Cryptography for Human Senses

Kimmo Halunen and Outi-Marja Latvala

VTT Technical Research Centre of Finland
P.O. Box 1100
FI-90571 OULU, Finland
[firstname.lastname]@vtt.fi

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 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 present ideas that could make cryptography more accessible to humans. We review previous research on this topic and some results that have been achieved. We propose several topics and problems that need to be solved in order to build cryptography for human senses. These measures range from practical implementations of existing methods and utilising a wider range of human senses all the way to building the theoretical foundations of this new form of cryptography.

Keywords: Cryptography, Human Senses, Provable Security

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 e.g. public key cryptography [13], digital signatures (e.g. [22]), secure and efficient encryption algorithms (e.g. AES [17]), homomorphic encryption [20] and multi-party computation [66]. 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. by Koblitz and Menezes [37, 36], 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. [2, 7]. 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, power consumption etc.

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 utilise a computer to carry out the cryptographic tasks. There is only one notable exception, *visual cryptography* [52], where a human user can decrypt the machine-encrypted message by merely looking at the correctly positioned shares of the message.

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 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.

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 in [10].

One problem with this development is that we have no mechanisms to use human senses 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, has been presented in [28].

This paper is organised as follows. The next section presents the previous work on the topic of cryptography (and other closely related fields) and human interaction with human senses. 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 of [52] shows how to construct a visual encryption of a picture (black and white) that can be decrypted by just watching the shares. The method is based on secret sharing and a picture can be encrypted into two or more shares. This requires machine computations. The decryption requires the different shares 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 color images [29], rotating images [61] and other capabilities [6, 31]. There are also applications of these ideas to authentication e.g. [4, 42, 12]. However, these only provide the user the possibility to decrypt the information from the shares of images. Furthermore, visual cryptography only provides perfect secrecy, which is only one possible security goal and the existing systems cannot achieve more advanced properties such as authenticated encryption or public key cryptography. The good point 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 [18] the authors present 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 formalisation 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 theoretical foundation for cryptography for human senses.

2.3 Computer-Aided Security Schemes

One possibility to help human users is to provide 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). An example of this can be found in [32]. They present symmetric and asymmetric encryption possibilities as well as user authentication method with computer-aided security schemes.

Although interesting and probably applicable for several applications, this type of approach is unsatisfactory from several points of view. Firstly, 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 in [32] are essentially systems, where part of the key is encoded as 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 (e.g. [9]), it is far from a perfect solution and not something that is completely accessible with human senses. On the other hand, the systems from [32] 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 their paper [56] Perrig and Song 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 visualisation methods. Their 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 [15] and T-Flag [43]. 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 [55]. 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 (see [54] for analysis of some of these methods).

Many human-verifiable authentication systems are based on visual cues like barcodes [49] or light [48]. 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 [24], shaking of the device [47], proximity of other devices [63] and combinations such as [57]. 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 [11]. 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 can be found in [39].

Some methods that aim for a larger trust than merely providing verifiable authentication to some system include for example SafeSlinger [16], where the authentication of the group of recipients is paired with easy to use secure file transfer and 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 at least initially to have close proximity or a secure channel to authenticate i.e. compare some hash values.

The cryptographic methods for securing electronic and online voting systems have been studied quite extensively from both technical, e.g., [34, 26] and societal and legal aspects, as in [51]. 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 [38] and in general, these

cannot be generalised to other types of computational tasks beyond voting. More comprehensive studies on these issues can be found for example in [1] and [27].

There are also some human-verifiable election systems, e.g., [40]. 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 [5] the authors present a method for human users to authenticate possibly untrusted terminals, which they use to access some remote services. The paper describes two different protocols that achieve this property for different threat models. In [53] the authors propose using human visual capabilities to digital rights management and user authentication based on schemas in visual memory. In [33] a method for authenticating pervasive devices with human protocols is presented and [35] presents a way for message authentication for humans.

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 applicable to arbitrary data. Also not all presented examples have rigorous security proofs, which could be applicable 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 [19] and [50].

In [19] the authors present PRISM, 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.

In [50] the authors present their system (iTurtle) for 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) and even in cases where this could be possible, new attacks or functionalities can change these. This would require updating the iTurtle device and as the authors of [50] put it, 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.

3 Cryptography for Human Senses

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 in, e.g., [12, 41, 3]. 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[1]. 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

[1] See http://www.who.int/mediacentre/factsheets/fs282/en/ for details.

interesting to note that currently CAPTCHA [65] 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.

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 [8, 45, 64].

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 utilised in the digital world, for example in user authentication [21]. Also synthetic odours can be realised and utilised [25]. 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. A simple way to convert a visual cryptography scheme to a scent-based scheme is probably not possible.

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

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[2], 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

[2] See https://www.wired.com/story/bell-labs-sleeve/ for some more information

with computers. For example, authors of [62] present the idea of pass-thoughts for user authentication.

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 realise 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 [18] 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 with human senses. Finding replacements for these building blocks is an interesting research problem and necessary to achieve human cryptography.

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, identity and attribute-based cryptography and 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 possibility 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 possibility 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 can we build cryptography around these human-friendly primitives? Would these require augmented or virtual reality solutions? For example, most people are able to catch a ball thrown at them with moderate speed and good accuracy. Many robots cannot perform such tasks. Is there some component of human abilities at work there 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 with human senses have good formalisms and security proofs and others do not. In any case, there is a great variety in the different notions, security targets and threat models that these systems apply. This of course reflects the variety of human senses and their many strengths and limitations.

With the exceptions of visual cryptography and visualizable encryption, the 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 formalised and (even partially) realised 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.

In Table 1 we present some of the most common goals for cryptographic systems and compare these with different methods and senses for realising 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 send something (that she herself did not), but in group settings or to a third party this is not possible.

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*

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
sender authentication	Partial	✓	N	N	N	N
nonrepudiation	N	✓	N	N	N	N

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.

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 utilise only the most universal properties that are available. For example, The World Color Survey[3] 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 [44], and that colour naming across languages reflect optimal divisions of an irregularly shaped perceptual colour space [60]. Moreover, a review on colour perception and naming [59] 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 [46]. 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 new-borns like the first example best [23].

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

[3] http://www1.icsi.berkeley.edu/wcs/

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* [58].

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 realise 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.

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 seconds). 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 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 [14]. However, this type of extraction is not possible by 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 presented the idea of cryptography for human senses. Such cryptography could be built upon the concepts of visual and visualizable cryptography, that have already been studied. However, 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 theoretical background. 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 can be utilised with human senses.

References

1. Adida, B.: Advances in cryptographic voting systems. Ph.D. thesis, Massachusetts Institute of Technology (2006)
2. Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J.A., Heninger, N., Springall, D., Thomé, E., Valenta, L., et al.: Imperfect forward secrecy: How diffie-hellman fails in practice. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 5–17. ACM (2015)
3. Andrabi, S.J., Reiter, M.K., Sturton, C.: Usability of augmented reality for revealing secret messages to users but not their devices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 89–102 (2015)
4. Askari, N., Moloney, C., Heys, H.M., et al.: Application of visual cryptography to biometric authentication. In: Newfoundland Electrical and Computer Engineering conference (2011)
5. Asokan, N., Debar, H., Steiner, M., Waidner, M.: Authenticating public terminals. Computer Networks 31(8), 861–870 (1999)
6. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. Theoretical Computer Science 250(1-2), 143–161 (2001)
7. Aviram, N., Schinzel, S., Somorovsky, J., Heninger, N., Dankel, M., Steube, J., Valenta, L., Adrian, D., Halderman, J.A., Dukhovni, V., et al.: Drown: Breaking tls using sslv2. In: USENIX Security Symposium. pp. 689–706 (2016)
8. Axon, L., Alahmadi, B., Nurse, J.R., Goldsmith, M., Creese, S.: Sonification in security operations centres: what do security practitioners think? Internet Society (2018)
9. Bonneau, J., Schechter, S.: Towards reliable storage of 56-bit secrets in human memory. In: 23rd USENIX Security Symposium (USENIX Security 14). pp. 607–623 (2014)
10. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., et al.: The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228 (2018)
11. Chen, C.M., Wang, K.H., Wu, T.Y., Pan, J.S., Sun, H.M.: A scalable transitive human-verifiable authentication protocol for mobile devices. Information Forensics and Security, IEEE Transactions on 8(8), 1318–1330 (2013)
12. Chow, Y.W., Susilo, W., Au, M.H., Barmawi, A.M.: A visual one-time password authentication scheme using mobile devices. In: International Conference on Information and Communications Security. pp. 243–257. Springer (2014)

13. Diffie, W., Hellman, M.E.: New directions in cryptography. Information Theory, IEEE Transactions on 22(6), 644–654 (1976)
14. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing 38(1), 97–139 (2008)
15. Ellison, C., Dohrmann, S.: Public-key support for group collaboration. ACM Transactions on Information and System Security (TISSEC) 6(4), 547–565 (2003)
16. Farb, M., Burman, M., Chandok, G.S., McCune, J., Perrig, A.: Safeslinger: An easy-to-use and secure approach for human trust establishment. Tech. rep., DTIC Document (2012)
17. FIPS, P.: 197. Advanced encryption standard (AES) 26 (2001)
18. Forte, A.G., Garay, J.A., Jim, T., Vahlis, Y.: Eyedecrypt—private interactions in plain sight. In: International Conference on Security and Cryptography for Networks. pp. 255–276. Springer (2014)
19. Franklin, J., Luk, M., Seshadri, A., Perrig, A.: Prism: enabling personal verification of code integrity, untampered execution, and trusted i/o on legacy systems or human-verifiable code execution. CyLab p. 41 (2007)
20. Gentry, C.: A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University (2009)
21. Gibbs, M.D.: Biometrics: body odor authentication perception and acceptance. ACM SIGCAS Computers and Society 40(4), 16–24 (2010)
22. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing 17(2), 281–308 (1988)
23. Gómez, D.M., Berent, I., Benavides-Varela, S., Bion, R.A.H., Cattarossi, L., Nespor, M., Mehler, J.: Language universals at birth. Proceedings of the National Academy of Sciences 111(16), 5837–5841 (2014), http://www.pnas.org/content/111/16/5837
24. Goodrich, M.T., Sirivianos, M., Solis, J., Tsudik, G., Uzun, E.: Loud and clear: Human-verifiable authentication based on audio. In: Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on. pp. 10–10. IEEE (2006)
25. Gosain, D., Sajwan, M.: Aroma tells a thousand pictures: digital scent technology a new chapter in it industry. Int. J. Curr. Eng. Tech 4, 2804–2812 (2014)
26. Gritzalis, D.A.: Principles and requirements for a secure e-voting system. Computers & Security 21(6), 539–556 (2002)
27. Gritzalis, D.A.: Secure electronic voting, vol. 7. Springer Science & Business Media (2012)
28. Halunen, K., Latvala, O.M., Karvonen, H., Häikiö, J., Valli, S., Federley, M., Peltola, J.: Human verifiable computing in augmented and virtual realities. White paper, http://www.vtt.fi/inf/julkaisut/muut/2017/human-verifiable-computing-white-paper.pdf (2017)
29. Hou, Y.C.: Visual cryptography for color images. Pattern recognition 36(7), 1619–1629 (2003)
30. Hsiao, H.C., Lin, Y.H., Studer, A., Studer, C., Wang, K.H., Kikuchi, H., Perrig, A., Sun, H.M., Yang, B.Y.: A study of user-friendly hash comparison schemes. In: Computer Security Applications Conference, 2009. ACSAC'09. Annual. pp. 105–114. IEEE (2009)
31. Ito, R., Kuwakado, H., Tanaka, H.: Image size invariant visual cryptography. IEICE transactions on fundamentals of electronics, communications and computer sciences 82(10), 2172–2177 (1999)

32. Jinno, Y., Tsuchiya, T., Ohki, T., Takahashi, K., Ogata, W., Nishigaki, M.: 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)
33. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Annual international cryptology conference. pp. 293–308. Springer (2005)
34. Karro, J., Wang, J.: Towards a practical, secure, and very large scale online election. In: Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual. pp. 161–169. IEEE (1999)
35. King, J., Dos Santos, A.: A user-friendly approach to human authentication of messages. In: International Conference on Financial Cryptography and Data Security. pp. 225–239. Springer (2005)
36. Koblitz, N., Menezes, A.: Another look at security definitions. Advances in Mathematics of Communications 7(1), 1–38 (2013)
37. Koblitz, N., Menezes, A.J.: Another look at" provable security". Journal of Cryptology 20(1), 3–37 (2007)
38. Kremer, S., Ryan, M., Smyth, B.: Election verifiability in electronic voting protocols. In: European Symposium on Research in Computer Security. pp. 389–404. Springer (2010)
39. Kumar, A., Saxena, N., Tsudik, G., Uzun, E.: A comparative study of secure device pairing methods. Pervasive and Mobile Computing 5(6), 734–749 (2009)
40. Kutyłowski, M., Zagórski, F.: Scratch, click & vote: E2e voting over the internet. In: Towards trustworthy elections, pp. 343–356. Springer (2010)
41. Lantz, P., Johansson, B., Hell, M., Smeets, B.: Visual cryptography and obfuscation: A use-case for decrypting and deobfuscating information using augmented reality. In: Financial Cryptography and Data Security, pp. 261–273. Springer (2015)
42. Latvala, O.M., Peng, C., Honkamaa, P., Halunen, K.: "speak, friend, and enter" - secure, spoken one-time password authentication. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). pp. 1–5 (Feb 2018)
43. Lin, Y.H., Studer, A., Chen, Y.H., Hsiao, H.C., Kuo, L.H., McCune, J.M., Wang, K.H., Krohn, M., Perrig, A., Yang, B.Y., et al.: Spate: small-group pki-less authenticated trust establishment. IEEE Transactions on Mobile Computing 9(12), 1666–1681 (2010)
44. Lindsey, D.T., Brown, A.M.: World color survey color naming reveals universal motifs and their within-language diversity. Proceedings of the National Academy of Sciences 106(47), 19785–19790 (2009), http://www.pnas.org/content/106/47/19785
45. Mancuso, V.F., Greenlee, E.T., Funke, G., Dukes, A., Menke, L., Brown, R., Miller, B.: Augmenting cyber defender performance and workload through sonified displays. Procedia Manufacturing 3, 5214–5221 (2015)
46. Marie, C., Kujala, T., Besson, M.: Musical and linguistic expertise influence preattentive and attentive processing of non-speech sounds. Cortex 48(4), 447 – 457 (2012), http://www.sciencedirect.com/science/article/pii/S0010945210002881
47. Mayrhofer, R., Gellersen, H.: Shake well before use: Authentication based on accelerometer data. In: Pervasive computing, pp. 144–161. Springer (2007)
48. Mayrhofer, R., Welch, M.: A human-verifiable authentication protocol using visible laser light. In: Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. pp. 1143–1148. IEEE (2007)

49. McCune, J.M., Perrig, A., Reiter, M.K.: Seeing-is-believing: Using camera phones for human-verifiable authentication. In: Security and privacy, 2005 IEEE symposium on. pp. 110–124. IEEE (2005)
50. McCune, J.M., Perrig, A., Seshadri, A., van Doorn, L.: Turtles all the way down: Research challenges in user-based attestation. Tech. rep., DTIC Document (2007)
51. Mitrou, L., Gritzalis, D., Katsikas, S.: Revisiting legal and regulatory requirements for secure e-voting. In: Security in the Information Society, pp. 469–480. Springer (2002)
52. Naor, M., Shamir, A.: Visual cryptography. In: Advances in Cryptology—EUROCRYPT'94. pp. 1–12. Springer (1995)
53. Nishigaki, M., Yamamoto, T.: Making use of human visual capability to improve information security. In: Availability, Reliability and Security, 2009. ARES'09. International Conference on. pp. 990–994. IEEE (2009)
54. Nithyanand, R., Saxena, N., Tsudik, G., Uzun, E.: Groupthink: usability of secure group association for wireless devices. In: Proceedings of the 12th ACM international conference on Ubiquitous computing. pp. 331–340. ACM (2010)
55. Peeters, R., Hermans, J., Maene, P., Grenman, K., Halunen, K., Häikiö, J.: n-auth: Mobile authentication done right. In: Proceedings of the 33rd Annual Computer Security Applications Conference. pp. 1–15. ACM (2017)
56. Perrig, A., Song, D.: Hash visualization: A new technique to improve real-world security. In: International Workshop on Cryptographic Techniques and E-Commerce. pp. 131–138 (1999)
57. Prasad, R., Saxena, N.: Efficient device pairing using "human-comparable" synchronized audiovisual patterns. In: Applied Cryptography and Network Security. pp. 328–345. Springer (2008)
58. Rajaniemi, H.: The Quantum Thief. St. Martin's Press (2012)
59. Regier, T., Kay, P.: Language, thought, and color: Whorf was half right. Trends in Cognitive Sciences 13(10), 439 – 446 (2009), http://www.sciencedirect.com/science/article/pii/S1364661309001454
60. Regier, T., Kay, P., Khetarpal, N.: Color naming reflects optimal partitions of color space. Proceedings of the National Academy of Sciences 104(4), 1436–1441 (2007), http://www.pnas.org/content/104/4/1436
61. Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z., Chen, K.: Sharing multiple secrets in visual cryptography. Pattern Recognition 40(12), 3633–3651 (2007)
62. Thorpe, J., van Oorschot, P.C., Somayaji, A.: Pass-thoughts: Authenticating with our minds. In: Proceedings of the 2005 Workshop on New Security Paradigms. pp. 45–56. NSPW '05, ACM, New York, NY, USA (2005), http://doi.acm.org/10.1145/1146269.1146282
63. Varshavsky, A., Scannell, A., LaMarca, A., De Lara, E.: Amigo: Proximity-based authentication of mobile devices. Springer (2007)
64. Vickers, P., Laing, C., Fairfax, T.: Sonification of a network's self-organized criticality for real-time situational awareness. Displays 47, 12–24 (2017)
65. Von Ahn, L., Blum, M., Hopper, N.J., Langford, J.: Captcha: Using hard ai problems for security. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 294–311. Springer (2003)
66. Yao, A.C.: Protocols for secure computations. In: Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on. pp. 160–164. IEEE (1982)