LDPC符号を用いたゼロ知識証明型認証方式について（II）

伊東 春香[1]　廣友 雅徳[1]　福田 洋治[2]　毛利 公美[3]　白石 善明[4]

概要：現在広く用いられている認証方式の安全性は，ほとんどが素因数分解，離散対数問題の困難性に基づいており，これらの問題が効率よく解けてしまえば，安全に利用できなくなる．このような課題に対して，耐量子計算機暗号やそれを応用した認証，署名方式が多く提案されている．しかしながら，それらの方式は計算量が大きくなるという問題がある．この問題に対して，著者らはLDPC符号を用いたゼロ知識証明型認証方式を提案している．この方式は，耐量子性である2元シンドローム復号問題に基づくゼロ知識証明型認証方式を改良し，LDPC符号の疎なパリティ検査行列を利用することで，認証の計算量を削減している．本稿では，著者らが提案している認証方式のセキュリティレベル，計算量，安全性について詳細に考察し，示す．

キーワード：ゼロ知識証明，認証，耐量子性，LDPC符号，シンドローム復号

On the Zero Knowledge Proof Type Authentication Scheme Using LDPC Codes (II)

Haruka Ito[1]　Masanori Hirotomo[1]　Youji Fukuta[2]　Masami Mohri[3]　Yoshiaki Shiraishi[4]

Abstract: Most of the safety of the currently widely used authentication method is based on the difficulty of prime factorization and discrete logarithm problem, and if these problems can be solved efficiently, it can not be used safely. In response to such a problem, many proposals have been made on post quantum computer cryptography and authentication and signature schemes applying the same. However, these methods have a problem that the calculation amount becomes large. In response to this problem, we have proposed a zero knowledge proof type authentication method using LDPC codes. This method improves the zero knowledge proof type authentication method based on the binary syndrome decoding problem which is durability, and the complexity of authentication is reduced by using the sparse parity check matrix of the LDPC codes. In this paper, the security level, computational complexity and safety of the authentication method proposed by the our are discussed and presented in detail.

Keywords: zero knowledge proof, authentication, post quantum, LDPC codes, syndrome decoding

1. はじめに

現在広く用いられている認証方式の大部分は，素因数分解や離散対数問題の困難性に基づいて安全性が保障されている．よって，素因数分解，離散対数問題が効率よく解けてしまえば，これらは全て安全に利用できなくなる．実際に，量子コンピュータ上でこの二つの問題を確率的多項式時間で解く方法が提案されており，量子コンピュータが実現されれば，各種プロトコルは安全に利用できなくなる．このような課題に対して，耐量子計算機暗号やそれを応用した認証，署名方式が多く提案されている．しかしながら，それらの方式は計算量が大きくなるという問題がある．

本研究では，耐量子性を有し，計算量が少ない認証方式を開発することを目的としている．公開鍵暗号としてLDPC

[1] 佐賀大学大学院工学系研究科
Graduate school of Science and Engineering, Saga University
[2] 近畿大学理工学部情報学科
Faculty of Science and Engineering, Kindai University
[3] 岐阜大学大学院工学研究科
Graduate School of Engineering, Gifu University
[4] 神戸大学大学院工学研究科
Graduate School of Engineering, Kobe University

符号を用いた計算量の小さい暗号 [1] や，公開鍵暗号の技術を応用したグループ認証方式 [2] が提案されている．本研究でこれらの応用を視野に入れ，耐量子性を有し，計算量が少ない認証方式を開発することを目標としている．

最近接符号問題に基づく公開鍵暗号として McEliece 暗号 [3] があり，2 元シンドローム復号問題に基づく公開鍵暗号として Niederreiter 暗号 [4] がある．これらに LDPC 符号 [5]，QC-LDPC 符号 [6]，MDPC 符号 [7] を用いて改良した暗号が提案されている [8]．しかし，計算量が非常に大きくなっている．一方，著者らは文献 [9] において，LDPC 符号を用いたゼロ知識証明型認証方式を提案している．この方式は Stern によって提案された 2 元シンドローム復号問題に基づくゼロ知識証明型認証方式を改良したものである．

本稿では，著者らが [9] において提案した，LDPC 符号を用いたゼロ知識証明型認証方式のセキュリティレベル，計算量，安全性について詳細に考察する．提案方式では，LDPC 符号の疎なパリティ検査行列の特徴を利用することで，Stern の認証方式よりもさらに計算量を削減することができることを示す．

2. 2 元シンドローム復号問題に基づくゼロ知識証明型認証方式

2.1 ゼロ知識証明型認証

ゼロ知識証明とは，証明者が知識を漏らすことなく検証者に命題などを証明する方法である．検証者 V が証明者 P が正当か否かを判定する認証について考える．P だけが持つ秘密情報 x を V に示すことで認証できるが，x を他者に開示することは嬉しくない．ゼロ知識証明型認証方式では「P は x を知っている」という命題 X に対し，x を開示することなく，P が V に命題 X を証明することで認証を行う．証明される命題 X には，「巨大な合成数の素因子を知っている」，「離散対数問題の解を知っている」など公開鍵暗号に利用されるものがある．ゼロ知識証明型認証方式は，次の特徴を持つ．

- 完全性：命題 X が真の場合，V は高確率で受理する
- 健全性：命題 X が偽の場合，V が受理する確率は無視できるほど小さい
- ゼロ知識性：P と V の対話証明で得られるデータは模倣できる

模倣とは，P と V の対話証明で得られるデータと識別ができない対話データを秘密情報 x を用いずに作成することである．x を不正に読み取ろうとする攻撃者は P と V の対話を x を用いずに模倣できるとする．このとき命題 X が真の場合，「命題 X が真である」以外の知識を攻撃者が得られないことを示している．

ゼロ知識証明は 2 者間でデータを交換し合う対話証明である．完全性・健全性は，ゼロ知識証明に限らず対話型証明と共通のものであり，ゼロ知識性があってはじめてゼロ知識証明となる．

2.2 2 元シンドローム復号問題

定義 1 2 元シンドローム復号問題

インスタンス： 2 元体 F_2 上の $k < n$ となる $n-k$ 行 n 列の行列 $\mathbf{H}$，$n-k$ 次元の行ベクトル $\boldsymbol{s}$，整数 $t > 0$

問題： $\mathbf{H}\boldsymbol{x}^T = \boldsymbol{s}^T$ を満たすハミング重みが t 以下の n 次元の行ベクトル $\boldsymbol{x}$ を求めよ．

この問題は，誤り訂正能力 t のパリティ検査行列 $\mathbf{H}$ とシンドローム $\boldsymbol{s}$ を与えて，ハミング重みが最小となる誤りベクトル $\boldsymbol{x}$ を求める問題となっている．

2 元シンドローム復号問題は NP 困難である [10]．しかし，$\mathbf{H}$ が特殊な構造をもっていた場合，容易な問題になり得る．例えば，リードソロモン符号などの線形符号の一部には距離 t までの誤りを効率良く訂正する代数的復号法が知られており，そのような符号と t が用いられた場合には，問題は容易になる．

Stern は，2 元シンドローム復号問題に基づくゼロ知識証明型認証方式として Stern の認証方式を提案している [11]．

3. LDPC 符号を用いたゼロ知識証明型認証方式

著者らは，文献 [9] において LDPC 符号を用いたゼロ知識証明型認証方式を提案している．この方式は Stern の認証方式 [11] を改良した認証方式である．Stern の認証方式において使用するパリティ検査行列 $\mathbf{H}$ の代わりに，LDPC 符号の疎なパリティ検査行列 $\mathbf{H}_l$ を利用する．

Stern の認証方式に疎なパリティ検査行列を利用する利点として，計算量が削減できることがあげられる．ベクトルと疎な行列の計算は，通常のベクトルと行列の計算より計算量が下がることが明らかである．具体的には，鍵生成，コミットメント，検証におけるシンドローム計算の計算量が下がる．

3.1 認証方式

LDPC 符号を用いた 2 元シンドローム復号問題に基づくゼロ知識証明型認証方式を説明する．証明者 P と検証者 V による 3 回のやり取りを 1 ラウンドとし，その 1 ラウンドの流れを図 1 に示す．この提案方式では秘密鍵，公開鍵をそれぞれ次のように生成し，以下のように手続きする．

秘密鍵

- ハミング重み $w(\leq t)$ の n 次元ベクトル $\boldsymbol{x}$
- 誤り訂正能力 t，$n-k$ 行 n 列の LDPC 符号の疎なパリティ検査行列 $\mathbf{H}_l$
- 行重み u，列重み u である $n-k$ 行 $n-k$ 列のランダムな正則行列 $\mathbf{S}$[*1]

[*1] 行重み u，列重み u のように全ての行重み，列重みを一定にした

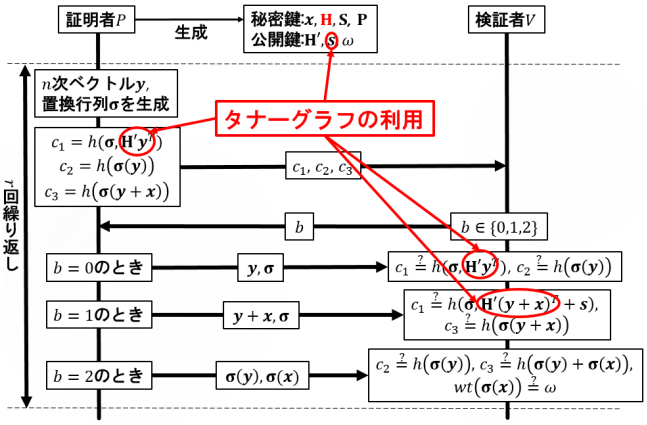

図 1　認証方式の流れ

- n 行 n 列のランダムな置換行列 $\mathbf{P}$

公開鍵

- $n-k$ 行 n 列の行列 $\mathbf{H}'(=\mathbf{SH}_l\mathbf{P})$
- $n-k$ 次元ベクトルのシンドローム $\boldsymbol{s}(=\boldsymbol{x}\mathbf{H}'^T)$
- ハミング重み w

ここでシンドローム $\boldsymbol{s}$ を計算する際に，タナーグラフを用いたシンドローム計算を行う．

Step1. 初期化：証明者 P は n 次元ベクトル $\boldsymbol{y}$ と置換 σ を生成する．

Step2. コミットメント：P はハッシュ関数 $h()$ を用いて，c_1, c_2, c_3 を次のように計算し，検証者 V に送信する．

$$c_1 = h(\sigma, \mathbf{H}'\boldsymbol{y}^T)$$
$$c_2 = h(\sigma(\boldsymbol{y}))$$
$$c_3 = h(\sigma(\boldsymbol{y}+\boldsymbol{x}))$$

ここで c_1 を計算する際に，タナーグラフを用いたシンドローム計算を行う．

Step3. チャレンジ：V は $b \in \{0,1,2\}$ から一つ値を選び，P に送信する．

Step4. レスポンス：P は b の値によって，次を V に送信する．

$b=0$ のとき，$(\boldsymbol{y}, \sigma)$

$b=1$ のとき，$(\boldsymbol{y}+\boldsymbol{x}, \sigma)$

$b=2$ のとき，$(\sigma(\boldsymbol{y}), \sigma(\boldsymbol{x}))$

Step5. 検証：V は b の値に従って，次が成立するか検証する．

$b=0$ のとき，$c_1 = h(\sigma, \mathbf{H}'\boldsymbol{y}^T), c_2 = h(\sigma(\boldsymbol{y}))$

$b=1$ のとき，$c_1 = h(\sigma, \mathbf{H}'(\boldsymbol{y}+\boldsymbol{x})^T + \boldsymbol{s}^T), c_3 = h(\sigma(\boldsymbol{y}+\boldsymbol{x}))$

$b=2$ のとき，$c_2 = h(\sigma(\boldsymbol{y})), c_3 = h(\sigma(\boldsymbol{y}) + \sigma(\boldsymbol{x})), W_H(\sigma(\boldsymbol{x})) = w$

ここで $b=0,1$ のとき c_1 を検証する際に，タナーグラフを用いたシンドローム計算を行う．

Step1〜5 の操作を r 回繰り返す．与えられた実数 ε に対して，検証の受理率が $1-\varepsilon$ 未満であれば認証失敗，そうでなければ認証成功とする．この方式において，1 回の繰り返しにおいて誤認証する確率は $\frac{2}{3}$ である．例えば，ISO/IEC-9798-5 で規定される認証失敗確率 $2^{-16}, 2^{-32}$ にするためには，それぞれ 28 回，56 回繰り返す必要がある．

3.2　疎なパリティ検査行列を用いた 2 元シンドローム復号問題

提案方式では，公開鍵から秘密鍵を求める困難性を 2 元シンドローム復号問題に帰着させている．本節では，2 元シンドローム復号問題に LDPC 符号の疎なパリティ検査行列を用いる方法を説明し，数値例を示す．

提案方式では，2 元シンドローム復号問題のパリティ検査行列 $\mathbf{H}$ に疎なパリティ検査行列 $\mathbf{H}_l$ を用いることを考えている．このため，LDPC 符号の復号法としてよく用いられる反復復号法を利用することで，2 元シンドローム復号問題を解く計算量が小さくなる可能性がある．よって，Stern の認証方式において $\mathbf{H}$ の代わりに疎なパリティ検査行列 $\mathbf{H}_l$ を用いた場合，公開鍵であるシンドローム $\boldsymbol{s}$ と疎なパリティ検査行列 $\mathbf{H}_l$ から秘密鍵である n 次元ベクトル $\boldsymbol{x}$ を求めることが容易になる．ゆえに，秘密鍵が不正者に漏れてしまう可能性があり，認証方式として望ましくない．一方，反復復号法はパリティ検査行列に短いサイクルが含まれている場合，復号能力が低下し正しい誤りを求められなくなる．この性質を利用し，パリティ検査行列の行重みと列重みをタナーグラフに短いサイクルができる程大きくし，反復復号法によって公開鍵 $\boldsymbol{s}, \mathbf{H}_l$ から秘密鍵 $\boldsymbol{x}$ を求めることを困難にする．この性質については，4 章において詳しく説明する．

提案方式では，次のような処理でパリティ検査行列を変形する．行重み u，列重み u の正則行列 $\mathbf{S}$ と，置換行列 $\mathbf{P}$ をそれぞれランダムに生成する．$\mathbf{H}_l$ の左から $\mathbf{S}$ を，右から $\mathbf{P}$ を掛けた行列を $\mathbf{H}'(=\mathbf{SH}_l\mathbf{P})$ とする．$\mathbf{H}'$ は $\mathbf{H}_l$ より行重みと列重みが大きくなり，短いサイクルを持つ行列になる．$\mathbf{H}'$ を公開鍵として公開し，$\mathbf{H}_l, \mathbf{S}, \mathbf{P}$ を秘密鍵とする．これにより公開鍵 $\boldsymbol{s}, \mathbf{H}'$ から $\mathbf{H}'\boldsymbol{x}^T = \boldsymbol{s}^T$ を満たす秘密鍵 $\boldsymbol{x}$ を求めることは困難となる．また $\mathbf{S}, \mathbf{P}$ を $\mathbf{H}_l$ に掛けたことによって，$\mathbf{H}'$ から $\mathbf{H}_l$ を求めることを不可能にする．

例 1　誤り訂正能力 1，符号長 10，符号化率 $\frac{1}{2}$，行重み 2，列重み 4 の (2,4) 正則 LDPC 符号のパリティ検査行列を例にして考える．

とき，行列 $\mathbf{S}$ が正則にならない場合がある．その場合はいずれかの行重みを 1 増やすことで，行列 $\mathbf{S}$ を正則にする．

$$\mathbf{H}_l = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

5 行 5 列の正則行列 $\mathbf{S}$ と，10 行 10 列の置換行列 $\mathbf{P}$ をランダムに生成する．

$$\mathbf{S} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$\mathbf{H}' = \mathbf{S}\mathbf{H}_l\mathbf{P}$ を計算すると次の行列となる．

$$\mathbf{H}' = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\mathbf{S}$ の行重みが u，$\mathbf{H}_l$ の行重みが d_r のとき，$\mathbf{H}_l$ が疎な行列であれば，$\mathbf{H}'$ の行重みは ud_r になることが期待される．このように $\mathbf{H}'$ の各行の 1 の数を多くすることで長さ 4 や 6 のような短いサイクルを作ることができる．これにより，反復復号法では復号が正しくできなくなる．実際に長さ 4 や 6 のサイクルができることについては，4 章において証明する．

3.3 タナーグラフを用いたシンドローム計算

LDPC 符号のパリティ検査行列 $\mathbf{H}_l$ の 1 は非常に少ない．そのため，$\mathbf{H}_l$ に行重み u の行列 $\mathbf{S}$ を掛けて作られる $\mathbf{H}'$ も

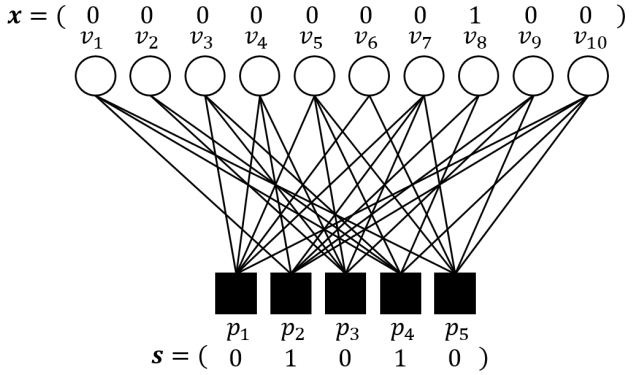

図 2 タナーグラフを利用したシンドローム計算

1 の数は少ないことになる．この性質を利用して，タナーグラフを利用したシンドローム計算を行う．

タナーグラフの変数ノードの集合を $V = \{v_1, v_2, ..., v_n\}$ とし，検査ノードにの集合を $P = \{p_1, p_2, ..., p_m\}$ とする．変数ノード v から v に接続する全ての検査ノードに対して，v に対応する受信語を送信する．検査ノードはパリティ検査条件に対応しているため，検査ノード p に接続する変数ノードの集合の和が p の値となる．求められた $(p_1\ p_2\ ...\ p_{n-k})$ がシンドロームの値となる．

例 2 例 1 における $\mathbf{H}'$ に対応したタナーグラフを用いる (図 2)．ベクトル $\boldsymbol{x}$ が次の場合のシンドローム $\boldsymbol{s}^T = \mathbf{H}'\boldsymbol{x}^T$ の計算を考える．

$$\boldsymbol{x} = (\ 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 1\quad 0\quad 0\ )$$

$\boldsymbol{x}$ を変数ノードに対応させ，変数ノード v から v に接続する全ての検査ノードに対して，v に対応する受信語の値を送信する．例えば，p_1 は $v_3, v_4, v_5, v_6, v_7, v_{10}$ と，p_2 は $v_1, v_4, v_7, v_8, v_9, v_{10}$, と，$p_3$ は $v_2, v_3, v_4, v_5, v_7, v_9$ と接続しているため，

$$\begin{aligned} p_1 &= v_3 + v_4 + v_5 + v_6 + v_7 + v_{10} = 0 \\ p_2 &= v_1 + v_4 + v_7 + v_8 + v_9 + v_{10} = 1 \\ p_3 &= v_2 + v_3 + v_4 + v_5 + v_7 + v_9 = 0 \end{aligned}$$

となる．このようにして，$p_1, p_2, ..., p_{n-k}$ の値をそれぞれ計算する．これらの値から $\boldsymbol{s} = (p_1\ p_2\ p_3\ p_4\ p_5)$ として次のシンドロームが求まる．

$$\boldsymbol{s} = (\ 0\quad 1\quad 0\quad 1\quad 0\ )$$

一般的にシンドロームの計算では，$n-k$ 行 n 列の行列と n 次元ベクトルの積を求めるために，$n(n-k)$ 回の乗算と $(n-1)(n-k)$ 回の加算を行うため，その計算量は $(2n-1)(n-k)$ になる．一方，タナーグラフを用いたシンドローム計算では，パリティ検査行列の非零要素の位置 (タナーグラフにおいてエッジで接続するノード) のみを演算するため行重み d_r のパリティ検査行列の場合，$(d_r-1)(n-k)$ 回の加算を行うだけで良くなり，計算量は $(d_r-1)(n-k)$ になる．

4. 提案方式の反復復号法による復号不可能性

行列 $\mathbf{S}$ は行重み 2，列重み 2 の場合，行列 $\mathbf{S}$ は正則（フルランク）にならないため，いずれかの行の重みを 1 増やした行列を $\mathbf{S}$ として使うが，本章では，全ての行重み 2，列重み 2 であると想定して証明する．いずれかの行の重みを 1 増やした行列についても同様に証明できるが，議論が細かくなるため，その証明は省く．

提案方式において，LDPC 符号の疎なパリティ検査行列 $\mathbf{H}_l$ に行重み u，列重み u の正則行列 $\mathbf{S}$ を掛けることにより，長さ 4 のサイクルを十分な数作る．但し，$\mathbf{H}_l$ を，

(d_c, d_r) 正則 LDPC 符号のパリティ検査行列と仮定する．以下の場合において，$u = 2$ のとき，つまり行重み 2，列重み 2 の正則行列 $\mathbf{S}$ を掛けることにより，十分な数の長さ 4 のサイクルができることを示す．

定理 1　$\mathbf{H}_l$ を長さ 4 のサイクルがない行重み d_r，列重み d_c の行列とする．$\mathbf{S}$ が行重み 2, 列重み 2 の場合, $\mathbf{H}' = \mathbf{SH_l}$ は各列に長さ 4 のサイクルができる．

(証明) $\mathbf{H}_l$ に行重み 2 の行列 $\mathbf{S}$ を掛ける場合，$\mathbf{H}'$ のある行は，$\mathbf{H}_l$ のある 2 行を XOR したものになる．$\mathbf{H}_l$ の i 行 $\boldsymbol{h}_i$ と j 行 $\boldsymbol{h}_j$ が XOR されて，$\mathbf{H}'$ の k 行 $\boldsymbol{h}'_k$ になるとする．$\mathbf{H}_l$ に長さ 4 のサイクルがないことから，$\boldsymbol{h}_i$ と $\boldsymbol{h}_j$ を XOR したとき，$\boldsymbol{h}_i$ の '1' が 2 個以上 $\boldsymbol{h}_j$ の '1' によって打ち消し合って 0 になることはない．よって，$\boldsymbol{h}'_k$ には，$\boldsymbol{h}_i$ の '1' を $d_r - 1$ 個以上含む．また，$\mathbf{H}_l$ に列重み 2 の行列 $\mathbf{S}$ を掛けることから，$\boldsymbol{h}_i$ は $\mathbf{H}'$ のもう一つの行にも XOR される．この $\mathbf{H}'$ の行を $\boldsymbol{h}'_l$ とする．$\boldsymbol{h}'_l$ にも同様に，$\boldsymbol{h}_i$ の '1' を $d_r - 1$ 個の '1' が同じ列にあり，これが長さ 4 のサイクルになる．

次に，上記の長さ 4 のサイクルが $\mathbf{H}'$ の全ての列にできることを示す．そのためには，$\mathbf{H}'$ の各列に '1' が 2 個以上あることを示せばよい．$\mathbf{H}_l$ に行重み 2 の行列 $\mathbf{S}$ を掛けることから，$\mathbf{H}'$ のある列は $\mathbf{H}_l$ のある 2 行を XOR したものになる．よって，$\mathbf{H}_l$ のある行とある行を XOR したとき，打ち消し合う '1' の数を a とすると，$\mathbf{H}'$ の列に含まれる '1' の数は，$2d_r - 2a$ になる．そのため，$\mathbf{H}'$ の列重みは偶数であり，1 になることはない．また，$\mathbf{H}'$ の列重みが 0 になるためには，$\mathbf{S}$ が同じ行ベクトルを 2 行持たなければならないが，そのような行列は正則ではない．したがって，$\mathbf{H}'$ の各列に '1' が 2 個以上ある．ゆえに，$\mathbf{H}'$ の全ての列に長さ 4 のサイクルができる．　□

定理 2　$\mathbf{H_l}$ を行重み d_r，列重み d_c の行列とする．$\mathbf{S}$ が行重み 2，列重み 2 のとき，$\mathbf{H}' = \mathbf{SH}_l$ は各列に長さ 4 または 6 のサイクルができる．

(証明) 定理 1 の証明と同様に，$\mathbf{H}_l$ に行重み 2 の行列を掛けたとき，$\mathbf{H}_l$ の i 行 $\boldsymbol{h}_i$ と j 行 $\boldsymbol{h}_j$ が XOR されて $\mathbf{H}'$ の k 行 $\boldsymbol{h}'_k$ になる場合を考える．定理 1 において $\mathbf{H}_l$ に長さ 4 のサイクルがない場合，長さ 4 のサイクルができることを示したため，$\mathbf{H}_l$ に長さ 4 のサイクルがある場合について考える．ここで，$\boldsymbol{h}_i$ と $\boldsymbol{h}_j$ を XOR するとき，$\boldsymbol{h}_i$ の $d_r - 1$ 個の '1' が $\boldsymbol{h}_j$ の '1' と打ち消し合って 0 になる場合と，$\boldsymbol{h}_i$ と $\boldsymbol{h}_j$ の '1' の打ち消し合いが $d_r - 2$ 個以下である場合に分けて考える．

(i)　$\boldsymbol{h}_i$ と $\boldsymbol{h}_j$ の '1' の打ち消し合いが $d_r - 2$ 個以下である場合

$\boldsymbol{h}'_k$ は $\boldsymbol{h}_i$ の '1' を 2 個以上含み，また，$\boldsymbol{h}_j$ の '1' を 2 個以上含む．このとき，定理 1 の証明と同様にして，$\mathbf{H}'$ は各列に長さ 4 のサイクルが必ずできることが示される．

(ii)　$\boldsymbol{h}_i$ の $d_r - 1$ 個の '1' が $\boldsymbol{h}_j$ の '1' と打ち消し合う場合

$\mathbf{H}'$ の k 行 j 列に 1 があれば，長さ 4 のサイクルができる．$\mathbf{H}_l$ の i 列の x 行に 1 がある場合，$\mathbf{S}$ の k 行 x 列に 1 があれば，$\mathbf{H}'$ の k 行 i 列に 1 が立つ．但し，$\mathbf{H}_l$ の x' 行 i 列に 1 があるとき，$\mathbf{S}$ の k 行 x' 列に 1 は立たない．同様に，$\mathbf{H}_l$ の y 行 j 列に 1 がある場合，$\mathbf{S}$ の k 行 y 列に 1 があれば，$\mathbf{H}'$ の k 行 j 列に 1 が立つ．但し，$\mathbf{H}_l$ の y' 行 j 列に 1 があるときには，$\mathbf{S}$ の k 行 y' 列に 1 は立たない．また，このような $\mathbf{S}$ が作れない場合でも，$\mathbf{H}'$ の i 列と j 列には必ず長さ 6 のサイクルが含まれる．　□

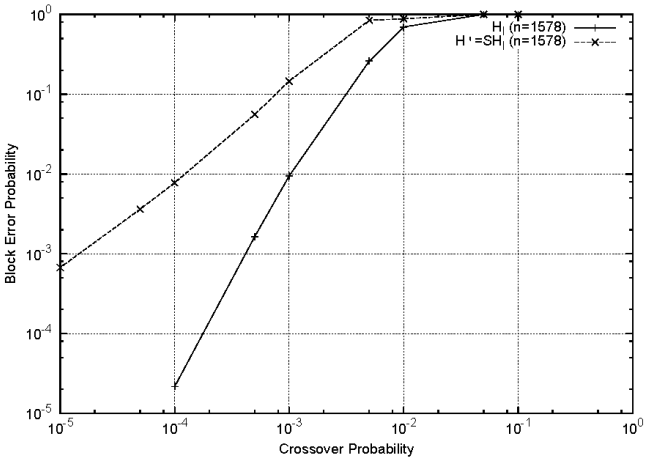

図 3　反復復号法による復号シミュレーションの結果

図 3 に Gallager の構成法で構成した符号長 1578 の (3,6) 正則 LDPC 符号のパリティ検査行列 $\mathbf{H}_l$ と，その $\mathbf{H}_l$ に行重み 2, 列重み 2 の正則行列 $\mathbf{S}$ を掛けた行列 $\mathbf{H}'$ による復号シミュレーションの結果を示す．この復号シミュレーションでは，2 元対称通信路における反復復号法（最大反復回数 100 回）を用いた．図 3 から，$\mathbf{H}'$ に長さ 4 のサイクルがあり，$\mathbf{H}_l$ より復号能力が劣化していることがわかる．

5. 認証方式のセキュリティレベル

2 元シンドローム復号問題に基づく認証方式のセキュリティレベルは Information Set Decoding(ISD) 攻撃によって評価できる [11]．2 元シンドローム復号問題は NP 困難な問題であるが，十分なセキュリティレベルを満たすためには，符号長 n，情報点数 k，誤り訂正能力 t を適切に設定する必要がある．ISD 攻撃は線形符号の最小重みの符号語を発見する確率的アルゴリズムであり，文献 [3][12][13][14] で提案されている．本稿では，ISD 攻撃の中でも最も効率の良い Ball Collision Decoding[12] を採用し，セキュリティ評価を行う．

Ball Collision Decoding における 1 回の繰り返し処理で重み t の誤りベクトルが得られる確率は次式で与えられる．

表 1　認証方式のセキュリティレベル別パラメータ

	検査行列の構成法	セキュリティレベル	(n,k,t)	(d_c,d_r)	u
Stern の認証方式	ゴッパ符号	50bit	(1024,524,50)	- -	-
		80bit	(2048,1751,27)	- -	-
提案方式	Gallager の構成法による LDPC 符号	50bit	(1578,789,36)	(3,6)	2
		80bit	(2982,1491,68)	(3,6)	2

表 2　認証方式の計算量

		Stern の認証方式		提案方式	
		計算式	計算量	計算式	計算量
公開鍵の生成				$\mathbf{H}'(=\mathbf{S}\mathbf{H}_l\mathbf{P})$	$ud_r(n-k)$
		$\boldsymbol{s}(=\boldsymbol{x}\mathbf{H}^T)$	$(2n-1)(n-k)$	$\boldsymbol{s}(=\boldsymbol{x}\mathbf{H}'^T)$	$(ud_r-1)(n-k)$
コミットメント	c_1	$\mathbf{H}\boldsymbol{y}^T$	$(2n-1)(n-k)$	$\mathbf{H}'\boldsymbol{y}^T$	$(ud_r-1)(n-k)$
	c_3	$\sigma(\boldsymbol{y}+\boldsymbol{x})$	n	$\sigma(\boldsymbol{y}+\boldsymbol{x})$	n
検証	$b=0$	$\mathbf{H}\boldsymbol{y}^T$	$(2n-1)(n-k)$	$\mathbf{H}'\boldsymbol{y}^T$	$(ud_r-1)(n-k)$
	$b=1$	$\mathbf{H}(\boldsymbol{y}+\boldsymbol{x})^T$	$(2n-1)(n-k)$	$\mathbf{H}'(\boldsymbol{y}+\boldsymbol{x})^T$	$(ud_r-1)(n-k)$
	$b=2$	$\sigma(\boldsymbol{y})+\sigma(\boldsymbol{x})$	n	$\sigma(\boldsymbol{y})+\sigma(\boldsymbol{x})$	n
		$W_H(\sigma(\boldsymbol{x}))=w$	n	$W_H(\sigma(\boldsymbol{x}))=w$	n

$$P_t=\frac{\binom{n-k-l_1-l_2}{t-p_1-p_2-q_1-q_2}\binom{k_1}{p_1}\binom{k_2}{p_2}\binom{l_1}{q_1}\binom{l_2}{q_2}}{\binom{n}{t}}$$

また，Ball Collision Decoding における 1 回の繰り返し処理の計算量は次式となる．

$$\begin{aligned}N=&\frac{1}{2}(n-k)^2(n+k)\\&+(l_1+l_2)\left\{\sum_{i=1}^{p_1}\binom{k_1}{i}+\sum_{i=1}^{p_2}\binom{k_2}{i}-k_1\right\}\\&+\min\{1,q_1\}\binom{k_1}{p_1}\sum_{i=1}^{q_1}\binom{l_1}{i}\\&+\min\{1,q_2\}\binom{k_2}{p_2}\sum_{i=1}^{q_2}\binom{l_2}{i}\\&+2(t-p_1-p_2-q_1-q_2)(p_1+p_2)\binom{k_1}{p_1}\binom{k_2}{p_2}\binom{l_1}{q_1}\binom{l_2}{q_2}\Big/2^{l_1+l_2}\end{aligned}$$

ただし，p_1，p_2，q_1，q_2，l_1，l_2 は Ball Collision Decoding において使用されるパラメータであり，$k=k_1+k_2$ である．このとき，work factor は，

$$WF=\frac{N}{P_t} \tag{1}$$

となる．式 (1) を用い Stern の認証方式を応用した提案方式の特定のセキュリティレベルにおけるパラメータを調査する．

提案方式の定めるべきパラメータはパリティ検査行列 $\mathbf{H}_l$ の符号長 n，情報点数 k，誤り訂正能力 t である．提案方式は，疎なパリティ検査行列であれば，正則，非正則に限らず実現できるが，2 元シンドローム復号問題を解くことが困難にするために，$\mathbf{H}'$ に小さなサイクルが含まれる必要がある．これは $\mathbf{H}'$ に含まれる非零要素の数に依存するため，本稿では，$\mathbf{H}_l$ を (d_c,d_r) 正則 LDPC 符号のパリティ検査行列とし，$\mathbf{S}$ を行重み u，列重み u の正則行列としてパラメータを定める．4 章において示した通り，$u=2$ において $\mathbf{H}'$ に十分多くの長さ 4 または 6 のサイクルを作ることができる．また，式 (1) の work factor はパリティ検査行列の誤り訂正能力，すなわち，符号の最小距離に依存する．本稿では，LDPC 符号のパリティ検査行列の構成法として代表的な Gallger の構成法 [15] で作られる (3,6) 正則 LDPC 符号で考え，最小距離は典型的最小距離である $d=0.02274n$ で評価した．

表 1 に Stern の認証方式と提案方式のセキュリティレベル別パラメータを示す．50bit，80bit のセキュリティレベルを保てるパラメータを示している．Stern の認証方式の 50bit のパラメータは [3]，80bit のパラメータは [14] のパラメータを使用しいる．

提案方式のパリティ検査行列は代数的な構造を持たず，また行列が疎であるという特徴を使う反復復号法も短いサイクルによって機能しないため，パリティ検査行列の構造を利用して提案方式を攻撃することができない．

6. 認証方式の計算量評価

Stern の認証方式と提案方式の計算量を比較する．認証方式において計算処理が発生する手続きは，公開鍵の生成，コミットメントにおける c_1,c_3 の生成，$b=0,1,2$ の場合における検証である．但し，ハッシュ関数 $h()$，$\mathbf{P}$ や $\sigma()$ の置換について，入力データのサイズが大きく異なることはない．

$\mathbf{H}_l$ の行重みが d_r，行列 $\mathbf{S}$ の行重み u であるため，$\mathbf{H}'$ の各行は重み d_r の行を u 個 XOR したものになる．そのため，公開鍵 $\mathbf{H}'=\mathbf{S}\mathbf{H}_l\mathbf{P}$ を生成するための計算量は次式となる．

$$ud_r(n-k)$$

表 3　認証方式のシンドローム計算の計算量

	検査行列の構成法	セキュリティレベル	計算量		
			$r=1$	$r=28$	$r=56$
Stern の認証方式	ゴッパ符号	50bit	2,730,357	48,815,505	96,607,511
		80bit	3,245,288	58,030,259	114,844,303
提案方式	Gallager の構成法による LDPC 符号	50bit	34,190	467,351	916,555
		80bit	64,610	883,169	1,732,045

3.3 節で示した通り，一般的にシンドロームの計算の計算量は次式となる．

$$(2n-1)(n-k)$$

また，提案方式においてシンドローム計算に用いる $\mathbf{H}'$ の行重みは $\mathbf{S}$ の行重み u と，$\mathbf{H}_l$ の行重み d_r を掛け合わせた ud_r となる．そのため，提案方式のシンドローム計算の計算量は次式となる．

$$(ud_r-1)(n-k)$$

このシンドローム計算の計算量に基づき作成した表 2 に，各手続きの計算式とその計算量の対応を示す．

検証はそれぞれ 1 ラウンドで確率 $\frac{1}{3}$ で計算される．そのため，r 回繰り返す Stern の認証方式の計算量は次式となる．

$$(2n-1)(n-k)+r\left\{\frac{5}{3}(2n-1)(n-k)+n\right\} \qquad (2)$$

また，r 回繰り返す提案方式の計算量は次式となる．

$$ud_r(n-k)\ +\ (ud_r-1)(n-k) \\ +\ r\left\{\frac{5}{3}(ud_r-1)(n-k)+n\right\} \qquad (3)$$

表 1 のパラメータを式 (2),(3) に適用し計算量評価をした．Stern の認証方式において，認証失敗確率を $2^{-16}, 2^{-32}$ にするためには，28 回，56 回繰り返す必要があるため，$r=1$，$r=28$，$r=56$ の場合の計算量を評価する．Stern の認証方式と提案方式のシンドローム計算の計算量を表 3 に示す．

7. まとめ

本稿では，著者らが [9] において提案した，LDPC 符号を用いたゼロ知識証明型認証方式のセキュリティレベル，計算量，安全性について詳細に考察した．提案方式は LDPC 符号の疎なパリティ検査行列の特徴を利用することで，認証方式として計算量が低く，耐量子性である 2 元シンドローム復号問題に基づく認証方式よりもさらに計算量を削減している．また，LDPC 符号を利用する際に反復復号法によって公開鍵から秘密鍵を求められる問題を疎なパリティ検査行列に短いサイクルを含ませることで解決している．そして，反復復号法はパリティ検査行列に短いサイクルが含まれている場合，復号能力が低下し正しい誤りを求められなくなることを説明した．また，タナーグラフを用いてシンドローム計算を行うことで，通常のシンドローム計算と比較して計算量を削減した．さらに，セキュリティレベルに対応したパラメータ n，k，t，d_c，d_r，u の値を定め，詳細な計算量を評価し，Stern の方式より提案方式の方が計算量が小さくなることを示した．

参考文献

[1] M. Baldi and F. Chiaraluce, “LDPC Codes in the McEliece Cryp-tosystem,” https://arxiv.org/pdf/0710.0142v1.pdf, Sep. 2007.

[2] T. R. Halford, “How to Prove Yourself to Multiple Parties:Energy-Efficient Multi-group Authentication,” Proc. IEEE MILCOM 2013, pp. 237–242, Nov. 2013.

[3] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” DSN Progress Report 42, pp.114–116, 1978.

[4] H. Niederreiter, “Knapsack-type cryptosystem based on algebraic coding theory,” Problems of Control and Information Theory, vol.15, no.2, pp.157–166, 1986.

[5] C. Monico, J. Rosenthal, and A. Shokrollahi, “Using low density parity check codes in the McEliece cryptosystem,” Proc 2000 IEEE Int. Symp. Inf. Theory, Sorrento, Italy, p.215, 2000.

[6] M. Baldi, M. Bodrato, and F. Chiaraluce, “A new analysis of the McEliece cryptosystem based on QC-LDPC codes,” in Security and Cryptography for Networks (SCN 2008), R. Ostrovsky, R. D. Prisco, and I. Visconti Eds., Lecture Notes in Computer Science, vol.5229. pp.246–262, Springer, Berlin, Heidelberg, 2008.

[7] R. Misoczki, J. P. Tillich, N. Sendrier, ENDRIER, and P. S. L. M. Barreto, “MDPC-McEliece: New McEliece variants from moderate density parity-check codes,” Proc. 2013 IEEE Int. Symp. Inf. Theory (ISIT 2013), Istanbul, Turkey, pp.2069–2073, 2013.

[8] M. Repka and P. Zajac, “Overview of the Mceliece cryptosystem and its security,” Journal of Slovak Academy of Sciences, vol.60, no.1, pp.57–83, Sep. 2014.

[9] 伊東春香，廣友雅徳，福田洋治，毛利公美，白石善明，“LDPC 符号を用いたゼロ知識証明型認証方式について，”信学技報，ICSS2017-7，pp.37–42，June 2017.

[10] E. R. Berlekamp, R. J. McEliece, and H. C. A. VAN Tilborg, “On the inherent intractability of certain coding problems,” IEEE Trans. Inf. Theory, vol.24, no 3, pp. 384–386, May. 1978.

[11] J. Stern, “A new paradigm for public key identification,” IEEE Trans. Inf. Theory, vol.42, no.6, pp.1757–1768, Nov. 1996.

[12] D. J. Bernstein, T. Lange, and C. Peters, “Smaller decoding exponents: Ball-collision decoding,” in Advances in Cryptology (CRYPTO 2011), P. Rogaway Ed., Lecture Notes in Computer Science, vol.6841. Springer,

Berlin, Heidelberg, 2011.
[13] J. Stern, "A method for finding codewords of small weight,"in Coding Theory and Applicatins 1988, G. Cohen and J. Wolfmann, Eds. Lecture Notes in Computer Science, vol.388, pp.106–113, New York: Springer-Verlag, 1989.
[14] D. J. Bernstein, T. Lange, and C. Peters "Attacking and defending the McEliece cryptosystem," in Post-Quantum Cryptography (PQCrypto 2008), J. Buchmann and J. Ding Eds., Lecture Notes in Computer Science, vol.5299, pp.31-46, Springer, Berlin, Heidelberg, 2008.
[15] R. G. Gallager, Low Density Parity Check Codes, Cambridge, MA: MIT Press, 1963.