Security Enhancement of Identity-Based Identification with Reversibility

Atsushi Fujioka[1], Taiichi Saito[2], and Keita Xagawa[1]

[1] NTT Secure Platform Laboratories,
3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan
{fujioka.atsushi,xagawa.keita}@lab.ntt.co.jp
[2] Tokyo Denki University,
5 Senju Asahi-cho, Adachi-ku, Tokyo 120-8551, Japan
taiichi@c.dendai.ac.jp

Abstract. In this paper, we discuss security enhancement for a natural class of identity-based identification (IBI) protocols.

We first introduce *reversible Σ-type* IBI protocol, which is an extension of reversible identification protocol by Kurosawa and Heng.

We next propose a transformations from a reversible IBI protocol secure against static-identity and passive attacks to another one secure against adaptive-identity and (active and) concurrent attacks. The transformation requires no other cryptographic primitives and no additional number-theoretic assumptions, and the security proof is accomplished without the random oracles.

Keywords: identity-based identification, reversible Σ-type identification, impersonation under active and concurrent attacks.

1 Introduction

Identification is an important research topic in information and communication security, and *identity-based identification* (IBI) provides functionality of identification in *identity-based setting* [15]. The functionality is realized with a protocol between a *prover* and a *verifier*, where the prover wants to show the identity to the verifier, and the verifier needs not to have any other information related to the prover except the prover's identity. For engaging the protocol, IBI requires a *private key generator* (PKG) as other identity-based cryptographic primitives do so. The PKG publishes a public parameter to setup an identification system. It generates a secret key corresponding to a given identity of an entity, and gives the secret key to the entity. The entity performs identification with the given secret key. Thus, this concludes that IBI has three phases: Setup, Extract, and Identification.

Security of IBI protocols is defined by an experiment of an adversary who acts as (cheating) verifiers to gather much knowledge in the *learning phase* after the *setup phase* and then acts as a (cheating) prover to impersonate some entity in the *challenge phase*. We say that the protocol is secure when the probability that, in the experiment, the adversary succeeds in impersonation is negligible.

T.W. Chim and T.H. Yuen (Eds.): ICICS 2012, LNCS 7618, pp. 202–213, 2012.

The first security formulation for IBI was given by Kurosawa and Heng [11], and Bellare, Namprempre, and Neven provided formal descriptions of IBI [2].

A strong security notion of IBI protocols is defined as *security against impersonation under concurrent attacks* [3]. Roughly speaking, an adversary in the security model against impersonation under passive attacks (called imp-pa *model* [3]) is only allowed to eavesdrop communications in identification, though an adversary in the security model against impersonation under active attacks (called imp-aa *model* [3]) is allowed to *sequentially* access entities who prove their identities. If an identification protocol is secure against an adversary is allowed to *concurrently* access entities who prove their identities, it is said to be secure against impersonation under concurrent attacks (imp-ca *secure* [3]).

In addition, the security notions of IBI protocols are classified depending on selection of identities. The imp-atk security is also called *security against impersonation under adaptive-identity attacks* (adapt-id-imp-atk *security*) [2,14], where atk denotes a type of attacks such that $\mathsf{atk} \in \{\mathsf{pa}, \mathsf{aa}, \mathsf{ca}\}$. We can consider a weak version of the adapt-id-imp-atk security such that an adversary requests secret keys of identities only at the beginning of the learning phase, which is called *security against impersonation under static-identity attacks* (stat-id-imp-atk *security*) [14].

Security Enhancement of Identity-Based Identification. Along with these formulations, a few security enhancement techniques have been investigated [7,14]. A well-known OR-proof technique [7] enhances the security of standard identification protocols from the passive security to the concurrent security. Moreover, it is applicable also to IBI protocols, if the underlying IBI protocol is *Σ-type* [8], which is a similar property to *Σ-protocol* [6]. Furthermore, Rückert proposed another security enhancement technique which can convert a stat-id-imp-atk secure IBI protocol to an imp-atk secure IBI protocol where atk denotes a type of attacks such that $\mathsf{atk} \in \{\mathsf{pa}, \mathsf{aa}, \mathsf{ca}\}$ [14]. The technique is applicable to any IBI protocols, however, it needs a chameleon hash function [10] as an additional cryptographic primitive.

Though both the techniques do not require the random oracles [4] for their security proofs, a chameleon hash function is still necessary when we convert a stat-id-imp-pa secure IBI protocol to an adapt-id-imp-ca secure one combining the OR-proof technique and the Rückert technique. To the best of our knowledge, there is no security enhancement transformation from a stat-id-imp-pa secure IBI protocol to an adapt-id-imp-ca secure one without an additional primitive.

Our Contributions. We first introduce *reversible Σ-type* IBI protocol, which is an extension of reversible identification protocol by Kurosawa and Heng [12]. When we apply the identity-based construction [2] to a reversible identification [12], we obtain a reversible Σ-type IBI protocol. We also note that many IBI protocols from signature schemes in [11] are reversible Σ-type.

We next propose a transformations from a stat-id-imp-pa secure reversible IBI protocol to another adapt-id-imp-ca secure one. The transformation requires no other cryptographic primitives and no additional number-theoretic assumptions, and the security proof is accomplished without the random oracles.

Organization. We give a definition of identity-based identification and a related notion in **Section 2**. **Section 3** provides a security enhancement technique, its security proof and discussions with the related works.

2 Definitions

In this section, we present a definition of identity-based identification (IBI) protocols and introduce a property similar to Σ-type [8]. We adopt the definition of IBI protocols in [2].

Identity-Based Identification. We adopt the definition of IBI protocols in [2]. Let $\mathsf{IBI} = (\mathsf{SetUp}, \mathsf{KG}, \mathsf{P}, \mathsf{V})$ be an IBI protocol, where SetUp is the master-key-generation algorithm that on input 1^κ outputs *mpk* and *msk*, KG is the user-key-generation algorithm that on input (mpk, msk, id) outputs sk_{id}, P is the prover algorithm that, taking inputs *mpk*, *id* and sk_{id}, interacts with V, and V is the verifier algorithm that, taking inputs *mpk* and *id*, interacts with P and finally outputs $dec \in \{accept, reject\}$.

The PKG uses SetUp to generate master public key *mpk* and secret key *msk*, publicizes *mpk* and keeps *msk* secret. It also uses KG to generate a secret key sk_{id} for the entity of an identity *id*. The entity having *id* uses P, as a prover. The prover interacts with another entity who uses V as a verifier to convince the verifier that the identity is *id*. If both the entities correctly follows the protocol, V outputs *accept*.

We describe the formal definitions of security of IBI based on the following experiments $\mathbf{Exp}^{\mathsf{adapt\text{-}id\text{-}imp\text{-}atk}}_{\mathsf{IBI},\mathcal{I}}(\kappa)$ between a challenger and an impersonator $\mathcal{I} = (\mathsf{CV}, \mathsf{CP})$, where atk denotes a type of attacks such that $\mathsf{atk} \in \{\mathsf{pa}, \mathsf{aa}, \mathsf{ca}\}$.

Experiment $\mathbf{Exp}^{\mathsf{adapt\text{-}id\text{-}imp\text{-}atk}}_{\mathsf{IBI},\mathcal{I}}(\kappa)$**:**

Setup Phase: The challenger obtains $(mpk, msk) \leftarrow \mathsf{SetUp}(1^\kappa)$ and initializes HU, CU, TU, $PS \leftarrow \emptyset$, where HU, CU, and TU denote the sets of honest users, corrupted users, and target users, respectively, and PS denotes the set of provers' sessions. The impersonator CV is given the security parameter 1^κ and the master public key *mpk*.

Learning Phase: The impersonator CV can query to the oracles Init, Corr and Conv when $\mathsf{atk} = \mathsf{pa}$, and also to Prov when $\mathsf{atk} = \{\mathsf{aa}, \mathsf{ca}\}$. Note that $id \notin HU \setminus TU$ means that *id* is target user, corrupted user, or non-initiated user.

- The oracle Init receives input *id*. If $id \in HU \cup CU \cup TU$, then Init returns $\perp$. Otherwise, it obtains $sk_{id} \leftarrow \mathsf{KG}(mpk, msk, id)$, adds *id* to HU, and provides CV with *id*.
- The oracle Corr receives input *id*. If $id \notin HU \setminus TU$, then Corr returns $\perp$. Otherwise, it adds *id* to CU, deletes *id* from HU, and returns sk_{id} to CV.

- The oracle Conv receives input id. If $id \notin HU$, then Conv returns $\perp$. Otherwise it returns a transcript of a transaction between the prover with identity id and a verifier.
- (only when $\mathsf{atk} = \mathsf{aa}$) The oracle Prov receives inputs id, s, and M_{in}. If $id \notin HU \setminus TU$, then Prov returns $\perp$. Otherwise if $PS = \emptyset$, it sets $PS = \{(id, s)\}$, picks a random coin ρ, and sets a state of the prover $st_{\mathsf{P}}[(id, s)] \leftarrow (mpk,\ sk_{id},\ \rho)$. Next, it obtains $(M_{out},\ st_{\mathsf{P}}[(id, s)]) \leftarrow \mathsf{P}(M_{in},\ st_{\mathsf{P}}[(id, s)])$. Finally, it returns M_{out}. If M_{out} is the final message of the protocol, Prov sets $PS \leftarrow \emptyset$.
- (only when $\mathsf{atk} = \mathsf{ca}$) The oracle Prov receives inputs id, s, and M_{in}. If $id \notin HU \setminus TU$, then Prov returns $\perp$. If $(id, s) \notin PS$, then it adds (id, s) to PS, picks a random coin ρ, and sets a state of the prover $st_{\mathsf{P}}[(id, s)] \leftarrow (mpk,\ sk_{id},\ \rho)$. Next, it obtains $(M_{out},\ st_{\mathsf{P}}[(id, s)]) \leftarrow \mathsf{P}(M_{in},\ st_{\mathsf{P}}[(id, s)])$. Finally, it returns M_{out}.

Challenge Phase: CV outputs a target identity id^* and st_{CP}. If id^* is not in HU then the challenger outputs 0 and halts. Otherwise, the challenger sets $TU \leftarrow \{id^*\}$, and gives st_{CP} to CP. CP can query to the oracles Init, Corr, and Conv, (and Prov when $\mathsf{atk} = \mathsf{aa}$ or ca) as in the learning phase. Finally, the challenger obtains $(tr,\ dec) \leftarrow \mathbf{Run}[\mathsf{CP}(st_{\mathsf{CP}})^{\textsc{Init},\textsc{Corr},\textsc{Conv}(,\textsc{Prov})} \leftrightarrow \mathsf{V}(mpk,\ id^*)]$ and outputs dec.

In the case of $\mathsf{atk} = \mathsf{aa}$, the Prov oracle allows only a single session at a time. On the other hand, in the case of $\mathsf{atk} = \mathsf{ca}$, it allows multiple sessions at the same time.

Definition 2.1. *Let* $\mathsf{IBI} = (\mathsf{SetUp},\ \mathsf{KG},\ \mathsf{P},\ \mathsf{V})$ *be an IBI protocol and* $\mathcal{I} = (\mathsf{CV},\ \mathsf{CP})$ *an impersonator. Let* κ *be a security parameter. The advantage of* $\mathcal{I}$ *in attacking* IBI *is defined by*

$$\mathbf{Adv}_{\mathsf{IBI},\mathcal{I}}^{\textsf{adapt-id-imp-atk}}(\kappa) := \Pr\left[\ \mathbf{Exp}_{\mathsf{IBI},\mathcal{I}}^{\textsf{adapt-id-imp-atk}}(\kappa) = accept\ \right].$$

We say that an IBI protocol, IBI, *is* secure against impersonation under adaptive-identity and concurrent attacks (adapt-id-imp-ca secure) *if* $\mathbf{Adv}_{\mathsf{IBI},\mathcal{I}}^{\textsf{adapt-id-imp-ca}}(\kappa)$ *is negligible for every polynomial-time impersonator* $\mathcal{I}$, *is* secure against impersonation under adaptive-identity and active attacks (adapt-id-imp-aa secure) *if* $\mathbf{Adv}_{\mathsf{IBI},\mathcal{I}}^{\textsf{adapt-id-imp-aa}}(\kappa)$ *is negligible for every polynomial-time impersonator* $\mathcal{I}$, *and is* secure against impersonation under adaptive-identity and passive attacks (adapt-id-imp-pa secure) *if* $\mathbf{Adv}_{\mathsf{IBI},\mathcal{I}}^{\textsf{adapt-id-imp-pa}}(\kappa)$ *is negligible for every polynomial-time impersonator* $\mathcal{I}$.

According to [14], we also describe a weaker security definition of IBI based on the following experiments $\mathbf{Exp}_{\mathsf{IBI},\mathcal{I}}^{\textsf{stat-id-imp-atk}}(\kappa)$ ($\mathsf{atk} \in \{\mathsf{pa},\ \mathsf{aa},\ \mathsf{ca}\}$) between a challenger and an impersonator $\mathcal{I} = (\mathsf{CV},\ \mathsf{CP})$.

Experiment $\mathbf{Exp}_{\mathsf{IBI},\mathcal{I}}^{\textsf{stat-id-imp-atk}}(\kappa)$**:**

Setup Phase: At the beginning of this phase, the impersonator CV issues a single corruption query $(id_1,\ \ldots,\ id_t)$ to the challenger before seeing master public key. The challenger is given the security parameter 1^κ, obtains $(mpk, msk) \leftarrow \mathsf{SetUp}(1^\kappa)$, and computes $sk_{id_i} \leftarrow \mathsf{KG}(mpk, msk, id_i)$ for all i $(1 \leq i \leq t)$. It sets $CU \leftarrow \{id_1, id_2, \ldots, id_t\}$ and then returns $(sk_{id_1}, \ldots, sk_{id_t})$ to CV. The challenger initializes HU, TU, $PS \leftarrow \emptyset$. The impersonator CV is given the security parameter 1^κ and the master public key mpk.

Learning and Challenge Phases: The learning and challenge phases are defined as the same way as those in the experiments $\mathbf{Exp}^{\mathsf{adapt\text{-}id\text{-}imp\text{-}atk}}_{\mathsf{IBI},\mathcal{I}}(\kappa)$, except that the impersonator $\mathcal{I}$ is not allowed to additional queries to Corr during these phases.

Definition 2.2. *Let* $\mathsf{IBI} = (\mathsf{SetUp}, \mathsf{KG}, \mathsf{P}, \mathsf{V})$ *be an IBI protocol and* $\mathcal{I} = (\mathsf{CV}, \mathsf{CP})$ *an impersonator. Let* κ *be a security parameter. The advantage of* $\mathcal{I}$ *in attacking* IBI *is defined by*

$$\mathbf{Adv}^{\mathsf{stat\text{-}id\text{-}imp\text{-}atk}}_{\mathsf{IBI},\mathcal{I}}(\kappa) := \Pr\left[\ \mathbf{Exp}^{\mathsf{stat\text{-}id\text{-}imp\text{-}atk}}_{\mathsf{IBI},\mathcal{I}}(\kappa) = accept\ \right].$$

We say that IBI *is* secure against impersonation under static-identity and concurrent attacks ($\mathsf{stat\text{-}id\text{-}imp\text{-}ca}$ secure) *if* $\mathbf{Adv}^{\mathsf{stat\text{-}id\text{-}imp\text{-}ca}}_{\mathsf{IBI},\mathcal{I}}(\kappa)$ *is negligible for every polynomial-time* $\mathcal{I}$*, is* secure against impersonation under static-identity and active attacks ($\mathsf{stat\text{-}id\text{-}imp\text{-}aa}$ secure) *if* $\mathbf{Adv}^{\mathsf{stat\text{-}id\text{-}imp\text{-}aa}}_{\mathsf{IBI},\mathcal{I}}(\kappa)$ *is negligible for every polynomial-time* $\mathcal{I}$*, and is* secure against impersonation under static-identity and passive attacks ($\mathsf{stat\text{-}id\text{-}imp\text{-}pa}$ secure) *if* $\mathbf{Adv}^{\mathsf{stat\text{-}id\text{-}imp\text{-}pa}}_{\mathsf{IBI},\mathcal{I}}(\kappa)$ *is negligible for every polynomial-time* $\mathcal{I}$.

Reversible Σ-Type IBI Protocol. We define an analogue of Σ-protocols in the context of IBI protocols. Let $\mathsf{IBI} = (\mathsf{SetUp}, \mathsf{KG}, \mathsf{P}, \mathsf{V})$ be an identity-based identification protocol.

Suppose that communication between P and V is realized by the following three-move protocol through which five polynomial-time algorithms $(\Sigma_{\mathsf{ibi\text{-}gnc}}, \Sigma_{\mathsf{ibi\text{-}cmt}}, \Sigma_{\mathsf{ibi\text{-}clg}}, \Sigma_{\mathsf{ibi\text{-}rsp}}, \Sigma_{\mathsf{ibi\text{-}chk}})$ are used, and that $\Sigma_{\mathsf{ibi\text{-}cmt}}$, $\Sigma_{\mathsf{ibi\text{-}rsp}}$, and $\Sigma_{\mathsf{ibi\text{-}chk}}$ are deterministic.

$\mathsf{P} \rightarrow \mathsf{V}$**:** P computes $r \leftarrow \Sigma_{\mathsf{ibi\text{-}gnc}}(mpk, id)$, $x = \Sigma_{\mathsf{ibi\text{-}cmt}}(mpk, id, r)$ and sends x to V.

$\mathsf{V} \rightarrow \mathsf{P}$**:** V computes $c \leftarrow \Sigma_{\mathsf{ibi\text{-}clg}}(mpk, id)$ and sends c to P.

$\mathsf{P} \rightarrow \mathsf{V}$**:** P computes $y = \Sigma_{\mathsf{ibi\text{-}rsp}}(mpk, id, sk_{id}, r, c)$ and sends y to V.

V**:** V outputs *accept* if $x = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk, id, c, y)$ holds, and, *reject* otherwise.

Let $\textsc{Rnd}_{(mpk,id)}$ denote a set $\{r \mid r \leftarrow \Sigma_{\mathsf{ibi\text{-}gnc}}(mpk, id)\}$, and assume that r is uniformly distributed over $\textsc{Rnd}_{(mpk,id)}$.

We call this type of three-move IBI protocols *canonical*, and moreover, we call an IBI protocol IBI *reversible Σ-type* if it is canonical and satisfies three properties: *y-uniformity*, *special soundness*, *special commitment*, and *special response.*

y-Uniformity: Let $\textsc{Res}_{(mpk,id)}$ be a set $\{y \mid y \leftarrow \Sigma_{\mathsf{ibi\text{-}rsp}}(mpk, id, sk_{id}, r, c), c \leftarrow \Sigma_{\mathsf{ibi\text{-}clg}}(mpk, id), r \in \textsc{Rnd}_{(mpk,id)}\}$. For any fixed (mpk, id, sk_{id}, c),

$y = \Sigma_{\mathsf{ibi\text{-}rsp}}(mpk,\ id,\ sk_{id},\ r,\ c)$ is uniformly distributed over $\mathrm{Res}_{(mpk,id)}$ if r is uniformly distributed over $\mathrm{Rnd}_{(mpk,id)}$.

Special Soundness: We can compute the user secret key sk_{id} for an identity id from mpk, id and two accepting transcripts $(x,\ c,\ y)$ and $(x,\ \tilde{c},\ \tilde{y})$ such that $c \neq \tilde{c}$. That is, there is a polynomial-time algorithm $\Sigma_{\mathsf{ibi\text{-}ext}}$ that takes as inputs mpk, id and two transcripts $(x,\ c,\ y)$ and $(x,\ \tilde{c},\ \tilde{y})$ satisfying $x = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ id,\ c,\ y) = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ id,\ \tilde{c},\ \tilde{y})$ and $c \neq \tilde{c}$, and outputs sk_{id}.

Special Commitment: We can compute r from mpk, id, sk_{id}, c, y such that $\Sigma_{\mathsf{ibi\text{-}cmt}}(mpk,\ id,\ r) = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ id,\ c,\ y)$. That is, there is a polynomial-time algorithm $\Sigma_{\mathsf{ibi\text{-}rvs}}$ that takes as inputs mpk, id, sk_{id}, c, and y, and outputs r.

Special Response: We can generate y only from mpk and id such that for some r and c, $\Sigma_{\mathsf{ibi\text{-}cmt}}(mpk,\ id,\ r) = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ id,\ c,\ y)$ holds, and the generated y is randomly and uniformly distributed over $\mathrm{Res}_{(mpk,id)}$. That is, there is a polynomial-time algorithm $\Sigma_{\mathsf{ibi\text{-}gnr}}$ that takes as inputs mpk and id, and outputs y.

Note that the y-uniformity and special response properties imply the following *special zero-knowledge* property.

Special Zero-Knowledge: We can obtain an accepting transcript from a challenge c, mpk and id. That is, there is a polynomial-time algorithm $\Sigma_{\mathsf{ibi\text{-}sim}}$ that takes on inputs mpk, id and c such that $c \leftarrow \Sigma_{\mathsf{ibi\text{-}clg}}(mpk,\ id)$, runs $y \leftarrow \Sigma_{\mathsf{ibi\text{-}gnr}}(mpk,\ id)$ and $x \leftarrow \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ id,\ c,\ y)$, and outputs $(x,\ y)$. The distribution of transcripts generated by $\Sigma_{\mathsf{ibi\text{-}clg}}$ and $\Sigma_{\mathsf{ibi\text{-}sim}}$ is indistinguishable from that of real transcripts.

3 Proposed Security Enhancement Transformations

3.1 Description

Here we propose a generic transformation that converts any stat-id-imp-pa secure reversible Σ-type IBI protocol into an adapt-id-imp-ca secure IBI one. We note that, in conversion, x and id are treated as challenges. Our transformation modifies a three-move transaction $(x,\ c,\ y)$ of the underlying protocol into another three-move one $((X',\ Y',\ X''),\ c,\ (x,\ y,\ Y''))$ such that $Y' \leftarrow \Sigma_{\mathsf{ibi\text{-}gnr}}(mpk,\ \tilde{id})$, $X' = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ \tilde{id},\ id,\ Y')$, $Y'' \leftarrow \Sigma_{\mathsf{ibi\text{-}gnr}}(mpk,\ \tilde{id})$, and $X'' = \Sigma_{\mathsf{ibi\text{-}chk}}(mpk,\ \tilde{id},\ x,\ Y'')$, where $\tilde{id}$ is a fixed string called *master identity* and is a part of master public key for the constructed IBI protocol.

Let $\mathsf{IBI}' = (\mathsf{SetUp}',\ \mathsf{KG}',\ \mathsf{P}',\ \mathsf{V}')$ be a reversible Σ-type IBI protocol, where $(\mathsf{P}',\ \mathsf{V}')$ is realized by $(\Sigma'_{\mathsf{ibi\text{-}gnc}},\ \Sigma'_{\mathsf{ibi\text{-}cmt}},\ \Sigma'_{\mathsf{ibi\text{-}clg}},\ \Sigma'_{\mathsf{ibi\text{-}rsp}},\ \Sigma'_{\mathsf{ibi\text{-}chk}})$ and the y-uniformity, special soundness, and special commitment properties are shown by $(\Sigma'_{\mathsf{ibi\text{-}gnr}},\ \Sigma'_{\mathsf{ibi\text{-}ext}},\ \Sigma'_{\mathsf{ibi\text{-}rvs}})$.

From this Σ-type IBI protocol IBI', we construct another IBI protocol $\mathsf{IBI} = (\mathsf{SetUp},\ \mathsf{KG},\ \mathsf{P},\ \mathsf{V})$ as follows.

SetUp: It takes as input 1^κ, runs $(mpk',\ msk') \leftarrow \mathsf{SetUp}'(1^\kappa)$, $(mpk'',\ msk'') \leftarrow \mathsf{SetUp}'(1^\kappa)$, chooses a master identity $\tilde{id}$, and outputs $(mpk,\ msk) = ((mpk',\ mpk'',\ \tilde{id}),\ msk')$.

KG: It takes as input (mpk, msk, id), parses mpk and msk as $mpk = (mpk', mpk'', \tilde{id})$ and $msk = msk'$, respectively, runs $Y'_{id} \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk'', \tilde{id})$, $X'_{id} = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, id, Y'_{id})$, $sk'_{id} \leftarrow \mathsf{KG}'(mpk', msk', X'_{id})$ and outputs $sk_{id} = (sk'_{id}, X'_{id}, Y'_{id})$.

P: P takes as input (mpk, id, sk_{id}), and parses mpk and sk_{id} as $mpk = (mpk', mpk'', \tilde{id})$ and $sk_{id} = (sk'_{id}, X'_{id}, Y'_{id})$, respectively.

V: V takes as input (mpk, id), and parses mpk as $mpk = (mpk', mpk'', \tilde{id})$.

$\mathsf{P} \rightarrow \mathsf{V}$: P computes $r \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnc}}(mpk', X'_{id})$, $x = \Sigma'_{\mathsf{ibi\text{-}cmt}}(mpk', X'_{id}, r)$, $Y'' \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk'', \tilde{id})$, $X'' = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, x, Y'')$, and sends (X'_{id}, Y'_{id}, X'') to V.

$\mathsf{V} \rightarrow \mathsf{P}$: V computes $c \leftarrow \Sigma'_{\mathsf{ibi\text{-}clg}}(mpk', X'_{id})$ and sends c to P.

$\mathsf{P} \rightarrow \mathsf{V}$: P computes $y = \Sigma'_{\mathsf{ibi\text{-}rsp}}(mpk', X'_{id}, sk'_{id}, r, c)$ and sends (x, y, Y'') to V.

V: V outputs *accept* if $x = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk', X'_{id}, c, y)$, $X'_{id} = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, id, Y'_{id})$ and $X'' = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, x, Y'')$ hold, and, *reject* otherwise.

SETUP

$\mathsf{SetUp}(1^\kappa)$

$(mpk', msk') \leftarrow \mathsf{SetUp}'(1^\kappa)$
$(mpk'', msk'') \leftarrow \mathsf{SetUp}'(1^\kappa)$
choose a master identity $\tilde{id}$
output $(mpk, msk) = ((mpk', mpk'', \tilde{id}), msk')$

EXTRACT

$\mathsf{KG}(mpk, msk, id)$

$mpk = (mpk', mpk'', \tilde{id})$
$msk = msk'$
$Y'_{id} \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk'', \tilde{id})$
$X'_{id} = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, id, Y'_{id})$
$sk'_{id} \leftarrow \mathsf{KG}'(mpk', msk', X'_{id})$
outputs $sk_{id} = (sk'_{id}, X'_{id}, Y'_{id})$

IDENTIFICATION

$\mathsf{P}(mpk, id, sk_{id})$		$\mathsf{V}(mpk, id)$
$mpk = (mpk', mpk'', \tilde{id})$		$mpk = (mpk', mpk'', \tilde{id})$
$sk_{id} = (sk'_{id}, X'_{id}, Y'_{id})$		
$r \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnc}}(mpk', X'_{id})$		
$x = \Sigma'_{\mathsf{ibi\text{-}cmt}}(mpk', X'_{id}, r)$		
$Y'' \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk'', \tilde{id})$		
$X'' = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, x, Y'')$	(X'_{id}, Y'_{id}, X'')	
	$\longrightarrow$	$c \leftarrow \Sigma'_{\mathsf{ibi\text{-}clg}}(mpk', X'_{id})$
	c	
$y = \Sigma'_{\mathsf{ibi\text{-}rsp}}(mpk', X'_{id}, sk_{id}, r, c)$	$\longleftarrow$	
	(x, y, Y'')	
	$\longrightarrow$	check $x = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk', X'_{id}, c, y)$,
		$X'_{id} = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, id, Y'_{id})$, and
		$X'' = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, x, Y'')$
		output *accept* if all hold;
		otherwise, output *reject*

Fig. 1. Proposed Transformation

3.2 Security

In this section, we show that the proposed transformation can enhance the security of reversible Σ-type IBI protocols from the security against impersonation under static-identity and passive attacks (i.e., stat-id-imp-pa security) to the security against impersonation under adaptive-identity and (active and) concurrent attacks (i.e., adapt-id-imp-ca security).

Theorem 3.1. *If there exists a* stat-id-imp-pa *secure reversible Σ-type IBI protocol, then there exists an* adapt-id-imp-ca *secure IBI protocol.*

Proof (Sketch). Suppose that there exists an adapt-id-imp-ca impersonator, $\mathcal{I} = (\mathsf{CV}, \mathsf{CP})$, against IBI. We construct a stat-id-imp-pa impersonator, $\mathcal{I}' = (\mathsf{CV}', \mathsf{CP}')$, against IBI'. Here we outline the construction.

Suppose that $\mathcal{I}'$ obtains two accepting transcripts $((X'_{id^*}, Y'_{id^*}, X''), c, (x, y, Y''))$ and $((X'_{id^*}, Y'_{id^*}, X''), \tilde{c}, (\tilde{x}, \tilde{y}, \tilde{Y}''))$ by rewinding $\mathcal{I}$. There are two cases that (A) $x \neq \tilde{x}$ or (B) $x = \tilde{x}$. We call the impersonator $\mathcal{I}$ that makes the former and latter transcripts a type A and type B impersonator, respectively.

From Type A Impersonator: We first describe the case that $\mathcal{I}$ is a type A impersonator, because it is easier. In the setup phase of the static-identity experiment, $\mathcal{I}'$ issues no corruption query to its stat-id-imp-pa challenger. $\mathcal{I}'$ receives mpk_e from the challenger. It generates $(mpk_s, msk_s) \leftarrow \mathsf{SetUp}'(1^\kappa)$, chooses $\tilde{id}$, and sets $mpk' = mpk_s$, $mpk'' = mpk_e$, and $mpk = (mpk', mpk'', \tilde{id})$. $\mathcal{I}'$ starts the experiment with the impersonator $\mathcal{I}$ by feeding mpk.

In the learning phase, since $\mathcal{I}'$ has msk', it can generate sk'_{id} and then sk_{id}. Thus, $\mathcal{I}'$ can perfectly simulate the oracles.

In the challenge phase, $\mathcal{I}$ declares the target identity id^*, and then, $\mathcal{I}'$ declares $\tilde{id}$ as the target identity. $\mathcal{I}'$ rewinds $\mathcal{I}$ and obtains two transcripts $((X'_{id^*}, Y'_{id^*}, X''), c, (x, y, Y''))$ and $((X'_{id^*}, Y'_{id^*}, X''), \tilde{c}, (\tilde{x}, \tilde{y}, \tilde{Y}''))$. We can classify the transcripts into two cases: If X'_{id^*} has already been generated for a distinct identity $id \neq id^*$, then $\mathcal{I}'$ obtains two accepting transcripts under mpk'' and $\tilde{id}$, that is, $(X'_{id^*}, id^*, Y'_{id^*})$ and (X'_{id}, id, Y'_{id}) with $X'_{id^*} = X'_{id}$. $\mathcal{I}'$ can extract $sk_{\tilde{id}}$ from the two transcripts due to the special soundness property, and wins the stat-id-imp-pa experiment. Otherwise, it has the transcripts for distinct x and $\tilde{x}$. It extracts $sk_{\tilde{id}}$ from the two accepting transcripts, (X'', x, Y'') and $(X'', \tilde{x}, \tilde{Y}'')$ under mpk'' and $\tilde{id}$ due to the special soundness property, and wins the stat-id-imp-pa experiment.

From Type B Impersonator: We next consider the case that $\mathcal{I}$ is a type B impersonator. Let Q be an upperbound of the number of the INIT queries from $\mathcal{I}$. In the setup phase of the static-identity experiment, $\mathcal{I}'$ generates $(mpk_s, msk_s) \leftarrow \mathsf{SetUp}'(1^\kappa)$, chooses $\tilde{id}$, and sets $mpk'' = mpk_s$. $\mathcal{I}'$ then guesses $i^* \in \{1, \ldots, Q\}$ such that in the i^*-th INIT query, $\mathcal{I}$ initializes the target identity id^*. Next, $\mathcal{I}'$ generates $sk''_{\tilde{id}} \leftarrow \mathsf{KG}'(mpk'', msk'', \tilde{id})$. $\mathcal{I}'$ generates Q random identities id'_i $(1 \leq i \leq Q)$, converts id'_i to X'_i with $\hat{Y}_i$ using mpk'', and issues a corruption query $(X'_1, \ldots, X'_{i^*-1}, X'_{i^*+1}, \ldots, X'_Q)$ to the challenger. Then $\mathcal{I}'$ receives the secret keys $(sk'_1, \ldots, sk'_{i^*-1}, sk'_{i^*+1}, \ldots, sk'_Q)$ for $(X'_1, \ldots, X_{i^*-1},$

X_{i^*+1}, …, X'_Q) and the master public key mpk_e. It sets $mpk' = mpk_e$ and sets $mpk = (mpk', mpk'', \tilde{id})$ (see Fig. 2). $\mathcal{I}'$ starts the experiment with $\mathcal{I}$ by feeding mpk.

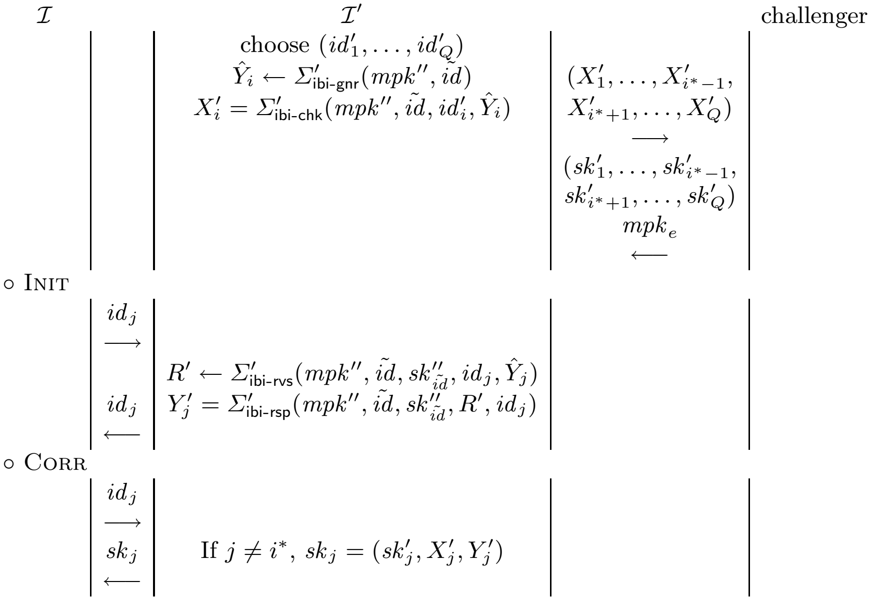
$\mathcal{I}$
$\mathcal{I}'$
challenger
choose $(id'_1, \ldots, id'_Q)$
$\hat{Y}_i \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk'', \tilde{id})$
$X'_i = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, id'_i, \hat{Y}_i)$
$(X'_1, \ldots, X'_{i^*-1}, X'_{i^*+1}, \ldots, X'_Q)$ $\longrightarrow$
$(sk'_1, \ldots, sk'_{i^*-1}, sk'_{i^*+1}, \ldots, sk'_Q)$
mpk_e $\longleftarrow$
∘ Init
id_j $\longrightarrow$
$R' \leftarrow \Sigma'_{\mathsf{ibi\text{-}rvs}}(mpk'', \tilde{id}, sk''_{\tilde{id}}, id_j, \hat{Y}_j)$
$Y'_j = \Sigma'_{\mathsf{ibi\text{-}rsp}}(mpk'', \tilde{id}, sk''_{\tilde{id}}, R', id_j)$
id_j $\longleftarrow$
∘ Corr
id_j $\longrightarrow$
If $j \neq i^*$, $sk_j = (sk'_j, X'_j, Y'_j)$
sk_j $\longleftarrow$

Fig. 2. Sketch of Init and Corr oracle simulation

In the learning phase, $\mathcal{I}'$ answers the oracle queries as follows: On an Init query id_j, $\mathcal{I}$ computes Y'_j such that $X'_j = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, id_j, Y'_j)$ by using $\Sigma'_{\mathsf{ibi\text{-}rvs}}$ and $\Sigma'_{\mathsf{ibi\text{-}rsp}}$. On a Corr query id, if $id = id_{i^*}$ then $\mathcal{I}$ aborts. Otherwise, since $id = id_j$ for $j \neq i^*$, $\mathcal{I}$ can return $sk_{id} = (sk'_j, X'_j, Y'_j)$ (see Fig. 2).

On a Prov query id_i ($id_i \neq id_{i^*}$), $\mathcal{I}$ answers the query by using $sk_{id} = (sk'_i, X'_i, Y'_i)$. The problem arises on id_{i^*}, since $\mathcal{I}'$ does not have sk'_{i^*}. Even in this case, $\mathcal{I}'$ can simulate id_{i^*} by using $sk''_{\tilde{id}}$. Given id_{i^*} with a session s, then it simulates the conversation $(\hat{x}, \hat{c}, \hat{y})$ and the commitment X'' of $\hat{x}$, and returns $(X'_{i^*}, Y'_{i^*}, X'')$. On the query (id_{i^*}, s, c), it newly generates the conversation (x, c, y) and computes a decommitment Y'' by using $sk''_{\tilde{id}}$ and x. Then, it returns (x, y, Y'') (see Fig. 3).

In the challenge phase of the inner experiment, $\mathcal{I}$ declares the target identity id^*. We see that $id^* = id_{i^*}$ occurs with probability $1/Q$. Otherwise, $\mathcal{I}'$ aborts. $\mathcal{I}'$ randomly chooses two challenges c and $\tilde{c}$ and obtains two transcripts $((X'_{id^*}, Y'_{id^*}, X''), c, (x, y, Y''))$ and $((X'_{id^*}, Y'_{id^*}, X''), \tilde{c}, (\tilde{x}, \tilde{y}, \tilde{Y}''))$. Suppose that both transcripts are accepted. If X'_{id^*} equals to X'_i for $i \neq i^*$, then $\mathcal{I}'$ aborts. If $x \neq \tilde{x}$ then $\mathcal{I}'$ aborts. Otherwise, $\mathcal{I}'$ obtains two accepting transcripts (x, c, y) and $(x, \tilde{c}, \tilde{y})$ under mpk' and $X'_{id^*} = X'_{i^*}$. Due to the special soundness, $\mathcal{I}'$

$$\begin{array}{l|c|l}
\multicolumn{1}{c}{\mathcal{I}} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\mathcal{I}'} \\
\circ\ \textsc{Prov} & & \\
 & id_{i^*} & \\
 & \longrightarrow & \hat{c} \leftarrow \Sigma'_{\mathsf{ibi\text{-}clg}}(mpk', X'_{i^*}) \\
 & & \hat{y} \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk', X'_{i^*}) \\
 & & \hat{x} = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk', X'_{i^*}, \hat{c}, \hat{y}) \\
 & & \hat{Y} \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk'', \tilde{id}) \\
 & (X'_{i^*}, Y'_{i^*}, X'') & X'' = \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk'', \tilde{id}, \hat{x}, \hat{Y}) \\
 & \longleftarrow & \\
 & & \\
 & c & \\
 & \longrightarrow & y \leftarrow \Sigma'_{\mathsf{ibi\text{-}gnr}}(mpk', X'_{i^*}) \\
 & & x \leftarrow \Sigma'_{\mathsf{ibi\text{-}chk}}(mpk', X'_{i^*}, c, y) \\
 & & R \leftarrow \Sigma'_{\mathsf{ibi\text{-}rvs}}(mpk'', \tilde{id}, sk''_{\tilde{id}}, x, \hat{Y}) \\
 & (x, y, Y'') & Y'' = \Sigma'_{\mathsf{ibi\text{-}rsp}}(mpk'', \tilde{id}, sk''_{\tilde{id}}, R, x) \\
 & \longleftarrow &
\end{array}$$

Fig. 3. Sketch of Prov oracle simulation on id_{i^*}

can extract sk_{i^*}. Then, $\mathcal{I}'$ declares X'_{i^*} as the target identity and can win the stat-id-imp-pa experiment. □

Due to page limitation, the proof of Theorem 3.1 is given in the final version of this paper.

3.3 Discussions

On Reversible Σ-Type Protocols. Kurosawa and Heng [12] defined a *reversible* property for identification protocols, and showed the conversion of the reversible identification protocol to trapdoor commitment scheme and vice versa. They also constructed an online/offline signature scheme, directly combining a signature scheme and a reversible identification protocol [12, Section 5]. The constructed scheme has smaller size of public keys than that of a scheme based on the Shamir-Tauman construction [16], which simply combines a signature scheme and a trapdoor commitment scheme.

Canetti et al. [5] defined *augmented Σ-protocol*, which is an extension of Σ-protocol for proving knowledge for some relation and has a property similar to "reversible" for standard identification. They then construct an identity-based trapdoor commitment scheme [1] from any signature scheme with an augmented Σ-protocol.

From a *reversible Σ-type* IBI protocol, which is an extension of reversible identification protocol [12], we can construct a trapdoor commitment scheme. In addition, we can construct a multi-trapdoor commitment [9], identity-based trapdoor commitment [1], simulation-sound trapdoor commitment [13], and non-malleable trapdoor commitment [13] from it.

We observe that many IBI protocols fall into reversible Σ-type. Kurosawa and Heng [12] noted that many practical identification protocols have the reversible property. Applying to the reversible identification protocol the certificate-based construction by Bellare, Namprempre, and Neven [2], which constructs an IBI protocol from an identification protocol and a digital signature scheme, we obtain a reversible Σ-type IBI protocol. We also note that the Kurosawa-Heng construction [11] can convert a signature scheme with an augmented Σ-protocol into a reversible Σ-type IBI protocol.

On Security Enhancements. It is known that a trapdoor commitment scheme enhances the security of IBI protocol from the static-identity setting to the adaptive-identity setting [14]. Consequently we may apply the constructed trapdoor commitment to the IBI protocol in order to enhance its security.

However, we present a transformation that converts a stat-id-imp-pa secure IBI protocol to an adapt-id-imp-ca secure one. In this transformation, an instance of an underlying IBI protocol is directly combined with another instance of the same IBI protocol, instead of constructing multi-trapdoor commitment and simply combining it with IBI protocol. The obtained IBI protocol attains more efficiency than the one by simple combination of the underlying IBI protocol with the multi-trapdoor commitment schemes, as well as we see in the construction of online/offline signature schemes in [12].

Yang et al. [17] presented a construction of IBI protocols secure under weak-selective-identity attacks in the standard model. In this paper, we discuss only security under adaptive-identity and static-identity attacks (adapt-id-imp-atk and stat-id-imp-atk), not weak-selective-identity attacks. In [8], it is shown that security under weak-selective-identity attacks is not stronger than stat-id-imp-atk security, and stat-id-imp-atk security is not stronger than adapt-id-imp-atk security.

4 Conclusion

We introduced *reversible Σ-type* IBI protocol, which is an extension of reversible identification protocol by Kurosawa and Heng [12]. Then, we proposed a security enhancement technique for reversible Σ-type identity-based identification protocols. The proposed transformation can convert a stat-id-imp-pa secure IBI protocol to an adapt-id-imp-ca secure one. It requires no other cryptographic primitives and no additional assumptions, and the security proof is done without the random oracles.

References

1. Ateniese, G., de Medeiros, B.: Identity-Based Chameleon Hash and Applications. In: Juels, A. (ed.) FC 2004. LNCS, vol. 3110, pp. 164–180. Springer, Heidelberg (2004)
2. Bellare, M., Namprempre, C., Neven, G.: Security proofs for identity-based identification and signature schemes. Journal of Cryptology 22(1), 1–61 (2009); A preliminary version appeared in EUROCRYPT 2004 (2004)

3. Bellare, M., Palacio, A.: GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 162–177. Springer, Heidelberg (2002)
4. Bellare, M., Rogaway, P.: Random oracle are practical: A paradigm for designing efficient protocols. In: CCS 1993, pp. 62–73. ACM (1993)
5. Canetti, R., Dodis, Y., Pass, R., Walfish, S.: Universally Composable Security with Global Setup. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 61–85. Springer, Heidelberg (2007), http://eprint.iacr.org/2006/432
6. Cramer, R.: Modular Design of Secure, yet Practical Cryptographic Protocols. PhD thesis, University of Amsterdam (1996)
7. Feige, U., Shamir, A.: Witness indistinguishable and witness hiding protocols. In: STOC 1990, pp. 416–426. ACM (1990)
8. Fujioka, A., Saito, T., Xagawa, K.: Security Enhancements by OR-Proof in Identity-Based Identification. In: Bao, F., Samarati, P., Zhou, J. (eds.) ACNS 2012. LNCS, vol. 7341, pp. 135–152. Springer, Heidelberg (2012)
9. Gennaro, R.: Multi-trapdoor Commitments and Their Applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 220–236. Springer, Heidelberg (2004)
10. Krawczyk, H., Rabin, T.: Chameleon signatures. In: NDSS 2000, pp. 143–154. Internet Society (2000)
11. Kurosawa, K., Heng, S.-H.: From Digital Signature to ID-based Identification/Signature. In: Bao, F., Deng, R.H., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 248–261. Springer, Heidelberg (2004)
12. Kurosawa, K., Heng, S.-H.: The power of identification schemes. International Journal of Applied Cryptography (IJACT) 1(1), 60–69 (2008); A preliminary version appeared in PKC 2006 (2006)
13. MacKenzie, P., Yang, K.: On Simulation-Sound Trapdoor Commitments. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 382–400. Springer, Heidelberg (2004)
14. Rückert, M.: Adaptively Secure Identity-Based Identification from Lattices without Random Oracles. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 345–362. Springer, Heidelberg (2010)
15. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
16. Shamir, A., Tauman, Y.: Improved Online/Offline Signature Schemes. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 355–367. Springer, Heidelberg (2001)
17. Yang, G., Chen, J., Wong, D.S., Deng, X., Wang, D.: A new framework for the design and analysis of identity-based identification schemes. Theoretical Computer Science 407(1-3), 370–388 (2008); A preliminary version appeared ACNS 2007 (2007)