Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Seminarska naloga

Bluetooth

Naziv študija: Informacijski sistemi in odločanje
v okviru podiplomskega magistrskega programa

Naziv predmeta: Kriptografija in računalniška varnost

Učitelj: **doc. dr**. Aleksandar Jurišić

Študent: Matej Grom, 24930473
elektronska pošta: matej.grom@fri.uni-lj.si
http://aris.fri.uni-lj.si/~grommate

Ljubljana, 13. 7. 2004

Kazalo

1. Uvod

Tako kot se ljudje radi povezujemo med seboj, prav tako želimo med seboj povezovati naprave. Nihče namreč ne obvlada vsega, kot celota pa smo močnejši. Prav tako povezane specializirane naprave nudijo precej večjo funkcionalnost za ugodno ceno, kot pa ena velika univerzalna. Dokler so bile te naprave velike in smo jih težko prenašali naokoli, nas je motil le gozd žic, ki se je spletal okrog posameznega mesta, kjer so bile povezane v celoto.
Prva učinkovita rešitev priklapljanja naprav brez žic so bili infrardeči vmesniki. Zadovoljevali so potrebe po povezovanju naprav, ki so občasno prišle v stik, brez lomljenja priključkov in prepletanja po goščavi kablov. Imeli pa so eno veliko pomanjkljivost. Niso podpirali mobilnosti. To pomeni, če si samo malo premaknil eno ali drugo napravo ni bilo daleč do prekinitve povezave, saj so morale naprave komunicirati v vidnem polju.
Bluetooth prinaša ugodje radijskega prenosnega medija, da se napravam ni potrebno medsebojno optično videti. Le dovolj blizu morajo biti skupaj. Ta prednost pa prinaša tudi velike probleme pri zaščiti prenesenih podatkov, saj jih lahko prestreza ali ponareja tudi kdo, ki ga ne vidimo, podatki pa mu nikakor niso namenjeni.

Namen seminarske naloge je pregledati kakšne varnostne mehanizme so uporabili v bluetooth protokolu, kot tudi koliko sploh prispeva varnost bluetootha k celotni varnosti komunikacij, ki jih preko tega protokola uporablja navaden uporabnik osebnega računalnika.

Predstavitev se začne z zgodovino bluetooth protokola in umestitvijo v omrežno infrastrukturo, ki se uporablja v današnjih informacijskih sistemih. Velikokrat se namreč izkaže, da je bluetooth le najnižja omrežna plast.
V drugem delu poglavja 3 so opisani še načini delovanja bluetooth protokola na fizični in varnostni plasti.
V osrednjem poglavju 4 je predstavljen celoten potek vzpostavljanja varne povezave in kreiranja šifrirnih ključev, kot tudi kateri algoritmi se uporabljajo. Na koncu sledi predstavitev stanja uporabe protokola bluetooth danes. Tako s stališča razširjenosti, kot s stališča upoštevanja specifikacije na področju varnosti.

2. Omrežja

Najbolj opazna lastnost omrežij je njihova večplastnost, Vidmar [3]. Vsaka nižja plast omogoča določene storitve višji plasti. Višja plast pa s pomočjo storitev nižjih plasti tvori virtualni kanal na svojem komunikacijskem nivoju. Virtualno se v komunikaciji plasti pogovarjajo med sabo preko virtualnih kanalov, medtem ko za fizični prenos podatkov skrbijo nižje plasti, Vidmar [3]. Tako je najvišja plast aplikacijska (spletni brskalnik se pogovarja s spletnim strežnikom). Nižja, transportna plast pa v resnici poskrbi za komunikacijo, to je prenos paketov med napravama, ki komunicirata. Končno najnižja fizična plast poskrbi, da se podatki res lahko prenašajo po mediju, na katerega je naprava priključena. Seveda lahko komunikacija poteka preko mnogo fizičnih plasti.
Po OSI[1] omrežnem modelu skrbi za varnost povezave predzadnja predstavitvena plast, Herfurt [5]. V TCP/IP modelu pa je predstavitvena plast kar del aplikacijske plasti. Torej morajo aplikacije same poskrbeti za varnost in šifriranje podatkov med prenosom.
Čeprav je bluetooth tudi sam omrežni protokol z večplastno zgradbo, pa velikokrat služi le v prenosne namene višjenivojskim protokolom. Zato je potreba po varnosti različna od vrst uporabe, ki jih želijo posamezni uporabniki. Za varnost lahko pri uporabi višjenivojskih protokolov poskrbijo ti protokoli, medtem, ko pri osnovni komunikaciji med bluetooth storitvami naprav (na primer tiskanje na tiskalnik) ni uporabljen noben višjenivojski protokol, ki bi zagotavljal varnost povezave. Torej moramo pri ugotavljanju potreb po varnosti protokola bluetooth najprej določiti, kje v množici komunikacijskih storitev, ki jih uporabljamo, se sploh nahaja. Če za varnost povezave skrbimo na ravni aplikacijskega protokola TCP/IP ni nobene potrebe po dodatnem ščitenju fizične plasti komunikacije, ki jo v takem primeru znotraj TCP/IP opravlja bluetooth.

2.1. Vrste omrežij

Delitev omrežij glede na razsežnosti, kot so lokalna (LAN[2]) in prostrana (WAN[3]) z vedno bolj razširjeno uporabo interneta in večanjem zmogljivosti prenosnih kanalov vedno bolj izgublja pomen. Kot nekakšen kompromis so se pojavila mestna omrežja (MAN[4]). Vendar uporabnik pri svojem delu ponavadi sploh ne opazi po kakšni vrsti omrežja se danes prenašajo njegovi podatki. Prav tako tudi naprave priključene v to omrežje nimajo nobenih mehanizmov za zaznavanje razlik, razen poznavanja naslovov partnerskih naprav.
Bluetooth spada v novo vrsto osebnih omrežij (PAN[5]). Pojem osebnega omrežja je relativno nov pojem, bluetooth pa je prvi v družini teh protokolov, katerih razmah se pričakuje v prihodnjem desetletju.

Osebno omrežje

Osebno omrežje ima povsem druge zahteve glede zanesljivosti prenosnih poti in varnosti. Zaradi kratkega dometa in majhnih oddajnih moči morajo biti radijski protokoli odporni proti motnjam močnejših naprav, ki delujejo v istem frekvenčnem spektru, ki je običajno splošno dostopen in uporabljan.

[1] OSI – Open System Interconnection, omrežni model, Vidmar [3]
[2] LAN – Local Area Network
[3] WAN – Wide Area Network
[4] MAN – Metropolotan Area Network
[5] PAN – Personal Area Network

Naprave uporabljajo frekvenčni spekter, ki predstavlja javno dobro. Zato je v njem velika gneča in sami fizični prenosni protokoli morajo biti odporni proti takim motnjam pri dostopu do skupinskega medija.
Pri zagotavljanju varnosti pa imamo na voljo tudi drug komunikacijski kanal, ki omogoča varno prenašanje simetričnih ključev in gesel med napravami ob vzpostavitvi povezave. Ta varni kanal je kar uporabnik sam. Uporabnik le združuje poljubne naprave v osebno omrežje in jih ima vsaj v času priklopa v omrežje vedno na dosegu. Tako se v veliki meri izognemo pastem napada, ko bi se lahko napravi lažno predstavili ena drugi.
Vsa osebna omrežja uporabljajo tehniko izredno hitrega menjavanja frekvenc (Frequency Hoping). V preteklosti je že ta tehnika predstavljala veliko zagotovilo varnosti komunikacije. Danes pa to nikakor več ne zadošča. Menjavanje frekvenc je pravzaprav nuja zaradi učinkovite izrabe frekvenčnega pasu v katerem deluje množica naprav.

3. Bluetooth

3.1. Zgodovina

Bluetooth standard verzija 1.0 je bil sprejet leta 1999, medtem ko je bil leta 2001 sprejet standard verzija 1.1 Trenutno je aktualna verzija 1.2, ki je ugledala luč sveta leta 2003, medtem ko je verzija 2.0 zaenkrat dostopna samo razvijalcem.
Leta 2001 je bil ustanovljen Bluetooth Special Interest Group (SIG), ki skrbi za promocijo in ugled standarda. Danes je bluetooth v vzponu svoje resnično uporabne poti. Na tržišču se pojavlja vedno več raznovrstnih naprav, ki ga podpirajo. Problemi z združljivostjo so vedno manjši in tudi uporabniške izkušnje so vedno boljše. Tako je bluetooth uspešno prestal fazo navdušenja in razočaranja ter počasi prehaja v zrelo fazo, ko je že presegel uporabo samo na področju mobilne telefonije.

3.2. Osnovne ideje

Osnovna ideja je povezovanje mobilnih naprav med seboj in z ostalimi elektronskimi napravami na kratke razdalje brez kablov in za majhno ceno. Tako tretira brezžična omrežja kot komplementarna, saj skrbijo pretežno za prenos podatkov na večje razdalje, možnostjo hkratnega priklopa večih naprav in z večjimi propustnostmi. Ker lahko med seboj povežemo zelo pester nabor naprav, je prav tako pester nabor aplikacij, ki naj bi jih uporabljale te naprave. Ker je najšibkejši člen v verigi ponavadi kritičen, mora biti bluetooth prilagojen tudi napravam z zelo majhno zmogljivostjo. Tako procesorsko in spominsko, kot tudi prostorsko in energetsko, pa tudi vhodno/izhodni vmesniki za komunikacijo z uporabniki so lahko problem. Problem je v tem, da so brezžične naprave po svoji naravi prenosne in s tem težijo k svoji majhnosti. Tako na primer nimajo vse naprave tipkovnice ali zaslona. Mnoge premorejo le kakšen gumb in led diodo ali pa še tega ne.

3.3. Razširitve

Predvsem se v zadnjem času pojavljajo težnje po povečanju pasovne širine, da bi pohitrili komunikacije, kot tudi po podaljšanem dometu naprav. Ker v računalništvu postane vsaka zmogljivost hitro premajhna, bluetooth to doživlja že na samem začetku uvajanja v širšo uporabo. Tako pasovno širino pri standardu 2.0 širijo s slabega megabita na 12 megabitov na sekundo, kar je primerljivo s starejšim standardom USB[6] 1.1 ali WLAN[7] 802.11b, ki danes zadovoljujeta večino potreb za ožičen priklop perifernih naprav na računalnike ali računalnikov na omrežja. Prav tako poskušajo povečati domet z dosedanjih 10m vidne razdalje na 100m. Vendar večja pasovna širina in domet pomenita tudi večjo energijsko potratnost takšne komunikacije in večje antene, kar pa ni primerno in potrebno za manjše naprave, ki bodo še vedno delovale po starem standardu, saj nimajo nikakršnih potreb po večjih zmogljivostih.

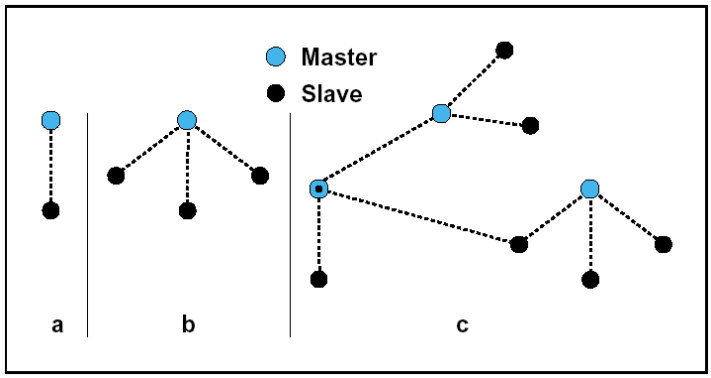
[6] USB – Universal Serial Bus. Odprti standard namenjen priklopu večih naprav preko samo enih vrat na računalniku. Naprave lahko poljubno dodajamo in odvzemamo med delovanjem. Je neke vrste ožičeni bluetooth.
[7] WLAN – Wireless Local Area Network. 802.11b je starejša izvedba protokola. Sodobnejša izvedba je 802.11g

3.4. Delovanje

Celice

Vsaka naprava v omrežju bluetooth lahko igra nadrejeno (master) ali podrejeno (slave) vlogo. Naprave se povežejo v celico, ki jo imenujemo piconet. Vsak piconet ima natančno eno nadrejeno napravo, preko katere poteka komunikacija med vsemi ostalimi napravami. Vsaka naprava je član najmanj ene piconet celice. Preko naprav, ki pripadajo večim celicam hkrati, lahko tudi virtualno povežemo naprave, ki pripadajo različnim celicam. Primer vseh režimov delovanja prikazuje Slika 1. Na sliki so trije režimi povezovanja naprav v omrežja:

a) enostavni (single slave)
b) večodjemalski (multi slave)
c) kombinirano omrežje (scatternet)



Slika 1: Režimi povezovanja naprav Bluetooth v omrežja piconet

Za uporabnike je to povezovanje v omrežja piconet neopazno, pomembno pa je zaradi razdeljevanja ključev, ki se uporabljajo pri varovanih komunikacijah med napravami. Kot je že zgoraj omenjeno, vse naprave v piconetu komunicirajo samo z nadrejeno napravo. Če hočejo podrejene naprave komunicirati med seboj, morajo to komunikacijo izvesti preko nadrejene naprave.
Današnje široko uporabljane naprave so večinoma še nezmožne povezovanja v kombinirano omrežje. Pričakujemo, da bodo tega sposobne z izpopolnitvijo programske opreme in razširjenimi zahtevami uporabnikov po združljivosti. Prav tako so zaenkrat redke implementacije povezovanja naprav v načinu multi slave. Zato v nalogi velja enostaven način povezovanja naprav za privzeti način, če ni drugače omenjeno.

3.4.1. Vzpostavljanje povezav

Bluetooth ima v načinu, ko je potrebna varnost poseben način seznanjanja obeh naprav imenovan pairing (parjenje). Parjenje za uporabnike ob pravilni implementaciji ni zahtevno opravilo. Namen parjenja je, da se napravama omogoči varna komunikacija in da potem kasneje ne bi bilo več potrebne identifikacije obeh naprav, če sta le obe sposobni shraniti osnovno informacijo o tej povezavi. Parjenje ponavadi poteka z izmenjavo *PIN*[8] kode, ki jo vnesemo v obe napravi. Takšna izmenjava *PIN* kode je mogoča, ker naprave komunicirajo na izredno kratko razdaljo. Nekaterim napravam z omejenimi vnosnimi zmožnostmi pa je sploh nemogoče ročno vnesti *PIN* in ga lahko spremenimo šele po vzpostavljeni povezavi. *PIN*

[8] PIN – Personal Identification Number

koda je tudi edina informacija, ki jo imata napravi na razpolago kot skupno skrivnost, ki je osnova izračuna ključa povezave.
Parjenje je logična operacija, ki jo vidi uporabnik. Podrobnosti vzpostavljanja varne povezave med napravami bodo opisane v poglavju 3.5.2

3.5. Varnost

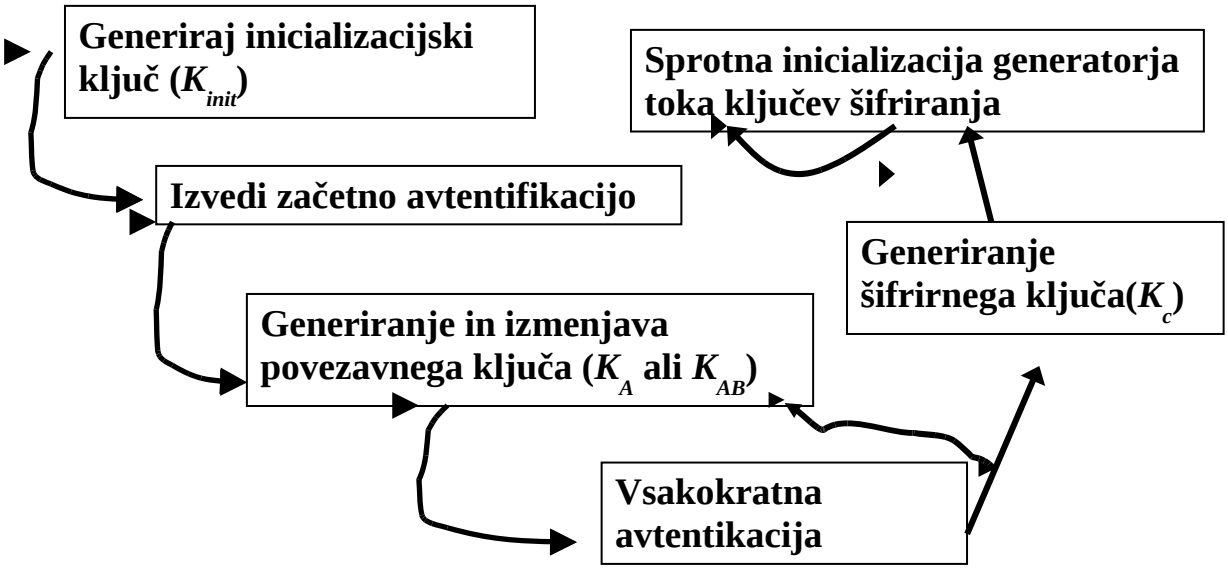
3.5.1. Varnostni nivoji delovanja

- Naprave lahko komunicirajo v povsem nezaščitenem načinu. Torej, da samo ponudijo storitev, če jo kdo zahteva.
- V malo bolj omejenem načinu lahko nezaščitene ponudijo le določene storitve, medtem, ko za zaščitene storitve že zahtevajo parjenje.
- V zaščitenem načinu se najprej zahteva parjenje, preden se sploh lahko nadaljuje s predstavitvijo razpoložljivih storitev.

Tako za izmenjavo »vizitk« zadostuje nezaščiten način, medtem, ko je za dostop do pomembnejših storitev potrebno izvesti parjenje. Takšna kritična storitev je na primer vzpostavitev klicne modemske povezave na mobilnem telefonu. Če dostopa do nje ne bi zaščitili, bi jo lahko marsikdo zlorabil kot brezplačen dostop do interneta ali podatkov v napravi za vdiralca.

3.5.2. Zaščiteni način

V zaščitenem načinu naprave prenašajo šifrirane podatke. V protokolu bluetooth je šifriranje in odšifriranje samih podatkov izvedeno s funkcijo XOR, medtem ko je večja pozornost namenjena neprestanemu spreminjanju ključev, ki se uporabljajo pri šifriranju. V zaščitenem načinu se namreč generator toka ključev za šifriranje podatkov na novo inicializira za vsak prenešeni paket. Naslednja slika prikazuje osnovni potek paritvene procedure in generiranje začetnih ključev:



Slika 2: Procedura parjenja in generiranja kriptirnih ključev

Vsi ključi, ki se uporabljajo v zaščitenem načinu so tajni in nikoli ne zapustijo naprave, ampak jih napravi izračunata na osnovi *PIN* izmenjanega na začetku procedure parjenja.

Vsi opisi varnostnih mehanizmov v tej nalogi veljajo za enostavni piconet. Torej za povezovanje podrejene in nadrejene naprave, kar je danes običajen način povezovanja bluetooth naprav. V ostalih kompleksnejših primerih so postopki in v njih uporabljeni ključi prilagojeni številu naprav in njihovim vrstam povezav. Vse skupaj pa ne vpliva na razumevanje osnovnega načina varovanja brezžičnega prenosa.

4. Bluetooth šifrirni algoritmi in varnost

Kot že omenjeno v prejšnjem poglavju, bluetooth šifrira podatke s funkcijo seštevanja po modulu 2 (XOR), medtem ko precej več procesorske moči porabi za izračun ključev, katerih algoritem za izračun se inicializira ob prenosu vsakega paketa.
Izračun šifrirnih in avtentikacijskih ključev temelji na pomičnih registrih s povratno zanko in kriptosistemu SAFER+[9], ki je bil tudi kandidat prvega kroga pri izbiri AES. Algoritem je cenjen zaradi majhne porabe računalniških virov, kar je pravzaprav osnovni pogoj za uporabo v bluetooth napravah.
Algoritem SAFER+ je, tako kot vsi simetrični algoritmi, občutljiv za napad »Meet in the Middle«, ki temelji na odkrivanju ključev na osnovi tajnopisa in čistopisa. Ker pa bluetooth uporablja SAFER+ samo za izračun ključev, ki predstavljajo osnovo za šifriranje podatkov, ki se prenašajo naj bi bilo znatno oteženo poznavanje čistopisa, ki bi omogočalo razbitje. Poleg tega se algoritem, ki izračunava bluetooth kriptirne ključe inicializira z vsakim podatkovnim paketom, medtem ko se SAFER ključi zamenjajo in uporabljajo samo ob vsaki avtentikaciji.
Prav tako se podatki šifrirani s SAFER sploh ne prenašajo med napravama v celoti, ampak samo majhen del potreben za avtentikacijo, kar opisuje poglavje 4.1.2

4.1. Ključi, ki jih uporablja bluetooth

Oznaka ključa	Naziv ključa	Dolžina	Opis ključa
BD_ADDR	Naslov naprave	48 bit	Javno znan naslov naprave, edinstven za vsako napravo
K_{Link}	Zasebni avtentikacijski	128 bit	Povezavni ključ. Določa povezavo med napravama.
K_c	Zasebni enkripcijski	1-16 byte	Generiran na osnovi avtentikacijskega. Zgenerira se ob vzpostavitvi vsake šifrirane povezave.
RAND	Naključni	128 bit	Rezultat algoritma za generiranje naključnih števil.

Tabela 1: Vrste ključev, ki jih hranijo naprave Bluetooth.

[9] Secure And Fast Encryption Routine, http://encyclopedia.thefreedictionary.com/SAFER

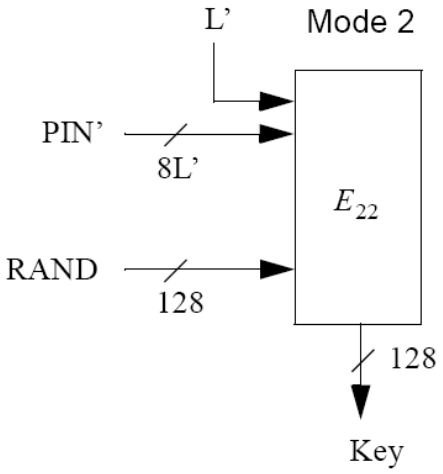
Kot prikazuje Tabela 1 sta dva od ključev naprav poznana, medtem ko povezavni ključ in enkripcijski ključ nikoli ne zapustita naprave. Tako v zaščitenem, kot tudi v povsem nezaščitenem načinu. Zasebni avtentikacijski ali povezavni ključ je namreč tudi osnova za izračun enkripcijskega ključa, če se napravi kasneje dogovorita za kriptiran način komunikacije. Za vzpostavitev kriptirane povezave potrebuje naprava bluetooth samo te podatke.

4.1.1. Zasebni avtentifikacijski ali povezavni ključi (K_{Link})

K_A	Ključ naprave	Generiran med inicializacijo naprave in se redko spreminja
K_{AB}	Kombinacijski ključ	Se generira za vsako povezavo
K_{init}	Inicializacijski ključ	V uporabi samo za prenos inicializacijskih parametrov, potem se izbriše
K_{master}	Skupinski ključ	Broadcast ključ za šifriranje v primeru skupinskega oddajanja

Tabela 2: Vrste povezavnih ključev

Inicializacijski ključ je začetni ključ povezave in je osnova za prenos ključa naprave ali izračun kombinacijskega ali skupinskega ključa. Pri izračunu inicializacijskega ključa se tudi uporabi edini simetrični ključ na katerega imajo vpliv uporabniki. *PIN*, ki je ena od vhodnih spremenljivk, kar prikazuje Slika 3. Spremenljivka *L'* predstavlja dolžino *PIN* v bytih.



Slika 3: Izračun inicializacijskega ključa K_{Init}

Dolžina *PIN* je med 4 in 16 bytov. Nikakor pa ni mogoče izračunati inicializacijskega ključa dveh naprav, ki uporabljata statičen *PIN*. Vedno mora vsaj ena naprava podpirati vnos *PIN*. Načeloma se *PIN* vnaša preko vnosnih enot naprave. Če pa naprave zahtevajo najvišjo stopnjo varnosti in bi bil vnos predolgega *PIN* preveč zahtevno opravilo za uporabnike, pa lahko za prenos *PIN* poskrbimo tudi z drugimi kriptografskimi metodami. *PIN* je namreč edina prava skrivnost, ki jo poznata samo napravi v komunikaciji.

Ostali trije ključi, ki jih prikazuje tabela 2, se uporabljajo kot pravi ključ povezave. Inicializacijski ključ se namreč po določitvi pravega ključa povezave izbriše.

Uporaba **ključa naprave** (K_A) se iz varnostnih razlogov odsvetuje. Uporablja se samo v primerih ko ima ena od naprav izredno omejene pomnilniške in vnosne zmogljivosti, da ne more kreirati drugačnega povezavnega ključa. Ključ naprave se spreminja izredno redko. Ponavadi samo kadar želimo onemogočiti dostop kakšni napravi, ki je s to napravo že komunicirala.
Ključ naprave namreč pomeni, da velja za vse naprave, ki komunicirajo s to napravo enak povezavni ključ. Torej njegova sprememba pomeni rušenje vseh vzpostavljenih povezav. Prav tako je s tem vprašljiva učinkovitost šifriranja podatkov med prenosom, saj tako omejena naprava nima nobene skrivnosti, ki bi jo lahko delila z drugo napravo in bi ne bila dostopna tudi ostalim napravam, s katerimi je povezana z istim povezavnim ključem.

Kombinacijski ključ je najbolj splošen ključ povezave med napravama. Enolično določa povezanost dveh naprav in z njegovo razveljavitvijo razveljavimo samo to povezavo. Poleg tega napravi tudi dokaj pogosto menjata kombinacijski ključ, kar otežuje sledenje povezave, če se uporabnik premika.

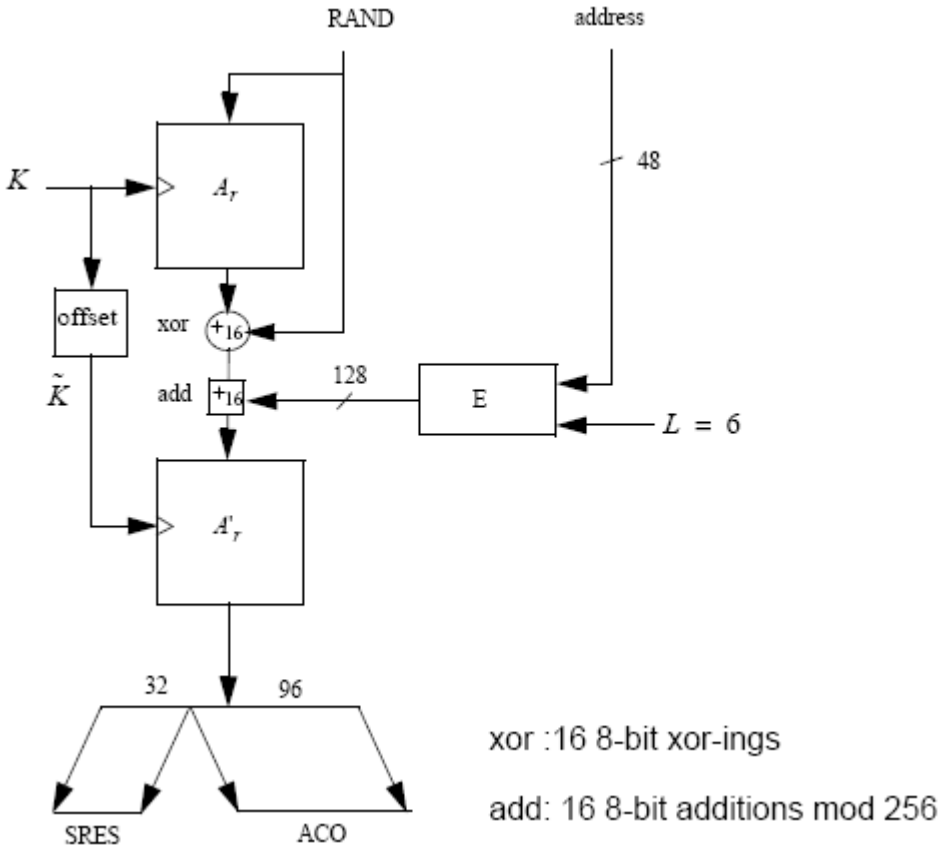
Skupinski ključ se uporablja samo v večodjemalskih piconetih. Njegov glavni namen je boljši izkoristek pasovne širine. Saj nadrejena naprava določi vsem napravam enoten ključ, torej postane tudi celoten promet viden vsem napravam, ki so vključene v ta piconet. Nadrejena naprava lahko tako z enkratno oddajo informacije, le to dostavi vsem podrejenim napravam brez nepotrebnih ponavljanj. To pomeni, da je tudi šifriran promet dosegljiv vsem napravam v večodjemalskem piconetu.

Obstaja več postopkov zamenjave ključa povezave. Odvisno od načina delovanja piconeta in uporabe vrste ključa za povezavo. Načeloma velja, da lahko napravi ključ povezave zamenjata kadarkoli in da se zamenja s pomočjo predhodnega ključa povezave. Ključ povezave se vedno zamenja ob novi vzpostavitvi povezave.
Torej tudi ob zamenjavi ključa le ta ne potuje med napravama ampak si ga napravi izračunata na osnovi naključnih števil, ki si jih izmenjata na podlagi starega ključa povezave.

4.1.2. Avtentikacija

Po določitvi povezavnega ključa se morata napravi A in B še avtenticirati. Torej potrditi ena drugi, da sta izračunali pravi povezavni ključ. V osnovi je avtentikacija tipična »challenge-response« procedura. Naprava A pošlje napravi B naključno 128 bitno število *RAND*. Ta potem na osnovi ostalih znanih podatkov in povezavnega ključa izračuna določeno vrednost, ki jo naprava A preveri z istim algoritmom. Avtentikacijski algoritem in njegove rezultate prikazuje Slika 4.
Vhodni podatki so naključna številka, ki jo pošlje preverjajoča naprava, naslov preverjane naprave in ključ povezave. Preverjana naprava vrne vrednost *SRES*, medtem ko vrednost *ACO* obdrži zase.
Funkcija A_r predstavlja šifriranje s simetričnim algoritmom SAFER+ v osmih korakih. Vsak korak obdela 16 bitov ključa, medtem ko je celotna dolžina ključa 128 bitov.
Podobna ji je funkcija A_r'. Razlika med njima je v tem, da se z dodatno substitucijsko operacijo na začetku tretjega koraka algoritma SAFER+ pri A_r' povzroči nepovratno enkripcijo, kar oteži odkrivanje ključev za nazaj, kot tudi onemogoči zlorabo avtentikacijskega mehanizma za namene šifriranja. Kot substitucijski ključ vzame vhodne podatke prvega kroga algoritma.
Ključ *K'* je izračunan iz prvotnega ključa *K* s substitucijskimi operacijami.

Škatla E s substitucijskimi operacijami 48 bitni naslov preverjane naprave raztegne na 128 bitov.

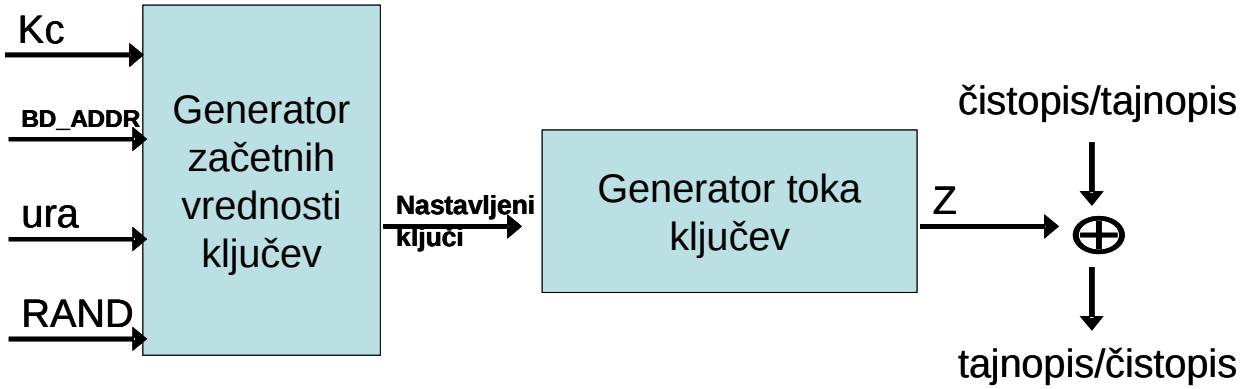


Slika 4: Avtentifikacijski algoritem

SRES je vrednost, ki se preverja na obeh straneh in potrjuje pravilnost avtentikacije. Je edini rezultat avtentikacije, ki se prenaša med napravama.
ACO služi poleg povezavnega ključa kot osnova za izračun enkripcijskega ključa K_c v primeru kriptirane komunikacije med dvema napravama. Iz tega izhaja, da je avtentikacija osnova za uporabo enkripcije v najpogosteje uporabljanih povezavah bluetooth. *ACO* se med napravama ne prenaša, jo pa morata napravi shraniti za primer vzpostavitve šifrirane povezave.

4.1.3. Šifriranje

Zadnja faza pred šifriranjem in odšifriranjem prenesenih podatkov je izračun toka kriptirnih ključev, ki se inicializira za vsak podatkovni paket posebej. Za vsak podatkovni paket velja, da se prenaša znotraj enega urinega cikla. To zagotavlja spremembo stanja najmanj ene od vhodnih spremenljivk potrebnih za generator začetnih vrednosti toka ključev.
Šifrirni avtomat prikazuje Slika 5. Edina skrivnost pri generiranju ključev je vrednost K_c. Vrednost K_c se izračuna na osnovi *ACO*, ki izhaja iz avtentifikacijskega algoritma, in K_{Link}, ki sta tajna ter *RAND*, ki se prenese med napravama. Prav tako se tudi K_c nikoli ne prenaša med napravama. Vse ostale podatke potrebne za generator začetnih vrednosti toka ključev posreduje nadrejena naprava. Vsi ostali podatki se prenesejo z nadrejene (master) naprave na podrejeno.



Slika 5: Tok ključev za vsak paket podatkov

Generator toka ključev temelji na metodi Massey – Rueppel [7]. Tok se sestavlja iz štirih LFSR[10]. Ker je metoda Massey - Rueppel občutljiva na korelacijske napade, se z veliko frekvenco ponastavljanja začetnega stanja sklepa, da je nevarnost uspešnega napada izjemno majhna.

4.2. Uporaba v praksi

V poglavju 4.1 je opisan celoten postopek, ki ga morajo izvesti naprave bluetooth, če želijo komunicirati na varen način. Edina skrivnost ki si jo naprave delijo je *PIN* koda. Zato se uporabi le pri izračunu inicializacijskega ključa, ki se uporabi samo pri prvi avtentikaciji. Kasneje se *PIN* skrije že za XOR preslikavo dveh naključnih števil, ki se uporabi pri izračunu ključa povezave. Rezultati kasnejših avtentikacijskih funkcij so skriti za dvojnim SAFER+ algoritmom. Enkripcijski ključ povezave je zgostitvena funkcija rezultata avtentikacijske funkcije in nekaterih drugih naključnih podatkov. Medtem ko se same podatke med prenosom šifrira na osnovi toka ključev.

4.2.1. Primer

V primeru bom prikazal paritev kot izgleda za uporabnika, ter kaj je uporabniku skrito. Varno želimo povezati mobilni telefon in računalnik. Predhodno je bluetooth vmesnik računalnika nastavljen tako, da se povezuje samo v varnem načinu. Zahtevo po povezavi poda mobilni telefon.

Ko bluetooth vmesnik računalnika zazna zahtevo po povezovanju sproži paritveno proceduro, saj mu tako velijo njegove privzete varnostne nastavitve. Na obeh napravah se na zaslonu pojavi zahteva po vnosu *PIN*. Ko uporabnik vnese enak *PIN* na obeh napravah, se prične kreiranje inicializacijskega ključa, mobilni telefon pa pošlje tudi naključno število *RAND*. Pogajanje o velikosti ključev ni potrebno, saj obe napravi podpirata največjo velikost ključa 128 bitov. Inicializacijski ključ hkrati postane tudi prvi povezavni ključ.

Ker se napravi povezujeta izvedeta tudi zamenjavo povezavnega ključa. Povezavni ključ K_{AB} se izračuna iz dveh naključnih števil, ki si jih izmenjata napravi s šifriranjem z obstoječim povezavnim ključem. Nov povezavni ključ se izračuna kot XOR izmenjanih naključnih števil.

Po določitvi svežega povezavnega ključa se morata napravi še avtenticirati, kar hkrati tudi pomeni uspešno spremembo povezavnega ključa. Telefon pošlje računalniku zahtevo po avtentikaciji in naključno število *RAND*. Računalnik vrne vrednost *SRES* in telefon preveri, če njegova vrednost odgovarja izračunani vrednosti. Vrednost *ACO* se ohrani za izračun

[10] LFSR – Linear Feedback Shift Register

kriptirnih ključev. Potem uporabnik običajno dobi na zaslonu izpisano sporočilo o uspešno opravljeni paritveni proceduri.

4.2.2. Priporočila bluetooth foruma

Pot do izračuna kriptirnega ključa je dokaj dolga, vendar algoritmi niso procesorsko zahtevni. Zato lahko napadalec ob spremljanju paritvene procedure s ugibanjem pravega *PIN* izračuna ključ povezave in tako zlorabi tako dobljene podatke. Zato tudi bluetooth forum odsvetuje parjenje naprav na javnih mestih. Kasneje se je do ključa povezave precej težje dokopati saj se sproti spreminja.
En od predlogov je tudi uporaba dovolj dolgih *PIN* ključev. Namreč najbolj kritično je sledenje procedure parjenja. Takrat lahko napadalec v primeru uporabe dovolj kratkega in enostavnega *PIN* z lahkoto z uporabo grobe sile izračuna ključ povezave. Tako je v primeru najpogosteje uporabljanega štirimestnega *PIN* dovolj preskusiti samo 10000 kombinacij. Pri napadu napadalec sploh ne napada neposredno naprav, ki jim želi prisluškovati ali pošiljati lažne podatke, ampak poskuša iz različnih uganjenih *PIN* restavrirati vrednost *SRES*, ki si jo napravi izmenjata ob uspešni avtentikaciji. Poleg tega so uporabniki pri določanju PIN dokaj praktični in navajeni parjenja z napravami brez tipkovnic, ki imajo privzeto vrednost *PIN* 0000. Kasneje postane ključ povezave tako kompleksen da ga je težko uganiti na kakršenkoli znan način.
Bluetooth je predvsem namenjen komunikaciji mobilnih naprav na kratke razdalje. Torej bi moral napadalec stalno slediti uporabnika po več mestih, da bi lahko učinkovito zlorabljal njegove naprave, saj se ključ povezave tudi občasno menja. Po zamujeni zamenjavi ključa povezave pa postane razbitje tega ključa po trenutnem prepričanju izredno težavno.

5. Trenutno stanje uporabe tehnologije bluetooth

5.1. Mobilna telefonija

Proizvajalci iz sveta mobilne tehnologije so glavni promotorji uporabe bluetooth tehnologije. Programska oprema, ki podpira delovanje naprav, počasi prehaja v zrelo fazo. Uporabniki imajo vedno manj problemov s stabilnostjo in uporabo naprav. Najbolj je razširjena uporaba brezžičnih bluetooth slušalk. Veliko ne zaostaja tudi uporaba z namenom koriščenja telefona kot brezžičnega vmesnika za povezavo v internet od kjerkoli in telefon lahko še vedno ostane v žepu suknjiča. Vedno bolj pa je tudi priljubljena sinhronizacija in samo upravljanje nastavitev telefona v povezavi z osebnim računalnikom, ki ima precej bolj prijazen uporabniški vmesnik za urejanje koledarjev in imenika. Zaradi boljše tipkovnice, kot tudi precej večjega in kvalitetnejšega zaslona.
Zmogljivejši novejši pametni[11] telefoni postajajo prave male shrambe podatkov, ki jih lahko uporabniki prenašajo z enega mesta na drugega brez zapletov z omrežjem.
Tudi nove funkcionalnosti telefonov, kot so digitalna fotografija, večpredstavnostna sporočila[12], polifonična zvonjenja in ostale postavljajo nove zahteve po povezljivosti in poenostavljenim upravljanjem z vsebinami. Namreč v telefonih in ostalih prenosnih žepnih napravah se z dodatkom vedno cenejših in zmogljivejših pomnilniških kartic nahaja prava

[11] Smartphone je pojem za mobilni telefon, ki poleg primarne funkcije telefoniranja nudi še širšo paleto storitev. Tako naj bi imel razširjene zmogljivosti vhodno/izhodnih enot in pomnilnika.
[12] MMS – MultiMedia Messages - večpredstavnostna sporočila

gora podatkov, ki si je pred leti nihče ni predstavljal. Ponavadi želijo uporabniki te podatke enostavno in poceni izmenjavati z računalniki na delovnem mestu ali doma.

5.2. Avtomobilska industrija

Tudi avtomobili so danes vedno bolj podobni računalnikom na štirih kolesih. Pri karambolu jim najbrž manjka samo še opcija „Start New Game”. Zato so pričakovanja avtomobilske in z njo povezanih industrij ogromne. Od možnosti nadzora avtomobila z osebnim računalnikom ali mobilnim telefonom do nakupa določenih podatkov na bencinskih servisih kot so osvežene karte mest za avtomobilsko navigacijo. Seveda se tudi tukaj najprej pojavljajo že vgrajene inštalacije za prostoročno telefoniranje.

5.3. Računalništvo

Čeprav v zadnjem času na področju računalništva obstoja konvergenca tehnologij se na področju brezžičnih povezav porajajo vedno novi standardi. Tako se za potrebe brezžičnega povezovanja računalnikov in računalniških perifernih enot glede na potrebe bluetooth kosa s standardom WLAN. Ceni vmesnikov sta za obe vrsti povezovanja podobni. Vendar je WLAN znatno hitrejši. Zahteva pa precej več energije in ima večji domet. Prav tako zaenkrat še ni implementiran v manjših napravah iz mobilnega sveta, ki služijo samo kot priključki k računalniku in ne potrebujejo velikih kapacitet za prenos podatkov. Zato je WLAN komplementarna tehnologija, ki dopolnjuje funkcionalnost bluetooth, saj je WLAN predstavnik LAN omrežij, medtem ko je bluetooth predstavnik PAN omrežij.

5.4. Grožnje

Ker je na svetu največ bluetooth vmesnikov vgrajenih v mobilne telefone, so tudi ti najbolj izpostavljeni raznoraznim poskusom napadov. Največja pomanjkljivost bluetootha je namreč ta, da nikjer ne zapoveduje varne povezave, ampak jo aplikacije lahko uporabijo, če to želijo. Ljudje pa so telefone še vedno pripravljeni uporabljati pretežno za telefoniranje in brez ovir v obliki raznoraznih potrjevanj.
Ponavadi ni kriva specifikacija varnosti v bluetooth protokolu, ampak samo večje ali manjše napake v implementacijah varnosti v programski opremi posameznih naprav. Tako se je pojavilo več vrst zlorab napak bluetooth protokolu [4]:

- **BlueSnarf**

Snarf zloraba je omogočena na napravah, ki ne zahtevajo parjenja za dostop do določenih storitev, poleg tega pa tudi ne zahtevajo odobritve uporabnika za uporabo teh storitev. Tako je v mnogih telefonih na voljo telefonski imenik in drugi osebni podatki brez da bi lastnik sploh vedel, da jih je oddal ali dodal [5]. Poleg tega ponavadi ni ščiten klicni dostop, kar bi mnogi lahko zlorabljali za dostop do plačljivih številk.
Raziskovalci, ki se borijo proti takim zlorabam, na strani proizvajalcev dostikrat naletijo na očitke o paranoji [5]. Predvsem v primerih, če za vsako potrditev vzpostavitve povezave zahtevajo poseg uporabnika.

- **Backdoor**

Je precej nevarnejši od napada Snarf. Praktično je njegova nadgradnja, vendar zahteva predhodno parjenje naprav. Torej se napadalec ne more kar pojaviti. Slabost pa temelji na implementaciji, kjer aplikacija ob izbrisu naprave iz registra parjenih naprav ne izbriše tudi povezavnega ključa. Torej lahko napadalec še vedno izkorišča vse storitve, ki mu jih bluetooth naprava nudi, brez vednosti njenega lastnika. Ponavadi tudi na zaslonu telefona ni nobenega znaka, da napravo uporablja še kdo drug. Tako postane dostopen celoten pomnilnik naprave, nastavitve in celo komunikacije, kar lahko vodi tudi k prisluškovanju telefonskih pogovorov.

- **BlueBug**

Temelji na podobnem principu kot BlueSnarf. Izkorišča podobne pomanjkljivosti v implementaciji varnostnih postopkov. Uporablja le povsem drug protokol dostopa do bluetooth naprave [6].

- **Bluejacking**

Bluejacking je na prvi pogled praktično nedolžna zloraba protokola parjenja ali nezavarovane storitve izmenjave vizitk. Storitev je podobna spam elektronski pošti. Torej osveščenim uporabnikom ne povzroča škode. Seveda je lahko s pošiljanjem zavajajočih sporočil pri neukih uporabnikih povzročena tudi škoda.
To lastnost uporabljajo predvsem v nočnih klubih za premagovanje ovir pri spoznavanju, saj si lahko anonimno brezplačno pošiljajo sporočila, medtem ko pošiljatelj in prejemnik vesta samo, da imata naprave v medsebojnem dosegu bluetooth signala.

Zaščita

Edina povsem varna zaščita pred nevarnimi vrstami napadov je izklop vmesnika bluetooth na javnih krajih, kjer obstaja možnost napada. Zaradi relativno kratkega dometa signala ta območja niso velika. Veliko lahko za svojo zaščito naredimo že s tem da napravo ne damo na razpolago za odkrivanje drugim napravam.
To tehniko izkoriščajo tudi že nekateri novejši operacijski sistemi telefonov [5], ki so v starejših izvedbah imeli napake. Saj ostane po vklopu bluetooth vmesnika telefon viden samo še kakšno minuto, potem pa je na razpolago samo že parjenim napravam.

Virusi

Protivirusni programi danes obstajajo predvsem za osebne in zmogljivejše računalnike. Bluetooth predstavlja komunikacijski kanal med zelo raznolikimi napravami. Znotraj tega kanala naprave nudijo samo določene storitve. Zaradi raznolikosti in pestrosti je sam bluetooth z vidika virusnih epidemij trenutno nezanimiv za pisce virusov. Poleg tega se mora virus širiti preko nekega prenosnega medija in mora napadati določene gostiteljske aplikacije in izkoriščati varnostne pomanjkljivosti, ki omogočajo njegovo nadaljnje razmnoževanje.
Privlačnost izkoriščanja napak v programski opremi, ki uporablja bluetooth pa postaja vedno večja s poenotenjem platform, na katerih delujejo mobilne naprave. Zaradi vseh ostalih dejavnikov, ki vplivajo na uspešnost virusov je uporaba bluetooth protokola zaenkrat še vedno precej varnejša, kot uporaba interneta ali nalaganje nepreverjenih brezplačnih aplikacij za mobilne naprave.

6. Zaključek

Krog naprav z vgrajeno bluetooth tehnologijo se vsak teden poveča za milijon. Sama varnost je v specifikaciji protokola ustrezno opredeljena, medtem ko se pri implementaciji pojavljajo večje in manjše napake. Ob prehodu bluetooth tehnologije v zrelo fazo so se začela pojavljati opozorila o možnih pomanjkljivosti implementacije varnostnih mehanizmov, ki bi bili nujno potrebni za zaščito občutljivih podatkov v napravah.
Zato lahko v prihodnosti pričakujemo tudi prve varnostne popravke za mobilne telefone. Podobno kot je to postala ustaljena praksa pri operacijskih sistemih in ostali varnostno občutljivi programski opremi.
Še vedno obstaja precej večja verjetnost kraje zaupnih podatkov in zlorabe telefonskega računa v primeru kraje ali izgube same naprave, ki je še vedno najpogostejši primer kraje notranjih zaupnih podatkov podjetij. Medtem pa se moramo zavedati kakšne grožnje nam pretijo z razširjeno uporabo povezovanja naprav preko bluetooth.
Prav tako nam pri uporabi varnostnih rešitev vgrajenih v bluetooth in z njo povezanimi nevšečnostmi veliko pomaga tudi poznavanje ostalih tehnologij, ki jih uporabljamo skladno z bluetooth napravami. Včasih uporaba bluetooth varnostnih elementov sploh ni potrebna.

7. Literatura

[1] Bluetooth SIG, Specification of the Bluetooth system, Version 1.2, Nov 2003

[2] Muller T., Bluetooth Security Architecture, Version 1.0, Jul 1999

[3] Vidmar T., Računalniška omrežja in storitve, Apr 1997, ISBN 961-6056-31-X

[4] Ben Laurie Adam Laurie. Serious flaws in bluetooth security lead to disclosure
of personal data. Technical report, A.L. Digital Ltd.,
http://bluestumbler.org/,
January 2004.

[5] Herfurt Martin, Bluesnarfing @ CeBit 2004, Mar. 2004

[6] http://agentsmith.salzburgresearch.at/agentsmith_projects_bluebug.html

[7] J. L. Massey and R. A. Rueppel, "Linear Ciphers and Random Sequence Generators with Multiple Clocks", pp. 74-87 in Advances in Cryptology (Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science No. 209). Heidelberg and New York: Springer 1985. 12