Human-Computer Cryptography: An Attempt

Tsutomu Matsumoto
Division of Electrical and Computer Engineering
Yokohama National University
156 Tokiwadai, Hodogaya, Yokohama 240, Japan
email: tsutomu@mlab.dnj.ynu.ac.jp facsimile: +81-45-338-1157

Abstract

Can you securely prove your identity to a host computer by using no dedicated software at your terminal and no dedicated token at your hands ? Conventional password checking schemes don't need such a software and hardware but have a disadvantage that an attacker who has correctly observed an input password by peeping or wiretapping can perfectly impersonate the corresponding user. Conventional dynamic (one-time) password schemes or zero-knowledge identification schemes can be securely implemented but require special software or hardware or memorandums. This paper develops human-friendly identification schemes such that a human prover knowing a secret key in her or his brain is asked a visual question by a machine verifier, who then checks if an answer sent from the prover matches the question with respect to the key. The novelty of these schemes lies in their ways of displaying questions. This paper also examines an application of the human identification schemes to human-computer cryptographic communication protocols.

Keywords: authentication, human-computer interaction, passwords, information security.

1 Introduction

This paper examines some sort of cryptographic communication between users (human beings) and computers (machines). Compared to computer-computer cryptography very small number of papers have been written on human-computer cryptography. This subject is emerging and not systematically developed but increases its importance. Thus the present author would like to challenge it and provide various imagination on the topic.

Human identification is a necessary item for access control mechanisms [1][2]. Figures 1 and 2 show typical threats to human identification schemes and illustrate the above mentioned difference between widely-used conventional password schemes and the interactive human identification schemes firstly examined in [3]. The same reference contains a brief description on the feature and significance of the latter class by contrast with schemes such as [1][4] requiring auxiliary devices or [5][6] software for human provers.

CCS '96, New Delhi, India
© 1996 ACM 0-89791-829-0/96/03..$3.50

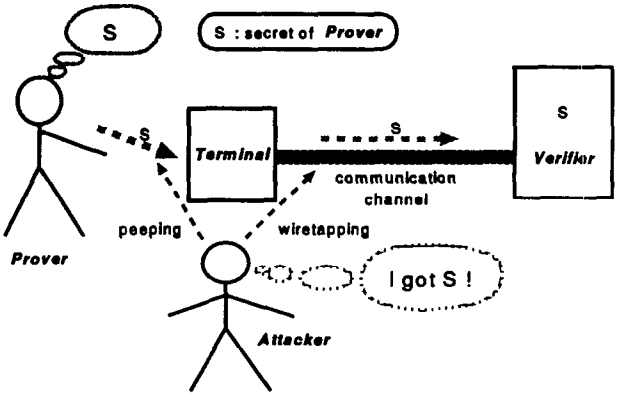

Figure 1: Conventional Password Schemes

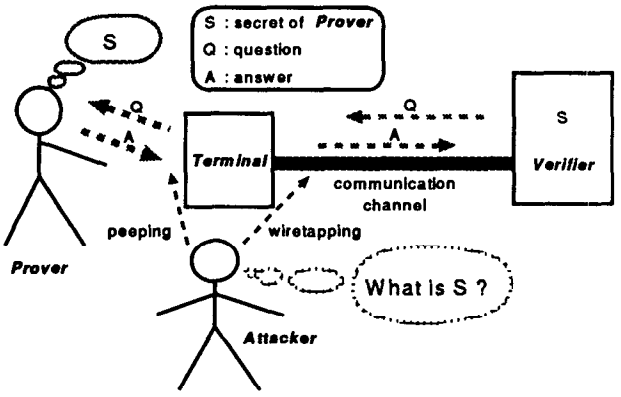

Figure 2: Interactive Human Identification Schemes

The resistance of such schemes can be evaluated by the probability $P(n)$ of which an attacker can correctly answer a given question after obtaining n (≥ 0) pairs of questions and correct answers. An interactive identification scheme proposed in [3] and its variant [7] are ingeniously designed, but their resistance has been developed only by heuristic arguments [3][7] and no exact probabilities $P(n)$ are known for $n \geq 1$.

This paper presents human-friendly cryptographic human identification schemes with novel ideas of displaying questions. Linear algebra supports theoretical basis of these schemes and clarifies their rigorous profiles of $P(n)$.

This paper also shows a key idea to convert the human identification schemes to human-computer cryptographic communication protocols.

2 Basic Schemes

2.1 Basic Identification Protocol

Let s be a prime power, u and v positive integers. Also let $\mathbf{F}_s$ and $\mathbf{F}_s{}^v$ respectively represent the finite field of order s and the vector space $\{[x_1, \cdots, x_v] \mid x_1, \cdots, x_v \in \mathbf{F}_s\}$ consisting of all v-dimensional row vectors over $\mathbf{F}_s$.

Now we define a basic protocol to be conducted by two players: *Prover* $\widetilde{\mathbf{P}}$ who claims that $\widetilde{\mathbf{P}}$ is a person $\mathbf{P}$; *Verifier* $\widetilde{\mathbf{V}}$ who acts as a machine $\mathbf{V}$ and communicates with $\widetilde{\mathbf{P}}$.

Protocol 0.
Preparation Phase

0. *Key Sharing* $\mathbf{P}$ and $\mathbf{V}$ agree on a *key* (a u-tuple of column vectors) $K_{\mathbf{P}} = [\mathbf{k}_1, \cdots, \mathbf{k}_u]$ where $\mathbf{k}_1{}^{\mathrm{T}}, \cdots, \mathbf{k}_u{}^{\mathrm{T}}$ are uniformly chosen at random from $\mathbf{F}_s{}^v$, and keep the key secret. Symbol $\mathbf{k}_i^{\mathrm{T}}$ denotes the transposition of vector $\mathbf{k}_i$.

Interaction Phase

1. *Request* $\widetilde{\mathbf{P}}$ requests $\widetilde{\mathbf{V}}$ to decide "$\widetilde{\mathbf{P}} = \mathbf{P}$".

Serially or concurrently for $i = 1, \cdots, u$, entities $\widetilde{\mathbf{P}}$ and $\widetilde{\mathbf{V}}$ execute steps 2 and 3.

2. *Challenge* $\widetilde{\mathbf{V}}$ generates a *question* $\mathbf{q}_i \in \mathbf{F}_s{}^v - \{\mathbf{0}\}$, and sends it to $\widetilde{\mathbf{P}}$. When $\widetilde{\mathbf{V}} = \mathbf{V}$, we assume that $\mathbf{q}_i$ is selected randomly and uniformly from $\mathbf{F}_s{}^v - \{\mathbf{0}\}$.

3. *Response* $\widetilde{\mathbf{P}}$ sends an *answer* $a_i \in \mathbf{F}_s$ to $\widetilde{\mathbf{V}}$. When $\widetilde{\mathbf{P}} = \mathbf{P}$, we assume that

$$a_i = \mathbf{q}_i \mathbf{k}_i \in \mathbf{F}_s \tag{1}$$

4. *Acknowledgment* If $\widetilde{\mathbf{V}} = \mathbf{V}$, then using $K_{\mathbf{P}}$, *Verifier* $\widetilde{\mathbf{V}}$ checks whether equation (1) holds or not for each $i = 1, \cdots, u$. $\widetilde{\mathbf{V}}$ judges "$\widetilde{\mathbf{P}} = \mathbf{P}$" if and only if all of them hold. Then $\widetilde{\mathbf{V}}$ informs $\widetilde{\mathbf{P}}$ whether $\widetilde{\mathbf{V}}$ has judged "$\widetilde{\mathbf{P}} = \mathbf{P}$" or not.

Here we explain meaning of parameters. Parameter s means the varieties of each answer, parameter v means the dimension of vectors, and parameter u means the number of questions, or equivalently, the number of answers. We can observe the following features.

Proposition 1. For Protocol 0, the key, answers, and questions are respectively described by $u \cdot v \cdot \log_2 s$ [bit], $u \cdot \log_2 s$ [bit], and

$$D_0(s, v, u) = u \cdot v \cdot \log_2 s \quad \text{[bit]} \tag{2}$$

2.2 Application to Human-Computer Cryptographic Communication

On the basic human identification protocol, if we interpret $[\mathbf{a}_1, \cdots, \mathbf{a}_u]$ as a plaintext and $[\mathbf{q}_1, \cdots, \mathbf{q}_u]$ as the corresponding ciphertext, then it is obvious that the basic protocol can be applied as a tool for cryptographic communication from a computer to a human user. Introducing redundancy to plaintext $[\mathbf{a}_1, \cdots, \mathbf{a}_u]$ is effective to gain higher authenticity. If we replace the basic protocol by applied protocols to be described in the following sections, then we can derive methods of cryptographic communication that are easy for human users to perform deciphering mentally.

We can utilize the availability of such cryptographic communication channels with confidentiality and authenticity from a computer sender to a human receiver to construct cryptographic channels from a human sender to a computer receiver by the following general method.

1) A computer selects a one-time session key to a human user by a cryptographic channel from the computer to the human user. A session key is a message such that "Please use data 3149 for sending message 0 and data 5872 for message 1."

2) The human user mentally deciphers the ciphertext from the computer to get the one-time session key in the user's brain. With respect to the session key the user mentally constructs a ciphertext corresponding to a plaintext that the user really wants to communicate. Then the user sends the ciphertext to the computer.

3) The computer deciphers the received ciphertext to obtain a plaintext from the human user. The computer sends back the obtained plaintext through the cryptographic channel from the computer to the human user.

4) The human user mentally deciphers the ciphertext from the computer and verifies whether the recovered plaintext coincides with that the user sent in step 2).

3 Security of Basic Protocol

3.1 Taxonomy of Attacks

An *attack* is an action by an entity $\mathbf{A}$, *attacker*, who is different from $\mathbf{P}$ and $\mathbf{V}$, to aim at letting $\mathbf{V}$ decide "$\mathbf{A} = \mathbf{P}$". An attack succeeds if and only if $\mathbf{V}$ judges "$\mathbf{A} = \mathbf{P}$". We can distinguish three types depending on the knowledge the attacker can utilize.

Blind Attack An attack by $\mathbf{A}$ who has been given no pair of a question to $\mathbf{P}$ and the corresponding answer from $\mathbf{P}$. Let $\mathrm{P}(s, v, u; 0)$ denote the least upper bound (LUB) of the success probability of any blind attack to Protocol 0.

Known Q & A Attack An attack by $\mathbf{A}$ who has observed n (≥ 1) pairs of given questions and corresponding answers. Let $\mathrm{P}(s, v, u; n)$ denote the LUB of the success probability of any known Q & A attack to Protocol 0.

Chosen Q & A Attack An attack by $\mathbf{A}$ who has acted as $\widetilde{\mathbf{V}} = \mathbf{A}$ and observed n (≥ 1) pairs of chosen questions and corresponding answers. Let $\widehat{\mathrm{P}}(s, v, u; n)$ denote the LUB of the success probability of any chosen Q & A attack to Protocol 0.

3.2 Success Probabilities

We can prove the following profiles. See Figures 3, 4, and 5.

Proposition 2. We have

$$\mathrm{P}(s, v, u; 0) = \left(\frac{1}{s}\right)^u \tag{3}$$

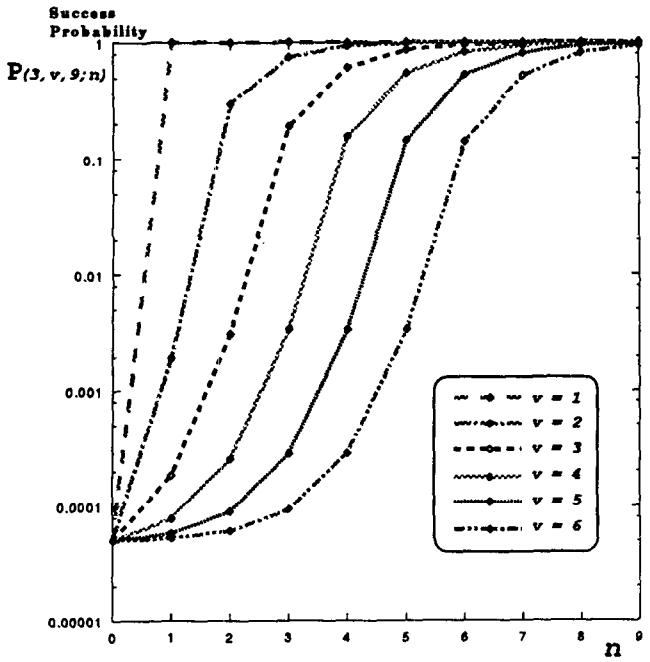

Figure 3: Examples of $\mathrm{P}(s,v,u;n)$

- s: varieties of each answer
- v: dimension of vectors
- u: number of questions, or answers
- n: number of observations

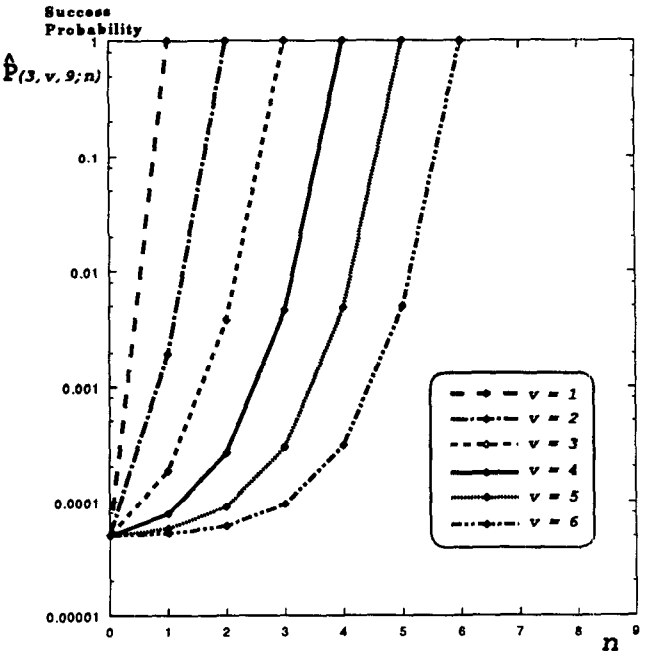

Figure 4: Examples of $\widehat{\mathrm{P}}(s,v,u;n)$

- s: varieties of each answer
- v: dimension of vectors
- u: number of questions, or answers
- n: number of observations

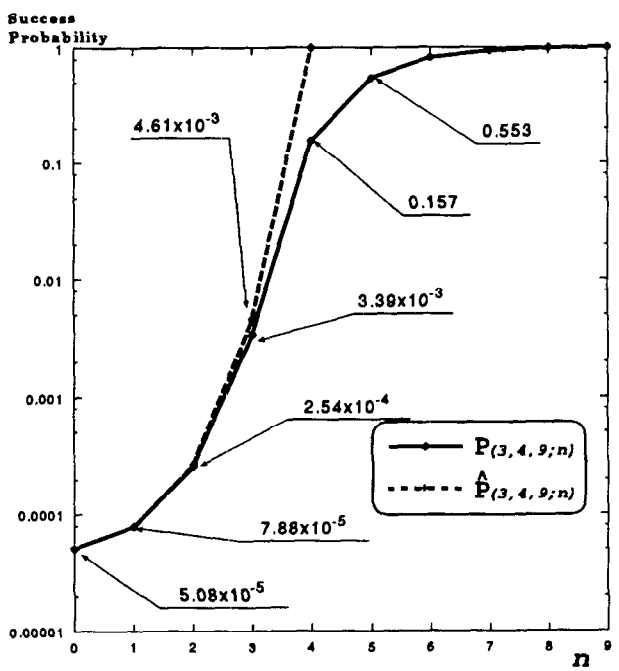

Figure 5: $\mathrm{P}(s,v,u;n)$ vs. $\widehat{\mathrm{P}}(s,v,u;n)$

- s: varieties of each answer
- v: dimension of vectors
- u: number of questions, or answers
- n: number of observations

Proposition 3. For $n \geq 1$, we have

$$\begin{aligned} & \mathrm{P}(s,v,u;n) \qquad (4) \\ = & \left(\frac{1}{s} + (1-\frac{1}{s}) \cdot \frac{1}{s^v - 1} \cdot \sum_{l=1}^{v} (s^l - 1) \cdot \mathrm{R}(s,v;n,l)\right)^u \end{aligned}$$

where for $0 \leq l \leq v$ the quantity $\mathrm{R}(s,v;n,l)$ is the probability that the vector space spanned by n vectors selected uniformly and randomly from $\mathbf{F}_s^v - \{\mathbf{0}\}$ has dimension of l. See Figure 3.

Proposition 4. For $0 \leq n \leq v$ we have

$$\widehat{\mathrm{P}}(s,v,u;n) = \left(\frac{1}{s} + (1-\frac{1}{s}) \cdot \frac{s^n - 1}{s^v - 1}\right)^u \qquad (5)$$

See Figure 4.

Proposition 5. For $0 \leq n \leq v$ we have

$$\begin{aligned} & \left(\frac{1}{s} + (1-\frac{1}{s}) \cdot \frac{s^n - 1}{s^v - 1} \cdot \prod_{m=0}^{n-1} (1 - \frac{s^m - 1}{s^v - 1})\right)^u \\ \leq \; & \mathrm{P}(s,v,u;n) \qquad (6) \\ \leq \; & \widehat{\mathrm{P}}(s,v,u;n). \end{aligned}$$

See Figures 3, 4, and 5.

3.3 Proof of Proposition 2

A blind attack selects answer a'_i independently from given question $\mathbf{q}_i$ and secret key $\mathbf{k}_i$. Therefore

$$\Pr(a'_i = \mathbf{q}_i\mathbf{k}_i) = \sum_{e\in\mathbf{F}_s} \Pr(a' = e)\Pr(\mathbf{q}_i\mathbf{k}_i = e) \quad (7)$$

Since $\mathbf{q}_i$ is selected uniformly at random from $\mathbf{F}_s^v - \{\mathbf{0}\}$ and $\mathbf{k}_i^{\mathrm{T}}$ from $\mathbf{F}_s^v$, we have for any given $e \in \mathbf{F}_s$

$$\Pr(\mathbf{q}_i\mathbf{k}_i = e) = \frac{1}{s} \quad (8)$$

which implies that

$$\Pr(a'_i = \mathbf{q}_i\mathbf{k}_i) = \sum_{e\in\mathbf{F}_s} \Pr(a' = e)\frac{1}{s} = \frac{1}{s} \quad (9)$$

Thus we have

$$\mathrm{P}(s, v, u; 0) = \prod_{i=1}^{u} \Pr(a'_i = \mathbf{q}_i\mathbf{k}_i) = \left(\frac{1}{s}\right)^u \quad (10)$$

which proves Proposition 2.

3.4 Proof of Proposition 3

Since it is clear that

$$\mathrm{P}(s, v, u; n) = \mathrm{P}(s, v, 1; n)^u \quad (11)$$

we examine the case $u = 1$.

Let the number of observation be $n \geq 1$. Let $\mathbf{q}^j$ and a^j respectively denote the question and answer that attacker **A** gets at the j th observation. These are linked by key $\mathbf{k}$ not known to attacker **A**:

$$a^j = \mathbf{q}^j\mathbf{k} \quad j = 1, \cdots, n \quad (12)$$

Assume that $\mathbf{q}^1, \cdots, \mathbf{q}^n$ are selected by **V**. That is, we assume that these are chosen uniformly at random from $\mathbf{F}_s^v - \{\mathbf{0}\}$. Let

$$W_n = < \mathbf{q}^1, \cdots, \mathbf{q}^n > \quad (13)$$

denote the subspace of $\mathbf{F}_s^v$ spanned by $\mathbf{q}^1, \cdots, \mathbf{q}^n$.

For newly given question $\mathbf{q} \in \mathbf{F}_s^v$ of what probability can attacker **A** generate answer $a \in \mathbf{F}_s$ satisfying

$$a = \mathbf{q}\mathbf{k} \quad (14)$$

is our concern.

Let us consider the following attack.

Attack 1

case 1. If $\mathbf{q} \in W_n$, since there exists $\alpha^j \in \mathbf{F}_s$ such that $\mathbf{q} = \sum_{j=1}^n \alpha^j\mathbf{q}^j$, attacker **A** answers $a = \sum_{j=1}^n \alpha^j a^j$.

case 2. If $\mathbf{q} \notin W_n$ then attacker **A** conducts a blind attack.

This attack fully utilizes linear-algebraic knowledge used for constructing the basic protocol. In this sense it is the strongest known Q & A attack to Protocol 0.

Thus let $\mathrm{P}(s, v, 1; n)$ denote the success probability of Attack 1. First we have

$$\begin{aligned}
&\mathrm{P}(s, v, 1; n) \\
&= \Pr(a = \mathbf{q}\mathbf{k}) \\
&= \Pr(a = \mathbf{q}\mathbf{k}, \mathbf{q} \in W_n) + \Pr(a = \mathbf{q}\mathbf{k}, \mathbf{q} \notin W_n) \\
&= \Pr(a = \mathbf{q}\mathbf{k} \mid \mathbf{q} \in W_n) \cdot \Pr(\mathbf{q} \in W_n) \\
&\quad + \Pr(a = \mathbf{q}\mathbf{k} \mid \mathbf{q} \notin W_n) \cdot \Pr(\mathbf{q} \notin W_n) \\
&= 1 \cdot \Pr(\mathbf{q} \in W_n) + \frac{1}{s} \cdot \Pr(\mathbf{q} \notin W_n) \\
&= \Pr(\mathbf{q} \in W_n) + \frac{1}{s} \cdot [1 - \Pr(\mathbf{q} \in W_n)] \\
&= \frac{1}{s} + (1 - \frac{1}{s}) \cdot \Pr(\mathbf{q} \in W_n) \quad (15)
\end{aligned}$$

On the other hand, by

$$\begin{aligned}
\Pr(\mathbf{q} \in W_n) &= \sum_{l=0}^{v} \Pr(\mathbf{q} \in W_n \mid \dim(W_n) = l) \\
&\quad \cdot \Pr(\dim(W_n) = l) \quad (16)
\end{aligned}$$

and by

$$\begin{aligned}
\Pr(\mathbf{q} \in W_n \mid \dim(W_n) = l) &= \frac{\#\mathbf{F}_s^l - \{\mathbf{0}\}}{\#\mathbf{F}_s^v - \{\mathbf{0}\}} \\
&= \frac{s^l - 1}{s^v - 1} \quad (17)
\end{aligned}$$

we have

$$\begin{aligned}
&\Pr(\mathbf{q} \in W_n) \\
&= \frac{1}{s^v - 1} \sum_{l=1}^{v} (s^l - 1) \cdot \Pr(\dim(W_n) = l) \quad (18)
\end{aligned}$$

Thus we have Proposition 3.

3.5 How to Evaluate $\mathrm{R}(s, v; n, l)$

Function $\mathrm{R}(s, v; n, l)$ has been defined as the probability that the vector space spanned by n vectors selected uniformly and randomly from $\mathbf{F}_s^v - \{\mathbf{0}\}$ has dimension of l. Thus immediately we have

Proposition 6. If $l = 0$ or $l > n$ or $l > v$ then $\mathrm{R}(s, v; n, l) = 0$.

Let D denote the region such that

$$D = \{(n, l) \mid n \geq 1,\ 1 \leq l \leq v,\ l \leq n\} \quad (19)$$

Proposition 7. For $(n, l) \in D$, we have

$$\begin{aligned}
&\mathrm{R}(s, v; n, l) \\
&= (1 - \frac{s^{l-1} - 1}{s^v - 1}) \cdot \mathrm{R}(s, v; n - 1, l - 1) \quad (20) \\
&\quad + \frac{s^l - 1}{s^v - 1} \cdot \mathrm{R}(s, v; n - 1, l)
\end{aligned}$$

In particular, for $(l, l) \in D$ we have,

$$\mathrm{R}(s, v; l, l) = \prod_{m=0}^{l-1} (1 - \frac{s^m - 1}{s^v - 1}) \quad (21)$$

Proof) Apparently we have

$$\begin{aligned} & \mathrm{R}(s,v;n,l) \\ = \; & \Pr(\dim(W_n)=l, \dim(W_{n-1})=l-1) \\ & +\Pr(\dim(W_n)=l, \dim(W_{n-1})=l) \\ = \; & \Pr(\dim(W_n)=l \,|\, \dim(W_{n-1})=l-1) \\ & \cdot \mathrm{R}(s,v;n-1,l-1) \\ & +\Pr(\dim(W_n)=l \,|\, \dim(W_{n-1})=l) \\ & \cdot \mathrm{R}(s,v;n-1,l) \end{aligned} \tag{22}$$

where

$$\begin{aligned} & \Pr(\dim(W_n)=l \,|\, \dim(W_{n-1})=l-1) \\ = \; & \Pr(\mathbf{q}^n \notin W_{n-1} \,|\, \dim(W_{n-1})=l-1) \\ = \; & 1-\Pr(\mathbf{q}^n \in W_{n-1} \,|\, \dim(W_{n-1})=l-1) \\ = \; & 1-\frac{s^{l-1}-1}{s^v-1}, \end{aligned} \tag{23}$$

$$\begin{aligned} & \Pr(\dim(W_n)=l \,|\, \dim(W_{n-1})=l) \\ = \; & \Pr(\mathbf{q}^n \in W_{n-1} \,|\, \dim(W_{n-1})=l) \\ = \; & \frac{s^l-1}{s^v-1} \end{aligned} \tag{24}$$

which implies the first half of Proposition 7. For the second half, by

$$\begin{aligned} & \mathrm{R}(s,v;l,l) \\ = \; & (1-\frac{s^{l-1}-1}{s^v-1}) \cdot \mathrm{R}(s,v;l-1,l-1) \\ & +\frac{s^l-1}{s^v-1} \cdot \mathrm{R}(s,v;l-1,l) \end{aligned} \tag{25}$$

and by $\mathrm{R}(s,v;l-1,l)=0$, we have

$$\mathrm{R}(s,v;l,l) = (1-\frac{s^{l-1}-1}{s^v-1}) \cdot \mathrm{R}(s,v;l-1,l-1) \tag{26}$$

This shows that for $l=1,\cdots,v$,

$$\mathrm{R}(s,v;l,l) = \prod_{m=0}^{l-1}(1-\frac{s^m-1}{s^v-1}) \tag{27}$$

By Propositions 6 and 7 we can calculate value $\mathrm{R}(s,v;n,l)$ for every element in region D. Therefore we can evaluate $\mathrm{P}(s,v,u;n)$ using Proposition 3.

3.6 Proof of Propositions 4 and 5

For $n \le v$, if chosen sequence of questions

$$\mathbf{q}^1, \quad \cdots, \quad \mathbf{q}^n \tag{28}$$

are linearly independent then for given question $\mathbf{q}$ we have

$$\begin{aligned} \Pr(\mathbf{q} \in W_n) &= \sum_{l=1}^{v} \frac{s^l-1}{s^v-1} \cdot \Pr(\dim(W_n)=l) \\ &= \frac{s^n-1}{s^v-1} \end{aligned} \tag{29}$$

Thus we have Proposition 4 assuming that for the case $n=0$ quantity $\widehat{\mathrm{P}}(s,v,u;0)$ coincides with $\mathrm{P}(s,v,u;0)$.

Proposition 5 can be verified by Propositions 3, 4, and 7.

4 Visual Identification Protocols

Computing the scalar multiplication in equation (1) seems hard for ordinary persons. To avoid this difficulty we direct our attention to a characteristic of human vision. Assume a *screen* where a lot of points lie at determined locations and that each point is labeled by a symbol selected from a finite set. Assume a *keyboard* where each symbol in the set can be input. We use the fact that ordinary persons can quickly focus on a predetermined point and input the corresponding label into the keyboard.

4.1 Protocol 1

Let Ω be a set of s^v elements. In Protocol 1, each question $\mathbf{q}_i$ in Protocol 0 is assigned a question-expression,

$$Q_i = \{(\omega, q_i(\omega)) \,|\, \omega \in \Omega\}, \quad q_i(\omega) = \mathbf{q}_i \cdot \psi_i(\omega)^{\mathrm{T}} \in \mathbf{F}_s \tag{30}$$

where ψ_i is a bijection from Ω onto $\mathbf{F}_s{}^v$. *Prover* remembers u-tuple $[k_1, k_2, \cdots, k_u]$ over Ω as a key. For each $i=1,\cdots,u$, *Prover* answers $q_i(k_i)$ to given question-expression Q_i. Note that $\psi_i(k_i)^{\mathrm{T}} = \mathbf{k}_i$ and $q_i(k_i) = a_i$. Protocol 1 has the following properties.

Proposition 8. The LUB of success probability of blind, known, and chosen Q & A attack to Protocol 1 is upper bounded by that of the corresponding attack to Protocol 0.

Proposition 9. In Protocol 1, the question-expressions are described by

$$D_1(s,v,u) = u \cdot s^v \cdot \log_2 s \quad [\text{bit}] \tag{31}$$

and the key and answers are respectively described by $u \cdot v \cdot \log_2 s$ [bit] and $u \cdot \log_2 s$ [bit].

Example 1. Matrix Scheme Figure 6 shows an example where $(s,v,u)=(3,3,9)$, $\mathbf{F}_s = \{0,1,2\}$, and

$$\Omega = \{*, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \cdots, \mathrm{W}, \mathrm{X}, \mathrm{Y}, \mathrm{Z}\} \tag{32}$$

This example displays $u=9$ question-expressions concurrently. Figures 7 and 8 depict implemented examples over the World Wide Web. Also see Figure 10 for the environment. Server writes question-expressions by HTML (Hypertext Markup Language) and provides them to Client where NCSA Mosaic is installed as a WWW browser. Note that there is no need to install any dedicated software to Client for the purpose of human identification.

Example 2: Map Scheme. Figure 9 depicts an example where $(s,v,u)=(3,4,9)$, $\mathbf{F}_s = \{1,2,3\}$, and Ω is the set of 81 sampled names of railway stations. The question-expression is the set of pairs of station names and figures (or colors) appearing in small circles put on the locations of the stations.

This example displays $u=9$ question-expressions serially. The route map helps *Prover* to remember a key and to quickly look for the location of a remembered station and recognize the figure. From this example we can see that such a relation among the elements of Ω can greatly reduce load of human provers.

A device for displaying question-expressions may be also used to input answers. A liquid crystal panel with touch-sensing function and a standard PC display linked with a mouse are the examples. When such a device is available we can implement the map scheme so that for each given question-expression let *Prover* input the answer by touching or clicking any one of the small circles showing the figure (or color) that is the answer.

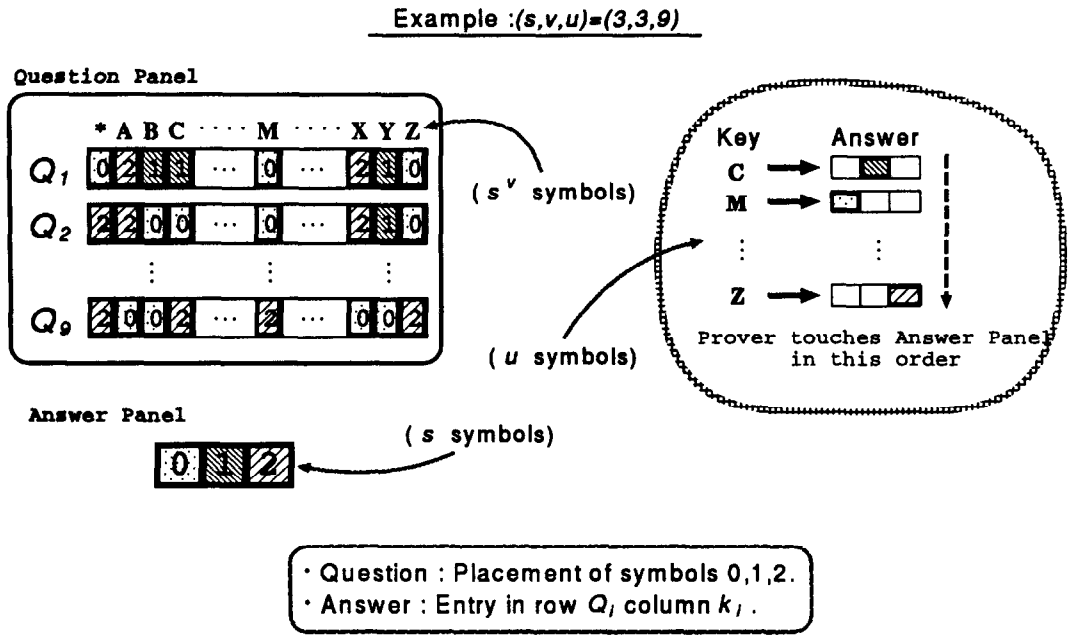

Figure 6: An Implementation of Protocol 1: Matrix Scheme ($(s, v, u) = (3, 3, 9)$)

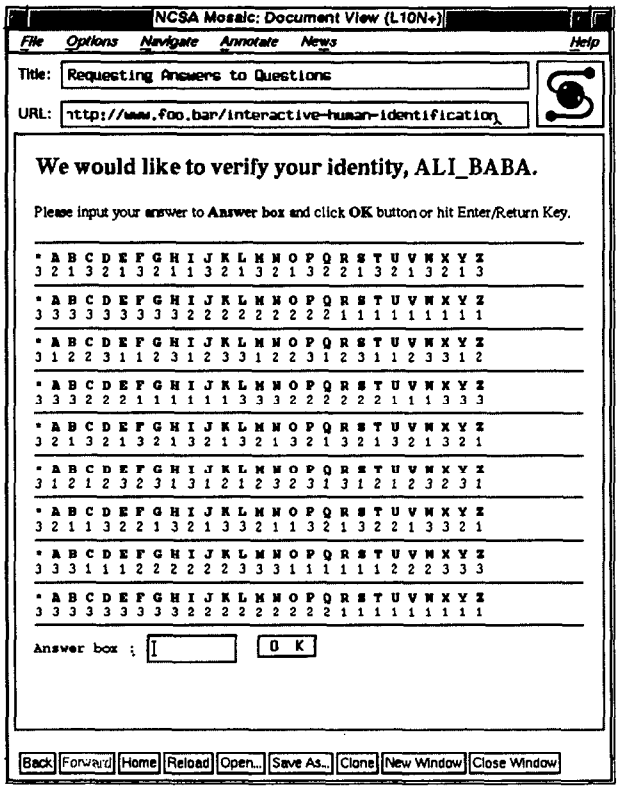

Figure 7: Demonstration on NCSA Mosaic 1

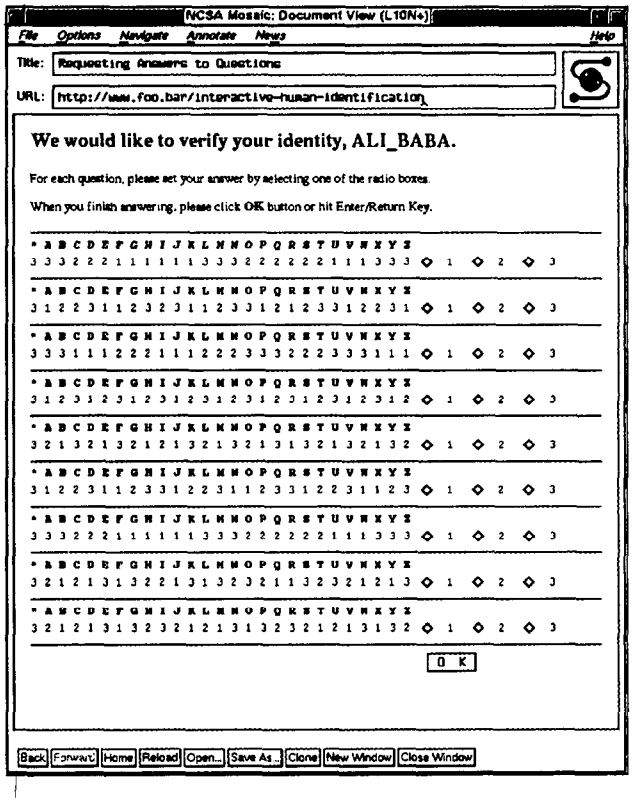

Figure 8: Demonstration on NCSA Mosaic 2

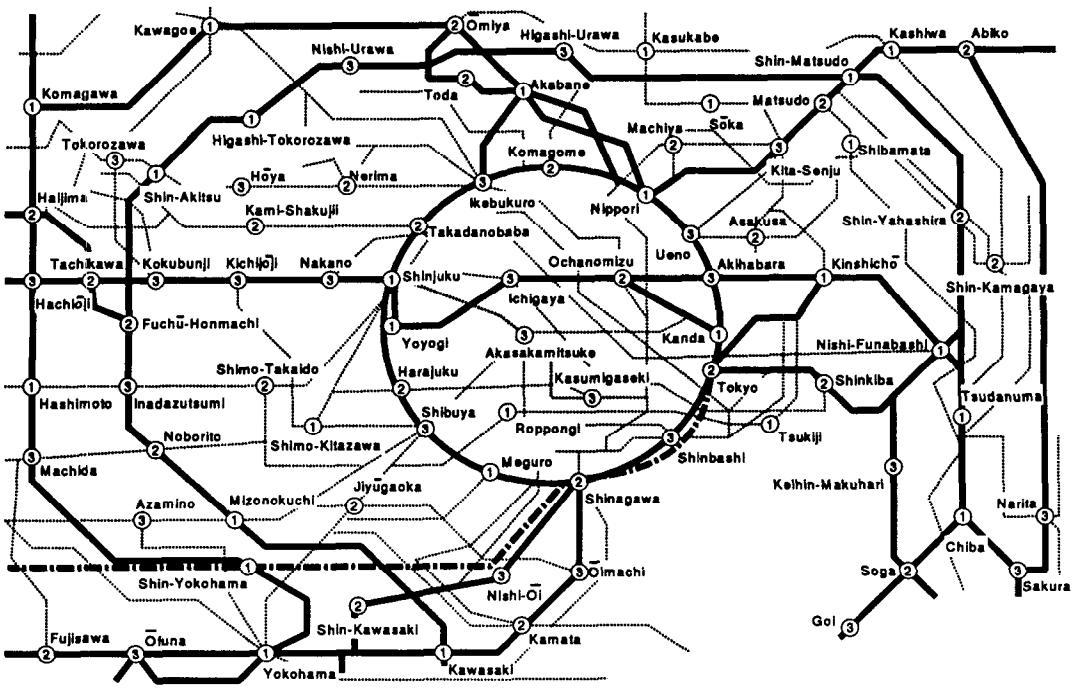

Figure 9: An Implementation of Protocol 1: Map Scheme ($(s, v, u) = (3, 4, 9)$)

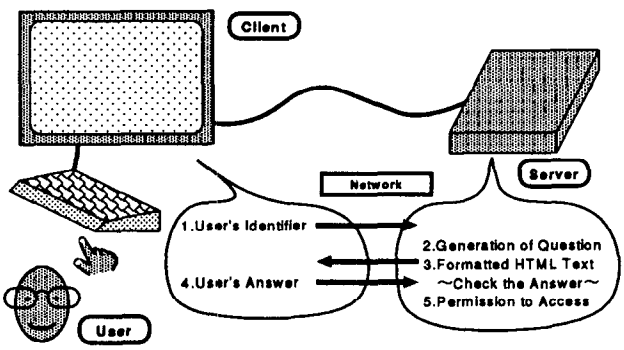

Figure 10: Environment

4.2 Protocol 2

Propositions 2, 3, 4 and 8 imply that to increase resistance against attacks we should make s, v, and u grow. Human memory capacity limits u. Capacity of a screen to display question-expressions or human visual ability of discriminating points limit s and v according to Proposition 9.

Now we point out a middle approach between Protocol 0 and Protocol 1 to reduce the amount of data for displaying a question-expression. Let m ($\leq v$) be a positive integer. Recall Protocol 0. We divide v into $v = \sum_{f=1}^{m} v_f, \quad v_f > 0$. Correspondingly for $i = 1, \cdots, u$, we divide $\mathbf{q}_i$ and $\mathbf{k}_i^{\mathrm{T}}$ as $\mathbf{q}_i = [\mathbf{q}_{i1}, \cdots, \mathbf{q}_{im}]$ and $\mathbf{k}_i^{\mathrm{T}} = [\mathbf{k}_{i1}^{\mathrm{T}}, \cdots, \mathbf{k}_{im}^{\mathrm{T}}]$ so that by letting $a_{if} = \mathbf{q}_{if}\mathbf{k}_{if} \in \mathbf{F}_s$ for $f = 1, \cdots, m$, we have $a_i = \sum_{f=1}^{m} a_{if}$.

Thus we can derive a scheme, called Protocol 2, that

1) for each $f = 1, \cdots, m$ *Verifier* challenges a sub-question-expression like in Protocol 1;

2) *Prover* makes in mind a sub-answer for each sub-question-expression;

3) *Prover* mentally sums up all of the sub-answers to have an answer;

4) then *Prover* inputs the answer to *Verifier*.

Protocol 2 has the following properties.

Proposition 10. The LUB of success probability of blind, known, and chosen Q & A attack to Protocol 2 is upper bounded by that of the corresponding attack to Protocol 0.

Proposition 11. In Protocol 2, the key, answers, and the question-expressions are respectively described by $u \cdot v \cdot \log_2 s$ [bit], $u \cdot \log_2 s$ [bit], and

$$D_2(s, v, u) = u \cdot (\sum_{f=1}^{m} s^{v_f}) \cdot \log_2 s \quad \text{[bit]} \qquad (33)$$

Prover should make addition(s) over $\mathbf{F}_s$ but the value $D_2(s, v, u)$ can be far smaller than $D_1(s, v, u)$. See Table 1.

Example 3: Game Scheme. Reducing load of *Prover* we translate the $\mathbf{F}_s$ addition into some binary operation that can be readily done by ordinary persons. Here we utilize the *Janken* game of 'paper', 'stone' and 'scissors'. The rule of the game is that 'paper' wins 'stone', 'stone' wins 'scissors', and 'scissors' wins 'paper'. Let $s = 3$ and $m = 2$. See Figure 11. This example is designed so that the verifier displays $u = 9$ question-expressions serially.

In the figure, the left and right screen respectively displays a question-expression of $(s, v) = (3, 3)$. In the left screen, element 0, 1, and 2 is respectively mapped to hand 'stone', 'scissors', and 'paper'. In the right, element 0, 1, and 2 is respectively mapped to 'stone', 'paper', and 'scissors'.

Table 1: Complexity of Displaying Question-Expression ($s = 3$)

Protocol i		$D_i(s,v,u)/u\log_2 s$	$v=1$	2	3	4	5	6	7	8	9
Protocol 0		v	1	2	3	4	5	6	7	8	9
Protocol 1		s^v	3	9	27	81	243	729	2187	6561	19683
Protocol 2	$m=2$	$2s^{v/2}$	-	6	-	18	-	54	-	162	-
	$m=3$	$3s^{v/3}$	-	-	9	-	-	27	-	-	81

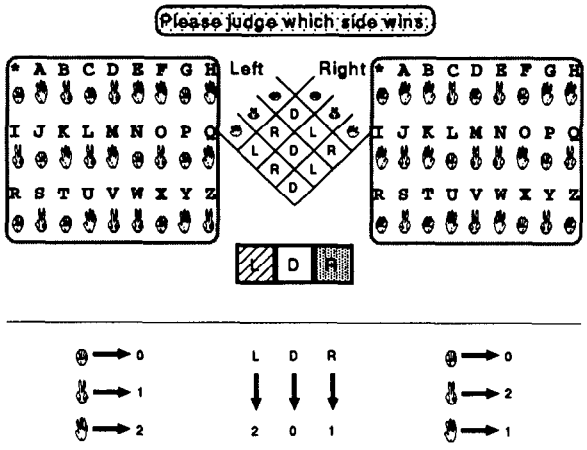

Figure 11: An Implementation of Protocol 2: Two-Player Game Scheme ($(s,v,u) = (3,6,9)$)

Prover selects a hand from the left screen with respect to a key and one from the right screen in a similar way. *Prover* mentally matches both the hands and answers the winner. Namely, if the left (the right, resp.) wins the answer is to click button L (button R, resp.) and if the game is drawn it is to click button D. Note that the rule of the game is exactly the same as the $\mathbf{F}_3$ addition if we interpret L, D, and R respectively as 2, 0, and 1.

We can implement the case where $m > 2$ by a similar way: We translate symbol L (D, R, resp.) into hand 'paper' ('stone', 'scissors', resp.) and conduct an elimination tournament by matching one of L, D, and R with a hand selected from another question-expression newly displayed in the right screen.

When $m = 3$ we can implement the case by another way: Addition of three items can be translated in the scenario of three-player Janken game such that the result of addition equals to the number of winners in the game. See Figure 12.

5 Discussion

As an approach for cryptography between human users and computers we have examined interactive human identification schemes that can resist Q & A attacks in some extent. We have also shown a key idea to convert the human identification schemes to cryptographic communication protocols.

Applied protocols utilize visual characteristic and require human provers only fairly simple manipulations. The author has started an experimental study to measure the complexity of identification or cryptographic processing for human users.

The important subject is to further investigate whether we can develop practically appealing human identification protocols and applications to cryptographic communication along with the suggested line.

One of practical ways of implementing our protocols is

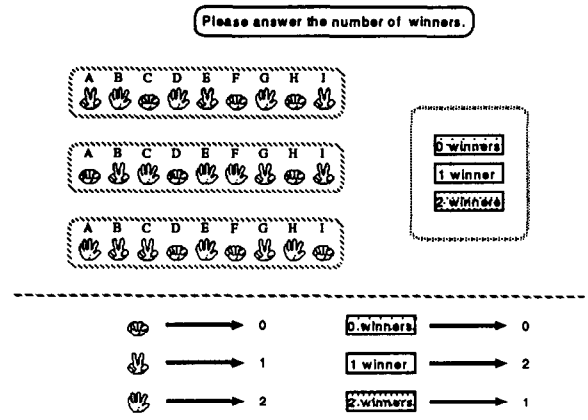

Figure 12: Another Implementation of Protocol 2: Three-Player Game Scheme ($(s,v,u) = (3,6,9)$)

to use one of the proposed identification schemes in conjunction with cryptographically strong methods such as S/KEY [6] which cannot be resistant to peeping of secret inputting procedure.

Acknowledgment

The author would like to thank Ryo Mizutani for his help in implementing the proposed schemes, Jean-Jacques Quisquater for valuable discussions, and anonymous reviewers for their comments.

References

[1] D.M. Davies and W.L. Price, Security for Computer Networks, Chapter 7, John Wiley and Sons, 1984.

[2] J.G. Steiner, C. Neuman and J.I.Schiller, "Kerberos: An authentication service for open network systems," USENIX Conference Proceedings, pp.191-202, February 1988.

[3] T. Matsumoto and H. Imai, "Human identification through insecure channel," Advances in Cryptology — EUROCRYPT'91, Lecture Notes in Computer Science No.547, pp.409-421, Springer-Verlag, 1991.

[4] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," Advances in Cryptology — CRYPTO'86, Lecture Notes in Computer Science No.263, pp.186-194, Springer-Verlag, 1987.

[5] L. Lamport, "Password authentication with insecure communication," Communications of ACM, Vol.24, No.11, pp.770-772, 1981.

[6] N.M. Haller, "The S/KEY™ one-time password system," Proceedings of Internet Society Symposium on Network and Distributed System Security, pp.151-157, 1994.

[7] C.H. Wang, T. Hwang and J.J. Tsai, "On the Matsumoto and Imai's human identification scheme," Advances in Cryptology — EUROCRYPT'95, Lecture Notes in Computer Science No.921, pp.382-392, Springer-Verlag, 1995.