**VTT Technical Research Centre of Finland**

# Review of the use of human senses and capabilities in cryptography

Halunen, Kimmo; Latvala, Outi-Marja

*Published in:*
Computer Science Review

*DOI:*
10.1016/j.cosrev.2020.100340

Published: 01/02/2021

*Document Version*
Publisher's final version

Computer Science Review 39 (2021) 100340

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

# Review of the use of human senses and capabilities in cryptography

Kimmo Halunen, Outi-Marja Latvala *

*VTT Technical Research Centre of Finland Ltd, Finland*

ARTICLE INFO

*Article history:*
Received 21 February 2020
Received in revised form 20 November 2020
Accepted 27 November 2020
Available online xxxx

*Keywords:*
Cryptography
Human senses
Provable security
Visual cryptography

ABSTRACT

Cryptography is a key element in establishing trust and enabling services in the digital world. Currently, cryptography is realized with mathematical operations and represented in ways that are not readily accessible to human users. Thus, humans are left out of the loop when establishing trust and security in the digital world. In many areas the interaction between users and machines is being made more and more seamless and user-friendly, but cryptography has not really enjoyed such development. In this paper, we review the previous research on utilizing human senses and capabilities in cryptography. We present the most relevant existing methods and summarize the current state of the art. In addition, we propose several topics and problems that need to be solved in order to build cryptography that is more accessible to humans. These range from practical implementations of existing methods and utilizing a wider range of human senses all the way to building the theoretical foundations for this new form of cryptography.



**Contents**



## 1. Introduction

Cryptography is a key building block in modern communication protocols and a necessary ingredient to many digital services. Advances in cryptography in the last 40–50 years have brought us public key cryptography [1], digital signatures (e.g. [2]), secure

* Corresponding author.
*E-mail address:* outi-marja.latvala@vtt.fi (O.-M. Latvala).

https://doi.org/10.1016/j.cosrev.2020.100340
1574-0137/

and efficient encryption algorithms (e.g. AES [3]), homomorphic encryption [4] and secure multi-party computation [5], to name a few examples. These are being utilized by billions of people daily in the form of different digital services such as messaging, online banking and shopping, web browsing, cloud computing etc.

Modern cryptography is based on provable security. This means that for a given cryptographic primitive or protocol there should be clearly defined security goals (and corresponding threat models) and a proof (usually by reduction) that shows how the proposed system achieves these goals and under what assumptions. Although there is some criticism towards this approach, e.g. [6,7], it is widely accepted as one of the best guarantees of (theoretical) security for cryptosystems. Of course, the actual implementations can and do suffer from various vulnerabilities and flaws that can be exploited, e.g. [8,9]. However, without a security proof, there would be even less evidence on the security of a cryptosystem, even if the implementation may fail in ways that are not envisioned in the original threat model, e.g. side channels through timing and power consumption.

Despite these advances and the benefits that have been gained, there is an area of cryptography that is not covered in great detail and which lacks comprehensive solutions. The current paradigm of provable security tends to leave the human users of systems out of the picture and to build the security models around the ubiquitous *client–server* model of communications. This model is of course perfectly adequate in machine to machine communications, but it is not enough for describing the human factor, which the user brings to the system.

In addition to the above paradigm, modern cryptography is almost completely outside of human capabilities. In order to use encryption, authentication and other cryptographic functionalities, users need to utilize a computer to carry out the cryptographic tasks. There are only a few notable exceptions, that have been studied in more detail, such as *visual cryptography* [10]. In visual cryptography a human user can decrypt the machine-encrypted message by merely looking at the correctly positioned shares of the message. More recently there has been proposed a theory on human computable functions that could be utilized in cryptography [11]. These ideas have been utilized in the context of password authentication [12,13], but not more generally in cryptography.

Bringing about a change in the current and in many ways very good paradigm raises some questions. What would this new approach achieve? Why would we need such human-friendly systems, when we have very good mechanisms that can be run on computers and computers are becoming more and more ubiquitous? The answer lies partly already in the second question and in the changes that are coming about in our society. We are now giving a lot of power to the machines and algorithms run by very opaque systems. Artificial intelligence (AI) and machine learning have become parts of our everyday life and different algorithms affect us in many ways. This development is not without problems and many potentially adverse effects of this development have been discussed (see [14] for a recent survey on the topic).

One problem with this development is that we have no mechanisms to use human senses and capabilities to evaluate the correctness of these computations and algorithms. This needs to change and there are valid and good cryptographic methods to build trust, transparency and privacy to these systems. The old adage of *"trust, but verify"* should apply to decisions made by AI and algorithms. However, we need cryptography that is accessible to human users and that can build trust and verification capabilities for human–machine interaction. Some ideas towards this kind of functionality, especially in the augmented and virtual reality domains, have been presented in [15].

**Table 1**
Achieving different cryptographic goals with different methods and senses. A ✓means that the goal is achievable with the method or sense and an "N" means that it is not achievable with currently known methods.

| Goal / method | Symmetric | Asymmetric | Vision | Hearing | Touch | Smell |
|---|---|---|---|---|---|---|
| Perfect secrecy | ✓ | ✓ | ✓ | N | N | N |
| IND-CPA | ✓ | ✓ | ✓ | N | N | N |
| IND-CCA | ✓ | ✓ | ✓ | N | N | N |
| Data integrity | ✓ | ✓ | N | N | N | N |
| Dender authentication | Partial | ✓ | N | N | N | N |
| Nonrepudiation | N | ✓ | N | N | N | N |

To further illustrate the motivation behind this paper we drew Fig. 1. It depicts the difference between what our basic client–server model should ideally and hopefully be, what it actually is, and how allowing human users to naturally interact with cryptography could change the situation.

The aim of this paper is to review the existing research on the use of human senses in cryptography and cryptographic protocols. The results of this review will point out the possible gaps and thus also the potential future research direction in this field (see Table 1 on Section 2.9 for details). These open problems will be discussed in the later sections of this article.

This paper is organized as follows. The next section presents and summarizes the previous work on the topic of cryptography with human senses and capabilities. The third section presents our ideas on how to address this problem and what possible venues of research could lead into better solutions. We end the paper with discussion and conclusions of our work.

## 2. Previous work

Previous work directly focusing on this problem of cryptography for human senses is fairly scarce. There are many ways in which usability of security measures has been studied and also interesting proposals on specific domains such as authentication, where some focus has been given to user-friendliness and some results have been achieved. On the other hand, comprehensive solutions to the problem of cryptography for human senses are not available. Furthermore, there is an almost complete lack of theoretical study over this topic.

### 2.1. Visual cryptography

Visual cryptography is one of the only solutions that address the problem of cryptography for human senses. The original idea from [10] shows how to construct a visual encryption of a picture (black and white) that can be decrypted by just looking at the shares. The method is based on the method of secret sharing from [16] and a picture can be encrypted into two or more shares. This requires machine computations. In decrypting the message, the different shares need to be aligned correctly. After this, the secret image appears and the user can see the secret image without any computational help.

There are several extensions to the original scheme for example to colour images [17], rotating images [18] and other capabilities [19,20]. Different kinds of visual cryptography schemes have been compiled in surveys before, for example in [21] and [22]. Comparisons of technical merits for different schemes is out of scope for this paper.

There are also applications of these ideas to authentication e.g. [23–25]. However, these only provide the user the possibility to decrypt the information from the shares of images. Furthermore, visual cryptography only provides *perfect secrecy*. Despite the name, it is only one possible security goal and it is not suitable for many applications of modern cryptography. The

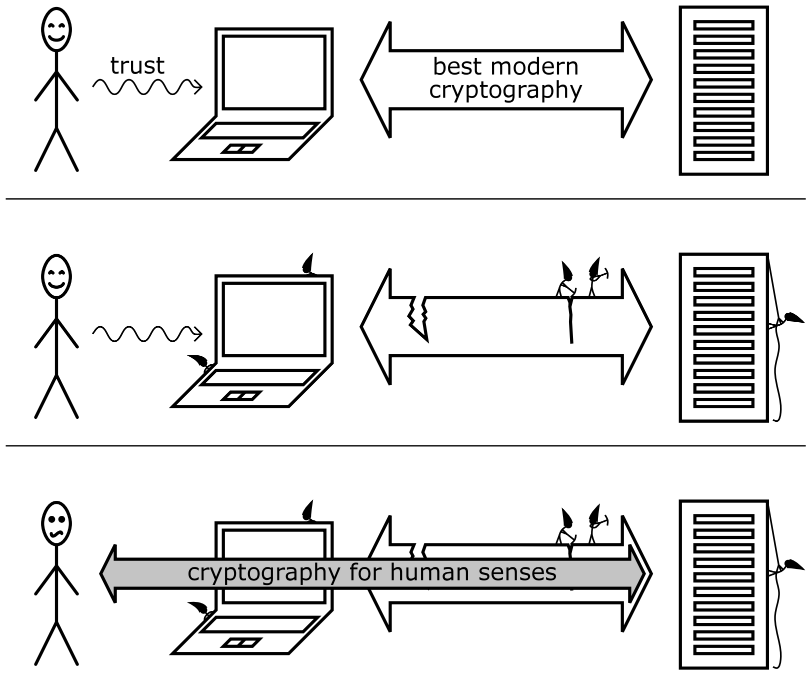


**Fig. 1.** The first image presents the status quo in an ideal world: cryptography used between machines is strong and implemented without faults. The user is trusting and happy that things simply work. The second image depicts the status quo as it really is: malicious actors may compromise any part of the system, and not everything is implemented to perfection in the first place. The user remains trusting and happy. The third image represents our motivation: a human user that is included in the cryptographic processes in a way natural to us is able to perceive the problems. They are less happy, but more informed.

existing systems cannot achieve more advanced properties such as authenticated encryption or public key cryptography. The good aspect of visual cryptography is that there is a security proof for these schemes and a well-founded theory around the problem.

### 2.2. Visualizable encryption

In [26] the authors present the EyeDecrypt system for using augmented reality (AR) in solving some of the issues related to untrusted terminals and shoulder surfing. Different solutions to this problem have been proposed earlier and the more interesting part of the paper is the formalization of *visualizable encryption*.

This extends the normal CPA (chosen plaintext attack) and CCA (chosen ciphertext attack) adversarial models and respective security games more towards systems, where also the human behaviour and interaction with the different devices is taken into account. They are able to show that it is possible to construct CPA- and CCA-secure visualizable encryption schemes from respective regular encryption schemes together with secure hash and MAC functions.

Still their system is only for vision and only implements symmetric encryption, which requires a key exchange between the server and the user device. This key exchange is not defined to have any human verifiable or visualizable components. Thus, this system is a promising start, but not a full solution to the problem of human cryptography. However, these systems enjoy a security proof and thus form a good start of a theoretical foundation for cryptography for human senses.

### 2.3. Computer-aided security schemes

One possibility to help human users is to provide the users with computer-aided systems, where human user provides part of the secret information and then the input terminal augments this by brute force with the help of some external information (a hint). This has been proposed in [27] and the authors present symmetric and asymmetric encryption possibilities as well as a user authentication method with computer-aided security schemes.

Although interesting and probably suitable for several applications, this type of approach is unsatisfactory from several points of view. First of all, it places trust in the terminal that the human user uses for cryptographic tasks. This is something that cryptography for human senses should overcome. That is, users should be able to perform the cryptographic tasks directly themselves from the output of the terminal and to be able to notice if something is not correct. The users should not be made to rely on the terminal to work for them.

Secondly, the proposed methods of [27] are essentially systems, where part of the key is encoded as a human password (randomized) and the other part is brute-forced by the terminal and the cryptographic processes are same as in conventional systems. Although it is possible to have human users memorize even difficult passwords [28], it is far from a perfect solution and not something that is completely accessible with human senses. On the other hand, the systems in [27] enjoy fairly simple security proofs as they can rely on tried and true regular encryption schemes with very little modifications.

### 2.4. Hash visualization

In [29] the authors present the idea of hash visualization. Their premise is that human users are not good at comparing meaningless strings (e.g. hash values in hexadecimal), but are more attuned into seeing differences in pictures. They propose a mechanism called *Random Art* to implement their visual hashing scheme. They also propose a formalism to evaluate and provide proofs of security for hash visualization systems, but unfortunately are unable to prove the Random Art construction secure in this framework.

This line of work has continued in different forms and [30] presents a comparison of different hash visualization methods. The study considers nine different methods, where some are based on strings of characters (in different languages) and some on visual images e.g. Random Art, Flag [31] and T-Flag [32]. The results show, that the accuracy is good (97%–98% for all other methods except English words with "only" 94%) when comparing easy pairs (great differences), but much worse for hard pairs (small differences) except for Random Art (94%). On the other hand, the authors state that even though Random Art is capable of displaying 160-bits of entropy, there is no proof that this would be equal to the perceived entropy that the users actually experience when viewing the images.

Hash visualization has been used in some applications to establish the authenticity of connections and keys, e.g. in the n-Auth mobile authentication scheme [33]. However, these systems do not provide the level of security and formalism that is required for cryptography for human senses. Furthermore, this is yet another technology that is based on vision and leaves out other senses.

### 2.5. Authentication of users, devices and computations

A substantial amount of work has been done related to different authentication schemes with human-verifiable outcomes. In these schemes the goal is that human users can verify the result of the authentication (e.g. device pairing) in a simple way. The methods vary from visual comparison of some values in the devices to be authenticated to physical actions such as bumping the phones together ([34] gives an analysis of some of these methods).

Many human-verifiable authentication systems are based on visual cues like barcodes [35] or light [36]. These offer users the possibility to visually check that the authentication was correctly performed and that there are no attackers meddling in the middle. This type of visual feedback is efficient to check.

Of course, vision is not the only way for users to check the result of an authentication. Other types of comparison methods include sound [37], shaking of the device [38], proximity of other devices [39] and combinations such as demonstrated in [40]. The goal of all these is to provide a method for the users to gain assurance that the authentication has been performed correctly or to make sure that the authentication cannot be performed without the user's consent.

The scalability of some of the above methods has been questioned and some improvements to that have been proposed in [41]. There are also many other proposals in the same vein as those already presented. A good survey on the topic of device pairing (authentication) and comparison of different methods has been made by [42].

Some methods that aim for a larger trust than merely providing verifiable authentication to a system include for example SafeSlinger [43], where the authentication of a group of recipients is paired with an easy to use secure file transfer as well as other protocols. However, this is still a very constrained form of verification as there is no human-verifiable component after the establishment of keys. The protocol also relies on the group of people to have close proximity or a secure channel to authenticate i.e. compare some hash values, at least initially.

The cryptographic methods for securing electronic and online voting systems have been studied quite extensively from both technical [44,45] and societal and legal aspects [46]. There are methods that provide at least in theory a possibility to hold secure and anonymous elections in this fashion. In many cases verifiability is not completely human-centric [47], and usually these cannot be generalized to other types of computational tasks beyond voting. More comprehensive studies on these issues can be found for example in [48] and [49].

There are also some human-verifiable election systems, e.g., [50]. These give the voters a way to verify that their ballot has been correctly included in the tally of the votes. As such, they provide another special case of computing that has verifiability with human senses, but not a comprehensive solution to the problem of cryptography or even "just" authentication with human senses only.

There are also many other areas, where solutions to single problems related to authentication and human capabilities have been addressed. In [51] a method for human users to authenticate possibly untrusted terminals is presented and it is used to access some remote services. The paper describes two different protocols that achieve this property for different threat models. In [52] the authors show a method for using human visual capabilities to digital rights management and user authentication based on schemas in visual memory. There have also been proposals for a method for authenticating pervasive devices with human protocols [53] and a way for message authentication for humans [54].

The problem with all of the above systems is that the verification that they provide for human senses is only applicable in a very narrow use case. For a cryptographic system to be widely applicable, it needs to be able to process arbitrary data. Also not all presented examples have rigorous security proofs, which could be adapted to constructions that are more general.

### 2.6. PRISM & iTurtle

The above methods in authentication are focused on very specific use cases and are not applicable to general computations as such. There are methods that aim for more general authentication and verifiability of computations and digital systems. The most far reaching results are from [55] and [56].

First there is PRISM [55], a system for human users to authenticate a (legacy) system with very little trust on external technology. Their proposed implementation requires the user to have a list of challenge–response pairs with related timing information and a watch to measure time. The challenge is presented to the device and both the response and the execution time are measured. If these do not match to the list, the user will not trust the device.

The PRISM system shows some ways, in which humans can be included in the verification of a computational device. However, the solution is only partial and it requires the system under investigation to be of very limited functionality. The system should not have any connectivity to the Internet, for example. Thus, it is not of use in a modern environment where almost everything is connected to the Internet. On the other hand, PRISM has a security proof in its threat model.

The iTurtle [56] is a trusted device for attesting the functionality of other devices that the user has. Their proposal is a theoretical one and they explicitly want to avoid using cryptography in their device, as it would make the device too complex to their liking. Their system design is based on having a trusted device (the iTurtle) with very limited functionality (red/green lights for reject/accept) and having that device test other devices and software for "known-good" configurations, before using them.

This approach is also interesting, but the limitations of the system are such that it is not suitable for solving most of the problems that could be solved with cryptography for human senses. For example, it is next to impossible to define known-good configurations to a complex system (say, a smart phone or an operating system). Even in cases where this could be possible, new attacks or functionalities can change what a known-good configuration is. This would require updating the iTurtle device and as mentioned in [56], how would this device know the difference between a legitimate update and a malicious attack. Especially, as the device would not have capacity to do cryptographic operations. Furthermore, there is no security proof for iTurtle.

The main limitation of both of these approaches is still in their scope. Although more generic than mere user authentication or voting they still impose a lot of restrictions on the data, systems, hardware and software that can be verified. However, they contain elements that could be applicable in more generic cryptography for human senses.

### 2.7. Security proofs including human elements

Many of the methods above do not have a security proof or the human element is not clearly present in the proof. There are several different ways in which human elements have been incorporated in to security proofs in some cryptographic systems. This section reviews some of the most relevant ones.

One of the first protocols for secure human authentication is presented in [57]. Their protocol is secure against active adversaries, but is unfortunately too inefficient to be used in practice. The method is based on error correcting codes and provides user authentication between a user and a server. As with many other protocols of this nature, this only yields authentication and not other cryptographic properties. The main advantage of this protocol is in the rigorous security proof that is lacking in many alternatives. The paper states that the goal is to build a $(.1, .1, 10)$ human executable protocol. This means that 90% of the population would succeed in the protocol in 10 s with a probability of 90%. The construction presented in the paper achieves $(.9, .2, 300)$ human executable protocol (10% of population with 80% probability in 300 s).

Also in [58] security proofs for protocols involving humans are presented. The high-level aim is in human followable security. In the paper they provide a solution to a much simpler problem that they call human perceptible freshness. Their application area is the Transport Layer Security (TLS) protocol [59]. Their systems adds a layer of communications with human understandable form on top of the regular TLS protocol. Thus the human has a possibility to accept or reject the connection after the initial TLS handshake, if the human perceptible freshness check does not pass. Again this protocol is of limited use as a general cryptographic protocol, but the concepts are valuable and applicable in a wider context as well.

Two generic *human authenticated key exchange* (HAKE) protocols are defined and proofs for the security of such systems are provided in [60]. The protocols work with three parties, a human user, a terminal and a server. In this way, the protocol extends the conventional client–server model by including also a human user.

There are also several definitions on human aspects of computing that are employed in the protocols. The authors define human compatible computation that can then be utilized in challenge–response protocols for key exchange. The concepts are human-readable, human-writeable, human-memorizable, human-computable and human-sampleable.

These are defined again in a very visual fashion with ASCII symbols being considered readable and writable by humans. Also the other three concepts are defined by heuristic assumptions on average human capabilities.

The formalism of [60] is excellent and provides great results on the topic of authenticated key exchange. However, after the key exchange, the active parties in the encrypting and decrypting data are the terminal and the server. Thus the HAKE protocols do not solve the problem of providing cryptography for human senses. This could be achieved, if the keys could be incorporated to a cryptographic protocol for human senses.

One of the most advanced applications with a security proof is from [61]. Their method enables two human users to compute a value of a function $f(x, y)$, where $x$ and $y$ represent the private inputs of the different parties without the aid of computer systems. This method combines the secret sharing methods of visual cryptography, with the theory of garbled circuits. The process for the human users is physical and involves using scissors and transparencies in addition to visual cryptography.

In [60] there is no usability evaluation of the system and their construction is not very simple to follow, especially when more involved functions would be evaluated with this method. Furthermore, the security proof is valid only for the honest-but-curious adversarial model. However, the result is very promising and shows that there are possibilities in applying human capabilities even in more advanced cryptography.

### 2.8. Complexity of human computation

Recently, there have been some advances in defining the human computational capabilities. The authors in [11] define a complexity theory for human computational capabilities and provide examples of human computable pseudorandom generators and one-way functions. These are essential building blocks in modern cryptography and the theory is well founded and sound. It can also be applied in many contexts and provides a good foundation for building new cryptographic systems more accessible to human users.

The main applications of this theory are passwords, which have been studied in [13] and [12]. The results are promising, although the time to learn the functions that are used to generate and protect the passwords is considerable. The upside with passwords is that repetition comes quite naturally and this reinforces the learning of the necessary functions.

These works provide an excellent background for more complex cryptographic systems that we envision in the following section. The main shortcoming of this type of computational approach to cryptography with human capabilities is that it is much less intuitive to users than for example visual cryptography and visualizable encryption, which have been discussed earlier. Thus the application of this type of schemes requires more effort from the users.

### 2.9. Summary of the state of the art

To summarize our findings on the state of the art for current cryptographic methods for human senses, we have compiled two tables.

In Table 1 we present some of the most common goals for cryptographic systems and compare these with different methods and human capabilities for realizing cryptographic systems. As can be seen, traditional symmetric and asymmetric cryptography can achieve most or all goals, whereas human senses have only had success with visual methods. The partial result in the symmetric encryption with sender authentication means that in one-on-one connections the other participant can be assured that the other participant has sent something (that she herself did not), but in group settings or to a third party this is not possible.

We have left out other human capabilities besides human senses from Table 1 as out of scope for this time. However, we believe that there are several human capabilities that might be possible for applications even in cryptography. These will be discussed in later sections of this paper and these contain interesting future research problems. We have also excluded the more advanced cryptographic goals such as homomorphic encryption, secure multi-party computation etc. as these are not yet as commonly available even with traditional, computer-executed methods. Thus, the results of [61] are not shown in the table. Even if that result would be included, the system is still limited to visual perception and would not add to the capabilities of other senses.

A summary of different concepts of cryptography for human senses and capabilities is presented in Table 2. The way the concepts are defined varies a lot, but here we have used a two point scale to assess whether the definition is more heuristic or quantitative in nature. Threat models are available for some of the concepts, as are use cases. The more mature concepts can be achieved in many different ways, but the less developed ones do not have an implementation, yet.

It is also interesting to note, that many of the threat models are very specific to each of the given constructions. Thus, there is no unified theoretical setting from which these systems are built. For some notions the threat model has not even been defined. The conclusion from this is that the field has not yet matured towards more universal theory and definitions.

## 3. Cryptography for human senses and capabilities

In order to achieve new levels for cryptography for human senses and some applications for users, we propose different venues of further research. These can and should all be approached in parallel in order to achieve a real shift towards more human-friendly cryptography.

### 3.1. Extending and applying visual cryptography

The lowest hanging fruit on this new research venue (in our opinion) would be to start applying and extending the currently known visual cryptography methods. Some work towards this end has already been done by, e.g., [25,64,65]. Applications for the more advanced methods have not been reported, but these could be forthcoming in suitable AR applications, for example.

Another direction would be to extend the capabilities of visualizable encryption to public key cryptography, authenticated encryption, digital signatures etc. This would require also new definitions and theory for such systems. For this reason, it is probably a much harder and long-term endeavour.

The main shortcoming of visual cryptography (and visualizable encryption) is that it requires a certain level of visual capability from the user, which is not available to all humans. For example, the WHO (World Health Organization) states that over 250 million people suffer from impaired vision. Out of these, approximately 36 million are totally blind [66]. Thus, a remarkable number of people (especially elderly people) would be left out from the benefits of human cryptography, if only visual or visualizable cryptography would be available. It is interesting to note that currently CAPTCHA [67] security questions on websites tend to have a button, which provides the visual challenge in an audible form. Having similar functionality for visual and visualizable encryption is most likely very difficult if not completely impossible. Furthermore, this functionality has been used to defeat the very protection the CAPTCHA aims to provide [68].

### 3.2. Cryptography for other senses

It is peculiar to note that for other senses such as hearing, there are no cryptographic constructions similar to visual cryptography. As sound is formed of waves and with superposition one can achieve e.g. noise cancelling, it is entirely possible to think that at least similar secret sharing schemes as in visual cryptography could be fairly easy to construct. This could be formed from two or more sounds that in themselves are "random noise", but in some specific conditions cancel out to form an understandable sound of some sort. Thus, not only visual, but also auditory cryptography could be achieved. This could be another way to start expanding cryptography to human senses. After all, sonification (the use of non-speech audio to convey information) is already being tested in network monitoring and situation awareness contexts, see for example [69–71].

Of course, there are also other senses available for human users. The sense of smell is interesting and less applied and studied in the digital context than vision and hearing. There are some ideas on how this could be utilized in the digital world, for example in user authentication [72]. Synthetic odours can be realized and utilized, too [73,74]. Whether or not scents can work as an effective method for human cryptography is an open question. The sense of smell is quite different from vision and hearing, as it is based on detecting different kinds of molecules while the other two are based on detecting electromagnetic or pressure waves. There probably is no simple way to convert a visual cryptography scheme to a scent-based scheme.

Tactile feedback for users has also been used for example in gaming and mobile phone alerts for several years. With the increase in VR devices and services, even more immersive tactile feedback systems have been realized. Such systems offer possibilities for using this part of human senses for cryptography as well.

One interesting possible venue would be to use some form of tactile gloves and a surface capable for projecting dots as in Braille system. A possible direction of research could be to see, if the ideas from visual cryptography could be extended to this type of information, where parts of the Braille come from the surface and parts from the glove.

The idea of haptic gloves is becoming quite popular. In addition to the straightforward gaming gloves under development for various VR or AR platforms, there is the Sleeve by Nokia Bell Labs [75], an armband that is supposed to convey emotions between users. If such a device can indeed assess a user's emotional state accurately, that data could be used for other purposes as well. This is similar to the idea of using brain–computer-interface technology for interacting with computers. For example, in [76] the idea of pass-thoughts for user authentication is presented.

### 3.3. Beyond symmetric cryptography

To really change the current paradigm of human-friendly cryptographic systems there needs to be advances in the capabilities of the cryptographic systems that are possible to realize with human senses. For example, visual cryptography offers "only" perfect secrecy, which has been deemed inadequate for most modern cryptographic needs and is being replaced by systems that offer CPA or CCA security. Most importantly, perfect secrecy does not offer any authentication on the data. Currently, the preferred standard for symmetric encryption systems is authenticated encryption with associated data. This can be achieved with a secure block cipher and a suitable mode of operation. Visualizable encryption provides theoretical foundations for such approach, but the actual implementation of the method of [26] falls short of providing these fully.

Because public-key cryptography has been a key enabler in many digital services, it would be important to have such capabilities for human cryptography. To this end, there is currently no research either in theory or in practice. The public key systems (both traditional and post-quantum) are based on heavy mathematics that is not practical to apply to human senses. Finding replacements for these building blocks is an interesting research problem and a necessary step to achieve cryptography for human senses and capabilities.

Of course, there is no reason to stop at only public key cryptography. If such systems could be devised, there could be possibilities to build (partially) homomorphic encryption systems [4], identity and attribute-based cryptography [77,78] and

**Table 2**
Different concepts of cryptography for human senses and their capabilities.

| Concept | Def.[a] | Threat model | Use case | Achievability |
|---|---|---|---|---|
| Visual cryptography [10] | Q | Perfect secrecy | Decryption | Multiple methods |
| Visualizable cryptography [26] | Q | CPA & CCA | Decryption & verification | One method / partial |
| Visual hashing [29,30] | Q | Near-one-way function[b] | Verification | Multiple methods |
| Human compatible function families [60] | H | HAKE[b] | Authenticated Key Exchange | Multiple methods |
| Human followable security [58] | H | Undefined | Verification | Not currently possible |
| Human perceptible freshness [58] | H | H-ACCE[b] | Session authentication | Generic compiler presented |
| Human perceptible authenticator [62] | H | Active adversary [63] | User authentication | One method |
| Human executable protocols [57] | H | Passive & active adversary[b] | User authentication | Multiple methods |
| Human computation [11] | Q | Turing machine with unbounded computation time[b] | Pseudo-randomness, one-way functions and passwords | Multiple methods |

[a]This column signifies whether the concept is defined more heuristically (H) or quantitatively (Q) in the original paper.
[b]The threat model is specific to a construction presented in the original paper.

many other concepts that have been proposed and studied in traditional cryptography. Again finding suitable methods that do not require excessive computation is a key problem to be solved.

### 3.4. Encryption with human senses and abilities

Although it might be argued that decryption and verification with human senses are more important, the option to also encrypt (and sign) with human senses and abilities should not be dismissed as a research problem. All the existing systems work on the assumption that the encryption part of the cryptography is done by a computer. Only decryption (or verification) is done by human senses.

Building a fully-fledged system for human cryptography would of course require the ability to encrypt information without the help of computers. For authentication, one could use handwritten signatures, which has been common in the past. However, making sure that these are not copied or altered in transit in digital form is not guaranteed by any means and also the human verification might be susceptible to errors.

Traditionally systems that enable humans to encrypt and decrypt have been horribly insecure against computer-aided adversaries. The question then becomes: *What are the things that humans can do better than machines and computers in a way that other machines and computers cannot decipher the results of those actions?* It is safe to say that mathematics is probably not the way to go. The next problem is how to build cryptography around these human-friendly primitives. Would these require augmented or virtual reality solutions? Is there some component of human abilities that could be used to build cryptographic systems? All these questions would require extensive research and experimentation to find good answers.

### 3.5. Theoretical foundations

As mentioned in the previous sections, some of the currently available methods for applying cryptography to human senses have good formalisms and security proofs while others do not. In any case, there is a great variety of different notions, security targets and threat models that these systems apply, as can be seen from Table 2. This of course reflects the variety of human senses and their many strengths and limitations.

With the exceptions of visual cryptography and visualizable encryption, many of the proposed notions have not been tightly linked to existing cryptographic security notions such as perfect secrecy, CPA- and CCA-security. Thus, there is a lack of common theoretical foundation upon which cryptography for human senses could be built. Formulating this theoretical foundation is necessary to have similar provable security guarantees for human cryptography as for traditional cryptography.

As already mentioned, there should also be more advanced forms of cryptography such as public-key cryptography available for human senses. An open question is, can this be formalized and (even partially) realized with similar constructions as in visualizable encryption. The constructions of visualizable encryption are quite straightforward applications of the existing security notions. It may very well be that more complex constructions are needed for public-key cryptography for human senses. Also related to theoretical foundations are impossibility results that would reveal that some forms of human cryptography are not possible to achieve. Forming these foundations is an interesting topic of future research and something that is outside of the scope of this paper.

## 4. Discussion

The main question that needs to be answered before cryptography for human senses becomes reality is: *What are the human advantages over computers and machines?* When such advantages are identified, there should be studies in how these could be leveraged towards cryptography and then how to make these work over digital media and to scale at a global level.

We propose to shift the paradigm from defining security goals in a way that leads to cryptographic systems only accessible to computers and other machines, towards a more human-friendly cryptography. We argue that it should be possible to build cryptographic protocols and primitives that have meaningful security goals and provable security under reasonable assumptions and that are accessible with human senses and human intelligence and "computing power". The capabilities of the human user should be integral to the scheme.

One interesting property of human users that needs to be taken into account is the question of cultural differences and their effect on the possibilities of cryptography for human senses. Traditional cryptography is universal in the sense that its functionality is not dependent on the age, gender, ethnicity or any other attribute of the user. Ideally, cryptography for human senses would also be universal to all people.

Because there are both differences and similarities in the way people from different backgrounds perceive things, these need to be considered and preferably utilize only the most universal properties that are available. For example, The World Colour Survey [79] was established to find out if there are universal constraints on cross-language colour naming, and if there is an evolutionary progression according to which languages gain colour terms over time. Analysis of this data has found, e.g., that there are some universal processes that control the naming of colours [80], and that colour naming across languages reflect optimal divisions of an irregularly shaped perceptual colour space [81]. Moreover, a review on colour perception and naming [82] finds that even though language does affect colour perception, it only affects the right visual field via the activation of the language regions of the left hemisphere of the brain.

Language also affects the way we hear the world: for example, in Finnish non-musicians and French musicians pre-attentive and attentive processing of duration was enhanced compared to French non-musicians [83]. This is due to the fact that Finnish is a quantity language, and differentiating between "tuli" (fire), "tuuli" (wind) and "tulli" (Customs) is important. Nevertheless, even in languages there seems to be some universality available. Certain structures seem to be preferable to others, e.g. a syllable like "blif" is preferred to syllables like "bdif" and "lbif". Even newborns like the first example best [84].

One argument that might go against the idea of cryptography for human senses is that one might envision a future of enhanced humans that have abilities to interact with cryptographic protocols in a native way. Such ideas are currently more mainstream in science fiction, but it might be that at some point this could be possible in reality. One example of such future is presented in Hannu Rajaniemi's novel *The Quantum Thief* [85].

In the book, the Martian society has developed a very elaborate system called *gevulot* (Hebrew for "limits"), which is essentially a PKI system that allows the people to achieve various levels of privacy and even choose what parts of conversations and interactions can be "remembered" by the parties involved. The citizens of Mars have developed skills and an etiquette on how to use this system in their daily lives. Of course, the people living in the society have vastly transcended our current human capabilities.

On the other hand, it might be possible to realize a system much like *gevulot* with current cryptographic methods such as attribute-based encryption, homomorphic encryption and other advanced cryptographic primitives. Thus, it would be great to have these systems work in a way that would be accessible to ordinary humans. This then would be an argument in favour of researching cryptography for human senses.

Another argument against cryptography for human senses is user discomfort. As the current paradigm is reliant on heavy mathematics and things just seem to work, it is understandable that a regular user would not want to get involved with cryptography. Therefore, the usability aspects of cryptography for human senses are very important, so that the ease of use overcomes the discomfort of getting involved. Moreover, in the current state of cryptography there is no place for the human user in the trust chain, and without further research we cannot even offer people the option to get involved.

One possible additional human capability that could be used is the perception of elapsed time as already done with PRISM. Time is usually available from many different and independent sources and humans can approximate the elapsed time with some accuracy (say whether something took 5 or 50 s), although there are a lot of things that can interfere with the perception of time, for example stimulants and depressants, emotions, and age. Of course, this does not give us very much to work on, but it could be a way to build e.g. some form of authentication to a human cryptography system.

The limitations of different senses and human understanding of different visual, auditory and haptic sensory input has already been mentioned. The challenge that this poses towards the theoretical development of cryptography for human senses is the common requirement of *correctness* of cryptosystems. Correctness means that for any message $m$, encryption function $E$ and decryption function $D$ we must have $D(E(m)) = m$.

However, humans tend to make all sorts of mistakes with sensory perception and thus it may not be possible to have cryptography that satisfies the traditional correctness definition. Having a probabilistic definition for correctness might work, but it raises the question, what is the result of $D(E(m))$, when the human recognition fails. Will this become a possible side channel for adversaries and/or an opportunity for denial-of-service type of attacks?

Another challenge is the key generation and other randomness that is necessary for modern cryptography to function. Natural sources have some entropy available, but how can humans use this entropy without technical devices. On the other hand, if only entropy from the humans participating in the cryptographic operations is used, will there be enough to provide secure encryption.

Biometrics can be used to provide entropy and there are methods to make this uniform as required by cryptographic protocols e.g. via fuzzy extractors [86]. However, this type of extraction is not possible with human senses. Furthermore, humans tend to be bad at generating randomness as evidenced for example by the poor choices of passwords that people use for user authentication.

## 5. Conclusion

In this paper, we have reviewed the current state of the art in cryptography for human senses. Such cryptography has mostly been built upon the concepts of visual and visualizable cryptography, that have already been studied in some detail. Thus there is a lack of methods that utilize other senses and human capabilities. Furthermore, the current methods cannot realize many of the security goals for modern cryptography as can be seen from Table 1.

To achieve more advanced security goals and to build a wider range of capabilities (e.g. message authentication), there needs to be further research both in implementations as wells as on the theoretical foundations. In addition, the possibilities of other senses than vision should be examined to find new cryptographic techniques for human senses. We are confident that research in this area will yield better and more human-friendly cryptographic methods that are more accessible with human capabilities. This will then result in better building blocks for trust in our ever more connected and digital world.

## CRediT authorship contribution statement

**Kimmo Halunen:** Conceptualization, Investigation, Writing - original draft, Writing - review & editing, Supervision, Project administration, Funding acquisition. **Outi-Marja Latvala:** Conceptualization, Investigation, Writing - original draft, Writing - review & editing, Visualization.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgement

The research has been funded by the EUREKA/Celtic-Plus, Finland cluster project SENDATE.

## References

[1] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory 22 (6) (1976) 644–654.
[2] S. Goldwasser, S. Micali, R.L. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, SIAM J. Comput. 17 (2) (1988) 281–308.
[3] Pub, NIST FIPS, 197: Advanced encryption standard (AES), Fed. Inf. Process. Stand. Publ. 197 (441) (2001) 0311.
[4] C. Gentry, A Fully Homomorphic Encryption Scheme (Ph.D. thesis), Stanford University, 2009.
[5] A.C. Yao, Protocols for secure computations, in: Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on, IEEE, 1982, pp. 160–164.
[6] N. Koblitz, A.J. Menezes, Another look at "provable security", J. Cryptol. 20 (1) (2007) 3–37.
[7] N. Koblitz, A. Menezes, Another look at security definitions, Adv. Math. Commun. 7 (1) (2013) 1–38.
[8] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J.A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, et al., Imperfect forward secrecy: How diffie-hellman fails in practice, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2015, pp. 5–17.
[9] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J.A. Halderman, V. Dukhovni, et al., DROWN: Breaking TLS using SSLv2, in: USENIX Security Symposium, 2016, pp. 689–706.
[10] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology, EUROCRYPT'94, Springer, 1995, pp. 1–12.
[11] M. Blum, S. Vempala, The complexity of human computation: A concrete model with an application to passwords, 2017, arXiv:1707.01204.
[12] S. Samadi, S. Vempala, A.T. Kalai, Usability of humanly computable passwords, in: Sixth AAAI Conference on Human Computation and Crowdsourcing, 2018.
[13] J. Blocki, M. Blum, A. Datta, S. Vempala, Towards human computable passwords, in: 8th Innovations in Theoretical Computer Science Conference, Vol. 67, ITCS 2017, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017, p. 10.
[14] M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, et al., The malicious use of artificial intelligence: Forecasting, prevention, and mitigation, 2018, arXiv preprint arXiv:1802.07228.
[15] K. Halunen, O.-M. Latvala, H. Karvonen, J. Häikiö, S. Valli, M. Federley, J. Peltola, Human verifiable computing in augmented and virtual realities, 2017, White paper, http://www.vtt.fi/inf/julkaisut/muut/2017/human-verifiable-computing-white-paper.pdf.
[16] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.
[17] Y.-C. Hou, Visual cryptography for color images, Pattern Recogn. 36 (7) (2003) 1619–1629.
[18] S.J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, K. Chen, Sharing multiple secrets in visual cryptography, Pattern Recognit. 40 (12) (2007) 3633–3651.
[19] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theoret. Comput. Sci. 250 (1–2) (2001) 143–161.
[20] R. Ito, H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Trans. Fund. Electron. Commun. Comput. Sci. 82 (10) (1999) 2172–2177.
[21] R. Bhatnagar, M. Kumar, Visual cryptography: A literature survey, in: 2018 Second International Conference on Electronics, Communication and Aerospace Technology, ICECA, IEEE, 2018, pp. 78–83.
[22] P. Punithavathi, S. Geetha, Visual cryptography: A brief survey, Inf. Secur. J.:Global Persp. 26 (6) (2017) 305–317.
[23] N. Askari, C. Moloney, H.M. Heys, et al., Application of visual cryptography to biometric authentication, in: Newfoundland Electrical and Computer Engineering Conference, 2011.
[24] O.-M. Latvala, C. Peng, P. Honkamaa, K. Halunen, "Speak, Friend, and Enter" - secure, spoken one-time password authentication, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS, 2018, pp. 1–5.
[25] Y.-W. Chow, W. Susilo, M.H. Au, A.M. Barmawi, A visual one-time password authentication scheme using mobile devices, in: International Conference on Information and Communications Security, Springer, 2014, pp. 243–257.
[26] A.G. Forte, J.A. Garay, T. Jim, Y. Vahlis, EyeDecrypt—Private interactions in plain sight, in: International Conference on Security and Cryptography for Networks, Springer, 2014, pp. 255–276.
[27] Y. Jinno, T. Tsuchiya, T. Ohki, K. Takahashi, W. Ogata, M. Nishigaki, A study on construction and security of computer-aided security schemes, in: The 2017 International Conference on Computational Science and Computational Intelligence, CSCI'17, IEEE, 2017.
[28] J. Bonneau, S. Schechter, Towards reliable storage of 56-bit secrets in human memory, in: 23rd USENIX Security Symposium, USENIX Security 14, 2014, pp. 607–623.
[29] A. Perrig, D. Song, Hash visualization: A new technique to improve real-world security, in: International Workshop on Cryptographic Techniques and E-Commerce, 1999, pp. 131–138.
[30] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, B.-Y. Yang, A study of user-friendly hash comparison schemes, in: Computer Security Applications Conference, 2009. ACSAC'09. Annual, IEEE, 2009, pp. 105–114.
[31] C. Ellison, S. Dohrmann, Public-key support for group collaboration, ACM Trans. Inf. Syst. Secur. 6 (4) (2003) 547–565.
[32] Y.-H. Lin, A. Studer, Y.-H. Chen, H.-C. Hsiao, L.-H. Kuo, J.M. McCune, K.-H. Wang, M. Krohn, A. Perrig, B.-Y. Yang, et al., SPATE: small-group PKI-less authenticated trust establishment, IEEE Trans. Mob. Comput. 9 (12) (2010) 1666–1681.
[33] R. Peeters, J. Hermans, P. Maene, K. Grenman, K. Halunen, J. Häikiö, n-Auth: Mobile authentication done right, in: Proceedings of the 33rd Annual Computer Security Applications Conference, ACM, 2017, pp. 1–15.
[34] R. Nithyanand, N. Saxena, G. Tsudik, E. Uzun, Groupthink: usability of secure group association for wireless devices, in: Proceedings of the 12th ACM International Conference on Ubiquitous Computing, ACM, 2010, pp. 331–340.
[35] J.M. McCune, A. Perrig, M.K. Reiter, Seeing-is-believing: Using camera phones for human-verifiable authentication, in: Security and Privacy, 2005 IEEE Symposium on, IEEE, 2005, pp. 110–124.
[36] R. Mayrhofer, M. Welch, A human-verifiable authentication protocol using visible laser light, in: Availability, Reliability and Security, 2007. ARES 2007. the Second International Conference on, IEEE, 2007, pp. 1143–1148.
[37] M.T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, E. Uzun, Loud and clear: Human-verifiable authentication based on audio, in: Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on, IEEE, 2006, p. 10.
[38] R. Mayrhofer, H. Gellersen, Shake well before use: Authentication based on accelerometer data, in: Pervasive Computing, Springer, 2007, pp. 144–161.
[39] A. Varshavsky, A. Scannell, A. LaMarca, E. De Lara, Amigo: Proximity-Based Authentication of Mobile Devices, Springer, 2007.
[40] R. Prasad, N. Saxena, Efficient device pairing using "human-comparable" synchronized audiovisual patterns, in: Applied Cryptography and Network Security, Springer, 2008, pp. 328–345.
[41] C.-M. Chen, K.-H. Wang, T.-Y. Wu, J.-S. Pan, H.-M. Sun, A scalable transitive human-verifiable authentication protocol for mobile devices, Inf. Forensics Secur., IEEE Trans. 8 (8) (2013) 1318–1330.
[42] A. Kumar, N. Saxena, G. Tsudik, E. Uzun, A comparative study of secure device pairing methods, Pervasive Mob. Comput. 5 (6) (2009) 734–749.
[43] M. Farb, M. Burman, G.S. Chandok, J. McCune, A. Perrig, Safeslinger: An Easy-To-Use and Secure Approach for Human Trust Establishment, Tech. Rep., DTIC Document, 2012.
[44] J. Karro, J. Wang, Towards a practical, secure, and very large scale online election, in: Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual, IEEE, 1999, pp. 161–169.
[45] D.A. Gritzalis, Principles and requirements for a secure e-voting system, Comput. Secur. 21 (6) (2002) 539–556.
[46] L. Mitrou, D. Gritzalis, S. Katsikas, Revisiting legal and regulatory requirements for secure e-voting, in: Security in the Information Society, Springer, 2002, pp. 469–480.
[47] S. Kremer, M. Ryan, B. Smyth, Election verifiability in electronic voting protocols, in: European Symposium on Research in Computer Security, Springer, 2010, pp. 389–404.
[48] B. Adida, Advances in Cryptographic Voting Systems (Ph.D. thesis), Massachusetts Institute of Technology, 2006.
[49] D.A. Gritzalis, Secure Electronic Voting, Vol. 7, Springer Science & Business Media, 2012.
[50] M. Kutyłowski, F. Zagórski, Scratch, click & vote: E2e voting over the Internet, in: Towards Trustworthy Elections, Springer, 2010, pp. 343–356.
[51] N. Asokan, H. Debar, M. Steiner, M. Waidner, Authenticating public terminals, Comput. Netw. 31 (8) (1999) 861–870.
[52] M. Nishigaki, T. Yamamoto, Making use of human visual capability to improve information security, in: Availability, Reliability and Security, 2009. ARES'09. International Conference on, IEEE, 2009, pp. 990–994.
[53] A. Juels, S.A. Weis, Authenticating pervasive devices with human protocols, in: Annual International Cryptology Conference, Springer, 2005, pp. 293–308.
[54] J. King, A. Dos Santos, A user-friendly approach to human authentication of messages, in: International Conference on Financial Cryptography and Data Security, Springer, 2005, pp. 225–239.

[55] J. Franklin, M. Luk, A. Seshadri, A. Perrig, PRISM: enabling personal verification of code integrity, untampered execution, and trusted i/o on legacy systems or human-verifiable code execution, CyLab (2007) 41.
[56] J.M. McCune, A. Perrig, A. Seshadri, L. van Doorn, Turtles All the Way Down: Research Challenges in User-Based Attestation, Tech. Rep., DTIC Document, 2007.
[57] N.J. Hopper, M. Blum, Secure human identification protocols, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2001, pp. 52–66.
[58] K. Radke, C. Boyd, Security proofs for protocols involving humans, Comput. J. 60 (4) (2017) 527–540.
[59] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, Tech. Rep., RFC 5246, 2008.
[60] A. Boldyreva, S. Chen, P.-A. Dupont, D. Pointcheval, Human computing for handling strong corruptions in authenticated key exchange, in: Computer Security Foundations Symposium (CSF), 2017 IEEE 30th, IEEE, 2017, pp. 159–175.
[61] P. D'Arco, R. De Prisco, Secure computation without computers, Theoret. Comput. Sci. 651 (2016) 11–36.
[62] S. Gajek, M. Manulis, A.-R. Sadeghi, J. Schwenk, Provably secure browser-based user-aware mutual authentication over TLS, in: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ACM, 2008, pp. 300–311.
[63] D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inform. Theory 29 (2) (1983) 198–208.
[64] P. Lantz, B. Johansson, M. Hell, B. Smeets, Visual cryptography and obfuscation: A use-case for decrypting and deobfuscating information using augmented reality, in: Financial Cryptography and Data Security, Springer, 2015, pp. 261–273.
[65] S.J. Andrabi, M.K. Reiter, C. Sturton, Usability of augmented reality for revealing secret messages to users but not their devices, in: Eleventh Symposium on Usable Privacy and Security, SOUPS 2015, 2015, pp. 89–102.
[66] World Health Organisation, Blindness and vision impairment, 2018, http://www.who.int/mediacentre/factsheets/fs282/en/, (Accessed: 19 December 2018).
[67] L. Von Ahn, M. Blum, N.J. Hopper, J. Langford, CAPTCHA: Using hard AI problems for security, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2003, pp. 294–311.
[68] K. Bock, D. Patel, G. Hughey, D. Levin, unCaptcha: a low-resource defeat of recaptcha's audio challenge, in: Proceedings of the 11th USENIX Conference on Offensive Technologies, USENIX Association, 2017, p. 7.
[69] L.M. Axon, B. Alahmadi, J.R.C. Nurse, M. Goldsmith, S. Creese, Sonification in security operations centres: what do security practitioners think? 2018, arXiv:1807.06706.
[70] V.F. Mancuso, E.T. Greenlee, G. Funke, A. Dukes, L. Menke, R. Brown, B. Miller, Augmenting cyber defender performance and workload through sonified displays, Proc. Manuf. 3 (2015) 5214–5221.
[71] P. Vickers, C. Laing, T. Fairfax, Sonification of a network's self-organized criticality for real-time situational awareness, Displays 47 (2017) 12–24.
[72] M.D. Gibbs, Biometrics: body odor authentication perception and acceptance, ACM SIGCAS Comput. Soc. 40 (4) (2010) 16–24.
[73] D. Gosain, M. Sajwan, Aroma tells a thousand pictures: digital scent technology a new chapter in IT industry, Int. J. Curr. Eng. Tech. 4 (2014) 2804–2812.
[74] K. Salminen, J. Rantala, P. Isokoski, M. Lehtonen, P. Müller, M. Karjalainen, J. Väliaho, A. Kontunen, V. Nieminen, J. Leivo, et al., Olfactory display prototype for presenting and sensing authentic and synthetic odors, in: Proceedings of the 2018 on International Conference on Multimodal Interaction, ACM, 2018, pp. 73–77.
[75] E. Stinson, This gadget communicates human emotions through touch, 2018, https://www.wired.com/story/bell-labs-sleeve/, (Accessed: 12 July 2018).
[76] J. Thorpe, P.C. van Oorschot, A. Somayaji, Pass-thoughts: Authenticating with our minds, in: Proceedings of the 2005 Workshop on New Security Paradigms, NSPW '05, ACM, New York, NY, USA, 2005, pp. 45–56, http://dx.doi.org/10.1145/1146269.1146282.
[77] A. Shamir, Identity-based cryptosystems and signature schemes, in: G. Blakley, D. Chaum (Eds.), Advances in Cryptology, in: Lecture Notes in Computer Science, vol. 196, Springer Berlin Heidelberg, 1985, pp. 47–53.
[78] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2005, pp. 457–473.
[79] P. Kay, B. Berlin, L. Maffi, W.R. Merrifield, R. Cook, The World Color Survey, CSLI Publications Stanford, 2009.
[80] D.T. Lindsey, A.M. Brown, World Color Survey color naming reveals universal motifs and their within-language diversity, Proc. Natl. Acad. Sci. 106 (47) (2009) 19785–19790, arXiv:http://www.pnas.org/content/106/47/19785.full.pdf.
[81] T. Regier, P. Kay, N. Khetarpal, Color naming reflects optimal partitions of color space, Proc. Natl. Acad. Sci. 104 (4) (2007) 1436–1441, arXiv:http://www.pnas.org/content/104/4/1436.full.pdf.
[82] T. Regier, P. Kay, Language, thought, and color: Whorf was half right, Trends Cogn. Sci. 13 (10) (2009) 439–446.
[83] C. Marie, T. Kujala, M. Besson, Musical and linguistic expertise influence pre-attentive and attentive processing of non-speech sounds, Cortex 48 (4) (2012) 447–457.
[84] D.M. Gómez, I. Berent, S. Benavides-Varela, R.A.H. Bion, L. Cattarossi, M. Nespor, J. Mehler, Language universals at birth, Proc. Natl. Acad. Sci. 111 (16) (2014) 5837–5841, arXiv:http://www.pnas.org/content/111/16/5837.full.pdf.
[85] H. Rajaniemi, The Quantum Thief, St. Martin's Press, 2012.
[86] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, SIAM J. Comput. 38 (1) (2008) 97–139.