Word Count: 1271

Plagiarism Percentage 4%

Matches

1 **World Wide Web Match**
View Link

2 **World Wide Web Match**
View Link

3 **World Wide Web Match**
View Link

4 **World Wide Web Match**
View Link

5 **World Wide Web Match**
View Link

Suspected Content

Survey on Elliptic Curve Cryptography A R PRASHANTH computer science dept. PES University bangalore, India prashanthathunt@gmail.com Abstract—Elliptic Curve Cryptography has been studied since 1986 for academic and industrial purposes . elliptic Curve Cryptography provides more security on a shorter key size .It is mainly used in public key cryptography. It is widely used in Internet of Things (IoT) , in military communication , to exchange symmetric key between parties there are many applications . it takes less memory and is faster to compute . it can be used for low end devices . In this era everyone wants it to be fast , instant and also very secure hence Elliptic Curve Cryptography is coming up as it provides high security and smaller key size . still to find make it more efficient it has to be made hardware accelerate . it has to be made or built inside every hardware unit (if required) so that we get fast , efficient output . we need to have a light weight Elliptic Curve Cryptography as well for better efficiency . although it may provide little less security. In this survey paper we are going to discuss on, how the Elliptic Curve can be used in Cryptography , why it is important to use hardware accelerators to accelerate the speed of encryption and decryption process . we will see how the authentication scheme of Elliptic Curve cryptography. What are the various fields Elliptic Curve cryptography is been used like

Elliptic Curve Diffie- Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) which 3 is used in bitcoin currently Index Terms—ECC, elliptic Curve, cryptography I. INTRODUCTION

Elliptic curve cryptography uses elliptic curve theory to build a public key 5

encryption technique which is fast , more efficient and smaller in key size . It is used mostly with a combination of encryption methods

like Rivest–Shamir–Adleman (RSA) or Diffie-Hellman key exchange 4

.a 160 bit ecc key can provide as much as 1024bit key size RSA/DSA that is almost 1:3 ratio as we go higher 224 bit of ecc provides 2048 bits of RSA/DSA which is almost 1:6 ratio as we increase the number a 521bit ecc give as much as security as a 15360 bit RSA which his 64 time more secure and dealing with 15360bit of number is a lot of computation to handle . hence Elliptic curve cryptography is used to make it more secure and fast with lesser key size . The main objective of Elliptic curve cryptography let say cryptography in this case is to protect our data using different cryptography algorithms . so the cryptographic algorithm we use should be feasible should cost less than the original data cost for sending it . What I meant to say is that protecting the data should not cost more than the original data itself . Although Elliptic curve cryptography uses less power and it is very efficient than other methods we still need to make it more feasible and faster by using hardware accelerators which can give support at hardware level . Elliptic curve cryptography is mainly used in communi- cation of data where privacy or we can say protecting the data is more important . But in this digital world everybody’s first priority is privacy so we need to have a better faster and reliable system . In future there maybe a better solution for this problem but currently Elliptic curve cryptography combined with other methods like RSA or diffie hellman key exchange methods make the current know techniques feasible , more efficient which uses less computation power and provides higher security . such examples are Elliptic Curve Digital Signature Algorithm(ECDSA) which is currently used by bitcoin (a cryptocurrency invented by Satoshi Nakamoto in 2008 and it was started in 2009) to ensure the transaction are made to the rightful owners and the funds can only be spend by the owner and owner only . It uses just 256 bits unsigned int that is 32 bytes Thanks to elliptic curve cryptography for providing far more security than a 15000+ bits rsa could provide . Elliptic Curve Digital signature algorithm is faster than RSA for signing and decryp- tion . so it’s a win-win situation . Another example is the Elliptic curve Diffie Hellman - it’s the same as the Diffie Hellman protocol but uses the Elliptic curve for better security and it’s faster too. II. ALGORITHM USED WITH SECURITY PARAMETER

Weierstraß equation of elliptic curve E defined over K using affine coordinates is 2

E: y2 + a1xy + a3y = x3 + a2x2 + a4x + a6 where a1,a2,a3,a4, a5 ,a6 belongs to K 1

1st we will briefly talk about the mathematics of elliptic curve general properties of Elliptic Curve general formula of Elliptic curve is E:y2 = x3 + ax + b general Elliptic curve diagram calculating multiples of G in an Elliptic curve To calculate the multiple of G drew a tangent to at that point. See where it intersects the curve . Draw a parallel line in y axis see where it intersects the curve . There you go u have the the next multiple of

G . It may look very simple because its the basic example . but as we make the equation complex it is practically impossible to trace 150bits length of multiple of G. What makes it so secure is that it is easy to calculate multiples of G but where as going back is very hard . It is computationally very hard to go back from a multiple of G to G(starting point) III. WORKING Hardware implementation will has to be done in chip level or we can say nano level so that it can have high degree of performance then what we see using normal CPU or GPU or even TPUs. It should not be a separate unit from the rest of the unit or like a chip . It has to be mounted to the CPU or any kind of microprocessors so that there will no latency in sharing the data between our hardware accelerator and the output stream . Fig. 2. Algorithm Scheduler Fig. 1. Practical Elliptic curve Fig. 3. Multiplier architecture Those are the working diagram of hardware implementation of Elliptic curve cryptography IV. VERIATIONS WITH RESPECT TO MAIN ALGORITHM There are in total 3 algorithms will be proposed in this paper V. APPLICATIONS In day to day scenario public key cryptography is most im- portant as people are demanding for privacy of their personal data. As the digit world is increasing their demand on data , the cybersecuiry plays a important role in it to protect the data of individual . So every application which has to communicate over a an unreliable network need public key cryptography to maintain data privacy . Performaces of RSA cryptographic algorithms Vs ECC on 90MHz pentium chip VI. CONCLUSION Considering the performance of the hardware accelerator we can say that it can be used for every communication devices which is in need of data privacy . which provides you higher performance. The only way now is to make the Elliptic curve cryptography more faster sacrificing flexibility is to make it in hardware level . We saw that hardware support can really boost the performance of Elliptic curve cryptography . Is Elliptic curve cryptography quantum resistant ? In fact yes . so Elliptic curve cryptography is not going anywhere for at-least few decades so it is better to make it in hardware level so that it can out-stand and can be used by everyone without worrying about the performance or the cost of encryption over the cost of data . To truly minimise the cost of encryption hardware implementation is necessary . ACKNOWLEDGMENT Thanking the PES Institution and therefore the Teachers for his or her support, Guidance and encouragement. REFERENCES Fig. 4. Performance Table on different hardware