Tech Juris

A White Paper prepared for
Asian School of Cyber Laws
www.asianlaws.org

```
3048 0241 00C0 324
68E1 9E52 7EB1 E8F
84BF D79D 1106 56F
6512 C8FE E421 1A3
2AC4 B955 FCD2 0F0
458C B195 4C4F 6C3
CA00 B0FF CADC AFA
```

An Introduction to Blind Digital signatures

ASCL White Papers can be downloaded from:
www.asianlaws.org/whitepapers

Tech Juris
The Technology Lawyers
www.techjuris.com

ASCL-WP-IS-Tec-DS-02

Introduction

A major drawback of electronic commerce is the lack of privacy. Every online transaction you make is recorded and a detailed report on your spending habits can be easily compiled for the benefit of spammers, your enemies and even the income tax department!

The need for anonymous electronic transactions is satisfied by Blind Signatures, which enable digital cash systems. These systems do not reveal any information about the spender and in this way are similar to cash.

Blind signatures provide a system for signing electronic data in such a way that the signature can be authenticated without revealing the identity of the person on whose behest it was signed.

Like most information security concepts, blind digital signatures depend upon the assumed existence of "one-way functions". Simply put, a one-way function is a function that is mathematically feasible to compute, but is mathematically infeasible to inverse i.e. computing f***(x)*** given ***x***, is feasible, but for a given ***y*** computing an ***x*** such that ***f(x) = y*** is infeasible.

Two such one-way functions are the multiplication of primes and discrete exponentiation.

The function for the multiplication of primes computes

$$N = P*Q,$$

where ***P*** and ***Q*** are prime numbers.

So, to invert this function you must factor integers that are the product of two prime numbers. Although computers can easily multiply 250 digit primes, it will take the fastest of computers billions of years to factor a 500-digit number known to be the product of two primes!

Discrete exponentiation functions produce a triple ***(p,g,x)*** from the triple ***(p,g,e)***, where ***x*** is congruent to g^e ***modulo p***. The inverse of this function (i.e the unique ***e*** such that ***x*** is congruent to g^e ***modulo p***) is known as the discrete logarithm of ***x*** with respect to ***(g, p)***. Even the fastest of computers are unable to compute this discrete logarithm in a reasonable amount of time.

"Trapdoor functions" are special cases of one-way functions that are invertible with the possession of some extra information i.e., the trapdoor.

Principles that make Blind Signatures Secure

To be considered secure, a blind signature must provably hide the identity of the holder of the signature. Only then will the signature ensure that the anonymity of the holder of the signature is retained. This is known as the **blindness property**.

A blind signature must also be provably infeasible to forge. A forger must be unable to forge or generate a valid signature even if he collects a number of valid signatures. This is known as the **non-forgeability property**.

The proofs of the security of digital signatures can be classified into two major categories: Complexity-based proofs and proofs based on a random oracle model. It has been proven that complexity-based proofs are stronger than the proofs based on the random oracle model.

Common Electronic Cash Applications

Blind digital signatures are used in several applications including digital cash systems, electronic voting systems etc. In this White Paper we will discuss their application to digital cash.

Traceable Digital Cash

By nature, Digital Signatures are a method for authenticating electronic messages. The transaction is as under:

- The signer composes the electronic record that is to be signed
- The signer then creates his digital signature for the record by using his private key (in reality it is not the entire electronic record itself but its hash result that is used to create the digital signature)
- The signer sends the electronic record and the digital signature to the recipient
- The recipient uses the signer's public key to verify whether the contents of the electronic record have been tampered and whether the purported signer has in reality signed the electronic record.

In a traceable digital cash system, the transaction would be as follows:

- The bank's customer (say Pooja) applies for digital cash (say Rs. 500)
- The bank deducts Rs 500 from Pooja's account and issues her an electronic record containing a number (say 102345987).

- This electronic record is signed with the bank's 500 rupee private key (the bank has a different key pair for each denomination of currency that it issues)

- This electronic record is now a 500 rupee digital coin bearing number 102345987.

Armed with her this digital coin Pooja can purchase goods and services online. Suppose she visits the website of Shyam, a software vendor and decides to buy an anti-virus software priced at Rs 500. The transaction would proceed as follows:

- She would place an order with Shyam and submit her 500 rupee digital coin.

- Shyam (or rather his computer) would immediately verify the authenticity of the digital coin using the bank's public key (which he would obtain from the bank's servers in real time).

- Shyam's computer would also check whether the particular coin number has been reported to the bank as being used.

- In this case, since the coin is being used for the first time, there would be no trouble and the transaction would end with Pooja being allowed to download the software and the bank being informed that the particular coin has been used up.

- At the end of the day (or business period), Shyam would submit all the coins to the bank and his account would be credited with the relevant amount.

Pooja would be unable to use the coin again as it has been reported to the bank in real time that the coin has been used.

This system provides security for all the parties to the transaction, namely the bank, the vendor and the customer.

- The bank's digital signature ensures that the customer knows that it is a valid digital coin.

- The vendor is able to verify that the digital coin is legal tender

- The bank can ensure that the note is not spent more than once.

The drawback of this system is that there is no privacy for the customer. At the click of a button the bank can ascertain the customers spending habits.

Chaum-Fiat-Naor On-Line Anonymous Electronic Cash System

Untraceable Digital Cash provides anonymity to the spender. David Chaum is called the father of blind signatures and in particular of anonymous digital cash as he was the first to introduce the topic and the first to come up with such an untraceable and unlinkable digital cash scheme.

The Chaum-Fiat-Naor system maintains the anonymity of the user of the cash, but if the user tries to "cheat" the system his/her identity is revealed. In other words, Pooja and the bank collectively create a bank note that is:

- impossible to forge and
- protects the identity of Pooja

This scheme is based on a blinding of the RSA signature. The system functions as follows:

- Pooja chooses a number ***x*** from the bank, where ***x*** is a serial number of the electronic bank note that she wants. The bank keeps a record of all the serial numbers ***(x)*** that it releases.

- Pooja then applies a one-way function ***f()*** to ***x*** i.e., Pooja calculates ***f(x)***. She doesn't send this answer to the bank.

- Pooja chooses a random number ***r*** and calculates $f(x)*r^3$. This is done in order to blind the signature.

- The resulting answer is sent to the bank, which takes the cube root of that answer i.e. the bank calculates $r*f(x)^{1/3}$.

- As the bank only receives the answer it does not know the value of either ***r*** or ***f(x)***.

- The bank verifies Pooja's identity through her identity document and debits her account by the value of the electronic bank note.

- The bank then, sends its answer back to Pooja who divides that answer by her random number ***r*** to obtain $f(x)^{1/3}$.

- Her digital cash is thus $(x, f(x)^{1/3})$. Pooja now has a piece of electronic cash that could only have been signed by the bank and that will maintain her anonymity.

- Pooja's identity is hidden from the bank due to the random number ***r*** that she applies to the one-way function and takes off when she receives her bank note. This blinding number is what maintains her secrecy.

- The bank will take the n^{th} root of the bank note depending on what denomination of currency it is. For example a Rs. 10 note would be $^{1/3}$, Rs. 20 note would be $^{1/5}$, a Rs. 50 note would be $^{1/7}$ and a Rs. 100 note would be $^{1/11}$.

- When Pooja visits Shyam's website and spends her anonymous digital cash, Shyam can verify the digital signature on the electronic bank note and so will accept it.

- Shyam sends ***x***, the serial number of the electronic note, to the bank who will cross it off its list of serial numbers. If the serial number ***x*** is not on the bank's list Shyam will know that Pooja is trying to defraud him by spending the same electronic note again.

- This process ensures that an electronic bank note is not spent more than once. This is an online-system, as the bank has to be online at all times to make this system possible.

Asian School of Cyber Laws

Pune | Bangalore | Kolkata | Nagpur

OUR SERVICES

Information Security

- Training
- Consultancy
- White papers
- Workshops

Technology Law

We provide training, consultancy, workshops, and white papers in the following areas of law:

- Media Laws
- Semi-conductor Law
- Intellectual Property Law
- PKI Law
- Cyber Law
- Drafting
- Software valuation
- Audits
- Arbitration
- E-contracts

In addition, we conduct a Diploma course in Information Technology Law.

Cyber Crime Investigation

- Training
- Consultancy
- Search and seizure operations
- White papers
- Certified Courses

CONTACT US

Regd. Office

6, Rajas, Above IDBI, Pashan Road, Pune 411008
Ph: 91 20 5890894 / 95
Fax: 91 20 5675600

Email: info@asianlaws.org
URL: www.asianlaws.org