International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.181-190
http://dx.doi.org/10.14257/ijsia.2016.10.10.17

An Improved Zero-knowledge Identification Scheme based on Quasi-Dyadic Codes

Mu Han[1], Xiaolin Feng[2] and Shidian Ma[3]

[1,2]*School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China*
[3]*Automotive Engineering Research Institute, Jiangsu University, Zhenjiang 212013, China*
[1]*hanmu@ujs.edu.cn;* [2]*fengxl92@163.com;* [3]*masd@ujs.edu.cn*

Abstract

In this paper we present an improved version of the zero-knowledge identification scheme based on algebraic coding theory. Our protocol is related to the Véron's identification scheme but permits a lower communication complexity by transferring two hash values in each round instead of three. And the protocol decreases the cheating probability to about 1/2 instead of 2/3 which reduces the rounds of the protocol. Furthermore, we construct the parity-check matrix in a quasi-dyadic form in order to dramatically reduce the matrix size. In sum, the new scheme has good properties of having a small matrix size, computation complexity, and for an overall communication cost of 22.8kb for authentication.

Keywords*: Post-quantum cryptography, Zero-knowledge, Identification, Quasi-dyadic, Véron's scheme*

1. Introduction

In 1994, Shor [1] proposed a quantum algorithm for integer factorization, which poses a threat to most cryptosystems in use today. If quantum computers come to reality, the cryptosystems whose security relies on number theory can be broken in polynomial time. Fortunately, there are no quantum attacks known for code-based cryptosystems, which means these cryptosystems can possibly resist to a quantum computer. And code-based cryptosystems [2] are very fast and easy to implement compared to number theory based systems. The first code-based public key cryptographic system [3] was published by McEliece in 1978. McEliece's scheme is considered to be secure after extensively analyzed for more than thirty years. However, the cryptosystem is impractical because of the enormous key size.

There has been a lot of work done by designing special codes so as to reduce the public key size. In 1986, Niederreiter [4] proposed a new code-based scheme by using Generalized Reed-Solomon (GRS) codes which were assumed to allow smaller key sizes. Unfortunately, Niederreiter's proposal was proved to be insecure subsequently. In the following years, a number of cryptosystems [5-10] were proposed by using different codes such as MDPC, QD-Goppa codes, *etc*. And the public key size can be reduced much more by exploiting the Toeplitz structure [11].

An identification scheme can be done by using a zero-knowledge interactive protocol, which is a two-party protocol that enables party P called a prover to prove his identity to the other party V called a verifier, without V being able to learn anything secret or mistaking P for someone else. There has been a number of identification schemes proposed these years [2, 12-15]. In 1993, Stern [13] proposed the first zero-knowledge identification schemes based on hard problem from syndrome decoding. In 1996, Véron

ISSN: 1738-9976 IJSIA

[15] designed a scheme based on the hardness of the general decoding problem that reduced slightly the communication cost. In 2010, Cayrel, Véron and El Yousfi [12] presented a scheme which decreased the communication even more. One year later, Aguilar, Gaborit and Schrek [2] proposed a double circulant scheme which reduced the communication cost and matrix size. However, the matrix size reduction cannot meet with the requirement of storage. These schemes still require too much memory to store the huge matrices.

Our Contribution. In this paper we design an improved zero-knowledge identification scheme with small communication costs as well as matrix size by using quasi-dyadic codes, and make comparisons with other code-based schemes.

Organization of the Paper. First, we recall some backgrounds on code-based cryptography in Section 2. Section 3 describes the code-based zero-knowledge identification scheme proposed by Véron. In Section 4, we introduce our improved identification scheme. Section 5 proves the completeness, zero-knowledge and soundness of the scheme. In Section 6 we discuss the performance of the scheme and make comparisons with the aforementioned schemes. Finally, we conclude in Section 7.

2. Preliminaries

In this section, we recall some backgrounds for code-based cryptography.

C[*n*,*k*,*t*] is a code with length *n*, dimension *k* and the error-correcting capability is up to *t* errors. The codimension of the code is *r* where *r*=*n*-*k*. Let F_q denote a finite field with *q* elements.

Definition 1 (Hamming weight). The Hamming weight of a vector $x \in \mathrm{F}_2^n$ is the number wt(*x*) of its nonzero components.

Definition 2 (Linear codes). A binary (*n*,*r*)-linear code C of length n, dimension *n*-*r* and codimension *r*, is a (*n*-*r*)-dimensional vector subspace of F_2^n. It is spanned by the rows of a matrix $G \in \mathrm{F}_2^{(n-r)\times n}$, called a generator matrix of C. Equivalently, it is the kernel of a matrix $H \in \mathrm{F}_2^{r\times n}$, called a parity-check matrix of C. The codeword $c \in C$ of a vector $m \in \mathrm{F}_2^{(n-r)}$ is $c = mG$. The syndrome $s \in \mathrm{F}_2^r$ of a vector $e \in \mathrm{F}_2^n$ is $s = He^T$. The dual $C^\perp$ of C is the linear code spanned by the rows of any parity-check matrix of C.

Definition 3 (Syndrome Decoding (SD) Problem).

Input: $H \xleftarrow{\$} \mathrm{F}_q^{r\times n}$, $y \xleftarrow{\$} \mathrm{F}_q^r$, and an integer $w > 0$.

Find: a word $s \in \mathrm{F}_q^n$ such that $wt(s) \le w$ and $Hs^T = y$.

This problem is proven to be NP-complete in [16, 17]. A dual version of the SD problem, which uses the generator matrix *G* instead of the parity-check matrix *H* of the code C, is defined as follow.

Definition 4 (General Decoding (GD) Problem).

Input: $G \xleftarrow{\$} \mathrm{F}_q^{k\times n}$, $y \xleftarrow{\$} \mathrm{F}_q^n$, and an integer $w > 0$.

Find: A pair $(m,e) \in \mathrm{F}_q^k \times \mathrm{F}_q^n$, where $wt(e) \le w$ such that $mG + e = y$.

Definition 5 (Dyadic matrix). Given a ring R and a vector $h = (h_0,...,h_{n-1}) \in R^n$, the dyadic matrix $\Delta(h) \in R^{n\times n}$ is the symmetric matrix with components $\Delta_{ij} = h_{i\oplus j}$, where $\oplus$ denotes bitwise exclusive-or. The sequence h is the signature of the dyadic matrix. The set of dyadic $n \times n$ matrices over R is denoted $\Delta(R^n)$. Given $t > 0$, $\Delta(t,h)$ denotes $\Delta(h)$ truncated to its first t rows.

A quasi-dyadic matrix is a block matrix whose components are dyadic submatrices. If *n* is a power of 2, then a $2^k \times 2^k$ dyadic matrix *M* can be recursively characterized as

$$M = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

where A and B are $2^{k-1} \times 2^{k-1}$ dyadic submatrices. It is obvious that the signature $h = (h_0, ..., h_{n-1})$ of a dyadic matrix coincides with its first row. And each row is a permutation of the signature *h*.

Definition 6 (Quasi-Dyadic Code). A quasi-dyadic (QD) code is a linear code which admits a quasi-dyadic parity-check matrix.

3. Code-Based Zero-Knowledge Identification Schemes

There are many zero-knowledge identification protocols based on coding theory. In these protocols, the prover P convinces the verifier V of his identity without revealing any additional information. In this section, we will show one representative scheme as follow.

3.1. The Véron Identification Scheme

In 1996, Véron [17] proposed a dual version of Stern scheme, which reduces the cost of communication but increases the key size. The scheme is based on general decoding problem.

Let G denote the public generator matrix of the code over F_2. The prover P receives the secret key $(m,e) \leftarrow F_2^k \times F_2^n$, s.t. $wt(e) = w$. Let $y = mG + e$, the prover's public key is $pk = (y, G, w)$. The Véron protocol is given in Figure 1.

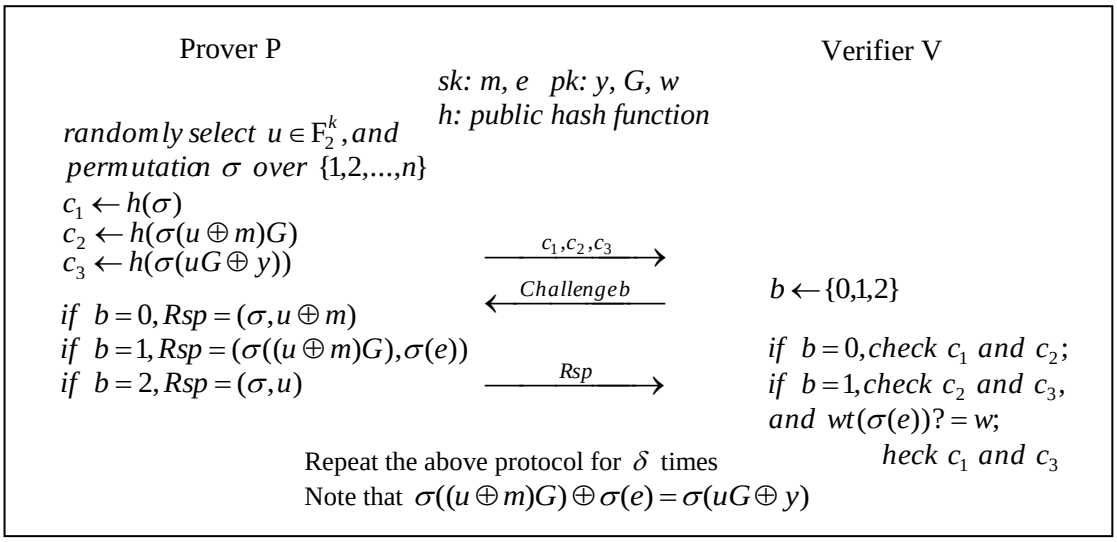


Figure 1. Véron Identification Protocol

As shown in Figure 1, the Véron protocol, as the Stern's one, is a three-pass interaction. In each round, the cheater's probability to win is 2/3, so the scheme needs $\delta = 28$ rounds to reduce the cheating probability to 2^{-16}.

4. A New Code-Based Zero-Knowledge Identification Scheme

In this section, we propose an improved identification scheme based on general decoding problem. This protocol is able to reduce the matrix size by using quasi-dyadic codes and the communication cost by sending fewer commitments. The protocol includes two parts: the key generation part and the identification part.

4.1. Key Generation Algorithm

A binary linear (*n*,*k*,*w*) code C, *r*=*n*-*k*. Let $H \in \mathrm{F}_q^{r\times n}$ denote the public parity check matrix of code C. Assuming that *H* is a quasi-dyadic matrix, the matrix size can be characterized in a simplified way. Let $G \in \mathrm{F}_q^{k\times n}$ denote the generation matrix of code C. Choose a random vector $m \in \mathrm{F}_q^k$ and $e \in \mathrm{F}_q^n$ with Hamming weight $wt(e) = w$. Perform $mG + e$ to get vector $y \in \mathrm{F}_q^n$. The secret key is (m,e), the public key is (y,G,w). The key generation algorithm is shown in Figure 2.

KEYGEN:
(n,k,w) *code C, generation matrix* $G \in \mathrm{F}_q^{k\times n}$
$m \in \mathrm{F}_q^k$, $e \in \mathrm{F}_q^n$, s.t. $wt(e) = w$, $y \leftarrow mG + e$
Output: $(sk, pk) = ((m,e),(y,G,w))$

Figure 2. Key Generation Algorithm

4.2. Identification Protocol

Each round in our new protocol is a five-pass interaction between the two parties, and the cheating probability for a malicious prover is very close to 1/2 in each round. The protocol is shown in Figure 3. The symbols c_1, c_2, c_3 denote three commitments, *h*(.) denotes a hash function and *Rsp* denotes a response corresponding to a challenge *b*.

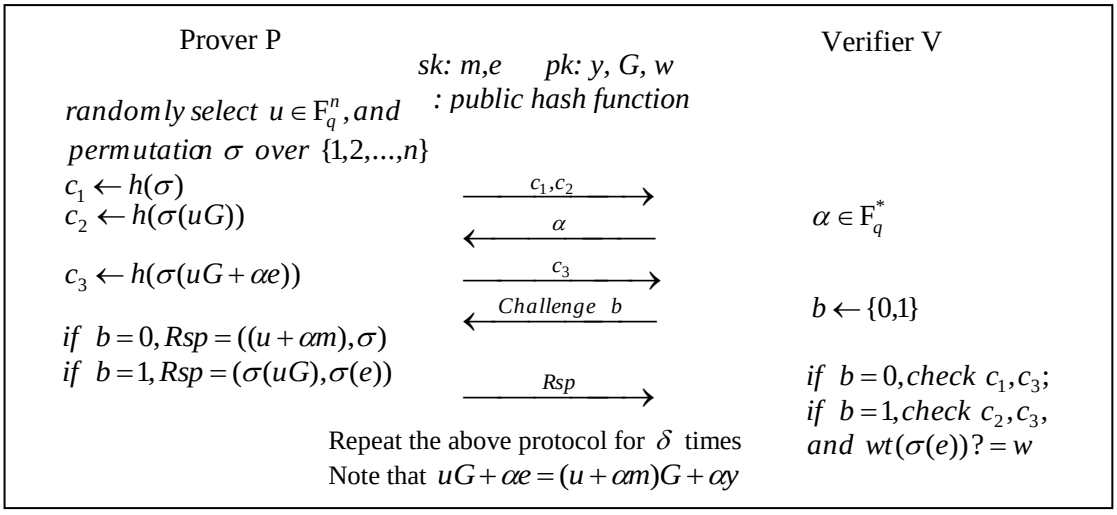


Figure 3. Identification Protocol

Since the verifier can recover two of the three hash values sent by the prover in each round, the protocol can be modified as follow: the prover sends a hash *h* of c_1, c_2 rather than sending both of them before he receives α from the verifier, then he answers to the challenge together with the missing hash value (one of c_1, c_2) after receiving the challenge bit *b*. In the verification step, the verifier is able to compute the hash *h* from the hash value recovered from the answer and the received hash value in the answer. In a general situation, the prover sends a hash of a sequence of the first two hash values from all rounds. In this case only the missing hash value needs to be sent in each round, thus

reducing the communication cost significantly. After δ rounds, the verifier checks the hash value *h*. Moreover, this way of proceeding is secure the same as the one in Figure 3 in the random oracle model. The interaction of each round is shown in Figure 4.

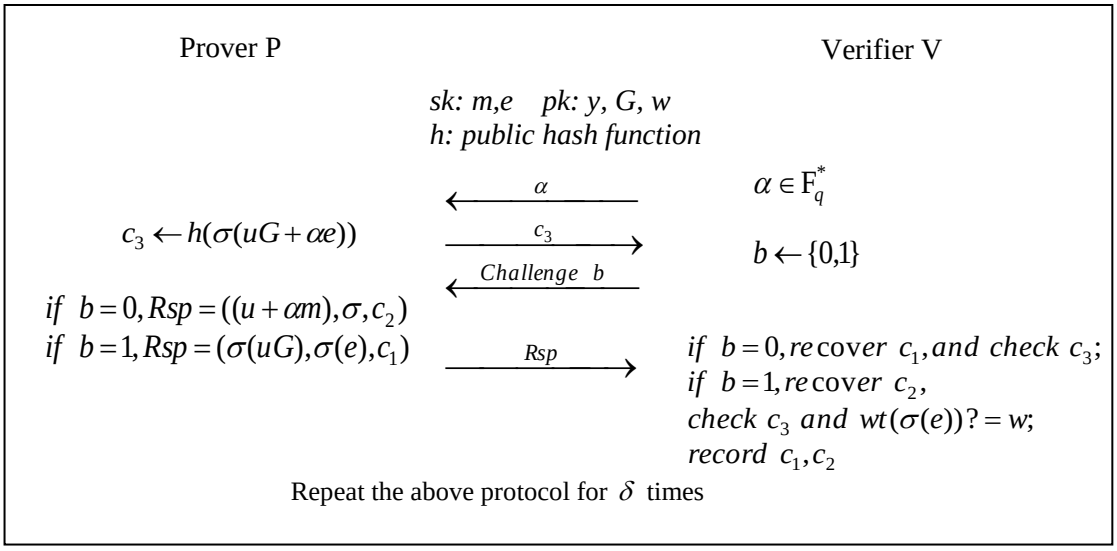


Figure 4. Two Hash Values Sent in Each Round

5. Security Proof

In this subsection, we provide the proofs for the completeness, zero-knowledge and soundness of the scheme. Since the protocols in Figure 3 and Figure 4 are the same, we proof the security of the protocol in Figure 3 instead of Figure 4.

Completeness: As shown in Figure 3, the random vector *u* and permutation σ are chosen by the prover, if he knows the secret key *s*, he can answer correctly no matter which bit challenge *b* is, *i.e.*, $c_1 = h(\sigma)$, $c_2 = h(\sigma(uG))$ and $c_3 = h(\sigma(uG + \alpha e))$, $wt(\sigma(e)) = w$.

Soundness: A malicious prover is able to success in each round with a probability no more than $(2q+1)/4q$.

In order to cheat the verifier, a malicious prover devises the strategies as follows to deal with the possible challenges which the verifier sends. In both strategies, the prover guesses α' as the value of α chosen by the verifier. In this case, he has a chance of $1/q$ to guess correctly. In the first strategy (st_1), the prover hopes to receive challenge $b = 0$. He chooses u, σ at random and $m', e', \bar{e}$ such that $m'G + e' = y$, $wt(e') \neq w$ and $wt(\bar{e}) = w$. Then he computes $c_1 = h(\sigma)$, $c_2 = h(\sigma(uG + \alpha'(e' + \bar{e})))$ and $c_3 = h(\sigma(uG + \alpha e'))$. Thus, he will be able to answer the challenge $b = 0$, and $b = 1$ with a probability of 1/q . In the second strategy (st_2), the prover hopes to receive challenge $b = 1$. He chooses u, σ at random and e' s.t. $wt(e') = w$. Then he computes $c_1 = h(\sigma)$, $c_2 = h(\sigma(uG))$ and $c_3 = h(\sigma(uG + \alpha e'))$. Thus, he can answer the challenge $b = 1$. Therefore, a strategy set $st = \{st_1, st_2\}$ to success in one round is

$$\Pr[success] = \sum_{i=1}^{2} P(st = st_i)[P(b = i-1) + (2-i)P(b = 2-i)P(\alpha = \alpha')] = (2q+1)/4q \cdot$$

Proposition 1. If an honest verifier $\bar{V}$ accepts a cheating prover $\tilde{P}$ proof with probability $\geq ((2q+1)/4q)^{\delta} + \varepsilon$, then there exists a polynomial time probabilistic

machine M which, with overwhelming probability, either retrieves the secret key or finds a collision for the hash function.

Proof. Let T be the execution tree of $(\tilde{P},\bar{V})$ corresponding to all possible questions of the verifier when the adversary has a random tape RA. $\bar{V}$ may ask $2q$ possible questions at each stage. First we are going to show that, unless a hash collision has been found, the secret key can be computed from a vertex with $q+1$ sons. Then we will show that a polynomial time M can find such a vertex in T with overwhelming probability.

Let V be a vertex with $q+1$ sons. This corresponds to a situation where 3 commitments c_1,c_2,c_3 have been made and where the $q+1$ queries were properly answered. Let $(c_3,(u+\alpha m),\sigma)$, $(c_3,\sigma(uG),z)$, $(c_3',(u'+\alpha' m'),\sigma')$, $(c_3',\sigma'(u'G),z')$ be the answers corresponding to the queries $(\alpha,0)$, $(\alpha,1)$, $(\alpha',0)$, $(\alpha',1)$, respectively. Note that $\alpha\neq\alpha'$ and z (resp. z') represents the expected value $\sigma(e)$ (resp. $\sigma(e')$), so $wt(z)=wt(z')=w$. We have

$$\begin{gathered}h(\sigma)=c_1=h(\sigma')\\ h(\sigma(uG))=c_2=h(\sigma'(u'G))\\ h(\sigma((u+\alpha m)G)+\alpha\sigma(y))=c_3=h(\sigma'((u'+\alpha' m')G)+\alpha'\sigma(y))\\ h(\sigma(uG)+\alpha z)=c_3=h(\sigma'(u'G)+\alpha' z')\end{gathered}$$

Thus, either a collision for the hash function has been found, or else

$$\frac{1}{\alpha+\alpha'}(\alpha m+\alpha' m')G+\sigma^{-1}(z)=y,$$

so, $e=\sigma^{-1}(z)$ with weight w and $\bar{m}=\frac{1}{\alpha+\alpha'}(\alpha m+\alpha' m')$ are valid secret keys that can be used to impersonate the real prover P.

Now, the assumption implies that the probability for T to have a vertex with $q+1$ sons is at least ε. Indeed, let us consider RA as a set of μ elements, where $\tilde{P}$ randomly picks its values, and let Q be the set $\mathrm{F}_q^*\times\{0,1\}$. These two sets are considered as probability spaces both of them with the uniform distribution.

A triple $(c,\alpha,b)\in(RA\times Q)^\delta$ represents the commitments, answers and queries exchanged between $\tilde{A}$ and $\bar{B}$ during an identification process. We will say that (c,α,b) is a "valid" triple, if the execution of $(\tilde{A},\bar{B})$ leads to the success state.

Let V be the subset of $(RA\times Q)^\delta$ composed of all the valid pairs. The hypothesis of the proposition means that:

$$\frac{card(V)}{card((RA\times Q)^\delta)}\geq\left(\frac{2q+1}{4q}\right)^\delta+\varepsilon.$$

Let Ω_δ be a subset of RA^δ such that:

-If $c\in\Omega_\delta$, then $(2q+1)^\delta+1\leq card\{(\alpha,b),(c,\alpha,b)\ be\ valid\}\leq(4q)^\delta$,

-If $c\in RA^\delta\setminus\Omega_\delta$, then $0\leq card\{(\alpha,b),(c,\alpha,b)\ be\ valid\}\leq(2q+1)^\delta$.

Then, $V=\{valid\ (c,\alpha,b),c\in\Omega_\delta\}\bigcup\{valid\ (c,\alpha,b),c\in RA^\delta\setminus\Omega_\delta\}$, therefore:

$card(V)\leq card(\Omega_\delta)(4q)^\delta+(\mu^\delta-card(\Omega_\delta))(2q+1)^\delta$.

Thus

$$\frac{card(V)}{card((RA\times Q)^{\delta})} \le \left(\frac{card(\Omega_{\delta})}{card(RA^{\delta})} + (2q+1)^{\delta} \left((4q)^{-\delta} - \frac{card(\Omega_{\delta})}{card((RA\times Q)^{\delta})} \right) \right)$$
$$\le \frac{card(\Omega_{\delta})}{card(RA^{\delta})} + \left(\frac{2q+1}{4q} \right)^{\delta}$$

It follows that:

$$\frac{card(\Omega_{\delta})}{card(RA^{\delta})} \ge \varepsilon .$$

This shows that the probability that an adversary might answer to (at least) $(2q+1)^{\delta}+1$ of the verifier's queries, by choosing random values, is greater than ε. Now, if more than $(2q+1)^{\delta}+1$ queries are bypassed by an adversary then $T(RA)$ has at least $(2q+1)^{\delta}+1$ leaves, *i.e.*, $T(RA)$ has at least a vertex with $q+1$ sons.

So, by repeating the interaction $1/\varepsilon$ times, the adversary may find an execution tree T with such a vertex with probability very close to 1. This proves that either the hash function is not collision-free, or the qSD problem is intractable in polynomial time. The probability of an adversary to success in δ rounds is: $\Pr(success) \le 1/2^{\delta}$.

Zero-Knowledge: The zero-knowledge property is that no information can be deduced from the protocol in polynomial time except the knowledge of the public data.

The idea is to build a simulator which is indistinguishable from the real execution in polynomial time. The simulator is built to make a valid instance in each round. The challenge b=0 can be answered by a random permutation σ', a random vector v, $c_1 = h(\sigma')$ and $c_3 = h(\sigma'(vG + \alpha e))$. Notice that (v, σ') and $(u + \alpha m, \sigma)$ are indistinguishable. The challenge b=1 can be answered by a random permutation π, a vector z of weight w, a random vector u, $v = \pi(uG)$, $c_2 = h(v)$ and $c_3 = h(v + \alpha z)$. Notice that (v, z) and $(\sigma(uG), \sigma(e))$ are indistinguishable.

Thus, in 2δ rounds on average, the simulator produces a communication tape indistinguishable from another communication tape corresponding to a fair identification process executed in δ rounds.

6. Parameters for Authentication

The parameters for Code C are (n, k, w), the co-dimension r=k=n/2. Let N be the number of bits needed to encode an element of F_q, l_h denote the length of the public hash function h, l_{σ} denote the length of the seed used to generate the permutation σ, and δ denote the number of rounds. In our scheme, we design the parity-check matrix H in a quasi-dyadic form. The performance of our scheme is shown below:

Matrix size: $N \times n$

Length of the public identification: $N \times r$

Length of the secret key: $N \times (k+n)$

Communication cost: $l_h + \delta(2l_h + N + 1 + (k + l_{\sigma} + N \times n \times 2)/2)$

Prover's computation: $\delta((k \times n + w + k)multiplies + (k \times n + w + k)additions)$

We use the following parameters the same as those in the CVE scheme: $n = 128, k = 64, w = 49, q = 256$. In Stern and Véron schemes, we set the parameters as $n = 700$, $k = 350$, $w = 75$. The security of the above schemes is at least 2^{80}. We suggest

that the length of the seed is 128 bits and the hash value is 160 bits. The comparisons among our scheme and others for a 2^{-16} cheating probability are shown in Table 1, the matrix size and the communication cost comparisons are also shown in Figure 5 and Figure 6, respectively. It is obviously to observe that the matrix size and communication cost in our scheme are much less than other schemes.

Table 1. The Performances among Identification Schemes for a 2^{-16} Cheating Probability

	Stern 3	Stern 5	Véron	CVE	Our scheme
Rounds	28	16	28	16	16
Matrix size(bits)	122500	122500	122500	32768	1024
Public Id(bits)	350	2450	700	512	1024
Secret key(bits)	700	4900	1050	1024	1536
Communication(bits)	42019	62272	35485	39056	23344
Prover's computation	$2^{22.72}$ op. over F_2	$2^{21.91}$ op. over F_2	$2^{22.71}$ op. over F_2	$2^{16.02}$ mult+ $2^{16.02}$ add op. over F_{256}	$2^{17.02}$ mult+ $2^{17.02}$ add op. over F_{256}

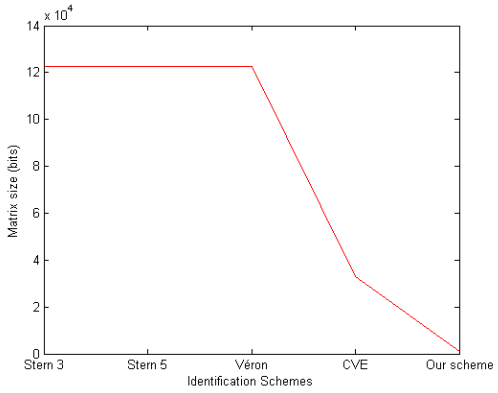


Figure 5. Matrix Size Comparisons

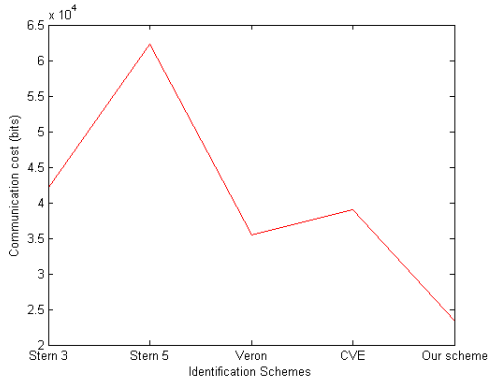


Figure 6. Communication Cost Comparisons

7. Conclusion

In this paper, we presented a new way to reduce the public matrix size and the communication cost for zero-knowledge identification scheme. The proposed scheme is

based on quasi-dyadic codes over a q-ary field. We devised a new interactive protocol to cut down the number of commitments in each round, thus reduce the communication cost for the overall scheme to 23344 bits. And the security analyses show that the proposed scheme meet with the completeness, soundness and zero-knowledge properties. Such secure and small parameters makes it possible to be applied in new potential scenarios such as smart cards, VANET or apple pay.

Acknowledgments

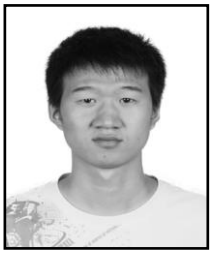
This research is supported by the National Natural Science Foundation of China (No. 61300229) and Six Talent Peaks Project of Jiangsu Province (No. DZXX-012).

References

[1] P. W. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on, **(1994)**, pp. 124-134.
[2] C. Aguilar, P. Gaborit and J. Schrek, "A new zero-knowledge code based identification scheme with reduced communication", IEEE Information Theory Workshop 2011, pp. 648-652.
[3] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory", Technical report, DSN Progress report, **(1978)**, pp. 42-44.
[4] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory", Problems of Control and Information Theory, vol. 15, no. 2, **(1986)**, pp. 159-166.
[5] M. Baldi, F. Bambozzi and F. Chiaraluce, "On a family of circulant matrices for quasi-cyclic low-density generator matrix codes", IEEE Transactions on Information Theory, vol. 57, no. 9, **(2011)**, pp. 6052-6067.
[6] M. Baldi, M. Bianchi and F. Chiaraluce, "Optimization of the parity-check matrix density in QC‐LDPC code-based McEliece cryptosystems", Workshop on Information Security Over Noisy and Lossy Communication Systems (IEEE ICC 2013).
[7] S. Heyse, I. von Maurich and T. Güneysu, "Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices", Cryptographic Hardware and Embedded Systems (CHES) 2013 LNCS, **(2013)**, pp. 273-292.
[8] C. Löndahl, T. Johansson, M. K. Shooshtari, M. Ahmadian-Attari and M. Reza-Aref, "Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension", Des. Codes Cryptography, **(2015)**, pp. 1-19.
[9] R. Misoczki and P. S. L. M. Barreto, "Compact McEliece keys from Goppa Codes", Selected Areas in Cryptography (SAC 2009). LNCS, vol. 5867, **(2009)**, pp. 376-392.
[10] R. Misoczki, J.-P. Tillich, N. Sendrier and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes", 2013 IEEE International Symposium on Information Theory Proceedings (ISIT), **(2013)**, pp. 2069-2073.
[11] B. Malek, A. Miri and L. Orozco-barbosa, "Backward Link Authentication For RFID Tags", 2011 IEEE International Conference on RFID-Technologies and Applications, **(2011)**, pp. 348-352.
[12] P.-L. Cayrel, P. Véron and S. M. E. Y. Alaoui, "A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem", Selected Areas in Cryptography (SAC 2010), LNCS, 6544, pp. 171-186.
[13] J. Stern, "A New Identification Scheme Based on Syndrome Decoding", Advances in Cryptology (CRYPTO' 93), LNCS, (1994), pp. 13-21.
[14] J. Stern, "Designing identification schemes with keys of short size", Advances in Cryptology (CRYPTO' 94), LNCS, **(1994)**, pp. 164-173.
[15] P. Véron, "Improved Identification Schemes Based on Error-Correcting Codes", Applicable Algebra in Engineering, Communication and Computing, vol. 8, no. 1, **(1996)**, pp. 57‐69.
[16] S. Barg, "Some new NP-complete coding problems", Probl. Peredachi Inf., vol. 30, no. 3, **(1994)**, pp. 23-28.
[17] E. Berlekamp, R. McEliece and H. van Tilborg, "On the inherent intractability of certain coding problems", IEEE Transactions on Information Theory, vol. 24, no. 3, **(1978)**, pp. 384-386.

Authors

Mu Han, she was born in 1980. She received the B.S. and M.S. degree from HeFei University of Technology (HFUT), Hefei, in 2004 and 2007, respectively. She received the Ph.D. degree with the Department of Computer Science and Engineering, Nanjing University of Science and Technology (NUST), in 2011. She has worked for Jiangsu University since 2011, and now she is an Associate Professor. Her main research interests include information security, cryptography, and coding theory.



Xiaolin Feng, he was born in Hubei Province, China, in 1992. He received the B.S. Degree from Jiangsu University, Zhenjiang, in 2014. He is currently pursuing the M.S. Degree with the Department of Computer Science and Communication Engineering, Jiangsu University. His reasearch interests include information security, cryptography, and coding theory.

Shidian Ma, he was born in 1978. He received the B.S. and M.S. degree from HeFei University of Technology (HFUT), Hefei, in 2002 and 2005, respectively. He has worked for Jiangsu University since 2011, and now he is an Associate Professor. His main research interests include wireless communications, automobile electronic control, and road traffic safety control.