Using bilinear maps and its applications for one forward-secure signature scheme

Pin-Chang Su,
Department of Electrical Engineering, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-San, Tao-Yuan 333, Taiwan, ROC

Henry Ker-Chang Chang
Graduate Institute of Business Administration, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-San, Tao-Yuan 333, Taiwan, ROC

Abstract
In this paper, a method for the automatic handwritten signature verification (AHSV) is described. The method relies on global features that summarize different aspects of signature shape and dynamics of signature production. For designing the algorithm, we have tried to detect the signature without paying any attention to the thickness and size of it. The results have shown that the correctness of our algorithm detecting the signature is more acceptable. In this method, first the signature is pre-processed and the noise of sample signature is removed. Then, the signature is analyzed and specification of it is extracted and saved in a string for the comparison. At the end, using adapted version of the dynamic time warping algorithm, signature is classified as an original or a forgery one.

Keywords: Off-line handwritten signature verification; Optimal DTW algorithm; Pattern recognition

Introduction
Encryption emerged from the Crypt and Graphy. The secret data are hidden within science studies. Knowledge of classical and modern cryptography is divided into two major categories of Modern Cryptography and Classical Cryptography whose definition slightly differs from that presented above. Today, cryptography is considered a branch of computer science and math. It is also closely related to the science of information theory, computer security and engineering. In today’s world, the growth of the Internet and other communication facilities, ensuring the safety and health of ties is getting more and more. Complexity of human relationship such as trust in electronic relationships does not exist; hence, the need for knowledge of the conditions guarantees that relationship. With this definition, the science of cryptography, secure communications, so that no encryption, there are no guarantees in the world of digital communications. Generally, classical cryptography encryption (Encryption) is a very important part of the course is limited to modern cryptography is also accounted for. Reversing this process is when converting ordinary information, encoding and decoding data, indecipherable and clean (Decryption). It is clear that the encoding is important because it will always encrypted data and plays an important role in human life. A digital signature is a type of asymmetric cryptography. The letter is signed by the sender is not forged. Digital signatures in many respects are similar to traditional signatures that are based on asymmetric cryptograph, digital signature schemes are the files must be properly effective. Digital signatures should also be undeniable signatures in order to create the sense that not a signatory to the private key remains secret person. Messages signed with a digital signature to provide a bit of that. Such as email, contracts or messages that are sent through the rules of other encodings. Digital signatures are often used to accomplish electronic signatures. In some countries, such as America and EU, electronic signatures have their own rules.
In 1996 the United Nations published the UNCITRAL Model Law on Electronic Commerce. The model law was highly influential in the development of electronic signature laws around the world, including in the US. A digital signature is a type of asymmetric cryptography. When a message is sent through an insecure channel, a digital signature that can be properly completed claim for a recipient reason to believe the sender to the recipient or in other words digital signature can be ensure that which is signed by the sender and not the fake letter. Digital signatures are handy in many respects similar to traditional signatures, digital signatures properly done is very difficult from a manually signed. Digital signatures are based on asymmetric cryptographic schemes and must be done properly to be effective. Messages signed with a digital signature to provide a bit of that such as email, contracts or messages that are sent through the rules of other encodings. Digital signatures are often used to accomplish electronic signatures. In some countries, such as America and EU, electronic signatures have their own rules. However, laws concerning electronic signatures do not make clear whether the digital signatures are not properly handled or what their significance is meant. In general, the rules are not clear to users and sometimes lead them astray.

2.1. Digital Signature scheme
A digital signature scheme is a quintuple \((P, A, K, S, V)\) the following conditions are fulfilled:
- \(P\) is a finite set of possible messages.
- \(A\) may be a finite set.
- \(K\) is the key space. Finite set of possible keys. For every \(k \in K\), a signature algorithm \(\text{sig}_k \in S\) and a corresponding verification algorithm \(\text{ver}_k \in V\) available. Whatever: \(P \times A \rightarrow \{\text{true, false}\} \& \text{ver functions, Such that for each text and each } y \in A \times x \in P\) following conditions is established.

\[
\text{ver}_k (x, y) = \begin{cases} 
\text{true} & \text{if } y = \text{sig}_k(x) \\
\text{false} & \text{if } y \neq \text{sig}_k(x)
\end{cases}
\]

2.2. Digital signature features
Some features of digital signature are as follows:
- You cannot be falsified.
- Recipients must be able to validate signatures.
- Signers should be able to later deny their signature.
- Digital signatures cannot be fixed, but a function of the input text that is supposed to be signed.

2.3. RSA key generation algorithm
The digital signature scheme from the RSA public key encryption system arose. This scheme is based on the hard problem of decomposing an integer. Signer chooses two prime numbers \(p \& q\) and \(n \& \phi (n)\) can be calculated. He also chooses a random number and if the number \(b) ba \equiv 1 \pmod{\phi}\) can be calculated.

The pair \((n, b)\) public key and private key RSA signatures are RSA signature generation algorithm is set to be signed text. Therefore, one of the algorithms used to generate the signature \(s\). RSA signature verification algorithm is supposed to be the signature \(S\) on \(m\) text. Therefore, one can use the following algorithm.

\[
M = s^b \pmod{n}
\]

If the above relation is satisfied, otherwise the signature is valid and invalid signatures.

Features of RSA
- digital signature RSA RSA encryption works exactly the opposite
- too slow
- Review the use of functions is not an appropriate instrument for signing long messages.

2.4. Rabin signature
The Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. However the Rabin cryptosystem has the
advantage that the problem on which it relies has been proved to be as hard as integer
factorization, which is not currently known to be true of the RSA problem. It has the
disadvantage that each output of the Rabin function can be generated by any of four possible
inputs; if each output is a ciphertext, extra complexity is required on decryption to identify
which of the four possible inputs was the true plaintext. The process was published in
January 1979 by Michael O. Rabin. The Rabin cryptosystem was the first asymmetric
cryptosystem where recovering the entire plaintext from the ciphertext could be proven to be
as hard as factoring.

3. The Rabin Cryptosystem
The Rabin Cryptosystem is an asymmetric key encryption based on number-theoretic
problems related to the hardness of factoring. For that reason, some number theory has to be
present before we can explain the cryptosystem. In this section the basic mathematical
concepts are needed to understand the cryptosystem are introduced. Some examples will be
shown for a better comprehension.

3.1. The Chinese Remainder Theorem
The Chinese remainder theorem is a result about congruences in number theory. It was first
published in the 3rd to 5th centuries by Chinese mathematician Sun Tzu. In its basic form
the Chinese remainder theorem will determine a number \( n \) that when divided by some given
divisors leave given remainders. The original form of the theorem is contained in the 5th-
century book *Sunzi’s Mathematical Classic*.

(Suppose \( n_1, n_2, \ldots, n_k \) are positive integers that are pairwise coprime. Then, for any given
sequence of integers \( a_1, a_2, \ldots, a_k \), there exists an integer \( x \) solving the following system of
simultaneous congruences.

\[
x \equiv a_1 \pmod {n_1} \\
x \equiv a_2 \pmod {n_2} \\
\vdots \\
x \equiv a_k \pmod {n_k}
\]

Furthermore, all solutions \( x \) of this system are congruent modulo the product, \( N = n_1n_2 \ldots n_k \).
Hence \( x \equiv y \pmod {n_i} \) for all \( 1 \leq i \leq k \), if and only if \( x \equiv y \pmod N \).

Sometimes, the simultaneous congruences can be solved even if the \( n_i \)’s are not pairwise
coprime. A solution \( x \) exists if and only if:

\[
a_i \equiv a_j \pmod {\gcd(n_i, n_j)} \quad \text{for all } i \text{ and } j
\]

All solutions \( x \) are then congruent modulo the least common multiple of the \( n_i \).

Sun Tzu’s work contains neither a proof nor a full algorithm. What amounts to an algorithm
for solving this problem was described by Aryabhata. A modern restatement of the theorem
in algebraic language is that for a positive integer \( n \) with prime factorization
\( p_1^{r_1}p_2^{r_2} \ldots p_k^{r_k} \) we have the isomorphism between a ring and the direct product of its prime power parts:

\[
\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \mathbb{Z}/p_2^{r_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{r_k}\mathbb{Z}
\]

The theorem can also be restated in the language of combinatorics as the fact that
the infinite arithmetic progressions of integers form a Helly family.

**Theorem 1**: Let \( r \) and \( s \) be positive integers which are relatively prime and
let \( a \) and \( b \) be any two integers. Then there is an integer
\( N \) such that:

\( N = a \mod r \) and \( N = b \mod s \).

Moreover, \( N \) is uniquely determined modulo \( r \cdot s \). The theorem can be generalized as follows.

Given a set of simultaneous congruences:

\[
x \equiv a_i \pmod {m_i}
\]

\( N \) such that:

\( N = a \mod r \) and \( N = b \mod s \).

Moreover, \( N \) is uniquely determined modulo \( r \cdot s \). The theorem can be generalized as follows.

Given a set of simultaneous congruences:

\[
x \equiv a_i \pmod {m_i}
\]
for $i = 1,..., r$ and for which the $m_i$ are pairwise relatively prime, the solution of the set of congruences is:

$$x \equiv a_1 b_1 \frac{M}{m_1} + \ldots + a_r b_r \frac{M}{m_r} \mod M$$

$$M = m_1 m_2 \ldots m_r$$

and $\frac{M}{m_i} \cdot b_i \equiv 1 \mod m_i$.

### 3.2. Quadratic Residues

The discussion of quadratic residues will be divided into two parts: quadratic residues modulo a prime $p$, and the quadratic residues modulo a composite $N$, where $p$ and $q$ are odd primes and $N = pq$.

**Quadratic Residues Modulo a Prime:** Let $G$ be a group. An element $y \in G$ is called quadratic residue if there exists another element $x \in G$ such that:

$$x^2 = y$$

If there is no such $x$, then $y$ is called a quadratic nonresidue. In this case $\text{QR}_q$ denotes the set of quadratic residues of a given group and $\text{QNR}_q$ the quadratic non-residues. Also, when the given group is $\mathbb{Z}_q$ for a Prime $q$, the element $y$ is a quadratic residue if:

$$x^2 = y \mod q$$

Example: Let’s go to compute the quadratic residues mod 11. Computing the range of numbers $0 < x < \frac{q}{2}$ is enough for reason of symmetry:

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n^2 \mod 11$</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

- $1 \to 1^2 = 1 \to 1 \mod 11 = 1$
- $2 \to 2^2 = 4 \to 4 \mod 11 = 4$
- $3 \to 3^2 = 9 \to 9 \mod 11 = 9$
- $4 \to 4^2 = 16 \to 16 \mod 11 = 5$
- $5 \to 5^2 = 025 \to 25 \mod 11 = 3$

So, we can conclude that the elements belonging to $\mathbb{Z}_q^*$ which are quadratic residues mod 11 are the set of elements $\{1, 3, 4, 5, 9\}$ and the non-quadratic residues mod 11 the elements $\{2, 6, 7, 8, 10\}$.

**Theorem 2:** Let $q > 2$ be a prime. Then every quadratic residue has exactly two square roots and the numbers of solutions are:

- 1 solution if $y = 0$.
- 2 solutions if $y \neq 0$.

Proof: Let $y \in \mathbb{Z}_q^*$ be a QR. By definition, there exists an $x \in \mathbb{Z}_q^*$ such:

$$x^2 = y \mod q \text{ and } (-x)^2 = x^2 = y \mod q$$

Furthermore, $-x \neq x \mod q$
If \(-x = x \mod q\) then \(2x = 0 \mod q\) which implies \(q|2x\).
This means that either \(q|2\) or \(q|x\), impossible since \(q\) is prime > 2 and \(0 < x < q\). Therefore \([x \mod q]\) and \([-x \mod q]\) must be different elements of \(\mathbb{Z}_q^*\), so \(y\) has at least two square roots.
Now, let \(x, z \in \mathbb{Z}_q^*\) be square roots of \(y\). Then \(x^2 = y = z^2 \mod q\), which means that \(x^2 - z^2 = 0 \mod q\). Hence \((x-z)(x+z) = 0 \mod q\). Since \(q\) is a prime either \(q|(x - z)\) or \(q|(x + z)\). In the first case, \(z = x \mod q\) and in the second case \(z = -x \mod q\), showing that \(y\) has only the square roots: \(\pm x \mod q\).

**Theorem 3:** The number of quadratic residues and quadratic non-residues in \(\mathbb{Z}_q^*\) is equal:

\[
[\text{QR}_q] = [\text{QNR}_q] = \frac{q-1}{2}
\]

**Proof:** Let \(\mathbb{Z}_q^*\) a cyclic group of order \(q \equiv 1\) and let \(g\) be a generator of this group, which means that:

\[
\mathbb{Z}_q^* = \{g, g^2, ..., g^{q-1}\}
\]

As \(q\) is odd, \(q \equiv 1\) must be even. So half of all elements between 1 and \(q - 1\) have an even exponent. Since \(2|j\), being \(j\) an even number, for half of the all elements in \(\{g^1, g^2, ..., g^{q-1}\}\) we have that \(g^i \in \mathbb{Z}_q^*\) for some even integer \(i\). So finally, we can conclude that half of all elements are QR.

Example: If we continue with the previous example, but we compute all numbers, we get:

<table>
<thead>
<tr>
<th>(n)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>(n^2 \mod 11)</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

As we can see, each quadratic equation mod 11 has exactly two solutions. For example, the equation \(x^2 = 4 \mod 11\) has the solutions 2 and 9, or the equation \(x^2 = 9 \mod 11\) has the solutions 3 and 8.

Also, we can see that there are the same number of quadratic residues and quadratic non-residues:

\[
\{1, 3, 4, 5, 9\} \in \text{QR}_{11}
\]

\[
\{1, 3, 4, 5, 9\} \in \text{QNR}_{11}
\]

\[
\frac{(q - 1)}{2} = \frac{(11 - 1)}{2} = 5
\]

One way to express if an element \(y\) is a quadratic or non-quadratic residue mod \(q\) is using the Legendre symbol:

\[
L_q(y) = \begin{cases} +1 & \text{if } y \in \text{QR}_q, \\ -1 & y \in \text{QNR}_q \end{cases}
\]

**Theorem 4:** Let \(q > 2\) be a prime. Then:

\[
L_q(y) = y^{(q-1)/2} \mod q
\]

**Proof:** As we proofed before, a quadratic residue \(x\) modulo \(q\) can be expressed as \(x = g^i\) for some
even integer i and an arbitrary generator g of $z_q^*$. If we suppose now $i = 2j$ with $j$ an integer:

$$x^{\frac{(q-1)}{2}} = (g^{2j})^{\frac{(q-1)}{2}} = g^{(q-1)/2} = 1^j$$

We have shown that $x^{\frac{(q-1)}{2}} = 1 = l_q(x) \mod q$. Now, if $x \in \text{QR}_q$ : $x = g^i$ for some odd integer i.

Let now $i = 2j + 1$. Then

$$x^{\frac{(q-1)}{2}} = (g^{2j+1})^{\frac{(q-1)}{2}} = (g^{2j})^{\frac{(q-1)}{2}} g^{(q-1)/2} = g^{\frac{q-1}{2}} \mod q$$

Now: $(g^{\frac{q-1}{2}})^2 = g^{q-1} = 1 \mod q$

And so $g^{\frac{q-1}{2}} \equiv \pm 1 \mod q$ Since $[\pm 1 \mod q]$ are the two square roots of 1. Since g is a generator, $g^{\frac{q-1}{2}} \equiv -1 = L_p(x) \mod p$.

Example: Let’s go to apply the Legendre theorem to some elements:

$L_{11}(4) = 4^5 \mod 11 = 1 \rightarrow 4 \in \text{QR}_{11}$

$L_{7}(2) = 2^3 \mod 7 = 1 \rightarrow 2 \in \text{QR}_7$

From these propositions, it is possible to derive an algorithm for checking if a determined element y is a quadratic residue or not:

$$y^{\frac{q-1}{2}} \mod q = \begin{cases} +1 & \text{if } y \in \text{QR}_q \\ -1 & \text{if } y \in \text{QN}R_q \end{cases}$$

Example:

$1^5 \mod 11 \leftrightarrow -1 \mod 11 = 1 \rightarrow 1 \in \text{QR}_q$
$2^5 \mod 11 \leftrightarrow 32 \mod 11 = 10 \rightarrow 2 \in \text{QN}R_q$
$3^5 \mod 11 \leftrightarrow 243 \mod 11 = 1 \rightarrow 3 \in \text{QR}_q$
$4^5 \mod 11 \leftrightarrow 1024 \mod 11 = 1 \rightarrow 4 \in \text{QR}_q$
$6^5 \mod 11 \leftrightarrow 724 \mod 11 = 10 \rightarrow 5 \in \text{QN}R_q$

Finally, the quadratic residues follow a property called multiplicative property of quadratic residues. 6

**Theorem 5:** Let $q \geq 2$ be a prime and $x, y \in z_q^*$. Then:

$$L_q(xy) = L_q(x) \cdot L_q(y)$$

Proof: $L_q(xy) = (xy)^{\frac{q-1}{2}} = x^{\frac{q-1}{2}} y^{\frac{q-1}{2}} = L_q(x) L_q(y) \mod q$

Since $L_q(xy),L_q(x),L_q(y) = \pm 1$ equality holds over the integers as well.

Using the previous theorem it is possible to derive

$$xx' \in \text{QR}_q$$
$$yy' \in \text{QR}_q$$
$$xy \in \text{QN}R_q$$

Where $x, x' \in \text{QR}_q$ and $y, y' \in \text{QN}R_q$.

**Quadratic Residues modulo a Composite:** Now, the elements belong to the group $z_N^*$, where N = pq with $p,q$ distinct primes. Applying the Chinese remainder theorem, $z_N^*$ can be expressed as

$Z_N^* = Z_p^* \times Z_q^*$ then, an element belonging to this group is denoted by $y \leftrightarrow (yp, yq)$ where $yp = y \mod p$ and $yq = y \mod q$. 6

**Theorem 6:** An element $y$ is a quadratic residue modulo $N$ if and only if $yp$ is a quadratic residue mod $p$, and $yq$ is a quadratic residue mod $q$. 
Proof: Let \( y \in QR_n \) and \( x \in \mathbb{Z}_N^* \) such that \( x^2 = y \mod N \). Then \( (x_p, x_q) \leftrightarrow y = x^2 \leftrightarrow (x_p, x_q)^2 = ([x_p^2 \mod p], [x_q^2 \mod q]) \)

We have a shown that:

\[ y_p = x_p^2 \mod p \text{ and } y_q = x_q^2 \mod q \]

and \( yp \) and \( yq \) are quadratic residues modulo \( p \) and \( q \) respectively. On the other hand, if \( y \leftrightarrow (yp, yq) \) and \( yp, yq \) are quadratic residues respectively, then there exist \( xp \in \mathbb{Z}_p^* \) and \( xq \in \mathbb{Z}_q^* \) such that \( x \leftrightarrow (xp, xq), x \in \mathbb{Z}_N^* \). Then, reversing the steps we have shown that \( x \) is a square root of \( y \mod N \).

Example: Let \( q = 3 \) and \( p = 5 \), then \( N = 15 \). First we have to compute the quadratic residues modulo 3 and modulo 5:

\[
\begin{align*}
Z_3^* & : \\
1: 1^2 \mod 3 & = 1 \\
2: 2^2 \mod 3 & = 1 \to \{1\} \in QR_3 \\
\end{align*}
\]

\[
\begin{align*}
Z_5^* & : \\
1: 1^2 \mod 5 & = 1 \\
2: 2^2 \mod 5 & = 4 \\
3: 3^2 \mod 5 & = 4 \\
4: 4^2 \mod 5 & = 1 \{1,4\} \in QR_5 \\
\end{align*}
\]

Now, we can compute the quadratic residues modulo \( N=15 \):

\[
\begin{align*}
1: 1^2 \mod 3 & = 1 \to 1 \in QR_{15} \\
2: 2^2 \mod 3 & = 2 \to 2 \mod 5 = 4 \\
4: 4^2 \mod 3 & = 1 \to 4 \in QR_{15} \\
7: 7^2 \mod 3 & = 1 \to 7 \mod 5 = 4 \\
8: 8^2 \mod 3 & = 2 \to 8 \mod 5 = 4 \\
11: 11^2 \mod 3 & = 2 \to 11 \mod 5 = 1 \\
13: 13^2 \mod 3 & = 1 \to 13 \mod 5 = 4 \\
14: 14^2 \mod 3 & = 2 \to 14 \mod 5 = 1 \\
\end{align*}
\]

Then: \( \{1,4\} \in QR_{15}^* \)

Now, each quadratic residue \( y \in QR_N \) has four square roots unlike the two square roots that the quadratic residues \( x \in QR_q \) had. These square roots are given by the elements:

\((xp, xq), (-xp, xq), (xp, -xq), (-xp, -xq)\)

Example: the element 4 is a quadratic residue mod 15 \( 2^2 = 4 \mod 15 \). The square roots are given by:

\[
\begin{array}{cccccccc}
2 & 1 & 2 & 4 & 7 & 8 & 1 & 1 \\
n^2 \mod 15 & 1 & 4 & 1 & 4 & 4 & 1 & 4 \\
\end{array}
\]

\((2 \mod 5, 2 \mod 3) = (2, 2) \leftrightarrow 2\)

\((2 \mod 5, -2 \mod 3) = (2, 1) \leftrightarrow 7\)

\((-2 \mod 5, 2 \mod 3) = (3, 2) \leftrightarrow 8\)

\((-2 \mod 5, -2 \mod 3) = (3, 1) \leftrightarrow 13\)

As a consequence of this proposition, it is possible to conclude that only the fourth part of the elements of are quadratic residues, since squaring modulo \( N \) is a four-to-one function or since \( y \in \mathbb{Z}_N^* \) is a quadratic residue if and only if \( yp \) and \( yq \) are quadratic residues modulo \( \mathbb{Z}_N^* \) and \( \mathbb{Z}_N^* \) respectively. So there is a correspondence between \( QR_N \) and \( QR_q \times QR_p \):
Example: As we compute before: \{1; 2; 4; 7; 8; 11; 13; 14\} \in \mathbb{Z}_{15}^{+} \text{ elem.} \{1, 4\} \in QR_{15} \rightarrow 2 \text{ elem.} \{2, 7, 8, 11, 13, 14\} \in QR_{15}^{+} \rightarrow 6 \text{ elem.}

It is possible to extend the definition of Legendre symbol to the case of a composite \( N \), being now called the Jacoby symbol:

\[
J_N(x) = J_p(x)J_q(x) = \begin{cases} 
\frac{p-1}{2} \cdot \frac{q-1}{2} & \text{if } x \in QR_p, \\
-1 & \text{if } x \not\in QR_p.
\end{cases}
\]

In the case modulo a prime \( p \), \( Lp(x) = 1 \) meant that \( x \in QR_p \), otherwise, \( Lp(x) = -1 \) meant that \( x \not\in QR_p \). In contrast, in this case that is not true.

As we know\(\text{ }\) \((xp, xq) \in QR \) only if \( xp \in QR_p \) and \( xq \in QR_q \), that is

\[
J_p(x) = J_q(x) = \begin{cases} 
1 & \text{if } x \in QR_N, \\
0 & \text{if } x \not\in QR_N.
\end{cases}
\]

If \( x \) is a quadratic residue modulo \( N \), then \( JN(x) = 1 \). But also this result can occur if \( xp \in QR_N^+ \) and \( xq \in QR_N^+ \):

\[
J_p(x) = J_q(x) = -1 \rightarrow J_n(x) = J_p(x)J_q(x) = 1.
\]

Then, we can conclude that the Jacoby symbol of \( x \mod N \) must be 1 if \( x \in QR_N^+ \), but on the other side, the value 1 not ensure that \( x \in QR_N \). Despite this conclusion, there is also an algorithm able to recognize quadratic residuosity modulo a composite of known factorization, \( N \):

\[
y^{\frac{p-1}{2}} \mod p \cdot y^{\frac{q-1}{2}} \mod q = \begin{cases} 
1 & \text{if } y \in QR_N^+, \\
0 & \text{else if } y \not\in QR_N^+.
\end{cases}
\]

Example: Assume \( N = pq = 3 \times 5 \). Let’s go to apply the algorithm to find it out if the next elements are quadratic residues modulo 15 or not:

\[(1^1 \mod 3)(1^2 \mod 5) \rightarrow 1 \times 1 = 1 \rightarrow 1 \not\in QR_{15},
\]
\[(2^1 \mod 3)(2^2 \mod 5) \rightarrow 2 \times 4 \not\equiv 2 \not\equiv 2 \in QR_{15},
\]
\[(3^1 \mod 3)(3^2 \mod 5) \rightarrow 0 \times 4 \equiv 0 \equiv 3 \not\equiv 3 \not\equiv 3 \in QR_{15},
\]
\[(4^1 \mod 3)(4^2 \mod 5) \rightarrow 1 \times 1 \equiv 1 \equiv 4 \equiv 4 \not\equiv 4 \in QR_{15}.
\]

The quadratic residues modulo a \( N \), also follow the multiplicative property. In this case:

**Theorem 7:** Let \( N = pq \) be a product of distinct, odd primes and \( x, y \in Z_N^+ \) then

\[
J_N(xy) = J_N(x)J_N(y)
\]

Proof:

\[
J_N(xy) = J_p(xy)J_q(xy) = J_p(x)J_q(x)J_p(y)J_q(y) = J_p(x)J_q(x)J_p(y)J_q(y) = J_N(x)J_N(y)
\]

**3.3. The Rabin Cryptosystem**

The previous section showed how it is possible to recognize a quadratic residue modulo \( N \) if the factorization \( N \) is known. The Rabin Cryptosystem is based on the idea that computing square roots modulo a composite \( N \) is simple when the factorization is known, but very complex when it is unknown.

The Rabin cryptosystem is an asymmetric system, so requires two different keys, a public key and a private key, one to encrypt the text and the other one to decrypt it. The first step is to choose the key which is defined by:

\[
K = \{n, p, q\}
\]

Where \( p \) and \( q \) are primes such that \( p; q \equiv 3 \mod 4 \), which are the private key. The public key is \( n = pq \). Then, to encrypt the message \( m \), the encryption function is applied

\[
e_k(m) = m^e \mod n = c
\]

The result is the cipher text, \( c \). Now the encoded message can be sent. Once the message reaches the destination, it must be decrypted. For that, the decryption function is applied:
Since the encryption function \( e_K \) is not an injection function, the decryption is not ambiguous. There exist four square roots of \( c \mod n \) (\( c = m^2 \mod n \)), so there are four possible messages, \( m \). The decryption try to determine \( m \) such that:

\[
m^2 \equiv c \mod n
\]

and this is equivalent to solving the two congruences

\[
z^2 \equiv c \mod p
\]
\[
z^2 \equiv c \mod q
\]

Then

\[
m_p = c^{\frac{p+1}{4}} \mod p
\]
\[
m_q = c^{\frac{p+1}{4}} \mod q
\]

Finally, the four square roots of \( c \mod n \) can be computed applying the Chinese remainder theorem to the system of congruences:

\[
+m_p \mod p
\]
\[
-m_p \mod p
\]
\[
+m_q \mod q
\]
\[
-q \mod q
\]

Example: Let \( n = 77 = pq = 11 \times 7 \) and \( m = 32 \). First, the message \( m \) must be encoded using the encryption function:

\[
e_k(32) = 32^2 \mod 77 = 23 = c
\]

The encoded message \( c = 23 \) is sent. The receiver must decrypt the message, so has to find the square roots of 23 modulo 7 and modulo 11. The decryption algorithm is applied:

\[
m_p = 23^{\frac{7+1}{4}} \mod 7 = 4
\]
\[
m_q = 23^{\frac{11+1}{4}} \mod 11 = 1
\]

and the system of congruences \( x \equiv q_i b_i \frac{M}{M_i} \) is:

\[
+m_p \mod 7 = 4 \mod 7
\]
\[
-m_p \mod 7 = 3 \mod 7
\]
\[
+m_q \mod 11 = 1 \mod 11
\]
\[
-q \mod 11 = 10 \mod 11
\]

Finally we can apply the Chinese remainder theorem to compute the four square roots:

First we compute \( b_1 \) and \( b_2 \) such

\[
\frac{N}{7} \cdot b_1 \equiv 1 \mod 7 \rightarrow b_1 = 2
\]
\[
\frac{N}{11} \cdot 2 \equiv 1 \mod 11 \rightarrow b_2 = 8
\]

Now, we can compute the solutions

1) \( x \equiv 4 \mod 7 \) and \( x \equiv 1 \mod 11 \): \( x = a_1 x b_1 x_{\frac{M}{p}} + a_2 x b_2 x_{\frac{M}{q}} = 4 \times 2 \times 11 + 1 \times 8 \times 7 \cdot x \equiv 144 = 67 \mod 77 \rightarrow x = 67
\]

2) \( x \equiv 3 \mod 7 \) and \( x \equiv 1 \mod 11 \): \( x = a_1 x b_1 x_{\frac{M}{p}} + a_2 x b_2 x_{\frac{M}{q}} = 3 \times 2 \times 11 + 1 \times 8 \times 7 \cdot x \equiv 122 = 45 \mod 77 \rightarrow x = 45
\]

3) Now, we can take the advantage of symmetry to get the other two result:

\[
7767=10 \rightarrow x=10
\]
\[
7745=32 \rightarrow x=32
\]

Finally, the original message must be 10, 32, 45 or 67. One way to be able to recognize which of all messages was the sent message is adding some information to the message, called redundant information.
4. RSA Cryptosystem

The most important public-key cryptosystem is the RSA cryptosystem on which one can also illustrate a variety of important ideas of modern public-key cryptography. For example we will discuss various possible attacks on the RSA cryptosystem and various other problems related to security of the RSA cryptosystems. A special attention will be given to the problem of factorization of integers that play such an important role for security of RSA. Several factorization methods will be presented and discussed. In doing that, we will illustrate modern distributed techniques to factorize very large integers.

4.1. Features of RSA

Advantages
- The type of key algorithms, much longer than the conventional algorithms (secret key) sequence.
- Speed of conventional encryption algorithms, public key algorithms is lower
- The most well known and widely used public-key encryption algorithm.
- Lack of denial by the sender
- Possibility of authenticated sender to receiver

Disadvantages
- Low Speed
- Large size keys
- Requires more computer resources
- Irreparable harm if disclosure of the private key.

4.2. Design and Use of RSA Cryptosystem

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Prime multiplication is very easy, integer factorization seems to be unfeasible:

a) Choose two large (512 - 1024 bits) primes \( p, q \) and denote
\[
    n = pq, \phi(n) = (p - 1)(q - 1)
\]
b) Choose a large \( d \) such that \( \gcd(d, \phi(n)) = 1 \) and compute \( e = d^{-1} \mod \phi(n) \)
c) Public key: \( n \) (modulus), \( e \) (encryption algorithm)
d) Trapdoor information: \( p, q, d \) (decryption algorithm)
   Plaintext \( w \)
   Encryption: cryptotext \( c = w^e \mod n \)
   Decryption: plaintext \( w = c^d \mod n \)

Details: A plaintext is first encoded as a word over the alphabet \( \{0, 1, \ldots, 9\} \), then divided into blocks of length \( i - 1 \), where \( 10^{i-1} < n < 10^i \). Each block is taken as an integer and decrypted using modular exponentiation

Some Examples for the design and use of RSA cryptosystems are as follows:
- By choosing \( p = 41, q = 61 \) we get \( n = 2501, f(n) = 2400 \)
- By choosing \( d = 2087 \) we get \( e = 23 \)
- By choosing \( d = 2069 \) we get \( e = 29 \)
- By choosing other values of \( d \) we get other values of \( e \).
Let us choose the first pair of encryption/decryption exponents (\( e = 23 \) and \( d = 2087 \)).

Plaintext: KARLSRUHE
Encoding: 10001711187200704
Since $10^3 < n < 10^4$, the numerical plaintext is divided into blocks of 3 digits. 6 plaintext integers are obtained:

100, 017, 111, 817, 200, 704

**Encryption:**

$100^{23} \mod 2501, 17^{23} \mod 2501, 111^{23} \mod 2501$

$817^{33} \mod 2501, 200^{33} \mod 2501, 704^{33} \mod 2501$

Provides cryptotexts: 2306, 1893, 621, 1380, 490, 313

**Decryption:**

$2306^{2087} \mod 2501 = 100, 1893^{2087} \mod 2501 = 17$

$621^{2087} \mod 2501 = 111, 1380^{2087} \mod 2501 = 817$

$490^{2087} \mod 2501 = 200, 313^{2087} \mod 2501 = 704$

**4.3. Correctness of RSA**

Let $c = w^e \mod n$ be the cryptotext for a plaintext $w$, in the cryptosystem with $n = pq$, $ed = 1 \pmod{\phi(n)}$, $\gcd(d, \phi(n)) = 1$

In such a case

$$w = c^d \mod n$$

and, if the decryption is unique, $w = c^d \mod n$.

**Proof:** Since $ed \equiv 1 \pmod{\phi(n)}$, there exist a $j \in N$ such that $j\phi(n) + 1$

- Case 1. Neither $p$ nor $q$ divides $w$. In such a case $\gcd(n, w) = 1$ and by the Euler's Totien Theorem we get that $c^d = w^d = w^{j\phi(n) + 1} = w \mod n$

- Case 2. Exactly one of $p,q$ divides $w$ - say $p$. In such a case $w^{e \phi(q) \mod p}$ and by Fermat's Little theorem $w^{\phi(q) \equiv 1 \pmod{q}}$

  $w^{q-1} \equiv 1 \pmod{q}$

  $w^{\phi(n)} \equiv 1 \pmod{q}$

  $w^{\phi(n)} \equiv 1 \pmod{q}$

  $w^{ed} = w \mod (q)$

  Therefore

  $w \equiv w^{ed} \equiv c^d \mod n$

- Case 3 Both $p,q$ divide $w$. This cannot happen because, by our assumption, $w < n$.

**4.4. RSA Challenge**

One of the first descriptions of RSA was presented by Gardner (1977) in his paper RSA inventors presented the following challenge.

**Decrypt the cryptotext:**

9686 9613 7546 2206 1477 1409 2225 4355 8829 0575 9991 1245 7431 9874 6951 2093 0816 2982
2514 5708 3569 3147 6622 8839 8962 8013 3919 9055 1829 9451 5781 5154

**Encrypted using the RSA cryptosystem with 129 digit number, called also RSA129:**

$n$: 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706
935 245 733 897 830 597 123 513 958 705 058 989 075 147 599 290 026 879 543 541.

And with $e = 9007$

**5. Designing a Good RSA CRYPTOSYSTEM**

**5.1. How to choose large primes $p,q$?**
Choose randomly a large integer \( p \), and verify, using a randomized algorithm, whether \( p \) is prime. If not, check \( p + 2, p + 4, \ldots \), From the Prime Number Theorem if follows that there are approximately

\[
\frac{2^d}{\log 2^d} - \frac{2^{d-1}}{\log 2^{d-1}}
\]

d bit primes. (A probability that a 512-bit number is prime = 0.00562.)

5.2. What kind of relations should be between \( p \) and \( q \)?
2.1 Difference \( |p-q| \) should be neither too small nor too large.
2.2 \( \gcd(p-1, q-1) \) should not be large.
2.3 Both \( p-1 \) and \( q-1 \) should contain large prime factors.
2.4 Quite ideal case: \( q, p \) should be safe primes such that also \( (p-1)/2 \) and \( (q-1)/2 \) are primes (83,107, 10^{100} - 166517 are examples of safe primes).

5.3. How to choose \( e \) and \( d \)?
1. Neither \( d \) nor \( e \) should be small
2. \( d \) should not be smaller than \( n^{1/4} \). (For \( d \leq n^{1/4} \) a polynomial time algorithm is known to determine \( d \).

Claim 1: Difference \( |p-q| \) should not be small.
Indeed, if \( |p - q| \) is small, and \( p > q \), then \( (p + q)/2 \) is only slightly larger than \( n \) because

\[
\frac{(p+q)^2}{4} - n = \frac{(p-q)^2}{4}
\]

In addition is a square, say \( y^2 \).
In order to factor \( n \) it is then enough to test \( x > \) until such \( x \) is found that \( x^2 - n \) is a square, say \( y^2 \). In such a case

\[
p + q = 2x, \quad p - q = 2y
\]

and therefore \( p = x + y, \quad q = x - y \).

Claim 2: \( \gcd(p-1, q-1) \) should not be large. Indeed, in the opposite case \( s = \text{lcm}(p-1, q-1) \) is much smaller than

\[0(n) \text{ If } d' e \equiv 1 \mod s \text{ then for some integer } k, \quad c^{d'} \equiv w^{ed} \equiv w^{k+1} \equiv w \mod n\]

Since \( p - 1|s, q - 1|s \) and therefore \( w^{ks} \equiv 1 \mod p \) and \( w^{ks+1} \equiv w \mod q \). Hence, \( d' \) can serve as a decryption exponent. Moreover, in such a case \( s \) can be obtained by testing.

6. Importance Of Factorization For Breaking RSA
The importance of factorization for breaking RSA are:
- If integer factorization is feasible, then RSA is breakable
- There is no proof that factorization is needed to break RSA.
- If a method of breaking RSA would provide an effective way to get a trapdoor information, then factorization could be done effectively.
- There are setups in which RSA can be broken without factoring modulus \( n \).

7. Security Of RSA
None of the numerous attempts to develop attacks on RSA has turned out to be successful. There are various results showing that it is impossible to obtain even only partial Information about the plaintext from the cryptotext produced by the RSA Cryptosystem. We will show that were the following two functions, computationally polynomially equivalent, be efficiently computable, then the RSA cryptosystem with the encryption (decryption) algorithm \( e_k \) \( (d_k) \) would be breakable.

\[
\text{parity}_e(c) = \text{the least significant bit of such an } w \text{ that } e_k(w) = c;
\]

\[
\text{half}_e(c) = 0 \text{ if } 0 \leq w < \frac{n}{2} \text{ and } \text{half}_e(c) = 1 \text{ if } \frac{n}{2} \leq w \leq n - 1.
\]

We show two important properties of the functions \( \text{half} \) and \( \text{parity} \).
1. Polynomial time computational equivalence of the functions \( \text{half} \) and \( \text{parity} \) follows from the following identities

\[
\text{half}_{ek}(c) = \text{parity}_{ek}(c \times e_k(2) \mod n)
\]

and the multiplicative rule \( e_k(w) e_k(w) = e_k(w, w) \).

2. There is an efficient algorithm to determine plaintexts \( w \) from the cryptotexts \( c \) obtained by RSA-decryption provided efficiently computable function \( \text{half} \) can be used as the oracle.  

**Breaking RSA Using an Oracle**

Algorithm:

```plaintext
for i = 0 to \( [\log n] \) do
    c_i <- half(c); c <- (c \times e_k(2)) \mod n
    l <- 0; u <- n
for i = 0 to \( [\log n] \) do
    m <- (l + u) / 2;
    if \( c_i = 1 \) then l <- m else u <- m;
    w <- [u]
```

Indeed, in the first cycle \( c_i = \text{half}(c \times (e_k(2))^i) = \text{half}(e_k(2^i w)) \), is computed for \( 0 \leq i \leq \log n \).

In the second part of the algorithm binary search is used to determine interval in which \( w \) lies. For example, we have that: 

\[
\text{half}(e_k(w)) = 0 = w \in \left[0, \frac{n}{2}\right)
\]

\[
\text{half}(e_k(2w)) = 0 = w \in \left[0, \frac{n}{4}\right) \cup \left[\frac{n}{2}, \frac{3n}{4}\right)
\]

\[
\text{half}(e_k(4w)) = 0 = w \in \left[\frac{n}{8}, \frac{3n}{8}\right)
\]

8. Results and Discussion

There are many results for RSA showing that certain parts are as hard as whole. For example any feasible algorithm to determine the last bit of the plaintext can be converted into a feasible algorithm to determine the whole plaintext.

Example Assume that we have an algorithm \( H \) to determine whether a plaintext \( x \) designed in RSA with public key \( e, n \) is smaller than \( n / 2 \) if the cryptotext \( y \) is given.

We construct an algorithm \( A \) to determine in which of the intervals \((jn/8, (j + 1)n/8)\), \( 0 \leq j \leq 7 \) the plaintext lies.

Basic idea \( H \) is used to decide whether the plaintexts for cryptotexts \( x^e \mod n \), \( 2^e \mod n \), \( 4^e \mod n \) are smaller than \( n / 2 \).

Answers

- yes, yes, yes  \( 0 < x < n/8 \)  no, yes, yes  \( n/2 < x < 5n/8 \)
- yes, no  \( n/8 < x < n/4 \)  no, yes, no  \( 5n/8 < x < 3n/4 \)
- yes, no, yes  \( n/4 < x < 3n/8 \)  no, no, yes  \( 3n/4 < x < 7n/8 \)
- yes, no, no  \( 3n/8 < x < n/2 \)  no, no, no  \( 7n/8 < x < n \)

8.1. RSA with A Composite “To Be A Prime”

Let us explore what happens if some integer \( p \) used, as a prime, to design a RSA is actually not a prime.

Let \( n = pq \) where \( q \) be a prime, but \( p = p_1 p_2 \), where \( p_1, p_2 \) are primes. In such a case

\[
\phi(n) = (p_1 - 1)(p_2 - 1)(q - 1)
\]

But assume that the RSA-designer works with \( \phi(n) = (p - 1)(q - 1) \)

---

144
Let \( u = \text{lcm}(p_1 - 1, p_2 - 1, q - 1) \) and let \( \gcd(w, n) = 1 \). In such a case
\[
\begin{align*}
    w^{p_1 - 1} &\equiv 1 \pmod{p_1}, \\
    w^{p_2 - 1} &\equiv 1 \pmod{p_2}, \\
    w^{q - 1} &\equiv 1 \pmod{q}.
\end{align*}
\]

And as a consequence
\[
    w^u = 1 \pmod{n}.
\]

In such a case \( u \) divides \( \varphi(n) \) and let us assume that also \( u \) divides \( \varphi(n) \). Then
\[
    w^{\varphi(n) - 1} = w \pmod{n}.
\]

So if \( e \varphi(n) \equiv 1 \pmod{\varphi(n)} \), then encryption and decryption work as if \( p \) were prime. \( ^7 \)

8.2. Private-Key versus Public-Key Cryptography

The prime advantage of public-key cryptography is increased security - the private keys do not ever need to be transmitted or revealed to anyone. Public key cryptography is not meant to replace secret-key cryptography, but rather to supplement it, to make it more secure.

Example RSA and DES are usually combined as follows
1. The message is encrypted with a random DES key
2. DES-key is encrypted with RSA
3. DES-encrypted message and RSA-encrypted DES-key are sent.

This protocol is called RSA digital envelope. In software (hardware) DES is generally about 100 (1000) times faster than RSA. If \( n \) users communicate with secret-key cryptography, they need \( n (n - 1) / 2 \) keys. In the case they use public key cryptography \( 2n \) keys are sufficient.

Public-key cryptography allows spontaneous communication. \( ^7 \)

If RSA is used for digital signature then the public key is usually much smaller than private key \( \Rightarrow \) verification is faster. An RSA signature is superior to a handwritten signature because it attests both to the contents of the message as well as to the identity of the signer. As long as a secure hash function is used there is no way to take someone’s signature from one document and attach it to another, or to alter the signed message in any way. The slightest change in a signed message will cause the digital signature verification process to fail. Digital signature are the exact tool necessary to convert even the most important paper based documents to digital form and to have them only in the digital form. \( ^9 \)

8.3. Comparison with RSA Cryptosystem

The cryptosystems RSA and Rabin are very similar. Both are based on the hardness of factorization. The main difference is the fact that it is possible to prove that the problem of the Rabin cryptosystem is as hard as integer factorization, while hardness of solving the RSA problem is not possible to relate to the hardness of factoring, which makes the Rabin cryptosystem more secure in this way than the RSA.

Another difference is in the risk of attack. The Rabin cryptosystem is secure against a chosen plaintext attacks, however, the system can be broken using ciphertext attacks enabling the attacker to know the private key. RSA is also vulnerable to a chosen ciphertext attack, but the private key always remains unknown.

In terms of efficiency, the Rabin encryption process requires to compute roots modulo \( n \) more efficient than the RSA which requires the computation of \( n \)-th powers. About the decryption process both apply the Chinese remainder theorem. The disadvantage in decryption process of Rabin system is that the process produces four results, three of them false results, while the RSA system just get the correct one.

9. Conclusion

In this paper we reviewed the RSA algorithm discussed around Robin. The encryption algorithm is compared with the conclusions reached by the algorithm faster and more secure than RSA encryption Robin presented. And the digital signature after the signature of both algorithms reached this conclusion that Digital Robin is faster than RSA.
References


