11

Securing a Telecom Services Using Quantum Cryptographic Mechanisms

Abdallah Handoura
Ecole Nationale Supérieure des Télécommunications de Bretagne
France

1. Introduction

The architectural model of Internet telephony is rather different than that of the traditional telephone network. The base assumption is that all signaling and media flow over an IP-based network, either the public Internet or various intranets. IP-based networks, present the appearance at the network level that any machine can communicate directly with any other, unless the network specifically restricts them from doing so, through such means as firewalls. This architectural change necessitates a dramatic transformation in the architectural assumptions of traditional telephone networks. In particular, whereas in a traditional network a large amount of administrative control, such as call-volume limitation, implicitly resides at every switch, and thus additional controls can easily be added there without much architectural change, in an Internet environment an administrative point of control must be explicitly engineered into a network, as in a firewall; otherwise end systems can simply bypass any device which attempts to restrict their behavior. In addition, the Internet model transforms the locations at which many services are performed. In general, end systems are assumed to be much more intelligent than in the traditional telephone model; thus, many services which traditionally had to reside within the network can be moved out to the edges, without requiring any explicit support for them within the networks. Other services can be performed by widely separated specialized servers which result in call setup information traversing paths which might be extremely indirect when compared with the physical network's actual topology.

Most of the services and service features of ITU-T Q.1211 can be provided by the IETF's draft signaling standards for Internet Telephony, SIP (the Session Initiation Protocol) (Schulzrinne, 2001) and, for some more specialized features, its Call Control extensions (Johnston, 2002).

However, The growing globalization and the liberalization of the market telecommunications, necessitates a more global infrastructure of IN that satisfies the needs of different subscribed legal implied, especially for multinational services subscribed. A lot of these services are offered on a current system, but are often realized with specialists of the system. The concepts of IN for giving such service is a coherent and stable basis (Schulzrinne, 2001). Some security functions have been introduced already in current

systems, but they define constraints to user groups with the private line means, the proprietor equipment and proprietor algorithms or secrets.

There is a major difference between the realization of today service (limited) and the goals of the introduction of IN, however, the IN offer its services to a public world, open, and especially to offer the services that allow user groups to communicate by the public transmission and to change the equipment without unloading their intimacy and affluence of employment. Therefore, the services of security provides for the current network will not be sufficient for IN, the goal is more long. The defying of the aspect of the new security functions has to make then be publicly usable, economically feasible and insured all its at the same time.

2. Interconnecting SIP and telecom service application

The IN (Intelligent Network) functional architecture identifies several entities such as the service switching function (SSF), the service control functions (SCF), and the call control function (CCF) that model the behavior of the IN network. The CCF represents the normal activities of call and the connection processing in traditional switch, for two clients. The SSF model's additional functionality required for interacting with a service logic program executed by the SCF. The CCF and the SSF are generally co-located in specific switching centers, known as SSP, while the SCFs are hosted on dedicated computers known as SCP. The communication between the different nodes uses the INAP protocol.

Accessing IN services from the IMS network requires that one or more entities in these networks can play the role of an SSP and communicate with existing SCPs via the INAP protocol.

To realize services with SIP it is important that the SIP entity be able to provide features normally provided by the traditional switch, including operating as a SSP for IN features. The SIP entity should also maintain call state and trigger queries to IN-based services, just as traditional switches do.

The most expeditious manner for providing existing IN services in the IP domain is to use the deployed IN infrastructure as much as possible.

The creation of a service by SIP is possible by the three methods INVITE, Bye and options and fields of header SIP Contact, Also, Call-Disposition Replace and Requested-by that are extensions of SIP specified by IETF (Fing, 2001). Some services are already specified by IETF (Gisin, Ribordy, 2001) by using methods and fields of already quoted header: Call, Hold, Transfer of call, Return of call, Third party control.

The key to programming telecom services with SIP is to add logic that guides behavior at each of the elements in the system (Johnston, 2002). In a SIP proxy server, this logic would dictate where the requests are proxies to, how the results are processed, and how the packet should be formatted.

The basic model for providing logic for SIP services is shown in Figure 1. The figure shows a SIP server that has been augmented with service logic, which is a program that is responsible for creating the services. When requests and responses arrive, the server

passes information up to the service logic. The service logic makes some decisions based on this information, and other information it gathers from different resources, and passes instructions back to the server. The server then executes these instructions (Johnston, 2002).

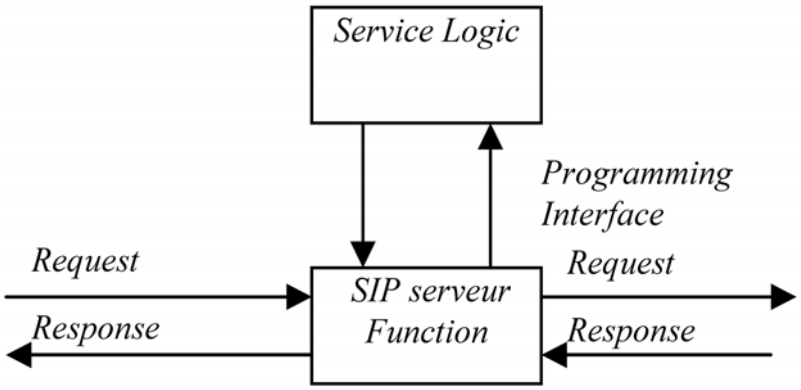


Fig. 1. Model for Programming SIP Services

The separation of the service logic from the server is certainly not new. This idea is inspired by the Intelligent Network (IN) concept (Chapron, 2001). This separation enables rapid development of new services; the idea also exists on the web.

The mechanisms used in these environments can provide valuable insight on how a solution for SIP, IN integration. SIP does not operate the model of call IN directly to access to services IN, the trick is then to bypass the machine of states of the entity SIP with the layer IN such that the acceptance of the call and the routing is executed by the native states and service machine are accessed to layers IN with the model of call IN (El Ouahidi, 2000). The model of service programming with SIP consists therefore in add on SIP server an IN layer, that manages the interconnection with the IN called SIN (SIP Intelligent Network) (Gurbani, 2002). This operation necessitates the definition of a correspondence between the model of call IN and the model of call SIP, it is to tell a correspondence between the state machine of the SIP protocol (SIP defines the header Record_Route that allows to order SIP server to function in mode with the states until the liberation of the call) and the state machine of IN. A call will be processed by the two machines, the state machine SIP processes the initiation of a call and the final reply deliverance, and the IN layer communicate with the intelligent point SCP to provide services during processing of the call (Gurbani, 2002). The figure 2 illustrates the integration SIP-IN.

Similarly to the machine of states IN, one defines the quoted calling and called the entity (O-SIP) and (T-SIP) which are entities corresponding, respectively, to the O-BCSM and T-BCSM of the model IN.

In the basic system of SIP, the SIP proxy with this control of call " intelligent " is defined to interconnect with intelligent network, this intelligence is realized by the use of control calls,

that can synchronize with the model of call IN (BCSM). According to RFC 2543 (SIP) one can define calls of the state machine of the SIP client and SIP server [7,8]. The 11 PICs of O_BCSM come into play when a call request (SIP INVITE message) arrives from an upstream SIP client to an originating SIN-enabled SIP entity running the IN call model. This entity will create an O_BCSM object and initialize it in the O_NULL PIC. The next seven IN PICs -- O_NULL, AUTH_ORIG_ATT, COLLECT_INFO, ANALYZE_INFO, SELECT_ROUTE, AUTH_ CALL_SETUP, CALL_SENT, O_Alerting and O_Active, can all be mapped to the SIP "Calling" state. Figure 3 below provides a visual mapping from the SIP protocol state machine to the originating half of the IN call model. Note that control of the call shuttles between the SIP protocol machine and the IN O_BCSM call model while it is being serviced.

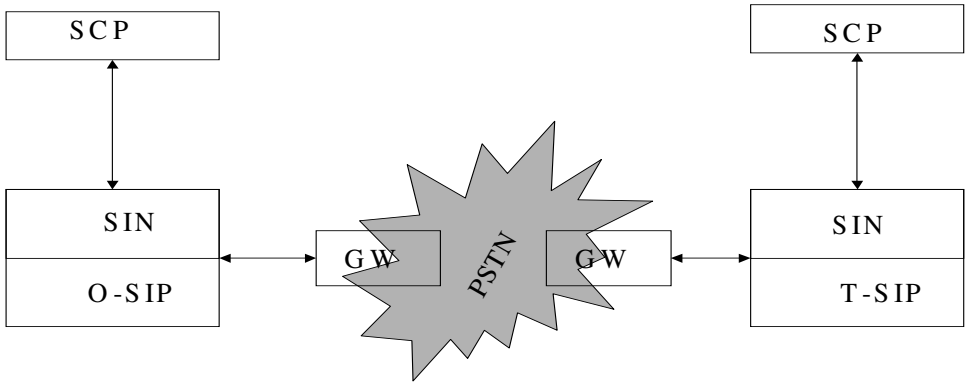


Fig. 2. Interconnection SIP-IN

The SIP "Calling" protocol state has enough functionality to absorb the seven PICs. From server of SIP proxy point of view, its initial state could be corresponded to the O_NULL PIC of the O_BCSM. Its processing state could be corresponded to the Auth_Ori_att, Collect_Info, Analyse_info, Select_ Route, Auth_Call_Setup, Senf_Call and O_Alerting PICs. Its success, confirmed and complete states could be corresponded to the O_Active PIC. Figure 4 below provides a visual mapping from the SIP protocol state machine to the terminating half of the IN Call model.

When the SIP server of termination receives the message INVITE, it creates the T_ BCSM object and initials it to the PIC T_Null, this operation is realized by the state " Proceeding " that orders the five PICs : T_Null, Auth_Ter_Att, Select_Facility, PICs of the T_BCSM. Its calling state could be corresponded to the prrsent_Call PIC. Its call processing state could be corresponded to the T_Alerting. Its complete state could be corresponded to the T_Active PIC.

The service-level call flows for Voice over IP communication where interconnecting between the PSTN and IP-based networks are necessary to complete a call.

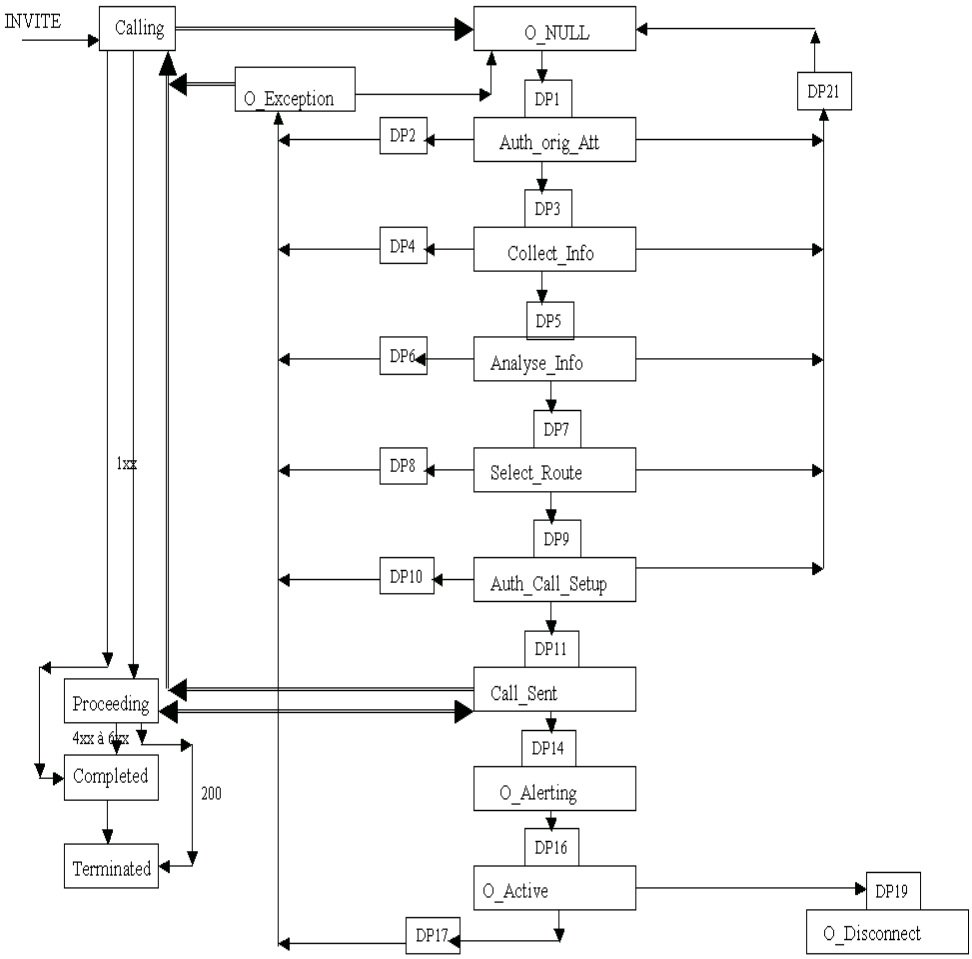


Fig. 3. Mapping from SIP to O_BCSM

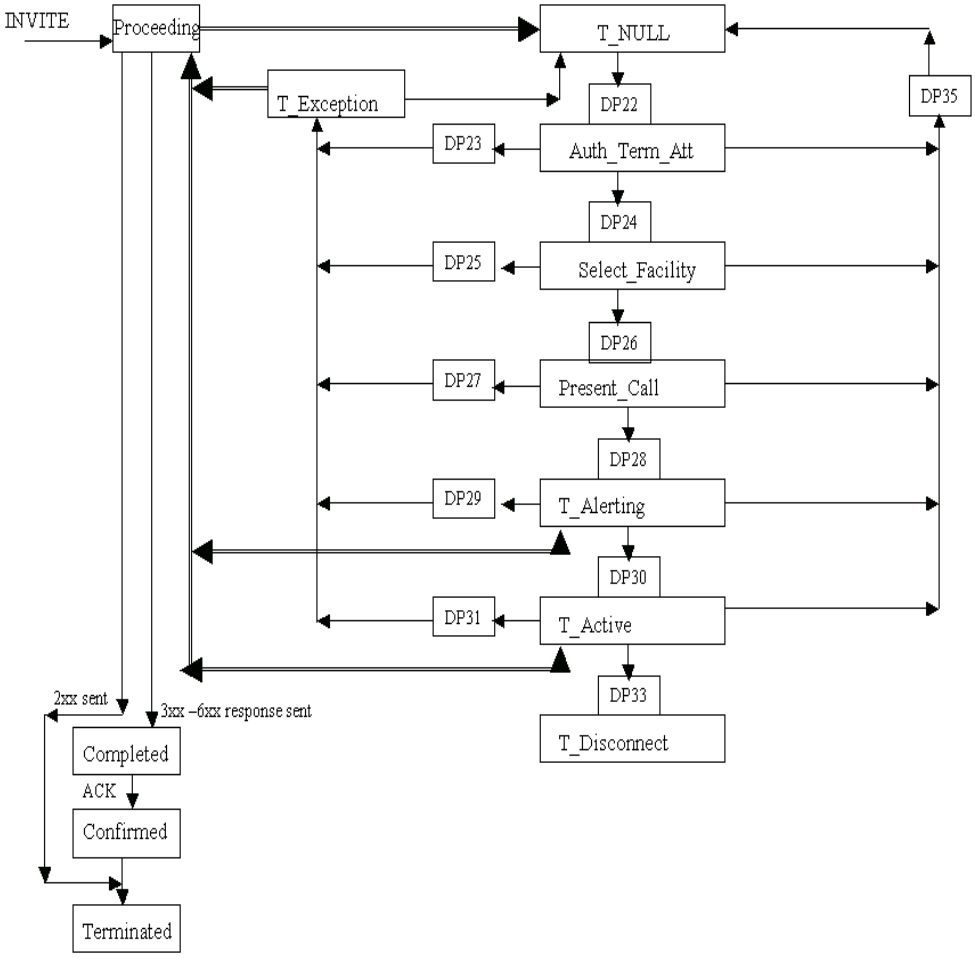


Fig. 4. Mapping from SIP to T_BCSM.

3. Threats in the intelligent network (telecom service)

As all elements of a network can be distributed geographically and that element of system IP is totally opened, several threats of security can rise and attack these different elements. The interconnection IN, is the process to execute a demand of service IN on the part of the user of service through at least two different autonomous areas. Typically, each area represents a system IN separated with different legal entities and entities of resource IN. The limp of the IN service is only to be executed, if the two different areas cooperates by exchanging management, control, and services of data on the basis of a legal contract (co-contract of operation). In this competition, each area applies these clean mechanisms to provide the integrity, the availability, and the intimacy of service users. If the two operators that distribute cooperate, they have to apply the same totality of mechanisms to exchange data between their SCPs and SDPs.

The main problems of security that pose in the multimedia communication area and the telephony over IP as well in a system IN under IP are following:

- Imitation of attack: users not authorized can try to access to services of IN. For example, in the case of service IMR a user not recorded can try to see video services.
- Simulating attack: A recorded user can try to avoid the policy of security and obtains illegitimately access to sensitive services. For example, a user with common access privileges can try to act as an administrator of service IN.
- Denial of Service attack: an adversary can try to block users to access to the services of IN. For example to send a great number of requests to the system simultaneously
- Communication to spy and alter: an adversary can try to spy and/or to modify the communication between a legitimate user and elements of service IN.
- Lack of responsibility: if IN is not capable to verify the communication between users and its elements of service, then it will not be possible to make these users responsible for their actions.

The list is not complete. In practice, nevertheless, one can be found confronted with others problems of security, considered as not belonging of the area of application (for example, problems linked, the policy of security, the security of the management system, to security of the implementation, the operational security or to the processing of security incidents). As well as the technological evolution on the soft, does not cease to increase in a manner not estimable, similarly, the technological connection tools to the system and the attack passive and active become impressive things?

If the system and its components are not sufficiently secured, a lot threats can occur. However, it is necessary always to consider:

- What is the probability of a threat (occurrence; likelihood)?
- What are the potential damages (impact)?
- What are the costs to prevent a threat?

Depending on these suppositions, the cost and the efficiency of security mechanisms has to be implemented. The potential of the threat depends on the implementation of IN, the specific service IN. They depend also on the implementation of security mechanisms (ex. PIN, strong authentication, placement of authentication, management of key, etc.).

Manufacturers as well as the groups of standardization make the work of the analysis of risks in the order to improve the security of systems IN. Although a many improvements have already been realized, concerning the security of access to SCP and SMP. New services and new architectural concepts necessitate supplementary improvements. The next figure, figure 5, presents places of the different threats.

Intelligent networks are distributed by nature. This distribution is realized not only to the superior level where the services are described as a collection of service feature (SF), but to too low levels, where the functional entities (FE) can be propagated on different physical entities (PE). Like the communications of various elements of the network are realized on the open and uncertain environment, the security mechanisms have to be applied.

A responsible of the system can prevent these threats of security by using the various mechanisms. The authentication has to be applied in the order to prevent users not authorized to earn the access to the distribution of services.

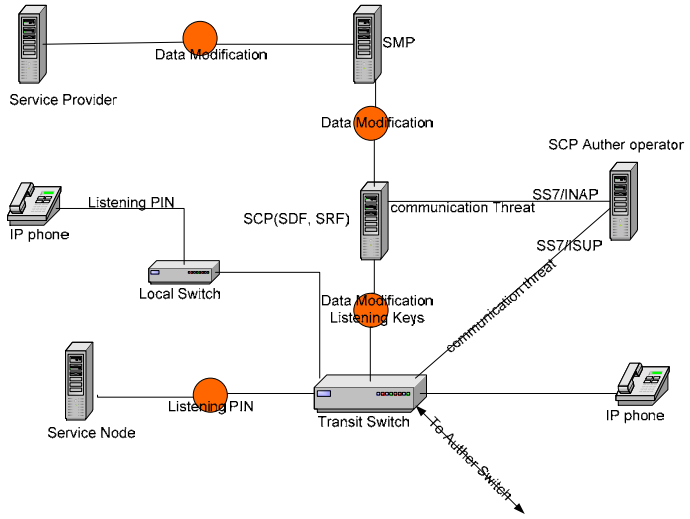


Fig. 5. Places of the different threats.

4. Secure the telecom service with SIP

SIP Communication is susceptible to confront several types of attack. The simplest attacks in the SIP permit to a hacker of earning the information on users' identities, services, media and topology of the distribution. This information can be employed to excute others types of attacks. The modification of attack occurs when an assailant intercept the effort and covers the signal and modify the SIP message in the order to change a certain characteristic of a service. For example, this sort of attack can be employed for diverting the flow of signaling by forcing a particular itinerary or for changing a recording of the user or modifying a profile of service (Profos, 2002). The sort of attack depends on the type of security (or insecurity) employed (the type of authentication, etc.). These attacks can also be employed for the denial of service.

The main two mechanisms of security employed with SIP: authentication and the encryption data. The authentication of data is employed to authenticate the sender message and insure that certain sensitive information of the message was not modified in the transit. It has to prevent an assailant to modify and/or listen in SIP requests and reply. SIP employs Proxy -Authentication, Proxy -Authorization, authorization, and WWW - Authentication of areas of the letterhead, similar to these of HTTP, for the authentication of the terminal system by the means of a numerical signature. Rather, proxy-by-proxy authentication can be executed by using the authentication protocols over Internet such that, the transport layer TLS or SSL and the network layer IPSEC.

The cryptography of data is employed to, ensure the confidentiality in SIP communication, allowing only the legal receiver client to decrypt and read data. It is usual of using algorithms of cryptography such that the DES (DES: Data Encryption Standard) and Advanced AES (AES: Advanced Encryption Standard). SIP endorses two forms of cryptography: end-to-end and hop-by-hop. The end-to-end encryption provides confidentiality for all information (some letterhead and the body of SIP message) that needs to be read by intermediate servers or proxy. The end-to-end encryption is executed by the mechanism S/MIME. On the contrary, the hop-by-hop encryption of whole SIP message can be employed in the order to protect the information that would have to be accessed by intermediate entities, such that letterhead *From*, *To* and *Via*. The security of such information prevents malevolent users to determine that calls, or to access to the information of the itinerary. The hop-by-hop encryption can be executed by external security mechanisms to SIP (IPSEC or TLS).

Before closing this poll of security mechanisms in SIP, it is necessary to consider the efforts of standardization processing to improve the security mechanisms for SIP. The most important matter here is the problem of the agreement on the chosen security mechanism between two SIP entities (user agents and/or proxy) that want to communicate by applying a level of «sufficient» security. For this reason, it is very important to define how a SIP entity can select an appropriate mechanism for communicating with a next proxy entity. One of the proposals for an agreement security mechanism that allows two agents of exchanging their clean security aptitudes of preferences in the order to select and apply a common mechanism is, when a client initiated the procedure, the SIP agent include in the first request sent to the neighbor proxy entity the list of its mechanisms of security sustained. The other element replies with a list of its clean security mechanisms and its parameters. The client selects then the common security mechanism preferred and use this chosen mechanism (ex, TLS), and contact the proxy by using the new mechanism of security (Jennings, 2002).

With this technique, another problem should be handled. It is the problem with the assertion and the validation of the identity of the user by SIP server. The SIP protocol allows a user to assert its identity by several manners (ex, in the letterhead); but the information of identity requested by the user is not verified in the fundamental SIP operation. On the other hand, an IP client of telephony could have required and insure the identity of a user in order to provide a specific service and/or to condition the type of service to the identity of the user himself. The model of SIP authentication could be a way of obtaining such identity; however, the user agents have not always the necessary information on key to authenticate with all the other agents. A model is proposed in (Profods, 2002) for «confirmed identity» which is based on the concept of a «confirmed area». The idea is, that when a user authenticates its clean identity with a proxy, the proxy

can share this authenticated identity (the confirmed identity) with all the other proxies in the «confirmed area». A confirmed area is a totality of proxies that have a mutual configuration of a security association. Such association of security represents a confidence between proxies. When a proxy in a «confirmed area» authenticates the identity of the author of a message, it adds a new letterhead to the message containing the confirmed identity of the user. Such identity can be employed by all other proxies belonging to the «confirmed area».

Using this mechanism the client UAC, is capable to identify himself to a proxy UAS, to an intermediate proxy or to a registration proxy. Therefore, the SIP authentication is applied only to the communications end-to-end or end-to-proxy; the authentication proxy-by-proxy would have to count on others mechanisms as IPsec or TLS.

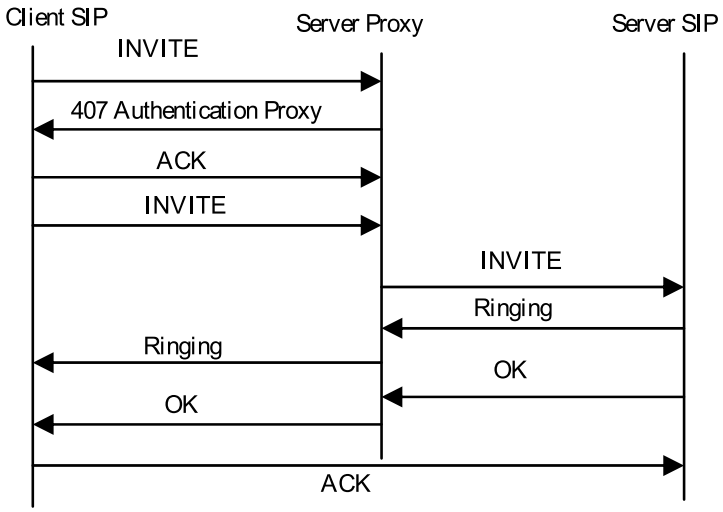


Fig. 6. Authentication SIP

The procedure of authentication is executed when the UAS, the proxy intermediate, or the necessary recording proxy for the call of the UAC has to be authenticated before accepting the call, or the recording. In the beginning the UAS sends a request of SIP message «text» (ex, INVITE). In the reception of this message, the UAS, proxy, or recording proxy decides that the authentication is necessary and sent to the client a specific SIP error message of the request of authentication. This error message represents a challenge. In the particular case, where the message of error is 401 (Unauthorized) is sent by UAS and recording, while when the message of error is 407 (Proxy Authentication Required) is sent by proxy server. The UAC receives the message of error, calculates the reply, and includes it in a new message of the SIP request. The next figure 6 shows the sequence of message for the case of request of authentication by the proxy server.

The UAC sends a message ACK immediately after that the message of error is received. This message closes the first transaction; then the second message INVITE opens a new transaction.

INVITE sip:xy@domain SIP/2.0
Via: SIP/2.0/UDP
To: xy <sip:xy@domain>
From: yx <sip:yx@domain>
Call-ID:
CSeq: 1 INVITE
Contact: <sip:yx@domain>
Content-Type: multipart/signed;boundary=…;
micalg=sha1;protocol=application/pkcs7-signature
Content-Length:
Content-Type: application/pkcs7-mime;
smime-type=envelopeddata; name=smime.p7m
Content-Disposition: attachment;handling=required;filename=smime.p7m
Content-Transfer-Encoding: binary
<envelopedData object encapsulating encrypted SDP attachment not shown>
Content-Type: application/pkcs7-signature;name=smime.p7s
Content-Disposition: attachment;handling=required;filename=smime.p7s
Content-Transfer-Encoding: binary
<signedData object containing signature not shown>

Fig. 7. S/MIME encryption in SDP

But this technique is a classic and it's based on a standard and classical mechanism. It will thus be preferable to propose a new technique based on sure cryptographic algorithms such as the quantum cryptography.

5. Elements necessitates security in telecom service

Manufacturers as well as the groups of standardization make the work of the analysis of risks in the order to improve the security of systems IN. Although a lot of improvements have already been realized, concerning the security of access to SCP and SMP. New services and new architectural concepts necessitate supplementary improvements. The next figure, figure 7, presents places of the different threats.

Intelligent networks are distributed by nature. This distribution is realized not only to the superior level where the services are described as a collection of service feature (SF), but to too low levels, where the functional entities (FE) can be propagated on different physical entities (PE). Like the communications of various elements of the network are realized on the open and uncertain environment, the security mechanisms have to be applied.

A responsible of the system can prevent these threats of security by using the various mechanisms. The authentication has to be applied in the order to prevent users not authorized to earn the access to the distribution of services.

The cryptography technique that allows detecting a spy and realized the security is the technique of quantum cryptography

6. Quantum cryptography

Quantum cryptography does not base security on unproven mathematical problems. Instead, the foundation of security lies in the properties of quantum mechanics (Gisin, Ribordy, 2001). Three such properties essential for quantum cryptography are:

1. We cannot make a measurement on an unknown quantum system without perturbing unless the measurement is an eigen operator to the quantum state being measured. This implies that an eavesdropper (conventionally called Eve) cannot make a measurement of an unknown quantum state in order to obtain some information about the key without introducing disturbances that can in turn be discovered by Alice and Bob.
2. We cannot make a copy of an unknown quantum state. This property is usually referred to as the no cloning theorem. It prevents an eavesdropper from simply intercepting the transmission and making copies of the transmitted quantum states in order to keep copies to make measurements on, while passing on an unperturbed quantum state to Bob.
3. We cannot measure the simultaneous values of non commuting observables on a single copy of a quantum state.

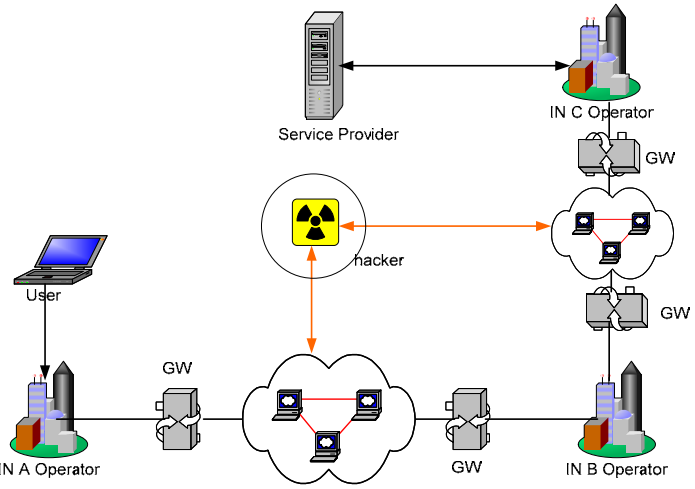


Fig. 8. Place of the hacker.

It ensures that the eavesdropper cannot construct a measurement that is an eigen operator to all quantum states used for the key distribution, i.e., it guarantees that it is impossible for the eavesdropper to only perform measurements that leave the quantum states unperturbed (Hoi, 2008).

Quantum cryptography cannot securely transmit predetermined information; it can only securely generate a random key. Once generated, this random key can be subsequently used in a symmetric cipher, such as the one-time pad or one of the modern symmetric ciphers, to securely transmit data over a classical communication channel. A running quantum cryptography channel will steadily generate new secret key material. Thus, quantum cryptography is solving the most difficult problem in modern cryptography, that of key distribution.

There are mainly two types of quantum key distribution (QKD) schemes. One is the prepare-andmea sure scheme, such as BB84, in which Alice sends each qubit in one of four states of two complementary bases; B92, in which Alice sends each qubit in one of two non-orthogonal states; six-state, in which Alice sends each qubit in one of six states of three complementary bases. The other is the entanglement based QKD, such as E91, in which entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits; BBM92, where each party measures half of the EPR pair in one of two complementary bases.

6.1 BB84 algorithm

BB84 is a quantum key distribution scheme developed by C. Bennett and G. Brassard in 1984. It is the first quantum cryptography protocol. The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption. It has the following the phases.

Step 1. Alice sends a random stream of bits consisting of 1's and 0's using a random selection of rectilinear and diagonal scheme over the quantum channel. On the other side Bob has to measure these photons. He randomly uses one of the two schemes (+ or X) to read the qubits. If he has used the right scheme he notes down the correct bits or he ends up noting down the wrong bits. This is because one cannot measure the polarization of a photon in 2 different 'basis' (rectilinear and diagonal in our case) simultaneously. For example, suppose Alice sends | using '+' scheme to represent 1 and Bob uses '+' scheme and notes down the bit as 1. For the second bit Alice sends \ using the 'X' scheme to represent 1 but Bob uses an incorrect scheme + and miss interprets it as either | or - noting it down correctly as 1 or 0 incorrectly.

Step 2. Alice talks to Bob over a regular phone line and tells the polarization schemes (and not the actual polarization) she had used for each qubit. Bob then tells Alice which of the schemes he had guessed it right. This gives the correct bits noted down by Bob. Based on this they discard all the bits Bob had noted down guessing the wrong scheme.

Step 3. The only way for Alice and Bob to check errors would be to read out the whole sequence of bits on an ordinary telephone line. This wouldn't be a wise idea. So Alice randomly picks some (say 100) binary digits out of the total number of bits that were measured using the correct scheme and checks just these. The probability of Eve being online and not affecting Bob's measurements of 100 bits is infinitesimally small. So if they find any discrepancy among the 100 digits they will detect Eve's presence and will discard the whole sequence and start over again. If not then they will just discard only those 100 digits discussed over phone and use the remaining 1000 digits to be used as one time pad (Johnston, 2002)

One advantage of quantum cryptography is the ability to detect an eavesdropper since Eve can never read the values with out altering them. For example, if Eve reads \ polarization using + scheme then he will be altering the polarization of the photon to either – or ↕, resulting in binary values 0 or 1 respectively. Eve might be able to get the actual (binary)

value of 1 but ends up altering the polarization for Bob. If Bob uses X scheme to measure the values he might get either \, which is what Alice sent or /, which is an incorrect measurement.

Bit Number	1	2	3	4	5	6	7	8
Alice : Bits	1	1	0	1	0	0	1	1
Alice : Scheme	+	+	+	+	X	X	X	+
Alice : Qubit	↕	↕	↔	↕	/	/	\	↕
Eve: Scheme	X	+	X	+	+	X	+	X
Eve: Qubit	/	↕	↕	↕	↔	/	↕	/
Bob: Scheme	+	X	X	+	+	X	X	+
Bob: Qubit	↕	\	\	↕	↔	/	/	↔
Bob: Bits	1	1	1	1	0	0	0	0
Selection	√			√		√	√	√

Fig. 8. Key Selection and detecting Eve's presence

Here the bits 1, 4, 6, 7, 8 are selected by Alice and Bob since both of them use the same detection scheme. But when they randomly check bits 1, 7 and 8 they find that the values are different. Through this they can detect the presence of the eavesdropper.

6.2 BB92 algorithm

In 1992, Charles Bennett proposed what is essentially a simplified version of BB84 in his paper, "Quantum cryptography using any two non-orthogonal states". The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

This security feature results from the use of a single or two photons. We know from quantum properties of photons that the measurement of spin of one gives the spin of the other. So if a given pulse sent from Alice is formed by entangled photons then Eve can split these photons using a beam splitter in such a way that he can direct one photon to his polarization detector and another to Bob's. But if only single photons are generated then in presence of a beam splitter the photons have to choose between Eve's and Bob's polarization detectors. This increases the error rate which the BB84 protocol will detect.

Thus, it is the singleness of the photon that guarantees security (Mohamed, 2007). The figure 9 represents a probability to spy detected vs photon number:

Pdet(n) = Pr{MBB84 |= Φdet} with Φdet = a PCTL equation, is True if spy is detected.

PCTL : probabilistic temporal logic (Xu, 2009)

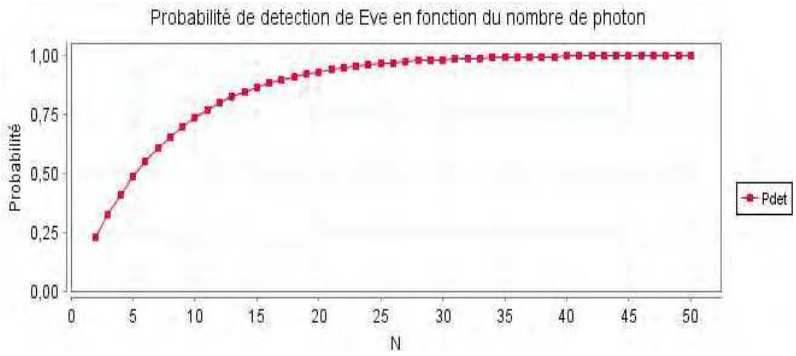


Fig. 9. Probability to spy detected

6.3 Quantum key distribution QKD

The BB84 protocol and its variants are the only known provably secure QKD protocols. Other QKD protocols (BB92), although promising, have yet to be proven secure. The benefits of QKD are that it can generate and distribute provably secure keys over unsecured channels and that potential eavesdropping can be detected (Mohamed, 2007). QKD can defeat the current computationally complex key exchange methods. Because QKD generates random strings for shared secrets, attaining a QKD system and reverse engineering its theory of operation would yield no mechanism to defeat QKD.

7. Implementation a quantum cryptography in SIP protocol over IMS network

The IMS has been *originally* conceived for mobile systems, but with the addition of *TISPAN* works in the *7* version 7, *the PSTN* are equally supported.

The IMS is a structured *of the architecture of Next* Generation *Network* (NGN) that allows the progressive introduction of *voice* application and multimedia in mobile and permanent *network*. The IMS *is used* with all types of systems (permanent, mo*bile* or wireless), including *a switching functions,* as GPRS, UMTS, CDMA 2000, WLAN, WiMAX, *DSL. An open interface between control and service layers allows mixing* calls/*session in a* different *access networks*. The IMS use*d a* cellular technolog*y* to provide an access in every *position*, and *Internet* technology to provide services.

The principle of the IMS consists on the one hand in *clearly* separate the transport layer of the *service* layer and on the other hand to use the transport layer for control and *signaling* functions so as to insure the quality of service wished for the *desired* application. IMS aims, to make the *network* a sort of middleware *layer* between applications and the access. Applications are been SIP, *or* not SIP, they pass by a *Gateway* before the connection to the controller of sessions.

Despite considerable advantages of the IMS, several limit render the IMS all alone is incapable to be beneficial for the creation and the exploitation of services by operators to the near users, it is in order that, one uses IN service into SIP protocol.

In my Application, I'm proposing a several IMS networks nodes for mobile application (figure10). The signaling into the different elements is assured with SIP over MAP (Mobile Application Protocol).

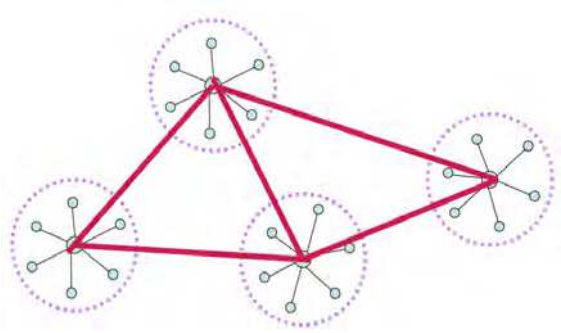
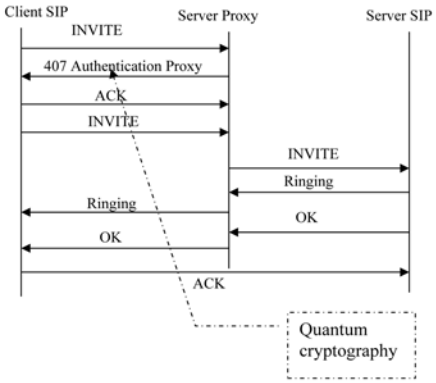


Fig. 10. IMS Network node

After this I'm developing a quantum cryptographic key distribution in SIP Body based on the BB84 algorithm (Bernhard, 2003), named qc:




```
INVITE sip:xy@domain SIP/2.0
Via: SIP/2.0/UDP
To: xy <sip:xy@domain>
From: yx <sip:yx@domain>
Call-ID:
CSeq: 1 INVITE
Contact: <sip:yx@domain>
Content-Type:
multipart/signed;boundary=…;
micalg=sha1;protocol=application/quantum
cryptography
Content-Length:
Content-Type: application/quantum
cryptography;
smime-type=envelopeddata; name=qc
Content-Disposition:
attachment;handling=required;filename=qc
Content-Transfer-Encoding: binary
<envelopedData object encapsulating
encrypted SDP attachment not shown>
Content-Type: application/quantum
cryptography;name=qc
Content-Disposition:
attachment;handling=required;filename=qc
Content-Transfer-Encoding: binary
<signedData object containing signature
not shown>
```

Fig. 11. QC into SIP request

The different ID of IMS clients is registered in a database developed with sql in QC server. I am proposing one QC server for one IMS server (see figure) and the transaction into these IMS servers is authenticate with BB84 protocol like a Kerberos protocol (Butler, 2006), figure 12.

After this, I am implementing my application over an IMS core (http://www.openimscore.org) open source IMS network and IMS client is UCT client IMS (http://uctimsclient.berlios.de). The figure 13 show a SIP client Request and figure 14 show an IMS network with QKD server.

8. Conclusion

Mobile networks has adopted the IN technology to provide to users of the new services that can be only obtained in the permanent system and improved management of mobility. With the SIP protocol under IP an attempt of the Mobile connection has IP and IN to define the new services as well as to exploit advanced techniques in the security developed for IP network becomes possible especially for IMS network. The SIP authentication is the alone technique proposed by SIP for the security for the terminal and subscribed. With quantum cryptography mechanism into SIP Authentication, the security between IMS client and P-CSCF or I-CSCF is assured and sure.

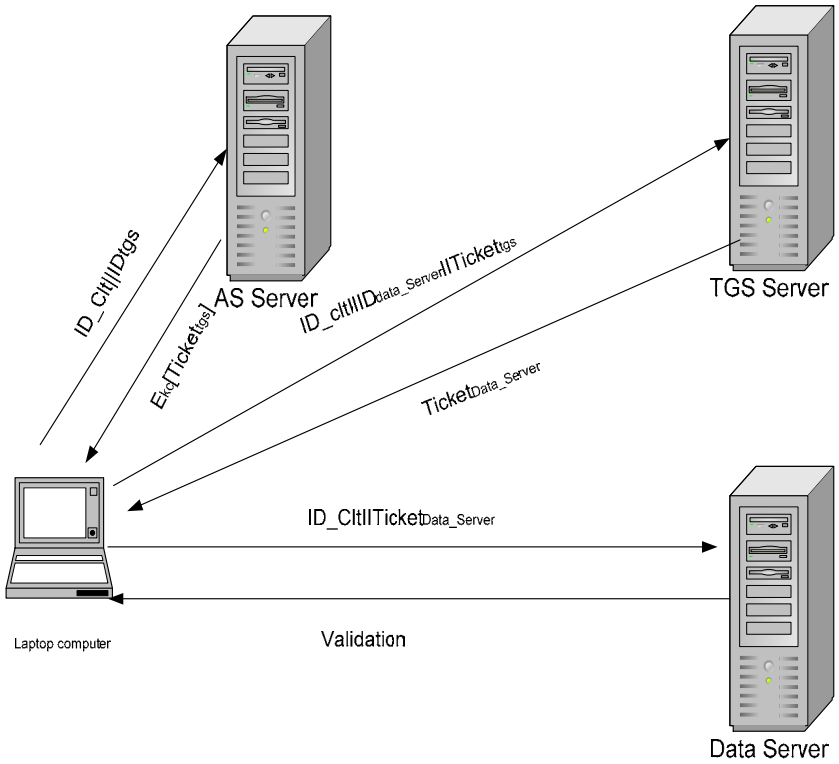


Fig. 12. Kerberos mechanism

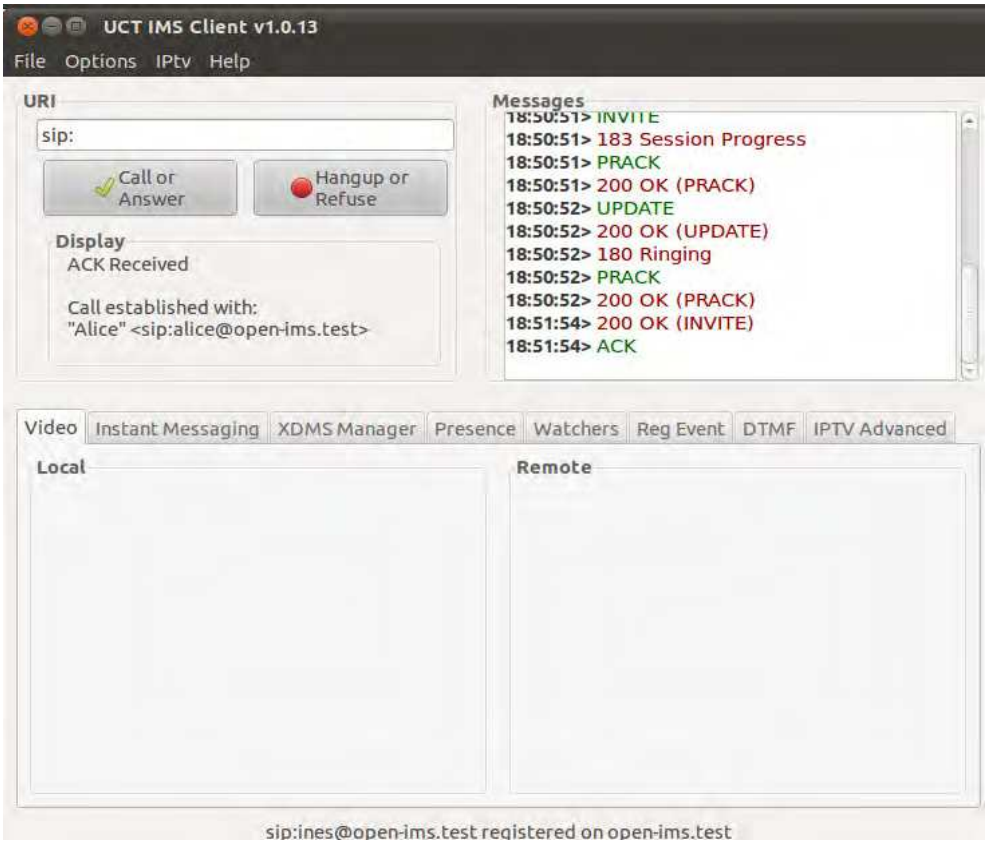


Fig. 13. SIP client request

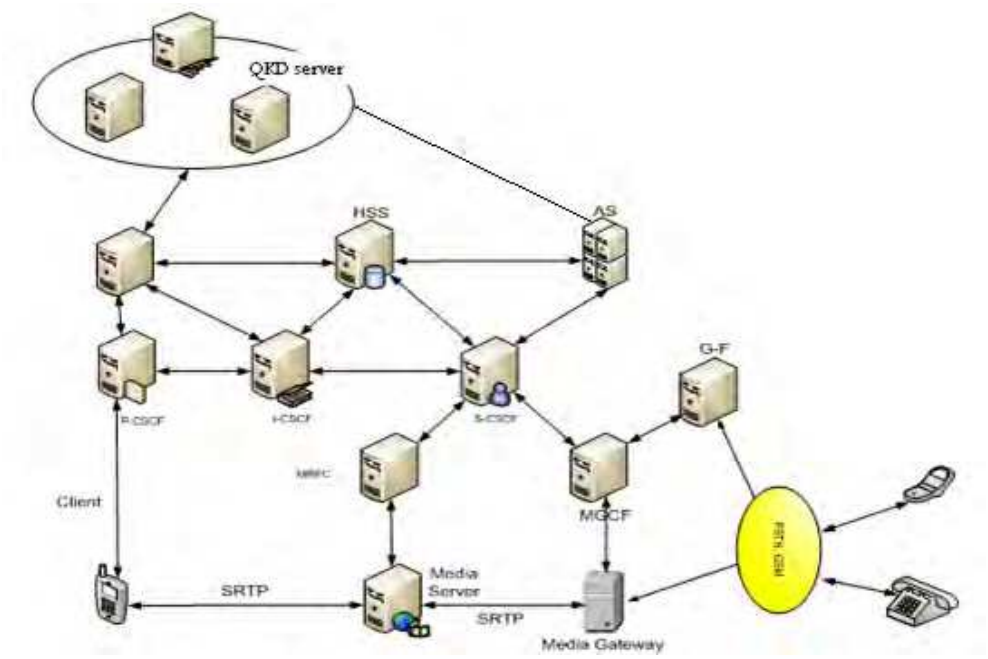


Fig. 14. IMS network with QKD server

9. References

Bulter, F. I, Cervesato, A. D. Jaggard, A. Scedrov,C. Walstad, Formal analysis for Kerberos 5, Theoretical Computer Science 367 (2006) 57 – 87.

Schulzrinne, H. The Session Initiation Protocol (SIP); hgs/SIP Tutorial may 2001.

Johnston, A & al, SIP service examples; draft-ietf-sip-service-examples-03.txt, June 2002.

Chapron, J. B, Chatras, An analysis of the IN call model suitability in the context of VoIP; Compter Networks 35 (2001) 521-535.

Hoi-Kwong Lo and Yi Zhao, Quantum cryptography. arXiv:0803.2507v4,1 Apr 2008.

El ouahidi, B & al, Internet/Telecommunication integration : Towards IN-capable SIP network; Revue internationale: Calculateurs parallèles réseaux et systèmes repartis, Hermès-Editions, Edition spéciale ingénierie des services de télécoms, 12(2) :259-280, December 2000.

Internet Draft , VK. Gurbani, Interworking SIP and Intelligent Network (IN) Applications; draft-gurbani-sin-02.txt, June 2002

EEEurescom Project P916 Supporting of H323 by IN, Providing IN functionality for H323 telephony calls, October 2000.

Gisin, N. G.Ribordy, W.Tittel and H.Zbinden, Quantum cryptography. arXiv:quant-ph/0101098v2 18 Sep 2001.

Fing, Principes et conditions de mise en oeuvre du standard ENUM en France; http://www.art-telecom.fr/publications/index-cp-enum.htm. 18 juin 2001.

Bernhard Omer, Classical Concepts in Quantum Programming. arXiv:quant-ph/0211100v2 29 Apr 2003.

Mohamed Saleh Mourad Debbabi, Verifying Security Properties of Cryptoprotocols: A Novel Approach. Fifth IEEE International Conference on Software Engineering and Formal Methods, IEEE 2007.

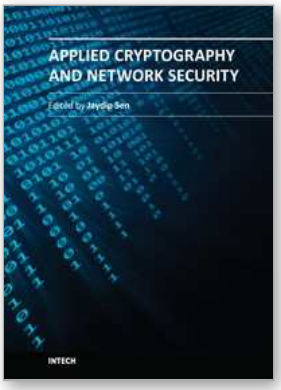
Xu Wei, Ma Yan, Liu Nan, Wu Dong-ying, A Formal Method for Analyzing Fair Exchange Protocols. 2009 WASE International Conference on Information Engineering.

Schweizer.L, Scripts et APIs pour la gestion de serveurs SIP ; www.tcom.ch; 23/12/2001.

http://www.openimscore.org.

Profos.D "Security requirements and concepts for Intelligents networks" , *Ascom Tech AG Bielstrasse 122, 4502 Solthurn.*

Jennings, C. Peterson, J and M. Watson,"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", <*draft-ietf-sip-asserted-identity-01*>, *June 2002.*



Applied Cryptography and Network Security
Edited by Dr. Jaydip Sen

ISBN 978-953-51-0218-2
Hard cover, 376 pages
Publisher InTech
Published online 14, March, 2012
Published in print edition March, 2012

Cryptography will continue to play important roles in developing of new security solutions which will be in great demand with the advent of high-speed next-generation communication systems and networks. This book discusses some of the critical security challenges faced by today's computing world and provides insights to possible mechanisms to defend against these attacks. The book contains sixteen chapters which deal with security and privacy issues in computing and communication networks, quantum cryptography and the evolutionary concepts of cryptography and their applications like chaos-based cryptography and DNA cryptography. It will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821