

Securitatea comunicațiilor *GSM*

Prof. Dr. Adrian Atanasiu

Universitatea București

March 8, 2017



1 Descrierea sistemului *GSM*

- Stația mobilă
- Subsistemul Stație de bază
- Subsistemul rețea

2 Rutarea apelurilor în *GSM*

3 Securitatea *GSM*

- Anonimitatea
- Autentificarea

4 Confidențialitate în *GSM*

- Algoritmul A5/1
- Algoritmul A5/2

5 Atacuri active asupra rețelelor *GSM*



GSM (Global System for Mobile Communications) a fost dezvoltat de 3GPP (*3rd Generation Partnership Project*) ca standard pentru comunicațiile celulare digitale.

Lucrările de proiectare au început în anul 1987, sistemul fiind realizat în forma finală prin cooperarea a 17 țări europene; punerea în funcțiune a primelor rețele *GSM* s-a realizat în 1991.



GSM (Global System for Mobile Communications) a fost dezvoltat de 3GPP (*3rd Generation Partnership Project*) ca standard pentru comunicațiile celulare digitale.

Lucrările de proiectare au început în anul 1987, sistemul fiind realizat în forma finală prin cooperarea a 17 țări europene; punerea în funcțiune a primelor rețele *GSM* s-a realizat în 1991.

La nivel mondial mai există:



GSM (Global System for Mobile Communications) a fost dezvoltat de 3GPP (*3rd Generation Partnership Project*) ca standard pentru comunicațiile celulare digitale.

Lucrările de proiectare au început în anul 1987, sistemul fiind realizat în forma finală prin cooperarea a 17 țări europene; punerea în funcțiune a primelor rețele *GSM* s-a realizat în 1991.

La nivel mondial mai există:

- **ADC (American Digital Cellular)** – sistemul digital nord-american,



GSM (Global System for Mobile Communications) a fost dezvoltat de 3GPP (*3rd Generation Partnership Project*) ca standard pentru comunicațiile celulare digitale.

Lucrările de proiectare au început în anul 1987, sistemul fiind realizat în forma finală prin cooperarea a 17 țări europene; punerea în funcțiune a primelor rețele GSM s-a realizat în 1991.

La nivel mondial mai există:

- *ADC (American Digital Cellular)* – sistemul digital nord-american,
- *JDC (Japonese Digital Cellular)* – sistemul digital din Japonia.



GSM (Global System for Mobile Communications) a fost dezvoltat de 3GPP (*3rd Generation Partnership Project*) ca standard pentru comunicațiile celulare digitale.

Lucrările de proiectare au început în anul 1987, sistemul fiind realizat în forma finală prin cooperarea a 17 țări europene; punerea în funcțiune a primelor rețele *GSM* s-a realizat în 1991.

La nivel mondial mai există:

- *ADC (American Digital Cellular)* – sistemul digital nord-american,
- *JDC (Japonese Digital Cellular)* – sistemul digital din Japonia.

Se estimează că în acest moment 82% din piața mobilă la nivel global folosește standardul *GSM*.

Numai câteva țări (Japonia, Coreea de Sud) nu se află sub acoperirea *GSM*.

Serviciile oferite de *GSM*

GSM asigură;

- #### ■ servicii de transfer de date

Serviciile oferite de *GSM*

GSM asigură;

- servicii de transfer de date,
 - teleservicii,

Serviciile oferite de GSM

GSM asigură;

- servicii de transfer de date,
 - teleservicii,
 - servicii suplimentare: identificarea apelantului, apel în așteptare, conversații multiple (conferințe) etc.



Serviciile oferite de *GSM*

GSM asigură;

- servicii de transfer de date,
- teleservicii,
- servicii suplimentare: identificarea apelantului, apel în așteptare, conversații multiple (conferințe) etc.

Teleserviciul de bază suportat de *GSM* este **telefonia**.

Semnalul vocal este codificat digital și transmis prin rețeaua *GSM* ca un flux de semnal digital.



Serviciile oferite de GSM

GSM asigură;

- servicii de transfer de date,
- teleservicii,
- servicii suplimentare: identificarea apelantului, apel în așteptare, conversații multiple (conferințe) etc.

Teleserviciul de bază suportat de GSM este **telefonia**.

Semnalul vocal este codificat digital și transmis prin rețeaua GSM ca un flux de semnal digital.

Un serviciu specific oferit de GSM: **Serviciul de Mesaje Scurte (SMS)**.



Rețeaua pe care se construiește sistemul GSM se împarte în:

- 1 *Stația mobilă (MS - Mobile Station)*: este componenta aflată la abonat.



Rețeaua pe care se construiește sistemul GSM se împarte în:

- 1 *Stația mobilă (MS - Mobile Station)*: este componenta aflată la abonat.
- 2 *Subsistemul Stație de bază (BSS - Base Station Subsystem)*: controlează legătura radio cu stația mobilă.



Rețeaua pe care se construiește sistemul GSM se împarte în:

- 1 *Stația mobilă (MS - Mobile Station)*: este componenta aflată la abonat.
- 2 *Subsistemul Stație de bază (BSS - Base Station Subsystem)*: controlează legătura radio cu stația mobilă.
- 3 *Subsistemul Rețea (Network Subsystem)*: principala componentă este *Centrul de comutație a serviciilor mobile (MSC - Mobile services Switching Center)*.



Stația mobilă

Stația mobilă

- 1 Un echipament mobil (numit și “*terminal*”): de obicei un telefon celular.



Stația mobilă

Stația mobilă

- 1 Un echipament mobil (numit și “*terminal*”): de obicei un telefon celular.
- 2 Un smartcard SIM (*Subscriber Identity Module*).



Echipamentul mobil

Este identificat în mod unic de *IMEI* (*International Mobile Equipment Identity*) – un cod care se găsește de obicei tipărit pe telefon, sub bateria de alimentare și este folosit strict pentru identificare, neavând o relație permanentă cu abonatul.



Echipamentul mobil

Este identificat în mod unic de *IMEI* (*International Mobile Equipment Identity*) – un cod care se găsește de obicei tipărit pe telefon, sub bateria de alimentare și este folosit strict pentru identificare, neavând o relație permanentă cu abonatul.

Componenta principală a unui telefon mobil este procesorul – care conține o unitate centrală *RISC* (cu set minimal de instrucțiuni) și un procesor cu semnal digital (*DSP*).



Echipamentul mobil

Este identificat în mod unic de *IMEI* (*International Mobile Equipment Identity*) – un cod care se găsește de obicei tipărit pe telefon, sub bateria de alimentare și este folosit strict pentru identificare, neavând o relație permanentă cu abonatul.

Componenta principală a unui telefon mobil este procesorul – care conține o unitate centrală *RISC* (cu set minimal de instrucțiuni) și un procesor cu semnal digital (*DSP*).

Procesorul *RISC* este responsabil de:

- 1 Manevrarea informației primite prin diversele canale (*BCCh*, *PCh* etc.).



Echipamentul mobil

Este identificat în mod unic de *IMEI* (*International Mobile Equipment Identity*) – un cod care se găsește de obicei tipărit pe telefon, sub bateria de alimentare și este folosit strict pentru identificare, neavând o relație permanentă cu abonatul.

Componenta principală a unui telefon mobil este procesorul – care conține o unitate centrală *RISC* (cu set minimal de instrucțiuni) și un procesor cu semnal digital (*DSP*).

Procesorul *RISC* este responsabil de:

- 1 Manevrarea informației primite prin diversele canale (*BCCh*, *PCh* etc.).
- 2 Stabilirea apelului și administrarea mobilității (căutarea rețelei, reactualizarea locației, decalajul în timp etc.).



Echipamentul mobil

Este identificat în mod unic de *IMEI* (*International Mobile Equipment Identity*) – un cod care se găsește de obicei tipărit pe telefon, sub bateria de alimentare și este folosit strict pentru identificare, neavând o relație permanentă cu abonatul.

Componenta principală a unui telefon mobil este procesorul – care conține o unitate centrală *RISC* (cu set minimal de instrucțiuni) și un procesor cu semnal digital (*DSP*).

Procesorul *RISC* este responsabil de:

- 1 Manevrarea informației primite prin diversele canale (*BCCh*, *PCh* etc.).
- 2 Stabilirea apelului și administrarea mobilității (căutarea rețelei, reactualizarea locației, decalajul în timp etc.).
- 3 Conexiunile prin interfețele externe ca *Bluetooth*, *USB* etc.





Cartela SIM

Cartela *SIM* (*Subscriber Identity Module*) este un smartcard care stochează informații esențiale, cum ar fi *IMSI* (*International Mobile Subscriber Identity*), *MSI* – un număr unic asociat fiecărui abonat, K_i (cheia secretă folosită pentru autentificare).



Cartela SIM

Cartela *SIM* (**Subscriber Identity Module**) este un smartcard care stochează informații esențiale, cum ar fi *IMSI* (*International Mobile Subscriber Identity*), *MSI* – un număr unic asociat fiecărui abonat, K_i (cheia secretă folosită pentru autentificare).

În general, informațiile sunt protejate printr-un număr personal de identificare (*PIN*).



Cartela SIM

Cartela *SIM* (*Subscriber Identity Module*) este un smartcard care stochează informații esențiale, cum ar fi *IMSI* (*International Mobile Subscriber Identity*), *MSI* – un număr unic asociat fiecărui abonat, K_i (cheia secretă folosită pentru autentificare).

În general, informațiile sunt protejate printr-un număr personal de identificare (*PIN*).

SIM-ul conține un microcontroller care generează valoarea *SRES* în procesul de autentificare. Este obligatoriu ca *SRES* să fie calculat în interiorul *SIM*-ului și nu în telefonul mobil, pentru a proteja cheia secretă K_i , care intervene și în procesul de autentificare.



Cartela SIM

Cartela *SIM* (**Subscriber Identity Module**) este un smartcard care stochează informații esențiale, cum ar fi *IMSI* (*International Mobile Subscriber Identity*), *MSI* – un număr unic asociat fiecărui abonat, K_i (cheia secretă folosită pentru autentificare).

În general, informațiile sunt protejate printr-un număr personal de identificare (*PIN*).

SIM-ul conține un microcontroller care generează valoarea *SRES* în procesul de autentificare. Este obligatoriu ca *SRES* să fie calculat în interiorul *SIM*-ului și nu în telefonul mobil, pentru a proteja cheia secretă K_i , care intervene și în procesul de autentificare. Datele sunt stocate pe *SIM* în directoare și fișiere într-o manieră similară stocării pe hard-ul unui PC.

Subsistemul Stație de bază

Subsistemul Stație de bază

Este responsabil pentru asigurarea traficului și a semnalului între stația mobilă și centrul de comutație a serviciilor mobile.

Subsistemul Stație de bază

Subsistemul Stație de bază

Este responsabil pentru asigurarea traficului și a semnalului între stația mobilă și centrul de comutație a serviciilor mobile.

Banda de frecvențe este formată din două sub-benzi:



Subsistemul Stație de bază

Subsistemul Stație de bază

Este responsabil pentru asigurarea traficului și a semnalului între stația mobilă și centrul de comutație a serviciilor mobile.

Banda de frecvențe este formată din două sub-benzi:

- 1 890 – 915 MHz: comunicarea de la Stația Mobilă la Stația de Bază (uplink);



Subsistemul Stație de bază

Subsistemul Stație de bază

Este responsabil pentru asigurarea traficului și a semnalului între stația mobilă și centrul de comutație a serviciilor mobile.

Banda de frecvențe este formată din două sub-benzi:

- 1** 890 – 915 MHz: comunicarea de la Stația Mobilă la Stația de Bază (uplink);
- 2** 935 – 960 MHz: comunicarea de la Stația de Bază la Stația Mobilă (downlink).



Subsistemul Stație de bază

Subsistemul Stație de bază

Este responsabil pentru asigurarea traficului și a semnalului între stația mobilă și centrul de comutație a serviciilor mobile.

Banda de frecvențe este formată din două sub-benzi:

- 1 890 – 915 MHz: comunicarea de la Stația Mobilă la Stația de Bază (uplink);
- 2 935 – 960 MHz: comunicarea de la Stația de Bază la Stația Mobilă (downlink).

Fiecare sub-bandă este împărțită în 124 perechi de frecvențe purtătoare, fiecare pereche având alocată o bandă de 200 kHz.

Fiecare frecvență purtătoare este utilizată pentru transportul a 8 canale telefonice distincte, multiplexate în timp (*TDMA*).



Subsistemul Stație de bază

Subsistemul Stație de bază

Este responsabil pentru asigurarea traficului și a semnalului între stația mobilă și centrul de comutație a serviciilor mobile.

Banda de frecvențe este formată din două sub-benzi:

- 1 890 – 915 MHz: comunicarea de la Stația Mobilă la Stația de Bază (uplink);
- 2 935 – 960 MHz: comunicarea de la Stația de Bază la Stația Mobilă (downlink).

Fiecare sub-bandă este împărțită în 124 perechi de frecvențe purtătoare, fiecare pereche având alocată o bandă de 200 kHz.

Fiecare frecvență purtătoare este utilizată pentru transportul a 8 canale telefonice distințe, multiplexate în timp (*TDMA*).

Transmisia se face în pachete în interiorul intervalului de timp alocat, cu o rată de 271 kbps.

Subsistemul Stație de bază

GSM folosește diverse canale pentru transmiterea datelor,
împărțite în

Subsistemul Stație de bază

GSM folosește diverse canale pentru transmiterea datelor,
împărțite în

- **Canale fizice** (determinate de timesloturi),



Subsistemul Stație de bază

GSM folosește diverse canale pentru transmiterea datelor, împărțite în

- **Canale fizice** (determinate de timesloturi),
- **Canale logice**: folosite pentru transmiterea datelor utilizatorului și a datelor de semnalizare.



Subsistemul Stație de bază

GSM folosește diverse canale pentru transmiterea datelor, împărțite în

- **Canale fizice** (determinate de timesloturi),
- **Canale logice**: folosite pentru transmiterea datelor utilizatorului și a datelor de semnalizare.

Dacă datele dintr-un canal logic sunt dedicate unui singur utilizator, atunci canalul este numit “**canal dedicat**”.

Dacă avem în vedere transmiterea de date pentru mai mulți utilizatori, canalul este numit “**canal comun**”.

Canalele dedicate sunt clasificate în:

- *Canalul de trafic* (*TCh*): pentru datele utilizatorilor.



Subsistemul Stație de bază

Canalele dedicate sunt clasificate în:

- *Canalul de trafic* (*TCh*): pentru datele utilizatorilor.
- *Canale asociate rapide de control* (*FACCh*): folosite pentru cereri neprogramate de control.



Canalele dedicate sunt clasificate în:

- *Canalul de trafic* (*TCh*): pentru datele utilizatorilor.
- *Canale asociate rapide de control* (*FACCh*): folosite pentru cereri neprogramate de control.
- *Canale asociate lente de control* (*SACCh*): folosite în direcția uplink pentru a raporta măsurile de calitate a semnalului din celula deservită și din cele vecine.
În sens invers, canalul este folosit pentru transmisia de comenzi de control de putere către stația mobilă.



Canalele dedicate sunt clasificate în:

- *Canalul de trafic (TCh)*: pentru datele utilizatorilor.
- *Canale asociate rapide de control (FACCh)*: folosite pentru cereri neprogramate de control.
- *Canale asociate lente de control (SACCh)*: folosite în direcția uplink pentru a raporta măsurile de calitate a semnalului din celula deservită și din cele vecine.
În sens invers, canalul este folosit pentru transmisia de comenzi de control de putere către stația mobilă.
- *Canale de control dedicate (DCh)*: multiplexate într-un canal de trafic standard. Sunt folosite pentru înregistrare, reactualizarea locației, autentificare și apelare.



Canalele dedicate sunt clasificate în:

- *Canalul de trafic* (*TCh*): pentru datele utilizatorilor.
- *Canale asociate rapide de control* (*FACCh*): folosite pentru cereri neprogramate de control.
- *Canale asociate lente de control* (*SACCh*): folosite în direcția uplink pentru a raporta măsurile de calitate a semnalului din celula deservită și din cele vecine.
În sens invers, canalul este folosit pentru transmisia de comenzi de control de putere către stația mobilă.
- *Canale de control dedicate* (*DCh*): multiplexate într-un canal de trafic standard. Sunt folosite pentru înregistrare, reactualizarea locației, autentificare și apelare.
- *Canal comun descendenter* (*AGCh*): utilizat pentru a transmite mobilului mesaje de alocare a unui canal dedicat.

Subsistemul Stație de bază

Pe lângă canalele dedicate – asignate unui singur utilizator – există și canale comune, dedicate tuturor utilizatorilor dintr-o celulă:



Subsistemul Stație de bază

Pe lângă canalele dedicate – asignate unui singur utilizator – există și canale comune, dedicate tuturor utilizatorilor dintr-o celulă:

- *Canal de sincronizare (SCh)*: folosit de stațiile mobile în timpul căutării rețelei și a celulei.



Subsistemul Stație de bază

Pe lângă canalele dedicate – asignate unui singur utilizator – există și canale comune, dedicate tuturor utilizatorilor dintr-o celulă:

- *Canal de sincronizare (SCh)*: folosit de stațiile mobile în timpul căutării rețelei și a celulei.
- *Canale de control emis (BCh)*: canale logice necesare transmisiei periodice a informațiilor generale.



Subsistemul Stație de bază

Pe lângă canalele dedicate – asignate unui singur utilizator – există și canale comune, dedicate tuturor utilizatorilor dintr-o celulă:

- *Canal de sincronizare (SCh)*: folosit de stațiile mobile în timpul căutării rețelei și a celulei.
- *Canale de control emis (BCh)*: canale logice necesare transmisiei periodice a informațiilor generale.
- *Canal de paging (PCh)*: canal logic care transportă mesajele de difuzare pe interfața radio; este folosit în principal pentru anunțarea mobilului despre apelurile primite.



Subsistemul Stație de bază

Pe lângă canalele dedicate – asignate unui singur utilizator – există și canale comune, dedicate tuturor utilizatorilor dintr-o celulă:

- *Canal de sincronizare (SCh)*: folosit de stațiile mobile în timpul căutării rețelei și a celulei.
- *Canale de control emis (BCh)*: canale logice necesare transmisiei periodice a informațiilor generale.
- *Canal de paging (PCh)*: canal logic care transportă mesajele de difuzare pe interfața radio; este folosit în principal pentru anunțarea mobilului despre apelurile primite.
- *Canal de acces aleator (RACH)*: canal de accesare a rețelei *MS – BTS*.
Este folosit de *MS* pentru a cere alocarea unui canal dedicat.

Subsistemul Stație de bază

Stația de bază (*BTS*)

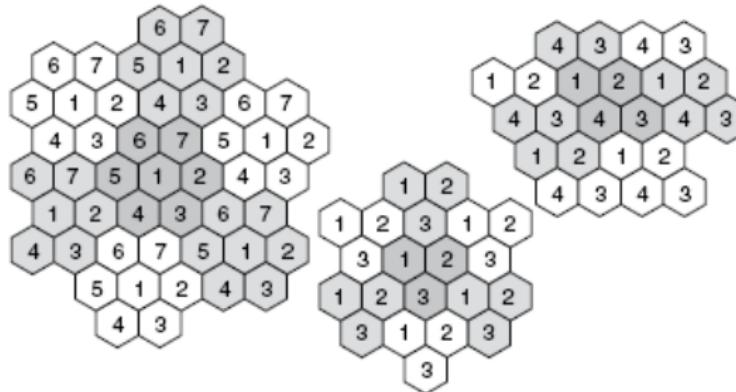
Componența cea mai vizibilă din rețeaua *GSM*.



Subsistemul Stație de bază

Stația de bază (BTS)

Componența cea mai vizibilă din rețeaua GSM.



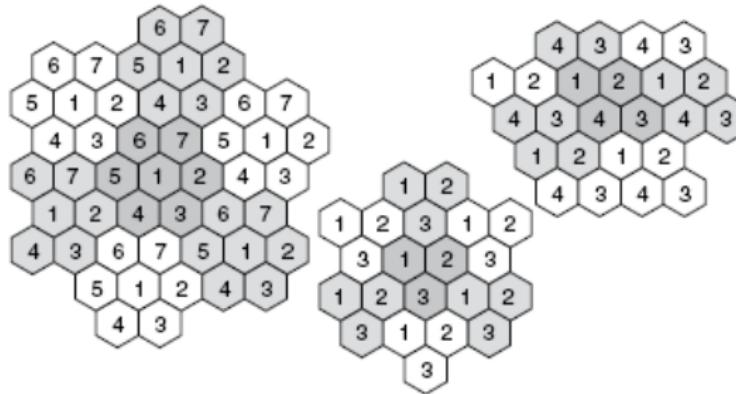
BTS conține echipamentul necesar transmiterii și primirii semnalului, antene și echipament pentru criptarea și decriptarea comunicațiilor cu *BSC* (*Base Station Controller*).



Subsistemul Stație de bază

Stația de bază (BTS)

Componența cea mai vizibilă din rețeaua GSM.



BTS conține echipamentul necesar transmiterii și primirii semnalului, antene și echipament pentru criptarea și decriptarea comunicațiilor cu *BSC* (*Base Station Controller*).

De obicei, un *BSC* are sub control până la 100 *BTS*.

Subsistemul Stație de bază

Având în vedere că emisiile stațiilor de bază diferite dintr-o rețea nu trebuie să interfereze, toate celulele învecinate trebuie să emită pe frecvențe diferite.



Subsistemul Stație de bază

Având în vedere că emisiile stațiilor de bază diferite dintr-o rețea nu trebuie să interfereze, toate celulele învecinate trebuie să emită pe frecvențe diferite.

Cum o celulă este înconjurată de multe altele, o stație de bază poate folosi doar un număr limitat de frecvențe diferite pentru a-și mări capacitatea.

Subsistemul Stație de bază

Interfața radio

Legătura între *BTS* și terminalul mobil.

Subsistemul Stație de bază

Interfața radio

Legătura între *BTS* și terminalul mobil.

Există două metode care permit stației de bază să comunice simultan cu mai mulți utilizatori.



Interfața radio

Legătura între *BTS* și terminalul mobil.

Există două metode care permit stației de bază să comunice simultan cu mai mulți utilizatori.

- 1 **Acces multiplu prin diviziune în frecvență (FDMA)**: utilizatorii pot comunica cu stația de bază pe frecvențe diferite, fără a interfera unii cu alții.



Interfața radio

Legătura între *BTS* și terminalul mobil.

Există două metode care permit stației de bază să comunice simultan cu mai mulți utilizatori.

- 1 **Acces multiplu prin diviziune în frecvență (*FDMA*)**: utilizatorii pot comunica cu stația de bază pe frecvențe diferite, fără a interfera unii cu alții.
- 2 **Acces multiplu prin diviziune în timp (*TDMA*)**: Utilizatorii sunt multiplexați în timp prin împărțirea în frame-uri cu durată de 4,615 ms.



Subsistemul Stație de bază

Interfața radio

Legătura între *BTS* și terminalul mobil.

Există două metode care permit stației de bază să comunice simultan cu mai mulți utilizatori.

1 **Acces multiplu prin diviziune în frecvență (*FDMA*)**: utilizatorii pot comunica cu stația de bază pe frecvențe diferite, fără a interfera unii cu alții.

2 **Acces multiplu prin diviziune în timp (*TDMA*)**: Utilizatorii sunt multiplexați în timp prin împărțirea în frame-uri cu durată de 4,615 ms.

Fiecare frame conține 8 *timeslot*-uri independente, fiecare *timeslot* fiind folosit pentru comunicarea cu alt utilizator.

Durata unui *timeslot* este de 0,577 ms și cuprinde 148 biți, cu o perioadă de gardă de 8,25 biți între slot-urile.

Subsistemul Stație de bază

Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.



Subsistemu Stație de bază

Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.

- Dacă un utilizator dorește să efectueze un apel vocal, să trimită un *SMS* etc, stația mobilă trimite un mesaj de cerere de canal către *BSC*, care verifică dacă există vreun canal *SDCCh* disponibil, și în caz afirmativ, îl activează.



Subsistemu Stație de bază

Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.

- Dacă un utilizator dorește să efectueze un apel vocal, să trimită un *SMS* etc, stația mobilă trimite un mesaj de cerere de canal către *BSC*, care verifică dacă există vreun canal *SDCCh* disponibil, și în caz afirmativ, îl activează.
Apoi *BSC* trimite un mesaj de asignare stației mobile prin *AGCh*, care include și numărul canalului *SDCCh* asignat.



Subsistemul Stație de bază

Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.

- Dacă un utilizator dorește să efectueze un apel vocal, să trimită un *SMS* etc, stația mobilă trimite un mesaj de cerere de canal către *BSC*, care verifică dacă există vreun canal *SDCCh* disponibil, și în caz afirmativ, îl activează.
Apoi *BSC* trimite un mesaj de asignare stației mobile prin *AGCh*, care include și numărul canalului *SDCCh* asignat.
- Stabilește canalele de semnalizare pentru apelurile primite sau mesajele scurte.



Subsistemul Stație de bază

Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.

- Dacă un utilizator dorește să efectueze un apel vocal, să trimită un *SMS* etc, stația mobilă trimite un mesaj de cerere de canal către *BSC*, care verifică dacă există vreun canal *SDCCh* disponibil, și în caz afirmativ, îl activează.
Apoi *BSC* trimite un mesaj de asignare stației mobile prin *AGCh*, care include și numărul canalului *SDCCh* asignat.
- Stabilește canalele de semnalizare pentru apelurile primite sau mesajele scurte.
- Menține conexiunea.



Subsistemul Stație de bază

Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.

- Dacă un utilizator dorește să efectueze un apel vocal, să trimită un *SMS* etc, stația mobilă trimite un mesaj de cerere de canal către *BSC*, care verifică dacă există vreun canal *SDCCh* disponibil, și în caz afirmativ, îl activează.
Apoi *BSC* trimite un mesaj de asignare stației mobile prin *AGCh*, care include și numărul canalului *SDCCh* asignat.
- Stabilește canalele de semnalizare pentru apelurile primite sau mesajele scurte.
- Menține conexiunea.
- Răspunde de controlul puterii de transmisie.



Controllerul Stației de bază (*BSC*)

Este responsabil de stabilirea, întreruperea și menținerea conexiunilor celulelor care sunt conectate la el.

- Dacă un utilizator dorește să efectueze un apel vocal, să trimită un *SMS* etc, stația mobilă trimite un mesaj de cerere de canal către *BSC*, care verifică dacă există vreun canal *SDCCh* disponibil, și în caz afirmativ, îl activează.
Apoi *BSC* trimite un mesaj de asignare stației mobile prin *AGCh*, care include și numărul canalului *SDCCh* asignat.
- Stabilește canalele de semnalizare pentru apelurile primite sau mesajele scurte.
- Menține conexiunea.
- Răspunde de controlul puterii de transmisie.
- Are în grijă controlul decalajului în timp.



Subsistemul rețea

Subsistemul rețea

Principale responsabilități:

- Stabilirea apelului;

Subsistemul rețea

Subsistemul rețea

Principale responsabilități:

- Stabilirea apelului;
- Controlul apelului;



Subsistemu[m] re[te]a

Subsistemu[m] re[te]a

Principale responsabilită[ți]:

- Stabilirea apelului;
- Controlul apelului;
- Rutarea apelurilor [ntre diferite centre de comuta[ie] fixe/mobile și alte re[te]ele.

Subsistemul rețea

Centrul de comutare a serviciilor (*MSC*)

Mobile Switching Center (MSC) asigură:



Subsistemul rețea

Centrul de comutare a serviciilor (MSC)

Mobile Switching Center (MSC) asigură:

- Înregistrarea utilizatorilor: când stația mobilă este pornită, ea se înregistrează în rețea, devenind accesibilă tuturor utilizatorilor.



Subsistemu retea

Centrul de comutare a serviciilor (MSC)

Mobile Switching Center (MSC) asigură:

- Înregistrarea utilizatorilor: când stația mobilă este pornită, ea se înregistrează în rețea, devenind accesibilă tuturor utilizatorilor.
- Stabilirea apelului și rutarea acestuia între doi utilizatori.



Centrul de comutare a serviciilor (MSC)

Mobile Switching Center (MSC) asigură:

- Înregistrarea utilizatorilor: când stația mobilă este pornită, ea se înregistrează în rețea, devenind accesibilă tuturor utilizatorilor.
- Stabilirea apelului și rutarea acestuia între doi utilizatori.
- Transmiterea mesajelor scurte SMS.



Subsistemul rețea

Registrul de localizare a vizitatorilor (VLR)

Reține informații despre fiecare utilizator care este servit la momentul curent de *MSC*; aceste informații sunt copii ale informațiilor originale stocate în *HLR*.

Scopul principal este reducerea numărului de mesaje între *MSC* și *HLR*.



Subsistemul rețea

Registrul de localizare a vizitatorilor (VLR)

Reține informații despre fiecare utilizator care este servit la momentul curent de *MSC*; aceste informații sunt copii ale informațiilor originale stocate în *HLR*.

Scopul principal este reducerea numărului de mesaje între *MSC* și *HLR*.

Când un utilizator ajunge în zona unui *MSC*, datele sunt copiate în *VLR*-ul aferent, fiind disponibile local pentru orice conexiune.



Subsistemu rețea

Registrul de localizare a vizitatorilor (VLR)

Reține informații despre fiecare utilizator care este servit la momentul curent de *MSC*; aceste informații sunt copii ale informațiilor originale stocate în *HLR*.

Scopul principal este reducerea numărului de mesaje între *MSC* și *HLR*.

Când un utilizator ajunge în zona unui *MSC*, datele sunt copiate în *VLR*-ul aferent, fiind disponibile local pentru orice conexiune.

Când acesta părăsește zona, informațiile respective sunt copiate din *HLR* în *VLR*-ul noului *MSC*, fiind șterse din *VLR*-ul anterior.



Subsistemul rețea

Registrul de localizare a vizitatorilor (*VLR*)

Reține informații despre fiecare utilizator care este servit la momentul curent de *MSC*; aceste informații sunt copii ale informațiilor originale stocate în *HLR*.

Scopul principal este reducerea numărului de mesaje între *MSC* și *HLR*.

Când un utilizator ajunge în zona unui *MSC*, datele sunt copiate în *VLR*-ul aferent, fiind disponibile local pentru orice conexiune.

Când acesta părăsește zona, informațiile respective sunt copiate din *HLR* în *VLR*-ul noului *MSC*, fiind șterse din *VLR*-ul anterior.

Deși este posibilă implementarea lui *VLR* ca o componentă hardware independentă, în majoritatea cazurilor el este o componentă software din *MSC*.

Subsistemul rețea

Registrul de localizare (*HLR*)

Este baza de date cu utilizatori a rețelei *GSM*: conține informații despre serviciile disponibile pentru fiecare utilizator în parte.



Subsistemu rețea

Registrul de localizare (HLR)

Este baza de date cu utilizatori a rețelei GSM: conține informații despre serviciile disponibile pentru fiecare utilizator în parte.

Exemplu

IMSI-ul (care identifică un utilizator) este stocat pe SIM și în HLR; el reprezintă cheia către orice informație despre utilizator.



Subsistemul rețea

Registrul de localizare (HLR)

Este baza de date cu utilizatori a rețelei GSM: conține informații despre serviciile disponibile pentru fiecare utilizator în parte.

Exemplu

IMSI-ul (care identifică un utilizator) este stocat pe SIM și în HLR; el reprezintă cheia către orice informație despre utilizator. Atunci când telefonul este deschis, se recuperează IMSI de pe SIM și este transmis către MSC care – la rândul său – poate cere informații din HLR referitoare la utilizatorul respectiv.



Subsistemul rețea

Registrul de localizare (HLR)

Este baza de date cu utilizatori a rețelei GSM: conține informații despre serviciile disponibile pentru fiecare utilizator în parte.

Exemplu

IMSI-ul (care identifică un utilizator) este stocat pe SIM și în HLR; el reprezintă cheia către orice informație despre utilizator. Atunci când telefonul este deschis, se recuperează IMSI de pe SIM și este transmis către MSC care – la rândul său – poate cere informații din HLR referitoare la utilizatorul respectiv.

Numărul de telefon al utilizatorului are o lungime de maxim 15 cifre; el conține codul țării, codul național destinație (corespunzător operatorului respectiv) iar restul cifrelor reprezintă numărul utilizatorului.



Subsistemul rețea

Centrul de autentificare (AC)

AC deține o cheie secretă K_i pentru fiecare utilizator, care este o copie a cheii K_i de pe cartela sa SIM.

Pentru anumite operații din rețea (cum ar fi stabilirea unui apel), utilizatorul este identificat prin K_i .



Centrul de autentificare (AC)

AC deține o cheie secretă K_i pentru fiecare utilizator, care este o copie a cheii K_i de pe cartela sa SIM.

Pentru anumite operații din rețea (cum ar fi stabilirea unui apel), utilizatorul este identificat prin K_i .

În AC se află de asemenea cheile de autentificare și de criptare pentru toți utilizatorii din HLR și din VLR-urile aflate în rețeaua furnizorului.



Centrul de autentificare (AC)

AC deține o cheie secretă K_i pentru fiecare utilizator, care este o copie a cheii K_i de pe cartela sa SIM.

Pentru anumite operații din rețea (cum ar fi stabilirea unui apel), utilizatorul este identificat prin K_i .

În AC se află de asemenea cheile de autentificare și de criptare pentru toți utilizatorii din HLR și din VLR-urile aflate în rețeaua furnizorului.

În particular, de aici sunt trimise triplete de tipul

$$(RAND, SRES, K_c)$$

necesare pentru procesul de autentificare.



Registrul de identificare a echipamentului (*EIR*)

EIR este o bază de date care stochează o listă cu toate echipamentele mobile valide în rețea, fiecare telefon fiind identificat prin *IMEI* (*International Mobile Equipment Identity*).



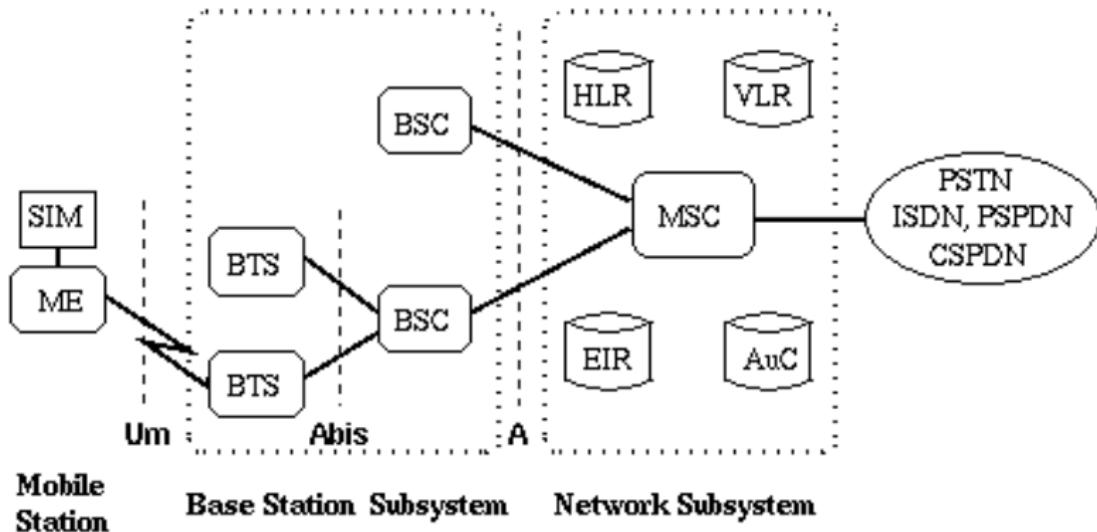
Registrul de identificare a echipamentului (*EIR*)

EIR este o bază de date care stochează o listă cu toate echipamentele mobile valide în rețea, fiecare telefon fiind identificat prin *IMEI* (*International Mobile Equipment Identity*).

Un *IMEI* este marcat ca fiind invalid dacă a fost declarat furat sau dacă tipul său este unul neaprobat.



Subsistemul rețea



SIM Subscriber Identity Module

ME Mobile Equipment

BTS Base Transceiver Station

BSC Base Station Controller

HLR Home Location Register

VLR Visitor Location Register

MSC Mobile services Switching Center

EIR Equipment Identity Register

AuC Authentication Center

Înregistrarea locației

Locația unei stații mobile este identificată de:

Înregistrarea locației

Locația unei stații mobile este identificată de:

- *codul țării respective (mobile country code) (MCC)*: trei cifre care identifică țara în care este situată rețeaua.

Înregistrarea locației

Locația unei stații mobile este identificată de:

- *codul țării respective (mobile country code) (MCC)*: trei cifre care identifică țara în care este situată rețeaua.
- *codul rețelei mobile (MNC)*: două cifre care identifică rețele (concurrente) din aceeași țară.

Înregistrarea locației

Locația unei stații mobile este identificată de:

- *codul țării respective (mobile country code) (MCC)*: trei cifre care identifică țara în care este situată rețeaua.
- *codul rețelei mobile (MNC)*: două cifre care identifică rețele (concurrente) din aceeași țară.
- *identitatea locației (LAI)*: identifică regiunea fizică (una sau mai multe celule) în care este localizată stația mobilă.

Înregistrarea locației

Locația unei stații mobile este identificată de:

- *codul țării respective (mobile country code) (MCC)*: trei cifre care identifică țara în care este situată rețeaua.
- *codul rețelei mobile (MNC)*: două cifre care identifică rețele (concurrente) din aceeași țară.
- *identitatea locației (LAI)*: identifică regiunea fizică (una sau mai multe celule) în care este localizată stația mobilă.

Aceste trei valori formează *IMSI*-ul care identifică în mod unic un utilizator.

Există trei tipuri de proceduri pentru actualizarea locației:

Există trei tipuri de proceduri pentru actualizarea locației:

- 1 **Înregistrarea**: când este deschisă o stație mobilă. Ea va căuta rețelele disponibile; când va găsi o astfel de rețea, stația mobilă va citi informații despre locație și va trimite *IMSI*-ul său rețelei respective.

Există trei tipuri de proceduri pentru actualizarea locației:

- 1 Înregistrarea:** când este deschisă o stație mobilă. Ea va căuta rețelele disponibile; când va găsi o astfel de rețea, stația mobilă va citi informații despre locație și va trimite *IMSI*-ul său rețelei respective.
- 2 Actualizarea periodică a locației:** este efectuată după o perioadă de timp predefinită de rețea și este trimisă constant tuturor stațiilor mobile active care monitorizează canalul de control.

Există trei tipuri de proceduri pentru actualizarea locației:

- 1 **Înregistrarea**: când este deschisă o stație mobilă. Ea va căuta rețelele disponibile; când va găsi o astfel de rețea, stația mobilă va citi informații despre locație și va trimite *IMSI*-ul său rețelei respective.
- 2 **Actualizarea periodică a locației**: este efectuată după o perioadă de timp predefinită de rețea și este trimisă constant tuturor stațiilor mobile active care monitorizează canalul de control.
- 3 Când stația mobilă detectează o **schimbare a regiunii** în care se află, va anunța rețeaua despre această schimbare.

Stabilirea apelului în *GSM*

- 1 Telefonul – trimite pe canalul *RACH* – un mesaj RANDOM REQUEST de 8 biți. Acesta solicită stației de bază alocarea resurselor radio pentru realizarea conексiunii.

Stabilirea apelului în *GSM*

- 1 Telefonul – trimite pe canalul *RACH* – un mesaj RANDOM REQUEST de 8 biți. Acesta solicită stației de bază alocarea resurselor radio pentru realizarea conexiunii.
- 2 Rețeaua trimite un mesaj IMMEDIATE REQUEST pe canalul *PAGCh*, care conține valoarea aleatoare primită de la telefon, detalii despre canalul alocat telefonului mobil, împreună cu alte informații tehnice.

Stabilirea apelului în GSM

- 1 Telefonul – trimite pe canalul *RACH* – un mesaj RANDOM REQUEST de 8 biți. Acesta solicită stației de bază alocarea resurselor radio pentru realizarea conexiunii.
- 2 Rețeaua trimite un mesaj IMMEDIATE REQUEST pe canalul *PAGCh*, care conține valoarea aleatoare primită de la telefon, detalii despre canalul alocat telefonului mobil, împreună cu alte informații tehnice.
Mobilul se va racorda imediat la canalul de trafic alocat.

Autentificarea

- 1 Rețeaua trimite o cerere de autentificare care include valoarea $RAND$ și un număr care va stoca cheia K_c rezultată.

Autentificarea

- 1 Rețeaua trimite o cerere de autentificare care include valoarea *RAND* și un număr care va stoca cheia K_c rezultată.
- 2 Mobilul răspunde cu valoarea *SRES* calculată,

Autentificarea

- 1 Rețeaua trimite o cerere de autentificare care include valoarea $RAND$ și un număr care va stoca cheia K_c rezultată.
- 2 Mobilul răspunde cu valoarea $SRES$ calculată,
- 3 Rețeaua cere mobilului – prin comanda $CIPHMOD$ – să înceapă criptarea; ea poate specifica algoritmul de criptare folosit și – eventual – cheia de criptare.
În paralel, rețeaua începe să decripteze informațiile primite.

Autentificarea

- 1 Rețeaua trimite o cerere de autentificare care include valoarea $RAND$ și un număr care va stoca cheia K_c rezultată.
- 2 Mobilul răspunde cu valoarea $SRES$ calculată,
- 3 Rețeaua cere mobilului – prin comanda $CIPHMOD$ – să înceapă criptarea; ea poate specifica algoritmul de criptare folosit și – eventual – cheia de criptare.
În paralel, rețeaua începe să decripteze informațiile primite.
- 4 Mobilul începe criptarea și decriptarea și răspunde cu mesajul $CIPHMODCOM$ criptat.
La cerere, el trimitе și $IMEI$ -ul.

Rutarea apelului între două stații mobile

Când *Alice* inițiază un apel mobil către *Bob*, apelul va fi rutat către *GMSC*-ul rețelei.

Rutarea apelului între două stații mobile

Când *Alice* inițiază un apel mobil către *Bob*, apelul va fi rutat către *GMSC*-ul rețelei.

Dacă rețeaua are mai multe astfel de “porți de intrare”, apelul este rutat către *GMSC*-ul de care aparține *Bob* (acel *GMSC* al cărui *HLR* atașat conține o înregistrare cu datele lui *Bob*).

Rutarea apelului între două stații mobile

Când *Alice* inițiază un apel mobil către *Bob*, apelul va fi rutat către *GMSC-ul* rețelei.

Dacă rețeaua are mai multe astfel de “porți de intrare”, apelul este rutat către *GMSC-ul* de care aparține *Bob* (acel *GMSC* al cărui *HLR* atașat conține o înregistrare cu datele lui *Bob*).

GMSC-ul va afla locația lui *Bob* prin lansarea unei cereri de localizare, la care răspunde un *HLR*.

Rutarea apelului între două stații mobile

Când *Alice* inițiază un apel mobil către *Bob*, apelul va fi rutat către *GMSC*-ul rețelei.

Dacă rețeaua are mai multe astfel de “porți de intrare”, apelul este rutat către *GMSC*-ul de care aparține *Bob* (acel *GMSC* al cărui *HLR* atașat conține o înregistrare cu datele lui *Bob*).

GMSC-ul va afla locația lui *Bob* prin lansarea unei cereri de localizare, la care răspunde un *HLR*.

Acesta va transmite către *GMSC* zona sau *MSC*-ul corespunzător lui *Bob*.



Rutarea apelului între două stații mobile

Când *Alice* inițiază un apel mobil către *Bob*, apelul va fi rutat către *GMSC*-ul rețelei.

Dacă rețeaua are mai multe astfel de “porți de intrare”, apelul este rutat către *GMSC*-ul de care aparține *Bob* (acel *GMSC* al cărui *HLR* atașat conține o înregistrare cu datele lui *Bob*).

GMSC-ul va afla locația lui *Bob* prin lansarea unei cereri de localizare, la care răspunde un *HLR*.

Acesta va transmite către *GMSC* zona sau *MSC*-ul corespunzător lui *Bob*.

Cu această informație, *GMSC*-ul poate ruta apelul către acel *MSC* care poate finaliza inițierea apelului.



Rutarea apelului între două stații mobile

Când *Alice* inițiază un apel mobil către *Bob*, apelul va fi rutat către *GMSC*-ul rețelei.

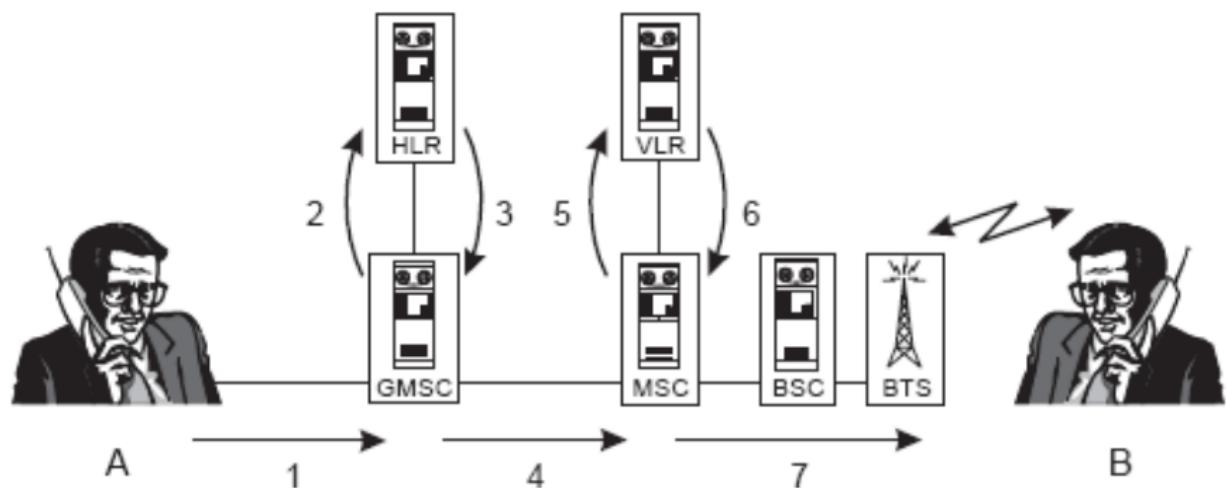
Dacă rețeaua are mai multe astfel de “porți de intrare”, apelul este rutat către *GMSC*-ul de care aparține *Bob* (acel *GMSC* al cărui *HLR* atașat conține o înregistrare cu datele lui *Bob*).

GMSC-ul va afla locația lui *Bob* prin lansarea unei cereri de localizare, la care răspunde un *HLR*.

Acesta va transmite către *GMSC* zona sau *MSC*-ul corespunzător lui *Bob*.

Cu această informație, *GMSC*-ul poate ruta apelul către acel *MSC* care poate finaliza inițierea apelului.

Mai departe, *MSC* este capabil să trimită apelul spre *Bob*, folosind *BTS*-ul corect.



Cerințe de securitate

Trei aspecte de securitate asigurate de sistemul *GSM*:

Cerințe de securitate

Trei aspecte de securitate asigurate de sistemul *GSM*:

- *Autentificarea utilizatorilor*: telefonul mobil trebuie să-și dovedească dreptul de acces la un anumit cont din rețeaua operatorului dorit.

Cerințe de securitate

Trei aspecte de securitate asigurate de sistemul GSM:

- *Autentificarea utilizatorilor*: telefonul mobil trebuie să-și dovedească dreptul de acces la un anumit cont din rețeaua operatorului dorit.
- *Anonimitatea utilizatorilor*: identificarea unui utilizator în rețea să fie o problemă dificilă pentru cineva din afara sistemului.

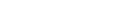
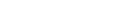
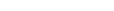
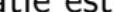
Cerințe de securitate

Trei aspecte de securitate asigurate de sistemul GSM:

- *Autentificarea utilizatorilor*: telefonul mobil trebuie să-și dovedească dreptul de acces la un anumit cont din rețeaua operatorului dorit.
- *Anonimitatea utilizatorilor*: identificarea unui utilizator în rețea să fie o problemă dificilă pentru cineva din afara sistemului.
- *Confidențialitatea*: informațiile comunicate wireless trebuie să fie protejate, iar accesarea lor să fie posibilă doar utilizatorilor destinați.



Securitatea GSM





Anonimitatea

Identificarea unui utilizator se face cu ajutorul numărului unic *IMSI* aflat pe *SIM*. Cum această informație este publică, este suficient ca cineva să-l intercepteze pentru a identifica utilizatorul corespunzător și a-i afla locația.

Proprietatea de anonimitate protejează identitatea utilizatorului față de cineva care dispune de *IMSI*-ul său.



Anonimitatea

Identificarea unui utilizator se face cu ajutorul numărului unic *IMSI* aflat pe *SIM*. Cum această informație este publică, este suficient ca cineva să-l intercepteze pentru a identifica utilizatorul corespunzător și a-i afla locația.

Proprietatea de anonimitate protejează identitatea utilizatorului față de cineva care dispune de *IMSI*-ul său.



Anonimitatea

GSM asigură anonimitatea folosind un identificator temporar pentru client – *TMSI* (*Temporary Mobile Subscriber Identity*) este valid numai local și este asignat utilizatorului atunci când cartela *SIM* s-a autentificat în rețea.

Pentru comunicarea cu acel *SIM*, rețeaua va folosi în continuare numai *TMSI*-ul alocat.



Anonimitatea

GSM asigură anonimitatea folosind un identificator temporar pentru client – *TMSI* (*Temporary Mobile Subscriber Identity*) este valid numai local și este asignat utilizatorului atunci când cartela *SIM* s-a autentificat în rețea.

Pentru comunicarea cu acel *SIM*, rețeaua va folosi în continuare numai *TMSI*-ul alocat.

La închidere, stația mobilă memorează *TMSI*-ul actual pe cartela *SIM*, pentru a fi accesibil atunci când este repornită.



Anonimitatea

GSM asigură anonimitatea folosind un identificator temporar pentru client – *TMSI* (*Temporary Mobile Subscriber Identity*) este valid numai local și este asignat utilizatorului atunci când cartela *SIM* s-a autentificat în rețea.

Pentru comunicarea cu acel *SIM*, rețeaua va folosi în continuare numai *TMSI*-ul alocat.

La închidere, stația mobilă memorează *TMSI*-ul actual pe cartela *SIM*, pentru a fi accesibil atunci când este repornită.

Pe de altă parte, se poate vorbi despre anonimitatea transmițătorului și a receptorului.



Anonimitatea

GSM asigură anonimitatea folosind un identificator temporar pentru client – *TMSI* (*Temporary Mobile Subscriber Identity*) este valid numai local și este asignat utilizatorului atunci când cartela *SIM* s-a autentificat în rețea.

Pentru comunicarea cu acel *SIM*, rețeaua va folosi în continuare numai *TMSI*-ul alocat.

La închidere, stația mobilă memorează *TMSI*-ul actual pe cartela *SIM*, pentru a fi accesibil atunci când este repornită.

Pe de altă parte, se poate vorbi despre anonimitatea transmițătorului și a receptorului.

Anonimitatea transmițătorului se referă la ascunderea identității expeditorului unui mesaj, iar *anonimitatea receptorului* oferă posibilitatea de a-l contacta pe destinatar chiar dacă acesta rămâne anonim.



Probleme legate de stabilirea anonimității

- Un abonat trebuie să poată fi accesat oricând: rețeaua trebuie să îl știe mereu locația – pentru a putea ruta apelurile sosite către el.



Probleme legate de stabilirea anonimității

- Un abonat trebuie să poată fi accesat oricând: rețeaua trebuie să îi știe mereu locația – pentru a putea ruta apelurile sosite către el.
 - Numărul de telefon al unei persoane – odată știut – poate fi considerat public: poate fi divulgat și altor persoane, chiar fără consimțământul proprietarului.



Probleme legate de stabilirea anonimității

- Un abonat trebuie să poată fi accesat oricând: rețeaua trebuie să îi știe mereu locația – pentru a putea ruta apelurile sosite către el.
- Numărul de telefon al unei persoane – odată știut – poate fi considerat public: poate fi divulgat și altor persoane, chiar fără consimțământul proprietarului.
- Apelurile *GSM* trebuie să se desfășoare în timp real și sunt facturate în funcție de timp, de regulile stabilite în contract etc.



Probleme legate de stabilirea anonimității

- Un abonat trebuie să poată fi accesat oricând: rețeaua trebuie să îi știe mereu locația – pentru a putea ruta apelurile sosite către el.
- Numărul de telefon al unei persoane – odată știut – poate fi considerat public: poate fi divulgat și altor persoane, chiar fără consimțământul proprietarului.
- Apelurile GSM trebuie să se desfășoare în timp real și sunt facturate în funcție de timp, de regulile stabilite în contract etc.

Transmițătorul trebuie să fie legat de o anume entitate ce poate fi identificată, astfel ca după un anumit interval de timp (de obicei lunar), operațiunile efectuate de el în rețea să poată fi facturate.

Anonimitatea

Atacuri asupra anonimității

Pot fi active sau pasive.



Atacuri asupra anonimității

Pot fi active sau pasive.

- 1 Atacatorul poate iniția un atac pasiv când doar “ascultă” traficul, fără a efectua acțiuni.



Anonimitatea

Atacuri asupra anonimității

Pot fi active sau pasive.

- 1** Atacatorul poate iniția un atac pasiv când doar “ascultă” traficul, fără a efectua acțiuni.
- 2** La o monitorizarea activă, atacatorul se implică prin fabricarea și inserarea unor mesaje, distrugerea altora etc.



Monitorizare pasivă

La fiecare pornire a unei stații mobile se atașează un *IMSI*, pentru a informa rețeaua asupra faptului că *IMSI*-ul respectiv este activ din acel moment.



Anonimitatea

Monitorizare pasivă

La fiecare pornire a unei stații mobile se atașează un *IMSI*, pentru a informa rețea asupra faptului că *IMSI*-ul respectiv este activ din acel moment.

Protocolul folosește procedura de actualizare a locației în care stația mobilă transmite un mesaj, împreună cu *IMSI*-ul său.

Dacă acesta nu este înregistrat în rețea, atunci nu îi este asociată nici o cheie K_i , iar criptarea nu poate fi aplicată.



Monitorizare pasivă

La fiecare pornire a unei stații mobile se atașează un *IMSI*, pentru a informa rețea asupra faptului că *IMSI*-ul respectiv este activ din acel moment.

Protocolul folosește procedura de actualizare a locației în care stația mobilă transmite un mesaj, împreună cu *IMSI*-ul său.

Dacă acesta nu este înregistrat în rețea, atunci nu îi este asociată nici o cheie K_i , iar criptarea nu poate fi aplicată.

Deci *IMSI* trebuie transmis în clar, iar un atacator care ascultă traficul, îl poate extrage.



Monitorizare activă

Oscar poate comunica cu stația mobilă.



Monitorizare activă

Oscar poate comunica cu stația mobilă.

El va folosi o procedură de identificare, în care rețeaua va efectua un IDENTITY REQUEST, cerând stației mobile, *IMSI*, *IMEI* sau *TMSI*.



Monitorizare activă

Oscar poate comunica cu stația mobilă.

El va folosi o procedură de identificare, în care rețeaua va efectua un IDENTITY REQUEST, cerând stației mobile, *IMSI*, *IMEI* sau *TMSI*.

Deoarece *GSM* nu verifică autenticitatea unui mesaj, *Oscar* poate pretinde că este stație de bază, obținând astfel – prin intermediul unui astfel de mesaj – informația dorită.



Monitorizare activă

Oscar poate comunica cu stația mobilă.

El va folosi o procedură de identificare, în care rețeaua va efectua un IDENTITY REQUEST, cerând stației mobile, *IMSI*, *IMEI* sau *TMSI*.

Deoarece *GSM* nu verifică autenticitatea unui mesaj, *Oscar* poate pretinde că este stație de bază, obținând astfel – prin intermediul unui astfel de mesaj – informația dorită.

După ce deține *IMSI*-ul, atacatorul își poate identifica victimă.

Anonimitatea

Următorul pas este găsirea *TMSI*-ului pe care rețeaua îl alocă stației mobile, astfel ca *Oscar* să-l poată asocia *IMSI*-ului; aceasta îi permite ulterior să urmărească mișările stației mobile.



Următorul pas este găsirea *TMSI*-ului pe care rețeaua îl alocă stației mobile, astfel ca *Oscar* să-l poată asocia *IMSI*-ului; aceasta îi permite ulterior să urmărească mișcările stației mobile.

TMSI-ul este criptat înainte de a fi transmis, deci Oscar va trebui să-l decripteze.

El va genera o situație în care cele două entități legitime care comunică să credă că dispun de capabilități diferite de criptare.



Anonimitatea

Următorul pas este găsirea *TMSI*-ului pe care rețeaua îl alocă stației mobile, astfel ca *Oscar* să-l poată asocia *IMSI*-ului; aceasta îi permite ulterior să urmărească mișcările stației mobile.

TMSI-ul este criptat înainte de a fi transmis, deci *Oscar* va trebui întâi să-l decripteze.

El va genera o situație în care cele două entități legitime care comunică să credă că dispun de capabilități diferite de criptare.

Oscar poate face acest lucru deoarece poate inseră, distruge sau fabrică mesaje – lucru posibil datorită faptului că *GSM* nu asigură integritatea mesajelor și nici autentificarea rețea-utilizator.

Autentificarea

Autentificare

Se evită situațiile când persoane neautorizate pătrund în rețea prezentând că sunt utilizatori acceptați ai rețelei.

Autentificare

Se evită situațiile când persoane neautorizate pătrund în rețea prezentând că sunt utilizatori acceptați ai rețelei.

Înainte de a avea acces la serviciile unei rețele *GSM*, un utilizator trebuie să se autentifice.

Autentificarea

- 1 La pornire, echipamentul mobil începe cu căutarea unei rețele wireless la care să se conecteze.
Când a găsit frecvența dorită, *SIM*-ul încearcă să se autentifice, trimițând un mesaj la *BTS* prin care cere accesul la rețea.



Autentificarea

- 1 La pornire, echipamentul mobil începe cu căutarea unei rețele wireless la care să se conecteze.
Când a găsit frecvența dorită, *SIM*-ul încearcă să se autentifice, trimițând un mesaj la *BTS* prin care cere accesul la rețea.
- 2 *BTS*-ul comunică cu centrul de comutare pentru a decide permiterea accesului, folosind un protocol provocare - răspuns, bazat pe cheia secretă K_i partajată între telefon și rețea.



Autentificarea

- 1 La pornire, echipamentul mobil începe cu căutarea unei rețele wireless la care să se conecteze.
Când a găsit frecvența dorită, *SIM*-ul încearcă să se autentifice, trimițând un mesaj la *BTS* prin care cere accesul la rețea.
- 2 *BTS*-ul comunică cu centrul de comutare pentru a decide permiterea accesului, folosind un protocol provocare - răspuns, bazat pe cheia secretă K_i partajată între telefon și rețea.
- 3 Centrul de comutare obține de la registrul de locații un triplet de forma $(RAND, SRES, K_c)$ unde:



Autentificarea

- 1 La pornire, echipamentul mobil începe cu căutarea unei rețele wireless la care să se conecteze.
Când a găsit frecvența dorită, *SIM*-ul încearcă să se autentifice, trimițând un mesaj la *BTS* prin care cere accesul la rețea.
- 2 *BTS*-ul comunică cu centrul de comutare pentru a decide permiterea accesului, folosind un protocol provocare - răspuns, bazat pe cheia secretă K_i partajată între telefon și rețea.
- 3 Centrul de comutare obține de la registrul de locații un triplet de forma $(RAND, SRES, K_c)$ unde:
 - 1 $RAND$ este un număr aleator pe 128 biți,



Autentificarea

- 1** La pornire, echipamentul mobil începe cu căutarea unei rețele wireless la care să se conecteze.

Când a găsit frecvența dorită, *SIM*-ul încearcă să se autentifice, trimițând un mesaj la *BTS* prin care cere accesul la rețea.

- 2** *BTS*-ul comunică cu centrul de comutare pentru a decide permiterea accesului, folosind un protocol provocare - răspuns, bazat pe cheia secretă K_i partajată între telefon și rețea.
- 3** Centrul de comutare obține de la registrul de locații un triplet de forma $(RAND, SRES, K_c)$ unde:
 - 1** *RAND* este un număr aleator pe 128 biți,
 - 2** *SRES* este un răspuns pe 32 biți de la *RAND*, semnat și generat folosind K_i ,



Autentificarea

- 1** La pornire, echipamentul mobil începe cu căutarea unei rețele wireless la care să se conecteze.
Când a găsit frecvența dorită, *SIM*-ul încearcă să se autentifice, trimițând un mesaj la *BTS* prin care cere accesul la rețea.
- 2** *BTS*-ul comunică cu centrul de comutare pentru a decide permiterea accesului, folosind un protocol provocare - răspuns, bazat pe cheia secretă K_i partajată între telefon și rețea.
- 3** Centrul de comutare obține de la registrul de locații un triplet de forma $(RAND, SRES, K_c)$ unde:
 - 1** $RAND$ este un număr aleator pe 128 biți,
 - 2** $SRES$ este un răspuns pe 32 biți de la $RAND$, semnat și generat folosind K_i ,
 - 3** K_c este cheia de sesiune pentru criptare, generată tot cu ajutorul lui K_i .

Autentificarea

- 4 După obținerea acestui triplet, *RAND* este trimis (via *BSC* și *BTS*) ca o provocare către stația mobilă.

Autentificarea

- 4 După obținerea acestui triplet, $RAND$ este trimis (via BSC și BTS) ca o provocare către stația mobilă.
- 5 Ca răspuns la provocare, cartela SIM a stației mobile va genera un $SRES$ – folosind algoritmul $A3$ și acel K_i păstrat stocat ($SRES = A3(K_i, RAND)$).



Autentificarea

- 4 După obținerea acestui triplet, $RAND$ este trimis (via BSC și BTS) ca o provocare către stația mobilă.
- 5 Ca răspuns la provocare, cartela SIM a stației mobile va genera un $SRES$ – folosind algoritmul $A3$ și acel K_i păstrat stocat ($SRES = A3(K_i, RAND)$).
- 6 Apoi, cartela SIM trimite $SRES$ -ul calculat către MSC , care îl compară cu $SRES$ -ul conținut în tripletul primit de la HLR . Dacă cele două coincid, MSC permite accesul în rețea.



Autentificarea

A3 și A8 nu sunt algoritmi în sine, ci etichetele unor funcții one-way, ceea ce asigură imposibilitatea descoperirii cheii K_i . Furnizorii de telefonie mobilă pot folosi orice algoritm pentru a genera SRES din K_i și RAND.



Autentificarea

A3 și A8 nu sunt algoritmi în sine, ci etichetele unor funcții one-way, ceea ce asigură imposibilitatea descoperirii cheii K_i . Furnizorii de telefonie mobilă pot folosi orice algoritm pentru a genera *SRES* din K_i și RAND.

Majoritatea implementărilor GSM combină A3 cu A8 și folosesc un singur algoritm: COMP128.



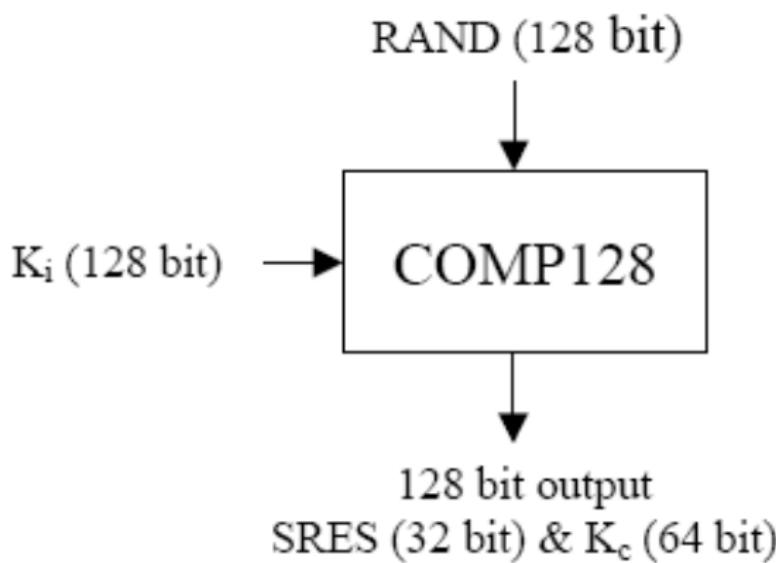
Autentificarea

A3 și A8 nu sunt algoritmi în sine, ci etichetele unor funcții one-way, ceea ce asigură imposibilitatea descoperirii cheii K_i . Furnizorii de telefonie mobilă pot folosi orice algoritm pentru a genera *SRES* din K_i și RAND.

Majoritatea implementărilor GSM combină A3 cu A8 și folosesc un singur algoritm: COMP128.

Acesta are la intrare cheia K_i și RAND și generează SRES pe 32 biti și un alt număr pe 54 de biți, căruia i se adaugă la sfârșit încă 10 biți egali cu 0, pentru a forma cheia de sesiune K_c pe 64 biți – folosită pentru asigurarea confidențialității.

Autentificarea



Cheia secretă K_i , identifierul *IMSI*, funcțiile A3 și A8 sunt stocate și implementate în cartela *SIM* a telefonului.
 K_i nu părăsește niciodată cartela *SIM*.

Autentificarea

Este remarcabilă relația de încredere între componentele rețelei între care se transmit informațiile confidențiale (centrul de comutare - registrul de locații, *BSC - MSC*).

Este remarcabilă relația de încredere între componentele rețelei între care se transmit informațiile confidențiale (centrul de comutare - registrul de locații, *BSC - MSC*).

Ea evidențiază o caracteristică a rețelei *GSM*: încercarea de a securiza numai partea wireless.

Motivul: *GSM* a evoluat din rețeaua de telefonie publică *PSTN* și își propune să fie cel puțin la fel de sigură.

Partea centrală a *PSTN* este securizată prin restricționarea accesului fizic la rețea.



Autentificarea

Este remarcabilă relația de încredere între componentele rețelei între care se transmit informațiile confidențiale (centrul de comutare - registrul de locații, *BSC - MSC*).

Ea evidențiază o caracteristică a rețelei *GSM*: încercarea de a securiza numai partea wireless.

Motivul: *GSM* a evoluat din rețeaua de telefonie publică *PSTN* și își propune să fie cel puțin la fel de sigură.

Partea centrală a *PSTN* este securizată prin restricționarea accesului fizic la rețea.

Totuși, există o relație între componente înfără rețelei centrale: *BTS - BSC*.

Ea rămâne o cale de atacuri posibile; de altfel, *GSM* nu specifică nici o metodă de securizare a acesteia.

Autentificarea

În *GSM*, entitatea autentificată este cartela *SIM* iar nu utilizatorul în sine.

Autentificarea

În GSM, entitatea autentificată este cartela *SIM* iar nu utilizatorul în sine.

Atunci când un client a pierdut echipamentul sau cartela *SIM*, el are responsabilitatea de a comunica aceasta către furnizorul său de telefonie mobilă.

Cum rețeaua menține o bază de date cu echipamentele valide – prin extrapolare – furnizorul de servicii ar putea avea și o bază cu *SIM*-urile valide.

Atac asupra algoritmului de autentificare prin acces fizic la cartela *SIM*

Deși *COMP128* nu a fost niciodată publicat oficial, el s-a aflat prin inginerie inversă.

Atac asupra algoritmului de autentificare prin acces fizic la cartela SIM

Deși COMP128 nu a fost niciodată publicat oficial, el s-a aflat prin inginerie inversă.

O criptanaliză lansată asupra lui a găsit cheia K_i partajată între telefonul mobil și rețea; având K_i , A3 și A8, clonarea cartelei GSM este simplu de realizat.

Atac asupra algoritmului de autentificare prin acces fizic la cartela *SIM*

Deși *COMP128* nu a fost niciodată publicat oficial, el s-a aflat prin inginerie inversă.

O criptanaliză lansată asupra lui a găsit cheia K_i partajată între telefonul mobil și rețea; având K_i , $A3$ și $A8$, clonarea cartelei *GSM* este simplu de realizat.

Securitatea întregului sistem *GSM* se bazează pe cheia secretă K_i .

Atac asupra algoritmului de autentificare prin acces fizic la cartela *SIM*

Deși *COMP128* nu a fost niciodată publicat oficial, el s-a aflat prin inginerie inversă.

O criptanaliză lansată asupra lui a găsit cheia K_i partajată între telefonul mobil și rețea; având K_i , $A3$ și $A8$, clonarea cartelei *GSM* este simplu de realizat.

Securitatea întregului sistem *GSM* se bazează pe cheia secretă K_i .
Odată ce intrusul *Oscar* este capabil să extragă cheia, el poate nu numai să asculte apelurile abonatului urmărit, dar se poate substitui acestuia în cadrul rețelei, efectuând apeluri în contul lui.



Autentificarea

În concluzie, COMP128 este compromis: *Oscar* poate observa intrarea și ieșirea în cadrul algoritmului A8 și – pe baza lor – poate calcula K_i (intrarea este o provocare aleatoare trimisă din rețeaua abonatului iar ieșirea este un răspuns de la SRES-ul telefonului mobil).



Autentificarea

În concluzie, COMP128 este compromis: *Oscar* poate observa intrarea și ieșirea în cadrul algoritmului A8 și – pe baza lor – poate calcula K_i (intrarea este o provocare aleatoare trimisă din rețeaua abonatului iar ieșirea este un răspuns de la SRES-ul telefonului mobil).

S-a constatat că un atacator cu acces fizic la telefonul țintă poate face o clonă (duplicat identic cu originalul) și poate efectua astfel apeluri frauduloase în contul abonatului.



Autentificarea

În concluzie, COMP128 este compromis: *Oscar* poate observa intrarea și ieșirea în cadrul algoritmului A8 și – pe baza lor – poate calcula K_i (intrarea este o provocare aleatoare trimisă din rețeaua abonatului iar ieșirea este un răspuns de la SRES-ul telefonului mobil).

S-a constatat că un atacator cu acces fizic la telefonul țintă poate face o clonă (duplicat identic cu originalul) și poate efectua astfel apeluri frauduloase în contul abonatului.

Implementarea acestui atac folosește un cititor de smartcard-uri și un computer.

Atacul presupune interogarea cardului de 150.000 de ori; cu un cititor de carduri capabil să efectueze aproximativ 6 invocări pe secundă, atacul durează 8 ore.



Autentificarea

În concluzie, COMP128 este compromis: *Oscar* poate observa intrarea și ieșirea în cadrul algoritmului A8 și – pe baza lor – poate calcula K_i (intrarea este o provocare aleatoare trimisă din rețeaua abonatului iar ieșirea este un răspuns de la SRES-ul telefonului mobil).

S-a constatat că un atacator cu acces fizic la telefonul țintă poate face o clonă (duplicat identic cu originalul) și poate efectua astfel apeluri frauduloase în contul abonatului.

Implementarea acestui atac folosește un cititor de smartcard-uri și un computer.

Atacul presupune interogarea cardului de 150.000 de ori; cu un cititor de carduri capabil să efectueze aproximativ 6 invocări pe secundă, atacul durează 8 ore.

O măsură împotriva acestui atac este folosirea pentru autentificare a unei funcții mai tari de dispersie criptografică.

Autentificarea

Două versiuni noi – *COMP128 – 2* și *COMP128 – 3* – au fost propuse pentru corectarea acestor probleme de securitate.

COMP128 – 3 rezolvă problema celor 10 biți nuli din cheia de sesiune K_c .



Autentificarea

Două versiuni noi – *COMP128 – 2* și *COMP128 – 3* – au fost propuse pentru corectarea acestor probleme de securitate.

COMP128 – 3 rezolvă problema celor 10 biți nuli din cheia de sesiune K_c .

Problemă: deoarece $A3$ și $A8$ sunt stocați pe *SIM* – se impune schimbarea cartelelor abonaților.



Autentificarea

Două versiuni noi – *COMP128 – 2* și *COMP128 – 3* – au fost propuse pentru corectarea acestor probleme de securitate.

COMP128 – 3 rezolvă problema celor 10 biți nuli din cheia de sesiune K_c .

Problemă: deoarece $A3$ și $A8$ sunt stocați pe *SIM* – se impune schimbarea cartelelor abonaților.

De aceea majoritatea furnizorilor de telefonie mobilă nu au adoptat aceste versiuni ci au păstrat *COMP128 – 1* aplicând o restricție asupra cartelei *SIM*: au fixat un număr maxim de invocări asupra cartelei (sub 150.000), după care aceasta se bloca.



Autentificarea

Două versiuni noi – *COMP128 – 2* și *COMP128 – 3* – au fost propuse pentru corectarea acestor probleme de securitate.

COMP128 – 3 rezolvă problema celor 10 biți nuli din cheia de sesiune K_c .

Problemă: deoarece $A3$ și $A8$ sunt stocați pe *SIM* – se impune schimbarea cartelelor abonaților.

De aceea majoritatea furnizorilor de telefonie mobilă nu au adoptat aceste versiuni ci au păstrat *COMP128 – 1* aplicând o restricție asupra cartelei *SIM*: au fixat un număr maxim de invocări asupra cartelei (sub 150.000), după care aceasta se bloca.

Datorită faptului că algoritmul se află pe cartela *SIM* – care este un smartcard, orice descoperire asupra vulnerabilităților acestuia are repercușiuni asupra securității informațiilor stocate pe *SIM*: *IMSI* și K_i .

Atacul *Side channel*

O metodă prin care cheia K_i poate fi extrasă fără a avea acces fizic la SIM.



Atacul *Side channel*

O metodă prin care cheia K_i poate fi extrasă fără a avea acces fizic la SIM.

Atacatorul găsește relația între informația de intrare și cea de ieșire transmisă în timpul calculelor din canalele anexe; de exemplu o sincronizare a operațiilor, consumul de energie, emanații electromagnetice etc.

S-a constatat că prin analiza acestor caracteristici se pot obține informații confidențiale.



Atacul *Side channel*

O metodă prin care cheia K_i poate fi extrasă fără a avea acces fizic la SIM.

Atacatorul găsește relația între informația de intrare și cea de ieșire transmisă în timpul calculelor din canalele anexe; de exemplu o sincronizare a operațiilor, consumul de energie, emanații electromagnetice etc.

S-a constatat că prin analiza acestor caracteristici se pot obține informații confidențiale.

Atacuri de partiționare

O clasă de atacuri descoperită de cercetătorii de la *IBM* și folosită pentru a ataca implementări de algoritmi care altfel ar rezista la atacurile side channel.



Atacuri de partiționare

O clasă de atacuri descoperită de cercetătorii de la *IBM* și folosită pentru a ataca implementări de algoritmi care altfel ar rezista la atacurile side channel.

Cu ajutorul lor, cheia de 128 biți din *COMP128* poate fi extrasă de pe un *SIM* folosind mai puțin de 1000 invocări cu intrări aleatoare, sau 255 intrări alese, sau doar 8 intrări special alese.



Atacuri de partiționare

O clasă de atacuri descoperită de cercetătorii de la *IBM* și folosită pentru a ataca implementări de algoritmi care altfel ar rezista la atacurile side channel.

Cu ajutorul lor, cheia de 128 biți din *COMP128* poate fi extrasă de pe un *SIM* folosind mai puțin de 1000 invocări cu intrări aleatoare, sau 255 intrări alese, sau doar 8 intrări special alese.

Deci un adversar care se află un posesia cartelei *SIM* poate extrage cheia secretă K ; în maxim un minut.



Atacuri de partiționare

O clasă de atacuri descoperită de cercetătorii de la *IBM* și folosită pentru a ataca implementări de algoritmi care altfel ar rezista la atacurile side channel.

Cu ajutorul lor, cheia de 128 biți din *COMP128* poate fi extrasă de pe un *SIM* folosind mai puțin de 1000 invocări cu intrări aleatoare, sau 255 intrări alese, sau doar 8 intrări special alese.

Deci un adversar care se află un posesia cartelei *SIM* poate extrage cheia secretă K ; în maxim un minut.

Atacul prin partiționare poate fi folosit mai ales contra algoritmilor bazați pe căutări în tabele foarte mari.

COMP128 este un astfel de exemplu; el utilizează căutări în 5 tabele de câte 512, 256, 128, 64 și respectiv 32 biți.

Atacuri wireless asupra algoritmului de autentificare

Deoarece nu întotdeauna este posibil un acces fizic la *SIM* s-a generat un atac wireless (pe calea undelor radio).

Această abordare introduce alt tip de obstacole:



Atacuri wireless asupra algoritmului de autentificare

Deoarece nu întotdeauna este posibil un acces fizic la *SIM* să se genereze un atac wireless (pe calea undelor radio).

Această abordare introduce alt tip de obstacole:

Oscar trebuie să poată simula *BTS*-ul ca unul legitim.

Aceasta înseamnă că el are nevoie de o stație de bază falsă, capabilă să genereze un semnal suficient de puternic aşa încât să depășească semnalul *BTS*-ului legitim.



Atacuri wireless asupra algoritmului de autentificare

Deoarece nu întotdeauna este posibil un acces fizic la *SIM* să se genereze un atac wireless (pe calea undelor radio).

Această abordare introduce alt tip de obstacole:

Oscar trebuie să poată simula *BTS*-ul ca unul legitim.

Aceasta înseamnă că el are nevoie de o stație de bază falsă, capabilă să genereze un semnal suficient de puternic aşa încât să depășească semnalul *BTS*-ului legitim.

O posibilă rezolvare a acestei probleme ar fi lansarea atacului atunci când semnalul stației legitime este foarte slab.

Autentificarea

În plus *Oscar* mai trebuie să ştie *IMSI*-ul sau *TMSI*-ul cartelei *SIM* pe care vrea să o cloneze.

Autentificarea

În plus *Oscar* mai trebuie să ştie *IMSI*-ul sau *TMSI*-ul cartelei *SIM* pe care vrea să o cloneze.

Când aceste resurse sunt disponibile, el va încerca să capteze staţia mobilă.

Aceasta va efectua imediat o cerere de actualizare a locaţiei.



Autentificarea

În plus Oscar mai trebuie să ştie *IMSI*-ul sau *TMSI*-ul cartelei *SIM* pe care vrea să o cloneze.

Când aceste resurse sunt disponibile, el va încerca să capteze stația mobilă.

Aceasta va efectua imediat o cerere de actualizare a locației.

Dacă pretinsa rețea a provocat telefonul mobil prin *TMSI*, *IMSI*-ul poate fi aflat ușor prin comanda *IDENTITY REQUEST*, la care telefonul trebuie să răspundă imediat.

Autentificarea

Pentru actualizarea locației, intrusul va iniția un proces de autentificare.

Imediat după ce obține o perche provocare - răspuns, el lansează o nouă procedură de autentificare.

Autentificarea

Pentru actualizarea locației, intrusul va iniția un proces de autentificare.

Imediat după ce obține o perche provocare - răspuns, el lansează o nouă procedură de autentificare.

Stația mobilă trebuie să răspundă la fiecare provocare pe care o trimite rețeaua *GSM*.

Autentificarea

Pentru actualizarea locației, intrusul va iniția un proces de autentificare.

Imediat după ce obține o perche provocare - răspuns, el lansează o nouă procedură de autentificare.

Stația mobilă trebuie să răspundă la fiecare provocare pe care o trimite rețeaua *GSM*.

Procedeul continuă până când *Oscar* va obține numărul de perechi necesare pentru a efectua clonarea.

Autentificarea

Dacă Oscar obține cheia K_i (prin clonarea cartelei) și interceptează valoarea $RAND$ prin wireless în timpul stabilirii apelului, el poate calcula cheia K_c (dacă este folosit algoritmul COMP128 sau un alt algoritm cunoscut) și poate asculta con vorbirea în timp real.



Autentificarea

Dacă Oscar obține cheia K_i (prin clonarea cartelei) și interceptează valoarea $RAND$ prin wireless în timpul stabilirii apelului, el poate calcula cheia K_c (dacă este folosit algoritmul COMP128 sau un alt algoritm cunoscut) și poate asculta con vorbirea în timp real.

După apariția primelor atacuri, GSM a creat alte două noi versiuni pentru COMP128.

Dacă furnizorii foloseau în continuare COMP128 – 1 limitând doar numărul de provocări, după apariția unui atac ce necesită doar 8 provocări, această restricție nu mai este eficientă: o cartelă SIM trebuie să poată răspunde la mai mult de 8 provocări pe parcursul unei zile.



Autentificarea

Ultima versiune a lui *COMP128* – a patra – se bazează pe un algoritm ce folosește standardul *AES*.

Ea este implementată în rețelele *UMTS*, ceea ce presupune emiterea de noi cartele pentru abonații rețelei, o reactualizare a soft-ului *HLR* și securitate contra clonării cartelei *SIM*.



Autentificarea

Ultima versiune a lui *COMP128* – a patra – se bazează pe un algoritm ce folosește standardul *AES*.

Ea este implementată în rețelele *UMTS*, ceea ce presupune emiterea de noi cartele pentru abonații rețelei, o reactualizare a soft-ului *HLR* și securitate contra clonării cartelei *SIM*.

Și noul algoritm este pasibil de atacuri.

Căutarea în tabele mari este folosită frecvent. Aplicată pe dispozitive limitate (smartcard-uri) ele sunt sensibile la atacuri side channel.



Autentificarea

Ultima versiune a lui *COMP128* – a patra – se bazează pe un algoritm ce folosește standardul *AES*.

Ea este implementată în rețelele *UMTS*, ceea ce presupune emiterea de noi cartele pentru abonații rețelei, o reactualizare a soft-ului *HLR* și securitate contra clonării cartelei *SIM*.

Și noul algoritm este pasibil de atacuri.

Căutarea în tabele mari este folosită frecvent. Aplicată pe dispozitive limitate (smartcard-uri) ele sunt sensibile la atacuri side channel.

Pentru a rezista, se înlocuiește căutarea într-o tabelă cu o serie de căutări în locații complet aleatoare folosind un tabel auxiliar, ceea ce nu permite nici o scurgere de informații.



Autentificarea

Ultima versiune a lui *COMP128* – a patra – se bazează pe un algoritm ce folosește standardul *AES*.

Ea este implementată în rețelele *UMTS*, ceea ce presupune emiterea de noi cartele pentru abonații rețelei, o reactualizare a soft-ului *HLR* și securitate contra clonării cartelei *SIM*.

Și noul algoritm este pasibil de atacuri.

Căutarea în tabele mari este folosită frecvent. Aplicată pe dispozitive limitate (smartcard-uri) ele sunt sensibile la atacuri side channel.

Pentru a rezista, se înlocuiește căutarea într-o tabelă cu o serie de căutări în locații complet aleatoare folosind un tabel auxiliar, ceea ce nu permite nici o scurgere de informații.

Metoda poate fi implementată cu succes în dispozitivele cu memorie limitată cum sunt telefoanele mobile, pentru că folosește foarte puțină memorie *RAM*.

Confidențialitate

Protejarea informației schimilate în timpul conversației și a informațiilor de control asociate cu stabilirea unui apel.

Confidențialitate

Protejarea informației schimilate în timpul conversației și a informațiilor de control asociate cu stabilirea unui apel.

Contextul de securitate este cheia de sesiune K_c pe 64 biți, rezultată în urmă aplicării lui COMP128.

Ea oferă confidențialitate pe interfața wireless *BTS - ME* (securizează comunicarea între echipamentul mobil și stația de bază).

GSM folosește tehnica de diviziune în timp pentru a face posibilă folosirea aceluiași canal radio pentru 8 utilizatori simultan.

GSM folosește tehnica de diviziune în timp pentru a face posibilă folosirea aceluiași canal radio pentru 8 utilizatori simultan.

Fiecare utilizator va transmite și primi informații numai pe durata uneia din cele 8 sloturi de timp disponibile în fiecare frame.

GSM folosește tehnica de diviziune în timp pentru a face posibilă folosirea aceluiași canal radio pentru 8 utilizatori simultan.

Fiecare utilizator va transmite și primi informații numai pe durata uneia din cele 8 sloturi de timp disponibile în fiecare frame.

Fiecare frame durează 4.6 milisecunde și este identificat printr-un număr asociat.



GSM folosește tehnica de diviziune în timp pentru a face posibilă folosirea aceluiași canal radio pentru 8 utilizatori simultan.

Fiecare utilizator va transmite și primi informații numai pe durata uneia din cele 8 sloturi de timp disponibile în fiecare frame.

Fiecare frame durează 4.6 milisecunde și este identificat prin un număr asociat.

O conversație GSM folosește 2 frame-uri: unul mergând de la stația de bază spre stația mobilă și celălalt parcurgând aceeași cale în sens invers.



GSM folosește tehnica de diviziune în timp pentru a face posibilă folosirea aceluiași canal radio pentru 8 utilizatori simultan.

Fiecare utilizator va transmite și primi informații numai pe durata uneia din cele 8 sloturi de timp disponibile în fiecare frame.

Fiecare frame durează 4.6 milisecunde și este identificat prin un număr asociat.

O conversație GSM folosește 2 frame-uri: unul mergând de la stația de bază spre stația mobilă și celălalt parcurgând aceeași cale în sens invers.

Fiecare din aceste frame-uri conține 114 biți de informație.



GSM folosește tehnica de diviziune în timp pentru a face posibilă folosirea aceluiași canal radio pentru 8 utilizatori simultan.

Fiecare utilizator va transmite și primi informații numai pe durata uneia din cele 8 sloturi de timp disponibile în fiecare frame.

Fiecare frame durează 4.6 milisecunde și este identificat prin un număr asociat.

O conversație GSM folosește 2 frame-uri: unul mergând de la stația de bază spre stația mobilă și celălalt parcurgând aceeași cale în sens invers.

Fiecare din aceste frame-uri conține 114 biți de informație. Deci la fiecare 4.6 milisecunde, stația mobilă primește 114 biți de informație de la stația de bază și trimită alți 114 biți de informație către aceasta.

Acești 228 biți au nevoie de protecție împotriva interceptării.

Algoritmul folosit pentru criptarea pachetelor de informații transmise wireless este A5.

A5 este un sistem de criptare fluid care generează o cheie unică pentru fiecare pachet de date folosind la intrare cheia de sesiune K_c pe 64 biți și numărul de secvență asociat frame-ului respectiv.

Algoritmul folosit pentru criptarea pachetelor de informații transmise wireless este *A5*.

A5 este un sistem de criptare fluid care generează o cheie unică pentru fiecare pachet de date folosind la intrare cheia de sesiune K_c pe 64 biți și numărul de secvență asociat frame-ului respectiv. Deoarece numărul de secvență al unui frame este ușor de aflat, confidențialitatea datelor transmise se bazează numai pe menținerea secretului cheii de sesiune K_c .

După ce a fost obținută cheia de sesiune, criptarea va începe imediat ce rețeaua *GSM* trimite echipamentului mobil o cerere de criptare.

Algoritmul folosit pentru criptarea pachetelor de informații transmise wireless este *A5*.

A5 este un sistem de criptare fluid care generează o cheie unică pentru fiecare pachet de date folosind la intrare cheia de sesiune K_c pe 64 biți și numărul de secvență asociat frame-ului respectiv. Deoarece numărul de secvență al unui frame este ușor de aflat, confidențialitatea datelor transmise se bazează numai pe menținerea secretului cheii de sesiune K_c .

După ce a fost obținută cheia de sesiune, criptarea va începe imediat ce rețeaua *GSM* trimite echipamentului mobil o cerere de criptare.

Spre deosebire de *A3* și *A8* care sunt implementați în *SIM*, algoritmul *A5* se află implementat hardware – direct în echipamentul mobil.

Există trei versiuni dezvoltate pentru A5:

Există trei versiuni dezvoltate pentru A5:

- 1 **A5/1**: folosită în țările membre ale CEPT (48 țări din Europa) și în Statele Unite). A fost lansată în 1987 și oferă cel mai înalt nivel de criptare wireless.
Deși folosește 64 biți, practic cheia nu depășește 54 biți, ultimii 10 biți fiind setați pe zero.



Există trei versiuni dezvoltate pentru A5:

- 1 **A5/1:** folosită în țările membre ale CEPT (48 țări din Europa) și în Statele Unite). A fost lansată în 1987 și oferă cel mai înalt nivel de criptare wireless.
Deși folosește 64 biți, practic cheia nu depășește 54 biți, ultimii 10 biți fiind setați pe zero.
- 2 **A5/2:** este mai slab decât A5/1 și este folosit preponderent în Asia.



Există trei versiuni dezvoltate pentru A5:

- 1 **A5/1:** folosită în țările membre ale CEPT (48 țări din Europa) și în Statele Unite). A fost lansată în 1987 și oferă cel mai înalt nivel de criptare wireless.
Deși folosește 64 biți, practic cheia nu depășește 54 biți, ultimii 10 biți fiind setați pe zero.
- 2 **A5/2:** este mai slab decât A5/1 și este folosit preponderent în Asia.
Schița celor doi algoritmi a fost ținută secret, dar a fost descoperită prin inginerie inversă în 1999 și este disponibilă pe Internet.

3 *A5/3* (din 2002). Ca securitate este mai puternic decât primele versiuni, dar este folosit numai în rețelele *UMTS* pentru generația a treia (3G).

Schema lui *A5/3* a fost făcută publică, construcția lui fiind bazată pe sistemul de criptare bloc KASUMI.



3 A5/3 (din 2002). Ca securitate este mai puternic decât primele versiuni, dar este folosit numai în rețelele UMTS pentru generația a treia (3G).

Schema lui A5/3 a fost făcută publică, construcția lui fiind bazată pe sistemul de criptare bloc KASUMI.

Înafara acestora mai există o versiune ieftină – și deci mai puțin complexă – numită A5/0, care nu presupune nici o criptare.

A5/1

Acceptă la intrare o cheie de sesiune K_c pe 64 biți și numărul de frame f pe 22 de biți care este public (fiecare frame are asociat un număr de frame, frame-urile consecutive având asociate numere consecutive).

A5/1

Acceptă la intrare o cheie de sesiune K_c pe 64 biți și numărul de frame f pe 22 de biți care este public (fiecare frame are asociat un număr de frame, frame-urile consecutive având asociate numere consecutive).

În fiecare frame, A5/1 este inițializat cu cheia de sesiune și cu numărul de frame.



Algoritmul A5/1

A5/1

Acceptă la intrare o cheie de sesiune K_c pe 64 biți și numărul de frame f pe 22 de biți care este public (fiecare frame are asociat un număr de frame, frame-urile consecutive având asociate numere consecutive).

În fiecare frame, A5/1 este inițializat cu cheia de sesiune și cu numărul de frame.

Cheia fluidă obținută la ieșire ocupă 228 biți și este împărțită în două jumătăți: primii 114 biți folosesc pentru criptarea datelor transmise de la rețea către telefonul mobil, iar restul – pentru criptarea datelor de la telefonul mobil către rețea.



Algoritmul A5/1

A5/1

Acceptă la intrare o cheie de sesiune K_c pe 64 biți și numărul de frame f pe 22 de biți care este public (fiecare frame are asociat un număr de frame, frame-urile consecutive având asociate numere consecutive).

În fiecare frame, A5/1 este inițializat cu cheia de sesiune și cu numărul de frame.

Cheia fluidă obținută la ieșire ocupă 228 biți și este împărțită în două jumătăți: primii 114 biți folosesc pentru criptarea datelor transmise de la rețea către telefonul mobil, iar restul – pentru criptarea datelor de la telefonul mobil către rețea.

Criptarea este realizată prin aplicarea operației XOR asupra datelor transmise și a jumătății corespunzătoare din cheia fluidă generată.

A5/1 are o stare internă pe 64 biți și este construit din trei circuite LFSR de lungime 19, 22 și respectiv 23 biți fiecare, notate $R1$, $R2$ și $R3$.

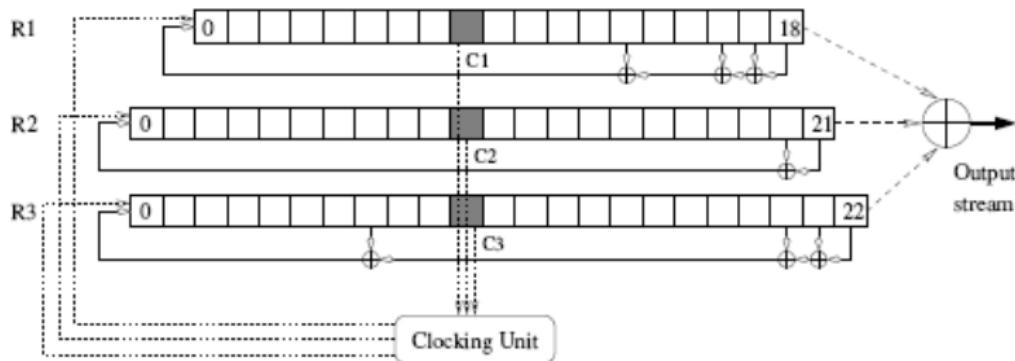


Algoritmul A5/1

A5/1 are o stare internă pe 64 biți și este construit din trei circuite LFSR de lungime 19, 22 și respectiv 23 biți fiecare, notate $R1$, $R2$ și $R3$.

La fiecare tact (*clocking*) fiecare registru calculează funcția de întoarcere, după care este deplasat la dreapta cu o poziție (cel mai din dreapta bit devine bit de ieșire) iar feedback-ul calculat este stocat în cea mai din stânga poziție din registru.

Algoritmul A5/1



Structura internă a algoritmului A5/1

Algoritmul A5/1

A5/1 este inițializat cu K_c și f în trei pași ($K_c[i]$ reprezintă al i -lea bit din K_c , iar $f[i]$ – al i -lea bit din f):

A5/1 este inițializat cu K_c și f în trei pași ($K_c[i]$ reprezintă al i -lea bit din K_c , iar $f[i]$ – al i -lea bit din f):

- 1** Setează $R1 = R2 = R3 = 0$.

A5/1 este inițializat cu K_c și f în trei pași ($K_c[i]$ reprezintă al i -lea bit din K_c , iar $f[i]$ – al i -lea bit din f):

- 1 Setează $R1 = R2 = R3 = 0$.
 - 2 For $i = 0$ to 63 do
 - 1 Aplică un tact pentru toți registrii
 - 2 $R1[0] \leftarrow R1[0] \oplus K_c[i]$; $R2[0] \leftarrow R2[0] \oplus K_c[i]$;
 $R3[0] \leftarrow R3[0] \oplus K_c[i]$.



Algoritmul A5/1

A5/1 este inițializat cu K_c și f în trei pași ($K_c[i]$ reprezintă al i -lea bit din K_c , iar $f[i]$ – al i -lea bit din f):

- 1 Setează $R1 = R2 = R3 = 0$.
- 2 For $i = 0$ to 63 do
 - 1 Aplică un tact pentru toți regiștrii
 - 2 $R1[0] \leftarrow R1[0] \oplus K_c[i]; R2[0] \leftarrow R2[0] \oplus K_c[i]; R3[0] \leftarrow R3[0] \oplus K_c[i].$
- 3 For $i = 0$ to 21 do
 - 1 Aplică un tact pentru toți regiștrii
 - 2 $R1[0] \leftarrow R1[0] \oplus f[i]; R2[0] \leftarrow R2[0] \oplus f[i]; R3[0] \leftarrow R3[0] \oplus f[i].$

Generarea cheii fluide se efectuează în 328 tacti, la fiecare tact producându-se un bit de ieșire.

La fiecare tact, ieșirea este un *XOR* între cei mai din dreapta biți ai celor trei registri.



Algoritmul A5/1

Generarea cheii fluide se efectuează în 328 tacti, la fiecare tact producându-se un bit de ieșire.

La fiecare tact, ieșirea este un *XOR* între cei mai din dreapta biți ai celor trei registri.

Cheia fluidă de 228 biți este generată astfel:



Generarea cheii fluide se efectuează în 328 tacti, la fiecare tact producându-se un bit de ieșire.

La fiecare tact, ieșirea este un *XOR* între cei mai din dreapta biți ai celor trei registri.

Cheia fluidă de 228 biți este generată astfel:

- 1 Execută inițializarea cu cheia K_c și numărul de frame f .



Algoritmul A5/1

Generarea cheii fluide se efectuează în 328 tacți, la fiecare tact producându-se un bit de ieșire.

La fiecare tact, ieșirea este un *XOR* între cei mai din dreapta biți ai celor trei registri.

Cheia fluidă de 228 biți este generată astfel:

- 1 Execută inițializarea cu cheia K_c și numărul de frame f .
- 2 Execută A5/1 pentru 100 tacți, fără a păstra ieșirea.



Algoritmul A5/1

Generarea cheii fluide se efectuează în 328 tacți, la fiecare tact producându-se un bit de ieșire.

La fiecare tact, ieșirea este un *XOR* între cei mai din dreapta biți ai celor trei registri.

Cheia fluidă de 228 biți este generată astfel:

- 1 Execută inițializarea cu cheia K_c și numărul de frame f .
- 2 Execută A5/1 pentru 100 tacți, fără a păstra ieșirea.
- 3 Execută A5/1 pentru 228 tacți, biții rezultați formând cheia fluidă.

A5/2

Se folosesc patru registri (de lungimi 19, 22, 23 și 17 biți), iar funcțiile de întoarcere ale primilor trei sunt identice ca pentru A5/1.

Algoritmul A5/2

A5/2

Se folosesc patru registri (de lungimi 19, 22, 23 și 17 biți), iar funcțiile de întoarcere ale primilor trei sunt identice ca pentru A5/1.

Algoritmul acceptă la intrare aceeași parametri ca și A5/1: o cheie K_c pe 64 biți și o valoare publică f pe 22 biți, derivată din numărul de frame (cunoscut public).



Algoritmul A5/2

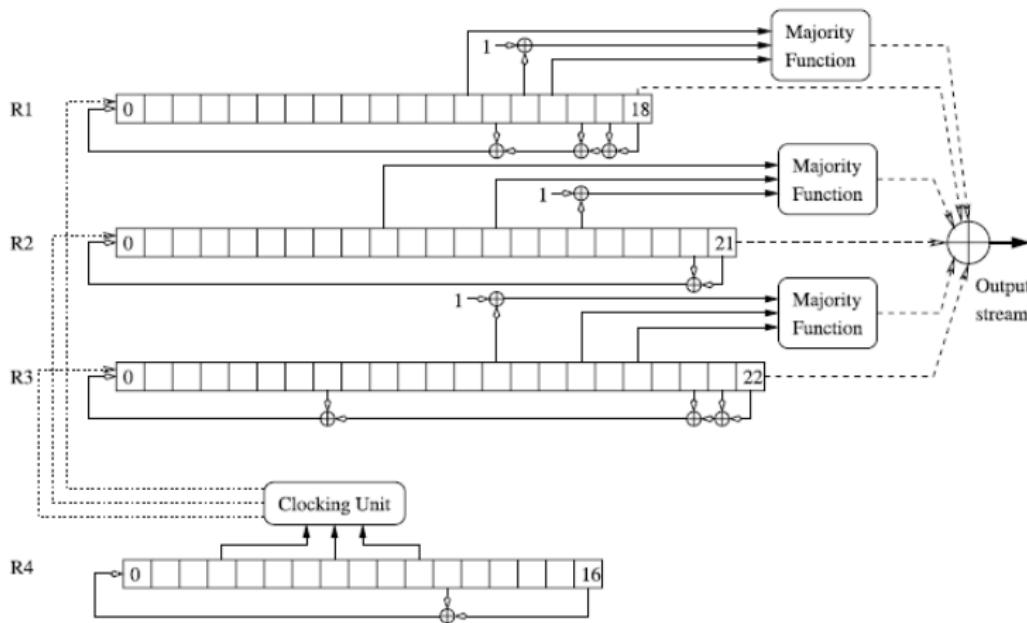
Valoarea lui f este obținută din numărul asociat frame-ului TDMA:

21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0



Obținerea valorii f

unde $T1$ este câtul împărțirii numărului de frame la $51 \times 26 = 1326$, $T2$ este restul împărțirii numărului de frame la 26 și $T3$ este restul împărțirii numărului de frame la 51.



Structura internă a algoritmului A5/2

Algoritmul A5/2

A5/2 este initializat cu K_c și f în patru pași:

A5/2 este inițializat cu K_c și f în patru pași:

- 1** Setează $R1 = R2 = R3 = R4 = 0$.

Algoritmul A5/2

A5/2 este inițializat cu K_c și f în patru pași:

- 1 Setează $R1 = R2 = R3 = R4 = 0$.
- 2 For $i = 0$ to 63 do

A5/2 este inițializat cu K_c și f în patru pași:

- 1 Setează $R1 = R2 = R3 = R4 = 0$.
 - 2 For $i = 0$ to 63 do
 - 1 Aplică un tact pentru cei patru registri.

A5/2 este initializat cu K_c și f în patru pași:

- 1** Setează $R1 = R2 = R3 = R4 = 0$.
 - 2** For $i = 0$ to 63 do
 - 1** Aplică un tact pentru cei patru registri.
 - 2** $R1[0] \leftarrow R1[0] \oplus K_c[i]$; $R2[0] \leftarrow R2[0] \oplus K_c[i]$;
 $R3[0] \leftarrow R3[0] \oplus K_c[i]$; $R4[0] \leftarrow R4[0] \oplus K_c[i]$;



Algoritmul A5/2

A5/2 este inițializat cu K_c și f în patru pași:

- 1** Setează $R1 = R2 = R3 = R4 = 0$.
- 2** For $i = 0$ to 63 do
 - 1** Aplică un tact pentru cei patru registri.
 - 2** $R1[0] \leftarrow R1[0] \oplus K_c[i]; R2[0] \leftarrow R2[0] \oplus K_c[i]; R3[0] \leftarrow R3[0] \oplus K_c[i]; R4[0] \leftarrow R4[0] \oplus K_c[i]$.
- 3** For $i = 0$ to 21 do
 - 1** Aplică un tact pentru primii trei registri.



Algoritmul A5/2

A5/2 este inițializat cu K_c și f în patru pași:

- 1** Setează $R1 = R2 = R3 = R4 = 0$.
- 2** For $i = 0$ to 63 do
 - 1** Aplică un tact pentru cei patru registri.
 - 2** $R1[0] \leftarrow R1[0] \oplus K_c[i]$; $R2[0] \leftarrow R2[0] \oplus K_c[i]$;
 $R3[0] \leftarrow R3[0] \oplus K_c[i]$; $R4[0] \leftarrow R4[0] \oplus K_c[i]$.
- 3** For $i = 0$ to 21 do
 - 1** Aplică un tact pentru primii trei registri.
 - 2** $R1[0] \leftarrow R1[0] \oplus f[i]$; $R2[0] \leftarrow R2[0] \oplus f[i]$;
 $R3[0] \leftarrow R3[0] \oplus f[i]$; $R4[0] \leftarrow R4[0] \oplus f[i]$.



Algoritmul A5/2

A5/2 este inițializat cu K_c și f în patru pași:

- 1** Setează $R1 = R2 = R3 = R4 = 0$.
- 2** For $i = 0$ to 63 do
 - 1** Aplică un tact pentru cei patru registri.
 - 2** $R1[0] \leftarrow R1[0] \oplus K_c[i]$; $R2[0] \leftarrow R2[0] \oplus K_c[i]$;
 $R3[0] \leftarrow R3[0] \oplus K_c[i]$; $R4[0] \leftarrow R4[0] \oplus K_c[i]$.
- 3** For $i = 0$ to 21 do
 - 1** Aplică un tact pentru primii trei registri.
 - 2** $R1[0] \leftarrow R1[0] \oplus f[i]$; $R2[0] \leftarrow R2[0] \oplus f[i]$;
 $R3[0] \leftarrow R3[0] \oplus f[i]$; $R4[0] \leftarrow R4[0] \oplus f[i]$.
- 4** Setează biții
 $R1[15] \leftarrow 1$, $R2[16] \leftarrow 1$, $R3[18] \leftarrow 1$, $R4[10] \leftarrow 1$.

Algoritmul A5/2

Procesul de generare a cheii poate fi sumarizat astfel:

- 1 Execută inițializarea cu cheia K_c și valoarea f .

Algoritmul A5/2

Procesul de generare a cheii poate fi sumarizat astfel:

- 1 Execută inițializarea cu cheia K_c și valoarea f .
- 2 Execută A5/2 pentru 99 tacti, ignorând ieșirea.

Algoritmul A5/2

Procesul de generare a cheii poate fi sumarizat astfel:

- 1 Execută inițializarea cu cheia K_c și valoarea f .
- 2 Execută A5/2 pentru 99 tacți, ignorând ieșirea.
- 3 Execută A5/2 pentru 228 tacți, iar biții rezultați formează cheia fluidă.

Procesul de generare a cheii poate fi summarizat astfel:

- 1 Execută inițializarea cu cheia K_c și valoarea f .
 - 2 Execută A5/2 pentru 99 tacți, ignorând ieșirea.
 - 3 Execută A5/2 pentru 228 tacți, iar biții rezultați formează cheia fluidă.

Procedura de criptare este identică cu cea a algoritmului A5/1.

Probleme legate de confidențialitatea GSM

- Partea de criptare este o caracteristică optională a rețelei.
Unele telefoane mobile (seria *Siemens S*) afișează pe ecran un simbol de tipul *!* dacă opțiunea de criptare este dezactivată.



Probleme legate de confidențialitatea GSM

- Partea de criptare este o caracteristică opțională a rețelei.
Unele telefoane mobile (seria *Siemens S*) afișează pe ecran un simbol de tipul ***!*** dacă opțiunea de criptare este dezactivată.
- Criptarea este utilizată numai pentru securizarea interfeței dintre stația mobilă și *BTS*.
Algoritmul folosit pentru criptarea legăturii stație mobilă - *BTS* nu este sigur, datorită puterii tot mai mare a hardware-lui.
Folosind un simplu atac prin forță brută, securitatea algoritmului poate fi compromisă în câteva ore.



Probleme legate de confidențialitatea GSM

- Partea de criptare este o caracteristică opțională a rețelei.
Unele telefoane mobile (seria *Siemens S*) afișează pe ecran un simbol de tipul ***!*** dacă opțiunea de criptare este dezactivată.
- Criptarea este utilizată numai pentru securizarea interfeței dintre stația mobilă și *BTS*.
Algoritmul folosit pentru criptarea legăturii stație mobilă - *BTS* nu este sigur, datorită puterii tot mai mare a hardware-lui.
Folosind un simplu atac prin forță brută, securitatea algoritmului poate fi compromisă în câteva ore.
- Numai rețeaua GSM are dreptul să verifice identitatea abonatului; stația mobilă nu poate verifica autenticitatea rețelei.



Algoritmul A5/2

- *GSM nu asigură protecția integrității pentru informațiile transmise.*

Absența unui mecanism care să o asigure înseamnă că la recepție nu se poate verifica dacă mesajul primit a fost modificat sau nu.

Se lasă astfel cale liberă pentru numeroase atacuri de tipul man-in-the-middle.



Algoritmul A5/2

- *GSM nu asigură protecția integrității pentru informațiile transmise.*
Absența unui mecanism care să o asigure înseamnă că la recepție nu se poate verifica dacă mesajul primit a fost modificat sau nu.
Se lasă astfel cale liberă pentru numeroase atacuri de tipul man-in-the-middle.
- *Algoritmii de criptare GSM nu sunt publicați în standardul GSM, deci nu sunt disponibili pentru analiza comunității de securitate.*

Falii ale protocolului *GSM*

- 1 Autentificarea poate fi executată numai între mobil și rețea, la începutul apelului, fiind numai la dispoziția rețelei.

Falii ale protocolului GSM

- 1 Autentificarea poate fi executată numai între mobil și rețea, la începutul apelului, fiind numai la dispoziția rețelei.
Dacă nu este efectuată nici o autentificare, K_c rămâne cel din conversația anterioară; în acest caz, rețeaua "autentifică" telefonul prin faptul că folosește același K_c pentru criptare.

Falii ale protocolului GSM

- 1 Autentificarea poate fi executată numai între mobil și rețea, la începutul apelului, fiind numai la dispoziția rețelei.
Dacă nu este efectuată nici o autentificare, K_c rămâne cel din conversația anterioară; în acest caz, rețeaua "autentifică" telefonul prin faptul că folosește același K_c pentru criptare.
- 2 Rețeaua alege algoritmul de criptare.

Falii ale protocolului GSM

- 1 Autentificarea poate fi executată numai între mobil și rețea, la începutul apelului, fiind numai la dispoziția rețelei.
Dacă nu este efectuată nici o autentificare, K_c rămâne cel din conversația anterioară; în acest caz, rețeaua "autentifică" telefonul prin faptul că folosește același K_c pentru criptare.
- 2 Rețeaua alege algoritmul de criptare.
- 3 Faptul că doar telefonul se autentifică la rețea permite existența stațiilor de bază false.



Falii ale protocolului GSM

- 1 Autentificarea poate fi executată numai între mobil și rețea, la începutul apelului, fiind numai la dispoziția rețelei.
Dacă nu este efectuată nici o autentificare, K_c rămâne cel din conversația anterioară; în acest caz, rețeaua "autentifică" telefonul prin faptul că folosește același K_c pentru criptare.
- 2 Rețeaua alege algoritmul de criptare.
- 3 Faptul că doar telefonul se autentifică la rețea permite existența stațiilor de bază false.
- 4 Protocolul de stabilire a cheii este independent de algoritmul folosit: K_c depinde numai de $RAND$ (ales de rețea), indiferent de algoritmul de criptare A5.

Falii ale protocolului GSM

- 1 Autentificarea poate fi executată numai între mobil și rețea, la începutul apelului, fiind numai la dispoziția rețelei.
Dacă nu este efectuată nici o autentificare, K_c rămâne cel din conversația anterioară; în acest caz, rețeaua "autentifică" telefonul prin faptul că folosește același K_c pentru criptare.
- 2 Rețeaua alege algoritmul de criptare.
- 3 Faptul că doar telefonul se autentifică la rețea permite existența stațiilor de bază false.
- 4 Protocolul de stabilire a cheii este independent de algoritmul folosit: K_c depinde numai de $RAND$ (ales de rețea), indiferent de algoritmul de criptare A5.
- 5 Aceeași valoare $RAND$ poate fi folosită ori de câte ori dorește rețeaua.

Recuperarea cheii K_c dintr-o conversație anterioară

Această cheie poate fi validă pentru con vorbiri ulterioare dacă rețeaua alege să nu efectueze protocolul de stabilire a unei noi chei.

Recuperarea cheii K_c dintr-o conversație anterioară

Această cheie poate fi validă pentru con vorbiri ulterioare dacă rețeaua alege să nu efectueze protocolul de stabilire a unei noi chei.

Calea cea mai simplă de a decripta conversații înregistrate este când *Oscar* are acces la cardul *SIM* al utilizatorului.

Atunci el îl poate alimenta cu *RAND*-ul folosit anterior în conversație.

Recuperarea cheii K_c dintr-o conversație anterioară

Această cheie poate fi validă pentru con vorbiri ulterioare dacă rețeaua alege să nu efectueze protocolul de stabilire a unei noi chei.

Calea cea mai simplă de a decripta conversații înregistrate este când *Oscar* are acces la cardul *SIM* al utilizatorului.

Atunci el îl poate alimenta cu *RAND*-ul folosit anterior în conversație.

SIM-ul calculează și întoarce spre intrus valoarea lui K_c (atacul este posibil pentru că *GSM* permite refolosirea valorii *RAND*).

Recuperarea cheii K_c dintr-o conversație anterioară

Această cheie poate fi validă pentru con vorbiri ulterioare dacă rețeaua alege să nu efectueze protocolul de stabilire a unei noi chei.

Calea cea mai simplă de a decripta conversații înregistrate este când *Oscar* are acces la cardul *SIM* al utilizatorului.

Atunci el îl poate alimenta cu *RAND*-ul folosit anterior în conversație.

SIM-ul calculează și întoarce spre intrus valoarea lui K_c (atacul este posibil pentru că *GSM* permite refolosirea valorii *RAND*).

Singura problemă este obținerea accesului fizic la cardul *SIM* al utilizatorului.

Atac de tipul man-in-the-middle

Oscar poate intercepta conversațiile în timp real prin lansarea unui atac man-in-the-middle.

Pentru aceasta, el simulează o stație de bază falsă pentru a comunica cu telefonul țintă, pretinzând rețelei că este stația mobilă.

Atac de tipul man-in-the-middle

Oscar poate intercepta conversațiile în timp real prin lansarea unui atac man-in-the-middle.

Pentru aceasta, el simulează o stație de bază falsă pentru a comunica cu telefonul țintă, pretinzând rețelei că este stația mobilă.

- 1 Când rețeaua inițiază protocolul de autentificare, ea trimitе lui *Oscar* o cerere de autentificare, pe care acesta – sub chipul stației de bază – o trimitе mai departe utilizatorului.

Atac de tipul man-in-the-middle

Oscar poate intercepta conversațiile în timp real prin lansarea unui atac man-in-the-middle.

Pentru aceasta, el simulează o stație de bază falsă pentru a comunica cu telefonul țintă, pretinzând rețelei că este stația mobilă.

- 1 Când rețeaua inițiază protocolul de autentificare, ea trimitе lui *Oscar* o cerere de autentificare, pe care acesta – sub chipul stației de bază – o trimite mai departe utilizatorului.
- 2 Utilizatorul calculează *SRES* pe care îl returnează lui *Oscar*, care îl va reține temporar, fără a-l retrimitе rețelei.

3 Oscar cere telefonului să înceapă criptarea folosind A5/2.

- 3 Oscar cere telefonului să înceapă criptarea folosind A5/2. Telefonul începe criptarea folosind A5/2 și trimite o certificare (acknowledgment numit *CIPHMODCOM - Cipher Mode Complete*, care confirmă că a început criptarea) criptată.

- 3 Oscar cere telefonului să înceapă criptarea folosind A5/2. Telefonul începe criptarea folosind A5/2 și trimite o certificare (acknowledgment numit *CIPHMODCOM - Cipher Mode Complete*, care confirmă că a început criptarea) criptată.
- 4 Oscar folosește atacul cu text criptat pentru a găsi K_c (în mai puțin de o secundă).

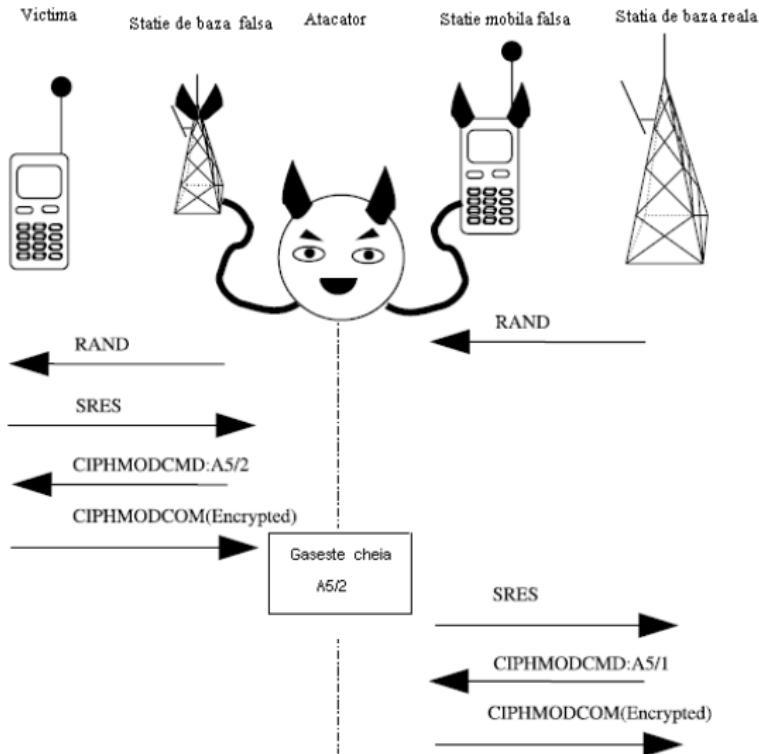
- 3 Oscar cere telefonului să înceapă criptarea folosind A5/2. Telefonul începe criptarea folosind A5/2 și trimite o certificare (acknowledgment numit *CIPHMODCOM - Cipher Mode Complete*, care confirmă că a început criptarea) criptată.
- 4 Oscar folosește atacul cu text criptat pentru a găsi K_c (în mai puțin de o secundă).
- 5 Abia acum Oscar trimite valoarea SRES spre rețeaua reală.

- 3 Oscar cere telefonului să înceapă criptarea folosind A5/2. Telefonul începe criptarea folosind A5/2 și trimite o certificare (acknowledgment numit *CIPHMODCOM - Cipher Mode Complete*, care confirmă că a început criptarea) criptată.
- 4 Oscar folosește atacul cu text criptat pentru a găsi K_c (în mai puțin de o secundă).
- 5 Abia acum Oscar trimite valoarea SRES spre rețeaua reală.
- 6 Acum Oscar este "autentificat" în rețea, care îi cere să înceapă criptarea folosind A5/1.

- 3 Oscar cere telefonului să înceapă criptarea folosind A5/2. Telefonul începe criptarea folosind A5/2 și trimite o certificare (acknowledgment numit *CIPHMODCOM - Cipher Mode Complete*, care confirmă că a început criptarea) criptată.
- 4 Oscar folosește atacul cu text criptat pentru a găsi K_c (în mai puțin de o secundă).
- 5 Abia acum Oscar trimite valoarea SRES spre rețeaua reală.
- 6 Acum Oscar este "autentificat" în rețea, care îi cere să înceapă criptarea folosind A5/1.
Intrusul cunoaște deja cheia K_c și poate trimite răspunsul criptat cu A5/1.

- 3 Oscar cere telefonului să înceapă criptarea folosind A5/2. Telefonul începe criptarea folosind A5/2 și trimite o certificare (acknowledgment numit *CIPHMODCOM - Cipher Mode Complete*, care confirmă că a început criptarea) criptată.
- 4 Oscar folosește atacul cu text criptat pentru a găsi K_c (în mai puțin de o secundă).
- 5 Abia acum Oscar trimite valoarea *SRES* spre rețeaua reală.
- 6 Acum Oscar este "autentificat" în rețea, care îi cere să înceapă criptarea folosind A5/1.
Intrusul cunoaște deja cheia K_c și poate trimite răspunsul criptat cu A5/1.

Din acest moment, rețeaua îl vede pe Oscar ca stație mobilă, iar Oscar poate continua conversația, sau poate încredența telefonului.



Atac neoptimizat asupra lui A5/2 (Barkan, Biham, Keller)

Atacul determină valoarea lui $R4$ scriind fiecare bit de ieșire ca un termen pătratic depinzând de $R1$, $R2$ și $R3$.

Atac neoptimizat asupra lui A5/2 (Barkan, Biham, Keller)

Atacul determină valoarea lui $R4$ scriind fiecare bit de ieșire ca un termen pătratic depinzând de $R1$, $R2$ și $R3$.

Având astfel biții de ieșire din patru frame-uri, se construiește un sistem de ecuații pătratice care se rezolvă prin liniarizare, recuperând valorile inițiale pentru $R1$, $R2$ și $R3$.

Atac neoptimizat asupra lui A5/2 (Barkan, Biham, Keller)

Atacul determină valoarea lui $R4$ scriind fiecare bit de ieșire ca un termen pătratic depinzând de $R1$, $R2$ și $R3$.

Având astfel biții de ieșire din patru frame-uri, se construiește un sistem de ecuații pătratice care se rezolvă prin liniarizare, recuperând valorile inițiale pentru $R1$, $R2$ și $R3$.

- 1 Se încearcă toate cele 2^{16} valori pentru $R4$;

Atac neoptimizat asupra lui A5/2 (Barkan, Biham, Keller)

Atacul determină valoarea lui $R4$ scriind fiecare bit de ieșire ca un termen pătratic depinzând de $R1$, $R2$ și $R3$.

Având astfel biții de ieșire din patru frame-uri, se construiește un sistem de ecuații pătratice care se rezolvă prin liniarizare, recuperând valorile inițiale pentru $R1$, $R2$ și $R3$.

- 1 Se încearcă toate cele 2^{16} valori pentru $R4$;
- 2 Pentru fiecare valoare se rezolvă sistemul liniarizat de ecuații care descriu biții de ieșire pentru patru frame-uri.

Atac neoptimizat asupra lui A5/2 (Barkan, Biham, Keller)

Atacul determină valoarea lui $R4$ scriind fiecare bit de ieșire ca un termen pătratic depinzând de $R1$, $R2$ și $R3$.

Având astfel biții de ieșire din patru frame-uri, se construiește un sistem de ecuații pătratice care se rezolvă prin liniarizare, recuperând valorile inițiale pentru $R1$, $R2$ și $R3$.

- 1 Se încearcă toate cele 2^{16} valori pentru $R4$;
- 2 Pentru fiecare valoare se rezolvă sistemul liniarizat de ecuații care descriu biții de ieșire pentru patru frame-uri.
- 3 Soluția obținută plus valoarea lui $R4_1$ (conținutul lui $R4$ după pasul 1 de initializare) este o sugestie pentru starea internă. Majoritatea valorilor lui $R4_1$ pot fi identificate ușor datorită inconsistențelor apărute la eliminarea gaussiană.

Complexitatea timp a atacului: sunt 2^{16} valori aleatoare pentru biții din $R4_1$.

Pentru fiecare valoare se rezolvă un sistem liniar binar de 656 variabile, care presupune $656^3 \approx 2^{28}$ operații XOR.

Deci, complexitatea totală este de aproximativ 2^{44} operații XOR.

Complexitatea timp a atacului: sunt 2^{16} valori aleatoare pentru biții din $R4_1$.

Pentru fiecare valoare se rezolvă un sistem liniar binar de 656 variabile, care presupune $656^3 \approx 2^{28}$ operații XOR.

Deci, complexitatea totală este de aproximativ 2^{44} operații XOR.

Autorii spun că implementarea algoritmului pe un sistem Linux 800 MHz Pentium III găsește starea internă în aproximativ 40 de minute (estimare 2003) și necesită puțină memorie (sistemul liniarizat ocupă aproximativ 54 KB).

Complexitatea timp a atacului: sunt 2^{16} valori aleatoare pentru biții din $R4_1$.

Pentru fiecare valoare se rezolvă un sistem liniar binar de 656 variabile, care presupune $656^3 \approx 2^{28}$ operații XOR.

Deci, complexitatea totală este de aproximativ 2^{44} operații XOR.

Autorii spun că implementarea algoritmului pe un sistem Linux 800 MHz Pentium III găsește starea internă în aproximativ 40 de minute (estimare 2003) și necesită puțină memorie (sistemul liniarizat ocupă aproximativ 54 KB).

Există și o versiune optimizată de atac, care durează mai puțin de o secundă.

Complexitatea timp și spațiu a atacului

Pentru un singur XOR între valorile f ale frame-urilor, timpul necesar pentru precalcoul este comparabil cu timpul necesar pentru efectuarea atacului în varianta neoptimizată: cam 40 minute.

Complexitatea timp și spațiu a atacului

Pentru un singur XOR între valorile f ale frame-urilor, timpul necesar pentru precalcoul este comparabil cu timpul necesar pentru efectuarea atacului în varianta neoptimizată: cam 40 minute.

În faza de atac, trebuie păstrate în memorie matricile (pentru operații rapide).

O singură matrice de sistem are cam $456 \cdot 16$ biți, deci sunt necesari cam 60 MBs pentru reținerea tabelului corespunzător a 2^{16} valori posibile ale lui $R4_1$.

Alți $64 \cdot 456 \cdot 2^{16} \approx 240$ MBs sunt necesari pentru păstrarea matricilor folosite la aflarea stării interne având $R4_1$ și cheia fluidă respectivă.

Complexitatea timp și spațiu a atacului

Pentru un singur XOR între valorile f ale frame-urilor, timpul necesar pentru precalcoul este comparabil cu timpul necesar pentru efectuarea atacului în varianta neoptimizată: cam 40 minute.

În faza de atac, trebuie păstrate în memorie matricile (pentru operații rapide).

O singură matrice de sistem are cam $456 \cdot 16$ biți, deci sunt necesari cam 60 MBs pentru reținerea tabelului corespunzător a 2^{16} valori posibile ale lui $R4_1$.

Alți $64 \cdot 456 \cdot 2^{16} \approx 240$ MBs sunt necesari pentru păstrarea matricilor folosite la aflarea stării interne având $R4_1$ și cheia fluidă respectivă.

În implementarea autorilor, atacul durează mai puțin de o secundă pe un PC.

Sfârșit