Journal of Universal Computer Science, vol. 12, no. 9 (2006), 1373-1384
submitted: 31/12/05, accepted: 12/5/06, appeared: 28/9/06 © J.UCS

The Additional Examination of the Kudo-Mathuria Time-Release Protocol

Péter Takács
(University Debrecen, Health College, Hungary
vtp@de-efk.hu)

Abstract: The purpose of the present paper is to give an expansion of the results of Michiharu Kudo and Anish Mathuria. We present the base-protocol and formulate three properties of the protocol with modal logic tools. After that we expand the base-protocol and prove four new properties. We prove that the third trusted partner can not read the message of the sender until a predetermined time.
Key Words: time-release cryptography, time capsule, Kudo-Mathuria protocol, formal verification of cryptographic protocols
Category: C.2.2

1 Introduction - The problem of 'time-capsule'

Cryptographic systems have two main parts basically: the area of transformations of encryptions and decryptions and the area of cryptographic protocols. Recently the planning and verifying of cryptographic protocols have developed tools. More separate trends have grown up during the development of the procedures.

The question of time-release cryptography was suggested by Timothy C. May in 1993 for first time [May 1995]. The aim of this protocol is to encrypt a message that cannot be decrypted by anyone (not even by the sender), until a predetermined time (time capsule). This protocol has many applications: closed sales bids in an auction, encrypt documents for long time, long-dated transactions, etc.

Ronald L. Rivest, Adi Shamir and David A. Wagner summarized two solutions in 1996 [Rivest, Shamir and Wagner 1996] - which are still acceptable nowadays. The first solution is based on computability. This is a mathematical puzzle (time-clock puzzle) that cannot be solved for at least a certain amount of time. The second one is based on involving a trusted agent - Trent (T) - who promise not to reveal certain information until a specific time.

Many people have been dealing with both recommended solutions since 1996. Michiharu Kudo and Anish Mathuria published a cryptographic protocol in 1999, which not only covered the second solution, but it was also analyzed by tools of mathematical logic [Kudo and Mathuria 1999].

Hereafter call this protocol Kodo-Mathuria K-M-P1 protocol.

The aim of the present paper is to give an expansion the results of Michiharu Kudo and Anish Mathuria [Kudo and Mathuria 1999]. We prove the expansions by tools of modal logic. The main aim is to prove that the third trusted partner can not read the message of the sender until a predetermined time. The expansions of the original protocol in this way expand the possible area of applications.

2 The Kudo-Mathuria K-M-P1 protocol

The K-M-P1 protocol encrypts a message that cannot be read by anyone (except the sender) until a specific time.

There are three participants in the original protocol: A (Alice) the sender, B (Bob) the receiver and T (Trent) the trusted agent. Let us assume T is capable of knowing the correct time while neither A nor B can tell the correct time on their own.

Let M_k denote the encryption of the message M under public key k and let M_k^{-1} denote the decryption or signature of the (secret-)message under secret key k^{-1}. The applied steps are the following (Protocol K-M-P1):

Step 1. A sends message to T asking him to generate time-key pair for some time t_8 in the future:

$$\{"enc", t_8\} .$$

Step 2. After receiving A's message, T generates a time-pair: $(tk_{t_8}, tk_{t_8}^{-1})$. T sends a signed message to A that contains the tk_{t_8} part of the time key-pair, which is needed for encryption:

$$\{\{"enc", t_8, tk_{t_8}\}k_T^{-1}\} .$$

T keeps the decryption key $tk_{t_8}^{-1}$ in secret until the time t_8.

Step 3. A verifies T's signature. If the signature is right then A sends message to B containing the name of A. This message is a call for communication:

$$\{A\} .$$

Step 4. B responds to A with random number N_b:

$$\{N_b\} .$$

This number is against replay-attack.

Step 5. After it A generates random number R_a and creates the next message:

$$\{\{\{X_a, R_a, A\}tk_{t_8}, A, B, t_8, N_b, tk_{t_8}\}k_A^{-1}, \{"enc", t_8, tk_{t_8}\}k_T^{-1}\} .$$

R_a guarantees the uniqueness of ciphertext.

Step 6. B verifies the signature of A and as a confirmation B sends back a certain part of the message with his signature:

$$\{\{\{\{X_a, R_a, A\}tk_{t_8}, A, B, t_8, N_b, tk_{t_8}\}k_A^{-1}\}k_B^{-1}\} .$$

Step 7. B sends a message to T giving the time t_8, when he wants to decrypt the original time-confidential message from A:

$$\{"dec", t_8\} .$$

Step 8. T waits until given time of A and then sends the right decryption key to B:

$$\{\{"dec", t_8, tk_{t_8}^{-1}\}k_T^{-1}\} .$$

□

Using this protocol we reach that the receiver B cannot decrypt the message X_a before the specific time. In addition the protocol certifies authenticity of A to B.

3 Formal methods of protocols

Inappropriately designed cryptographic protocol may contain flaws, that can be ideal starting points for attackers. Such flaws are hard to found. The academic literature publishes numerous example that flaws were not discovered for a long time. The researchers analysed these flaws with different methods and tools vainly.

For example, Dening and Sacco found security hole in Needham-Schroeder authenticated key distribution protocol in 1981 [Buttyán 1999]. This flaw allowed an intruder to use an old compromised session key as a new one. Burrows, Abadi and Needham found a similar security gap in the CCITT X.509 standard [Burrows, Abadi and Needham 1989].

The researchers use empirical tests, simulated attacks and formal planning and checking methods to eliminate errors of cryptographic protocols.

Formal methods have been used for a long time in planning and analysing communication protocols. A similar research started in the early nineties in the area of cryptographic protocols.

Formal methods can be used in the phase of specification, construction and verification of the cryptographic protocols. The research concentrates on formal verification of protocols. Using formal methods in the area of specification is an emerging part of the research. The planned constitution of protocols is still an undiscovered area.

An overall analysis of this issue was prepared by Buttyán [Buttyán 1999]. Further thorough overview can be read in the works of Rubin and Honeyman [Rubin and Honeyman 1993] as well as in the works of Meadows [Meadows 1995].

Meadows identified four main types of analysis of cryptographic protocols in her article published in 1995 [Meadows 1995]:

Using general purpose verification tools. We construct models and verify them with specific languages and general checking tools.
Using expert systems. We develop professional systems which allow us to replay the different scenarios of protocols.
Using general modal logic tools. We can use modal logic tools to resolve the notion of 'know' and 'believe/accept'. These terms are fundamental in the theory of cryptographic protocols.
Using algebraic tools. We can use mathematical algebraic tools to analyze cryptographic protocols.

In the following we are going to use modal logic tools to analyze protocol K-M-P1 and its extensions. Our main starting tools are the Burrows-Abadi-Needham logic (BAN logic) [Burrows, Abadi and Needham 1989]. We use the Coffey-Shaida-logic [Coffey and Saidha 1997] which is the extension of the fundamental BAN-logic. We apply the supplemented theory of this logic (time-dependent elements).

4 The proof of some properties of the protocol K-M-P1

We need to compose and formulate assertions when we prove the protocol properties. Then we verify or reject the assertions in the model.

Look the next assertions concerning protocol K-M-P1:

G1. Only A and T can decrypt the time-confidential message until a specific time.

G2. B can decrypt the time-confidential message at a specific time. B uses the key from T.

G3. B knows the origin of the time-confidential messages and the ways of the messages in the protocol.

In general we must create the next formal steps when we construct the model and verify the protocols.

4.1 Notations

We need the next notations, operators and functions in the extended Coffey-Saidha model [Kudo and Mathuria 1999]:

a, b, c, ... - general individual variables

ϕ - an arbitrary statement

Σ, Ψ - represent arbitrary entities

i, j - range over entities (possible values from ENT)

ENT - the set of possible entities

K knowledge operator - $K_{\Sigma,t}\phi$ means: Σ knows ϕ at time t

L knowledge predicate operator - $L_{\Sigma,t}x$ means: Σ knows and can reproduce object x at time t

B belief operator - $B_{\Sigma,t}\phi$ means: Σ believes at time t that statement ϕ is true

k **public key** - k_Σ is the public key of entity Σ

k^{-1} **private key** - k_Σ^{-1} is the private key of entity Σ

$e()$ **encryption function** - $e(x, k_\Sigma)$ means: encryption of x using key k_Σ (the output is generally a message)

$d()$ **decryption function** - $d(x, k_\Sigma^{-1})$ means: decryption of x using key k_Σ^{-1} and this function still means: signing of x (the output is generally a message)

S **emission operator** - $S(\Sigma, t, x)$ means: Σ sends message x at time t

R **reception operator** - $R(\Sigma, t, x)$ means: Σ receives message x at time t

C **'contains' operator** - $C(x, y)$ means: object x contains the object y (y may be cleartext or ciphertext in x)

σ **'obtain' operator** - $\sigma_{i,t}(x, y)$ means: i can obtain y from x at time t

Standard logical quantors - $\wedge$ conjunction; $\vee$ disjunction; $\neg$ complementation; $\rightarrow$ implication; $\exists$ existential quantification; $\forall$ universal quantification

4.2 Axioms

We fix the next axioms in the model:

A1(a). $K_{\Sigma,t}p \wedge K_{\Sigma,t}(p \to q) \to K_{\Sigma,t}q$

A1(b). $B_{\Sigma,t}p \wedge B_{\Sigma,t}(p \to q) \to B_{\Sigma,t}q$

A2(a). $K_{\Sigma,t}p \to p$

A3(a). $L_{i,t}x \to \forall t' \geq t \;\; L_{i,t'}x$

A3(b). $K_{i,t}x \to \forall t' \geq t \;\; K_{i,t'}x$

A3(c). $B_{i,t}x \to \forall t' \geq t \;\; B_{i,t'}x$

A4(a). $L_{i,t}y \wedge C(y,x) \to \exists j \in ENT \; L_{j,t}x$

A4(b). $C(x,x)$

A4(c). $C(x,y) \wedge C(y,z) \to C(x,z)$

A4(d). $C(e(x,k_\Sigma),x) \wedge C(d(x,k_\Sigma^{-1}),x)$

A5(a). $S(\Sigma,t,x) \to L_{\Sigma,t}x \wedge \exists i \in ENT \;\; (i \neq \Sigma) \;\; \exists t' > t \; R(i,t',x)$

A6(a). $R(\Sigma,t,x) \to L_{\Sigma,t}x \wedge \exists i \in ENT \;\; (i \neq \Sigma) \;\; \exists t' > t \; S(i,t',x)$

A6(b). $R(j,t,x) \wedge C(x,y) \wedge \sigma_{j,t}(x,y) \to \exists i \in ENT \; \exists t' < t \; \exists z(S(i,t',z) \wedge C(z,y) \wedge L_{i,t'}y \wedge \sigma_{j,t}(x,z) \wedge \sigma_{j,t}(z,y))$

A7(a). $L_{i,t}x \wedge L_{i,t}k_\Sigma \to L_{i,t}(e(x,k_\Sigma))$

A7(b). $L_{i,t}x \wedge L_{i,t}k_\Sigma^{-1} \to L_{i,t}(e(x,k_\Sigma^{-1}))$

A8(a). $\neg L_{i,t}k_\Sigma \wedge \forall t' < t \neg L_{i,t'}(e(x,k_\Sigma)) \wedge \neg(\exists y(R(i,t,y) \wedge C(y,e(x,k_\Sigma)) \wedge \sigma_{i,t}(y,e(x,k_\Sigma)))) \to \neg L_{i,t}(e(x,k_\Sigma))$

A8(b). $\neg L_{i,t}k_\Sigma^{-1} \wedge \forall t' < t \neg L_{i,t'}(d(x,k_\Sigma^{-1})) \wedge \neg(\exists y(R(i,t,y) \wedge C(y,d(x,k_\Sigma^{-1})) \wedge \sigma_{i,t}(y,d(x,k_\Sigma^{-1})))) \to \neg L_{i,t}(d(x,k_\Sigma^{-1}))$

A9(a). $L_{i,t}k_i^{-1} \wedge \forall j \in ENT \backslash \{i\} \neg L_{j,t}k_i^{-1}$

A10(a). $L_{i,t}(d(x,k_\Sigma^{-1})) \to L_{\Sigma,t}x$

A11(a). $L_{i,t}y \wedge \sigma_{i,t}(y,x) \to L_{i,t}x$

R1(a). from $\vdash p$ and $\vdash p \to q$ infer $\vdash q$ (Modus ponens)

R2(a). from $\vdash p$ infer $K_{\Sigma,t}p$

R2(b). from $\vdash p$ infer $B_{\Sigma,t}p$

K1(a). $K_{\Sigma,t}(p \wedge q) \rightarrow K_{\Sigma,t}p \wedge K_{\Sigma,t}q$

K2(a). $K_{\Sigma,t}p \wedge K_{\Sigma,t}q \rightarrow K_{\Sigma,t}(p \wedge q)$

TA1(a). $\forall t < \tau\ L_{T,t}tk_\tau^{-1} \wedge \forall i \in ENT\ (i \neq T)\ \neg L_{i,t}tk_\tau^{-1}$

TA2(a). $L_{i,t}x \wedge L_{i,t}tk_\tau \rightarrow L_{i,t}(e(x, tk_\tau))$

TA2(b). $L_{i,t}x \wedge L_{i,t}tk_\tau^{-1} \rightarrow L_{i,t}(d(x, tk_\tau^{-1}))$

TA3(a). $\neg L_{i,t}tk_\tau \wedge \forall t' < t\ \neg L_{i,t'}(e(x, tk_\tau)) \wedge \neg(\exists y(R(i,t,y) \wedge C(y, e(x, tk_\tau))$ $\wedge\ \sigma_{i,t}(y, e(x, tk_\tau)))) \rightarrow \neg L_{i,t}(e(x, tk_\tau))$

TA3(b). $\neg L_{i,t}tk_\tau^{-1} \wedge \forall t' < t\ \neg L_{i,t'}(d(x, tk_\tau^{-1})) \wedge \neg(\exists y(R(i,t,y) \wedge C(y, d(x, tk_\tau^{-1}))$ $\wedge\ \sigma_{i,t}(y, d(x, tk_\tau^{-1})))) \rightarrow \neg L_{i,t}(d(x, tk_\tau^{-1}))$

TA4(a). $L_{i,t}(e(x, tk_\tau)) \rightarrow L_{T,t}tk_\tau$

TA5(a). $\forall i \in ENT \backslash \{T\}\ \forall t < \tau\ L_{i,t}y \wedge y = e(y', tk_\tau) \wedge C(y', x) \rightarrow \neg\sigma_{i,t}(y, x)$

4.3 Protocol assumptions and general parameters

We use the next assumptions to accord the axioms and the assertions of protocol:

F1. $\forall t < t_8 \forall y S(A,t,y) \wedge C(y, d(x, tk_{t_8}^{-1})) \rightarrow y = e(y', tk_{t_8}) \wedge C(y', d(x, tk_{t_8}^{-1}))$

F2. $\forall t < t_8 \neg\exists y(S(T,t,y) \wedge C(y, d(x, tk_{t8}^{-1})))$

F3. $t_g < t_8$ (t_g denote the time when T generates the private key $tk_{t_8}^{-1}$)

F4. $\forall t < t_g\ \forall i \in ENT(i \neq A)\ \neg L_{i,t}d(x, tk_{t_8}^{-1})$

F5. $\forall t < t_g\ \forall i \in ENT\ \neg L_{i,t}tk_{t_8}$

F6. $K_{B,t_0}(L_{B,t_0}k_A)$

F7. $K_{B,t_0}(\forall t < t_0 \forall i \in ENT\ \neg L_{i,t}N_b)$

4.4 Aims of protocol and assertions

We formalize the protocol goals ($G1.$, $G2.$, $G3.$) in the logic as follows (t_8 is the specific time in the future (Step 1.) and $t_9 > t_8$; t_6 is the time of Step 6.):

Theorem 1 - G1. $\forall t < t_8\ \forall i \in ENT\ (i \neq T, A)\ \neg L_{i,t}(d(x, tk_{t_8}^{-1}))$.

Theorem 2 - G2. $L_{B,t_9}(d(x, tk_{t_8}^{-1}))$.

Theorem 3 - G3. $K_{B,t_6}\ (\exists t\ t_0 < t < t_6\ S(A,t,d(\{U,N_b\},k_A^{-1})))$, *where* $U = e(\{X_a,R_a,A\},tk_{t_8})$, A,B,t_8,tk_{t_8} .

We find the proofs of this theorems in [Kudo and Mathuria 1999].

Turn to further examinations of the protocol and describe the expansion of the protocol.

5 Further examination of the K-M-P1 protocol

Interception is one of the attacking ways of cryptographic protocols. The interceptor E possess the same information at the end of the protocol as B. Therefore E gets hold of the message from A. The interception of the steps 5. and 8. are enough. This is not a mistake from the point of view of the protocol since the base-task does not specify this kind of secrecy.

However, we can ask the following question: Can we extend the protocol in a way that the interceptor does not get a message from A?

We can set up two protective points: either we protect the key or we protect the message.

We modify the original K-M-P1 protocol in the first case as follows (**K-M-P2 protocol**): Let us protect the decryption key: instead of

$$\{\{"dec",t_8,tk_{t_8}^{-1}\}k_T^{-1}\}$$

use the next protocol step

$$\{\{"dec",t_8,\{tk_{t_8}^{-1}\}k_B\}k_T^{-1}\}\ .$$

Namely, we protect the decryption key $tk_{t_8}^{-1}$ with the public key of B.

We modify the original K-M-P1 protocol in the second case as follows (**K-M-P3 protocol**): Let us protect the message. Modify step 5. and 6. in the K-M-P1 protocol: instead of

$$\{\{\{X_a,R_a,A\}tk_{t_8},A,B,t_8,N_b,tk_{t_8}\}k_A^{-1},\{"enc",t_8,tk_{t_8}\}k_T^{-1}\}$$

in step 5. use the next protocol step

$$\{\{\{\{X_a,R_a,A\}tk_{t_8}\}k_B,A,B,t_8,N_b,tk_{t_8}\}k_A^{-1},\{"enc",t_8,tk_{t_8}\}k_T^{-1}\}\ .$$

This is similar to a box with two locks: we use the time-lock tk_{t_8} and the lock k_B of B.[1]

[1] We have several solving points in this case. We can apply encryption for the packet of message X_a too: $\{X_a\}k_B$ which leads to the same result. We get the same result if we use different order of keys.

This modification has an effect on step 6. too, since B repeats the part of the message of A: instead of

$$\{\{\{\{X_a, R_a, A\}tk_{t_8}, A, B, t_8, N_b, tk_{t_8}\}k_A^{-1}\}k_B^{-1}\}$$

use the next protocol step

$$\{\{\{\{\{X_a, R_a, A\}tk_{t_8}\}k_B, A, B, t_8, N_b, tk_{t_8}\}k_A^{-1}\}k_B^{-1}\} .$$

We must expand the Coffey-Shaida logic [Coffey and Saidha 1997] with additional pieces to examination the K-M-P2 and K-M-P3 protocols. We did not use attacker E in the axioms and conditions. E can execute passive attack against cryptosystem. E can eavesdrop every message of participants. We can amplify the assumptions with the following condition:

$$\forall t \ \ \forall i \in ENT \ \ L_{E,t}(S(i,t,x)) . \tag{F8.}$$

After that we can evolve propositions which describe the properties of new protocols. This propositions are the next:

Theorem 4 - G4. *$L_{E,t_9}(d(x, tk_{t_8}^{-1}))$. Attacker E - who eavesdrops messages - has the same information as B at time t_9 after the milestone t_8. Namely, E is able to decrypt the time-confidential messages, too.*

Proof G4. The proof is like theorem $G2$ in the original Kudo-Mathuria article. According to conditions E captures steps 5. and 8. of K-M-P1 protocol. Consequently the next statements are true

$$K_{E,t_6}(R(B, t_6, d(\{e(\{X_a, R_a, A\}, tk_{t_8}), A, B, t_8, N_b, tk_{t_8}\}, k_A^{-1}))) , \tag{1}$$
$$K_{E,t_9}(R(B, t_9, d(\{"dec", t_8, tk_{t_8}^{-1}\}, k_T^{-}1))) . \tag{2}$$

We can extract the appropriate parts since the message contains the signature and the message itself, too:

$$K_{E,t_6}(R(B, t_6, e(\{X_a, R_a, A\}, tk_{t_8}))) , \tag{3}$$
$$K_{E,t_9}(R(B, t_9, tk_{t_8}^{-1})) . \tag{4}$$

With the aid of the results (3), (4) and axiom $A2(a)$ it is possible to write:

$$R(B, t_6, e(\{X_a, R_a, A\}, tk_{t_8})) , \tag{5}$$
$$R(B, t_9, tk_{t_8}^{-1}) \tag{6}$$

and with the (5), (6), (F8.) and axiom $A6(a)$ it is possible:

$$L_{E,t_6}(e(\{X_a, R_a, A\}, tk_{t_8})) , \tag{7}$$
$$L_{E,t_9}(tk_{t_8}^{-1}) . \tag{8}$$

By the help of the (7) and axiom $A3(a)$ it can be formulated in the next way

$$L_{E,t_9}(e(\{X_a, R_a, A\}, tk_{t_8})) \tag{9}$$

with (8), (9) and axiom $TA2(b)$

$$L_{E,t_9}(d(e(\{X_a, R_a, A\}, tk_{t_8}), tk_{t_8}^{-1})) \; .$$

In other words this means we get the following result
(denote $x = e(\{X_a, R_a, A\}, tk_{t_8})$):

$$L_{E,t_9}(d(x, tk_{t_8}^{-1}))$$

which is as required. □

T is an absolute reliable partner - as rules of protocols. Let us forget this condition - for a while and for the sake of the examination - and suppose that T knows the messages of A and B:

$$\forall t \;\; \forall i \in ENT \;\; L_{T,t}(S(i,t,x)) \; . \tag{F9.}$$

At this point T is able to decrypt the time-confidential messages. Moreover T is capable of decrypting the messages (at time t_6) before B. It can be stated as follows:

Theorem 5 - G5. $L_{T,t_6}(d(x, tk_{t_8}^{-1}))$.

Proof G5. As a starting point for our proof we use the identity of the theorem $G2$ in the [Kudo and Mathuria 1999] article. We use the key generating role of T, too. In the first step we describe the next relations:

$$K_{T,t_6}(R(B, t_6, d(\{e(\{X_a, R_a, A\}, tk_{t_8}), A, B, t_8, N_b, tk_{t_8}\}, k_A^{-1}))) \; , \tag{1}$$

$$L_{T,t_6}(tk_{t_8}^{-1}) \; . \tag{2}$$

The proof is carried out analogously to the proof of the theorem $G4$. Let us convert (1) to the next form

$$L_{T,t_6}(e(\{X_a, R_a, A\} tk_{t_8})) \; . \tag{3}$$

With the aid of the axiom $TA2(b)$, we have

$$L_{T,t_6}(d(e(\{X_a, R_a, A\}, tk_{t_8}), tk_{t_8}^{-1})) \; . \tag{4}$$

Let us denote $x = e(\{X_a, R_a, A\} tk_{t_8})$ and then we obtain:

$$L_{T,t_6}(d(x, tk_{t_8}^{-1}))$$

which is as required. □

Theorem 6 - G6 - The case of the protocol K-M-P2. *Eavesdropper E cannot decrypt the encrypted message when we use the protocol K-M-P2 - not even if E knows every message of the partners.*

$$\neg L_{E,t_9}(d(x, tk_{t_8}^{-1})).$$

Proof G6. The proof is the same that of theorem $G4.$:

$$K_{E,t_6}(R(B, t_6, d(\{e(\{X_a, R_a, A\}, tk_{t_8}), A, B, t_8, N_b, tk_{t_8}\}, k_A^{-1}))) \ , \quad (1)$$

$$K_{E,t_9}(R(B, t_9, d(\{"dec", t_8, e(tk_{t_8}^{-1}, k_B)\}, k_T^{-}1))) \ . \quad (2)$$

Like steps of $G4.$:

$$L_{E,t_6}(e(\{X_a, R_a, A\}, tk_{t_8})) \ , \quad (3)$$

$$L_{E,t_9}(e(tk_{t_8}^{-1}, k_B)) \quad (4)$$

we have:

$$L_{E,t_9}(d(e(\{X_a, R_a, A\}, tk_{t_8}), e(tk_{t_8}^{-1}, k_B))) \ . \quad (5)$$

This relation shows we reach the decryption key $tk_{t_8}^{-1}$ only with the secret key k_B^{-1} of partner B. We can produce the form $L_{E,t_9}(d(x, tk_{t_8}^{-1}))$ only with key k_B^{-1}. □

Theorem 7 - G7 - The case of the protocol K-M-P3. *The absolute reliable partner T cannot decrypt the encrypted message if we use the protocol K-M-P3 - not even T knows every message of the partners.*

$$\neg L_{T,t_6}(d(x, tk_{t_8}^{-1})).$$

Proof G7. The proof is like that of theorems before.

$$K_{T,t_6}(R(B, t_6, d(\{e(e(y, k_B), tk_{t_8}), A, B, t_8, N_b, tk_{t_8}\}, k_A^{-1}))) \ ,$$

$$where \ y = \{X_a, R_a, A\} \ , \quad (1)$$

$$L_{T,t_6}(tk_{t_8}^{-1}) \quad (2)$$

whereof follow

$$L_{T,t_6}(d(e(e(y, k_B), tk_{t_8}), tk_{t_8}^{-1})), \ where \ \ y = \{X_a, R_a, A\} \ . \quad (3)$$

On the other hand this relation shows us the breaking-off of the description, too if we do not know the secret key k_B^{-1}. We cannot hold the statement

$$L_{T,t_6}(d(x, tk_{t_8}^{-1})), \ where \ x = e(\{X_a, R_a, A\}, tk_{t_8}) \ .$$

The opposite of the statement is true. □

The role of T is generating the key and proving it in the adequate time in the protocol K-M-P3. A and B are well assured that neither eavesdropper E nor absolute reliable partner T knows the contents of the messages. This fact is advantageous for T because this procedure protects T from charge of eavesdrop.

6 Conclusions

We presented the Kudo-Mathuria protocol (K-M-P1) in the first part of the paper. We examined three properties of the protocol with logic tools. After that we expanded the K-M-P1 protocol (K-M-P2, K-M-P3). We have proved four new properties of the expanded protocol.

We have developed and enhanced the original Kudo-Mathuria protocol. In this meaning we have expanded the fields of application of the protocol.

Acknowledgements
The author would like to thank professor Attila Pethő and Tamás Mihálydeák for supervising the proofs.

References

[Burrows, Abadi and Needham 1989] Michael Burrows, Martín Abadi, Roger Needham: "A Logic of Authentication"; Digital System Research Center, Research Report 39, 1989.

[Buttyán 1999] L. Buttyán: "Formal methods in te design of cyptography protocols (State of the Art)"; EPFL SSC Technical Report No. SSC/1999/038. - 26.11.1999.

[Coffey and Saidha 1997] T. Coffey, P. Saidha: "Logic for verifying public-key cryptographic protocols"; IEE Proc.-Comput. Digit. Tech. Vol. 144. No. 1. January, 1997.

[Kudo and Mathuria 1999] Michiharu Kudo, Anish Mathuria: "An Extended Logic for Analyzing Timed-Release Public-Key Protocols"; ICICS'99, Second Information Conference, Sydney, 1999.

[Kyntaja 1995] Timo Kyntaja: "A Logic of Authentication by Burrows, Abadi and Needham";
http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/ban.html.

[May 1995] Timothy C. May: "Time release Crypto";
http://cypherpunks.venona.com/date/1995/09/msg01183.html

[Meadows 1995] C. Meadows: "Formal verification of cryptographic protocols: A survey"; In Advances in Cryptology - ASIACRYPT'94, pages 135-150. Springer-Verlag. 1995.

[Rubin and Honeyman 1993] A.D. Rubin, P. Honeyman: "Formal Methods for the Analysis of Authentication Protocols"; CITI Technical Report 93-7. 1993.

[Rivest, Shamir and Wagner 1996] R. L. Rivest, A. Shamir, D. A. Wagner: "Time-Lock Puzzles and Timed-Release Crypto"; Technical Report, MIT Laboratory for Computer Science, 1996.