# 情報理論から広がるサイバー社会を支える各種応用技術

## ―情報理論とその応用シンポジウム２０２１―

森井　昌克
神戸大学大学院工学研究科　電気電子工学専攻

## アジェンダ

神戸大学

~~最初の信学会研究会での発表タイ~~ ~~符号の定義とその性質」（1982年）であり、SIT~~ ~~、1984年鬼怒川でのシンポジウム、内容は有限~~ ~~ろうか。その~~ ~~処理と符号理論の~~ ~~号理論およ~~ ~~の周辺を眺めながら、学位取得後、~~ ~~IoT機器、ア~~ ~~やマルウェア解析を中心としたサイバーセキュリティの~~ ~~をおこなっている。素数探索を目的とした計算機構成と寄り道も行いながらも、~~意識として、研究の 中心は符号理論であり、1990年初頭から最良符号構成に取り組み、 最近もMarkus Grassl(Univ. of Gdansk, Poland)が管理している 最良符号表(Code Tables: Bounds on the parameters of various types of codes)での2元誤り訂正符号のパラメータを多数更新 している。このような古典的な符号理論の知識がサイバー社会 での基盤技術に貢献している事例を中心に解説する。

**でも少しだけ話させて下さい**

**昨夜、いろいろと昔を思い出しましたので。**

**昔話はさっくりと除いて**

## アジェンダ

神戸大学

- 研究事始め
  - 最初の研究会発表は… 情報理論研究会がなぜか存在せず？
    - ハフマン符号化関係(学部)
    - 有限体理論(大学院修士)
      - 何故か修論は符号理論(Goppa符号関係)
  - 最初の学術論文は
    - 自己双対基底の存在定理(電子通信学会論文誌,1984)
  - 博士課程では
    - 符号理論
      - 代数的復号法、その応用を中心に
    - 暗号理論
      - 公開鍵暗号



## アジェンダ（２）

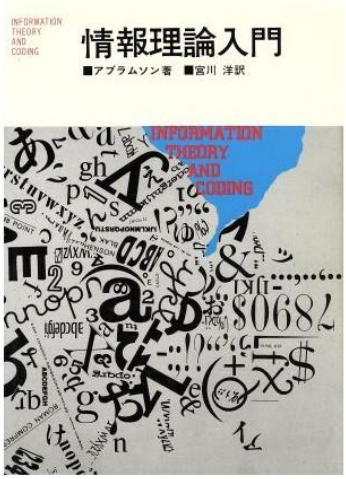
神戸大学

- その後の主な成果
  - 暗号とサイバーセキュリティを中心として
- しかし…
  - 自身では「(古典的？)符号理論とその応用」がメイン(と思っている)、たとえば…
    - 最良線形符号構成問題
    - QRコード

# アジェンダ

神戸大学

- 研究事始め
  - 最初の研究会発表は…
    - ハフマン符号関係(学部)
    - 有限体理論(大学院修士)
      - 何故か修論は符号理論(Goppa符
  - 最初の学術論文は
    - 自己双対基底の存在定理(電子通信
  - 博士課程では
    - 符号理論
      - 代数的復号法、その応用を中心に
    - 暗号理論
      - 公開鍵暗号






# 同時に構成可能な二元ハフマン符号の数(1982)

神戸大学

AL82-53

同時に構成可能な2元ハフマン符号の数

On the Number of Possible Binary Huffman Codes of Different Code Lengths that can be Constructed Simultaneously

今村 恭己, 森井 昌克 (佐賀大学電子工学科)

Kyoki IMAMURA and Masakatu MORII

Department of Electronics, Saga University

ABSTRACT: Let S be a discrete memoryless source which produces n letters with a fixed set of probabilities, $P_1, P_2, \cdots, P_n$. This paper shows that there exists such a set of probabilities that $M_n$ binary Huffman codes of different code lengths can be constructed simultaneously, where $M_n=\{\alpha^{n-1}-\beta^{n-1}\}/\sqrt{5}$ with $\alpha=(1+\sqrt{5})/2$ and $\beta=(1-\sqrt{5})/2$. A formula for determing the set of probabilities is given. It is also shown that for $n\geq 7$ there dose not exist such a set of probabilities that all the possible binary Huffman codes of different code lengths can be constructed simultaneously.

1. まえがき

本稿では，n個の記号をそれぞれ確率 $P_1, P_2, \cdots, P_n$ で独立に発生する情報源に対する2元ハフマン符号[1]をサイズnの2元ハフマン符号と呼び，同時に構成可能なサイズnの2元ハフマン符号の数とそのときの確率分布について調べる。議論を明確にするために，一般性を失うことなく

$$0<P_n\leq P_{n-1}\leq \cdots \leq P_2\leq P_1<1 \quad (1)$$

$$1\leq l_1\leq l_2\leq \cdots \leq l_{n-1}\leq l_n \quad (2)$$

を仮定する。

本稿では2元ハフマン符号のみを取り扱うので，以下では簡単にハフマン符号と書くことにする。本稿では相異なる符号長の組をもつ

$$M_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right] \quad (3)$$

通りのサイズnのハフマン符号が同時に構成可能であるような確率分布 $P_1, P_2, \cdots, P_n$ が存在することを示す。

同時に構成可能なハフマン符号の数とそのための確率分布に関しては，Golombの結果が文献(3)に引用されているが，n=4の場合の記述があるのみで，その詳細は不明である。

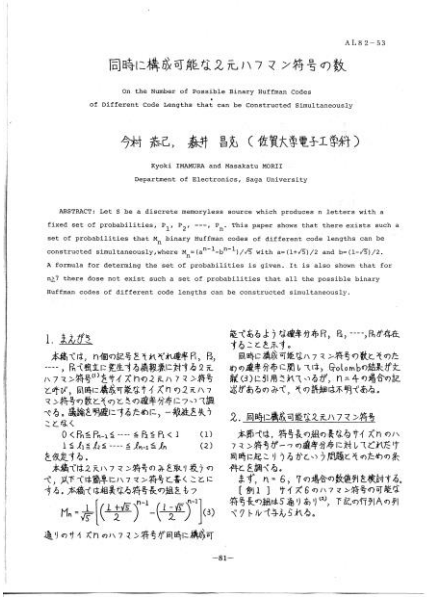
2. 同時に構成可能な2元ハフマン符号

本節では，符号長の組の異なるサイズnのハフマン符号が一つの確率分布に対してどれだけ同時に起こりうるかという問題とそのための条件とを調べる。

まず，n=6，7の場合の数値列を検討する。

[例1] サイズ6のハフマン符号の可能な符号長の組は5通りあり[2]，下記の行列Aの列ベクトルで与えられる。

## 同時に構成可能な二元ハフマン符号の数（１９８２）



AL82-53

同時に構成可能な2元ハフマン符号の数

On the Number of Possible Binary Huffman Codes of Different Code Lengths that can be Constructed Simultaneously

今村 恭己，森井 昌克（佐賀大学電子工学科）

Kyoki IMAMURA and Masakatu MORII
Department of Electronics, Saga University

ABSTRACT: Let S be a discrete memoryless source which produces n letters with a fixed set of probabilities, $P_1, P_2, \cdots, P_n$. This paper shows that there exists such a set of probabilities that $M_n$ binary Huffman codes of different code lengths can be constructed simultaneously, where $M_n=(a^{n-1}-b^{n-1})/\sqrt{5}$ with $a=(1+\sqrt{5})/2$ and $b=(1-\sqrt{5})/2$. A formula for determining the set of probabilities is given. It is also shown that for $n\geq 7$ there dose not exist such a set of probabilities that all the possible binary Huffman codes of different code lengths can be constructed simultaneously.

1. まえがき

本稿では，n個の記号とそれぞれ確率 $P_1, P_2, \cdots, P_n$ で相互に発生する情報源に対する2元ハフマン符号[1]をサイズnの2元ハフマン符号とが，同時に構成可能なサイズnの2元ハフマン符号の数とそのときの確率分布について調べる。議論を明確にするために，一般性を失うことなく

$0<P_n\leq P_{n-1}\leq \cdots \leq P_3\leq P_2<1$ (1)

$1\leq L_1\leq L_2\leq \cdots \leq L_{n-1}\leq L_n$ (2)

を仮定する。

本稿では2元ハフマン符号のみを取り扱うので，以下では簡単にハフマン符号と書くことにする。本稿では相異なる符号長の組をもつ

$$M_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right] \quad (3)$$

通りのサイズnのハフマン符号が同時に構成可能であるような確率分布 $P_1, P_2, \cdots, P_n$ が存在することを示す。

同時に構成可能なハフマン符号の数とそのための確率分布に関しては，Golombの結果が文献(3)に引用されているが，$n\leq 6$ の場合の記述があるのみで，その詳細は不明である。

2. 同時に構成可能な2元ハフマン符号

本節では，符号長の組の異なるサイズnのハフマン符号が一つの確率分布に対して2通り以上同時に起こりうるかという問題とそのための条件とを調べる。

まず，$n=6$，7の場合の数値例を検討する。

［例1］ サイズ6のハフマン符号の可能な符号長の組は5通りあり[2]，下記の行列Aの列ベクトルで与えられる。



### 3. むすび

異なる符号長の組をもつサイズnのハフマン符号で同時に構成可能なものの数 $M_n$ として，$M_n$ がフィボナッチ数列になるような場合が存在することを示し，そのときの確率分布の一般式を求めた。本稿の定理2で求めた $M_n$ は，例1，例2の数値例からもわかるように，同時に構成可能なハフマン符号の数の最大値であると予想される。



## 平面ハフマン符号の定理とその性質（１９８２）

AL82-54

平面ハフマン符号の定義とその性質

Definition of a Planar Huffman Code and its Property

森井 昌克，今村 恭己（佐賀大学電子工学科）

Masakatu MORII and Kyoki IMAMURA
Department of Electronics, Saga University

ABSTRACT: Let S be a discrete memoryless source which produces n letters, $a_1, a_2, \cdots, a_n$, with a fixed set of probabilities, $P_1, P_2, \cdots, P_n$. Let us assume that $P_1\geq P_2\geq \cdots \geq P_n>0$. Let us draw a code tree of any code for S so that the n terminal nodes of the code tree correspond from the one end to the another end to the n letters, $a_1, a_2, \cdots, a_n$ in that order. In this paper a uniquely decodable binary code of smallest average code-length is called a planar Huffman code if no two branches of its code tree cross. It is shown that for any binary Huffman code, C, for S, there exists one planar Huffman code which has the same code lengths as C.

1. まえがき

ハフマン符号[1][2][3]は，相互に離散的情報源の各記号を一意復号可能な符号に符号化する符号のうちで平均符号長が，最小になるという意味で最適な符号である。

ハフマン符号の構成法は，要するに，ハフマン符号化法によって，bottom-up式に符号木を作る作業である。しかし構成された符号木は，図1に示すように1つの符号長の組（2, 2, 3, 3, 4, 4, ……, $L_n$）に対して見かけ上1つとはかぎらない。





（図1） 符号長の組が（2, 2, 3, 3, 4, 4）であるような3通りの符号木。



### 4. むすび

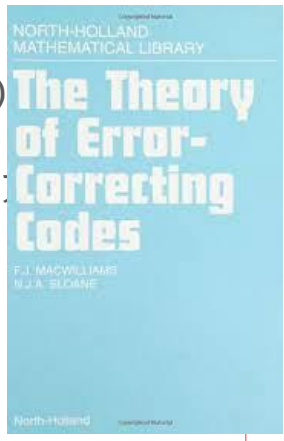
本稿によって，2元ハフマン符号の性質がその部分クラスである平面ハフマン符号の性質を調べることによって代替できる可能性を示した。また平面ハフマン符号自体，その符号木の単純なこと，あるいは系統的なことから，効率のよい符号化，あるいは復号化が期待できる。

サイズnのハフマン符号の可能な符号長の組がすべて同時に構成可能となるような確率分布 $P_1, P_2, \cdots, P_n$ は $n\geq 7$ の場合には存在しない。この問題に関しては別稿で報告したい。

# アジェンダ

神戸大学

- 研究事始め
  - 最初の研究会発表は…
    - ハフマン符号化関係(学部)
    - 有限体理論(大学院修士)
      - 何故か修論は符号理論(Goppa符号関係)
  - 最初の学術論文は
    - 自己双対基底の存在定理(電子通信学会論
  - 博士課程では
    - 符号理論
      - 代数的復号法、その応用を中心に
    - 暗号理論
      - 公開鍵暗号








神戸大学

## Prof. Masakatu Morii: for internet technology

- One of Heavy User for Internet
  - Stand at the dawn of the Internet
    - from 1980s
- Information and Communicatuion Researcher
  - Information Theory
  - *Satelite and Mobile Communications*
- Security and Cryptography
  - *First Paper*
    - A Theorem that GF ($2^{4m}$) has no Self-Complementary Normal Bases over GF (2) for Odd *m*, *IEICE Trans. 1984*
  - *Doctoral Thesis*
    - Efficient Algorithm Over Finite Fields And Their Applications To Coding Theory And Cryptography (1989)

神戸大学

## Normal Bases Theory (related)

- A Theorem that GF ($2^{4m}$) has no Self-Complementary Normal Bases over GF (2) for Odd *m*, *IEICE Trans. 1984*
- *Two classes of finite fields which have no self-complementary normal bases*, ISIT1985

Generalized, not me

***On the number of self-dual bases of*** $\mathrm{GF}(q^m)$ ***over*** $\mathrm{GF}(q)$

**Authors:** Dieter Jungnickel, Alfred J. Menezes and Scott A. Vanstone
**Journal:** Proc. Amer. Math. Soc. **109** (1990), 23-29

Perfecty Solved

神戸大学

## A Theorem that GF ($2^{4m}$) has no Self-Complementary Normal Bases over GF (2) for Odd *m*

Masakatu MORII, *Associate Member and*
Kyoki IMAMURA, *Member*

UDC 512.624 : 512.642

**SUMMARY** A self-complementary basis of a finite field corresponds to the orthonormal basis of a vector metric space. This paper presents a theorem that GF ($2^{4m}$) has no self-complementary normal bases over GF (2) if $m$ is odd, which was recently conjectured by one of the present authors.

神戸大学

The self-complementary normal basis is defined as follows.

[Definition 1] A normal basis, $\{\beta, \beta^q, \cdots, \beta^{q^{n-1}}\}$, of GF($q^n$) over GF($q$) is a self-complementary normal basis if

$$\mathrm{tr}(\beta^{2q^i}) = 1$$
$$\mathrm{tr}(\beta^{q^i}\ \beta^{q^j}) = 0 \quad (i \neq j) \tag{1}$$

for $i, j = 1, \cdots, n$, where tr( ) is the trace of GF($q^n$) over GF($q$) and defined for every element $\beta$ of GF($q^n$) by

$$\mathrm{tr}(\beta) = \beta + \beta^q + \cdots + \beta^{q^{n-1}}. \tag{2}$$



神戸大学

[Theorem 1] (MacWilliams and Sloane) If $n$ is odd, then GF($2^n$) has a self-complementary normal basis over GF(2).

[Theorem 2] If $m$ is odd, then a self-complementary normal basis of GF($2^{4m}$) over GF(2) does not exist.

PROCEEDINGS OF THE AMERICAN MATHEMATICAL SOCIETY

- Journals Home
- Search
- Author Info
- Subscribe
- Tech Support
- My Subscriptions
- Help

ISSN 1088-6826(e) ISSN 0002-9939(p)

Previous issue | This issue | Most recent issue | All issues (1950–Present) | Next issue
Previous article | Articles in press | Recently posted articles | Next article

***On the number of self-dual bases of*** $\mathrm{GF}(q^m)$ ***over*** $\mathrm{GF}(q)$

**Authors:** Dieter Jungnickel, Alfred J. Menezes and Scott A. Vanstone
**Journal:** Proc. Amer. Math. Soc. **109** (1990), 23-29

電子情報通信学会論文誌、1988年



## Goppa 符号の復号法に関する一考察

正　員　森井　昌克†　　正　員　笠原　正雄††

## A note on Decoding Method for Goppa Codes

Masakatu MORII† *and* Masao KASAHARA††, *Members*

†大阪大学工学部通信工学科，吹田市
Faculty of Engineering, Osaka University, Suita-shi, 565 Japan

**あらまし**　本稿では，誤り位置として0を有する一般的なGoppa符号の復号問題と，与えられた系列を生成する最小段数の線形帰還シフトレジスタ合成問題との間に存在する関係について考察する．

# アジェンダ

神戸大学

- 研究事始め
  - 最初の研究会発表は…
    - ハフマン符号化関係(学部)
    - 有限体理論(大学院修士)
      - 何故か修論は符号理論(Goppa符号関係)
  - 最初の学術論文は
    - 自己双対基底の存在定理(電子通信学会論文誌,1984)
  - **博士課程では**
    - **符号理論**
      - **代数的復号法、その応用を中心に**
    - **暗号理論**
      - **公開鍵暗号**



# 博士課程での代表的研究

神戸大学

Efficient Bit-Serial Multiplication and the Discrete-Time Wiener-Hopf Equation Over Finite Fields

MASAKATU MORII, MEMBER, IEEE, MASAO KASAHARA, SENIOR MEMBER, IEEE, AND DOUGLAS L. WHITING

PAPER

Efficient Construction of Gate Circuit for Computing Multiplicative Inverses over $GF(2^m)$

Masakatu MORII† *and* Masao KASAHARA††, *Members*

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 38, NO. 6, NOVEMBER 1992

**Generalized Key-Equation of Remainder Decoding Algorithm for Reed–Solomon Codes**

Masakatu Morii, *Member, IEEE,* and Masao Kasahara, *Senior Member, IEEE*

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 35, NO. 6, NOVEMBER 1989



神戸大学

# Efficient Bit-Serial Multiplication and the Discrete-Time Wiener-Hopf Equation Over Finite Fields

MASAKATU MORII, MEMBER, IEEE, MASAO KASAHARA, SENIOR MEMBER, IEEE, AND DOUGLAS L. WHITING

*Abstract* —Discrete time Wiener-Hopf equations (DTWHE) over finite fields are considered. It is shown that solving the DTWHE is equivalent to performing division over finite fields. This proof gives us a new interpretation of the relationship between bit-serial multiplication and DTWHE's. The interpretation enables us to understand bit-serial multiplication over GF($2^m$) more easily. As an example, new bit-serial multiplication methods for multiplying any two elements which can be done without performing any transformation, or with only a simple transformation of the bases are presented.



神戸大学

*Definition 5:* The discrete-time Wiener-Hopf equation [4] is defined as a system of linear inhomogeneous $t$ equations with $t$ unknowns $a_i$ $(i=0,1,\cdots,t-1)$, $2t-1$ constant coefficients $s_i$ $(i=0,1,\cdots,2t-2)$, that are not all zeros, and $t$ constants, $b_i$ $(i=0,1,\cdots,t-1)$ such that

$$\begin{bmatrix} s_{2t-2} & s_{2t-3} & \cdots & s_{t-1} \\ s_{2t-3} & s_{2t-4} & \cdots & s_{t-2} \\ \cdots & \cdots & & \cdots \\ s_{t-1} & s_{t-2} & \cdots & s_0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \cdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} b_{t-1} \\ b_{t-2} \\ \cdots \\ b_0 \end{bmatrix}. \quad (2.3)$$

In this section, we shall present a new theorem which proves that solving DTWHE is equivalent to performing division over a finite field. Let $v$ and $u$ be any elements over GF($q^m$). Then they can be represented by the following polynomials:

$$v(z) = v_{m-1}z^{m-1} + v_{m-2}z^{m-2} + \cdots + v_0 \qquad (4.1)$$

and

$$u(z) = u_{m-1}z^{m-1} + u_{m-2}z^{m-2} + \cdots + u_0 \qquad (4.2)$$

where $v_k$ $(k = 0, 1, \cdots, m-1) \in \mathrm{GF}(q)$ and $u_k$ $(k = 0, 1, \cdots, m-1) \in \mathrm{GF}(q)$. We represent $s = v/u$ as the polynomial:

$$s(z) = s_{m-1}z^{m-1} + s_{m-2}z^{m-2} + \cdots + s_0 \qquad (4.3)$$

where $s_k$ $(k = 0, 1, \cdots, m-1) \in \mathrm{GF}(q)$. We then have

$$s(z) = \frac{v(z)}{u(z)} \bmod f(z) \qquad (4.4)$$

where $f(z)$ is an irreducible polynomial of degree $m$ over GF($q$). Furthermore, $\alpha$ is the root of $f(z)$ over GF($q^m$).

*Theorem 2:*

$$\begin{bmatrix} \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^i), & \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+1}) & ,\cdots, & \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+m-1}) \\ \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+1}), & \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+2}) & ,\cdots, & \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+m}) \\ \cdots & \cdots & \cdots & \\ \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+m-1}), & \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+m}) & ,\cdots, & \sum_{i=0}^{m-1} u_i \mathrm{tr}(\beta\alpha^{i+2m-2}) \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ s_1 \\ \cdots \\ s_{m-1} \end{bmatrix} = \begin{bmatrix} \sum_{i=0}^{m-1} v_i \mathrm{tr}(\beta\alpha^i) \\ \sum_{i=0}^{m-1} v_i \mathrm{tr}(\beta\alpha^{i+1}) \\ \cdots \\ \sum_{i=0}^{m-1} v_i \mathrm{tr}(\beta\alpha^{i+m-1}) \end{bmatrix} \qquad (4.5)$$

where $\beta$ is an any element of GF($q^m$).

Theorem 2 shows that solving DTWHE over GF($q$) with $m$ unknowns is equivalent to performing the division of GF($q^m$).

神戸大学

## V. Bit-Serial Multiplication Based on the DTWHE Over GF(2)

In this section we shall describe the bit-serial multiplication algorithm based on the DTWHE over GF(2). It is proved that the concept of the dual basis is not necessarily essential when constructing the bit-serial multiplication. Our interpretation enables us to understand better the principles of constructing bit-serial multiplication.

From (4.4), we have

$$v(z) = s(z) \cdot u(z) \bmod f(z). \tag{5.1}$$

Thus we can calculate the right side of (5.1) from (4.5).



神戸大学

$$\begin{bmatrix} \tilde{v}_0 \\ \tilde{v}_1 \\ \cdots \\ \tilde{v}_{m-1} \end{bmatrix} = \begin{bmatrix} \mathrm{tr}(\beta), & \mathrm{tr}(\beta\alpha) & ,\cdots, & \mathrm{tr}(\beta\alpha^{m-1}) \\ \mathrm{tr}(\beta\alpha), & \mathrm{tr}(\beta\alpha^2) & ,\cdots, & \mathrm{tr}(\beta\alpha^{m}) \\ \cdots & \cdots & & \cdots \\ \mathrm{tr}(\beta\alpha^{m-1}), & \mathrm{tr}(\beta\alpha^{m}) & ,\cdots, & \mathrm{tr}(\beta\alpha^{2m-2}) \end{bmatrix} \cdot \begin{bmatrix} v_0 \\ v_1 \\ \cdots \\ v_{m-1} \end{bmatrix} \tag{5.2}$$

$$\begin{bmatrix} \tilde{u}_0 \\ \tilde{u}_1 \\ \cdots \\ \tilde{u}_{m-1} \end{bmatrix} = \begin{bmatrix} \mathrm{tr}(\beta), & \mathrm{tr}(\beta\alpha) & ,\cdots, & \mathrm{tr}(\beta\alpha^{m-1}) \\ \mathrm{tr}(\beta\alpha), & \mathrm{tr}(\beta\alpha^2) & ,\cdots, & \mathrm{tr}(\beta\alpha^{m}) \\ \cdots & \cdots & & \cdots \\ \mathrm{tr}(\beta\alpha^{m-1}), & \mathrm{tr}(\beta\alpha^{m}) & ,\cdots, & \mathrm{tr}(\beta\alpha^{2m-2}) \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \cdots \\ u_{m-1} \end{bmatrix}. \tag{5.3}$$

神戸大学

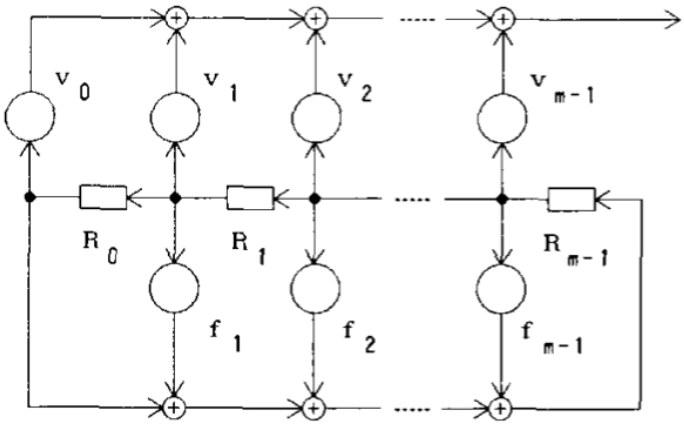



Fig. 2. Bit-serial multiplier using shift-register circuit.



神戸大学

## VII. Conclusion

In this paper we have given a new interpretation of the relationship between bit-serial multiplication and the discrete-time Wiener–Hopf equation. Our new interpretation enables us to understand the principles of constructing bit-serial multipliers over GF($2^m$) more clearly and more easily. We have presented new bit-serial methods for multiplying two field elements which can be used without performing any transformation, or with only a simple transformation of the bases.

Furthermore, we have proved that division within GF($q^m$) is equivalent to the DTWHE over GF($q$). This is both interesting and important since fast algorithms for the DTWHE over GF($q$) can be studied extensively in the near future.

THE TRANSACTIONS OF THE IEICE, VOL. E 72, NO. 1 JANUARY 1989



PAPER

# Efficient Construction of Gate Circuit for Computing Multiplicative Inverses over $GF(2^m)$

Masakatu MORII† *and* Masao KASAHARA††, *Members*

**SUMMARY** The theory of finite fields has been successfully applied to the constructing of the various algebraic codes, digital signal processing, and techniques of cryptography. Especially the theories on four operations are very important, because it is strongly related to the size and the throughput of the gate circuits for the various encoders and decoders. In this paper we shall give a new method for constructing the gate circuit that yields the multiplicative inverses over $GF(2^m)$. The method is based on a new algorithm for computing multiplicative inverses in $GF(2^m)$. The operations needed for our algorithm are rarely performed on $GF(2^m)$, but primarily on the subfields of $GF(2^m)$. When performing the multiplication and division over finite fields, the idea of using the subfield has been given wide attention. However the conventional algorithms taking advantage of this idea are not necessarily efficient from the practical point of view. We see that our algorithm proved superior to the conventional methods when $GF(2^m)$ has the subfield $GF(2^2)$.

27

神戸大学

**SUMMARY** The theory of finite fields has been successfully applied to the constructing of the various algebraic codes, digital signal processing, and techniques of cryptography. Especially the theories on four operations are very important, because it is strongly related to the size and the throughput of the gate circuits for the various encoders and decoders. In this paper we shall give a new method for constructing the gate circuit that yields the multiplicative inverses over $GF(2^m)$. The method is based on a new algorithm for computing multiplicative inverses in $GF(2^m)$. The operations needed for our algorithm are rarely performed on $GF(2^m)$, but primarily on the subfields of $GF(2^m)$. When performing the multiplication and division over finite fields, the idea of using the subfield has been given wide attention. However the conventional algorithms taking advantage of this idea are not necessarily efficient from the practical point of view. We see that our algorithm proved superior to the conventional methods when $GF(2^m)$ has the subfield $GF(2^2)$.



28

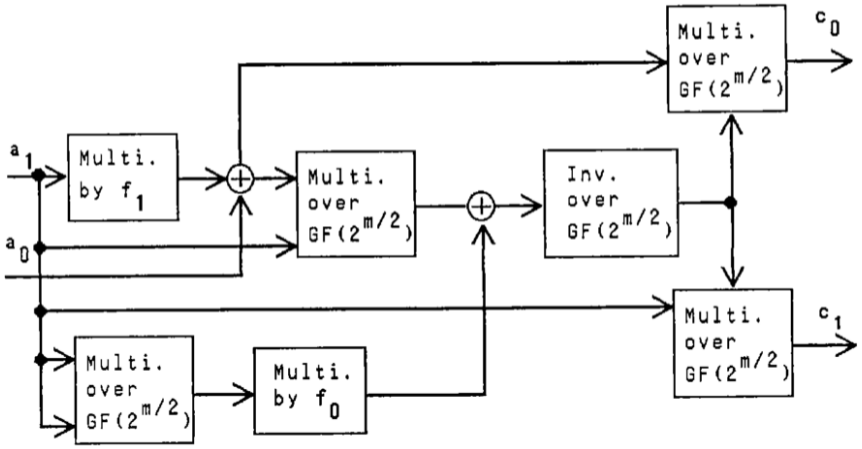


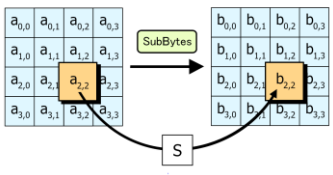

Fig. 1 Block diagram of the gate circuit generating multiplicative inverses over $GF(2^m)$.



# AES

事実上の国際標準暗号（２００１年）
- 基本的に換字置換（Ｓ－Ｂｏｘ）による設計
  - 有限体$GF(2^8)$演算を利用

**ＩＢＭが提案したＡＥＳアーキテクチャに採用**



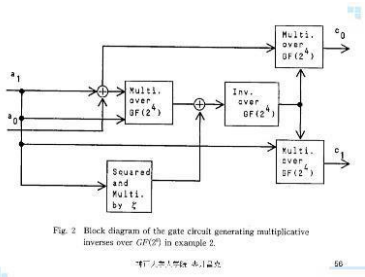




Fig. 2 Block diagram of the gate circuit generating multiplicative inverses over $GF(2^8)$ in example 2.

神戸大学

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 38, NO. 6, NOVEMBER 1992

# Generalized Key-Equation of Remainder Decoding Algorithm for Reed–Solomon Codes

Masakatu Morii, *Member, IEEE,* and Masao Kasahara,
*Senior Member, IEEE*

***Abstract*—A new key-equation of the remainder decoding algorithm is presented. It is noted that the key-equation presents a general relationship between the errors on the received codeword and the coefficients of the remainder polynomial. It is shown that we can derive several key-equations proposed by Welch–Berlekamp and others from our new key-equation. Furthermore useful properties of the key-equations in fast decoding of Reed–Solomon codes are given.**

***Index Terms*—Coding theory, decoding algorithm, Reed–Solomon codes, remainder decoding, Welch–Berlekamp algorithm.**

神戸大学

## ACKNOWLEDGMENT

The authors would like to thank Dr. D. L. Whiting of State of the Arts Consulting for sending helpful information on the remainder decoding algorithms. One of authors, M. Morii is also grateful to Prof. E. R. Berlekamp, University of Berkeley, for his helpful suggestions and observations.

神戸大学

論　文

離散対数を利用した公開鍵暗号系について

正　員　森井　昌克†　　正　員　笠原　正雄†

New Public Key Cryptosystem Using Discrete Logarithms over $GF(p)$

Masakatu MORII † *and* Masao KASAHARA †, *Members*

**あらまし**　本論文では，素体 $GF(p)$ 上の離散対数問題を落し戸一方向性関数（trap door one-way function）とする公開鍵暗号の一方式を提案する．本暗号は良く知られた公開鍵暗号である RSA 暗号と比較して，復号化変換はほぼ同等であるものの，暗号化変換に際しては，べき乗剰余演算を行わないために並列処理技法を容易に適用することができ，またメモリ等を利用することにより，計算量を大幅に減少させることができる．

本暗号はべき乗剰余演算を利用するという点で RSA 暗号と，更に，ナップザック型公開鍵暗号の拡張であるという点で Merkle と Hellman が提案した乗算型ナップザック暗号とにそれぞれ密接に関係している．従って本論文で提案する暗号方式は，これらの暗号の理論的な構造をより明白なものにするためにも興味深い結果を与えるものである．



# アジェンダ（２）

神戸大学

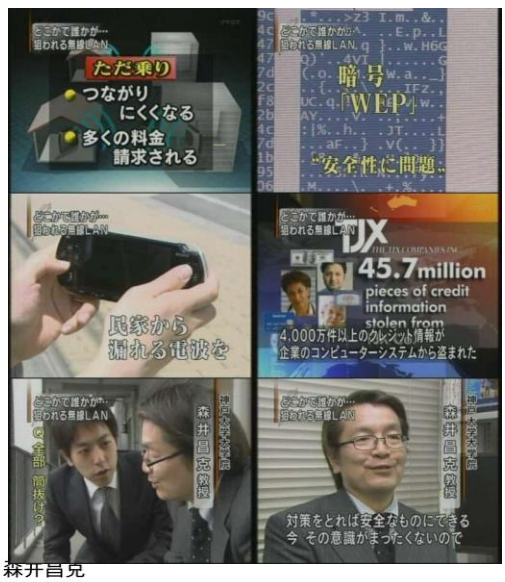
- その後の主な成果
  - 暗号とサイバーセキュリティを中心として
- しかし…
  - 自身では「（古典的？）符号理論とその応用」がメイン（と思っている）、たとえば…
    - 最良線形符号構成問題
    - QRコード


神戸大学

# 無線ＬＡＮ暗号化システムの安全性評価

神戸大学

2008年10月，我々は標準的な無線ＬＡＮ暗号規格であるＷＥＰを一瞬にして解読する方法を世界で初めて開発しました．いまだに利用されているＷＥＰですが．暗号としての効果はなくなったわけです．現在，その後継である，ＷＰＡやＷＰＡ２について，その安全性について研究を行っています．合わせて，安全な無線ＬＡＮの利用方法について研究開発を進めています．また，我々は無線ＬＡＮだけでなく，各種暗号についての安全性評価について，日々，研究開発を行っています．




神戸大学 森井昌克

神戸大学

## New Attack Cracks Common Wi-Fi Encryption in a Minute

**Japanese researchers have developed a way to crack WPA encryption in about a minute.**

Robert McMillan, IDG News Service

PCWORLD; 26 Aug 2009

Wed, 26 Aug 2009 23:40:11 -0700

Computer scientists in Japan say they've developed a way to break the WPA e
used in wireless routers in about one minute.

The attack gives hackers a way to read encrypted traffic sent between comput
types of routers that use the WPA (Wi-Fi Protected Access) encryption system.
developed by Toshihiro Ohigashi of Hiroshima University and Masakatu Morii o
who plan to discuss further details at a technical conference set for Sept. 25 in



## Other

*Topic: Networking* *Follow via:*

## Researchers crack WPA Wi-Fi encryption in 60 seconds

***Summary:*** *Computer scientists in Japan have developed a way to break the WPA encryption system used in wireless routers in just one minute.The attack, which rec computers and certain types of r Protected Access) encryption sys Ohigashi of Hiroshima Universit University.*

By Andrew Nusca for B
06:54 GMT (23:54 PD

## Cracked in 60 Seconds: WPA Falls

**WPA Busted Like a Cheap Toy**

**September 2, 2009**
**By Andy Patrizio**

It's been known for years that the Wired Equivalent Privacy or WEP protocol is easily broken, and that to be secure, wireless networks should use the more powerful protocol called Wi-Fi Protected Access, or WPA.

Now security experts say they've proven that WPA can be breached just as easily. A pair of researchers in Japan said that they developed a way to break WPA encryption in about one minute -- and will show how at a conference there next month.

WPA's viability has been in doubt since late 2008, when security researchers Martin Beck and Erik Tews demonstrated the ability to break the Temporal Key Integrity Protocol (TKIP) that provides WPA security within 15 minutes.

Now, Researchers Toshihiro Ohigashi of Hiroshima University and Masakatu Morii of Kobe University said they've improved on that. The pair has already discussed their findings in a paper presented at the Joint Workshop on Information Security held in Taiwan earlier this month and will discuss it again at a Sept. 25 event in Hiroshima.

## まだまだSSL/TLS脆弱性、花盛りですが

- この問題について詳しくは話しませんが…
  - 実は暗号システムの実装問題として我々の研究分野なのですが…
  - SSl/TLS on RC4の解読(脆弱性)FSE2013(3月)
    - 国内関係諸機関には2012年10月に報告
- BEAST, POODLE、そしてCREAM
  - POODLE
    - **Padding** Oracle Attack
  - CREAM
    - Cache-timing attack

Prof. Dan Bernstein says; …

SSL/TLSの脆弱性

神戸大学大学院 森井昌克 99

## SSL/TLSは終わった！

- BEASTとLucky13でSSL/TLSは終わったか？
  - BEAST[illegible]のみ有効、Lucky13はブロック暗号方式有効
- [illegible]SSL/TLS on RC4が健在！
  - Googleも使っているSSL/TLS on RC4へのシフトを推奨
  - SSL/TLS on RC4は高速、軽実装

神戸大学大学院 森井昌克 101

## 我々は、

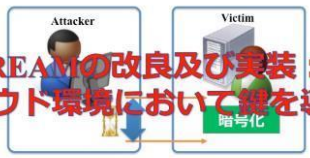
**2012年12月(2013年3月)**
**SSL/TLS on RC4の致命的な脆弱性を世界で初めて指摘**

**SSLの4割はSSL/TLS on RC4、特にgoogleはこれを利用、推進…そのわけは？**

神戸大学大学院 森井昌克 98

## 鍵回復攻撃の実行 12

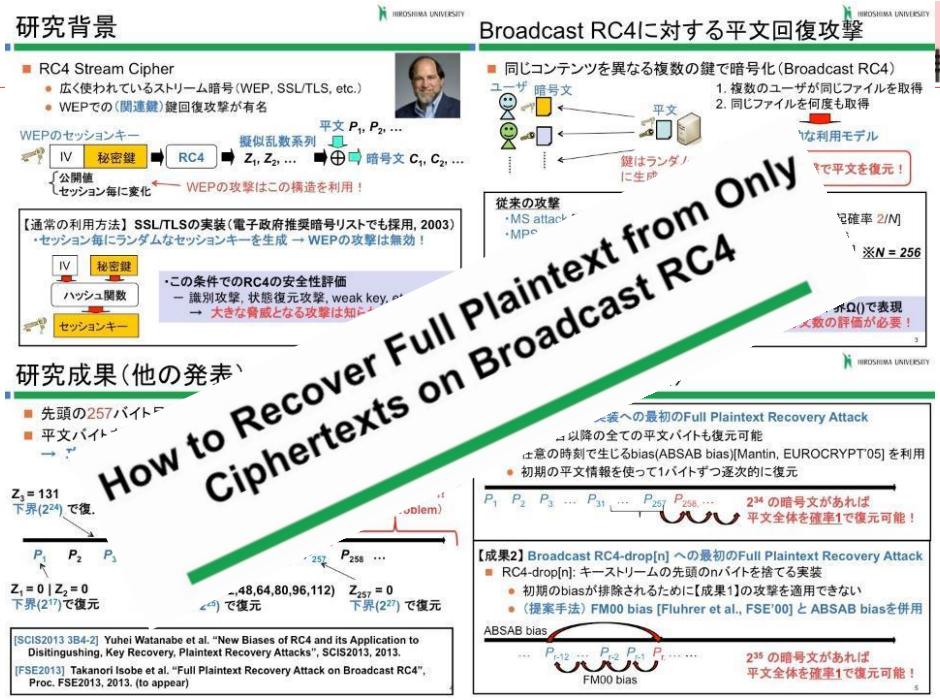
◆ キャッシュタイミング攻撃の実行




**CREAMの改良及び実装：クラウド環境において鍵を導出**

Attacker側で時間計測を行い，
BernsteinのCache-timing attacksと同様の攻撃を実行

➡復元に成功することも失敗することもある
ノイズの影響が大きい




## アジェンダ（２）

更に発展して？

- その後の主な成果
  - 暗号とサイバーセキュリティを中心として
- しかし…
  - 自身では「（古典的？）符号理論とその応用」がメイン（と思っている）、たとえば…
    - 最良線形符号構成問題
    - QRコード

# アジェンダ（２）

神戸大学

- その後の主な成果
  - 暗号とサイバーセキュリティを中心として
- しかし…
  - 自身では「(古典的？)符号理論とその応用」がメイン(と思っている)、たとえば…
    - 最良線形符号構成問題
    - QRコード



# 最良符号

神戸大学

## 最良符号

同一符号長 $n$, 同一情報点数 $k$ の符号の中で現在発見されている最大の最小距離 $d$ を有する符号

## 最良符号データベース

- *Markus Grassl* によってweb上で管理
  ( http://www.codetables.de/ )
- 255以下の各( $n$ , $k$ )線形符号の最良符号
- 様々な方法で
  新しい最小距離と理論的上界が更新

| n/k | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|
| 121 | 40-46 | 39-45 | 38-44 | 37-44 | 35-44 | 34-42 |
| 122 | 41-46 | 40-46 | 39-45 | 38-44 | 36-44 | 35-43 |
| 123 | 42-46 | 41-46 | 40-46 | 39-45 | 36-44 | 36-44 |
| 124 | 43-47 | 42-46 | 41-46 | 40-46 | 36-44 | 36-44 |
| 125 | 44-48 | 43-47 | 42-46 | 41-46 | 36-45 | 36-44 |
| 126 | 44-48 | 44-48 | 43-47 | 42-46 | 36-46 | 36-45 |
| 127 | 44-48 | 44-48 | 44-48 | 43-47 | 37-46 | 36-46 |
| 128 | 44-49 | 44-48 | 44-48 | 44-48 | 38-46 | 36-46 |
| 129 | 44-50 | 44-48 | 44-48 | 44-48 | 38-47 | 36-46 |
| 130 | 44-50 | 44-49 | 44-48 | 44-48 | 39-48 | 37-47 |

最小距離　理論的上界

→　最良符号には巡回符号やその修正符号が多く存在

# 最良誤り訂正線形符号構成問題

神戸大学

符号長 $n$ / 情報点数 $k$

| | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|
| 54 | 20 | 20 | 19–20 | 18–19 | 16–18 |
| 55 | 20–21 | Ja 20 | 20 | LC 19–20 | 16–19 |
| 56 | 20–22 | 20–21 | 20 | 20 | MoY 17–20 |
| 57 | Ja 21–22 | | | | 18–20 |
| 58 | GG 22–23 | 20–22 | 20–22 | 20–21 | 18–20 |
| 59 | 22–24 | 21–22 | Ja 20–22 | 20–22 | 19–21 |

発見者名　　発見者名

最小距離 ― 最小距離の上限

**最良誤り訂正線形符号のデータベース**

http://www.rz.uni-karlsruhe.de/~kg11/codetables/BKLC/BKLC_query.php

Lb(56,17) = 17　MoY

$(n,k,d_{\min})=(56,17,17)$最良誤り訂正符号

MoY: M. Morii & T. Yoshimura, email comm. Nov 1993-Jan 1994.

神戸大学 森井昌克

神戸大学

**Bounds on linear codes [57,17] over GF(2)**

lower bound: 18
upper bound: 20

**Construction**

```
Construction of a linear code
[57,17,18] over GF(2):
[1]:   [56, 17, 17] Linear Code over GF(2)
       Construction from a stored generator matrix
[2]:   [57, 17, 18] Linear Code over GF(2)
       ExtendCode [1] by 1

last modified: 2001-01-30
```

**From Brouwer's table (as of 2007-02-13)**

```
Lb(57,17) = 18 is found by adding a parity check bit to:
Lb(56,17) = 17 MoY

Ub(57,17) = 20 follows by a one-step Griesmer bound from:
Ub(36,16) = 10 follows by a one-step Griesmer bound from:
Ub(25,15) = 5 Si
```

**References**

**MoY:** M. Morii & T. Yoshimura, email comm. Nov 1993-Jan 1994.

**Si:** J. Simonis, *Binary even [25,15,6] codes do not exist*, IEEE Trans. Inform. Theory **IT-33** (Jan. 1987) 151-153.

## Bounds on the minimum distance of linear codes

神戸大学

### Bounds on linear codes [36,14] over GF(2)

lower bound: 11
upper bound: 11

### Construction

Construction type: **Mo**

```
Construction of a linear code
[36,14,11] over GF(2):
[1]:   [36,  14,  11] Linear Code over GF(2)
       Construction from a stored generator matrix

last modified: 2001-01-30
```

### From Brouwer's table (as of 2007-02-13)

```
Lb(36,14) = 11 Mo

Ub(36,14) = 11 is found by considering shortening to:
Ub(35,13) = 11 Ja
```

**References**

**Ja:** D.B. Jaffe, *Binary linear codes: new results on nonexistence*, 1996, **code.ps.gz**.

**Mo:** M. Morii, email comm., Sept. 1993.

神戸大学

| n/k | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | 31 | 20 | 17 | 16 | 16 | 15 | 13 | 12 | 12 | 12 | 11 | 10 | 9 | 8 | 8 | 8 |
| 32 | 32 | 21 | 18 | 16 | 16 | 16 | 14 | 13 | 12 | 12 | 12 | 10 | 10 | 8-9 | 8 | 8 |
| 33 | 33 | 22 | 18 | 16 | 16 | 16 | 14 | 14 | 12 | 12 | 12 | 11 | 10 | 9-10 | 8-9 | 8 |
| 34 | 34 | 22 | 19 | 17 | 16 | 16 | 15 | 14 | 13 | 12 | 12 | 12 | 10 | 10 | 9-10 | 8-9 |
| 35 | 35 | 23 | 20 | 18 | 16 | 16 | 16 | 15 | 14 | 12-13 | 12 | 12 | 11 | 10 | 10 | 9-10 |
| 36 | 36 | 24 | 20 | 18 | 17 | 16 | 16 | 16 | 14 | 13-14 | 12-13 | 12 | 12 | 11 | 10 | 10 |
| 37 | 37 | 24 | 20 | 19 | 18 | 17 | 16 | 16 | 15 | 14 | 13-14 | 12-13 | 12 | 12 | 10-11 | 10 |
| 38 | 38 | 25 | 21 | 20 | 18 | 18 | 16 | 16 | 16 | 14 | 14 | 13-14 | 12 | 12 | 11-12 | 10-11 |
| 39 | 39 | 26 | 22 | 20 | 19 | 18 | 17 | 16 | 16 | 15 | 14 | 14 | 12-13 | 12 | 12 | 11-12 |
| 40 | 40 | 26 | 22 | 20 | 20 | 18 | 18 | 16 | 16 | 16 | 15 | 14 | 13-14 | 12-13 | 12 | 12 |
| n/k | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 41 | 41 | 27 | 23 | 21 | 20 | 19 | 18 | 17 | 16 | 16 | 16 | 14-15 | 14 | 12-14 | 12-13 | 12 |
| 42 | 42 | 28 | 24 | 22 | 20 | 20 | 19 | 18 | 17 | 16 | 16 | 15-16 | 14 | 13-14 | 12-14 | 12-13 |
| 43 | 43 | 28 | 24 | 22 | 21 | 20 | 20 | 18 | 18 | 16-17 | 16 | 16 | 15 | 14 | 13-14 | 12-14 |
| 44 | 44 | 29 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17-18 | 16-17 | 16 | 16 | 15 | 14 | 13-14 |
| 45 | 45 | 30 | 25 | 24 | 22 | 22 | 20 | 20 | 18-19 | 18 | 16-18 | 16 | 16 | 16 | 14-15 | 14 |
| 46 | 46 | 30 | 26 | 24 | 23 | 22 | 21 | 20 | 19-20 | 18-19 | 17-18 | 16-17 | 16 | 16 | 15-16 | 14-15 |
| 47 | 47 | 31 | 26 | 24 | 24 | 23 | 22 | 21 | 20 | 19-20 | 18 | 16-18 | 16-17 | 16 | 16 | 15-16 |
| 48 | 48 | 32 | 27 | 24 | 24 | 24 | 22 | 22 | 20 | 20 | 18-19 | 17-18 | 16-18 | 16-17 | 16 | 16 |
| 49 | 49 | 32 | 28 | 25 | 24 | 24 | 23 | 22 | 20 | 20 | 19-20 | 18-19 | 17-18 | 16-18 | 16-17 | 16 |
| 50 | 50 | 33 | 28 | 26 | 24 | 24 | 24 | 23 | 21 | 20 | 20 | 18-20 | 18-19 | 17-18 | 16-18 | 16-17 |

## Bounds on the minimum distance of linear codes

### Bounds on linear codes [127,30] over GF(2)

lower bound: 37
upper bound: 46

### Construction

Construction type: **MoY**

```
Construction of a linear
code [127,30,37] over GF(2):
[1]:  [127, 30, 37] Linear Code over GF(2)
      Construction from a stored generator matrix

last modified: 2001-03-12
```

### From Brouwer's table (as of 2007-02-13)

```
Lb(127,30) = 37 MoY

Ub(127,30) = 46 is found by considering shortening to:
Ub(123,26) = 46 otherwise adding a parity check bit would contradict:
Ub(124,26) = 47 Bro
```

**References**

**Bro:** A.E. Brouwer, *The linear programming bound for binary linear codes*, IEEE Trans. Inform. Th. **39** (1993) 677-680.

**MoY:** M. Morii & T. Yoshimura, email comm. Nov 1993-Jan 1994.

| n/k | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |
|---|---|---|---|---|---|---|---|---|---|---|
| 121 | 40-46 | 39-45 | 38-44 | 37-44 | 35-44 | 34-42 | 33-42 | 32-42 | 32-41 | 32-40 |
| 122 | 41-46 | 40-46 | 39-45 | 38-44 | 36-44 | 35-43 | 34-42 | 33-42 | 32-42 | 32-41 |
| 123 | 42-46 | 41-46 | 40-46 | 39-45 | 36-44 | 36-44 | 35-43 | 34-42 | 33-42 | 32-42 |
| 124 | 43-47 | 42-46 | 41-46 | 40-46 | 36-44 | 36-44 | 36-44 | 35-43 | 34-42 | 33-42 |
| 125 | 44-48 | 43-47 | 42-46 | 41-46 | 36-45 | 36-44 | 36-44 | 36-44 | 35-43 | 34-42 |
| 126 | 44-48 | 44-48 | 43-47 | 42-46 | 36-46 | 36-45 | 36-44 | 36-44 | 36-44 | 35-42 |
| 127 | 44-48 | 44-48 | 44-48 | 43-47 | 37-46 | 36-46 | 36-45 | 36-44 | 36-44 | 36-43 |
| 128 | 44-49 | 44-48 | 44-48 | 44-48 | 38-46 | 36-46 | 36-46 | 36-45 | 36-44 | 36-44 |
| 129 | 44-50 | 44-48 | 44-48 | 44-48 | 38-47 | 36-46 | 36-46 | 36-46 | 36-44 | 36-44 |
| 130 | 44-50 | 44-49 | 44-48 | 44-48 | 39-48 | 37-47 | 36-46 | 36-46 | 36-45 | 36-44 |
| n/k | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

## 最良符号構成と重み分布導出

神戸大学

重み分布導出

全符号語のハミング重みとその符号語数の分布

・最小重み $d$ 周辺の局所重み分布は性能評価に利用
（誤り訂正能力・復号誤り率の近似値など）

・重み分布の導出は規模の大きな符号では困難

・$k$ - sparseアルゴリズム*：巡回符号の巡回構造を利用した導出法

最良符号構成

同一の符号長，情報点数の中で最大の誤り訂正能力を持つ符号

・最良符号には巡回符号やその修正符号が多く存在

⇒巡回構造を失う

*M.Mohri and M.Morii, “On Computing the Number of Codewords with Minimum Weight for Cyclic Codes,” IEICE A, vol.J79-A, no.4, pp963-972.



## 研究概要

神戸大学

巡回符号の修正符号に対する高速な重み分布導出法*

・$k$-sparse アルゴリズムの改良

▪ パンクチャド符号 ・ 拡大符号 ・ 短縮符号の最小重み符号語数の導出

修正符号を利用した効率的な最良符号構成法**

▪ 一般化パンクチャド符号を利用した構成法

・Zwanzgerの構成法（評価関数，バックトラック法）を利用

情報点数が大きな巡回符号を修正し，新しい最良符号を構成

計159個の最良符号を構成

*渡邉元幸, 森井昌克, “巡回符号のパンクチャド符号に対する重み分布導出の高速化,” 第36回情報理論とその応用シンポジウム(SITA2013), pp.75-80, 2013年.

**M. Watanabe and M. Morii, “A New Method for Constructing Good Linear Codes; update on the minimum distance of some linear codes,” The 35th Symposium on Theory and its Applications(SITA2012), pp.634-638, 2012.

# パンクチャド符号を利用した最良符号構成

神戸大学

修正符号を利用した効率的な最良符号構成法*

Zwanzgerの構成法

・評価関数を用いて追加列の組み合わせを決定

⇒ 最良符号となる可能性が高い符号のみを構成

評価関数を新たに定義

朝倉らの一般化パンクチャド符号を利用した構成法

・削除する検査ビットを無作為に変更しながら最良符号を探索

◆削除する検査ビットを評価関数によりヒューリスティックに決定

◆バックトラック法を用いて効率的に異なるパンクチャド符号を探索

→ 54個の最良符号を構成*

*M. Watanabe and M. Morii, “A New Method for Constructing Good Linear Codes; update on the minimum distance of some linear codes,” The 35th Symposium on Theory and its Applications(SITA2012), pp.634-638, 2012.



# 新たな最良符号の構成

神戸大学

修正符号を利用した効率的な最良符号構成法**

- 朝倉らの最良符号構成法を改良し効率的に探索

・削除する検査ビットを評価関数によりヒューリスティックに決定

＋

巡回符号の修正符号に対する高速な重み分布導出法により局所重み分布を効率的に導出

情報点数が大きな巡回符号を修正し，新しい最良符号を構成

計159個の最良符号を構成

**M. Watanabe and M. Morii, “A New Method for Constructing Good Linear Codes; update on the minimum distance of some linear codes,” The 35th Symposium on Theory and its Applications(SITA2012), pp.634-638, 2012.

# 新たに構成した最良符号

神戸大学

Table1 : Best Codes modified from (255, 21, 111) BCH Code

| | Best Code | Construction |
|---|---|---|
| 1 | (215, 20, 85) | [1] : (254, 20, 111) Linear Code over GF(2)<br>Shortening of (255, 21, 111) BCHCode at { 21 }<br>[2] : (215, 20, 85) Linear Code over GF(2)<br>Puncturing of [1] at { 21, 45, 51, 64, 73, 78, 84, 95, 97, 113, 117, 121, 128, 140, 142, 143, 151, 163, 172, 178, 179, 183, 187, 189, 190, 192, 194, 195, 202, 204, 209, 213, 218, 220, 233, 236, 246, 248, 254 } |
| 2 | (216, 20, 86) | ExtendCode (215, 20, 85) by 1 |
| 3 | (222, 20, 89) | [1] : (254, 20, 111) Linear Code over GF(2)<br>Shortening of (255, 21, 111) BCHCode at { 21 }<br>[2] : (222, 20, 89) Linear Code over GF(2)<br>Puncturing of [1] at { 29, 30, 32, 41, 57, 92, 121, 129, 140, 142, 144, 150, 151, 155, 167, 169, 178, 183, 186, 190, 192, 193, 194, 209, 218, 220, 221, 227, 228, 246, 248, 254 } |
| 4 | (223, 20, 90) | ExtendCode (222, 20, 89) by 1 |
| 5 | (209, 21, 81) | [1] : (209, 21, 81) Linear Code over GF(2)<br>Puncturing of (255, 21, 111) BCHCode at { 28, 34, 35, 36, 50, 52, 53, 55, 56, 59, 62, 64, 67, 71, 74, 78, 91, 100, 102, 106, 112, 118, 120, 129, 134, 139, 149, 157, 159, 161, 183, 184, 200, 203, 204, 214, 216, 219, 230, 242, 248, 251, 252, 253, 254, 255 } |
| 6 | (210, 21, 82) | ExtendCode (209, 21, 81) by 1 |
| 7 | (213, 21, 83) | [1] : (213, 21, 83) Linear Code over GF(2)<br>Puncturing of (255, 21, 111) BCHCode at { 24, 28, 34, 53, 56, 59, 67, 69, 71, 99, 100, 102, 105, 106, 118, 120, 121, 123, 134, 139, 155, 158, 159, 161, 165, 173, 179, 183, 184, 216, 219, 221, 222, 228, 239, 242, 248, 251, 252, 253, 254, 255 } |
| 8 | (214, 21, 84) | ExtendCode (213, 21, 83) by 1 |
| | | [1] : (234, 21, 89) Linear Code over GF(2) |

計159個の最良符号を構成



# つい、最近も

神戸大学

PAPER Special Section on Information Theory and Its Applications

## A Construction of Binary Punctured Linear Codes and A Supporting Method for Best Code Search*

Takuya OHARA†, *Nonmember*, Makoto TAKITA††, *Member*, *and* Masakatu MORII†, *Fellow*

**SUMMARY** Reduction of redundancy and improvement of error-correcting capability are essential research themes in the coding theory. The best known codes constructed in various ways are recorded in a database maintained by Markus Grassl. In this paper, we propose an algorithm to construct the best code using punctured codes and a supporting method for constructing the best codes. First, we define a new evaluation function to determine deletion bits and propose an algorithm for constructing punctured linear codes. 27 new best codes were constructed in the proposed algorithm, and 112 new best codes were constructed by further modifying those best codes. Secondly, we evaluate the possibility of increasing the minimum distance based on the relationship between code length, information length, and minimum distance. We narrowed down the target $(n, k)$ code to try the best code search based on the evaluation and found 28 new best codes.

We also propose a method to rapidly derive the minimum weight of the modified cyclic codes. A cyclic code loses its cyclic structure when it is modified, so we extend the $k$-sparse algorithm to use it for modified cyclic codes as well. The extended $k$-sparse algorithm is used to verify our newly constructed best code.

***key words:*** *best code, modified code, linear code, weight distribution, minimum distance*

2021-04-23

codes via puncturing cyclic and shortened cyclic codes:
$[213,30,73]_2$, $[227,36,73]_2$, $[229,35,75]_2$, $[230,33,77]_2$ from

Motoyuki Watanabe and Masakatu Morii,
"A New Method for Constructing Good Linear Codes; updating on the minimum distance of some linear codes,"
Proc. SITA2012, pp.636-638, Dec. 2012.

$[216,30,75]_2$, $[220,47,61]_2$, $[224,34,73]_2$, $[224,42,67]_2$, $[224,47,63]_2$, $[225,40,69]_2$, $[228,42,69]_2$, $[228,45,67]_2$, $[229,47,66]_2$, $[230,41,71]_2$, $[231,39,73]_2$, $[231,47,67]_2$, $[232,37,75]_2$, $[232,45,69]_2$, $[234,44,71]_2$, $[235,42,73]_2$, $[235,47,69]_2$, $[237,45,72]_2$, $[238,47,71]_2$, $[239,45,73]_2$, $[241,47,73]_2$, $[242,45,75]_2$ from

Takuya Ohara, Makoto Takita and Masakatu Morii,
"A Construction of Binary Punctured Linear Codes and A Supporting Method for Best Code Search,"
Proc. 2020 International Symposium on Information Theory and Its Applications (ISITA), Oct. 2020.
IEEE Xplore: 9366122

## QRコードの構成

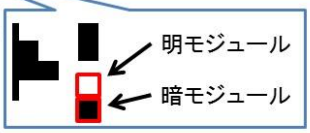


神戸大学

- 機能パターン
  - 位置検出
  - 位置合わせ
  - 型番情報
  - 形式情報
  - など

- 符号化領域
  - データ
  - 誤り訂正コード語
  - など

•QRコードは，モジュールと呼ばれる明暗の二値を持つ四角形を最小単位として構成




•大きく分けて機能パターン，符号化領域から成る

•機能パターンはデコーダでの読取り時に必要な構造
•符号化領域には，符号化された格納情報が記録される



## QRコードに関する研究

神戸大学

**この十数年、研究室において様々なQRコードに関する研究を行っている、例えば**

- 難読QRコードの高精度読み取りに関する研究
- QRコードの多重化に関する研究
- ハイブリッドQRコードに関する研究
- PA(Post Aesthetic) QRコードに関する研究
- HiddenQRコードに関する研究
- QRコードを用いた認証システムに関する研究
- FakeQRコードに関する研究
- **ホログラムQRコードに関する研究**
- その他

## PA（Post Aesthetic）QRコードに関する研究

神戸大学




## QRコードのセキュリティ

神戸大学

**「このQRコードを読み取ってくれないか」――街中での謎の声かけがTwitterで話題　セキュリティ企業も警鐘**

**ITmedia　2021年10月28日**

2021年10月28日 17時35分 公開

印刷　3098　Share　B!

PR GraphQL徹底入門。RESTと比較、API・フロントの実装から学ぶ
PR コアウェブバイタル対策進んでいますか。キャンペーン実施中

「僕達の新事業のQRコードを読み取ってもらえま
けにあったというツイートが話題を集めている。ツ
ストのせきぐちあいみさん（@sekiguchiaimi）。せ
と、27日に中目黒駅で見知らぬ男女2人に、前述のよ

「このQRコードを読み取ってくれないか」――街中での謎の声かけがTwitterで話題　セキュリティ企業も警鐘
ITmedia NEWS 10/28(木) 17:38

58件のコメント

森井昌克 | 10/28(木) 18:35

魅力的な言葉での前置きのあとでさえ、「ここにアクセスしてください」と誘うのは不審がられるとしても、「このＱＲコードを読み取ってください」と言われ、その誘いに乗る人は少なくないと言われます。テレビや雑誌でもＱＲコードを読み取るという作業が一般化し、スマホ決済にも使われ、ＱＲコードを読み込むこと自体に障壁がなく、躊躇することもないので安易に読み取ってしまうのです。その結果、悪意のあるサイトに導かれ、更なる詐欺の手口のきっかけとなってしまいます。ＱＲコードの最大の欠点は人がその意味を読み取れないことです。これは「安全なＱＲコードです」と言われても、何も保証されるものではありません。ＱＲコードを読み、そこに記されたサイトを訪れると、スマホの異常動作を模した画面となり、あたふたとしている間にスマホを操作されてマルウェア（コンピューターウイルス）を仕組まれてしまうことも考えられます。

# QRコードのセキュリティ

神戸大学

「AIはだませない」神話にだまされてはいけない

(1/2 ページ)

「人間は失敗や間違いをするけれど、機械は常に正確な判断ができるから」と、RPAやAIの導入を進める人や会社をよく見かけるかもしれません。でも、ちょっと待ってください。「AIや機械は間違えない」というその認識、本当に正しいのでしょうか？

2018年07月03日 07時00分 公開

印刷　通知　47

この記事は**会員限定**です。会員登録する

「人間は失敗や間違いをするけれど、機械は絶対にたことはありませんか？　確かに、「人間が見落とし単純な処理を繰り返しても認識精度が落ちない」など ります。しかし、機械やAIも「絶対に間違えない」 よらない盲点を突いた攻撃によって、過ちを冒すこと

**QRコードがスマホのカメラをだます？**

先日、興味深いニュースがありました。「QRコード 来のリンク先とは別の『偽サイト』のリンクを埋め込 まう」というものです。神戸大学の森井昌克教授率い る解説記事も出ています。

ITmedia　2018年7月3日

「人間は失敗や間違いをするけれど、機械は絶対に間違えない」と信じている人に出会ったことはありませんか？　確かに、「人間が見落としがちな部分を認識できる」「長時間、単純な処理を繰り返しても認識精度が落ちない」など、機械を導入するメリットはたくさんあります。しかし、機械やAIも「絶対に間違えない」わけではありません。人間には思いもよらない盲点を突いた攻撃によって、過ちを冒すこともあるのです。

**QRコードがスマホのカメラをだます？**

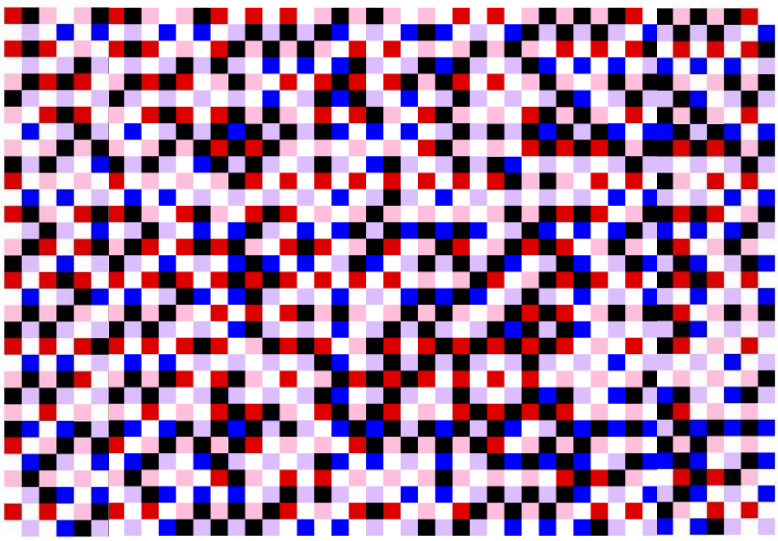
先日、興味深いニュースがありました。「QRコードにセキュリティ上の弱点があり、本来のリンク先とは別の『偽サイト』のリンクを埋め込んで、ユーザーの一部を誘導できてしまう」というものです。神戸大学の森井昌克教授率いる研究室が発表し、森井教授自身による解説記事も出ています。

(参考)

- 気を付けろ！QRコードに脆弱性？　その深刻さと騙されないための対策（森井昌克個人 -Yahoo!ニュース）

# HiddenQRコードに関する研究

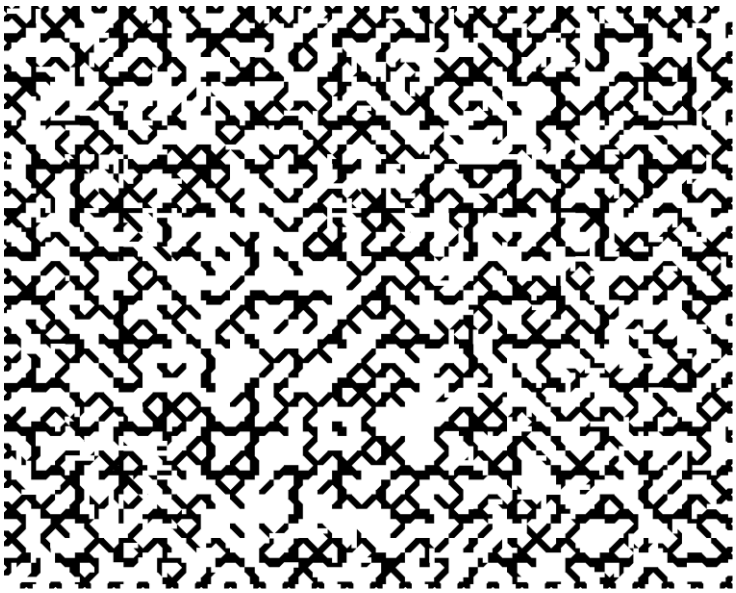
神戸大学



60

## HiddenQRコードに関する研究

神戸大学





## QRコードのセキュリティ

神戸大学

ニュース

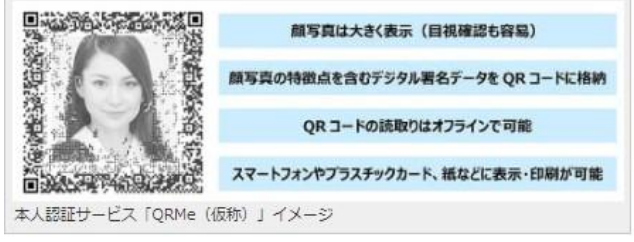
**セイコーソリューションズ、顔写真入りQRコードを活用した新たな本人認証サービス「QRMe（仮称）」を開発**

三柳 英樹　2021年6月14日 06:00

ツイート　リスト　B! 1　Pocket 3　いいね！5　シェア

セイコーソリューションズ株式会社は11日、大きな顔写真と一体化したQRコードを活用した本人認証サービス「QRMe（仮称）」の2021年秋以降の提供開始を目指し、新たにQRコードに関する特許を出願したと発表した。

本人認証サービス「QRMe（仮称）」は、ID／パスワード不要の本人認証サービス「認証BANK QR Auth」にて協働している神戸大学森井昌克教授が研究した、QRコードの生成技術をベースとしている。QRコードの中央に顔写真を大きく表示し、顔写真周辺に配置したドット部に顔写真から生成したデジタル署名データを格納する。




本人認証サービス「QRMe（仮称）」イメージ

# QRコードのセキュリティ

神戸大学

## 身分証明書に利用できるQRコードの開発

| | |
|---|---|
| 背景 | 身分証明書に用いられるICカードはコストがかかる |
| 目的 | QRコード化した身分証明書顔写真による本人認証システムの開発 |
| 成果 | idQRコードの開発 |

- スマホアプリで認証可能
- 鮮明かつ大きな写真と一体化
- QRコードの上位互換
- デジタル署名を施し、不正を防ぐ

神戸大学 森井昌克



# QRコードのセキュリティ

神戸大学

Fake QRコード

QRコードにおける誤り訂正符号の復号誤り特性と埋め草コードの仕様、ならびにQRコード自体の雑音性を利用


QRコードにセキュリティー上の弱点 不正サイトに誘導も

2018年6月23日 18時01分

A Construction of Fake QR Codes Based on Error-Correcting Codes

CANDAR 2018 : The Sixth International Symposium on Computing and Networking (Nov.28-30, 2018)

Fake QRコードの脅威

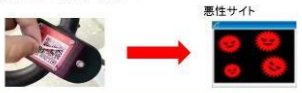
研究背景 3

QRコードを偽装した詐欺が増加している

偽装方法

・既存のQRコードの上に，悪性サイトに誘導するQRコードを貼り付ける．

→ 利用者はデコーダ無しに内容を把握できないため，偽装されていても気づかない．




しかし，このような偽装方法では必ず悪性サイトに誘導されるので特定されやすい．

特定されにくい偽装QRコードは存在するのか．．．？

偽装QRコードの危険性 5


復号誤り 11

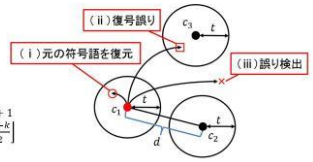
符号語 $c_1$ を格納したQRコードの読み取り時にノイズが発生し，．．．

（ⅰ）誤りを含んだシンボルが $t$ 個以下の場合
➡ 誤りを訂正し，元の符号語 $c_1$ を復元

（ⅱ）誤りを含んだシンボルが t 個より多く，他の復号領域内に入った場合
➡ 本来訂正されるべきではないシンボルが訂正され，$c_3$ を得る．（復号誤り）

（ⅲ）それ以外
➡ 誤り検出

RS符号 $(n, k, d)$
符号長：$n$
情報ブロックの容量：$k$
最小距離：$d = n - k + 1$
誤り訂正能力：$t = \left\lfloor \frac{n-k}{2} \right\rfloor$




偽装QRコード（デモ用） 26

# 符号理論とQRコードの脆弱性

**Fake QRコード**

**QRコードにおける誤り訂正符号の復号誤り特性と埋め草コードの仕様，ならびにQRコード自体の雑音性を利用**

誤り訂正符号 8

- データに冗長性を持たせることで誤りを訂正を可能とする技術

イメージ：こうべ→こうべ こうべ

（受信語）こ×べ こう× こうべ→こうべ

GF($2^8$)上の$(n, k)$ Reed-Solomon（RS）符号

符号長 $n$ シンボル

1シンボルは8ビット（01001100）

誤りはシンボルでカウント

（ⅰ）誤りが $t = \lfloor (n-k)/2 \rfloor$ シンボル以下の場合は誤りを訂正し，符号語 $c_1$ に復号
（ⅱ）誤りが $t = \lfloor (n-k)/2 \rfloor$ シンボルより多く，別の符号語の復号領域に入った場合，その符号語に復号（誤訂正）
（ⅲ）それ以外は誤り検出


QRコードにセキュリティー上の弱点 不正サイトに誘導も

2018年6月23日 18時01分

A Construction of Fake QR Codes Based on Error-Correcting Codes

CANDAR 2018 : The Sixth International Symposium on Computing and Networking (Nov.28-30, 2018)

—QR codes are used for various applications, such as eb pages and to make a settlement. Although users can cognize the existence of the QR codes, they need to use QR code decoder for reading the stored information s. A malicious one creates a fake QR code by making this feature and guides users to a malicious web page reless operation by the users. However, because fake always guided to a malicious site, the users detect the ode by looking it at attentively and take measures at lage. In this paper, we propose a construction method t codes which are hard to detect by a characteristic of correcting codes. Through evaluation experiments, we risk of the fake QR codes and call attention to this

rms—QR ruction

R code

Fake QRコードの脅威

32

のパラメータが決まる．

ル

誤り訂正ブロック

終端パターン

埋め草コード語

コードの最大容量に満たない場合に語として埋め込まれる．

に変更可能

神戸大学

## QRコードのユーザビリティの向上 1

QRコードの特徴
- 簡単に発行・配布ができる
- スマートフォンのカメラで撮影してすぐに読み取りが可能
- QRコード1つにつき，1つの情報にしかアクセスできない

QRコード1つで複数の情報に誘導出来たら？
- 利用者によって求める情報が異なるときに便利


神戸大学

## 2つの情報を出力するQRコード 2

- Two layer QR code[1]
  Top layerとBottom layerの二層を空間を開けて配置する

左右の撮影で出力情報を変える

利用アプリにより出力情報を変える


[1] T. Yuan et al., "Two-Layer QR Codes," in IEEE Transactions on Image Processing, vol. 28, no. 9, pp. 4413–4428, Sept. 2019, doi: 10.1109/TIP.2019.2908490.
[2] I. Tkachenko et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 571–583, March 2016, doi: 10.1109/TIFS.2015.2506546.

**ホログラムQRコード：複数の情報をもつQRコード，ある時はA,あるときはB**

神戸大学

## ホログラムQRコードの開発 3

複数の情報の出力を可能とするホログラムQRコードを提案

| QRコード | 印刷可能か | 専用のデコーダ | 複数の情報の出力方法 |
|---|---|---|---|
| Two layer QR Code | 不可能 | 不要 | 撮影角度の変更 |
| Two Level QR Code | 可能 | 必要 | 使用アプリの変更 |
| ホログラムQRコード[提案] | 可能 | 不要 | 撮影角度の変更 |

印刷可能
平面上に表現する必要がある
- QRコードの撮影は傾き補正されるため角度によって大きな視差を生み出すのは難しい

専用のデコーダーが不要
- QRコードの仕様の範囲内でQRコードを作成する必要がある
(Textured Patternのような特殊なものは使えない)

神戸大学

## ホログラムQRコードの開発 4

偽装QRコード[*]
印刷可能で専用のデコーダが不要
数ビットのノイズで出力情報が確率的に変化する(**誤訂正**)

＋

デコーダアプリの画像処理
左右から急角度で撮影すると完璧には補正しきれない

ホログラムQRコードの概要
- ✓ 左右から撮影することで数モジュールだけ視差を生み出す
- ✓ 数モジュールの視差により誤訂正を起こし別の情報を出力

**左右から撮影すると異なる情報を出力する印刷可能なQRコード**
Two layer QR Codeのようなハードウェア的制約がない

**評価実験により既存のデコーダで複数の情報を出力できることを確認**

[*]瀧田慎，大熊浩也，森井昌克，"二つの情報を出力するQRコードの構成
ー悪性サイトに誘導するQRコードの存在とその脅威ー"，電子情報通信学会論文誌，2020

**たとえば、右からカメラを向けるとA，左からカメラを向けるとB，上からカメラを向けるとC**

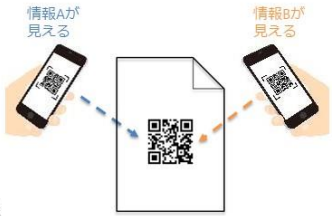
67

神戸大学

## 撮影角度で出力情報が変わるQRコード 5

ホログラムQRコード
- 通常のデコーダで利用可能で，ポスター等に印刷可能なQRコード
- 左右から撮影したときに，それぞれ別の情報が出力される

- 偽装QRコード[*]の手法を応用して複数の情報を出力
  - 誤り訂正符号の性質を応用
  - 数ビットだけ左右で見える符号語(データ)が変わればよい
- QRコードスキャナーの画像処理のときに起こる座標のずれを利用して撮影角度による差を生み出す




- ✓ **QRコードの左右から撮影することで数モジュールだけ視差を生み出す**
- ✓ **誤り訂正符号の訂正能力により全く別の情報を出力させる**

[*]瀧田慎，大熊浩也，森井昌克，"二つの情報を出力するQRコードの構成
ー悪性サイトに誘導するQRコードの存在とその脅威ー"，電子情報通信学会論文誌，2020

68

## まとめ

神戸大学

「(古典的？)符号理論とその応用」

- 最良線形符号構成問題
- QRコード

**符号理論のサイバー社会への応用**