New Digital Signature Scheme Using Polynomials Over Non-Commutative Groups

Dr. P. Vasudeva Reddy[1] G.S.G.N.Anjaneyulu[2] Dr. D.V. Ramakoti Reddy[3] Prof.M.Padmavathamma[4]

[1] Associate Professor, Dept. of Mathematics, A.U. College of Engg, Andhra University, Visakhapatnam–530 003.
[2] Associate Professor, Dept. of Mathematics, Narayana Engg .College, Nell ore. A.P- 524003
[3] Associate Professor, Dept. of Mathematics, A.U. College of Engg, Andhra University, Visakhapatnam–530 003.
[4] Professor, Dept. of Computer Science, ,S.V.University, Tirupati -517502

Summary
Digital signatures are probably the most important and widely used cryptographic primitive enabled by public key technology, and they are building blocks of many modern distributed computer applications, like, electronic contract signing, certified email, and secure web browsing etc. However, many existing signatures schemes lie in the intractability of problems closure to the number theory than group theory. In this paper, we propose a new Digital signature scheme based on general non-commutative group. The key idea of our scheme is that for a given non-commutative group, we define polynomials and take them as the underlying work stricture. By doing so, we implement a digital signature scheme. The security of the proposed signature scheme is based on the intractability of the Polynomial Symmetrical Decomposition Problem over the given non-commutative group.

Key words:
Public Key Cryptography, Digital Signatures, Polynomial rings, non-commutative groups, Decomposition problem, Diffie-Hellman problem.

1. Introduction

1.1 Background of Public Key Infrastructure and proposals based on Commutative Groups

There is no doubt that the Internet is affecting every aspect of our lives; the most significant changes are occurring in private and public sector organizations that are transforming their conventional operating models to internet based service models, known as e-Business, e-Commerce, and e-Government. Public Key Infrastructure (PKI) is probably one of the most important items in the arsenal of security measures that can be brought to bear against the aforementioned growing risks and threats. The design of reliable Public Key Infrastructure presents compendium-challenging problems that has fascinated researchers in computer science, electrical engineering and mathematics alike for the past few decades and are sure to continue to do so.

In their seminal paper "New directions in Cryptography" [2] Diffie and Hellman invited public key Cryptography and, in particular, digital signature schemes. The trapdoor one-way functions play an important role in the idea of PKC and digital signature schemes. To day, most successful signature schemes based on the difficulty of certain problems in particular large finite commutative rings. For example, see [2], [3] [6], [8], [9].

As addressed in [7], in order to enrich Cryptography, there have been many attempts to develop alternative PKC based on different kinds of problems. Historically, some attempts were made for a Cryptographic Primitives construction using more complex algebraic systems instead of traditional finite cyclic groups or finite fields during the last decade. The originator in this trend was [10], where a proposition to use non-commutative groups and semi groups in session key agreement protocol is presented.

According to our knowledge, the first signature scheme designed in an infinite non commutative groups was appeared in [5]. This invention is based on an essential gap existing between the Conjugacy Decision Problem (CDP) and Conjugate Search Problem (CSP) [4] in non-commutative group. In [1], Cao et.al. Proposed a new DH-like key exchange protocol and ElGamal – like cryptosystems using the polynomials over non-commutative rings.

1.2 Our contributions

In this paper, we would like to propose a digital signature scheme based on general non-commutative group. The key idea of our proposal is that for given non-commutative group, we define polynomials and take them as the underlying work structure. By doing so, we implement a digital signature scheme.

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

1.3 Outline of the paper

The rest of the paper is organized as follows. In Section 2, we present well known Cryptographic assumptions over non-commutative groups. In Section3, first we give some extensions to non-commutative groups and present necessary assumptions over non-commutative groups. In Section 4, we propose a digital signature scheme based on the underlying structure and assumptions. In section-5, we present an example of the proposed digital signature scheme in symmetric groups. Finally, concluding remarks are made in Sec.6.

2. Cryptographic Assumptions on Non-commutative Groups

2.1 Two Well-known Cryptographic Assumptions

In a non-commutative group G, two elements x, y are conjugate, written $x \sim y$, if $y = z^{-1} x z$ for some $z \in G$. Here z or z^{-1} is called a conjugator. Over a non commutative group G, we can define the following two cryptographic problems, which are related to conjugacy:

- ***Conjugator Search Problem (CSP):***
Given $(x,y) \in G \times G$, find $z \in G$ such that $y = z^{-1} x z$

-Decomposition Problem (DP):
Given $(x, y) \in G \times G$ and $S \subseteq G$, find $z_1, z_2 \in S$ such that $y = z_1 x z_2$

At present, we believe that for general non-commutative group G, both of the above problems CSP and DP are intractable.

2.2 Symmetrical Decomposition and Computational Diffie-Hellman Assumptions over Non-commutative Groups

Enlightened by the above problems, we would like to define the following Cryptographic problems over a non-commutative group G.

- ***Symmetrical Decomposition Problem (SDP):*** Given $(x, y) \in G \times G$ and $m, n \in Z$, find $Z \in G$ such that $y = z^m x z^n$.

- ***Generalized symmetrical Decomposition Problem (GSDP):***
Given $(x, y) \in G \times G$, $S \subseteq G$ and $m, n \in Z$, find $z \in S$ such that $y = z^m x z^n$.

Computational Diffie – Hellman (CDH) problem over Non-Commutative Group G:

Compute $x^{z_1 z_2}$ ($or\ x^{z_2 z_1}$) for given x, x^{z_1} *and* x^{z_2}, where $x \in G$, $z_1, z_2 \in S$.

At present, we have no clue to solve this kind of CDH problem without extracting z_1 (or z_2) from x and x^{z_1} (or x^{z_2}). Then, the CDH assumption over G says that CDH problem over G is intractable.

3. Building Blocks for Proposed Signature Scheme

3.1 Extension of non-commutative groups

Consider a non-commutative group $(G,1_G)$. Suppose that there is a ring $(R, +, \bullet, 1_R)$ and a monomorphism $Ø$: $(G, 1_G) \rightarrow (R, \bullet, 1_R)$. Then, the inverse mapping $Ø^{-1}$: $Ø(G) \rightarrow G$ is also a well – defined monomorphism for a, b € G, if $Ø(a) + Ø(b) \in Ø(G)$. We can assign a new element $c \in G$ as $c \underline{\Delta} Ø^{-1}[Ø(a) + Ø(b)]$ and call c as the quasi-sum of a and b, denoted by $c = a \oplus b$. Similarly, for $k \in R$ and $a \in G$, if $k.Ø(a) \in ?\ G)$, then we can assign a new element $d \in G$ as $d \underline{\Delta} Ø^{-1}[kØ(a)]$ and call d as the k quasi – multiple of a, denoted by $d = k \otimes a$.

Then, we can see that the monomorphism Ø is linear in sense of that the following equation holds.

Ø (k $\otimes$ a $\oplus$ b) = k. Ø (a) + Ø (b), for a, $b \in G$ and $k.Ø(a) + Ø(b) \in ?\ G)$.

Also, for $f(x) = z_0 + z_1 x + \text{----} + z_n x^n \in z[x]$ and $a \in G$, if $f(Ø(a)) = z_0 + z_1.Ø(a) + ... + z_n Ø(a)^n \in Ø(G)$, then we can assign a new element $e \in G$ as $e \underline{\Delta} Ø^{-1}[f(Ø(a))]$, and call e as the quasi-polynomial of f on a, denoted by $e = f(a)$.

Clearly, for arbitrary $a, b \in G$, $K \in R$ and $f(x) \in Z[x]$, $a \oplus b$, $k \otimes a$ and $f(a)$ are not always well – defined. But the following theorem holds.

Theorem: *For some a ∈G and some f(x), h(x), ∈ Z(x), if f (a) and h(a) are well defined , then*

(i) $Ø(f(a)) = f(Ø(a))$

(ii) f(a).h(a) = h(a).f(a).

3.2 Further assumptions on Non-commutative Groups

Suppose that (G, 1_G.) be a non-commutative group. For any randomly picked a ∈ G, we define a set $P_a \subseteq G$ by $P_a \triangleq \{f(a) \in Ø(G) / f(x) \in Z\ [x]\}$.

Then, we can define new versions of GSD and CDH problems over (G, ●) with respect to its subset P_a, and name them as polynomial symmetric decomposition (PSD) problem and polynomial Diffie – Hellman (PDH) problem – respectively.

- Polynomial Symmetrical Decomposition (PSD) problem over Non- commutative Group G:

Given (*a, x, y*) ∈ G^3 and *m, n, ∈ Z*, find $z \in P_a$ such that $y = z^m x z^n$ **.**

- Polynomial Diffie – Hellman (PDH) problem over Non-commutative Group G:

Compute $x^{z_1 z_2}$ ($or\ x^{z_2 z_1}$) for given a, x, X^{z_1} and X^{z_2}, where a, x ∈G and $z_1, z_2 \in P_a$.

Accordingly, the PSD (PDH) Cryptographic assumption says that PSD (PDH) problem over (G,●.) is intractable, i.e. there does not exist probabilistic polynomial time algorithm, which can solve PSD (PDH) problem over (G, ●).

4. Proposed Signature Scheme

Digital Signature Scheme from Non-commutative Groups

Now, Given a Non-commutative group(G, 1_G). there is ring (R, +, ●, 1_R) and a monomorphism Ø: (G, 1_G)→(R, ●, 1_R). Then the inverse mapping $Ø^{-1}$:(R,●,1_R) → (G,1_G) is also defined as monomorphism.

Initial setup

Given a non-commutative group, we assume that SDP on G is intractable .Pick two small positive integers m, n € Z & two elements p, q € G at random. Let H: ***M***→G be a cryptographic hash function then, the tuple

< G, m, n, p, q, M, H > is the public parameters of the system.

Key Generation

Alice wants to sign and send a message M to Bob for verification. Alice chooses a polynomial randomly f(x) € $Z_{>0}$[x] such that f{ Ø(p)}€ Ø(G) and then takes f (p) as her private key. Also she computes $y = f(p)^m q\ f(p)^n$. and publishes her public key as (p, q, y) € G^3

Signature Generation

Alice performs each of the following,

1. Alice selects a polynomial h(x) € Z[x] randomly such that h{Ø(p)}€ Ø(G) and takes h(p) as salt.
2. Compute $u = h(p)^m q\ h(p)^n$

$r = f(p)^m \{H(M)u\} f(p)^n$,

$s = h(p)^m\ r\ h(p)^n$,

$\alpha = h(p)^m\ r\ f(p)^n$,

$\beta = f(p)^m\ H(M)\ h(p)^n$,

$V_1 = h(p)^m H(M) h(p)^n$.

Then (u, s, α , β , V_1) is the Alice's signature on message M and sends it to Bob for verification.

Verification

To verify the Alice's signature (u, s, α , β , V_1), Bob do the following

1. compute $V_2 = \alpha\ y^{-1} \beta$
2. Bob accepts Alice's signature if $u^{-1}V_1 = s^{-1}V_2$ otherwise, he rejects the signature.

5. An Example For the Proposed Digital Signature Scheme Using Symmetric Group

Let us illustrate our signature scheme by using the symmetric group S_3 i.e. minimal non-commutative group. At first, we should choose a non-commutative group as the bridge for definition addable relation over S_3. We choose M_2 (Z_2), for convenience.

Next, we should find a monomorphism from S_3 to M_2 (Z_2). Let us define a mapping

Ø : $S_3 \rightarrow M_2(Z_2)$ as follows:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\to\begin{pmatrix}1&1\\0&1\end{pmatrix};$$
$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\to\begin{pmatrix}0&1\\1&0\end{pmatrix};$$
$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\to\begin{pmatrix}0&1\\1&1\end{pmatrix};$$
$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\to\begin{pmatrix}1&1\\1&0\end{pmatrix};$$
$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\to\begin{pmatrix}1&0\\1&1\end{pmatrix}.$$

It is not difficult to verify that Ø is a monomorphism. Define the hash function as

$H(M)=\begin{pmatrix}1 & 2 & 3\\ (M-1)\bmod 3 & (M-2)\bmod 3 & (M-3)\bmod 3\end{pmatrix}$ where $M\in M$

Key Generation

Private Key: She calculates

$$f(p) = Ø^{-1}\{f(Ø(p))\}$$
$$= Ø^{-1}\{4.\begin{bmatrix}0&1\\1&1\end{bmatrix}^2+\begin{bmatrix}0&1\\1&1\end{bmatrix}+2.I\}$$
$$= Ø^{-1}\left\{\begin{bmatrix}0&1\\1&1\end{bmatrix}\right\} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

as her private key.

Public key: She also calculates

$$y = f(P)^m q\, f(p)^n$$
$$=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^3\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^5$$
$$=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\in S_3$$

as her public key.

Suppose that, Alice chooses m =3,

$$n=5,\ p=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\ \&\ q=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

p, q $\in S_3$. Also she chooses a polynomial randomly, as $f(x) = 4x^2 + x + 2$.

Signature Generation

Alice also chooses, another random polynomial $h(x) = 4x^4 + x^3 + 4x^2 + 3x + 4$.

Compute $h(P) = Ø^{-1}\{h(Ø(P))\} =$

$$\phi^{-1}\left\{4\begin{bmatrix}0&1\\1&1\end{bmatrix}^4+\begin{bmatrix}0&1\\1&1\end{bmatrix}^3+4\begin{bmatrix}0&1\\1&1\end{bmatrix}^2+3\begin{bmatrix}0&1\\1&1\end{bmatrix}+4.I\right\}$$
$$= Ø^{-1}\left\{\begin{bmatrix}1&1\\1&0\end{bmatrix}\right\} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\in S_3.$$

Also she computes $u = h(P)^m q\, h(p)^n$

$$=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}^3\cdot\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}^5$$
$$=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$r = f(P)^3\{H(M)u\}f(p)^5$

$$=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$S = h(P)^3 r\, h(p)^5$

$$=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}*\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}*\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$\alpha = h(P)^3 r\, f(p)^5$

$$=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$\beta = f(P)^3 H(M)h(p)^5$

$$= \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$V_1 = h(P)^3 H(M)\, h(p)^5$

$$= \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

Alice sends (u, s, α, β, V_1) to bob , as her signature.

Signature Verification:

Bob receives (u, s, α, β, V_1) from Alice,

computes $V_2 = \alpha\, y^{-1} \beta$

$$= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$U^{-1}V_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$S^{-1}V_2 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

Bob accepts Alice's signature iff $U^{-1}V_2 = S^{-1}V_2$, Otherwise, he rejects the signature.

6. Conclusions

In this paper, we presented a signature scheme based on general non-commutative group. The key idea behind our scheme lies that we take polynomials over the given non-commutative group as the underlying work structure for constructing signature scheme. The security of the proposed signature scheme is based on the intractability of PSD problem i.e. the security assumption is that the polynomial symmetrical decomposition (PSD) problem over the given non-commutative group is intractable.

References

[1] Z. Cao, X. Dong and L. Wang. New Public Key Cryptosystems using polynomials over Non-commutative rings. Cryptology e-print Archive, 2007.

[2] W. Diffie and M.E. Hellman, New direction is cryptography, IEEE Transaction on information theory, Vol.22, pp 644-654, 1976.

[3] T. ElGamal, A public key cryptosystem, and a signature scheme based on discrete logarithms, IEEE transactions on information theory, Vol.31, PP 469-472, 1985.

[4] K.H. Ko et.al. New public-key cryptosystem using Braid Groups. Advances in cryptology, proc. CRYPTO 2000. LNCS 1880, PP. 166-183, Springer-verlag, 2000.

[5] K.H. Ko et. al., New signature scheme using conjugacy problem, Cryptology e print Archive: Report 2002/168, 2002.

[6] K. Komaya, V. Maurer, T. Okamoto and S. Vanstone, New PKC based on elliptic curves over the ring Zn, LNCS 516, PP.252-266, Springer-verlag 1992.

[7] E. Lee, Braid groups in cryptography, IEICE Trans. Fundamentals, vol.E87-A, no.5, PP. 986-992, 2004.

[8] S.S. Maglivers, D.R. Stinson and T. Van Trungn, new approaches to designing Public Key Cryptosystems using one-way functions and trapdoors in finite groups, Journal of cryptology, Vol.15, PP. 285-297, 2002.

[9] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital Signatures and public key Cryptosystems, communications of the ACM Vol. 27, PP.120-126, 1978.

[10] V. Sidelnikov, M. Cherepnev, V.Yaschenko, Systems of open distribution of keys based on non-commutation semi groups. Russian Acad. Sci. Dok L. math., PP. 48 (2), 566-567, 1993.

Dr. P.Vasudeva Reddy received M. Sc (Mathematics), PhD (Cryptography) from S.V. University, Tirupati, India. He is currently working as an associate professor in the department of mathematics, A.U College of Engineering, Andhra University, and Visakhapatnam, India. His field of interest includes Algebraic Number theory, secret sharing, Multi party computations, and cryptography.

G.S.G.N.Anjaneyulu received M.Sc (Mathematics) & M.phil (theory of semi rings) from S.V.University, Tirupati. .Currently he is perusing research for PhD (Digital signatures using semi ring structures). He is currently working as an associate professor in the department of mathematics, Narayana Engg. College, Nellore, Andhra Pradesh, India. His field of interests includes cryptography using algebraic structures.

Dr. D. V. Rama Koti Reddy received PhD from the department of Instrument Technology, Andhra University. He is currently working as an associate professor in the department Instrument Technology , A.U College of Engineering, Andhra University, Visakhapatnam, India. His field of interests includes bio informatics, Sensor Networking.

Prof M .Padmavathamma, born in Chittoor District, A.P., India, in 1963.She received M.Sc, M.Phil, M.Ed, PhD from S.V. University, Tirupati and M.S (Software Systems) from BITS PILANI. Currently she is working as Head, Department of Computer Science, S.V.University, Andhra Pradesh, India. Her research interests lie in the areas of Number theory, Cryptography, Network Security, Distributed Systems and Data Mining. She has published 25 research papers in national/International journals and conferences. She published TWO textbooks as one of the author. Also she is life member of International Association of Cryptology Research Society of India (IACR) and Andhra Pradesh Association of Mathematical Teachers (APAMT), India.