Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

XTR algorithm based encryption for Security in computer

Bushra Kamil Hilal [a],Mohammad Q.Jawad[b] , Dr. Ahmed W.Shehab[c]

Department of Computer information systems , College of Computer Science and information technology /University of Qadisiyah
Department of Biomedical InforMatics ,College of Biomedical Informatics University of IT And Communication
Department of Biomedical InforMatics ,College of Biomedical Informatics University of IT And Communication

bushra.k.h@qu.edu.iq
Mohammad.qassim 2002@uoitc .edu .iq
AHMED @uoitc .edu .iq

ARTICLE INFO

Article history:
Received: 20 /12/2022
Rrevised form: 27 /01/2023
Accepted : 01 /02/2023
Available online: 30 /03/2023

Keywords:

(Cryptography , XTR, Signature design, DSA, NR program, Field finite, Polynomial cyclostome in nature, Conjugate component, Trace)

ABSTRACT

The idea of XTR was first presented by Lenstra et al. in Crypto 2000. The efficient and compact subgroup trace representation is referred to as XTR Discrete logarithm (DLP) is considered as the basis for the security of the XTR. cipher system. It is regarded as a good substitute for the RSA and elliptic curve cryptosystems. We shall go into great detail on the mathematics underlying XTR and its uses in cryptography in this book chapter. Keywords \s• Cryptography\s• XTR

MSC..

https://doi.org/10.29304/jqcsm.2023.15.11294

1- Introduction:

can read processes and messages. There are two basic types of cryptography that offer confidentiality: symmetric key cryptography and asymmetric key cryptography. One of the fundamental drawbacks of symmetric key cryptosystem is that users must agree on a shared key before to talking with one another, necessitating previous contact between two parties. The key distribution problem is what's happening here. Asymmetric key cryptography was first established in 1976 when Scientists, including Davy, developed the concept of this key exchange protocol known as There is a protocol called Diffie-Hellman (DH) that has been changed in the name of this world. The first workable answer to the key distribution issue is the DH key exchange protocol. The multiplicative group GF(p) of a finite field GF(p) and its generator g are fixed as system parameters in the DH scheme. Each party will where a random key is made to be x and y, respectively, such that x, y be P1 and 0, where both parties agree on the secret key between them to the opposite party, each will send g x mod p and g y mod p .

∗Corresponding author

Email addresses:

Communicated by 'sub etitor'

They will produce the shared secret key g xy mod p in this manner. If the capacity of p is 1024 bits at least, while p 1 is as an initial storage value of 160 bits, the method will be safe. As a result, each side transmits the other 1024 bits. ElGamal proposed using The extent of the span is within the limits of GF (p r), r > 0 in place of the prime field GF in 1985, researcher Schnorr put a variation in the DH diagram since the year 90th and considered the subgroup G which is from the doubled group GF (p). The prime number q, which is thought to be exceedingly tiny in Comparison of the order of G and P1 The DH scheme's computational cost is lowered as a result, but the amount of bits that must be sent between each party stays the same .

According to Lenstra's 1997 proposal, the Schnorr method may be made more generic. After taking into account these subtotals suggested modified version of the DH system in which just one-third of the bits needed by the DH technique are exchanged. Howeve. Both schemes have the same level of security. It was demonstrated that When q (p 2 of p + 1) here the elements of a subset of the order q of GF (p 6) have to be represented using the square log of (p). They expanded the GF scheme in the same study (p r). The approach suggested by Brouwer et al. was enhanced by Lenstra et al. in 2000 .

The XTR is the name of this approach. ECSTR is the effective compressed subgroup tracer is what name XTR stands for. XTR takes into account That is, consider that banana q (as G) of GF is the subgroup of the first order where q (p 2 p + 1). The XTR group is the name of this subgroup (or XTR subgroup). An element of G is represented by its trace over GF in this approach (p 2). Since the arithmetic is performed across GF (p 2), 2log2 p bits were required to represent each element of G. In other words, XTR offered a smaller representation of the G element .

As opposed to the approach suggested by Brouwer et al., this strategy also improves communication. but at a lower computational expense. Be aware that LUC also employed the trace representation of the elements, with GF serving as the underlying field, and that XTR is not the only technique in which this is done (P 2). The discrete logarithm of the XTR set, and the crucial Diffie-Hellman theorem are perfectly safe when set above GF (pg. 6). Through this, XTR can be applied to any encryption system based on DLP and/or its derivatives. Standard encryption based on DLP. in the same article. shown that XTR may be used in place of RSA and ECC170-bit is equivalent security to 1024-bit RSA. A XTR cryptosystem's key and parameter selection is also more effective than the ECC's.

In light of this, it may be said that XTR required less overhead in terms of data storage, processing, and transmission than other cryptosystems of comparable security. This chapter's goal is to go into great detail regarding Mathematics is the most important application of the XTR algorithm and what came is to explain the principle of mathematics and behind XTR. We go through methods for choosing parameter values and locating an XTR group's generator in the same section.

2- A Few Definitions and Finite Field Results

In this paper, we show the p property of an initial p as GF (p r), i.e. r > 0. GF (p r) is closely related to p r. where GF (p r) is used to show the doubled group of GF (p r), whose origin is p r 1. GF (p t) GF (p r) is a finite extension of t r. When the polynomial f (X) = a n X n + a n 1 X n 1 + a 1 X + a 0 GF (p t) [X] and has no roots in GF, then it is considered irreducible (p t). If n = 1, f(X) is known as a polynomial. If GF (p r) is a root of f (X) and f (X) is an irreducible mononomial of degree s = rtZs = rtZ on GF (p t), then GF (pr) GF (pt) [] GF (pt) [X] and . GF (pr) ≅GF (pt) [] GF (pt) [X] GF (p r) g (X) mod f (X) is defined as g (X) GF (p t) & deg (g (X))) s Therefore, finding the representation of the GF element is sufficient to represent the GF element (p r).

Again, a vector of length s over GF (p t) can be used to determine the GF (p r) element, where the input is the g parameter. As a result, r log p is required to represent the GF (p r) element. Again, if f (X) is an irreducible monomial on GF (p t) and GF (p r) is the root of f (X), then piGF (pr) piGF (pr) piGF (pr) is the root of f (X)), where I = 0, 1, 2. The lower bound of the polynomial for GF (p r) over GF (p t) is thus m (X,) = (X) (X) (Xp) (Xp2) (Xpd1) GF (point) [X]. When pd = pd = , then m (X,) = (X) (Xp) (Xp2) (Xpd1) GF (pt) [X] where d is the lowest possible positive integer.,(X,) replace (X,) RT.

The elements are known as the GF union when I = 1, 2, and d = 1. (p r). Trace over GF (p t) is the name given to the sum of conjugate elements, i.e. d1i = 0pii = 0d1pi. It is denoted as Tr(). Let m (X,) be equal to X d + a d 1 X d 1 + a 0. Due to the fact that m (X,) GF (p t) [X], and I GF (p t), with I = 0 and 1 and d 1. In particular, ad1 = d1i = 0d1piGF (pt) ad1 = i = 0d1piGF (pt) and thus Tr () GF (p t), it should be noted that the element can also be represented by a polynomial minimum, M (X,) GF (ZT). Deg m (X,) should be rtrt in this case; Otherwise, GF (p k), where GF (p t) GF (p k) GF, will result in (p r).

Therefore, this method also needs r log p to represent the GF (p r) element. But in some cases, the relationship between the minimum coefficients of the polynomial allows the number of coefficients to be reduced and, as a consequence, tighter. In XTR, where the elements are represented by their traces and by the terms below to complete the model basis: If the conjugate, p, p, pd1, p, p, pd1 is linearly independent on GF, then the element GF (p r) is said to be a regular element (p R). For the natural element, GF (p r), which is base GF (p r) above GF (p t) and is referred to as having a natural base.

polynomial definitions:

For every positive integer, Integer limits are defined by n(X) = (X 1) (X 2) (X t), where X, 1, 2, and t are the first, second, and third roots of unity, respectively, i.e., n(X)=1kngcd(k,n)=1(Alternatively, it can be written as n (X)=dn(Xd1)(nd)n(X)=dn(Xd1)(nd), where ndnd is the Mobius function.

A subset of the order q is the set of the multiplier GF (p r) through the subset field of the identifiers q r (p) and q r, GF (p r) is referred to as a cyclostome subgroup. G q, p, and r stand for it.

3. XTR Foundation

The mathematics underlying the XTR will be thoroughly covered in this part. Parameter check techniques.

3-1 XTR Group

Others, led by Linestra, have proposed the XTR concept. In XTR, p 2 mod 3 and the subgroup defined with XTR is the subgroup G q, p or 6., which means that q p 2 p + 1 and q > 3, is a subgroup of it. , G q, p, and 6 are denoted as G. As with any element with the symbol G, the conjugates are, p2, p2, and p4 p4, so Tr() = + p2 + p4 GF(p2) Tr() = + p2 + p4 GF (p2). Additionally, for GF(p6) and GF(c1,c2)(p2)Tr(c1η1 + c2η2) = c1Tr (η1) + c2Tr (η2) Tr (c1η1 + c2η2) = c1Tr (η1) + c2Tr(η2) Specifically, if n =, then TR(μn) = μn + μnp2 + μnp4Tr (μn) = μn + μnp2 + μnp4As p2p1 mod (p2p+1) and p4 p mod (p 2 p + 1), respectively, and thus TR (μn) = μn + μn (p − 1) + μ − npTr (μn) = μn + μn (p 1) + μ − in addition, from It is easy to confirm that Tr (n) p = n (p 1) + n (p 1) + n (p 1) + np.X 3 Tr (n) X 2 + Tr (n) p X 1 GF (p 2) [X] is the minimum polynomial of n GF (p 2), which is (X n) (X n (p 1)) (X np).

Therefore, the minimum polynomial for μn ∈ G can be uniquely determined by Tr (μ n) ∈ GF (p 2). The function can define G GF (p 2) as n Tr(n), n Z. As a result of the above, only 2log2p is required to represent the G element. Tr(n) = Tr(n(p 1)) = Tr(np) proves It's not a single job. By the similarity between the two functions. The following two topics must be covered in order for the G account application description to be complete.

• How can the arithmetic operations of (p. 2) be performed in GF?

- Can the calculation be done to GF (pg. 2) in G with respect to what is required above?

3-2 Calculation of operations for section (pg. 2) in GF:

The result is that GF(p 2) a 1 + a 2: a 1, a 2 GF(p) & 2 + + 1 = 0. Since 2 + 1 + 1 equals 0, 1 + 2 equals 1(2 + 1) + 2 = (a 2 a 1) + (a 1) 2. f (X) = X 2 + X + 1 is an irreducible bound on GF for p 2 mod 3. (p). If the root of f (X) is GF (p 2), then GF (p2) ≅GF (p) [β] ≅GF (p) [X] ⟨f (X)⟩ GF (p2) GF (p) [β] ≅GF (p) [X] ⟨f (X)⟩

Therefore, GF(p2) ≅ {a1β+a2β2: a1, a2∈GF(p)&β2+β+1=0}GF(p2) ≅ {a1β+a2β2: a1, a2∈GF(p)&β2+β+1=0}. Keep in mind that since p 2 mod 3 and 3 = 1, the basis, 2 is identical to the conventional basis, p. Consequently, a 1 + a 2 p = a 1 + a 2 2 for a 1, a 2 GF(p). The symbol for an element t GF(p) is t t 2.

For p 2 mod 3 and a, b, and c GF(p), where a = a 1 + + a 2 + 2, b = b 1 + + c 2 + 2.

Wireless protection:

When a message is sent over the r The wireless information security system contains data security, computer security, network security, and wireless channel security [1,2]. path in a wireless network via free-space transmission, anyone nearby who has a suitable transceiver can listen in on the transmission. The eavesdropping is essentially undetected because neither the sender nor the intended recipient has any way To see the transmission and what was intercepted Two hackers were seen driving about Silicon Valley listening to networks on their laptops and boom antennas, according to The Wall Street Journal (April 27, 2001).

The wireless network, which is a component of the enterprise network, provides the attacker with one interface without the need for any physical preparations like internet cables. Due of their ease of loss, mobile computing devices are vulnerable to malicious attacker usage. Other clear and likely security concerns for wireless networks are listed by Russell [3] as well, including, to improve the security of the network and user locations, interference and accidental interference that leads to service degradation all of them need for the adoption of network security technology The wireless network has a new and secure solution And it is taken into consideration into account the limitations of wireless networks' computational capacity and how best to leverage the power source of mobile devices. Some of these needs seem to be met by XTRA VPN is a private network that operates over the Internet through a secure interconnection of business networks and remote users, as required. [4].

Networking, which stands for "peer-to-peer “connection, is established using a shared underlying non-exclusive communication medium Allow access is restricted to only association connections within the specified VPN system as IP. pa The transmission can be encrypted or confidential ckets modifying the VPN concept, XTR is chosen as the security solution. Applications for ElGamal encryption and decryption as well as Diffie-Hellman key agreement (XTR-DH) are included in the group of security applications known as XTR (XTR-ElGamal).

Cryptography:

The study of cryptography offers the necessary methods, formulas, and methods for implementing data confidentiality. Cryptography has many subfields, including encryption, authentication, and permission. Create and validate message digests and digital signatures as part of authentication. These techniques can guarantee that any data is real, that it came from the person who says they did, and that it wasn't changed during communication either unintentionally or to encrypt data for certain texts, a special encryption algorithm must be used maliciously.

The purpose of authorization is to make sure that the service is only used by authorized users You must use encryption; these are those functions robust. sufficient to prevent unauthorized access to the source data. The XTR algorithm is a public-key cipher in the context of cryptography. In the late 1970s, public key cryptosystems were developed with c It may be a problem that takes hundreds of years to solve. Here, two keys to the solution can be found, one public and the other secret considerable assistance from the growth of complexity theory [5].

It was noted that a cryptosystem with any chance. One might encrypt communications using the public key and decrypt them using the private key. As a result, only the owner of the private key would be able to Everyone has the

right to access and decrypt encrypted messages through public [6,5]. A new technique has been introduced within the public key cryptosystem to handle the stages involved in producing the secret key. It is described as a key exchange algorithm, in other words. The era of public key cryptosystems was introduced by a key exchange protocol developed by Diffie and Hellman using concepts from number theory [5].

Soon after, Rivest, Shamir, and Adleman created the first practical public key cryptosystem that could be used for both encryption and digital signatures [5]. Later, a number of open-source cryptosystems leveraging a variety of underlying concepts were developed. Several of them quickly Tebisn is not safe. However, Diffie-Hellman and RSA are the most effective protocols [6]. On the XTR public key cipher system, a Diffie-Hellman key exchange application was created.

Digital Signature:

Some variations of digital signatures can achieve integrity, authenticity, non-repudiation, and certification. ElGamal's or the Schnorr signature algorithm's underlying algorithm, DSA (Digital Signature Algorithm), is comparable. It is also reasonably effective for verifying signatures, though not quite as effective as RSA. The public key encryption method known as RSA was created by the company RSA. It relies on modular arithmetic and is frequently used with keys that are 512 bits long [5,6,7].

Algorithm:

The RSA algorithm is built using these fundamental steps:

1-The letters p and q can be chosen to represent two large numbers at random (usually 265 bits each)

2-Establish n = p. q

3-Select an integer that is substantially prime to (p-1) and e s.t. e n. (q-1)

4-Determine the value of d s.t d. e mod (p-1) (q-1) = 1.

5-The private key is and the public key is (e,n) (d,n)

6 - encoder mode is mod n . = (message) e mod n

7- The decoding pattern is m = (encoding) d mod n.

Elgamal world cipher system:

An extension of Diffie-original Hellman's concept for creating shared secret keys is the ElGamal public key cryptosystem. In essence, it creates a shared secret and utilizes it to encrypt a single block of data. The following definitions [5,6] are given for the Generalized ElGamal public key cryptosystem over finite fields. Definition [5,6]: Given that H = I I 0 is the subset that produces it towards the nether G be an active set with the set process, G component formation so that the discrete log problem in H is intractable. Assuming that P = G and C = G X G, we can define K = (G, a, a, a): a = a. The values are disclosed, but the secrecy is kept. If K = (G, a,), if k Z is a random (secret) number, if y1 = a k and y2 = x o k, then define Ek(x, k) = (y1, y2). Find Dk (y) = y2 o (y1 a) -1for the cipher text y = (y1, y2).

XTR:

The public key cryptography scheme known as XTR was created by Arjen Lenstra and Eric Verheul. The underlying group of XTR is a For all the specified fields there is a double set [8,9]. However, XTR has unique characteristics such requiring only one-third of the bits to sign and encrypt communications. This is accomplished by executing all computations Using the concepts of XTR, it is possible to represent the elements of the set, and all the keys of public and preferred algorithms that depend on logarithms can be implemented. [8,9].

Lenstra and Verheul claim that the technique is effective and may be a suitable replacement for elliptic curves, DSS, and even RSA. Compared to elliptic curves, it has the benefit of being fundamentally based on the same discrete log issue. DSS, for example, might make it easier for cryptographers and other users to accept it as a quick and reliable algorithm [7,10].

Discrete logarithm

XTR is the separate problem of a logarithm. "The challenge of computing n given only some y such that y = gn is known as a discrete logarithm. For integers, the problem is simple, but when working in diverse environments, it becomes untraceable [5,6,12]. working with fields like Galois Field, as an example. A prime field, also known as a Galois field, GF, is created when the chosen integer m equals p such that p is a prime number (p).

The discrete logarithm problem in the finite field GF(p) is therefore defined by computing n such that a = gn given two positive non-zero integers a and g (both less than p) (mod p). We can select g to ensure that there is a solution for n for any non-zero a. "P should be a huge prime number (around 10300 and n, generally, of the same magnitude) to make this problem cryptographically difficult" [5,6,12]. To find an integer such that a = an is the discrete log problem, according to definition [5,6]. (mod n). Due to the fact that gcd (, n) = 1, has a multiplicative inverse modulo n, which can be easily calculated using the Euclidean algorithm. Once we have log = -1 mod n, we can solve for a.

The problem is now thought of as having a hard factoring inside this new shape. Finding a polynomial-time technique to compute discrete logarithms in GF is unlikely (p). It would be possible that factoring issues might also be effectively resolved in such a scenario. The XTR public key cryptosystem is used to apply the discrete logarithm issue.
This is because there are numerous techniques for computing discrete logarithms over XTR, but solving the discrete over GF seems to be more difficult (p6). Additionally, employing XTR-based public key cryptosystems rather than factoring-based cryptosystems has some advantages in terms of key size [7,12].

Galois Fields are used by XTR:

A prime example of a finite filed with a q element where q = pn and n > 1 Z is the Galois Filed. A Galois Field is an extension field with a limited degree and characteristic p [6,7]. Defined [5, 6]: Assume that p is prime. Define Zp[x] as the collection of all polynomials in the ambiguous value of x. We build a ring by defining polynomial addition and multiplication in the conventional manner (and lowering coefficients modulo p). If there exists q(x) Zp[x] such that g(x) = q(x), then we say that for f(x), g(x) Zp[x], f(x) divides g(x) (notation f(x) | g(x)). f(x) Utilizing Galois Fields GF, XTR (p6). For instance, the definition of 2 as a primitive element of GF is GF (11) = 0,1, 2...,10. (11), The field components will therefore be 20 = 1 mod 11, 21 = 2 mod 11..., 24 = 5 mod 11, 25 = 10 mod 11...., and 210 = 1 mod 11.

. Super group GF(p6) and subgroup GF of the XTR (p2):

A base generator of a full-multiplicative group of a finite field with particular modifications is used by XTR. This generator is changed to the generator of a sufficiently large prime order q that is relatively tiny. employs a prime order q subgroup of the order p2 - p+1 subgroup of GF(p6), and the order q subgroup g produced by g is known as the XTR subgroup.

No appropriate GF subfield contains the XTR super group (p6). Computing discrete logarithms in g is hence, generally speaking, as difficult as it is in GF(p6) when combined with the selection of q [8,9]. This particular subgroup g is chosen by XTR because it not only offers full GF(p6) security but also exceptionally efficient representation at a low cost. For

instance, elements of the XTR super group can be represented using an element of GF(p6) as opposed to GF(p2) if one is ready to give up the distinction between elements and their conjugates (p6).

However, calculations are also conducted in GF(p2) rather than GF(p6) and can be completed much more quickly than usual. In other words, working in GF(p2) implies dealing with polynomials of the second degree, and working in GF(p6) means working with polynomials of the sixth degree. In addition to being substantially simpler to factor and reduce using the modulus, second degree polynomials also require fewer calculations to generate public data, choose a key, encrypt it, and decrypt it. By switching the computation from GF(p6) to GF(p2), we already outperformed the target by a factor of three computation reduction" [8,9].

XTR system build:

The XTR (g) coding system requires the three global values p, q, and Tr. There are various rules that specify how each of them functions. In order to make q | (p2-p+1) and the resulting fields and subsets sufficiently big to fend off known attacks, the prime numbers p and q are provided. Additionally, if p = 2 mod 3, it is discovered to be more effective. Primes like p 1 mod 3 can also be used, albeit the speed might not always be the same. Let P and Q represent the required bit lengths for the primes p and q [8,9].

The second algorithm:

The finite field and subgroup, p and q, are about 170 bits in size. search for random Z s.t. Q = r2 + r + 1 is the prime value for the q-bit. - Find k > Z at random. Q equals K and ST. p = r + k r2 +(1-k) (1-k) r+k is a P-bit 2 mod 3 prime. Given that p, q > 3 and c = Tr (g) for g GF(p2) s.t., find Tr (g) for g GF(p6) of order q | (p2-p+1) (g).

3th algorithm:

1- Calculate cp+1 using procedure 1 and set s.t. n = p+1 after selecting c GF(p2) GF(p).
2- Go back to step 1 if cp+1 GF(p).
3- To calculate c(p2-p+1)/q, use alg.1 st. n = (p2-p+1)/q.
4-If c(p2-p+1)/q = 3, go back to step 5. 5. Define Tr(g) as c(p2-p+1)/q.

Test bed Description:

This project's test environment is based on wireless LAN technology. The Linux 2.4.1-20 kernel is running on a PII Celeron 900 processor in the mobile node. The Ethernet already has an antenna that the AirPort Card uses. With a turbo 11.0 Mb speed, Ethernet is a WAP implementation offered by Lucent Technologies. Although it offers NAT and DHCP functions as in AirPort it is used as a wireless route [14]. Using XTR algorithm to achieve wireless transmission and deactivate Wireless Encryption Protocol (WEP).

The Dalhousie University Faculty of Computer Science's network, in this case the "public network," is directly connected to the AirPort Base Station. As previously mentioned, the XTR server functions on a computer running Linux. The client, however, where it is possible to work on a different device running different operating systems such as Linux, for example. Possible host-to-host binding through XTR between the mobile node and the client system The topology of the test bed is shown in Figure 1. An image of the active airport can be found in Figure 1.

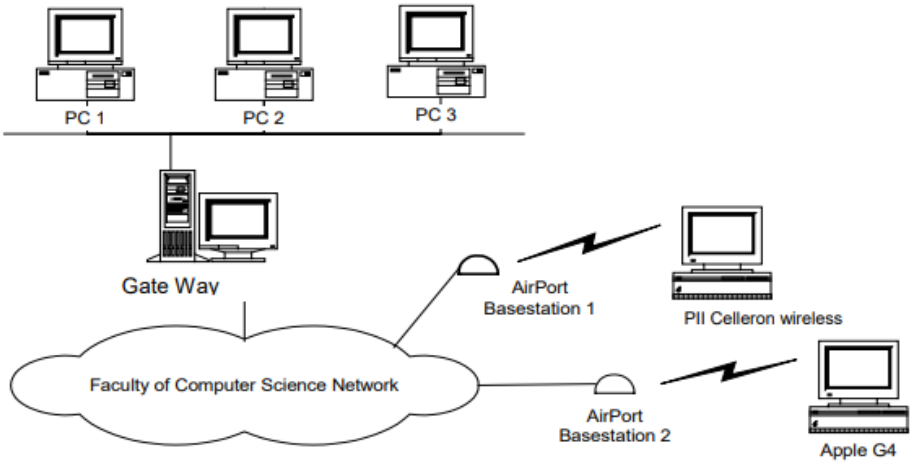

Fig.1 Network Topology

.

Fig. 2 hugs cs dal.ca

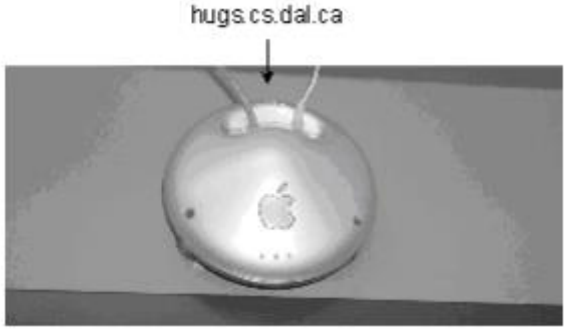

Fig. 2 hugs cs dal.ca

System functionality:

C is the mother language for the two-part XTR port. apps that use the free lip.h library for very lengthy numbers in addition to using segments from the free XTR implementations offered by Lenstra and Verheul [15]. The client (xtrClient.c) and server components of the software Through the wireless network, the client system is developed (xtrServer.c). Both server and the client application operations are shown in Figures 3 and 4.

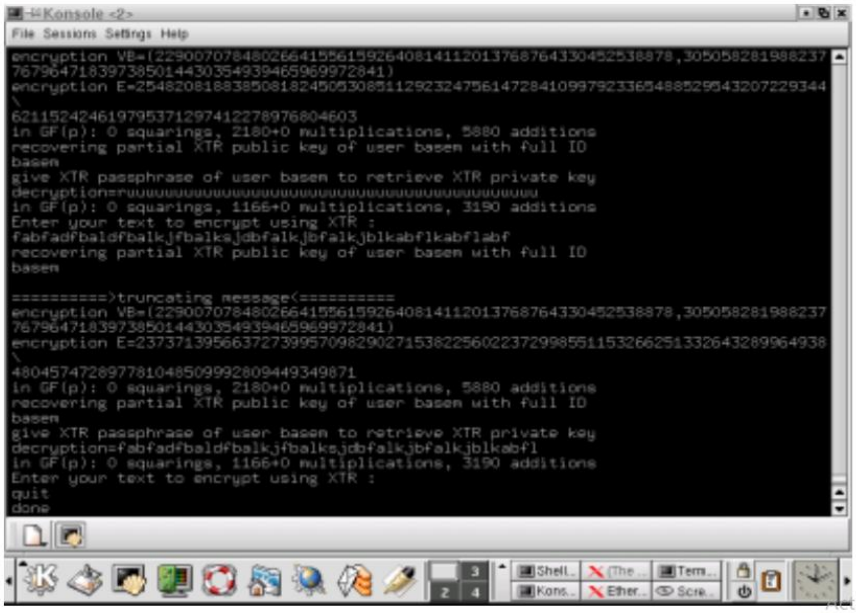

Fig.3 XTR Server Operation

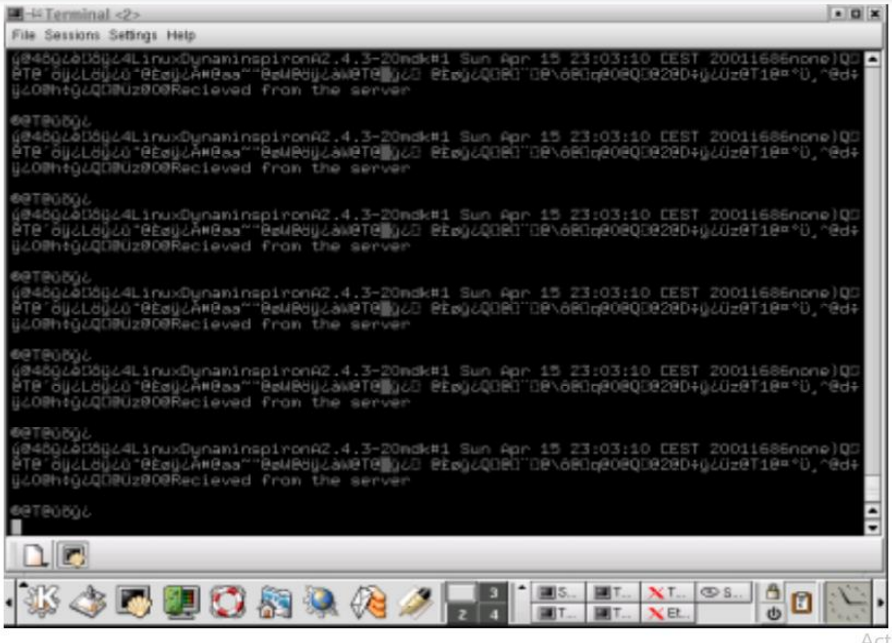

Fig. 4 XTR Client Operation

System Enc. & Dec:

Figure 5 shows how long it takes to encrypt data. It has been demonstrated 30 to 60 microseconds is the required encoding time. using input data of various sizes. This test shows how quickly the wireless system hardware can handle the XTR encryption engine. The graph displays a relationship between data length and CPU encryption time.

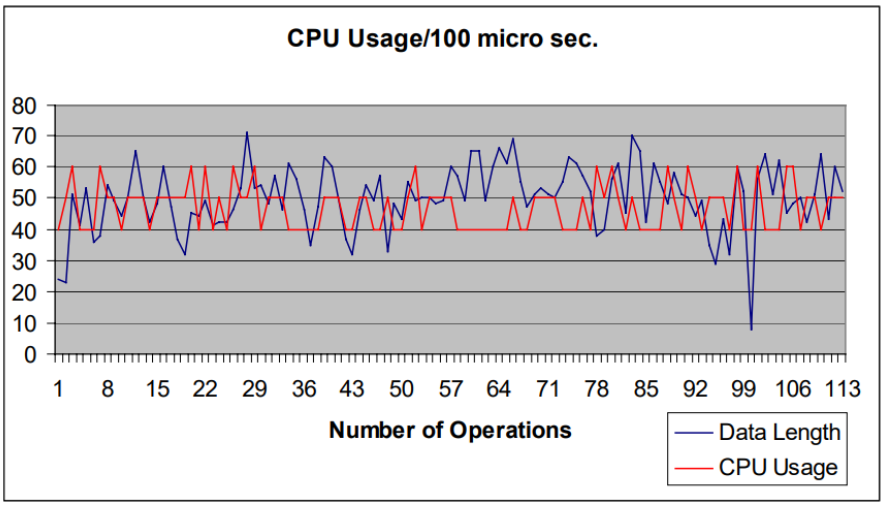

Fig. 5 CPU Usage in data Encryption process

Figure 6 shows the CPU consumption when running the XTR decryption engine. In contrast, utilizing the identical method resulted in encrypted data. It has been Where the time between 30 and 60 microseconds is the ideal bit for decoding. This test shows how quickly the wireless hardware system can decode data using the XTR decryption engine. It contains the generated performance results (in tabular format).

Conclusion:

This study demonstrated the implementation of the XTR public key cryptography system over a wireless network and evaluated its performance. The construction The project has achieved its goal of a robust and portable secure wireless network to execute a variety of wireless applications safely. In the area of computer networking, wireless networks technology has grown in importance.Network applications have the flexibility they require for mobile activities thanks to the adaptability of wireless network devices.

In general, the novel XTR concept, provides a clever method for wireless distributed architecture to reserve communication bandwidth and enhance compute load optimization. resulting in simple and lightweight security deployment.

The research thoroughly examined the theoretical and mathematical underpinnings of the XTR system as well as its wireless network implementation. The XTR public key cryptographic system was employed in this project to increase the security and speed of wireless communication, which is intrinsically insecure., between the weird node and the wireless node (server) a secure tunnel was built using XTR as a wireless security VPN solution.

Contribution of the Project:

This project's main contribution is the performance evaluation and implementation of XTR over wireless networks. The reduction of computing overhead and communication demands is the aim of XTR. The project succeeded in achieving the following objectives:

1- Analyze the theoretical and real-world effectiveness of the XTR public key cryptography system when used over wireless networks.

2- Distributed lightweight wireless security: Implement novel wireless network-based distributed lightweight security techniques. Data that is exchanged wirelessly between nodes is encrypted with the barest of operational needs.

XTR System Pros:

following is a description of the benefits that the wireless network has received from the implemented XTR public key cryptosystem:

1-Lessened computation overhead: XTR offers a 3x decrease in computation overhead.
2- Extending the range of wireless devices: Reducing communication costs and transmitting small, encrypted data files reduces bandwidth usage. This increases the reachability of wireless devices and increases CPU and bandwidth use.
3- Adjustment for wireless device bandwidth: The factor 3 computation takes into account the extra overhead that comes with wireless devices.

References:

[1] U. Varshney, "Recent Advances in Wireless Networking" IEEE Computer, vol. 33, pp. 100-103, June 2000.

[2] L. Korba, "Security System for Wireless Local Area Networks" in Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 1998, vol. 3, pp. 1550-1554.

[3] S. F. Russell, "Wireless network security for users", in proc. IEEE international conference on information technology: coding and computing, 2001, pp 172-177 April 2001 .

[4] Donald Davies and Wyn Price: "Security for Computer Networks", John Wiley, 1989.

[5] Bruce Schneier: "Applied Cryptography", second edition, John Wiley & Sons, 1996Cryptography book.

[6] Douglas R. Stinson, "Cryptography, Theory and Practice", CRC Press, 1995 .

[7] SSL cryptography corner, http://www.ssh.com/tech/crypto/algorithms.cfm, last visited April 17, 2002. [Online] .

[8] A. Lenstra, E. Verhuel "An overview of the XTR public key system", in proc. Public key cryptography and computational number theory conference, 2001.

[9] A. Lenstra, E. Verhuel " The XTR public key system", in proc. Cryptography- Crypto 2000 lecture notes in computer science, sping-verlag. 2000 pp. 97-101 .

[10] E. Verhuel, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystem", Proc. of Eurocrypt 2001.

[11] A. J. Menzes, "Comparing the security of ECC and RSA", manuscript, 2000, available at www.cacr.math.uwaterloo.ca/~ajmeneze [Online] .

[12] A. Odlyzko, "Discrete Logarithms", The past and the future, Designs, Codes and Cryptography, 19 (2000), 129-145.

[13] Lenstra, Verhuel XTR crypgographic system http://ecstr.com website, last visited April 17, 2002. [Online] .

[14] Apple Tech Info Library, "Airport: Difference between DSSS and FHSS" [Online], Available at: http://til.info.apple.com/techinfo.nsf/artnum/n58530 .

[15] Arjen K. Lenstra, 1989-2000, free lip.h, lip.c, long integer package, version 1.1. http://ecstr.com [Online].