Feeling is Believing: a secure template exchange protocol

Ileana Buhan, Jeroen Doumen, Pieter Hartel, Raymond Veldhuis,
{ileana.buhan, jeroen.doumen, pieter.hartel, r.n.j.veldhuis}@utwente.nl

University of Twente, Enschede, The Netherlands

Abstract. We use grip pattern based biometrics as a secure side channel to achieve pre-authentication in a protocol that sets up a secure channel between two hand held devices. The protocol efficiently calculates a shared secret key from biometric data. The protocol is used in an application where grip pattern based biometrics is used to control access to police hand guns.
Key Words: Ad-hoc authentication, fuzzy cryptography, biometrics;

1 Introduction

We are developing smart guns with grip pattern biometrics [11] for the police, to reduce the risk of officers being shot with their own weapon in case of a take away situation [7]. In this scenario a police handgun authenticates the owner by grip pattern biometrics integrated with the grip of the gun. Police officers often work in teams of two and each officer must be able to fire the other officer's weapon. Normally, teams are scheduled in advance so that appropriate templates can be loaded into the weapons at the police station. However, in emergency situation this is not possible; in this case police officers have to team up unprepared and exchange templates in the field. Biometric data is sensitive information thus during the exchange the templates must be protected. Officers may work with colleagues from other departments, even from neighboring countries, so a shared key, or a public key infrastructure where the certificate associated with these keys must be verifiable on-site is not realistic. Also, one cannot expect a police officer to perform some complicated interfacing operation with his gun in the field.

In this paper we present a solution that is both simple and effective. Each police officer owns a gun, that holds the owners stored biometric grip pattern template and is equipped with a grip pattern sensor and a short range radio. The users swap the devices, so that each device can measure the grip pattern of the other user. The devices are then returned to their owners. Each device now contains a genuine template of its owner and a measurement of the other user, called guest. The devices calculate a common key from the owner's template and the guest measurement. The act of the guest putting her hand on the user's device corresponds to sending a message on a secure side channel. Therefore, we have termed our protocol Feeling is Believing (FiB).

Securing the exchange of biometric templates is an instance of the *pairing problem*. As described by Saxena [9] the *pairing problem* is to enable two devices, which share no prior context, to agree upon a security association that they can use to protect their subsequent communication. Secure pairing must be resistant to a man-in-the-middle adversary who tries to impersonate one or both of these devices in the process. To

achieve secure pairing one cannot rely on any previously shared secret information. This problem can be solved in cryptography by the issue of certificates. As said before, due to the ad-hoc nature of the pairings we cannot rely on an existing communications channel to a certification authority that could validate certificates. Our approach is to use an additional physically authenticated side channel which is governed by humans.

Related Work Balfanz *et al.*[9] propose physical contact between devices. This type of channel has the property that the user can control precisely which devices are communicating. The authors extend this approach to location limited channels where they propose short range wireless infrared communication where the secret information is communicated when devices are in the line of sight. McCune *et al.* [6] propose to use a visual channel and make photographs of the hash codes of the public keys. This represents a major breakthrough especially from the point of user friendliness. In the same line of work, Googrich *et al.* [4] propose a human assisted authentication audio channel as a secure side channel. They use a text to speech engine for vocalizing a sentence derived from the hash of a device's public key. The pre-authentication channel is used mostly to authenticate public-keys. The hash of the public key is either vocalized [4] or photographed [6]. Others [12,10], use a Diffie-Hellman like key agreement scheme where short sequences transmitted on the private channel authenticate the key sent on the main channel. Our protocol is a Diffie-Hellman like protocol in the sense that both parties equally contribute to the session key. FiB achieves mutual authentication and the partial keys are extracted from the biometric identification data of the individual.

Contribution FiB can perform secure biometric template exchange in an ad-hoc situation, its main merit being user friendliness. We stress that the application domain for FiB is more general than the gun application. FiB can securely exchange template for any type of biometric system. FiB is formally verified to prove the security and origin authentication of templates. The workload of an intruder who is trying to guess the session key is evaluated in 9 different scenarios. To the best of our knowledge, this is the first time that a biometric is used as a location limited channel. Using biometrics and cryptography together brings up challenges. Biometric data is usually noisy. However the noise is not reproducible or uniformly random thus cryptography algorithms have difficulties in adjusting to this noise. We propose a new method for correcting errors in the keys generated from biometric data using a user specific error profile.

2 FiB Protocol Description

FiB solves the problem of secure template exchange and provide a solution for securing the ad-hoc transfer of private information between mobile, biometrically enabled devices in a scenario where no pre-distributed keys are available. The main threat is an intruder loading his template into one of the participating devices. Thus, we require the authorization of the device owner before his template is transferred. To preserve the privacy of the biometric template, it must be encrypted before being sent out.

Fuzzy Key Extraction. Before we turn to the protocol, we introduce the main tool. A fuzzy extractor as defined by Dodis *et al.* [1] is a public function that extracts robustly a binary sequence K from a noisy measurement F with the help of some public string H. Enrollment is performed by a function $\texttt{Gen}$, which on the input of the noise free biometric T and the chosen binary string K will compute a public string $H = \texttt{Gen}(T, K)$. During authentication, a second function $\texttt{Reg}$ takes as input a noisy measurement F and the public string H and outputs a binary string $K' = \texttt{Reg}(F, H)$. In a perfect world, $K' = K$ but in reality they might be slightly different. However, we expect that keys are close in terms of their Hamming distance when T and F are similar enough. Both T and F are multidimensional feature vectors and while for most of the features the authentication will work correctly, for some feature the noise might be too large. We write $K' = K + e$, where we assume that the Hamming weight of the error e, denoted with $\texttt{wt}(e)$ satisfies $\texttt{wt}(e) \leq t, 0 \leq t \ll n$.

FiB Protocol preliminaries Before we delve into the description of the protocol, which represents the core of our solution, we describe the context. Enrollment of users takes place before the protocol starts. During enrollment a low noise measurement T is taken, for each user. A key K of length n is generated and function $\texttt{Gen}$(T,K) outputs the helper data H. Then the user specific error profiles E is computed. The error profile is used by the protocol to lower the error rates of the biometric system, see subsection 4. This information is loaded into the device of the user. After the enrollment we have achieved that: (1) the identity of the user can be verified by his own device, and (2) a device is prepared to run the FiB protocol which allows secure template transfer so that *another device* can verify the identity of the user.

The Protocol. The principals that interact during the protocol are two devices D_a and D_b. Before the protocol starts each device knows the data of its owner, i.e. the template, the helper data constructed from the template, the key and the error profile. Hence initially D_a knows $\{T_a, H_a, K_a, E_a\}$ and D_b knows $\{T_b, H_b, K_b, E_b\}$. The message flow of the FiB protocol is shown in Figure 1. By $K'_a||K'_b$ we mean a combination of K'_a and K'_b, for example concatenation.

Actions of device D_a (Initiator). We assume that D_a starts the protocol. When an unknown grip pattern is detected, D_a broadcasts its helper data H_a on the wireless channel. H_a is constructed such that it does not reveal any significant information about T or K. Upon receiving message 4 from D_b, D_a uses the received H_b and F_b to extract $K_b^{'}$. The second part of the message is used to help D_a recover $K_a^{'}$. Since K_a and K'_a are close, D_a can use the error profile E_a to recover K'_a by flipping carefully chosen bits in K_a until it can successfully decrypt $\{F_a\}_{K_a^{'}}$. Since D_a can recognize a measurement coming from its own user, D_a can check the decryption results. When D_a successfully finds $K_a^{'}$ it sends message 7 to D_b. D_a verifies in step 11 that T_b matches the measurement received on the secure side channel in step 1.

Actions of device D_b (Responder). Device D_b receives H_a and detects an unknown grip pattern, F_a. The rest of the operations are similar to those of D_a. Both participants have to perform the same amount of computation.

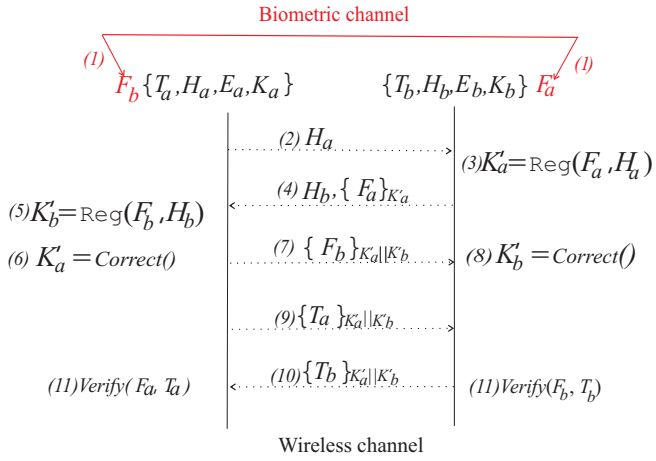

Fig. 1. *FiB protocol.*

FiB is a solution that offers confidentiality during data transfer and authentication. However, FiB does not guarantee what happens to the templates *after* the protocol ends. We emphasize that loading a template into ones device is similar to handing over a key to the device. At any time the owner of the template can access that device. In the scenario of the smartgun we assume that the sensitive information is stored in a tamper resistant storage environment where the templates cannot be ”taken out”.

3 Security evaluation for FiB protocol

There are two distinct, rigorous views of cryptography that have been developed over the years. One is a formal approach where cryptographic operations are seen as black box functions represented by symbolic expressions and their security properties are modelled formally. The other is based on a detailed computational model where cryptographic operations are seen as strings of bits and their security properties are defined in terms of probability and computational complexity of successful attacks. In the following we look at both aspects of security.

3.1 Formal verification of the FiB protocol with CoProVe

We have formally verified that FiB satisfies secrecy of the templates and mutual authentication. The adversary, named Eve, is a Dolev-Yao [3] intruder that has complete control of the communication channel. She can listen to, or modify messages on the main communication channel between the devices but cannot access the secure side channel. The tool used for this purpose is the constraint based security protocol verifier CoProVe by Corin and Etalle [2]. An earlier version of the protocol was verified and found buggy, the published version of the protocol above fixes the flaw found. A (security) protocol is normally verified using a model of the protocol, to avoid getting

bogged down in irrelevant detail. The quality of the model then determines the accuracy of the verification results. The basic difference between a protocol and a model lies in the assumptions made when modelling the protocol. We believe that the following assumptions are realistic:

1. *No biometric errors* We assume that the correction mechanism always works perfectly and thus the initiator knows the key used by the sender. Thus, we look only at complete protocol rounds. When the initiator cannot work out the key the protocol is aborted. In this case we assume that Eve cannot work out the key either.
2. *Modelling the secure side channel* We assume that when the protocol starts device D_a knows F_a and device D_b knows F_b while Eve knows neither because she cannot eavesdrop on the secure side channel.
3. *Classifier based verification in step 11 removed.* Because systems without an equational theory such as CoProVe cannot compare two terms, the last check before accepting a template cannot be modelled. This check prevents an intruder modifying messages 9 and 10 in the protocol.

We have verified the model in figure 1 with the assumptions above. We argue that the above abstractions do not affect the secrecy and the authentication property. Verification with CoProVe explores a scenario in which one of the parties involved in the protocol plays the role of the initiator (i.e. the party staring the protocol) and the other plays the role of the responder. A third party, the intruder learns all message exchanged by the initiator and the responder. The intruder can devise new messages and send them to honest participants as well as replay or delete messages. Should the intruder learn a secret key and a message encrypted with that key, then the intruder also knows the message. This is the classical Dolev-Yao intruder [3].
We have explored two scenarios that we believe to be realistic and representative for real attacks. In the first scenario two honest participants Alice and Bob are plagued by a powerful intruder who is assumed to know T_b (because the intruder might have communicated with Bob in a previous session).

In the scenario the intruder tries to load her own template T_i into D_a so as to be able to fire weapon T_a. This impersonation attack is found to be impossible by CoProVe under the assumption that the intruder does not know F_a or T_a. This is a realistic assumption since these are not transmitted in clear and the key used to encrypt is computed from data sent over the secure side channel. Verification thus shows that the intruder cannot impersonate D_b even though the intruder has knowledge of T_b.

In the second scenario one participant, Alice, has to deal with the intruder, who does not have useful initial knowledge. This scenario represents the case that Alice's device was stolen and the intruder tries to load his template into Alice's device and use it. Verification shows that T_a remains secret when Alice is the initiator of the protocol. This means that an intruder cannot trick Alice into disclosing her template data if she does not provide the intruder a sample of her biometric data. When Alice is the responder and the intruder has full access to the device (i.e. the intruder can submit his own biometric data), T_a will not be disclosed. This is because before the device sends anything useful on the wireless link the device will check whether his owner is there after step 3.

As a result in both scenarios we have verified the security and authentication authentication of responder to the initiator and authentication of initiator to responder.

3.2 Intruder's computational effort of guessing $K'_a||K'_b$.

To derive keys from fuzzy data we use a semi-known plain text attack in steps 6 and 8, to recover the session key. This approach can raise a couple of natural questions: "If both Alice (device D_a) and Bob (device D_b) have to guess the session key, how much more difficult is for Eve (the intruder) to do the same?", "What happens if Eve already knows the templates of Alice and or Bob?", "What kind of guarantees is this protocol offering?" To answer these questions we study the following scenarios:

AE(0) No previous contact between Alice and Eve.
AE(1) Eve records a measurement of Alice's biometric.From the helper data sent out in the clear Eve constructs K''_a.
AE(2) Eve had a protocol run with Alice and knows T_a and Eve can construct K_a.

We denote by $W(x \rightarrow y)$ the average number of trials that Eve, has to do to guess y when she knows x using the best guessing strategy. We analyze Eve's workload to guess K'_a in the three scenarios above.
In scenario $AE(2)$, Eve knows K_a and has to guess $K'_a = K_a + e$ where $\mathtt{wt}(e) \leq t$. Since Eve has no information about the noise distribution, she has to correct up to t errors. As the key length is n, there are $\binom{n}{i}$ different error patterns if the actual number of errors is i, thus on average she will have to guess:

$$W(K_a \rightarrow K'_a) \approx \frac{1}{2}\sum_{i=0}^{t}\binom{n}{i} + \frac{1}{2}.$$

In scenario $AE(1)$, Eve knows K''_a and has to guess K'_a where $K''_a = K_a + e'$, thus $K''_a = K'_a + e' + e$. Since $\mathtt{wt}(e' + e) \leq 2t$, Eve has workload:

$$W(K''_a \rightarrow K'_a) \approx \frac{1}{2}\sum_{i=0}^{2t}\binom{n}{i} + \frac{1}{2}.$$

In scenario $AE(0)$ Eve has no information on Alice thus she has to brute force all possibilities. Thus the number of trials is approximately:

$$W(0 \rightarrow K'_a) \approx \frac{2^n + 1}{2}.$$

Scenarios for Bob are analogous:

BE(0) No previous contact between Bob and Eve.
BE(1) Eve records a measurement of Bob.
BE(2) Eve had a previous round with Bob thus knows T_b and can construct K_b.

Eve's workload for guessing K'_b is equal to guessing K'_a in the analogous scenario. To achieve her goal of loading her template in one of the devices, Eve has to guess $K'_a||K'_b$ in all scenarios. Table 1 summarizes her workload. In each row we have the information that Eve knows about Bob and in the column the information that Eve knows about Alice. Due to the message flow in the protocol (see figure 1), Eve might

Table 1. *Guesswork required for Eve to compute the session key*

	AE(0)	AE(1)	AE(2)
BE(0)	$W(0 \to K'_a) \cdot W(0 \to K'_b)$	$W(K''_a \to K'_a) + W(0 \to K'_b)$	$W(K_a \to K'_a) + W(0 \to K'_b)$
BE(1)	$W(0 \to K'_a) \cdot W(K''_b \to K'_b)$	$W(K''_a \to K'_a) + W(K''_b \to K'_b)$	$W(K_a \to K'_a) + W(K''_b \to K'_b)$
BE(2)	$W(0 \to K'_a) \cdot W(K_b \to K'_b)$	$W(K''_a \to K'_a) + W(K_b \to K'_b)$	$W(K_a \to K'_a) + W(K_b \to K'_b)$

have an advantage if she has information about Alice. Eve can intercept message (4), $\{F_a\}_{K'_a}$ and recover K'_a if the biometrics allows for taking a decision on whether two measurements come from the same individual. This explains the plus sign between the work of guessing K'_a and the work of guessing K'_b in the columns where Eve has some knowledge about Alice. We can estimate an upper bound for the work load of Alice and Bob according to Pliam's [8] equation:

$$W_{Alice}(K_a \to K'_a) \leq \frac{1}{2}(\sum_{i=0}^{t} \binom{n}{i} + 1) - \frac{1}{2} \sum_{i=0}^{t} \binom{n}{t} \cdot \sum_{j=1}^{n} |E_j(\sigma, q) - \frac{1}{2^n}|.$$

Here $E_j(\sigma, q)$ represents the distribution of the noise, which is described below. The best case scenario for Eve, however unlikely, is [BE(2),AE(2)] when she had a previous round with both Alice and Bob. Even though she has both K_a and K_b her workload is at least twice as high compared to Alice or Bob. Moreover while for Eve all error patterns are equally likely, Alice and Bob have the error profile that makes recovery faster.

4 Experimental validation with real life data

The *Correct* function used during the FiB protocol uses a semi-known plain text attack to recover the key. We link the keys used in the protocol to the biometric data of a user using the template protection scheme proposed by Linnartz and Tuyls [5]. The purpose of using this function is to lower the error rate of the system by flipping bits on the result of function `Reg` in the order defined by the user specific user profile E.

Key search algorithm In classical symmetric cryptography to decrypt a message encrypted with a key K one must posses K. In particular, with a key K' that differs only in one bit from K, decryption will fail. The FiB protocol uses this apparent disadvantage of symmetric key cryptography as an advantage: K' is used to form the session key. The noise of the measurements is used as random salt [13] for the session key. The key search algorithm makes it possible to recover K'. We start the key search by assuming there are no errors in $K^{'}$, and we use $K^{'}$ for decryption. If decryption fails we assume that we have a one bit error. We start flipping one bit of the key according to the position indicated by the error profile, until we have exhausted the error profile. Then we assume that two bits are wrong and we try all combinations of two bits from the error profile. Finally if we reach the limit on the number of trials we assume that the key is coming from an intruder. The recovery of K' is a semi-known plain text attack.

When the correct value of $K^{'}$ is discovered the initiator will recognize the message encrypted with $K^{'}$. This is possible since the encrypted message is a biometric template. The initiator of the protocol possesses a fresh measurement of this template and hence is able to recognize a correct match. The verification is performed by a classifier based matching algorithm designed for this particular biometrics.

Error profile computation Linnartz et *al.* [**?**] propose a multiple quantization level system with odd-even bands. The embedding of binary data is done by shifting the template distribution to the center of the closest even-odd q interval if the value of the key bit is a 1, or to the center of an odd-even q interval if the value of the key bit is a 0. The calculation $\texttt{Gen}(t_i, k_i) = h_i$ proceeds component wise as follows, where $i = 1, n$:

$$\texttt{Gen}(t_i, k_i) = h_i = \begin{cases} (2p + \frac{1}{2}) \cdot q - t_i, & k_i = 1 \\ (2p - \frac{1}{2}) \cdot q - t_i, & k_i = 0. \end{cases}$$

where $p \in \mathbb{Z}$ is chosen such that $h_i \leq 2q$. During authentication the key is recovered by computing:

$$\texttt{Reg}(f_i, h_i) = \begin{cases} 1, & 2pq \leq f_i + h_i < (2p+1)q \\ 0, & (2p-1)q \leq f_i + h_i < 2pq. \end{cases}$$

However, during `Reg` whenever the difference between the measured f_i value and the template t_i is greater than $\frac{q}{2}$ we get an error in the key computation. Each key bit is extracted independently. Thus, the error profile is a vector of length n. The i-th value of the error profile represents the probability of the i-th key bit to be computed wrongly. We assume that the features are independent and normally distributed. The error profile is computed component-wise, using the function:

$$E_i(\sigma, q) = \sigma\ 2\sqrt{2} \sum_{i=0}^{\infty} \int_{\frac{(1+4i)}{2\sqrt{2}}\frac{q}{\sigma}}^{\frac{(3+4i)}{2\sqrt{2}}\frac{q}{\sigma}} e^{-x^2} dx \approx \sigma\ 2\sqrt{2} \int_{\frac{q}{\sigma\ 2\sqrt{2}}}^{\frac{3q}{\sigma\ 2\sqrt{2}}} e^{-x^2} dx,$$

During enrollment several different measurement have to be made for each user. The error profile is based on the fact that in practical situations the estimated standard deviation is different for different user. To compute the error profile we use the same data after dimensionality reduction that the classifier based matcher use.

Results. We implemented the key extraction described above. We wanted to see the influence of the correction mechanism on the overall error rates. The evaluation is performed on real life grip pattern biometric data collected from 41 police officers. A detailed description of this biometric can be found in Veldhuis *et al.* [11]. Each of the 41 officers contributed 25 different measurements. Approximately 75% of these samples(18), are used for training the algorithm and 25% (7) are used for testing. First, we reduce the dimensionality of the data to 40 independent features. For training and testing we use the same data that is used for verification by the classifier based recognition algorithm.Second, we embed the key bits using Linnartz and Tuyls scheme above. Figures 2 presents the results obtained from the collected data. We offer three conclusions

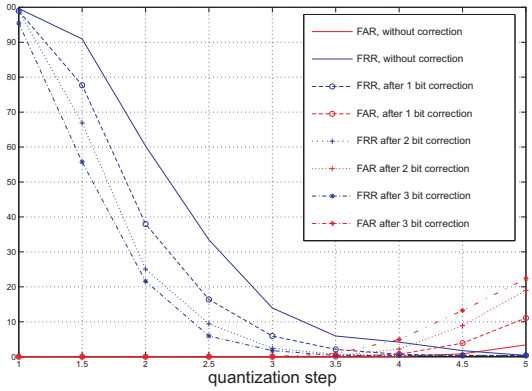

Fig. 2. Results on grip pattern data.

from this evaluation. The first conclusion is, as expected, the larger the quantization step the lower the FRR but the higher the FAR. We tested 8 different values for q, ranging from 1 to 5 in increments of 0.5. We did not try larger values for q because the FAR becomes unacceptably large. The second conclusion is that the influence of the correction algorithm is significant. For example for $q = 3$, without correction the FRR=13.93% and the FAR=0%. When we correct 1 bit the FRR goes down to 5.92%, while the FAR retains the same value 0%. After correcting 2 bits the FRR goes down to 2.43% while the FAR remains equal to 0%. Correcting 3 bits further reduces the FRR to 1.74% while the FAR increases only slightly to 0.07%. The third conclusion is that the correction mechanism is stable, meaning that the effect of correction is independent of the time when data in collected. Data was collected during two sessions and the performance of the correction algorithm is similar on both sets.

5 Conclusions

The contributions of this paper are threefold. Firstly, we propose FiB a protocol that can exchange biometric templates securely even though no prior security association exists between the participants. We are confident in the guarantees offered by FiB because we formally verify the protocol to prove security and origin authentication. Also, from the information theoretic point of view the workload of Eve is at least double of that of Alice or Bob in the unlikely scenario where Eve has interacted with Alice and Bob and where Eve possess the same key material. Moreover, in this case the biometric has to be favorable to Eve in that she has to be able to verify wheatear two noisy measurements are coming from the same user or not. Secondly, for the first time we propose to use biometrics as a secure side channel. The advantage of using biometrics compared to any other types of side channels is the extreme user friendliness. Thirdly, a new correction mechanism for correcting biometric errors based on user specific error profile is proposed. We present an evaluation of the performance in terms of FAR and FRR and we show that the correction algorithm significantly improves the overall results. Our

experiments show that by correcting only 1 bit in the overall key the FRR is reduced by approximately 50% while the FAR is not increased significantly. We believe that our approach can be applied to other types of biometrics.

6 Acknowledgements

The authors would like to thank Ricardo Corin and Sandro Etalle for helping formally verify the protocol using CoProVe.

References

1. X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith. Secure remote authentication using biometric data. In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 147–163. Berlin: Springer-Verlag, 2005.
2. R. Corin and S. Etalle. An improved constraint-based system for the verification of security protocols. In *9th Int. Static Analysis Symp. (SAS), Madrid, Spain*, volume LNCS 2477, pages 326–341, Berlin, September 2002. Springer-Verlag.
3. D. Dolev and A.Yao. On the security of public key protocols. *Information Theory, IEEE Transactions on*, 29:198– 208, 1983.
4. M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human-verifiable authentication based on audio. In *26th IEEE International Conference on Distributed Computing Systems (ICDCS 2006), 4-7 July 2006, Lisboa, Portugal*, page 10. IEEE Computer Society, 2006.
5. J.P Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *Audio-and Video-Based Biometrie Person Authentication, 4th International Conference, AVBPA 2003, Guildford, UK, June 9-11, 2003 Proceedings*, volume 2688, pages 393–402, 2003.
6. J. McCune, A. Perrig, and M. Reiter. Seeing-is-believing: using camera phones for human-verifiable authentication. *Security and Privacy, 2005 IEEE Symposium on*, pages 110–124, 2005.
7. NJIT. Personalized weapons technology project, progress report. Technical report, New Jersey Institute of Technology, April, 2001.
8. J. O. Pliam. Guesswork and variation distance as measures of cipher security. In *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*. Springer, 2000.
9. N. Saxena, J.Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel (short paper). *SP*, 0:306–313, 2006.
10. S. Vaudenay. Secure communications over insecure channels based on short authenticated strings. *Lecture Notes in Computer Science*, 3621:309 – 326, Nov 2005.
11. R.N.J. Veldhuis, A.M. Bazen, J.A. Kauffman, and P.H. Hartel. Biometric verification based on grip-pattern recognition. In *Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose, California, USA, January 18-22, 2004, Proceedings*, volume 5306 of *Proceedings of SPIE*, pages 634–641. SPIE, 2004.
12. F.L. Wong and F. Stajano. Multi-channel protocols for group key agreement in arbitrary topologies. In *4th IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2006 Workshops), 13-17 March 2006, Pisa, Italy*, pages 246–250. IEEE Computer Society, 2006.
13. T. D. Wu. The secure remote password protocol. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 1998, San Diego, California, USA*. The Internet Society, 1998.