RESEARCH ARTICLE OPEN ACCESS

A Secure signature with GPU facilitation

S.Chithra[1], E.Dilipkumar[2]
1PG Student, 2Associate Professor
1, 2, Department of MCA, Dhanalakshmi Srinivasan College of Engineering and Technology

Abstract:

Now a days we use digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer. There by we use Elliptic Curve Digital Signature Algorithm (ECDSA) for communicating data between Research Institution and their branches for a research report or any research in the university. This is an elliptic curve analogue of the Digital Signature Algorithm. Unlike the other ordinary discrete logarithm problem and the integer factorization problem, no sub exponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key bit is substantially greater in an algorithm that uses elliptic curves. If co-branch discovered anything regarding research means it should get approved by main branch for approval. While sending that report to their higher officials it should be very confidential. That information should not be hacked by any intermediate persons. For that, the technique which is used to encrypt the information is called Elliptical Curve Cryptography (ECC), using this technique the user could send their information in a very secure manner.

Keywords — - -

I. Introduction

SCOPE OF THE PROJECT

The project aims in providing security to the data send between a co-Research branch and research institution. This makes the data a trap door when there is loss of key i.e. only encryption is possible in easy way and decryption is impossible without the key even by the sender. It can be used mainly for secret project completion purpose in competition between the institutions in any case the data would not be trapped.

Elliptic Curve Digital Signature Algorithms (ECDSA) have recently come into strong consideration, particularly by the standards developers, as alternatives to established standard cryptosystems such as the integer factorization cryptosystems and the cryptosystems based on the discrete logarithm problem. Crypto-algorithms are always the most important core tool in security applications.

EXISTING SYSTEM

In many areas while transmitting the data between any users will be using the DSA algorithm or Digital signature algorithm. They also will have encrypting, digesting of message, and rebuilding the message by decryption. People use public-key cryptography to compute digital signatures by associating something unique with each person. When public-key cryptography is used to encrypt a message, the sender encrypts the message with the public key of the intended recipient. A digital signature is an electronic analogue of a hand-written signature that allows a

receiver to convince a third party that the message is in fact originated from the sender. Digital signatures are much more secure than hand-written signatures.

Diffie and Hellman introduced a key exchange protocol in their first publication along with their ideas of public key cryptography. Their protocol is known as Diffie-Hellman key exchange. Discrete Logarithm (DL) Schemes base their security on the intractability of the (ordinary) discrete logarithm problem in a finite field.

Problems in Existing System

- They have higher level of computing cost.
- The mathematics of the RSA algorithm has not been comprised, per second instead, computational brute-force has broken the keys. The defense is "simple" - keep the size of the integer to be factored ahead of the computational curve.

PROPOSED SYSTEM

We propose an approach to use the ecliptic curve cryptography to transmit between two users. They base their security on intractability of the elliptic curve discrete logarithm problem. An example is the Elliptic Curve Digital Signature Algorithm. Elliptic curve cryptography constitutes a fundamental and efficient technology for public key cryptosystems. Mathematicians have studied elliptic curves for more than a century. Besides their recent cryptographic applications, they are used in primarily testing and integer factorization. The digital signature schemes can provide data integrity, data origin authentication and non-repudiation, but not used to provide confidentiality. There are two processes:

- Generation of signature and
- Verification of signature.

ECDSA Signature Generation

The user A signs the message m using the following steps as shown below.

- Select a pseudorandom integer $k \in [1, n - 1]$.
- Compute $k \times P = (x_1, y_1)$ and $r = x_1 \bmod n$.
- If $x_1 \in$, GF (2^k), it is assumed that x_1 is represented as a binary number. If $r = 0$ then go to Step 1.
- Compute $k^{-1} \bmod n$.
- Compute $s = k^{-1}(H(m) + d * r) \bmod n$. Here H is the secure hash algorithm SHA-1.
  If $s = 0$ go to Step 1.
- The signature for the message m is the pair of integers (r, s).

ECDSA Signature Verification

The user B verifies A's signature (r, s) on the message m by applying the following steps as shown below

- Verify that r and s are integers in the interval [1, n-1].
- Compute $c = s^{-1} \bmod n$ and H(m).
- Compute $u_1 = H(m) * c \bmod n$ and $u_2 = r * c \bmod n$.
- Compute $u_1 \times P + u_2 \times Q = (x_0, y_0)$ and $v = x_0 \bmod n$.
- Accept the signature if $v = r$.

Advantage

- The key generated from this algorithm is so longer than the key generated from other algorithm.
- It has more security because of its bit length.
- It has less latency than the DSA.
- It has high throughput due to the use of GPU to generate its random key.

- Smaller key size
- Faster than RSA

ALGORITHM

Signature Generation

1. Calculate e=HASH(m) , where HASH is a cryptographic hash function, such as SHA-2.
2. Let z be the Ln leftmost bits of e, where Ln is the bit length of the group order O.
3. Select a cryptographically secure random integer k from [1, n-1].
4. Calculate the curve point (x , y)=k*g;
5. Calculate r=x1%n. If r=0, go back to step 3.
6. Calculate s=1/k (z + rdA) % n. If s=0, go back to step 3.
7. The signature is the pair (r, s).

VERIFICATION

1. Check that QA is not equal to the identity element O, and its coordinates are otherwise valid
2. Check that QA lies on the curve
3. Check that n*Qa = O.

After that, follows these steps:

1. Verify that r and s are integers in [1,n-1]. If not, the signature is invalid.
2. Calculate e=HASH(m), where HASH is the same function used in the signature generation.
3. Let z be the Ln leftmost bits of e.
4. Calculate w=1/s mod n.
5. Calculate u1=zw mod n and u2=rw mod n.
6. Calculate the curve point (x1,y1)=u1*G+U2*QA.
7. The signature is valid if r=x1 mod n, invalid otherwise.

TECHNICAL GLOSSARY

Security as service

Security as a service (SECaaS) is a business model in which a large service provider integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own, when total cost of ownership is considered.

Digital Signature

A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

Elliptic curve

In mathematics, an **elliptic curve** is a plane algebraic **curve** defined by an equation of the form y 2 = x 3 + a x + b {\display style y^{2}=x^{3}+ax+b} that is non-singular; that is, its graph has no cusps or self-intersections.

GPU

In a personal computer, a GPU can be present on a video card, or it can be embedded on the motherboard or in certain CPUs on the CPU die. The term GPU was popularized by Nvidia in 1999, who marketed the GeForce 256 as "the world's first GPU", or Graphics Processing Unit.

SCREENSHOT

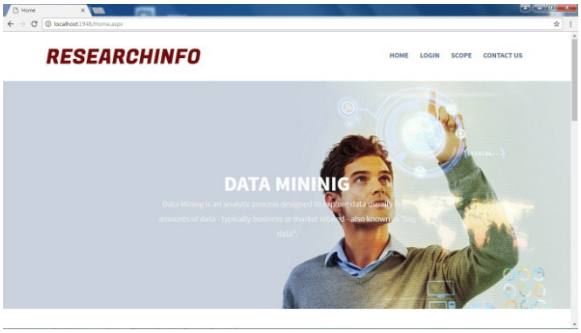

Fig. 1 Home Page

Fig. 2 Login Page

Fig. 6 File Transfer Page

Fig. 3 Registration Page

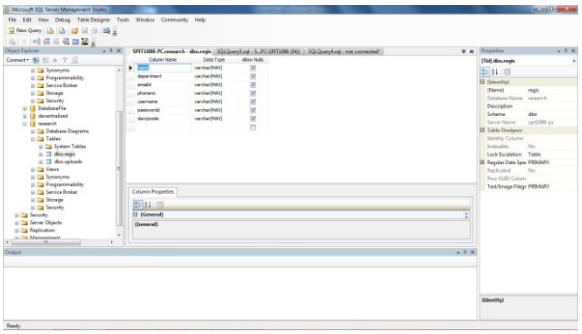

Fig. 7 Registration Page

Fig. 4 After Login

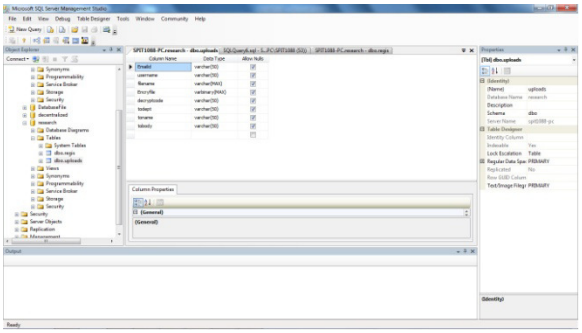

Fig. 8 File Transfer Table

Fig. 5 Profile Page