TÖBBCSATORNÁS KRIPTOGRÁFIAI PROTOKOLLOK GYAKORLATI VIZSGÁLATA

examining of multichannel cryptographic protocols

Takács Péter[1], Vályi Sándor[2]

DE OEC EK Egészségügyi Informatika Tanszék[1],

DE AMTC AVK Gazdaság- és Agrárinformatikai Tanszék[2]

Összefoglaló

Az informatikai eszközök mobilitásának növekedése révén egyre gyakrabban olyan környezetben kell megvalósítani a kriptográfiai primitívekkel kapcsolatos alapfeladatokat, amelyek nem tartalmaznak szerveroldali támogatást. Ezek a követelmények újabb és újabb kriptográfiai protokollok megszületését eredményezik. A megfelelő szintű biztonság elérésére egyre gyakrabban alkalmazzák az eszközök azon lehetőségét is, hogy azok több kommunikációs csatornát is képesek kezelni (vezeték nélküli elérés, manuális adatátvitel, vezetékes kapcsolat, stb.). Az általunk tanulmányozott MANual Authentication Protocol (MANA) főleg vezeték nélküli (wireless) eszközök hitelesítésére lett kialakítva. Ez a hitelesítés egy nem biztonságos vezeték nélküli csatornát egészít ki manuális adatátvitellel (mint második csatorna). Munkánk során a BAN-logikára épülő CSN-logikát bővítettük úgy, hogy az alkalmas legyen a többcsatornás kriptográfiai protokollok vizsgálatára. Eredményeink a következők: formális eszközökkel bebizonyítottuk, hogy a MANA protokollcsalád első tagja (MANA I) a kitűzött célt helyesen valósítja meg. Elemzésünkkel megállapítottuk, hogy a MANA II protokoll az elérni kívánt célnak csak részben felel meg, mivel olyan lépést tartalmaz, aminek gyengeségét kihasználva a két fél azonosító folyamata folyamatosan akadályozható. Végül javaslatot teszünk a feltárt MANA II hiba javítására.

Kulcsszavak
többcsatornás kriptográfiai protokollok, formális verifikáció, modális logika, MANA protokollcsalád

Abstract

By the growth of mobility of infocommunication devices we have to implement the cryptographic primitives in an environment without any support of trusted servers. These requirements induce development of new protocols. The multi-channel ability of the new devices is very useful to provide an appropriate level of security. The goal of protocol MANA is mainly authentication of wireless devices. In the process of authentication, the protocol utilizes a second manual channel besides a non-secured open channel. In this paper we have extended the BAN-logic based Coffey-Saidha-Newe theory to be usable in verification of multi-channel protocols. We have proved by formal method that the first variant (MANA I) is correct. We have pointed out that MANA II is only partially correct because it involves a step in the protocol that is a possible object of obstruction. Finally we propose a possible correction of protocol MANA II which eliminates this disadvantage.

Keywords
multi-channel cryptographic protocols, formal verification, modal logic, MANA protocol family

1. **Bevezetés**

2005-ben több mint 9 milliárd mikroprocesszort állítottak elő világszerte. Ezen alkatrészeknek csak kevesebb mint 2%-át építették be számítógépekbe (PC, Mac, Unix, stb.). A fennmaradó közel 8,8 milliárd processzor-egység beágyazott rendszerekbe került. [5]

Ma minden modernnek nevezett elektronikus eszköz rendelkezik egy vagy több beépített processzorral és a megfelelő működtető háttérrel. A zenés képeslapoktól kezdve a közlekedési lámpákon át a nukleáris erőművek vezérlő rendszeréig mind tartalmaznak vezérlő, működtető processzorokat. Ezek az egységek az egyszerűnek tekintett 4 bites mikrokontrollerektől kezdve a felsőbb szintű 128 bites processzorokig terjednek.
Az alkalmazott megoldások egy része a felhasználók számára közvetlenül elérhető, kezelhető és kezelendő, más része viszont "rejtett", a háttérben működik.
Környezetünkben - személyes környezet, lakás, - biztosan találunk több olyan berendezést, elektronikus eszközt, amely szintén tartalmaz mikroprocesszort. Gondolhatunk itt a mobiltelefonra, televízióra, rádióra, mosógépre, stb.
Ezen eszközök egyre nagyobb hányada kommunikációra, adatcserére is képes társaival, más eszközökkel. A kapcsolat vezeték segítségével, vagy vezeték nélkül, általában elektromágneses sugárzás felhasználására épül. Ennek okán a területi kiterjedés szerinti osztályozás szokásos kategóriái (LAN, MAN, WAN, stb.) mellett megjelent a PAN (Personal Area Network - Személyi hálózat) fogalma. A kapcsolódás lehet „kézi” („manual”), emberi beavatkozást igénylő, vagy automatikus. Az automatikus beállítású és önmenedzselő eszközökből épített PAN rendszerek ismét külön kategóriát alkotnak - ASPAN (Autoconfiguration and Self-management of Personal Area Networks) néven.
A PAN és ASPAN eszközök legalább egy alapvető különbséget mutatnak nagyobb méretű társaikhoz képest: a kiszolgáló háttér megléte vagy annak hiánya. A kisebb, személyes környezetben alkalmazott eszközök kommunikációját általában nem segíti szerver háttér. Ez az alapvető különbség számos következménnyel jár. Az egyik ezek közül a biztonság kérdése. PAN és ASPAN környezetben hasonló biztonsági és titkosítási kérdések merülnek fel, mint a nagyobb hálózatoknál: felhasználó azonosítás, kulcskezelés, rejtjelezés, digitális aláírás, üzenethitelesítés, stb. Kérdés az, hogy hogyan oldhatók meg ezek a feladatok szerver háttér, külső támogatás nélkül.
A továbbiakban egy speciális területtel, az „imprinting” kérdésével foglalkozunk. Ennek a feladatkörnek a lényege az, hogy a biztonságos és megfelelően védett kommunikációs folyamat kialakításához megfelelő paraméterek beállítására és átadására van szükség az eszközökön, az eszközök között. Magyarra fordítva: alapparaméterek beállítása és átadása - kriptográfiai inicializálás. Ezeken a beállításokon alapulnak a későbbi működés alapvető vonásai, így elmondható, hogy az inicializálási folyamat itt is igen érzékeny részét képezi a kriptográfiai rendszereknek. [8][13] Amennyiben lehetséges a kriptográfiai inicializálás lehallgatása, vagy más irányú támadása, az azt követő - az inicializálásra épülő, védeni kívánt - kommunikációs folyamat sebezhetővé válik.
Sok esetben védett csatornákat alkalmaznak az alapparaméterek beállítása során. PAN környezetben a biztonsági csatorna alapulhat
- rögzített kapcsolódáson (kábel, USB interfész, vonalkód leolvasó, stb.),
- emberi beavatkozáson (jelszavak leolvasása, beírása, átírása, stb.),
- egyéb „kis hatósugarú” technikán (másodlagos vezeték nélküli csatorna, stb.). [8]
Amikor két eszköz először kapcsolódik, semmi nem alapozza meg hitelességüket. PAN környezetben gyakran feltételezik azt, hogy az eszközök inicializáló folyamatában részt vesz egy aktívan közreműködő felhasználó is. Ez egyrészt megteremti a biztonsági csatorna könnyű kialakíthatóságának lehetőségét, másrészt módot ad a többfaktoros kriptográfia eredményeinek alkalmazására is. A használt protokollokban lehetőség van ellenőrizni azt, hogy mindkét PAN berendezés rendelkezik ugyanazzal az információval - kriptográfiai inicializálással -, amely kulcsfontosságú a későbbiekben.

Az általunk vizsgált MANA protokollcsalád hasonló célokkal és megoldási struktúrával bír, általában az inicializáló protokoll-folyamat adategyeztető szerepét tölti be. A következő fejezetekben bemutatjuk a MANA protokollcsaládot, majd néhány tagjának formális vizsgálata során elért eredményeinket.

2. A MANA protokollcsalád

A variánsokat figyelmen kívül hagyva négy alapprotokoll tartozik jelenleg a MANA protokollcsaládba. Ezek között az alapvető különbség a kommunikáló eszközök által alkalmazható input/output felszereltségben (billentyűzet, LED, kijelző, képernyő, beviteli gomb, nyomógomb, stb.) van. Legalább két csatorna áll rendelkezésre az adatok átvitelére. A nyilvános csatorna általában gyors és szélessávú; míg a nem nyilvános (védett) csatorna általában manuális csatorna kis kapacitással – a felhasználók olvassák és/vagy írják a csatornajeleket. [6][10][17]

Például a MANA I protokoll esetén az egyik eszköznek kijelzője és egy egyszerű input gombja, míg a másik eszköznek billentyűzete van és egy LED-el rendelkezik. MANA II esetén mindkét eszköznek kijelzője van input gombokkal. [6] A MANA III két eszköze billentyűzetet és LED-et használ. Az egyszerűnek nevezett input gombok (bináris kapcsoló) és output LED-ek (bináis kijelző) általában a protokoll végén az elfogadás, vagy elvetés jezésére szolgálnak. [8] A MANA IV protokoll inkább a csatornákra fekteti a hangsúlyt. Ez a megoldás a „Commitment Scheme”-re alapozva oldja meg a feladatot. [10] A MANA III-tól kezdve a csatornatulajdonságok a protokollokban egyre nagyobb szerepet kapnak.
A protokollcsalád közösnek tekintett feladata a kriptográfiai inicializálás. Ez itt konkrétan azt jelenti, hogy a protokollokban *A*-val és *B*-vel jelölt egységek egy D_A-val jelölt sztringet akarnak egyeztetni – közösen kialakítani és a későbbiekben a védett kommunikáció alapjaként felhasználni. A sztring például kialakítható a két egység nyilvános kulcsainak egymás után fűzésével, véletlenszám generálás eredményeként, vagy más alkalmas módon.

3. Formális vizsgálatok, a CSN-logika bővítése

A kriptográfiai protokollok vizsgálatára napjainkra két fő irányzatot alakított ki kutatás. Az egyik a számításelméleti megközelítés (főleg komplexitás-elméleti és valószínűségelméleti eszközök alkalmazása épülve), a másik pedig a formális megközelítés (főleg modális logikai eszközökre építve). [3][7][9][14]

A formális módszerek a kriptográfiai protokollok tervezésének és ellenőrzésének különböző szakaszaiban használhatók. A leginkább kutatott az ellenőrzés (verifikálás) szakasza. [2]
A modális logika alkalmazásának sémája a kriptográfiai protokollok ellenőrzése során a következő:
1. lépés: a vizsgált protokollok formalizálása,
2. lépés: a kezdeti feltételek meghatározása,
3. lépés: a protokoll céljainak meghatározása,
4. lépés: a célok levezetése a protokoll leírása során keletkezett formulákból, kezdeti feltételekből, logikai lépések egymásutánjával.
Munkánk során a BAN-logikán (Burrow-Abadi-Nedham) [1] alapuló CSN-logikát (Coffey-Saidha-Newe) [4] [12] fejlesztettük tovább.
A CSN-logika nem alkalmas a többcsatornás kriptográfiai protokollok vizsgálatára. A fejlesztés során úgy

bővítettük az eredeti rendszert, hogy az alkalmassá vált a megjelölt feladatra.
A CSN logika teljes és szabatos leírása terjedelmi okokból itt nem szerepelhet, de a következő vázlat elegendő útmutatást adhat az eredmények leírásához (teljes leírás található az említett [4], [12] cikkekben).
A logikai rendszer szintaktikai eszközöket tartalmaz a kommunikációban résztvevő egyedek és állapotok leírására, tartalmaz függvényeket és operátorokat. A rendszer alkalmazza a klasszikus logikai jeleket: konjunkció, duszjunkció, negálás, implikáció, stb. Használjuk az univerzális és az egzisztenciális kvantorokat, és más ismert matematikai jelölésmódokat. A rendszer hét következtetési szabályt sorol fel, amelyek megegyeznek a hagyományos logikai rendszerek következtetési szabályaival (modus ponens, általánosítási szabály, stb.).
Az axiómák két típusba sorolhatók: az első a logikai axiómák köre (4 axióma, A1-A4); a másik típusú axiómák a nem-logikai axiómák (10 axióma, A5-A15), amelyek a nyilvános- és a titkos kulcsú kommunikáció körét foglalják magukba. Ezek az axiómák leírják a kriptográfiai primitívek és a folyamat szereplőitől elvárt tulajdonságokat.
Az eredeti Coffey-Saidha rendszer ([4] A1-A10) a nyilvános kulcsú kriptográfiai protokollok analízise során alkalmazható, az axiómák második része ([12] Newe- Coffey, A11-A15) pedig a szimmetrikus kulcsú protokollok leírására.
A rendszer nem tartalmazta a többcsatornás protokollok körébe eső vizsgálatok megfogalmazásásnak lehetőségét, ami szükségessé tette a bővítést, ha többcsatornás protokollok formalizálására akarjuk használni az adott logikai rendszert. Ennek során a következő alapcélokat tűztük magunk elé:

1. Az eredeti rendszer kiterjesztése a csatornákat megkülönböztető jelölésmóddal.
2. A különböző csatornák eltérő tulajdonságainak leírási lehetőségének biztosítása.

Az említett célok megvalósítását a következő módon értük el. Külön jelöltük a csatornák számát, és megkülönböztettük a ch_i jelölés alsó indexében magukat a csatornákat. Fontos volt számunkra jelölni, hogy egy csatorna védett, vagy nyilvános, ennek jelölése külön szintaktikai elemet kapott. Amennyiben egy csatorna védett, meg tudjuk adni azoknak a felhasználóknak a halmazát, akik használják a csatornát.

A második cél elérésére a következőket alkalmaztuk: a csatornák eltérő tulajdonságait a protokollok formalizálása során a kezdeti feltételeknél adtuk meg minden esetben. Például axiómákkal írtuk le a biztonságos csatornák működésének alaptulajdonságait. Ezen axiómákat úgy választottuk meg, hogy a formális leírás a MANA protokoll leírásában informálisan elvárt tulajdonságokat írja le.
Ezeket a feltételeket figyelembe véve már lehetőségünk volt úgy bővíteni az eredeti CSN logikai rendszert, hogy az alkalmas legyen a többcsatornás protokollok alapvizsgálataira.
A következő lépésünk a bővítés során a csatorna-jelölés alkalmazása volt a logikai rendszerben. Ennek során az *R* fogadó és *S* küldő operátort kellett megváltoztatnunk, hogy bennük alkalmazhassuk a csatornajelölést. Így például az új $R(ch_i, A, t, x)$ operátor jelentése: az *A* egyed a *t* időpillanatban az *x* üzenetet fogadja a ch_i csatornán; az új $S(ch_i, A, t, x)$ operátor jelentése: az *A* egyed a *t* időpillanatban az *x* üzenetet küldi el a ch_i csatornán.
Az axiómákat átvizsgálva, az A5, A6, A8, A12 és A15 axiómákat kellett átfogalmaznunk a csatornajelek segítségével. Ahhoz, hogy a többcsatornás protokollokat elemezni tudjuk egy új, *A16* jelü axiómát vezettünk be. Ennek lényege a következő. Amennyiben ch_b csatorna védett és a ch_b csatornát *i* és *j* egyedek képesek használni és az *i* egyed a *t* időpontban az *x* üzenetet küldte a ch_b csatornán és a *j* egyed egy *y* üzenetet fogadott a *t'* időpontban a ch_b csatornán és *j* nem fogadott más üzenetet a ch_b csatornán a *t* és *t'* időpontok között, akkor az *x* és *y* üzenetek megegyeznek.
Számos más feltételt is rögzíteni lehetne az axiómarendszerben (például a különböző támadási lehetőségekből kiindulva finomítani lehet a csatorna-jelölési rendszert), de a bővítést ezen a ponton lezártuk, hogy a kialakított rendszer életképességét gyakorlati szinten is bizonyíthassuk többcsatornás protokollok

vizsgálata során. A továbbfejlesztés későbbi munka tárgyát képezheti.

4. A MANA protokollcsalád vizsgálata – MANA II módosítása

Az előző fejezetben bemutatott bővítés felhasználásával tanulmányoztuk a MANA protokollcsalád egyes tagjait. Eredményeink összefoglalva a következők:

Legyenek D_A és D_B a kialakítandó inicializáló paraméterek.

1. Tétel: A MANA I protokoll befejeződésekor mind az *A*, mind a *B* fél egyértelműen tudja, hogy $D_A=D_B$ teljesül, vagy nem. [15]

2. Tétel: Tegyük fel, hogy a MANA II protokoll működése során egy külső fél beavatkozott a kommunikációba, vagyis az *A* fél által elküldött D_A paraméter nem egyezik meg a *B* által kapott D_B paraméterrel. A MANA II protokoll befejeződésekor mind *A* és mind *B* is tudja, hogy $D_A \neq D_B$. [16]

3. Tétel: A MANA II protokoll elején helyesen átküldött D_A paraméter (ekkor $D_A=D_B$) nem garantálja, hogy a protokoll lezárásakor *A* és *B* is tudja, hogy $D_A=D_B$. [16]

A 3. és 5. tétel esetén a felek hiába rendelkeznek a helyes D_A értékkel, annak közös elfogadhatóságát a protokoll nem tudja garantálni. Mivel a felhasznált kulcsok nyilvános csatornán kerülnek továbbításra, egy támadó fél módosítani tudja értéküket, megzavarva a protokollt. Ismételt kulcsküldés már a protokoll hatáskörén kívül esik. Az újra és újra lejátszott eredménytelen protokoll-ismétlések pedig a felhasználók bizalmának elvesztését jelenthetik. Hasonló eset alakulhat ki, mint amikor biztonsági rendszereket kapcsolnak ki a generált téves riasztások elkerülésére.

Részletesebben **MANA II** esetén a következő megállapításokat tehetjük. [6]

Kiinduló feltételek és jelölések: *A, B, U* a protokoll szereplői (*A* és *B* vezeték-nélküli kommunikációra képes eszközök, *U* pedig az azokat kezelő felhasználó). A MANA II protokollban mindkét eszköznek egy kijelzője van (output), de nem rendelkeznek billentyűzettel (csak egy jelzőgomb, kapcsoló áll rendelkezésre – 1 bites input). A használt csatornák: ch_1 – nyilvános nagy kapacitású csatorna – vezeték-nélküli kapcsolat; ch_2, ch_3 – védett, kis kapacitású csatorna – emberi beavatkozással létrejövő csatorna, itt U olvassa az *A* és *B* kijelzőket.

A protokoll lépései a következők:

1. *A* elküldi *B*-nek a D_A paramétert a ch_1 csatornán. *B* D_B paramétert kap ch_1-en (ch_1 nem védett csatorna, így feltételezzük, hogy egy támadó képes megváltoztatni az üzenet tartalmát, ezt jelöljük ezen a módon).
2. *A* generál egy véletlen *K* kulcsot (16-20 bit), és kiszámítja az $m_K(D_A)$ ellenőrző összeget. Ezután *A* átküldi *K* és $m_K(D_A)$ értékeket *U*-nak a védett ch_2 csatornán (vagyis megjeleníti a kijelzőjén) . Itt m_K egy *K* inicializáló értékkel ellátott hash-függvényt formalizál.
3. *A* elküldi *K*-t *B*-nek ch_1 a csatornán. *B* *K'*-t kap.
4. *B* kiszámítja az $m_{K'}D_B$ értéket és elküldi *K'*-t és $m_{K'}D_B$-t U-nak a védett ch_3 csatornán (megjeleníti kijelzőjén).
5. *U* összeveti a *K* és *K'* és az $m_K(D_A)$ és $m_{K'}(D_B)$ értékeket a kijelzőkön. Jelölje *x* ennek az összehasonlításnak az eredményét. Legyen *x='1'* ha *K=K'* és $m_K(D_A)=m_{K'}(D_B)$. Legyen *x='0'* minden egyéb esetben. *U* ezután elküldi *x*-et *A*-nak a ch_2 csatornán (vagyis használja *A* input kapcsolóját).
6. Végül *U* elküldi *x*-et *B*-nek a ch_3 csatornán (használja *B* input kapcsolóját).

Elemzés és javaslatok: A kulcs a 3. lépésben kerül átküldésre a *B* félnek, aki egy ellenőrző összeget számít ki a kulcs segítségével, majd az összeget átküldi *U*-nak összevetésre. A gyakorlati megvalósítás többféle ellenőrző összeget használhat. Az eredeti MANA II protokoll kulcsolt hash függvényt alkalmaz. Amennyiben nem kulcshoz kötődő, hanem „hagyományos" hash függvényt alkalmazunk (MD sorozat, SHA sorozat, HAVAL, RIPEM sorozat, stb. [3] [11]), úgy feleslegessé válik a kulcs alkalmazása, a kulcsok átküldése.
A módosított protokoll a következő lépésekkel működhet:
1. *A* elküldi *B*-nek a D_A paramétert a ch_1 csatornán. *B* D_B paramétert kap ch_1-en.
2. *A* kiszámítja az $m(D_A)$ ellenőrző hash összeget és azt *U*-nak a védett ch_2 csatornán.
3. *B* kiszámítja az $m(D_B)$ hash értéket és elküldi ezt U-nak a védett ch_3 csatornán.
5. *U* összeveti a az $m(D_A)$ és $m(D_B)$ értékeket. Jelölje *x* ennek az összehasonlításnak az eredményét. Legyen $x='1'$ ha $m(D_A)=m(D_B)$. Legyen $x='0'$ minden egyéb esetben. *U* ezután elküldi *x*-et *A*-nak a ch_2 csatornán.
6. Végül *U* elküldi *x*-et *B*-nek a ch_3 csatornán.

A módosított protokoll kialakítása során természetesen figyelembe kell venni a szakirodalom ajánlásait, amelyekről többek között [11]-ben olvashatunk. A paraméterek beállítása során azon támadásoknak, amely a hash függvény alkalmazásakor előre beépített paraméterek ismeretén alapul gátja, hogy egyelőre nem ismeretes olyan algoritmikus támadás az általánosan használt hash-függvények esetén, amely tetszőleges input szöveghez vele azonos hash-értékkel rendelkező másik szöveget konstruál. Ugyanakkor az is elmondható, hogy a véletlen kulcsok megfelelő minőségű generálásához (eredeti protokoll 2. lépés) szintén megfelelő kezdeti paraméterek kellenek.

5. Összegzés

A napjainkban egyre nagyobb tért hódító személyes hálózatok (PAN, ASPAn, stb.) újabb és újabb protokollok megszületését indukálják. Ezeknek a protokolloknak az elemezése fontos, hiszen sok esetben érzékeny személyes adatokat közvetítenek (például egészségügyi rendszerek). Munkánk során a CSN-logikai rendszert bővítettük úgy, hogy az alkalmas legyen többcsatornás megoldások vizsgálatára. Bemutattuk a MANA protokollcsalád elemzése során elért eredményeinket. A II-es protokollokban támadható rés fedezhető fel, a protokollok működése megzavarható. A bemutatott megoldási javaslat a kriptográfiában gyakran használt hash függvényre épül, amelyek alkalmazása szintén sok megfontolást és gyakorlati tapasztalatot igényel. További céljaink között szerepel a vizsgált protokollok körének bővítése, az alkalmazott bővített CSN-logika felhasználhatóságának további igazolása.

Irodalomjegyzék

1. M. Burrows, M. Abadi, R. Needham (1989) A Logic of Authentication. Research Report 39., Digital System Research Center.

2. L. Buttyán (1999) Formal methods in the design of cyptographyprotocols (State of the Art), EPFL SSC Technical Report, No.SSC/1999/038.

3. Buttyán L., Vajda I. (2005) Kriptográfia és alkalmazásai. TypoTex Kiadó, Budapest, 99-110.

4. T. Coffey, P. Saidha (1997) Logic for verifying public-key cryptographic protocols, IEE Proc. Computers and Digital Techniques, Vol.\ 144. No. 1., 28--32.

5. Embedded Systems Glossary [http://www.netrino.com/Embedded-Systems/Glossary]

6. C. Gehrmann, C. J. Mitchell, K. Nyberg (2004) Manual authentication for wireless devices. Cryptobytes, 7(1) 29—37.

7. Gergely Á. (2005) Biztonságos útvonalválasztás ad hoc hálózatokban. Diplomamunka, Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informati-kai Kar, Híradástechnikai Tanszék, Budapest.

8. S. Goeman ed. (2002) Specification of Prototypes - D11, IST - 2000 - 25350 - SHAMAN, Public Report, 26-29.

9. Ködmön J. (1999) Kriptográfia. ComputerBooks, Budapest, 124-128,141-143.

10. S. Laur, K. Nyberg (2006) Efficient Mutual Data Authentication Using Manually Authenticated String: Extended Version. Cryptology ePrint Archive, Report 2005/424. A shorter more compact version was published at CANS 2006.

11. Minorov, I. (2005) Hash functions: Theory, attacks, and applications. Technical Report TR-2005-187, Microsoft Research.

12. T. Newe, T. Coffey (2003) Formal verification logic for hybrid security protocols. Comput. Syst. Sci. and Eng., Vol.\ 1., 17--25.

13. Pethő A. (2002) Paraméterválasztás nyilvános kulcsú kriptográfiai rendszereknél. Kriptográfia és alkalmazásai szeminárium, SZTAKI, Budapest.

14. B. Schneier (1996) Applied cryptography: Protocols, algorithms and source code in C. John Wiley & Sons, Inc. Second edition.

15. P. Takács (2007) The Extension of CNS-logic for Multi-Channel Protocols. Proceedings of the 7th ICAI Conference, Eger.

16. P. Takács, S. Vályi (2007) On Verification of the MANA Protocol Family. 7th Central European Conference on Cryptology, Smolenice, Slovakia.

17. F-L. Wong, F. Stajano (2005) Multi-channel protocols. Proceedings of Security Protocols Workshop, LNCS, Springer-Verlag.