Festschrift

LNCS 5393

Jacques Calmet
Willi Geiselmann
Jörn Müller-Quade (Eds.)

Mathematical Methods in Computer Science

Essays in Memory of Thomas Beth

Springer

Lecture Notes in Computer Science 5393

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Jacques Calmet Willi Geiselmann
Jörn Müller-Quade (Eds.)

Mathematical Methods in Computer Science

Essays in Memory of Thomas Beth

Springer

Volume Editors

Jacques Calmet
Willi Geiselmann
Jörn Müller-Quade
Universität Karlsruhe
Institut für Algorithmen und Kognitive Systeme
76128 Karlsruhe, Germany
E-mail: {calmet,geiselma,muellerq}@ira.uka.de

The illustration appearing on the cover of this book is the work of Daniel Rozenberg (DADARA).

Library of Congress Control Number: 2008940842

CR Subject Classification (1998): E.3, J.2, F.2, F.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-89993-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-89993-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12585199 06/3180 5 4 3 2 1 0

Preface

The conference Mathematical Methods in Computer Science (MMICS) was held in the memory of Thomas Beth during December 17–19 in Karlsruhe. The conference was meant to reflect the many interests of Thomas Beth. Even though these interests might seem diverse the mathematical methods employed and especially algebra as a language were the common denominator of all his scientific achievements. The 12 contributed talks reaching from t-designs to integrated circuits were selected from 30 submissions from 14 countries.

The contributed talks were complemented by three invited talks. Teo Mora gave a talk on "Decoding Cyclic Codes: The Cooper Philosophy" embracing the areas of coding theory and symbolic computation. These areas were especially appreciated by Thomas Beth, because they combine algebra and algorithmics. Richard Jozsa lectured about "Embedding Classical into Quantum Computation" in the area of quantum information. Quantum information was a focus of research of Tomas Beth since 1993 when he co-organized one of the earliest workshops on quantum cryptography in Dagstuhl. Quantum information became his passion in 1994 when the connection between the Fourier transformation and breaking the RSA crypto system became apparent via Shor's algorithm, which can factor integers in polynomial time on a quantum computer. The Fourier transform and cryptography were topics that played an important role in Thomas Beth's research and this connection, once again, justified his broad view on computer science.

We were especially delighted by the very personal talk from Fred Piper, a former colleague of Thomas Beth from the time he spent at Royal Holloway College. His talk was about "Zeros and Ones" and his abstract summarizes the scope of the conference better than we can do:

> Tom was a personal friend as well as being a colleague and collaborator. He was interdisciplinary in the truest sense of the word with expertise in computer science, mathematics and physics. In this short talk I will look at those areas where our personal interests overlapped. These began with finite projective planes, generalised on to block designs and then changed (from pure mathematics) to coding theory and cryptography. The talk will be historical with little technical detail but, using zeros and ones as the theme, will try to show that the path we followed was 'natural'.

Thomas Beth would have enjoyed this conference. His legacy should support us in our research projects and remind us to never forget the pleasure of intellectual work.

October 2008

Jacques Calmet
Willi Geiselmann
Jörn Müller-Quade

In Memoriam

Prof. Dr.-Ing. habil. Dr. rer. nat. Thomas Beth, professor and long-standing spokesman of the Institut für Algorithmen und Kognitive Systeme (IAKS), was born November 16, 1949 in Hannover. He studied mathematics, physics, and medicine at the Universität Göttingen and received his Dr. rer. nat. in Mathematics from the Universität Erlangen-Nürnberg in 1978 after four years of employment as a research associate.

After receiving the degree of Dr. Ing. habil. in the area of informatics in 1984 from the same university he was appointed Professor of Computer Science at the University of London and head of the Department of Computer Science and Statistics at the Royal Holloway College, University of London. There he created the research group for cryptography.

In 1985 he took a Chair of Informatics at the Universität Karlsruhe (TH) and, together with two colleagues, co-founded the Institut für Algorithmen und Kognitive Systeme, which he has represented as a spokesman ever since.

The scientific achievements of Prof. Beth were aimed at understanding algorithmic structures in larger systems or applications. This line of research, which started with his algebraic explanation of the general Fourier transform, was continued at his institute, becoming the groundwork in modern signal and image processing. Automated tools for the decomposition of signal transforms were one result of his research that yielded efficient algorithms for different applications. New methods for medical image processing were based on these methods and the algebraic models for signal transforms. Professor Beth recognized very early the importance of the wavelet transform for data compression and pattern

classification. This research was guided by the general idea to use mathematical techniques to develop solutions for a broad spectrum of tasks in signal processing and automatically realize these in very highly integrated circuits. This homogeneous development process avoids inefficiencies and design errors to a large extent.

Cryptology was another focus in the work of Prof. Beth, where he followed an analogous approach. As in his other work he kept an eye on the applicability of his methods, which is reflected by his work in the European Institute of System Security (E.I.S.S.) that he founded in 1988 and headed since then. In his research in cryptology he successfully applied methods from the mathematical areas of combinatorics and algebra. In 1982 he organized an international cryptology conference at Castle Feuerstein, from which the renowned series of EUROCRYPT conferences emerged.

With this background Thomas Beth was early on attracted by the newly emerging field of quantum computing. This area linking informatics, mathematics and physics appealed to him, not only as a researcher, but also due to the implications quantum computing has on cryptology. Encryption mechanisms which are classically considered to be secure become insecure with respect to techniques from quantum computing.

Thomas Beth became a pioneer of quantum computing on the national level as well as internationally. His activities led to the first priority program of the Deutsche Forschungsgemeinschaft and to the first European funding program in this area. In Germany he headed the first and largest research group on quantum computing in informatics.

In the Faculty for Informatics in Karlsruhe he was one of the initiators of the new scientific field of anthropomatics. This young area uses methods and models from informatics to describe the interaction of humans with their environment to supply solutions which are well adapted for individual requirements.

Teaching and research were inseparable for Prof. Beth. Passing on his knowledge was of great concern to him and he kept up a scientific dialogue at all levels: during lectures, at his institute, in the faculty and at national and international conferences. Many of his pupils are now in high positions in science and industry.

In spite of his severe illness he was actively involved in designing the future of informatics. Unfortunately, he could pursue this task for a quarter of a century only. He died on August 17, 2005.

Organization

MMICS 2008 was organized by the Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Germany.

Organizers

Jacques Calmet	Universität Karlsruhe, Germany
Willi Geiselmann	Universität Karlsruhe, Germany
Jörn Müller-Quade	Universität Karlsruhe, Germany

Program Committee

Jörn Müller-Quade	Universität Karlsruhe, Germany (Program Chair)
Jacques Calmet	Universität Karlsruhe, Germany
Reiner Creutzburg	Brandenburg University of Applied Sciences, Germany
Willi Geiselmann	Universität Karlsruhe, Germany
Dieter Gollmann	Technische Universität Hamburg-Harburg, Germany
María Isabel González Vasco	Universidad Rey Juan Carlos, Madrid, Spain
Markus Grassl	Österreichische Akademie der Wissenschaften, Austria
Dominik Janzing	Max Planck Institute for Biological Cybernetics, Tübingen, Germany
Dieter Jungnickel	Universität Augsburg, Germany
Andreas Klappenecker	Texas A&M University
Wolfgang Mathis	Universität Hannover, Germany
Harald Niederreiter	National University of Singapore
Markus Püschel	Carnegie Mellon University, USA
Rainer Steinwandt	Florida Atlantic University, USA
Felix Ulmer	Université Rennes 1, France
Roland Vollmar	Universität Karlsruhe, Germany

Table of Contents

Cryptography II

On the Security of Beth's Identification Schemes against Active and Concurrent Adversaries

Giovanni Di Crescenzo

Telcordia Technologies, Piscataway, NJ, USA
giovanni@research.telcordia.com

Abstract. One of the earliest identification schemes was proposed by Beth in [6]. Since its introduction, variations and generalizations of this scheme have been considered, and, recently, the property of security against passive impersonation was shown, under a weak unforgeability assumption on the hashed El Gamal signature scheme, for two such variants: one in the standard (i.e., not identity-based) and one in the identity-based model. However, the security of both protocols under active and concurrent impersonation attacks was left open.

In this paper we prove that very minor modifications to these schemes result in schemes that satisfy security under active and concurrent impersonation attacks, assuming a one-more-dlog assumption. The resulting protocols are just as efficient as the original variants, which are, in turn, somewhat more efficient (but less general) of the original one proposed by Beth.

1 Introduction

An identification scheme is a method for a party A to convince another party B of A's identity. While identification schemes are routinely used in real-life using physical proofs of identity (e.g., identity cards, driving licenses, etc.), computer technology has raised the problem of remote identification schemes; i.e., identification schemes where A and B are physically distant. As of today, several problems related to identification schemes have been studied, several security notions and schemes have been proposed, and the study of (remote) identification schemes is an important research area in Cryptography. Here, the most common scenario, which we also study in this paper, is that of A publishing a 'public key' and keeping secret a matching 'secret key', and using the secret key to identify to B.

Security Notions. Important problems in this area include formulating appropriate security notions for an identification scheme. A first natural notion that can be proposed is that an identification scheme is secure if no efficient adversary can impersonate A, even after witnessing many identification sessions between A and B (this notion is usually called 'security against an impersonation attack of passive type', since the adversary is passively eavesdropping sessions between A and B). Note that the adversary is not given the secret key. A second and

J. Calmet, W. Geiselmann, J. Müller-Quade (Eds.): Beth Festschrift, LNCS 5393, pp. 1–17, 2008.

stronger notion is that an identification scheme is secure if no efficient adversary can impersonate A, even after taking part in many sequential identification sessions with A, playing as B (this notion is usually called 'security against an impersonation attack of active type', since the adversary is actively involved in the sessions between A and B before attempting the impersonation attempt). An even stronger notion is 'security against an impersonation attack of concurrent type', which extends the previous notion in that the identification sessions played by the adversary with A before attempting its impersonation attempt can be run concurrently with multiple entities that use A's secret key.

Previous work. The first identification schemes have been given in [12,13,15] and were based on the hardness of the number-theoretic problem of quadratic residuosity modulo a composite integer. Another important contribution of [13] is the general paradigm of using zero-knowledge [15] proofs of knowledge in order to prove the knowledge of an identity without revealing its associated secret key. Since then, several improvements and variants of the mentioned schemes have been proposed, mostly motivated by efficiency considerations (we mention, in particular, [6,17,20,18], but see also references in [1]). Many of the mentioned schemes are efficient in all metrics of interest (i.e., time and communication complexity).

While some of the early identification schemes (e.g., [12,13,18]) were given a proof of security against active impersonation attacks (and can be showed to be secure against concurrent impersonation attacks), this was not immediately the case for other schemes. For instance, the popular schemes in [17,20] were only proved to be secure against active and concurrent attacks much later in [4]. Moreover, the status of other schemes, including Beth's scheme in [6], with respect to these security notions is currently unknown. Given the special efficiency of these schemes, it remains of great interest to prove, disprove their security against advanced security notions.

Our contribution. We consider the identification scheme from [6], which is one of the earliest identification scheme and is based on one of the most popular signature schemes (i.e., El Gamal signatures [5]). This scheme has already received some attention in the literature, as it was revised and generalized in [7,8], and further studied in [1].

The scheme in [6] had been proposed in the identity-based model, a more complex model than the standard model discussed above, where the user's secret key is somehow tied to the user's identity by a trusted authority. In [1] it was observed that many identification schemes proposed in the identity-based model had a corresponding scheme in the standard model, and viceversa, and a scheme in one model could be mapped to a scheme in the other model via a particular transformation, if some specific 'convertibility' condition was satisfied. The authors in [1] used this approach to surface several identification schemes in one model that were related to the known scheme in the other model, proved several security results on the surfaced schemes, and left some related open problems. In particular, they proposed an identification scheme in the standard model, which we call Beth-SI-0, that is uniquely related to (a slightly more efficient and

less general variant of) the identification scheme in the identity-based model from [6]. They also proved scheme Beth-SI-0 to be secure against passive impersonation, assuming the universal unforgeability under no-message attack of the hashed-message El Gamal signature scheme [5]. Using their transformation based on the convertibility property, they also proposed an identification scheme in the identity-based model, which we call Beth-IBI-0, preserving the same type of security. Finally, they left open the security of both schemes Beth-SI-0 and Beth-IBI-0 against active and concurrent impersonation attacks.

In this paper we define a very minor, seemingly irrelevant, variation of scheme Beth-SI-0, which we call Beth-SI-1, and prove it secure in the standard model against active and concurrent impersonation attacks, under a one-more-dlog assumption (see also [4,2] for related assumptions). Here, we note that scheme Beth-SI-1 maintains the same efficiency as scheme Beth-SI-0. We then observe that scheme Beth-SI-1 also satisfies the mentioned convertibility condition and thus obtain a scheme Beth-IBI-1 for which we can prove security against active and concurrent impersonation attacks, under the same intractability assumption, in the identity-based model. Our minor modification preserves the same time and communication efficiency of the starting schemes, which are, in turn, more efficient but less general variants of Beth's original scheme [6].

Organization of the paper. We start with basic modeling and formal definitions in Section 2. We review the El-Gamal signature scheme [5], and the identification scheme Beth-SI-0 in Section 3. We then describe scheme Beth-SI-1 and prove its security in Section 4. Finally, we discuss the extension to scheme Beth-IBI-1 in Section 5.

2 Definitions

In this section we give the scenario for identification schemes, defining the entities involved, the assumed connectivity among them, the phases, the (sub)protocols, and their security requirements. We start with some basic notations.

Basic notations. The expression $y \leftarrow S$ denotes the probabilistic process of randomly and independently choosing y from set S. The expression $y \leftarrow A(x_1, x_2, \ldots)$ denotes the (possibly probabilistic) process of running algorithm A on input $x_1, x_2, \ldots$ and any necessary random coins, and obtaining y as output. The expression $z \leftarrow (A(x_1, x_2, \ldots) \longleftrightarrow B(y_1, y_2, \ldots))$ denotes the (possibly probabilistic) process of running an interactive protocol [15] between algorithm A, taking as input $x_1, x_2, \ldots$ and any necessary random coins, and algorithm B, taking as input $y_1, y_2, \ldots$ and any necessary random coins, where tr is the sequence of messages exchanged by A and B as a result of this execution, and z is B's final output. If m_i denotes the i-th message sent by, say, algorithm A, in an interactive protocol $(A(x) \longleftrightarrow B(y))$, we also denote the process to create this message as $m_i \leftarrow A(x, m_1, \ldots, m_{i-1})$, where $m_1, \ldots, m_{i-1}$ are the previous messages exchanged between A and B.

System scenario and entities. We consider an arbitrary system (or network) containing services of interest to a number of *users*. Authorization to access such services is checked by a *server*, via an execution of a 2-party protocol, called *identification scheme*, run with the interested user. Such executions can happen sequentially (each execution starting after the previous one is finished) or concurrently (the server runs at the same time one execution with each one of many users). For simplicity, we assume that the communication link between each user and the server is private or not subject to attacks, although we note that the model in which this link is also subject to adversary attacks is of orthogonal focus in the areas of cryptography and security (but is not part of the standard model for identification schemes, as studied in the cryptography area, and in this paper as well). We also denote a user with the term 'prover' and the server with the term 'verifier', since in an identification scheme the user will prove her/his identity to the server.

Algorithms and Correctness Requirement. Let σ be a security parameter, expressed in unary notation (i.e., 1^σ). An *identification scheme* (with security parameter σ) consists of a *setup* algorithm or subprotocol, typically run between the server and a given user, or by the user alone; and an *identification* subprotocol, the latter in turn consisting of a *prover algorithm*, run by the user/prover, and a *verifier algorithm*, run by the server/verifier.

The setup algorithms that we consider, denoted as KG, are only run by the user. On input a security parameter σ in unary, algorithm KG returns a public key pk and a matching secret key sk, in time at most polynomial in σ.

The prover algorithm P is an interactive Turing machine, as defined in [15], that, given as input pk, sk, and the messages exchanged so far with the verifier algorithm, returns a new message for the server, in time polynomial in σ.

The verifier algorithm V is also an interactive Turing machine, that, given as input pk, and the messages exchanged so far with the prover algorithm, returns a new message for the user running the prover algorithm. At the end of the interaction with this user, V also returns a value in {accept,reject}, denoting whether the server positively identifies the user or not. In both cases, V runs in time polynomial in σ.

Informally, the (natural) correctness requirement states that at any time, a server positively identifies users with the appropriate secret key. A formal definition follows.

Definition 1. Let σ be a security parameter and let $\mathrm{IS} = (\mathrm{KG}, \mathrm{P}, \mathrm{V})$ be an identification scheme. We say that IS satisfies *correctness* if it holds that

$$\mathrm{Prob}\left[\,(pk, sk) \leftarrow \mathrm{KG}(1^\sigma); (tr, out) \leftarrow (\mathrm{P}(pk, sk) \longleftrightarrow \mathrm{V}(pk)); out = accept) = 1\,\right].$$

Security Requirements. As typically done in the literature on identification schemes, we study security against *impersonation*; that is, against an adversary that, given all public keys (but no secret key), tries to convince the server to

be an authorized user. We consider three types of impersonation attacks[1], of increasing strength:

1. *Passive Impersonation Attack:* after a pair of public and secret keys is generated, the adversary can choose to eavesdrop transcripts of executions of the identification scheme between P and V, until it decides to make an impersonation attempt; at this point, the adversary tries to make V accept without knowing the secret key.
2. *Active Impersonation Attack:* after a pair of public and secret keys is generated, the adversary can choose to engage, acting as a server, in sequential executions of the identification scheme with P until it decides to make an impersonation attempt; at this point, the adversary tries to make V accept without knowing the secret key.
3. *Concurrent Impersonation Attack:* this attack further extends the active attack in that the adversary can choose to engage, acting as a server, in concurrent executions of the identification scheme with a different instantiation of P (using the same public and private keys), until it decides to make an impersonation attempt; thus, at any given time, the adversary can decide to start a new session with a new instantiation of P, to continue a previous session by sending the next verifier's message, or to start the impersonation attempt.

Formally, for $x \in \{$ passive, active, concurrent $\}$, for any polynomial-time algorithm $A = (A_v, A_p)$, we define the experiment $Exp_x^{\mathrm{IS},A}$, that describes the x-type impersonation attack, and returns 1 (resp., 0) if the attack is successful (resp., not successful). We detail the experiments for $x =$ active and $x =$ concurrent, and then describe the minor variation needed to obtain the experiment for $x =$ passive.

$Exp^{\mathrm{IS},A}_{\mathrm{active}}(1^\sigma)$
1. $(pk, sk) \leftarrow \mathrm{KG}(1^\sigma)$
2. $a \leftarrow A_v(1^\sigma, pk)$
3. while $(a \neq attack)$ do
   $(tr, out) \leftarrow (P(pk, sk) \longleftrightarrow A_v(pk))$
   $(a, aux) \leftarrow A_v(1^\sigma, aux, tr, out)$
4. $(tr, out) \leftarrow (A_p(1^\sigma, aux) \longleftrightarrow V(pk))$
5. if $out = accept$ then **return:** 1
   else **return:** 0.

$Exp^{\mathrm{IS},A}_{\mathrm{concurrent}}(1^\sigma)$
1. $(pk, sk) \leftarrow \mathrm{KG}(1^\sigma)$
2. $(a, j, aux) \leftarrow A_v(1^\sigma, pk)$
3. $tr_j \leftarrow \emptyset$
4. while $(a \neq attack)$ do
   $mes_p \leftarrow P_j(pk, sk, tr_j)$
   $tr_j \leftarrow tr_j | mes_p$
   $(a, mes_v, j, aux) \leftarrow A_v(1^\sigma, aux, mes_p)$
   if $a = start$ then $tr_j \leftarrow \emptyset$
   if $a = continue$ then
   $tr_j \leftarrow tr_j | mes_v$
5. $(tr, out) \leftarrow (A_p(1^\sigma, aux) \longleftrightarrow V(pk))$
6. if $out = accept$ then **return:** 1
   else **return:** 0.

[1] In this paper we do not consider resetting impersonation attacks. Many popular schemes based on proofs of knowledge, like the ones we consider, are immediately insecure against resetting impersonation attacks.

$Exp^{\mathrm{IS},A}_{\mathrm{passive}}(1^\sigma)$ is quickly obtained from $Exp^{\mathrm{IS},A}_{\mathrm{active}}(1^\sigma)$ by replacing the line

$$\text{`}(tr, out) \leftarrow (P(pk, sk) \longleftrightarrow A_v(pk))\text{'}$$

in step 3 with the line

$$\text{`}(tr, out) \leftarrow (P(pk, sk) \longleftrightarrow V(pk))\text{'}.$$

We are now ready to define the security requirement for impersonation against passive, active or concurrent attacks.

Definition 2. Let σ be a security parameter and let $\mathrm{IS} = (\mathrm{KG}, \mathrm{P}, \mathrm{V})$ be an identification scheme. For $x \in \{$ passive, active, concurrent $\}$, we say that IS is *secure against an impersonation attack of type* x if for any algorithm $A = (A_v, A_p)$, it holds that

$$\mathrm{Prob}\left[b \leftarrow Exp^{\mathrm{IS},A}_x(1^\sigma) \,:\, b = 1 \right] \leq \epsilon,$$

for some function ϵ negligible in σ.

Remarks and Performance Metrics. An identification scheme secure against a concurrent (resp., active) attack is also secure secure against active (resp., passive) attack. Following previous papers in the literature, we also pay special attention to minimize the time complexity of both prover and verifier algorithms, as well as the communication complexity of the identification scheme (i.e., the length of the messages exchanged during the identification subprotocol, as a function of the security parameter).

3 Preliminaries

We start our analysis by recalling two preliminary schemes that will be useful to introduce our results. First, we review the El-Gamal signature scheme [5], which is used in different ways in both identification schemes described in this paper. Second, we review a recent identification scheme in the standard model, proposed in [1] and denoted as Beth-SI-0, which is obtained as a variant of Beth's identification scheme in the identity-based model [6].

3.1 El-Gamal Signature Scheme

The El-Gamal signature scheme is one of the earliest and most influential digital signature schemes in the cryptography literature. We recall some notation and then describe the scheme.

Some notation. Let 1^σ be a security parameter and let l be a challenge length function over the positive integers. Also, let G be a cyclic multiplicative group, and let q, g denote its order and a generator, respectively. We say that G has

prime order if q is prime. We also say that a probabilistic polynomial-time algorithm Gen is a *prime-order cyclic multiplicative group generator*, if, on input 1^σ, generates a triple $(desc(G), q, g)$, where $desc(G)$ denotes the description of a prime-order cyclic multiplicative group G, q denotes its order and g is a generator of G.

The El Gamal signature scheme. We actually recall a variant of the original scheme, called *hashed-message El Gamal signature scheme* where the message is processed by hashing it into an element of $\mathbb{Z}_q$, using a collision-resistant hash function H. This scheme can be formally defined as a triple (KG, Sign, Verify) of efficient algorithms, which are, in turn, defined as follows.

The Algorithm KG: On input security parameter 1^σ, run the following instructions: let $(desc(G), q, g) \leftarrow \mathrm{Gen}(1^\sigma)$ and $x \leftarrow \mathbb{Z}_q$, set $y = g^x$, $pk = (desc(G), q, g, X)$ and $sk = (pk, x)$, and return: (pk, sk).

The Algorithm Sign: On input $sk = (pk, x)$ and message M, where $pk = (desc(G), q, g)$, run the following instructions: let $r \leftarrow \mathbb{Z}_q$, set $R = g^r$ and $s = r^{-1}(H(M) - xR) \bmod q$, and return: (R, s)

The Algorithm Verify: On input pk, M, sig, where $pk = (desc(G), q, g)$, and $sig = (R, s)$, check that $X^R R^s \equiv g^{H(M)}$. If yes, return: 1 otherwise return: 0.

The El Gamal signature scheme (without the hashing-based message preprocessing) was first presented in [5] and variants of it have been studied in several works. Yet another variant, consisting of preprocessing the message by computing $H(R, M)$ instead of $H(M)$, was studied in [19] and proved to be secure, in the random oracle model, assuming the intractability of computing discrete logarithms.

3.2 The Identification Scheme Beth-SI-0

The identification scheme proposed in [6] is an identity-based identification scheme. In [1] an approach was proposed to uniquely bind any one in a large class of identification schemes in the standard model (also called "convertible" identification schemes) to an identification scheme in the identity-based model. By using this approach, the authors in [1] surfaced an identification scheme in the standard model that is uniquely related to (a slightly more efficient and less general variant of) the identity-based identification scheme in [6]. They also proved this scheme to be secure against passive impersonation, assuming the universal unforgeability under no-message attack of the hashed-message El Gamal signature scheme [5]. We now give some notation and then recall the formal description of the Beth-SI-0=(KG0,P0,V0) scheme.

Description of the scheme. In Figure 2 we formally describe the identification scheme Beth-SI-0, based on any prime-order cyclic multiplicative group generator Gen and any challenge length function l.

KEY GENERATION ALGORITHM: On input security parameter 1^σ, run the following instructions:

1. let $(\text{desc}(G), q, g) \leftarrow \text{Gen}(1^\sigma)$;
2. let $r, x, h \leftarrow \mathbb{Z}_q$;
3. set $R \leftarrow g^r$, $X \leftarrow g^x$ and $s \leftarrow r^{-1}(h - Rx) \bmod q$;
4. set $pk = (1^\sigma, \text{desc}(G), q, g, X, h)$ and $sk = (pk, R, s)$;
5. return: (pk, sk).

IDENTIFICATION PROTOCOL.
Common input: security parameter 1^σ and public key pk.
P's private input: secret key sk.

P(round 1):
1. let $y \leftarrow \mathbb{Z}_q$;
2. set $Y = R^{-y}$ and send (R, Y) to V

V(round 2):
1. let $c \leftarrow \mathbb{Z}_{2^{l(\sigma)}}$ and send c to P

P(round 3):
1. set $z \leftarrow y + cs \bmod q$ and send z to V

V(decision): if $R, Y \in G$, $z \in \mathbb{Z}_q$, and $g^{ch} \equiv R^z Y X^{cR}$, then return: *accept* else return: *reject*.

Fig. 1. The modified Beth's standard identification scheme from [1]

Properties of the scheme. Informally speaking, in scheme Beth-SI-0, the interaction between the prover algorithm P0 and the verifier algorithm V0 can be shown to have two properties: (1) it is a proof of knowledge of an El-Gamal signature (R, s) of the message h in the user's public key pk; (2) it is a honest-verifier zero-knowledge proof of knowledge of the value s in the El-Gamal signature. Both properties have an important role in [1] to prove, in the random oracle model, that scheme Beth-SI-0 secure against passive impersonation assuming that the hashed-message ElGamal signature scheme is universally unforgeable under no-message attacks. However, the security of Beth-SI-0 against active and concurrent impersonation is left as an open problem in [1]. In the next section we define a minor variation of Beth-SI-0, resulting in scheme Beth-SI-1, being provable secure against active and concurrent impersonation, under appropriate assumptions.

Note that the El-Gamal signature (R, s) of h can be computed by algorithm P0 using the secret key sk. Two further aspects are worth mentioning as an introduction to the remaining schemes in the paper. First, the component R of the El-Gamal signature (R, s) is part of the secret key sk, and in different executions of scheme Beth-SI-0 the honest prover sends precisely R in the clear to the verifier (but a dishonest prover may choose to use a value $R' \neq R$ instead). Second, the prover algorithm P0 can run multiple executions of scheme Beth-SI-0 in polynomial time when using the same El-Gamal signature (R, s) as an auxiliary input.

In the scheme Beth-SI-1 that we analyze in Section 4, we slightly modify Beth-SI-0 precisely in these two aspects. Specifically, we simply move the value R from the secret key sk to the public key pk. One positive consequence from this modification is that a dishonest prover will be easily caught if using a value $R' \neq R$ during the identification protocol.

4 The Identification Scheme Beth-SI-1

In this section we present our modification to the identification scheme Beth-SI-0 in the standard model, as described in Section 3. The resulting scheme, Beth-SI-1, is proved to be secure against concurrent (and thus, active) impersonation under the one-more-dlog assumption. We obtain the following

Theorem 1. The identification scheme IS = Beth-SI-1 with group generator Gen and challenge length function l is secure against an impersonation attack of concurrent type, under a one-more-dlog assumption. Specifically, for any adversary A running in time t_A, there exists an adversary B running in time $t_A + (q+1) \cdot O(k^3)$, such that

$$\text{Prob}\left[Exp^{IS,A}_{concurrent}(1^\sigma) = 1 \right] \leq 2^{-l(\sigma)} + \text{Prob}\left[Exp^{B}_{omd}(1^\sigma) = 1 \right],$$

where σ denotes a security parameter, q is the number of sessions run by A, k is the length of group elements, experiment $Exp^{IS,A}_{concurrent}$ is defined in Section 2 and experiment Exp^{B}_{omd} is defined in Section 4.

In the rest of this section we prove Theorem 1. First we describe scheme Beth-SI-1, then we present a one-more-dlog assumption, and finally we prove the scheme's security under this assumption, as stated in the theorem.

Description of scheme Beth-SI-1. Scheme Beth-SI-1=(KG1,P1,V1) is almost identical to scheme Beth-SI-0. In particular, the interaction between the prover algorithm P1 and the verifier algorithm V1 keeps the same two above properties: (1) it is a proof of knowledge of an El-Gamal signature (R, s) of the message h in the user's public key pk; (2) it is a honest-verifier zero-knowledge proof of knowledge of the value s in the El-Gamal signature. The main difference is as follows: in KG0, the component R of the El-Gamal signature (R, s) is part of the secret key sk, and in different executions of scheme Beth-SI-0 the honest prover sends precisely R in the clear to the verifier (but a dishonest prover may choose to use a value $R' \neq R$). Instead, in KG1, the value R is part of the user's public key; thus, P1 does not need to send this value to V1 and in different executions of scheme Beth-SI-0 both the honest prover and a dishonest prover are bound to use precisely the same value R. For completeness, we still present the formal description of Beth-SI-1 in Figure 2 (here, we use the same notations as for scheme Beth-SI-0).

KEY GENERATION ALGORITHM: On input security parameter 1^σ, run the following instructions:

1. let $(\text{desc}(G), q, g) \leftarrow \text{Gen}(1^\sigma)$;
2. let $r, x, h \leftarrow \mathbb{Z}_q$;
3. set $R \leftarrow g^r$, $X \leftarrow g^x$ and $s \leftarrow r^{-1}(h - Rx) \bmod q$;
4. set $pk = (1^\sigma, \text{desc}(G), q, g, R, X, h)$ and $sk = (pk, s)$;
5. return: (pk, sk).

IDENTIFICATION PROTOCOL.
Common input: security parameter 1^σ and public key pk.
P's private input: secret key sk.

P(round 1):
1. let $y \leftarrow \mathbb{Z}_q$;
2. set $Y = R^{-y}$ and send Y to V

V(round 2):
1. let $c \leftarrow \mathbb{Z}_{2^{l(\sigma)}}$ and send c to P

P(round 3):
1. set $z \leftarrow y + cs \bmod q$ and send z to V

V(decision): if $R, Y \in G$, $z \in \mathbb{Z}_q$, and $g^{ch} \equiv R^z Y X^{cR}$, then return: *accept* else return: *reject*.

Fig. 2. The identification scheme Beth-SI-1 in the standard model

The performance properties of Beth-SI-1 are essentially the same as for Beth-SI-0. The only difference is in the communication complexity, as in Beth-SI-0, the prover sends 2 elements from group G, while in Beth-SI-1 the prover sends only 1. We now concentrate on the proof that this scheme is secure against concurrent impersonation under the one-more-dlog assumption. We start by reviewing the latter assumption.

Our One-More-Dlog Assumption. We use the same notations on groups as from the previous section. Informally speaking, the one-more-dlog assumption postulates the hardness of obtaining n discrete logarithms of n challenge values from group G, while the number of available queries to an oracle solving the discrete logarithm problem is strictly less than n. An assumption of this type (i.e., the one-more-RSA-inversion assumption) was first proposed in [2] and used there to prove the security of Chaum's blind signature scheme [9], and used in [4] to prove the security of the Guillou-Quisquater's digital signature scheme [17] under active and concurrent attacks. A one-more-dlog assumption was first used in [1], where it was used to prove the security of Schnorr's digital signature scheme [20] under active and concurrent attacks. Our one-more-dlog assumption considers an efficient adversary interacting with two oracles:

1. a *challenge oracle* C_G that, on input $(1^\sigma, desc(G), q, g)$ and an empty query $query = \perp$ from the adversary, returns a random value $W \in G$,