Logging-independent Message Anonymity in the Relational Method

Pasquale Noce
Software Engineer at HID Global, Italy
pasquale dot noce dot lavoro at gmail dot com
pasquale dot noce at hidglobal dot com

May 26, 2024

Abstract

In the context of formal cryptographic protocol verification, logging-independent message anonymity is the property for a given message to remain anonymous despite the attacker's capability of mapping messages of that sort to agents based on some intrinsic feature of such messages, rather than by logging the messages exchanged by legitimate agents as with logging-dependent message anonymity.

This paper illustrates how logging-independent message anonymity can be formalized according to the relational method for formal protocol verification by considering a real-world protocol, namely the Restricted Identification one by the BSI. This sample model is used to verify that the pseudonymous identifiers output by user identification tokens remain anonymous under the expected conditions.

Contents

1 Logging-independent message anonymity and Restricted Identification

theory *Definitions*
imports *Main*
begin

1.1 Introduction

Logging-dependent message anonymity is the property for a message exchanged or otherwise used in a cryptographic protocol to remain anonymous although the attacker can log the messages generated or accepted by legitimate agents, and map any two observable messages contained in any such message to the same agent. An approach to modeling and verifying this security property according to the *relational method* for formal protocol verification has been described in [7], along with the method itself. This approach makes use of two further type constructors for messages, *IDInfo* and *Log*, as well as of two functions, *crypts* and *key-sets*. Particularly, *IDInfo* is used to model message anonymity, while the remaining constants are used to formalize the property for a message to be observable by the spy within some logged message.

Logging-independent message anonymity rather is the property for a given message to remain anonymous in spite of the attacker's capability of mapping messages of that sort to agents without resorting to message logging, namely by means of some intrinsic feature of such messages. From the above observation, it follows that *IDInfo* is the sole anonymity-related constant required if the only kind of anonymity of interest for a given protocol is the logging-independent one, whereas *Log*, *crypts*, and *key-sets* are unnecessary and can be left out of the model. It is also possible to include both kinds of anonymity in the model, in which case some protocol rule will enable the spy to map messages of some sort to agents only if they are observable within logged messages, while some other protocol rule will enable the spy to do so independently of this condition.

This paper illustrates how logging-independent message anonymity can be formalized according to the relational method by considering a real-world protocol, namely the Restricted Identification one by the BSI [1] [2], whose very purpose is to allow for the exchange of messages endowed with this security property.

1.2 Case study: the Restricted Identification protocol

The Restricted Identification protocol enables *user identification tokens* (e.g. electronic documents) to generate and output unambiguous *pseudonymous identifiers*, distinct for any given group of terminals of arbitrary granularity,

referred to as a *sector*, and usable to identify the tokens across different sessions taking place within the same sector. For example, such identifiers allow for the creation of sector-specific revocation lists, at the same time preserving the anonymity of the holder of any token included in such a list.

This protocol is based on a *Public Key Infrastructure (PKI)* comprising the token issuer, which owns a *revocation key pair* (SK_{Rev}, PK_{Rev}) and generates a *token key pair* (SK_{Tok}, PK_{Tok}) for each token, and sectors, each one endowed with its own *sector key pair* (SK_{Sec}, PK_{Sec}), where $PK_{Sec} = [SK_{Sec}]PK_{Rev}$. This PKI may use either an integer finite field or an elliptic curve group, as long as the selected domain parameters are cryptographically secure. In a real-world PKI, each sector has actually two distinct key pairs, which enables the tokens to generate as many different pseudonymous identifiers per sector, but this detail is irrelevant to the anonymity of such identifiers and can then be omitted from the model.

According to [1] [2], the Restricted Identification protocol may only be executed using the session keys established via Chip Authentication version 2/3, after performing Terminal Authentication version 2 with a terminal certificate containing both sector public keys' hashes (including domain parameters), whose authenticity is ensured by the certificate's signature. After requesting to start the protocol, which again is irrelevant and can be left out of the model, the terminal sends either of its sector public keys PK_{Sec} (including domain parameters) to the token, which in turn verifies that PK_{Sec}'s hash matches the one contained in the certificate and replies with its pseudonymous identifier $H([SK_{Tok}]PK_{Sec})$, where H is a hash function. If necessary (for instance, to insert it into a sector-specific revocation list), this identifier can be recomputed in the external world as $H([SK_{Sec}]([SK_{Rev}]PK_{Tok}))$, with the concurrence of both the token issuer and the entity responsible for the involved sector.

As a matter of fact, since the only purpose of the protocol model to be developed is to verify the logging-independent anonymity of token pseudonymous identifiers, without any confidentiality or authenticity concern, it is sufficient to model a simpler protocol in which the terminal and the token exchange their messages in plain, without using any session key. Moreover, since both Chip and Terminal Authentication are out of scope, the Restricted Identification protocol will be modeled as a stand-alone one. Consequently, although both of them are exchanged during Terminal Authentication in the real-world protocol, PK_{Sec}'s signature will be assumed to be exchanged with PK_{Sec} in the model, while the related verification key will be assumed to be known by the token a priori. The hash function used to sign PK_{Sec} may differ from the one used to compute token pseudonymous identifiers, but once more, this is just an omissible functional detail.

A further simplification, admissible for the same reason, is to let the token use domain parameters known a priori rather than the input ones, whose

presence in the input message can then be left out. Indeed, this prevents the spy from snatching SK_{Tok} by making an element of a smaller group pass for an authentic sector public key, which could be done by signing it with a compromised signature generation key. For example, if the PKI used a group of 128-bit order, SK_{Tok} could be disclosed by first searching the private key SK'_{Tok} associated with a fake identifier ranging in a group of 64-bit order n, and then detecting SK_{Tok} as the unique private key associated with a given genuine identifier among all those differing from SK'_{Tok} by a multiple of n. So, two searches within as many spaces of 2^{64} elements, which is a computationally feasible task nowadays, would suffice to find SK_{Tok}. However, such *small group attacks* can safely be ruled out as long as the initial state s_0 comprises an arbitrary set of compromised token private keys, given that verifying the conditions under which these keys remain secret is out of scope.

As a result of all the simplifications described above, the protocol that is going to be modeled is as follows.

1. Terminal $\rightarrow$ Token: $\{PK_{Sec}, \{H(PK_{Sec})\}_{SK_{Sign}}\}$

   The terminal sends the token a message consisting of its sector public key and a precomputed signature of this key.

2. Token $\rightarrow$ Terminal: $H([SK_{Tok}]PK_{Sec})$

   The token verifies that the hash of the received public key matches the signed one, and then replies with the pseudonymous identifier resulting from this key.

Unless it is compromised by means other than attacking the protocol, the anonymity of a given token pseudonymous identifier $H([SK_{Tok}]PK_{Sec})$ is expected to be vulnerable if and only if either SK_{Tok} is anonymity-compromised, or SK_{Sec} is compromised and there is another compromised sector private key SK'_{Sec} such that $H([SK_{Tok}]PK'_{Sec})$ is anonymity-compromised. In fact, the spy can detect the use of SK_{Tok} in $H([SK_{Tok}]PK_{Sec})$ in the former case, whereas in the latter one he can map $H([SK_{Tok}]PK_{Sec})$ to the same token as $H([SK_{Tok}]PK'_{Sec})$ by recognizing that $[SK_{Tok}]PK_{Sec} = [SK_{Sec} \times (SK'_{Sec})^{-1}]([SK_{Tok}]PK'_{Sec})$.

The purpose of the following formal development is precisely to formally prove the correctness of this expectation. In more detail, the *only if* conditional implied by the previous statement will be proven as an *anonymity property* in the next section, while the *if* conditional will be proven in the form of two *possibility properties* in the subsequent one. Since both relevant

attack options leverage the intrinsic features of token pseudonymous identifiers, namely the private keys used to generate them, logging-independent message anonymity has to be considered rather than logging-dependent one.

For further information about the formal definitions and proofs contained in this paper, see Isabelle documentation, particularly [6], [5], [3], and [4].

1.3 Agents, messages, protocol rules

Agents consist of an infinite population of tokens and sectors, identified through natural numbers, plus the spy. Actually, the model can safely ignore terminals altogether and assume that tokens are presented to sectors as a whole, since all the terminal-side messages used in the protocol refer to sectors rather than to individual terminals. The only possible exceptions are signature key pairs. In fact, although the entity signing terminal certificates is the same for every terminal in a given sector (in [1] and [2], it is named *Document Verifier*), nothing prevents that entity to use distinct signature generation keys for different terminals (for example, if their certificates are issued at different times). Nonetheless, the granularity of signature key pairs is irrelevant to the anonymity of token pseudonymous identifiers according to the previous considerations, so these key pairs can be associated with sectors as well.

As opposed to what happens in [7], there is no correlation here between any two agents *Token* n and *Sector* n marked with the same numeric identifier n. In fact, tokens and sectors are independent of each other, and any token may be presented to whatever sector.

type-synonym *agent-id* = *nat*

datatype *agent* =
  Token agent-id |
  Sector agent-id |
  Spy

As regards the key pairs for key agreement, private keys are identified by natural numbers, whereas public keys by sets of natural numbers. The implied interpretation is that *PubK S* stands for public key $[k]G$, where G is the group generator and k is the modular product of all the private keys referred to by the numeric identifiers in S, each one occurring as a factor exactly once. Using *multisets* of natural numbers instead of sets would have allowed private keys to be used as factors even more than once, but this option can be left out as the PKI does not provide for any public key computed in this way. The need for this ad hoc message format, like those used to represent session keys and Chip Authentication Data in [7],

confirms that reuse of the spy's capabilities' model in the inductive method is hindered by the likely need for ad hoc message formats in case of protocols using nontrivial public key cryptography [7].

Besides key agreement keys, messages comprise signature generation/verification keys (identified by the numeric identifiers of the respective sectors), hash values, cryptograms, and compound messages built via message concatenation. Furthermore, message anonymity is modeled by means of constructor *IDInfo* [7]. Since the anonymity of terminal-side messages is of no concern, the interpretation of message $\langle n,\ X\rangle$ is "message X is mapped to *Token* n", namely n is always interpreted as a token's numeric identifier rather than a sector's one.

type-synonym *key-id* = *nat*

datatype *agr-key* =
  PriK key-id |
  PubK key-id set

datatype *enc-key* =
  SigK agent-id |
  VerK agent-id

datatype *msg* =
  AgrKey agr-key |
  EncKey enc-key |
  Hash msg |
  Crypt enc-key msg |
  MPair msg msg |
  IDInfo agent-id msg

syntax
  -MPair :: ['*a*, *args*] ⇒ '*a* ∗ '*b* ((2{|-,/ -|}))
  -IDInfo :: [*agent-id*, *msg*] ⇒ *msg* ((2⟨-,/ -⟩))
translations
  {|*X*, *Y*, *Z*|} ⇌ {|*X*, {|*Y*, *Z*|}|}
  {|*X*, *Y*|} ⇌ *CONST MPair X Y*
  ⟨*n*, *X*⟩ ⇌ *CONST IDInfo n X*

abbreviation *SigKey* :: *agent-id* ⇒ *msg* **where**
SigKey ≡ *EncKey* ∘ *SigK*

abbreviation *VerKey* :: *agent-id* ⇒ *msg* **where**
VerKey ≡ *EncKey* ∘ *VerK*

abbreviation *PriKey* :: *key-id* ⇒ *msg* **where**
PriKey ≡ *AgrKey* ∘ *PriK*

abbreviation *PubKey* :: *key-id set* ⇒ *msg* **where**
PubKey ≡ *AgrKey* ∘ *PubK*

primrec *InvK* :: *enc-key* ⇒ *enc-key* **where**
InvK (*SigK n*) = *VerK n* |
InvK (*VerK n*) = *SigK n*

abbreviation *InvKey* :: *enc-key* ⇒ *msg* **where**
InvKey ≡ *EncKey* ∘ *InvK*

inductive-set *parts* :: *msg set* ⇒ *msg set*
for *H* :: *msg set* **where**

parts-used [*intro*]:
X ∈ *H* ⟹ *X* ∈ *parts H* |

parts-crypt [*intro*]:
Crypt K X ∈ *parts H* ⟹ *X* ∈ *parts H* |

parts-fst [*intro*]:
{|*X*, *Y*|} ∈ *parts H* ⟹ *X* ∈ *parts H* |

parts-snd [*intro*]:
{|*X*, *Y*|} ∈ *parts H* ⟹ *Y* ∈ *parts H*

definition *parts-msg* :: *msg* ⇒ *msg set* **where**
parts-msg X ≡ *parts* {*X*}

Constant *Rev-PriK* is the numeric identifier of the revocation private key, while functions *Sec-PriK* and *Tok-PriK* map the numeric identifiers of sectors and tokens to those of the respective sector/token private keys. It is assumed that these functions are injective, as well as that their ranges do not contain *Rev-PriK* and are disjoint, and such axioms are proven to be consistent by showing that there exist three constants satisfying all of them. On the whole, these axioms just model the assumption that private keys are generated by cryptographically secure means throughout the PKI, so that the probability for any given private key to occur more than once within the PKI is negligible.

consts *Rev-PriK* :: *key-id*

consts *Sec-PriK* :: *agent-id* ⇒ *key-id*

consts *Tok-PriK* :: *agent-id* ⇒ *key-id*

specification (*Rev-PriK Sec-PriK Tok-PriK*)
sec-prik-inj: *inj Sec-PriK*
tok-prik-inj: *inj Tok-PriK*
sec-prik-rev: *Rev-PriK* $\notin$ *range Sec-PriK*
tok-prik-rev: *Rev-PriK* $\notin$ *range Tok-PriK*
sec-prik-tok-prik: *range Sec-PriK* $\cap$ *range Tok-PriK* = {}
by (*rule exI* [*of* - *0*], *rule exI* [*of* - $\lambda n.\ n + n + 1$],
rule exI [*of* - $\lambda n.\ n + n + 2$], *auto simp*: *inj-on-def*, *arith*)

abbreviation *Gen-PubKey* :: *msg* **where**
Gen-PubKey $\equiv$ *PubKey* {}

abbreviation *Rev-PriKey* :: *msg* **where**
Rev-PriKey $\equiv$ *PriKey Rev-PriK*

abbreviation *Rev-PubKey* :: *msg* **where**
Rev-PubKey $\equiv$ *PubKey* {*Rev-PriK*}

abbreviation *Tok-PriKey* :: *agent-id* $\Rightarrow$ *msg* **where**
Tok-PriKey n $\equiv$ *PriKey* (*Tok-PriK n*)

abbreviation *Tok-PubKey* :: *agent-id* $\Rightarrow$ *msg* **where**
Tok-PubKey n $\equiv$ *PubKey* {*Tok-PriK n*}

abbreviation *Sec-PriKey* :: *agent-id* $\Rightarrow$ *msg* **where**
Sec-PriKey n $\equiv$ *PriKey* (*Sec-PriK n*)

abbreviation *Sec-PubKey* :: *agent-id* $\Rightarrow$ *msg* **where**
Sec-PubKey n $\equiv$ *PubKey* {*Sec-PriK n*, *Rev-PriK*}

abbreviation *Sign* :: *agent-id* $\Rightarrow$ *msg* $\Rightarrow$ *msg* **where**
Sign n X $\equiv$ *Crypt* (*SigK n*) (*Hash X*)

abbreviation *ID* :: *agent-id* $\Rightarrow$ *msg* $\Rightarrow$ *msg* **where**
ID n X $\equiv$ *case X of AgrKey* (*PubK S*) $\Rightarrow$ *PubKey* (*insert* (*Tok-PriK n*) *S*)

The spy's starting knowledge, as defined by the initial state s_0, consists of the following messages.

- All the public keys used in the PKI (including the group generator).
- All token pseudonymous identifiers (in both hashed and non-hashed formats).
- Compromised private keys used in the PKI (excluding the revocation one, assumed to be secret).

- Mappings of all token public keys, compromised token private keys, and anonymity-compromised token pseudonymous identifiers (in both hashed and non-hashed formats) to the respective tokens.

consts *bad-sigk* :: *agent-id set*

consts *bad-sec-prik* :: *agent-id set*

consts *bad-tok-prik* :: *agent-id set*

consts *bad-id* :: (*agent-id* × *agent-id*) *set*

type-synonym *event* = *agent* × *msg*

type-synonym *state* = *event set*

abbreviation *used* :: *state* ⇒ *msg set* **where**
used s ≡ *Range s*

abbreviation *spied* :: *state* ⇒ *msg set* **where**
spied s ≡ *s* `` {*Spy*}

abbreviation s_0 :: *state* **where**
s_0 ≡ {*Spy*} × ({*Gen-PubKey*, *Rev-PubKey*} ∪
SigKey ‘ *bad-sigk* ∪ *Sec-PriKey* ‘ *bad-sec-prik* ∪ *Tok-PriKey* ‘ *bad-tok-prik* ∪
range VerKey ∪ *range Sec-PubKey* ∪ *range Tok-PubKey* ∪
range (λ(*n*, *m*). *ID n* (*Sec-PubKey m*)) ∪
range (λ(*n*, *m*). *Hash* (*ID n* (*Sec-PubKey m*))) ∪
range (λ*n*. ⟨*n*, *Tok-PubKey n*⟩) ∪
{⟨*n*, *Tok-PriKey n*⟩ | *n*. *n* ∈ *bad-tok-prik*} ∪
{⟨*n*, *ID n* (*Sec-PubKey m*)⟩ | *n m*. (*n*, *m*) ∈ *bad-id*} ∪
{⟨*n*, *Hash* (*ID n* (*Sec-PubKey m*))⟩ | *n m*. (*n*, *m*) ∈ *bad-id*})

Protocol rules are defined here below. Particularly, for any public key $[SK_1 \times ... \times SK_n]G$ known to the spy, they enable him to generate public key $[SK_1 \times ... \times SK_n \times SK_{n+1}]G$ for any additional, compromised private key SK_{n+1}, as well as public key $[SK_1 \times ... \times SK_{i-1} \times SK_{i+1} \times ... \times SK_n]G$ for any compromised private key SK_i, where $1 \leq i \leq n$ (which is equivalent to multiplying the original public key by $(SK_i)^{-1}$). The spy can also map the resulting public keys to the same token, if identified, as the original public key, in the latter case as long as the related token private key still occurs as a factor in the resulting modular product. Furthermore, the spy can associate a token with any known public key whose modular product of private keys contains the corresponding token private key as a factor, provided that this key is compromised.

abbreviation *rel-sector* :: (*state* × *state*) *set* **where**
rel-sector ≡ {(*s*, *s'*) | *s s' m*.
s' = *s* ∪ {*Sector m*, *Spy*} × {{|*Sec-PubKey m*, *Sign m* (*Sec-PubKey m*)|}}}

abbreviation *rel-token* :: (*state* × *state*) *set* **where**
rel-token ≡ {(*s*, *s'*) | *s s' m n S*.
s' = *s* ∪ {*Token n*, *Spy*} × {*Hash* (*ID n* (*PubKey S*))} ∧
{|*PubKey S*, *Sign m* (*PubKey S*)|} ∈ *used s*}

abbreviation *rel-pubk-less* :: (*state* × *state*) *set* **where**
rel-pubk-less ≡ {(*s*, *s'*) | *s s' A S*.
s' = *insert* (*Spy*, *PubKey* (*S* − {*A*})) *s* ∧
{*PriKey A*, *PubKey S*} ⊆ *spied s*}

abbreviation *rel-pubk-more* :: (*state* × *state*) *set* **where**
rel-pubk-more ≡ {(*s*, *s'*) | *s s' A S*.
s' = *insert* (*Spy*, *PubKey* (*insert A S*)) *s* ∧
{*PriKey A*, *PubKey S*} ⊆ *spied s*}

abbreviation *rel-hash* :: (*state* × *state*) *set* **where**
rel-hash ≡ {(*s*, *s'*) | *s s' X*.
s' = *insert* (*Spy*, *Hash X*) *s* ∧
X ∈ *spied s*}

abbreviation *rel-dec* :: (*state* × *state*) *set* **where**
rel-dec ≡ {(*s*, *s'*) | *s s' K X*.
s' = *insert* (*Spy*, *X*) *s* ∧
{*Crypt K X*, *InvKey K*} ⊆ *spied s*}

abbreviation *rel-enc* :: (*state* × *state*) *set* **where**
rel-enc ≡ {(*s*, *s'*) | *s s' K X*.
s' = *insert* (*Spy*, *Crypt K X*) *s* ∧
{*X*, *EncKey K*} ⊆ *spied s*}

abbreviation *rel-sep* :: (*state* × *state*) *set* **where**
rel-sep ≡ {(*s*, *s'*) | *s s' X Y*.
s' = *s* ∪ {*Spy*} × {*X*, *Y*} ∧
{|*X*, *Y*|} ∈ *spied s*}

abbreviation *rel-con* :: (*state* × *state*) *set* **where**
rel-con ≡ {(*s*, *s'*) | *s s' X Y*.
s' = *insert* (*Spy*, {|*X*, *Y*|}) *s* ∧
{*X*, *Y*} ⊆ *spied s*}

abbreviation *rel-id-pubk-less* :: (*state* × *state*) *set* **where**
rel-id-pubk-less ≡ {(*s*, *s'*) | *s s' n A S*.

$s' = insert\ (Spy, \langle n, PubKey\ (S - \{A\})\rangle)\ s \wedge$
$\{PriKey\ A, PubKey\ (S - \{A\}), \langle n, PubKey\ S\rangle\} \subseteq spied\ s \wedge$
$Tok\text{-}PriK\ n \in S - \{A\}\}$

abbreviation *rel-id-pubk-more* :: $(state \times state)\ set$ **where**
$rel\text{-}id\text{-}pubk\text{-}more \equiv \{(s, s') \mid s\ s'\ n\ A\ S.$
$s' = insert\ (Spy, \langle n, PubKey\ (insert\ A\ S)\rangle)\ s \wedge$
$\{PriKey\ A, PubKey\ (insert\ A\ S), \langle n, PubKey\ S\rangle\} \subseteq spied\ s\}$

abbreviation *rel-id-pubk-prik* :: $(state \times state)\ set$ **where**
$rel\text{-}id\text{-}pubk\text{-}prik \equiv \{(s, s') \mid s\ s'\ n\ S.$
$s' = insert\ (Spy, \langle n, PubKey\ S\rangle)\ s \wedge$
$\{Tok\text{-}PriKey\ n, PubKey\ S\} \subseteq spied\ s \wedge$
$Tok\text{-}PriK\ n \in S\}$

abbreviation *rel-id-hash* :: $(state \times state)\ set$ **where**
$rel\text{-}id\text{-}hash \equiv \{(s, s') \mid s\ s'\ n\ X.$
$s' = s \cup \{Spy\} \times \{\langle n, X\rangle, \langle n, Hash\ X\rangle\} \wedge$
$\{X, Hash\ X\} \subseteq spied\ s \wedge$
$(\langle n, X\rangle \in spied\ s \vee \langle n, Hash\ X\rangle \in spied\ s)\}$

definition *rel* :: $(state \times state)\ set$ **where**
$rel \equiv rel\text{-}sector \cup rel\text{-}token \cup rel\text{-}pubk\text{-}less \cup rel\text{-}pubk\text{-}more \cup$
$rel\text{-}hash \cup rel\text{-}dec \cup rel\text{-}enc \cup rel\text{-}sep \cup rel\text{-}con \cup$
$rel\text{-}id\text{-}pubk\text{-}less \cup rel\text{-}id\text{-}pubk\text{-}more \cup rel\text{-}id\text{-}pubk\text{-}prik \cup rel\text{-}id\text{-}hash$

abbreviation *in-rel* :: $state \Rightarrow state \Rightarrow bool$ (**infix** $\vdash$ *60*) **where**
$s \vdash s' \equiv (s, s') \in rel$

abbreviation *in-rel-rtrancl* :: $state \Rightarrow state \Rightarrow bool$ (**infix** $\models$ *60*) **where**
$s \models s' \equiv (s, s') \in rel^*$

end

2 Anonymity of token pseudonymous identifiers

theory *Anonymity*
imports *Definitions*
begin

This section contains a proof of anonymity property *id-anonymous*, which states that a token pseudonymous identifier remains anonymous if its anonymity is not compromised by means other than attacking the protocol and neither attack option described in section 1.2 is viable. As shown here below, this property can be proven by applying rules *rtrancl-induct* and *rtrancl-start* in a suitable combination [7].

proposition *rtrancl-start* [*rule-format*]:
$(x,\ y) \in r^* \Longrightarrow P\ y \longrightarrow \neg\ P\ x \longrightarrow$
$(\exists\, u\ v.\ (x,\ u) \in r^* \wedge (u,\ v) \in r \wedge (v,\ y) \in r^* \wedge \neg\ P\ u \wedge P\ v)$
(**is** - $\Longrightarrow$ - $\longrightarrow$ - $\longrightarrow$ $(\exists\, u\ v.\ ?P_2\ x\ y\ u\ v)$)
proof (*erule rtrancl-induct*, *simp*, (*rule impI*)+)
fix *y z*
assume
A: $(x,\ y) \in r^*$ **and**
B: $(y,\ z) \in r$ **and**
C: $P\ z$
assume $P\ y \longrightarrow \neg\ P\ x \longrightarrow (\exists\, u\ v.\ ?P_2\ x\ y\ u\ v)$ **and** $\neg\ P\ x$
hence *D*: $P\ y \longrightarrow (\exists\, u\ v.\ ?P_2\ x\ y\ u\ v)$ **by** *simp*
show $\exists\, u\ v.\ ?P_2\ x\ z\ u\ v$
proof (*cases* $P\ y$)
case *True*
with *D* **obtain** *u v* **where** $?P_2\ x\ y\ u\ v$ **by** *blast*
moreover from *this* **and** *B* **have** $(v,\ z) \in r^*$ **by** *auto*
ultimately show *?thesis* **by** *blast*
next
case *False*
with *A* **and** *B* **and** *C* **have** $?P_2\ x\ z\ y\ z$ **by** *simp*
thus *?thesis* **by** *blast*
qed
qed

proposition *state-subset*:
$s \models s' \Longrightarrow s \subseteq s'$
by (*erule rtrancl-induct*, *auto simp add*: *rel-def image-def*)

proposition *spied-subset*:
$s \models s' \Longrightarrow spied\ s \subseteq spied\ s'$
by (*rule Image-mono*, *erule state-subset*, *simp*)

proposition *parts-init*:
$parts\ (used\ s_0) = used\ s_0$
by (*rule equalityI*, *rule-tac* [!] *subsetI*, *erule-tac* [*2*] *parts-used*,
erule parts.induct, *auto*)

proposition *parts-idem* [*simp*]:
$parts\ (parts\ H) = parts\ H$
by (*rule equalityI*, *rule subsetI*, *erule parts.induct*, *auto*)

proposition *parts-mono*:
$H \subseteq H' \Longrightarrow parts\ H \subseteq parts\ H'$
by (*rule subsetI*, *erule parts.induct*, *auto*)

lemma *parts-union-1*:

parts $(H \cup H') \subseteq$ *parts* $H \cup$ *parts* H'
by (*rule subsetI*, *erule parts.induct*, *auto*)

lemma *parts-union-2*:
parts $H \cup$ *parts* $H' \subseteq$ *parts* $(H \cup H')$
by (*rule subsetI*, *erule UnE*, *erule-tac* [!] *parts.induct*, *auto*)

proposition *parts-union* [*simp*]:
parts $(H \cup H') =$ *parts* $H \cup$ *parts* H'
by (*rule equalityI*, *rule parts-union-1*, *rule parts-union-2*)

proposition *parts-insert*:
parts (*insert* X H) = *parts-msg* $X \cup$ *parts* H
by (*simp only*: *insert-def parts-union*, *subst parts-msg-def*, *simp*)

proposition *parts-msg-mono*:
$X \in H \Longrightarrow$ *parts-msg* $X \subseteq$ *parts* H
by (*subgoal-tac* $\{X\} \subseteq H$, *subst parts-msg-def*, *erule parts-mono*, *simp*)

proposition *parts-msg-agrkey* [*simp*]:
parts-msg (*AgrKey* K) = $\{$*AgrKey* $K\}$
by (*subst parts-msg-def*, *rule equalityI*, *rule subsetI*, *erule parts.induct*, *auto*)

proposition *parts-msg-hash* [*simp*]:
parts-msg (*Hash* X) = $\{$*Hash* $X\}$
by (*subst parts-msg-def*, *rule equalityI*, *rule subsetI*, *erule parts.induct*, *auto*)

lemma *parts-crypt-1*:
parts $\{$*Crypt* K $X\}$ $\subseteq$ *insert* (*Crypt* K X) (*parts* $\{X\}$)
by (*rule subsetI*, *erule parts.induct*, *auto*)

lemma *parts-crypt-2*:
insert (*Crypt* K X) (*parts* $\{X\}$) $\subseteq$ *parts* $\{$*Crypt* K $X\}$
by (*rule subsetI*, *simp*, *erule disjE*, *blast*, *erule parts.induct*, *auto*)

proposition *parts-msg-crypt* [*simp*]:
parts-msg (*Crypt* K X) = *insert* (*Crypt* K X) (*parts-msg* X)
by (*simp add*: *parts-msg-def*, *rule equalityI*, *rule parts-crypt-1*, *rule parts-crypt-2*)

lemma *parts-mpair-1*:
parts $\{\{\!|X,\ Y|\!\}\} \subseteq$ *insert* $\{\!|X,\ Y|\!\}$ (*parts* $\{X\} \cup$ *parts* $\{Y\}$)
by (*rule subsetI*, *erule parts.induct*, *auto*)

lemma *parts-mpair-2*:
insert $\{\!|X,\ Y|\!\}$ (*parts* $\{X\} \cup$ *parts* $\{Y\}$) $\subseteq$ *parts* $\{\{\!|X,\ Y|\!\}\}$
by (*rule subsetI*, *simp*, *erule disjE*, *blast*, *erule disjE*, *erule-tac* [!] *parts.induct*, *auto*)

proposition *parts-msg-mpair* [*simp*]:
parts-msg $\{\!|X,\ Y|\!\} = insert\ \{\!|X,\ Y|\!\}\ (parts\text{-}msg\ X \cup parts\text{-}msg\ Y)$
by (*simp add*: *parts-msg-def*, *rule equalityI*, *rule parts-mpair-1*, *rule parts-mpair-2*)

proposition *parts-msg-idinfo* [*simp*]:
parts-msg $\langle n,\ X\rangle = \{\langle n,\ X\rangle\}$
by (*subst parts-msg-def*, *rule equalityI*, *rule subsetI*, *erule parts.induct*, *auto*)

proposition *parts-msg-parts*:
$[\![(A,\ X) \in s;\ Y \in parts\text{-}msg\ X]\!] \Longrightarrow Y \in parts\ (used\ s)$
by (*subgoal-tac* $X \in parts\ (used\ s)$, *drule parts-msg-mono* [*of X*], *auto*)

proposition *prikey-spied*:
$[\![s_0 \models s;\ PriKey\ K \in parts\ (used\ s)]\!] \Longrightarrow PriKey\ K \in spied\ s$
by (*induction rule*: *rtrancl-induct*, *subst* (*asm*) *parts-init*,
auto simp: *rel-def parts-insert dest*!: *parts-msg-parts*)

proposition *prikey-crypt* [*simplified*]:
$[\![(Spy,\ Crypt\ K\ (PriKey\ K')) \in s;\ s_0 \models s]\!] \Longrightarrow PriKey\ K' \in spied\ s$
by (*erule prikey-spied*, *blast*)

proposition *prikey-mpair-fst* [*simplified*]:
$[\![(Spy,\ \{\!|PriKey\ K,\ Y|\!\}) \in s;\ s_0 \models s]\!] \Longrightarrow PriKey\ K \in spied\ s$
by (*erule prikey-spied*, *blast*)

proposition *prikey-mpair-snd* [*simplified*]:
$[\![(Spy,\ \{\!|Y,\ PriKey\ K|\!\}) \in s;\ s_0 \models s]\!] \Longrightarrow PriKey\ K \in spied\ s$
by (*erule prikey-spied*, *blast*)

proposition *rev-prikey-secret*:
$s_0 \models s \Longrightarrow Rev\text{-}PriKey \notin spied\ s$
by (*induction rule*: *rtrancl-induct*, *insert sec-prik-rev tok-prik-rev*,
auto simp: *rel-def dest*: *prikey-crypt prikey-mpair-fst prikey-mpair-snd*)

proposition *sec-prikey-secret*:
$[\![s_0 \models s;\ n \notin bad\text{-}sec\text{-}prik]\!] \Longrightarrow Sec\text{-}PriKey\ n \notin spied\ s$
by (*induction rule*: *rtrancl-induct*, *insert sec-prik-inj sec-prik-tok-prik*, *auto simp*:
rel-def inj-on-def image-def dest: *prikey-crypt prikey-mpair-fst prikey-mpair-snd*)

proposition *tok-prikey-secret*:
$[\![s_0 \models s;\ n \notin bad\text{-}tok\text{-}prik]\!] \Longrightarrow Tok\text{-}PriKey\ n \notin spied\ s$
by (*induction rule*: *rtrancl-induct*, *insert tok-prik-inj sec-prik-tok-prik*, *auto simp*:
rel-def inj-on-def image-def dest: *prikey-crypt prikey-mpair-fst prikey-mpair-snd*)

proposition *idinfo-spied*:
$[\![s_0 \models s;\ \langle n,\ X\rangle \in parts\ (used\ s)]\!] \Longrightarrow \langle n,\ X\rangle \in spied\ s$
by (*induction rule*: *rtrancl-induct*, *subst* (*asm*) *parts-init*,

auto simp: *rel-def parts-insert dest*!: *parts-msg-parts*)

proposition *idinfo-crypt*:
$[\![(Spy,\ Crypt\ K\ \langle n,\ X\rangle) \in s;\ s_0 \models s]\!] \Longrightarrow \langle n,\ X\rangle \in spied\ s$
by (*erule idinfo-spied*, *blast*)

proposition *idinfo-mpair-fst*:
$[\![(Spy,\ \{\!|\langle n,\ X\rangle,\ Y|\!\}) \in s;\ s_0 \models s]\!] \Longrightarrow \langle n,\ X\rangle \in spied\ s$
by (*erule idinfo-spied*, *blast*)

proposition *idinfo-mpair-snd*:
$[\![(Spy,\ \{\!|Y,\ \langle n,\ X\rangle|\!\}) \in s;\ s_0 \models s]\!] \Longrightarrow \langle n,\ X\rangle \in spied\ s$
by (*erule idinfo-spied*, *blast*)

proposition *idinfo-hash-hash* [*rotated*]:
$[\![s_0 \models s;\ (Spy,\ \langle n,\ Hash\ (Hash\ X)\rangle) \in s]\!] \Longrightarrow \langle n,\ Hash\ X\rangle \in spied\ s$
by (*induction arbitrary*: *X rule*: *rtrancl-induct*, *auto simp*: *rel-def dest*: *idinfo-crypt idinfo-mpair-fst idinfo-mpair-snd*)

proposition *sec-prik-eq*:
$\{Tok\text{-}PriK\ n,\ Sec\text{-}PriK\ m,\ Rev\text{-}PriK\} =$
$\{Tok\text{-}PriK\ n,\ Sec\text{-}PriK\ m',\ Rev\text{-}PriK\} \Longrightarrow m' = m$
by (*erule equalityE*, *drule subsetD* [**where** $c = Sec\text{-}PriK\ m$], *simp*, *insert sec-prik-inj sec-prik-rev sec-prik-tok-prik*, *auto simp*: *inj-on-def image-def*)

proposition *id-identified*:
assumes
A: $s_0 \models s$ **and**
B: $(n,\ m) \notin bad\text{-}id$ **and**
C: $n \notin bad\text{-}tok\text{-}prik$ **and**
D: $\langle n,\ Hash\ (ID\ n\ (Sec\text{-}PubKey\ m))\rangle \in spied\ s$
shows $m \in bad\text{-}sec\text{-}prik \wedge$
$(\exists\, m'.\ m' \neq m \wedge m' \in bad\text{-}sec\text{-}prik \wedge (n,\ m') \in bad\text{-}id)$
proof −
let $?P_1 = \lambda s.\ \langle n,\ Hash\ (ID\ n\ (Sec\text{-}PubKey\ m))\rangle \in spied\ s$
let $?P_2 = \lambda s.\ \exists\, S.\ \langle n,\ PubKey\ S\rangle \in spied\ s \wedge Sec\text{-}PriK\ m \in S$
let $?P_3 = \lambda S\ s.\ \langle n,\ Hash\ (PubKey\ S)\rangle \in spied\ s$
let $?P_4 = \lambda S\ s.\ \langle n,\ PubKey\ S\rangle \in spied\ s \wedge Rev\text{-}PriK \in S \wedge$
$(\forall\, m.\ Sec\text{-}PriK\ m \in S \longrightarrow (n,\ m) \notin bad\text{-}id)$
have *E*: $\forall\, m.\ Sec\text{-}PriK\ m \neq Rev\text{-}PriK$
by (*rule allI*, *rule notI*, *subgoal-tac Rev-PriK* $\in$ *range Sec-PriK*, *simp add*: *sec-prik-rev*, *rule range-eqI*, *rule sym*)
have $\exists\, u\ v.\ s_0 \models u \wedge u \vdash v \wedge v \models s \wedge \neg\ ?P_1\ u \wedge\ ?P_1\ v$
using *A* **and** *B* **and** *D* **by** (*rule-tac rtrancl-start*, *auto dest*: *sec-prik-eq*)
then obtain $u_1\ v_1$ **where** *F*: $s_0 \models u_1 \wedge u_1 \vdash v_1 \wedge \neg\ ?P_1\ u_1 \wedge\ ?P_1\ v_1$
by *blast*
moreover from *this* **have** *G*: $\langle n,\ ID\ n\ (Sec\text{-}PubKey\ m)\rangle \in spied\ u_1$
by (*auto simp*: *rel-def dest*: *idinfo-crypt idinfo-mpair-fst idinfo-mpair-snd*

idinfo-hash-hash)
ultimately have $\exists\, u\ v.\ s_0 \models u \wedge u \vdash v \wedge v \models u_1 \wedge \neg\ ?P_2\ u \wedge\ ?P_2\ v$
using B **and** E **by** (*rule-tac rtrancl-start*, *insert*
sec-prik-inj sec-prik-tok-prik, *auto simp*: *inj-on-def image-def*)
then obtain $u_2\ v_2$ **where** H: $s_0 \models u_2 \wedge u_2 \vdash v_2 \wedge \neg\ ?P_2\ u_2 \wedge\ ?P_2\ v_2$
by *blast*
moreover from *this* **have** *Tok-PriKey n* $\notin$ *spied* u_2
using C **by** (*rule-tac tok-prikey-secret*, *simp*)
ultimately have *Sec-PriKey m* $\in$ *spied* u_2
proof (*auto simp*: *rel-def dest*: *idinfo-crypt idinfo-mpair-fst idinfo-mpair-snd*)
fix S
assume (*Spy*, $\langle n,$ *Hash* (*AgrKey* (*PubK S*))$\rangle$) $\in u_2$
moreover assume I: *Sec-PriK m* $\in S$
hence $\langle n,$ *Hash* (*PubKey S*)$\rangle \notin$ *spied* s_0
using B **and** E **by** (*insert sec-prik-inj sec-prik-tok-prik*,
auto simp: *inj-on-def image-def*)
ultimately have $\exists\, u\ v.\ s_0 \models u \wedge u \vdash v \wedge v \models u_2 \wedge \neg\ ?P_3\ S\ u \wedge\ ?P_3\ S\ v$
using H **by** (*rule-tac rtrancl-start*, *simp-all*)
then obtain $u_3\ v_3$ **where** $s_0 \models u_3 \wedge u_3 \vdash v_3 \wedge v_3 \models u_2 \wedge$
$\neg\ ?P_3\ S\ u_3 \wedge\ ?P_3\ S\ v_3$
by *blast*
moreover from *this* **have** $\langle n,$ *PubKey S*$\rangle \in$ *spied* v_3
by (*auto simp*: *rel-def dest*: *idinfo-crypt idinfo-mpair-fst idinfo-mpair-snd*
idinfo-hash-hash)
ultimately have $\langle n,$ *PubKey S*$\rangle \in$ *spied* u_2
by (*rule-tac subsetD* [*of spied* v_3], *rule-tac spied-subset*, *simp*)
hence *Sec-PriK m* $\notin S$
using H **by** *simp*
thus (*Spy*, *AgrKey* (*PriK* (*Sec-PriK m*))) $\in u_2$
using I **by** *contradiction*
qed
hence I: *m* $\in$ *bad-sec-prik*
using H **by** (*erule-tac contrapos-pp*, *rule-tac sec-prikey-secret*, *simp*)
from B **and** E **and** G **have** $\exists\, S.\ ?P_4\ S\ u_1$
by (*rule-tac exI* [*of* - {*Tok-PriK n*, *Sec-PriK m*, *Rev-PriK*}],
insert sec-prik-inj sec-prik-tok-prik, *auto simp*: *inj-on-def image-def*)
moreover have $\neg\ (\exists\, S.\ ?P_4\ S\ s_0)$
by (*insert tok-prik-rev*, *auto*)
ultimately have $\exists\, u\ v.\ s_0 \models u \wedge u \vdash v \wedge v \models u_1 \wedge$
$\neg\ (\exists\, S.\ ?P_4\ S\ u) \wedge (\exists\, S.\ ?P_4\ S\ v)$
using F **by** (*rule-tac rtrancl-start*, *simp*)
then obtain $u_4\ v_4\ S$ **where**
J: $s_0 \models u_4$ **and** K: $u_4 \vdash v_4$ **and** L: $\neg\ (\exists\, S.\ ?P_4\ S\ u_4) \wedge\ ?P_4\ S\ v_4$
by *blast*
have M: $[\![(Spy, \langle n,$ *AgrKey* (*PubK S*)$\rangle) \in u_4$; *Rev-PriK* $\in S$;
$\forall\, m.$ *Sec-PriK m* $\in S \longrightarrow (n,\ m) \notin$ *bad-id*;
$\forall\, S.$ *Rev-PriK* $\in S \longrightarrow (Spy, \langle n,$ *AgrKey* (*PubK S*)$\rangle) \in u_4 \longrightarrow$
$(\exists\, m.$ *Sec-PriK m* $\in S \wedge (n,\ m) \in$ *bad-id*)$]\!] \Longrightarrow$ *False*
by *blast*

from K **and** L **have** $\exists\, m'.\ m' \neq m \wedge m' \in \mathit{bad\text{-}sec\text{-}prik} \wedge (n,\ m') \in \mathit{bad\text{-}id}$
proof (*simp add*: *rel-def*, (*erule-tac disjE*, (*clarsimp*, (*erule-tac disjE*,
drule-tac sym, *simp*, (*drule-tac idinfo-crypt* [*OF - J*] | *drule-tac*
idinfo-mpair-fst [*OF - J*] | *drule-tac idinfo-mpair-snd* [*OF - J*]), *blast*)+)*?*,
blast)+, (*erule-tac disjE*, *erule-tac* [*2*] *disjE*, *erule-tac* [*3*] *disjE*; *clarsimp*))
fix $n'\ S'\ A$
assume
N: $\forall\, S.\ \mathit{Rev\text{-}PriK} \in S \longrightarrow (\mathit{Spy},\ \langle n,\ \mathit{AgrKey}\ (\mathit{PubK}\ S)\rangle) \in u_4 \longrightarrow$
$(\exists\, m.\ \mathit{Sec\text{-}PriK}\ m \in S \wedge (n,\ m) \in \mathit{bad\text{-}id})$ **and**
O: $\forall\, m.\ \mathit{Sec\text{-}PriK}\ m \in S \longrightarrow (n,\ m) \notin \mathit{bad\text{-}id}$ **and**
P: $\mathit{Rev\text{-}PriK} \in S$ **and**
Q: $(\mathit{Spy},\ \langle n',\ \mathit{AgrKey}\ (\mathit{PubK}\ S')\rangle) \in u_4$ **and**
R: $(\mathit{Spy},\ \mathit{AgrKey}\ (\mathit{PriK}\ A)) \in u_4$
assume $n = n' \wedge S = S' - \{A\} \vee (\mathit{Spy},\ \langle n,\ \mathit{AgrKey}\ (\mathit{PubK}\ S)\rangle) \in u_4$
thus *?thesis*
proof (*rule disjE*, *drule-tac* [*2*] M [*OF - P O N*]; *clarsimp*)
assume S: $n = n'$ **and** $S = S' - \{A\}$
moreover from *this* **obtain** m' **where**
$\mathit{Sec\text{-}PriK}\ m' \in S'$ **and** T: $(n,\ m') \in \mathit{bad\text{-}id}$
using N **and** P **and** Q **by** *blast*
ultimately have $A = \mathit{Sec\text{-}PriK}\ m'$
using O **by** (*rule-tac ccontr*, *simp*)
hence $\mathit{Sec\text{-}PriKey}\ m' \in \mathit{spied}\ u_4$
using R **by** *simp*
hence $m' \in \mathit{bad\text{-}sec\text{-}prik}$
by (*rule contrapos-pp*, *rule-tac sec-prikey-secret* [*OF J*])
thus $\exists\, m'.\ m' \neq m \wedge m' \in \mathit{bad\text{-}sec\text{-}prik} \wedge (n',\ m') \in \mathit{bad\text{-}id}$
using B **and** S **and** T **by** *auto*
qed
next
fix $n'\ S'\ A$
assume
N: $\forall\, S.\ \mathit{Rev\text{-}PriK} \in S \longrightarrow (\mathit{Spy},\ \langle n,\ \mathit{AgrKey}\ (\mathit{PubK}\ S)\rangle) \in u_4 \longrightarrow$
$(\exists\, m.\ \mathit{Sec\text{-}PriK}\ m \in S \wedge (n,\ m) \in \mathit{bad\text{-}id})$ **and**
O: $\forall\, m.\ \mathit{Sec\text{-}PriK}\ m \in S \longrightarrow (n,\ m) \notin \mathit{bad\text{-}id}$ **and**
P: $\mathit{Rev\text{-}PriK} \in S$ **and**
Q: $(\mathit{Spy},\ \langle n',\ \mathit{AgrKey}\ (\mathit{PubK}\ S')\rangle) \in u_4$ **and**
R: $(\mathit{Spy},\ \mathit{AgrKey}\ (\mathit{PriK}\ A)) \in u_4$
assume $n = n' \wedge S = \mathit{insert}\ A\ S' \vee (\mathit{Spy},\ \langle n,\ \mathit{AgrKey}\ (\mathit{PubK}\ S)\rangle) \in u_4$
thus *?thesis*
proof (*rule disjE*, *drule-tac* [*2*] M [*OF - P O N*]; *clarsimp*)
assume $n = n'$ **and** S: $S = \mathit{insert}\ A\ S'$
moreover have $A \neq \mathit{Rev\text{-}PriK}$
using R **by** (*rule contrapos-pn*, *insert rev-prikey-secret* [*OF J*], *simp*)
ultimately obtain m' **where** $\mathit{Sec\text{-}PriK}\ m' \in S'$ **and** T: $(n,\ m') \in \mathit{bad\text{-}id}$
using N **and** P **and** Q **by** *blast*
hence $(n,\ m') \notin \mathit{bad\text{-}id}$
using O **and** S **by** *simp*
thus $\exists\, m'.\ m' \neq m \wedge m' \in \mathit{bad\text{-}sec\text{-}prik} \wedge (n',\ m') \in \mathit{bad\text{-}id}$

```
    using T by contradiction
  qed
next
  fix n' S'
  assume
    N: ∀ S. Rev-PriK ∈ S ⟶ (Spy, ⟨n, AgrKey (PubK S)⟩) ∈ u₄ ⟶
      (∃ m. Sec-PriK m ∈ S ∧ (n, m) ∈ bad-id) and
    O: ∀ m. Sec-PriK m ∈ S ⟶ (n, m) ∉ bad-id and
    P: Rev-PriK ∈ S
  assume n = n' ∧ S = S' ∨ (Spy, ⟨n, AgrKey (PubK S)⟩) ∈ u₄ and
    (Spy, AgrKey (PriK (Tok-PriK n'))) ∈ u₄
  thus ?thesis
    by (erule-tac disjE, drule-tac [2] M [OF - P O N],
     insert tok-prikey-secret [OF J C], simp-all)
next
  fix n' X
  assume
    N: ∀ S. Rev-PriK ∈ S ⟶ (Spy, ⟨n, AgrKey (PubK S)⟩) ∈ u₄ ⟶
      (∃ m. Sec-PriK m ∈ S ∧ (n, m) ∈ bad-id) and
    O: ∀ m. Sec-PriK m ∈ S ⟶ (n, m) ∉ bad-id and
    P: Rev-PriK ∈ S and
    Q: (Spy, ⟨n', X⟩) ∈ u₄ ∨ (Spy, ⟨n', Hash X⟩) ∈ u₄
  assume n = n' ∧ AgrKey (PubK S) = X ∨
    (Spy, ⟨n, AgrKey (PubK S)⟩) ∈ u₄
  thus ?thesis
  proof (rule disjE, drule-tac [2] M [OF - P O N]; clarsimp)
    assume R: n = n' and S: X = AgrKey (PubK S)
    {
      assume (Spy, ⟨n', X⟩) ∈ u₄
      hence (Spy, ⟨n, AgrKey (PubK S)⟩) ∈ u₄
        using R and S by simp
    }
    moreover {
      assume (Spy, ⟨n', Hash X⟩) ∈ u₄
      hence ?P₃ S u₄
        using R and S by simp
      moreover have ¬ ?P₃ S s₀
        using O by auto
      ultimately have ∃ u v. s₀ ⊨ u ∧ u ⊢ v ∧ v ⊨ u₄ ∧ ¬ ?P₃ S u ∧ ?P₃ S v
        using J by (rule-tac rtrancl-start)
      then obtain u₃ v₃ where s₀ ⊨ u₃ ∧ u₃ ⊢ v₃ ∧ v₃ ⊨ u₄ ∧
        ¬ ?P₃ S u₃ ∧ ?P₃ S v₃
        by blast
      moreover from this have ⟨n, AgrKey (PubK S)⟩ ∈ spied v₃
        by (auto simp: rel-def dest: idinfo-crypt idinfo-mpair-fst idinfo-mpair-snd
         idinfo-hash-hash)
      ultimately have ⟨n, AgrKey (PubK S)⟩ ∈ spied u₄
        by (rule-tac subsetD [of spied v₃], rule-tac spied-subset, simp)
    }
```

ultimately have $(Spy, \langle n, AgrKey\ (PubK\ S)\rangle) \in u_4$
using Q **by** *blast*
thus $\exists\, m'.\ m' \neq m \wedge m' \in bad\text{-}sec\text{-}prik \wedge (n', m') \in bad\text{-}id$
by (*drule-tac* M [OF - P O N], *simp*)
qed
qed
thus *?thesis*
using I **by** *simp*
qed

theorem *id-anonymous* [*rotated*]:
$[\![m \notin bad\text{-}sec\text{-}prik \vee \neg\ (\exists\, m'.\ m' \neq m \wedge m' \in bad\text{-}sec\text{-}prik \wedge (n, m') \in bad\text{-}id);$
$s_0 \models s;\ (n, m) \notin bad\text{-}id;\ n \notin bad\text{-}tok\text{-}prik]\!] \Longrightarrow$
$\langle n, Hash\ (ID\ n\ (Sec\text{-}PubKey\ m))\rangle \notin spied\ s$
by (*erule contrapos-pn*, *drule id-identified*, *blast*+)

end

3 Possibility of anonymity compromise for token pseudonymous identifiers

theory *Possibility*
imports *Anonymity*
begin

This section proves possibility properties *tok-id-identified*, *sec-id-identified*, which altogether state that the spy can map a token pseudonymous identifier to the related token if either attack option described in section 1.2 is viable. Both properties are proven by construction, namely by creating as many sample protocol runs such as to satisfy their conclusions if their assumptions are fulfilled.

definition *tok-id-pubk-prik* :: *agent-id* ⇒ *agent-id* ⇒ *state* **where**
tok-id-pubk-prik n m ≡
insert (*Spy*, ⟨*n*, *ID n* (*Sec-PubKey m*)⟩) s_0

definition *tok-id-hash* :: *agent-id* ⇒ *agent-id* ⇒ *state* **where**
tok-id-hash n m ≡
insert (*Spy*, ⟨*n*, *Hash* (*ID n* (*Sec-PubKey m*))⟩) (*tok-id-pubk-prik n m*)

proposition *tok-id-pubk-prik-rel*:
$n \in bad\text{-}tok\text{-}prik \Longrightarrow s_0 \models tok\text{-}id\text{-}pubk\text{-}prik\ n\ m$
by (*subgoal-tac* (s_0, *tok-id-pubk-prik n m*) ∈ *rel-id-pubk-prik*,
rule r-into-rtrancl, *auto simp*: *tok-id-pubk-prik-def rel-def image-def*, *blast*)

proposition *tok-id-pubk-prik-msg*:
$n \in$ *bad-tok-prik* $\Longrightarrow$
$\{$*ID* n (*Sec-PubKey* m), *Hash* (*ID* n (*Sec-PubKey* m)),
$\langle n$, *ID* n (*Sec-PubKey* $m)\rangle\} \subseteq$ *spied* (*tok-id-pubk-prik* n m)
by (*auto simp*: *tok-id-pubk-prik-def*)

proposition *tok-id-hash-rel*:
$n \in$ *bad-tok-prik* $\Longrightarrow s_0 \models$ *tok-id-hash* n m
by (*rule rtrancl-into-rtrancl*, *erule tok-id-pubk-prik-rel* [*of* - m],
subgoal-tac (*tok-id-pubk-prik* n m, *tok-id-hash* n m) $\in$ *rel-id-hash*,
frule-tac [*2*] *tok-id-pubk-prik-msg* [*of* - m], *auto simp*: *tok-id-hash-def rel-def*)

theorem *tok-id-identified*:
$n \in$ *bad-tok-prik* $\Longrightarrow \exists s.\ s_0 \models s \wedge \langle n$, *Hash* (*ID* n (*Sec-PubKey* $m))\rangle \in$ *spied* s
by (*rule exI* [*of* - *tok-id-hash* n m], *drule tok-id-hash-rel* [*of* - m],
simp add: *tok-id-hash-def*)

definition *sec-pubk-less* :: *agent-id* $\Rightarrow$ *state* **where**
sec-pubk-less $n \equiv$
insert (*Spy*, *PubKey* $\{$*Tok-PriK* n, *Rev-PriK*$\}$) s_0

definition *sec-id-pubk-less* :: *agent-id* $\Rightarrow$ *state* **where**
sec-id-pubk-less $n \equiv$
insert (*Spy*, $\langle n$, *PubKey* $\{$*Tok-PriK* n, *Rev-PriK*$\}\rangle$) (*sec-pubk-less* n)

definition *sec-id-pubk-more* :: *agent-id* $\Rightarrow$ *agent-id* $\Rightarrow$ *state* **where**
sec-id-pubk-more n $m \equiv$
insert (*Spy*, $\langle n$, *ID* n (*Sec-PubKey* $m)\rangle$) (*sec-id-pubk-less* n)

definition *sec-id-hash* :: *agent-id* $\Rightarrow$ *agent-id* $\Rightarrow$ *state* **where**
sec-id-hash n $m \equiv$
insert (*Spy*, $\langle n$, *Hash* (*ID* n (*Sec-PubKey* $m))\rangle$) (*sec-id-pubk-more* n m)

lemma *sec-id-identified-1*:
$\{$*Tok-PriK* n, *Sec-PriK* m, *Rev-PriK*$\} \neq \{$*Tok-PriK* n', *Rev-PriK*$\}$
by (*simp add*: *set-eq-iff*, *rule exI* [*of* - *Sec-PriK* m], *insert*
sec-prik-rev sec-prik-tok-prik, *simp add*: *image-def*, *drule spec* [*of* - m], *auto*)

lemma *sec-id-identified-2*:
(*Spy*, *PubKey* $\{$*Tok-PriK* n, *Rev-PriK*$\}) \notin s_0$
by (*insert tok-prik-rev sec-id-identified-1*, *simp add*: *image-def*,
drule spec [*of* - n], *auto simp*: *set-eq-iff*)

lemma *sec-id-identified-3*:
$\{$*Tok-PriK* n, *Rev-PriK*$\} =$

$\{Tok\text{-}PriK\ n,\ Sec\text{-}PriK\ m,\ Rev\text{-}PriK\} - \{Sec\text{-}PriK\ m\}$
by (*insert sec-prik-rev sec-prik-tok-prik*, *auto*)

lemma *sec-id-identified-4*:
$PubK\ \{Tok\text{-}PriK\ n,\ Sec\text{-}PriK\ m,\ Rev\text{-}PriK\} =$
$PubK\ (insert\ (Sec\text{-}PriK\ m)\ \{Tok\text{-}PriK\ n,\ Rev\text{-}PriK\})$
by *auto*

proposition *sec-pubk-less-rel*:
$[\![\{m,\ m'\} \subseteq bad\text{-}sec\text{-}prik;\ (n,\ m) \notin bad\text{-}id;\ (n,\ m') \in bad\text{-}id]\!] \Longrightarrow$
$s_0 \models sec\text{-}pubk\text{-}less\ n$
by (*subgoal-tac* $(s_0,\ sec\text{-}pubk\text{-}less\ n) \in rel\text{-}pubk\text{-}less$, *rule r-into-rtrancl*,
simp add: *rel-def*, *subst sec-pubk-less-def*, *subst sec-id-identified-3* [*of* - m'],
simp, (*rule exI*)+, *subst insert-ident*, *subst sec-id-identified-3* [*symmetric*],
insert sec-id-identified-2, *auto*)

proposition *sec-pubk-less-msg*:
$[\![\{m,\ m'\} \subseteq bad\text{-}sec\text{-}prik;\ (n,\ m) \notin bad\text{-}id;\ (n,\ m') \in bad\text{-}id]\!] \Longrightarrow$
$\{Sec\text{-}PriKey\ m,\ Sec\text{-}PriKey\ m',\ PubKey\ \{Tok\text{-}PriK\ n,\ Rev\text{-}PriK\},$
$ID\ n\ (Sec\text{-}PubKey\ m),\ Hash\ (ID\ n\ (Sec\text{-}PubKey\ m)),$
$\langle n,\ ID\ n\ (Sec\text{-}PubKey\ m')\rangle\} \subseteq spied\ (sec\text{-}pubk\text{-}less\ n) \wedge$
$\{\langle n,\ PubKey\ \{Tok\text{-}PriK\ n,\ Rev\text{-}PriK\}\rangle,\ \langle n,\ ID\ n\ (Sec\text{-}PubKey\ m)\rangle,$
$\langle n,\ Hash\ (ID\ n\ (Sec\text{-}PubKey\ m))\rangle\} \cap$
$spied\ (sec\text{-}pubk\text{-}less\ n) = \{\}$
by (*insert sec-id-identified-2*, *auto simp*: *sec-pubk-less-def image-def*
dest: *sec-prik-eq*)

proposition *sec-id-pubk-less-rel*:
$[\![\{m,\ m'\} \subseteq bad\text{-}sec\text{-}prik;\ (n,\ m) \notin bad\text{-}id;\ (n,\ m') \in bad\text{-}id]\!] \Longrightarrow$
$s_0 \models sec\text{-}id\text{-}pubk\text{-}less\ n$
by (*rule rtrancl-into-rtrancl*, *erule sec-pubk-less-rel*, *assumption*+,
subgoal-tac $(sec\text{-}pubk\text{-}less\ n,\ sec\text{-}id\text{-}pubk\text{-}less\ n) \in rel\text{-}id\text{-}pubk\text{-}less$,
frule-tac [*2*] *sec-pubk-less-msg*, *simp-all add*: *sec-id-pubk-less-def rel-def*,
(*rule exI*)+, *subst sec-id-identified-3* [*of* - m'], *subst* (*asm*) (*1 2*)
sec-id-identified-3, *subst insert-ident*, *insert sec-prik-tok-prik*, *auto*)

proposition *sec-id-pubk-less-msg*:
$[\![\{m,\ m'\} \subseteq bad\text{-}sec\text{-}prik;\ (n,\ m) \notin bad\text{-}id;\ (n,\ m') \in bad\text{-}id]\!] \Longrightarrow$
$\{Sec\text{-}PriKey\ m,\ ID\ n\ (Sec\text{-}PubKey\ m),\ Hash\ (ID\ n\ (Sec\text{-}PubKey\ m)),$
$\langle n,\ PubKey\ \{Tok\text{-}PriK\ n,\ Rev\text{-}PriK\}\rangle\} \subseteq$
$spied\ (sec\text{-}id\text{-}pubk\text{-}less\ n) \wedge$
$\{\langle n,\ ID\ n\ (Sec\text{-}PubKey\ m)\rangle,\ \langle n,\ Hash\ (ID\ n\ (Sec\text{-}PubKey\ m))\rangle\} \cap$
$spied\ (sec\text{-}id\text{-}pubk\text{-}less\ n) = \{\}$
by (*drule sec-pubk-less-msg*, *insert sec-id-identified-1*,
auto simp: *sec-id-pubk-less-def*)

proposition *sec-id-pubk-more-rel*:
$[\![\{m,\ m'\} \subseteq bad\text{-}sec\text{-}prik;\ (n,\ m) \notin bad\text{-}id;\ (n,\ m') \in bad\text{-}id]\!] \Longrightarrow$
$s_0 \models sec\text{-}id\text{-}pubk\text{-}more\ n\ m$

by (*rule rtrancl-into-rtrancl*, *erule sec-id-pubk-less-rel*, *assumption*+,
subgoal-tac (*sec-id-pubk-less n*, *sec-id-pubk-more n m*) ∈ *rel-id-pubk-more*,
frule-tac [*2*] *sec-id-pubk-less-msg*, *simp-all add*: *sec-id-pubk-more-def rel-def*,
(*rule exI*)+, *subst sec-id-identified-4*, *subst* (*asm*) (*1 3*) *sec-id-identified-4*,
subst insert-ident, *simp-all*)

proposition *sec-id-pubk-more-msg*:
⟦{*m*, *m'*} ⊆ *bad-sec-prik*; (*n*, *m*) ∉ *bad-id*; (*n*, *m'*) ∈ *bad-id*⟧ ⟹
{*ID n* (*Sec-PubKey m*), *Hash* (*ID n* (*Sec-PubKey m*)),
⟨*n*, *ID n* (*Sec-PubKey m*)⟩} ⊆ *spied* (*sec-id-pubk-more n m*) ∧
⟨*n*, *Hash* (*ID n* (*Sec-PubKey m*))⟩ ∉ *spied* (*sec-id-pubk-more n m*)
by (*drule sec-id-pubk-less-msg*, *auto simp*: *sec-id-pubk-more-def*)

proposition *sec-id-hash-rel*:
⟦{*m*, *m'*} ⊆ *bad-sec-prik*; (*n*, *m*) ∉ *bad-id*; (*n*, *m'*) ∈ *bad-id*⟧ ⟹
s_0 ⊨ *sec-id-hash n m*
by (*rule rtrancl-into-rtrancl*, *erule sec-id-pubk-more-rel*, *assumption*+,
subgoal-tac (*sec-id-pubk-more n m*, *sec-id-hash n m*) ∈ *rel-id-hash*,
frule-tac [*2*] *sec-id-pubk-more-msg*, *auto simp*: *sec-id-hash-def rel-def*)

theorem *sec-id-identified*:
⟦{*m*, *m'*} ⊆ *bad-sec-prik*; (*n*, *m'*) ∈ *bad-id*⟧ ⟹
∃ *s*. s_0 ⊨ *s* ∧ ⟨*n*, *Hash* (*ID n* (*Sec-PubKey m*))⟩ ∈ *spied s*
by (*cases* (*n*, *m*) ∈ *bad-id*, *blast*, *rule exI* [*of* - *sec-id-hash n m*],
drule sec-id-hash-rel, *simp-all add*: *sec-id-hash-def*)

end

References

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Technical Guideline TR-03110 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), version 2.21*, Dec. 2016.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Technical Guideline TR-03110 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, version 2.21*, Dec. 2016.

[3] A. Krauss. *Defining Recursive Functions in Isabelle/HOL*. https://isabelle.in.tum.de/website-Isabelle2021/dist/Isabelle2021/doc/functions.pdf.

[4] T. Nipkow. *A Tutorial Introduction to Structured Isar Proofs*. https://isabelle.in.tum.de/website-Isabelle2011/dist/Isabelle2011/doc/isar-overview.pdf.

[5] T. Nipkow. *Programming and Proving in Isabelle/HOL*, Feb. 2021. https://isabelle.in.tum.de/website-Isabelle2021/dist/Isabelle2021/doc/prog-prove.pdf.

[6] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, Feb. 2021. https://isabelle.in.tum.de/website-Isabelle2021/dist/Isabelle2021/doc/tutorial.pdf.

[7] P. Noce. The Relational Method with Message Anonymity for the Verification of Cryptographic Protocols. *Archive of Formal Proofs*, Dec. 2020. https://isa-afp.org/entries/Relational_Method.html, Formal proof development.