be to distinguish whether it is in experiment 0 with a pseudorandom function, or in experiment 1 with a truly random function.

Let k denote the security parameter. Formally we have:

$$Adv_D^{PRF}(k) = |\Pr[EXP(0) = 1] - \Pr[EXP(1) = 1|$$

Reset-Secure Identification Schemes

An identification scheme consists of three probabilistic polynomial-time algorithms: Keygen, Prover and Verifier.

Keygen takes in the security parameter 1^k and generates a public/private key pair for the user $\langle pk, sk \rangle$.

Prover takes in the private key sk while Verifier takes in the public key pk. Together they run the sigma protocol as such:

1) Prover sends the commitment CMT.
2) Verifier selects and sends a random challenge CHA from a set of predefined challenges.
3) Prover calculates his response RSP based on the challenge and returns it Verifier. Verifier will then choose to accept/reject based on the response given.

An adversary towards an identification scheme is an impersonator. For normal identification schemes an impersonator can be a passive one, where he only eavesdrops on conversations, or an active one where he can play a cheating verifier to learn information by interacting with honest users before attempting impersonation.

We consider the strongest conventional impersonator toward an identification scheme, namely the concurrent attacker who is an active attacker but can run simultaneous interactions with honest users concurrently. Let the advantage of this impersonator attacking a standard identification scheme sI be given as $Adv_{I_{CI}}^{sI}(k)$, where k is the security parameter.

For reset-secure identification schemes, an additional concurrent reset-attacker is defined. This attacker is more powerful than the conventional passive/active attacker and is able to run several instances of the prover interactions concurrently, interleaving executions and performing reset actions on the prover states. Bellare et al. (2000) first formalized these two types of concurrent reset attackers as CR1 and CR2 respectively.

For the CR1 attacker, the adversary may interact with the honest user's Prover algorithm as a verifier and in addition to identification queries, be able to perform a reset action for the Prover algorithm to any state. Later the adversary performs the impersonation attempt.

For the CR2 attacker, the adversary may do all the actions described for the CR1 attacker, but may attempt impersonation whenever it wishes to. Therefore, the CR1 attacker is a special case of CR2 attack.

We describe the security for the reset-secure identification scheme by the following game played between a challenger C and an impersonator I.

Keygen: C takes in the security parameter 1^k, generates $\langle pk, sk \rangle$ and passes pk to I.

Phase 1: I is able to make the following queries:

i) Identification queries: I interacts as a cheating verifier with a prover simulated by C to learn information.

ii) Reset queries: I resets the prover simulated by C to any state that it wishes within the three-step sigma protocol.

Phase 2: I changes mode into a cheating prover trying to convince C. For CR2 I, it can still continue to make any of the queries from Phase 1. I

wins if it manages to convince C to accept its interaction with non-negligible probability.

Define the advantage of this reset attacker against a conventional identification scheme as $Adv_{I_{RI}}^{sI}(k)$, where k is the security parameter.

Bellare et al. (2001) also proposed four techniques in order to secure identification schemes that are constructed using the sigma protocol against reset attackers, which are naturally insecure against reset attacks. We briefly describe the four techniques here:

1) Stateless digital signatures: a prover can authenticate himself to a verifier by showing the capability of signing random documents the verifier chooses. Here the message becomes the challenge while the signature is used as the response. Statelessness is required so that the reset attacker cannot reset the state of the signer. However, this is generally a two-move protocol.
2) Encryption schemes: a prover can authenticate himself to a verifier by showing the capability to decrypt random ciphertexts the verifier chooses. Here the ciphertext becomes the challenge while the message becomes the response. However, reset-security requires that an encryption scheme secure against chosen-ciphertext attacks be used.
3) Trapdoor commitments: this technique uses a trapdoor commitment scheme to 'commit' a verifier's challenge. This commitment is used as the generator for the prover's salt using a pseudorandom function. One can therefore verify that upon revealing the verifier's challenge, the salt can be regenerated in order to create the proper response for the verifier. If the prover was reset, the regeneration of the salt would yield a different (and invalid) response.
4) Zero-knowledge proof of membership: a prover proves membership in a hard language rather than proving that it has a witness for the language. This is done by using a resettable zero-knowledge proof of language membership, as defined by Canetti et al. (2000).

In this work, we utilize the third technique as a generic way to construct reset-secure ABID schemes. Bellare et al. (2001) utilized the third technique to convert concurrent-secure conventional identification schemes into reset secure ones using trapdoor commitment schemes and pseudorandom functions. The advantage of the reset-impersonator as defined with their transform is given as:

$$Adv_{I_{RI}}^{sI}(k) = Adv_{I_{CI}}^{sI}(k) + Adv_{D}^{PRF}(k) + Adv_{A}^{TDC}(k)$$

ABID Schemes

Let $U = \{1, \ldots, u\}$ be an attribute Universe. An access structure A, which means an access policy, is defined as a subset of $2^U \backslash \phi$. We only treat monotone access structures.

An ABID scheme consists of four PPT algorithms: Setup, KeyGen, Prover, Verifier.

Setup(1^k,U) $\rightarrow$ **(PK, MSK)**. Setup takes as input the security parameter λ and the attribute universe U. It outputs a public key PK and a master secret key MSK.

KeyGen(PK, MSK, S) $\rightarrow SK_S$. A key-generation algorithm KeyGen takes as input the public key PK, the master secret key MSK and an attribute set S. It outputs a secret key SK_S corresponding to S.

Prover(PK, SK_S) and Verifier(PK, A). Prover and Verifier are interactive algorithms. Prover takes as input the public key PK and the secret key K_S . Here the secret key SK_S is given to Prover by an authority that runs KeyGen(PK, MSK, S). Verifier takes as input the public key PK and an attribute set S. Prover is provided Verifier's access structure A by the first round. Prover and Verifier interact with each other for some, at most constant rounds. Then, Verifier finally returns its decision bit b. $b = 1$ means that Verifier $accepts$ Prover in the sense Prover has a secret key SK_S such that S satisfies A. $b = 0$ means that Verifier $rejects$ Prover.

We require correctness of an ABID scheme that for any 1^k and U, and if $S \in A$, then the probability of Verifier outputting an $accept$ be always true, namely

$$\Pr[(PK, MSK) \leftarrow Setup(1^k, U);$$
$$SK_S \leftarrow KeyGen(PK, MSK, S);$$
$$b \leftarrow \langle P(PK, SK_S), V(PK, A) \rangle : b = 1] = 1$$

Lastly let the concurrent-impersonator attacking an ABID scheme be defined as $Adv_{I_{CI}}^{ABID}(k)$, where k is the security parameter.

PROOF OF THE RESET-SECURITY OF THE TWO-MOVE PROTOCOL

In this section we review Anada et al.(2013)'s two-move ABID scheme and show the security proof against reset attacks.

Review of Anada et al. (2013)'s Two-Move ABID Scheme

A ciphertext-policy ABKEM, CP-ABKEM, consists of four probabilistic polynomial time algorithms: (Setup, KeyGen, Encap, Decap).

Setup($1^k, U$) $\rightarrow$ (PK, MSK). Setup takes as input the security parameter 1^k and the attribute universe U. It returns a public key PK and a master secret key MSK.

KeyGen(PK, MSK, S) $\rightarrow$ SK_S. A key generation algorithm KeyGen takes as input the public key PK, the master secret key MSK and an attribute set $S \subset U$. It returns a secret key SK_S that corresponds to S.

Encap(PK, A) $\rightarrow$ (κ, ψ). Encap takes as input the public key PK and an access structure A. It returns a random KEM key κ and its encapsulation ψ (we also call it a ciphertext).

Decap(PK, SK_S, ψ) $\rightarrow$ $\hat{}\kappa$. Decap takes as input the public key PK, an encapsulation ψ and a secret key SK_S. It returns a decapsulation result $\hat{}\kappa$ of ψ under SK_S. We assume that Decap is deterministic. This assumption is not limiting because almost all known decapsulation algorithms are deterministic.

We require correctness of CP-ABKEM that for any 1^k and U, and if $S \in A$, then the Decap will always return a valid decapsulation result all the time, namely

$$\Pr[(PK, MSK) \leftarrow Setup(1^k, U); \\ SK_S \leftarrow KeyGen(PK, MSK, S); \\ (\kappa, \psi) \leftarrow Encap(PK, A); \\ \hat{}\kappa \leftarrow Decap(PK, SKS, \psi) : \kappa = \hat{}\kappa] = 1.$$

CP-ABKEM is called secure against chosen-ciphertext attacks on one-wayness (OW-CCA secure) if, for any PPT adversary that issues decapsulation queries, the success probability for the adversary to return the correct decapsulation of a received, not queried encapsulation generated legitimately, is negligible in the security parameter.

Let CP-ABKEM= (KEM.Setup, KEM.KeyGen, KEM.Encap, KEM.Decap) be a CP-ABKEM. Then ABID= (Setup, KeyGen, Encap, Decap) is obtained as a challenge-and-response protocol of encapsulation-and-decapsulation.

Security Proof of the Two-Move ABID scheme against Reset Attacks

Theorem. *If CP-ABKEM is OW-CCA secure against chosen-ciphertext attacks on one-wayness (OW-CCA), then the derived ABID is secure against (prover-)reset attacks.*

Proof. Since an interaction consists of challenge-and-response of encapsulation-and-decapsulation, (prover-) reset query is the same as decapsulation query. Hence any PPT adversary that executes reset attacks on the derived ABID can be converted into a PPT adversary that executes OW-CCA on an underlying CP-ABKEM. By the assumption, the underlying CP-ABKEM is secure against OW-CCA and hence the derived ABID is secure against (prover-) reset attacks.

GENERIC CONSTRUCTION OF 3-MOVE RESET-SECURE ABID SCHEME

In this section, we present a new and generic idea for modifying three-move ABID schemes to be secure against reset attacks. We utilize Bellare et al. (2001)'s third paradigm, which is to use a trapdoor commitment scheme, and embed this scheme within the three-move ABID scheme. We begin with a concurrent-secure ABID scheme and perform the conversion in Figure 1. The resulting scheme consists of four-moves.

The construction of the scheme is described in Figure 1.

Setup($1^k, U$)$\rightarrow$ $(PK := (PK_{ABID}, PK_{TDC}), MSK)$:

Setup takes in the security parameter 1^k and the space of the attribute universe U and outputs the public key and master secret key $\langle PK = (PK_{ABID}, PK_{TDC}), MSK\rangle$. However, the public key consists of two components, one for the ABID scheme PK_{ABID} and the other for the trapdoor commitment scheme PK_{TDC}.

KG(PK_{ABID}, MSK, S)$\rightarrow SK_S$:

Keygen KG takes in the public key for the ABID scheme, PK_{ABID}, the master secret key MSK and the set of attributes S and outputs the secret key SK_S corresponding to S.

Prover($PK_{ABID}, PK_{TDC}, SK_S$):		**Verifier(PK, A)**
		$CHA_V \leftarrow ABID_{CHA}(1^k)$ $TDCMT \leftarrow TDC_{CMT}(PK_{TDC}, CHA_V; R_C)$
$R_{ABID} \leftarrow PRF(R_P, TDCMT)$ $CMT \leftarrow ABID_{CMT}(SK_S, R_{ABID}, A)$	$\xleftarrow{TDCMT, A}$ $\xrightarrow{CMT}$ $\xleftarrow{CHA_V \| \| R_C}$	
IF $TDC_{VF}(PK_{TDC}, TDCMT, CHA_V \| \| R_C) = accept$ THEN $RSP \leftarrow ABID_{RSP}(SK_S, CMT, CHA_V; R_{ABID})$ ELSE $RSP = \perp$	$\xrightarrow{RSP}$	$dec \leftarrow ABID_{VF}(PK_{ABID}, A, CMT, CHA_V RSP)$

Prover and Verifier engage in the identification protocol as follows:

1) Upon receiving an initialization message from Prover, Verifier first generates a commitment $TDCMT$ for his random challenge CH_V using the trapdoor commitment scheme's commit algorithm TDC_{CMT} and sends it to the Prover along with the access policy A.
2) Prover evaluates $TDCMT$ and his own internal coins R_P with a pseudorandom function PRF and generates the salt R_{ABID}. This salt is used to generate his commitment CMT and is sent to Verifier.
3) Verifier then sends his random challenge CH_V and random coins R_C to the Prover.
4) The Prover uses the trapdoor commitment scheme's public key PK_{TDC}, the Verifier's trapdoor commitment $TDCMT$, as well as the newly received challenge $CHA_V$and random coins from the Verifier R_C to reveal the commitment for verification.
5) If verification of the commitment is an $accept$, Prover will then calculate the response RSP for the ABID scheme and send it to the Verifier. Otherwise it aborts.
6) Verifier then outputs the decision on whether to accept the Prover's response

or not.

Figure 1: Generic Construction of 3-move Reset-Secure ABID Scheme

Security Analysis

Our generic transformation derives security for reset attacks against ABID schemes similarly to how Bellare et al. (2001) derives security for reset attacks for conventional identification schemes using their third technique. To begin with we assume the security of a concurrent-secure ABID scheme. Then additionally the reset-impersonator will have perform any of the following in order to successfully impersonate:

1) Break the concurrent-security of the underlying ABID scheme. This advantage is given by $Adv_{I_{CI}}^{ABID}(k)$.
2) Break the binding capability of the trapdoor commitment scheme to find another commitment that corresponds to the initial challenge sent by the verifier. This advantage is given by $Adv_{A}^{TDC}(k)$.
3) Distinguish between the pseudorandom function and a truly random function to predict the output of the commit step. This advantage is given by $Adv_{D}^{PRF}(k)$.

Putting them all together we obtain the security bound for the reset attacker against ABID scheme as:

$$Adv_{I_{RI}}^{ABID}(k) = Adv_{I_{CI}}^{ABID}(k) + Adv_{D}^{PRF}(k) + Adv_{A}^{TDC}(k)$$

CONCLUSION

In this paper, we provided a review of the security notions of reset-secure identification as well as ABID schemes. We then reviewed Anada et al. (2013)'s ABID scheme with two-move identification protocol and showed that it is secure against reset attacks. Then, we give a generic construction to modify three-move ABID schemes to be reset secure. Future work would be to construct a concrete construction with provable security to an intractable mathematical assumption as a case study for the transformation work.

ACKNOWLEDGEMENTS

The authors are grateful to the Ministry of Education of the Government of Malaysia for partially funding this research under The Fundamental Research Project Scheme (No.: FRGS/2/2013/ICT07/MMU/03/5).

REFERENCES

Al-Riyami, S. S., and Paterson, K. G. 2003. Certificateless public key cryptography. *In Advances in Cryptology-ASIACRYPT 2003* (pp. 452-473). Springer Berlin Heidelberg.

Anada, H., Arita, S., Handa, S., and Iwabuchi, Y. 2014. Attribute-based identification: Definitions and efficient constructions. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*,*97*(5), 1086-1102.

Anada, H., Arita, S. and Sakurai, K. 2014. Attribute-Based Identification Schemes of Proofs of Knowledge. *SCIS2014*, 3E3-3.

Anada, H., Arita, S., and Sakurai, K. 2014. Attribute-based signatures without pairings via the fiat-shamir paradigm. In *Proceedings of the 2nd ACM workshop on ASIA public-key cryptography* (pp. 49-58). ACM.

Anada, H., Arita, S. and Seiko Arita, Kouichi Sakurai. 2015, January. Attribute-Based Signatures from Proof of Knowledge of Signatures. *SCIS2015*, 2D3-2.

Bellare, M., Fischlin, M., Goldwasser, S., and Micali, S. 2001. Identification protocols secure against reset attacks. In *Advances in Cryptology—EUROCRYPT 2001* (pp. 495-511). Springer Berlin Heidelberg.

Bellare, M., Namprempre, C., and Neven, G. 2009. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, *22*(1), 1-61.

Boneh, D., and Franklin, M. 2001, January. Identity-based encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO 2001* (pp. 213-229). Springer Berlin Heidelberg.

Canetti, R., Goldreich, O., Goldwasser, S., and Micali, S. 2000, May. Resettable zero-knowledge. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing* (pp. 235-244). ACM.

Chin, J. J., Phan, R. C. W., Behnia, R. and Heng, H. 2013. An Efficient and Provably Secure Certificateless Identification Scheme. *SECRYPT 2013*: 371-378.

Chin, J. J., Behnia, R., Heng, H. and Phan, R. C. W., 2014. Cryptanalysis of a Certificateless Identification Scheme. *Security and Communication Networks*: 7, 4.

Cramer, R., Damgård, I., and Nielsen, J. B. 2001. *Multiparty computation from threshold homomorphic encryption* (pp. 280-300). Springer Berlin Heidelberg.

Dehkordi, M. H., and Alimoradi, R. 2014. Certificateless identification protocols from super singular elliptic curve. *Security and Communication Networks*, *7*(6), 979-986.

Feige, U., and Shamir, A. 1990, April. Witness indistinguishable and witness hiding protocols. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing* (pp. 416-426). ACM.

Fiat, A., and Shamir, A. 1987, January. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology—CRYPTO'86* (pp. 186-194). Springer Berlin Heidelberg.

Kurosawa, K., and Heng, S. H. 2004. From digital signature to ID-based identification/signature. In *Public Key Cryptography–PKC 2004* (pp. 248-261). Springer Berlin Heidelberg.

Sahai, A., and Waters, B. 2005. Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005* (pp. 457-473). Springer Berlin Heidelberg.

Shamir, A. 1985, January. Identity-based cryptosystems and signature schemes. In *Advances in cryptology* (pp. 47-53). Springer Berlin Heidelberg.

Thorncharoensri, P., Susilo, W., and Mu, Y. 2009. Identity-based identification scheme secure against concurrent-reset attacks without random oracles. In*Information Security Applications* (pp. 94-108). Springer Berlin Heidelberg.

Waters, B. 2011. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography–PKC 2011* (pp. 53-70). Springer Berlin Heidelberg.

Wu, J., and Stinson, D. R. 2009. An efficient identification protocol secure against concurrent-reset attacks. *Journal of Mathematical Cryptology*, *3*(4), 339-352.