Zero-Knowledge Authentication Schemes Using Quasi-Polynomials over Non-Commutative Groups

Maheswara Rao Valluri*

School of Mathematical & Computing Sciences, Fiji National University, P.Box.No:7222, Derrick Campus, Suva, Fiji.

*Corresponding author: maheswara.valluri@fnu.ac.fj

Abstract:
A zero-knowledge authentication scheme is a type of authentication scheme, which gives no knowledge beyond the authenticity identifying an entity and is probabilistic than deterministic authentication scheme. This paper proposes Diffie-Hellman and Fiat-Shamir like zero-knowledge authentication schemes on general non-commutative groups. The key idea of our proposal is that for a given non-commutative group one can define quasi-polynomials and takes them as underlying work structure. In doing so, one can implement the schemes. The security of the proposed schemes is based on the intractability of the quasi-polynomial symmetrical decomposition problem over the given non-commutative group.

Keywords:
Authentication; Decomposition Problems; Non-Commutative Groups; Security; Zero-Knowledge

1. INTRODUCTION

The rapid world-wide development of electronic transaction signifies a strong demand for fast and cheap secret key distribution system that is essential for electronic commerce or electronic banking transactions. In traditional cryptography, the secret key distribution problem is a major problem. It was solved with the invention of public key cryptosystem by Diffie-Hellman, allowing one entity to send a message secretly to another entity even if they do not share any secret key in advance. However, this is only application in practice if some trust in the identifying of communicating parties can be established. One tool for doing this is zero knowledge authentication scheme. The zero-knowledge authentication scheme is authentication scheme which gives no knowledge beyond the authenticity. Recently, very effective zero-knowledge authentication schemes have been constructed, however, they only provide authentication and not confidentiality.

In 1976, Diffie and Hellman introduced the idea of public key cryptography (PKC) [1]. Later, many PKC schemes had been proposed and broken. The trapdoor one-way functions play the key role in the idea of PKC. Today, most successful PKC schemes are based on the perceived difficulty of certain problems in particular large finite commutative rings. For example, the difficulty of solving integer factoring problem (IFP) defined over $\mathbb{Z}_n$ (where $n$ is the product of primes) forms the ground of the basic RSA cryptosystem [2], variants of RSA and elliptic curve version of RSA like KMOV [3]. Another good case is that the
ElGamal – type PKC family [4] is based on the difficulty of solving the discrete logarithm problem (DLP) defined over a finite fields $Z_p$ (where $p$ is a large prime), of course a commutative ring.

As addressed in [5], in order to enrich cryptography, there have been many attempts to develop alternative PKC based on different kinds of hard 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 [6], where a proposition to use non-commutative groups and semigroups in session key agreement protocol was presented.

According to the author’s knowledge, the first zero-knowledge authentication scheme in an infinite non-commutative groups appeared in [7]. In [8], Cao et al. proposed a new Diffie-Hellman like key exchange protocol and ElGamal like cryptosystems using the quasi-polynomials over non-commutative groups. This enabled the authors of [8–10] to construct a public key cryptosystems and digital signatures. Diffie-Hellman key agreement scheme also allows constructing two-pass challenge-response and iterated three-pass challenge-response zero-knowledge authentication schemes.

In this paper, Diffie-Hellman and Fiat-Shamir like zero-knowledge authentication schemes based on general non-commutative groups are proposed. The key idea of the schemes is that for given non-commutative group, one can generate quasi-polynomials and take them as the underlying work structure. By doing so, one can implement the zero-knowledge authentication schemes.

The rest of the paper is organized as follow. In section 2, well-known cryptographic assumptions over non-commutative groups are presented. In section 3, first one gives some extensions to non-commutative groups and presents necessary assumptions over non-commutative groups. In section 4, Diffie-Hellman and Fiat-Shamir like zero-knowledge authentication schemes based on underlying structure and assumptions are proposed, and also their security issues are discussed. Finally, concluding remarks are made in section 5.

### 2. CRYPTOGRAPHIC ASSUMPTIONS ON NON-COMMUTATIVE GROUPS

As in [8], one can define the following cryptographic problems over a non-commutative group G.

- **Symmetrical Decomposition problem (SDP):** Given $(x, y) \in G \times G$, and $m, n \in \mathbb{Z}$, the set of integers, 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 $m, n \in \mathbb{Z}$, 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 $x \in G$, and $z_1, z_2 \in S$, for $S \subseteq G$.

At present, there is no clue to solve this kind of CDH problem without extracting $z_1$ (or $z_2$) from $x$ and $x^{z_1}$ (or $x^{z_2}$). Hence, the CDH assumption over G says that CDH problem over G is intractable. i.e., there is no probabilistic polynomial time algorithm which can solve CDH problem over G with non-negligible accuracy with respect to problem scale.

### 3. BUILDING BLOCKS FOR PROPOSED AUTHENTICATION SCHEMES

In this section, one presents the extension of non-commutative groups, as in [8].
3.1 Extension of Non-Commutative Groups

Consider a non-commutative group \((G, \cdot, 1_G)\). Suppose that there is a ring \((R, +, \cdot, 1_R)\) and a monomorphism \(\varphi : (G, \cdot, 1_G) \to (R, +, 1_R)\). Then, the inverse map \(\varphi^{-1} : \varphi(G) \to G\) is also a well-defined monomorphism and for \(a, b \in G\), if \(\varphi(a) + \varphi(b) \in \varphi(G)\). One can assign a new element \(c \in G\) as \(c^\varphi = \varphi^{-1}[\varphi(a) + \varphi(b)]\) 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 \(k \cdot \varphi(a) \in \varphi(G)\), then one can assign a new element \(d \in G\) as \(d^\varphi = \varphi^{-1}[k \cdot \varphi(a)]\) and call it as the \(k\) quasi-multiple of \(a\), denoted by \(d = k \otimes a\). Then, one can see that the monomorphism \(\varphi\) is linear in sense of that the following equalities hold:

\[
\varphi(k \otimes a \oplus b) = k \cdot \varphi(a) + \varphi(b), \quad \text{for } a, b \in G \text{ and } [k \cdot \varphi(a) + \varphi(b)] \in \varphi(G).
\]

Further, for \(f(x) = z_0 + z_1 x + \cdots + z_n x^n \in \mathbb{Z}[x]\) and \(a \in G\), if \(f(\varphi(a)) = z_0 1_R + z_1 \varphi(a) + \cdots + z_n \varphi(a)^n \in \varphi(G)\), then one can assign a new element \(e \in G\) as \(e^\varphi = \varphi^{-1}[f(\varphi(a))]\), 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 \(f(x) \in \mathbb{Z}[x]\), \(a \oplus b, k \otimes a\) and \(f(a)\) are not always well-defined. But, one can prove that the following theorem holds.

**Theorem:** For some \(a \in G\) and some \(f(x), h(x) \in \mathbb{Z}[x]\) if \(f(a)\) and \(h(a)\) are well defined, then

1. \(\varphi(f(a)) = f(\varphi(a))\)
2. \(f(a) \cdot h(a) = h(a) \cdot f(a)\).

3.2 Further Assumptions on Non-Commutative Groups

Let \((G, \cdot, 1_G)\) be a non-commutative group. For any randomly picked element \(a \in G\), one can define a set \(P_a \subseteq G\) by

\[
P_a \triangleq \{f(a) \in \varphi(G) / f(x) \in \mathbb{Z}[x]\}.
\]

Then, one can define new versions of GSD and CDH problems over \((G, \cdot)\) with respect to its subset \(P_a\), and name them as quasi-polynomial symmetrical decomposition (QPSD) problem and quasi-polynomial Diffie-Hellman (QPDH) problem respectively.

**Quasi-Polynomial Symmetrical Decomposition (QPSD)** Problem over Non-Commutative Group \(G\):

Given \((a, x, y) \in G^3\) and \(m, n \in \mathbb{Z}\), find \(z \in P_a\) such that \(y = z^m \times z^n\).

**Quasi-Polynomial Diffie-Hellman (QPDH)** Problem over Non-Commutative Group \(G\):

Compute \(x^{z_1}z_2\) (or \(x^{z_2}z_1\)) for given \(a, x, z_1\) and \(x^2\), where \(a, x \in G\), and \(z_1, z_2 \in P_a\).

Accordingly, the QPSD (QPDH, respectively) cryptographic assumption says that QPSD (QPDH, respectively) problem over \((G, \cdot)\) is intractable, i.e. there does not exist probabilistic polynomial time algorithm which can solve QPSD (QPDH, respectively) problem over \((G, \cdot)\) with non-negligible accuracy with respect to problem scale.

4. PROPOSED AUTHENTICATION SCHEMES

In this section, Diffie-Hellman and Fiat-Shamir like zero-knowledge authentication schemes are proposed. The security of the schemes relies on quasi-polynomial symmetrical decomposition problem over the given non-commutative group.
4.1 Diffie-Hellman Like Zero-Knowledge Authentication Scheme from Non-Commutative Groups:

The Diffie-Hellman like zero-knowledge authentication scheme is a two-pass challenge-response scheme and is a perfectly honest-verifier zero-knowledge.

This scheme contains the following main steps:

**Initial Setup:** Consider the non-commutative group \((G, \cdot)\). Pick two small positive integers \(m, n \in \mathbb{Z}\) and two elements \(p, q \in G\) at random. Let \(H : \mathcal{M} \rightarrow G\) be a cryptographic hash function. Then, set the tuple \(<G, m, n, p, q, \mathcal{M}, H>\) as the public parameters of the system.

**Key Generation:** First the Prover chooses a random quasi-polynomial \(f(x) \in \mathbb{Z}[x]\) such that \(f(\varphi(p)) \in \varphi(G)\) and takes \(f(p)\) as private key, then computes and publishes public key \(y = f(p)^m q f(p)^n \in G\).

**Authentication:** To begin authentication,

(a) the Verifier chooses a random quasi-polynomial \(h(x) \in \mathbb{Z}[x]\) such that \(h(\varphi(p)) \in \varphi(G)\) and computes the challenge \(u = h(p)^m q h(p)^n \in G\) then sends to the Prover.

(b) The Prover sends the response \(w = H(f(p)^m u f(p)^n) \in G\), to the Verifier.

(c) The Verifier checks \(w = H(h(p)^m y h(p)^n) \in G\).

4.2 Security Analysis

In this subsection, one can examine the completeness, soundness and honest-verifier zero-knowledge of the proposed scheme, in particular regarding the observation of the communication by a third party.

**Completeness:** Assume that the Prover sent \(w^1\) at step (b). Then the Verifier accepts the Prover’s key, if and only if, \(w^1 = H(h(p)^m y h(p)^n)\). The latter relation is equivalent to \(w^1 = H(h(p)^m f(p)^m q f(p)^n h(p)^n)\)

\[
= H(f(p)^m (h(p)^m q h(p)^n) f(p)^n)
\]

\[
= H(f(p)^m u f(p)^n) = w.
\]

**Soundness:** Assume that a cheater \(A'\) is accepted with non-negligible probability. This means that \(A'\) can compute \(H(h(p)^m y h(p)^n)\) with non-negligible probability. As \(H\) is supposed to be an ideal hash-function, this means that \(A'\) can compute an element \(r \in G\) satisfying \(H(r) = H(h(p)^m y h(p)^n)\) with non-negligible probability. There are two possibilities: either \(r = h(p)^m y h(p)^n\) which contradicts the hypothesis that the quasi-polynomial symmetric decomposition Problem for \(h(p)\) is hard, or \(r \neq h(p)^m y h(p)^n\), which means that Cheater \(A'\) and the Verifier are able to find a collision for \(H\), contradicting the hypothesis that \(H\) is collision-free.

**Honest-Verifier Zero-knowledge:** Consider the probabilistic Turing machine defined as follow: It chooses random quasi-polynomial \(h(p)\) using same drawing as the honest verifier, and outputs the instances \((h(p), H(h(p)^m y h(p)^n))\). Then, the instances generated by this simulator follow the same probability distribution as the one generated by the interactive pair (the Prover, the Verifier).

For active attacks, the security is ensured by the hash function \(H\): if \(H\) is a collision – free hash function, these attacks are ineffective. One of the possible choices for \(H\) is discussed in Appendix.
4.3 Fiat-Shamir like Zero-Knowledge Authentication Scheme from Non-Commutative Groups

The Fiat-Shamir like zero-knowledge authentication scheme [11] is a three-pass iterated challenge-response scheme. This scheme has to be repeated k times if one desires to reduce the probability of successful forgery to \( \frac{1}{2^k} \).

This scheme contains the following main steps:

**Initial Setup:** Given the non-commutative group \((G, \cdot)\), pick two small positive integers \(m, n \in \mathbb{Z}\) and two elements \(p, q \in G\) at random. Then, set the tuple \(<G, m, n, p, q>\) as the public parameters of the system.

**Key Generation:** First the Prover chooses a random quasi-polynomial \(f(x) \in \mathbb{Z}[x]\) such that \(f(\phi(p)) \in \phi(G)\) and takes \(f(p)\) as private key, then computes and publishes public key \(y = f(p)^m q f(p)^n \in G\).

**Authentication:** To begin authentication, the Prover chooses a random quasi-polynomial \(h(x) \in \mathbb{Z}[x]\) such that \(h(\phi(p)) \in \phi(G)\) and computes the commitment \(u = h(p)^m y h(p)^n \in G\) then sends to the Verifier. The Verifier chooses a random bit \(c\) and sends it as a challenge to the Prover.

(a) If \(c = 0\), then the Prover sends \(v(p) = h(p)\) to the Verifier. The Verifier aborts the authentication and rejects unless the equality \(u = v(p)^m y v(p)^n\) is satisfied.

(b) If \(c = 1\), then the Prover sends \(v(p) = f(p).h(p)\) to the Verifier. The Verifier aborts the authentication and rejects unless the equality \(u = v(p)^m q v(p)^n\) is satisfied.

After k successful rounds, the Verifier accepts the authentication.

4.4 Security Analysis

In this subsection, one can examine the completeness, soundness and zero knowledge of the proposed scheme.

**Completeness:** In step (a), \(u = h(p)^m y h(p)^n\). i.e. \(u = v(p)^m y v(p)^n\).

In step (b), using \(v(p) = f(p).h(p)\), one can find \(v(p)^m q v(p)^n\)

\[
= (f(p).h(p))^m q (f(p).h(p))^n
\]

\[
= h(p)^m (f(p)^m q f(p)^n) h(p)^n
\]

\[
= h(p)^m y h(p)^n = u.
\]

Hence the Verifier accepts a correct answer at each repetition, so he accepts the Prover proof of identity with probability 1.

**Soundness:** Suppose the Prover does not possess the secret \(f(p)\). Then, during any given round, the Prover can provide only one of \(v(p) = h(p)\) or \(v(p) = f(p).h(p)\). Therefore, an honest verifier will reject with probability in each round \(\frac{1}{2}\) which implies an over all probability of \(2^{-k}\) that a cheating prover will not be caught.

**Zero knowledge:** Consider the following probabilistic Turing machine \(M'\):

-Step 1: \(M'\) randomly selects a bit \(c\) and a quasi-polynomial \(v(p)\).

-Step 2: For \(c = 0\), \(M'\) computes \(u = v(p)^m y v(p)^n\); for \(c = 1\), \(M'\) computes \(v(p)^m q v(p)^n = (f(p).h(p))^m q (f(p).h(p))^n\)

\[
= h(p)^m (f(p)^m q f(p)^n) h(p)^n
= h(p)^m y h(p)^n = u
\]
Step 3: $M'$ initiates a protocol with the Verifier, sends $u$ to the Verifier; the Verifier replies with the bit $c^1$;

Step 4: For $c = c^1$, $M'$ outputs the triple $(u, c, v(p))$, otherwise it resets to step 1.

Since probability distribution of $h(p)$ in the authentication scheme is assumed to be right invariant, one can obtain the same probability distribution for the $v(p)$'s generated by $M'$ as for Prover’s ones. Moreover, since in case $c = 1$ one can have $v(p)^m q v(p)^n$

$$= (f(p) \cdot h(p))^m q (f(p) \cdot h(p))^n$$

$$= h(p)^m (f(p)^m q f(p)^n) h(p)^n$$

$$= h(p)^m y h(p)^n = u.$$

Thus, using the same assumption, one can obtain the same probability distribution for the $u$'s arising for $c = 0$ and those arising for $c = 1$. As a consequence, One cannot distinguish the two cases, and the probability to have $c = c^1$ is equal to $1/2$.

5. CONCLUSION

In this paper, Diffie-Hellman and Fiat-Shamir like zero-knowledge authentication schemes based on the intractability of quasi-polynomial symmetrical decomposition problem over general non-commutative groups have been proposed and also security issues have been discussed.

APPENDIX

Hash function: There are several ways of conceiving hash function suitable for scheme A, depending on the choice of implementation.

In order to define a hash function, we choose a prime $p$ and set $Z_p$ as the message space $\mathcal{M}$. Then, we define a collision resistance hash function $H : G \in M_2(Z_p) \rightarrow \mathcal{M} = M_2(Z_p), m_{ij} \rightarrow 2^{m_{ij}} \mod p$.

References


About This Journal

ISA is an open access journal published by Scientific Online Publishing. This journal focus on the following scopes (but not limited to):

- Access Control
- Authentication and Authorization
- Database Security
- E-Commerce Security
- Encryption and Decryption
- Grid Security
- Information Hiding and Watermarking
- Information Privacy
- Intrusion Detection
- Network Security
- OS Security
- Security Engineering
- Security for Personal Information
- Security Models
- Security Protocols

Welcome to submit your original manuscripts to us. For more information, please visit our website: http://www.scipublish.com/journals/ISA/

You can click the bellows to follow us:

- Facebook: https://www.facebook.com/scipublish
- Twitter: https://twitter.com/scionlinepub
- LinkedIn: https://www.linkedin.com/company/scientific-online-publishing-usa
- Google+: https://google.com/+ScipublishSOP

SOP welcomes authors to contribute their research outcomes under the following rules:

- Although glad to publish all original and new research achievements, SOP can’t bear any misbehavior: plagiarism, forgery or manipulation of experimental data.
- As an international publisher, SOP highly values different cultures and adopts cautious attitude towards religion, politics, race, war and ethics.
- SOP helps to propagate scientific results but shares no responsibility of any legal risks or harmful effects caused by article along with the authors.
- SOP maintains the strictest peer review, but holds a neutral attitude for all the published articles.
- SOP is an open platform, waiting for senior experts serving on the editorial boards to advance the progress of research together.