Rational authentication protocols

Long H. Nguyen
Oxford University Computing Laboratory

***Abstract*—We use ideas from game theory to transform two families of authentication protocols so that even an intruder attacks a protocol, its payoff will still be lower than when it does not. This is particularly useful in resisting or discouraging a powerful and *rational* intruder (as present in military applications) who makes many attempts to break a protocol because (1) even the intruder fails, a denial of service attack is still mounted successfully, and (2) in a password-based protocol, the chance of a successful attack increases quite significantly as more and more attempts are launched to guess the password.**

I. Introduction

Ideas from game theory have been used to design a number of rational secret sharing schemes recently [11], [9], [13], [8], [12]. In such a protocol, each party is initially allocated a share of a secret from a trusted dealer, and the secret can be reconstructed only when a sufficient number of shares are combined together. While parties in rational secret sharing schemes can act on their own interests,[1] i.e. all parties want to learn secret above all but otherwise prefer that no other players learn secret, this notion of players' rationality or self-interest is not applicable in authentication and key-agreement protocols. For example, all trustworthy nodes should always incorporate to complete an authentication protocol successfully instead of being self-interested, because it is in their mutual interest to agree on the same (and possibly public) data.

We instead observe that in a hostile environment, such as military and battle fields, there is always the presence of a powerful intruder who can intercept and modify data transmitted over a high-bandwidth but insecure channel, such as WiFi or the Internet. It is always in the intruder's interest to intervene and attempt to break many protocol runs, i.e. as in game theory the intruder here is *rational* in the sense that he or she always tries to maximise his or her payoff. In other words, the intruder does no worse (and potentially does better) by attacking many protocol runs because:

- With some probability ϵ: his or her attack is successful, and this means that the intruder successfully manages to fool trustworthy parties into, for example, believing corrupt data.[2]
- With probability $1-\epsilon$: his or her attack is not successful, but then at least the intruder has successfully mounted a denial of service attack, and thus has prevented honest parties from agreeing on the same data. In a password-based protocol, an incorrect guess of a short password means that the chance of correctly guessing the password will increase quite significantly in subsequent runs, which further encourages the intruder to mount another attack.

- In many cases, e.g. password-based protocols, we can put a limit k on the number of failed attempts an intruder can make. Under such a circumstance, a rational intruder only quits or stops attacking the protocol when (1) it is successful in the t^{th} attempt where $t \leq k$, or (2) it fails in all k attempts.

These features motivate us to use techniques in game theory to redesign authentication protocols to discourage this kind of rational intruder.

Our main contribution is a general transformation in which we introduce *irrational* behaviours an honest node can pursue under some probability, such that even a dishonest node or the intruder deviates from a run its payoff will still be lower than in an equilibrium where everyone faithfully follows the protocol. In other words, the intruder does not have any incentive to attack a protocol, which is very similar to the concept of Nash equilibrium in game theory. We then demonstrate how this protocol transformation works and benefits two families of authentication protocols, namely password-based authentication (or key agreement) schemes [2], [3], [4] and manual authentication protocols [1], [6], [14], [16], [17], [18], [19], [26], though other cryptographic applications can potentially benefit from our work. We note that our analysis works best with protocols that are immune to (off-line) searching and analysis, i.e. the only way an intruder can gain any advantage is by interacting with or intervening in a protocol. For otherwise, there is no need for a rational intruder to interact and attack a protocol in the way we describe earlier, because most of the work can be done off-line quietly.

In Section II, we present our protocol transformation as well as use it to protect authentication protocols against an intruder who only can attack up to a single protocol run (or a single-run attack). This analysis will be formally extended to deal with multiple-run attacks on both password-based authentication schemes of Section III and manual authentication protocols of Section IV.

While we believe that we are the first to study the notion of including irrational behaviours into honest parties' activities tailored specifically for authentication protocols, such idea can be traced back to earlier work in other context of rational secret sharing protocols. In order to encourage an intruder to give up attacking a protocol, it is probably inevitable that we need to give something,

[1] It is equally important to point out that similar notion of self-interested parties also applies to rational exchange protocols whose concept was introduced by Syverson [25] and subsequently formalised in a game theory model by Buttyán et al. [5]. In a fair exchange, a party accepts to deliver an item iff it receives another item in return, and hence it makes sense for protocol participants to be self-interested.

[2] Both families of authentication protocols considered in this paper have ϵ in the range $[2^{-32}, 2^{-16}]$, which makes a successful attack far more likely than the chance of breaking ciphers or cryptographic hash functions whose security is of order 2^{80} or 2^{160}.

which is less damaging than a successful attack, back to the intruder in each normal run. Both rational secret sharing schemes of Gordon and Katz [11] and Fuchsbauer et al. [9] follow this strategy by allowing a trustworthy dealer to send invalid shares of secret to players at the beginning of some iterations, or forcing honest nodes to proceed in a sequence of fake runs followed by a single real one. Both of these require extra rounds of protocol runs, as in the case in our protocol transformation of Table I.

II. Protocol transformation

For simplicity pairwise authentication schemes are considered, where two trustworthy parties A and B want to authenticate or agree on the same data, though our protocol transformation and analysis can be generalised to group authentication scenarios [19], [27]. In these authentication schemes, it is in the parties' interest to follow the protocol, since both A and B seek to agree on the same data. The job of a rational intruder is to break a protocol run and maximise his or her payoff. No specific protocol is given until multiple-run attacks are considered in subsequent sections, because for single-run attacks our suggested changes in the behaviour of honest parties are independent of the type of authentication protocols whether they are based on passwords [2], [3], [4] or human interactions [1], [17], [18], [19], [26], [27]. These changes, which are summarised in Tables I and II, aim to discourage the intruder from attacking a protocol.

Using the protocol transformation specified in Table I, we arrive at the following theorem.

Theorem 1: *Suppose that an intruder can only attack up to a single run of an authentication protocol and succeed with probability ϵ, then to discourage the intruder from attacking this protocol, this inequality must hold:*

$$\alpha > \frac{\epsilon U^+ + (1-\epsilon)U^-}{U}$$

Proof: If the intruder does not misbehave, his or her expected payoff in each run is αU. If the intruder misbehaves, his or her expected payoff of a single-run attack is $\epsilon U^+ + (1-\epsilon)U^-$. To achieve our aim, we need to find the value of α such that the following inequality holds:

$$\begin{aligned} \alpha U &> \epsilon U^+ + (1-\epsilon)U^- \\ \alpha &> \frac{\epsilon U^+ + (1-\epsilon)U^-}{U} = \frac{U^- + \epsilon(U^+ - U^-)}{U} \end{aligned}$$

So as long as this is true, it is in the intruder's interest not to intervene and manipulate data transmitted in any protocol run. ∎

We observe that no matter how big U^+ is, $\epsilon(U^+ - U^-)$ can be made extremely small relative to U and U^-, e.g. increasing the length of the password or universal hash functions as in protocols of Sections III and IV will exponentially

Protocol transformation

In an authentication protocol where parties seek to agree on the same data, we introduce the following irrational behaviour to resist a rational intruder.

- With probability α: honest party A will authenticate or transmit some useless and random data which might include a random (RSA or Diffie-Hellman) public key pk_A whose corresponding private key is not known to A, so that even when a run is complete and successful, i.e. the intruder does not misbehave, it is a waste of time for the other honest party B to receive and possibly use pk_A to encrypt and transmit confidential data to A.

  When this happens, after a period of time A will initiate another run with B to revoke all useless data agreed in the previous run and to authenticate meaningful data. Since it is in the intruder's interest that A deliberately authenticates useless data, we denote U the intruder's payoff in this case.

- With probability $1-\alpha$: party A faithfully follows the protocol, and thus if the intruder does not misbehave the protocol run will be successful, and there is no payoff for the intruder in this case.

When the intruder intervenes and modifies data transmitted in a protocol run, then regardless of whether A misbehaves or not, there are two possibilities:

- With probability ϵ the intruder's attack is successful and its payoff is U^+.

- With probability $1-\epsilon$ the intruder's attack fails but it will still be given some payoff U^- for stopping A and B agreeing on the same data.

Based on the damages an intruder can cause to honest parties, it is clear that $U^+ \geq U \geq U^-$.

Table I
Protocol transformation.

Intruder attacks	Strategy of party A	Outcome of protocol	Payoff of intruder
No	Faithful	Succeed	0
No	Unfaithful	Succeed	U
Yes	Any	Succeed	U^+
Yes	Any	Fail	U^-

Table II
A summary of the game.

decrease the value of the successful probability ϵ. Hence, the above inequality can be simplified to

$$\alpha > U^-/U$$

We did not specify the range of value of U^- in Table I because when the intruder benefits from a denial of service attack (for stopping parties agreeing on the same data and/or further knowledge of a password) then U^- is probably not too small relative to U. On the other hand, U^- becomes very small or perhaps insignificant if we also consider honest parties' suspicion that an intruder is active after several failed protocol runs.

The above analysis only takes into account single-run attacks, in practice a rational intruder as defined in Section I would attack many protocol runs until (s)he is successful. For this reason, it is desirable that we consider the case of multiple-run attacks on authentication protocols.

III. Multiple-run attacks on password-based protocols

Any secure password-based (authentication or key-agreement) protocol needs to resist off-line searching, i.e. the only way to find out a guess of a password is correct is to interact with the protocol. Our analysis here applies to many secure password-based protocols, but for clarity we give the definition of the Diffie-Hellman-based Encrypted Key Exchange scheme of Bellovin and Merritt [2], [3]. This protocol establishes a shared private key g^{xy}, where g^x and g^y are Diffie-Hellman keys of A and B, from a short password pw using an encryption scheme $E_{pw}()$ and a cryptographic hash function $hash()$. Since passwords are usually very short and unchanged for a period of time, the chance of a successful attack increases quite significantly as more and more attempts are launched to guess the passwords. We stress that this feature of a password-based scheme, which is different from other kinds of authentication protocol, is particularly relevant to our discussion, because it will encourage the intruder to keep guessing the password in many protocol runs until (s)he finally gets it right.

Password-based Encrypted Key Exchange EKE [2], [3]
1. $A \longrightarrow B \ : \ A \parallel E_{pw}(g^x)$
2. $B \longrightarrow A \ : \ E_{pw}(g^y) \parallel hash(sk \parallel 1)$
where $sk = hash(A \parallel B \parallel g^x \parallel g^y \parallel g^{xy})$
3. $A \longrightarrow B \ : \ hash(sk \parallel 2)$

In practice we usually limit the number of failed attempts an intruder can make, e.g. three wrong guesses and the protocol will stop running, and thus we denote k the limit of number of attacks an intruder can launch on a protocol. If a password is randomly selected from $\{1, \ldots, n\}$, then[3] $1 \leq k \leq n$ and the chance of correctly guessing the password the first time is $\epsilon = \epsilon_1 = 1/n$. If an attacker's first guess is incorrect, then the second guess is successful with probability $\epsilon_2 = 1/(n-1)$. For all $k \in \{1, \ldots, n\}$ we have $\epsilon_k = 1/(n-k+1)$. We summarise the intruder's accumulative payoff and probability that (s)he is successful (or unsuccessful) up to k attempts in Table III. We note that these k attempts do not need to be consecutive and can be interleaved with any number of protocol runs which are not attacked by the intruder.

[3]It does not make sense for $k > n$ because there are at most n different values for a password, provided that the password is unchanged throughout the intruder's multiple-run attack.

No. of attempts	Outcome	Probability	Payoff of intruder
1	Succeed	$\epsilon = \epsilon_1 = \frac{1}{n}$	U^+
2	Succeed	$(1-\epsilon_1)\epsilon_2 = \frac{1}{n}$	$U^- + U^+$
3	Succeed	$(1-\epsilon_1)(1-\epsilon_2)\epsilon_3 = \frac{1}{n}$	$2U^- + U^+$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
t	Succeed	$\epsilon_t \Pi_{i=1}^{t-1}(1-\epsilon_i) = \frac{1}{n}$	$(t-1)U^- + U^+$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	Succeed	$\epsilon_k \Pi_{i=1}^{k-1}(1-\epsilon_i) = \frac{1}{n}$	$(k-1)U^- + U^+$
k	Fail	$\Pi_{i=1}^{k}(1-\epsilon_i) = \frac{n-k}{n}$	kU^-

Table III
A summary of the game against a password-based protocol.

To discourage an intruder from attacking a protocol in multiple runs, we use the protocol transformation of Table I. The following theorem demonstrates that as k increases the probability α that honest party A behaves irrationally also goes up but very slowly.

Theorem 2: *Suppose that an intruder is allowed to attack a password-based protocol up to k runs for any $k \in \{1, \ldots, n = 1/\epsilon\}$, and the intruder quits iff (s)he is successful in the t^{th} attempt where $t \leq k$ or fails in all k attempts as seen in Table III. Then to discourage the intruder from attacking the protocol, this inequality must hold:*

$$\alpha > \frac{\epsilon U^+ + (1-\epsilon)U^-}{U} + \left(\frac{U^+ - U^-}{U}\right)\frac{k-1}{n(2n-k+1)}$$

Proof: When an intruder decides to attack a protocol up to k runs, from Table III, the expected (or average) number of protocol runs the intruder intervenes is

$$N = \frac{1}{n} + \frac{2}{n} + \frac{3}{n} + \cdots + \frac{k}{n} + \frac{k(n-k)}{n} = \frac{k(2n-k+1)}{2n}$$

Similarly, the expected accumulative payoff of the intruder's multiple-run attack can be computed as follows

$$\begin{aligned} P &= \frac{U^+}{n} + \frac{U^- + U^+}{n} + \cdots + \frac{(k-1)U^- + U^+}{n} + \frac{k(n-k)U^-}{n} \\ &= \frac{kU^+}{n} + U^-\left[\frac{1}{n} + \frac{2}{n} + \cdots + \frac{k-1}{n} + \frac{k(n-k)}{n}\right] \end{aligned}$$

$$= \frac{kU^+}{n} + \frac{k(2n-k-1)U^-}{2n}$$

Since the payoff an intruder gets from not attacking a protocol in each run is αU, in order to discourage the intruder from attacking a password-based protocol up to k runs, we must have:

$$\begin{aligned}
\alpha UN &> P \\
\alpha &> \frac{kU^+}{nUN} + \frac{k(2n-k-1)U^-}{2nUN} \\
\alpha &> \frac{2U^+}{(2n-k+1)U} + \frac{(2n-k-1)U^-}{(2n-k+1)U} \\
\alpha &> \left(\frac{1}{n} + \frac{k-1}{n(2n-k+1)}\right)\frac{U^+}{U} + \\
&\quad \left(1 - \frac{1}{n} - \frac{k-1}{n(2n-k+1)}\right)\frac{U^-}{U} \\
\alpha &> (\epsilon+\Delta)\frac{U^+}{U} + (1-\epsilon-\Delta)\frac{U^-}{U} \\
\alpha &> \frac{\epsilon U^+ + (1-\epsilon)U^-}{U} + \left(\frac{U^+ - U^-}{U}\right)\Delta
\end{aligned}$$

where $\Delta = \frac{k-1}{n(2n-k+1)}$. ∎

Since $n \geq k \geq 1$, as k increases then so do both Δ and α, and moreover $\epsilon > \Delta \geq 0$. This implies that

- The difference between the bounds for α with respect to single-run (see Theorem 1) and n-run attacks is $\left(\frac{U^+-U^-}{U}\right)\Delta < \epsilon\left(\frac{U^+-U^-}{U}\right)$, which can be made arbitrarily small by exponentially decreasing the value of ϵ, i.e. increasing the password length.
- If this protocol can discourage a k-run attack, then it can also discourage a t-run attack for any $t \leq k$.

IV. Multiple-run attacks on manual authentication protocols

In contrast to password-based schemes, the chance of a successful attack on a manual authentication protocol run remains unchanged regardless of how many times an attack is launched. This property applies to all secure protocols of this type, whether they provide oneway, pairwise or group authentication [19].

Our analysis here applies to every manual authentication protocol, but for clarity we give the pairwise version of the SHCBK protocol of the author [18], [19], [20]. In this scheme, parties A and B want to authenticate their public data $m_{A/B}$ from human interactions to remove the need of passwords, private keys and PKIs. The single arrow ($\longrightarrow$) indicates an unreliable and high-bandwidth link (e.g. WiFi or the Internet) where messages can be maliciously altered, whereas the double arrow ($\Longrightarrow$) represents an authentic and unspoofable channel. The latter is not a private channel (i.e. anyone can overhear it) and it is usually very low-bandwidth since it is implemented by humans, e.g., human conversations, text messages or manual data transfers between devices. $hash()$ and $uhash()$ are cryptographic and universal hash functions. Long random keys $k_{A/B}$ are generated by A/B, and k_A must be kept secret until after k_B is revealed in Message 2. Operators $\|$ and $\oplus$ denote bitwise concatenation and exclusive-or.

A pairwise manual authentication protocol [18], [19], [20]		
1. $A \longrightarrow B$	:	$m_A, hash(k_A)$
2. $B \longrightarrow A$	:	m_B, k_B
3. $A \longrightarrow B$	:	k_A
4. $A \Longrightarrow B$	:	$uhash(k_A \oplus k_B, m_A \parallel m_B)$

To ensure both parties share the same data, the human owners of devices A and B have to compare a short universal hash value of 16–32 bits manually. Since the universal hash key $k_A \oplus k_B$ always varies randomly from one to another run, the probability of a successful attack on a each protocol run ϵ equals the collision probability of the universal hash function.[4]

Definition 1: [7], [22], [24] *An ϵ-almost universal hash function, $uhash : R \times X \rightarrow Y$, must satisfy that for every $m, m' \in X$ $(m \neq m')$: $Pr_{\{k \in R\}}[uhash(k, m) = uhash(k, m')] \leq \epsilon$*

Intuitively the value of α (the probability that party A behaves irrationally as defined in Table I) required to discourage the intruder from attacking a manual authentication protocol in multiple runs should be the same as in a single run of Theorem 1. But we will formally state and prove this result in Theorem 3.

Theorem 3: *Suppose that an intruder is allowed to attack a manual authentication protocol up to k runs for any $k \geq 1$, and the intruder quits iff (s)he is successful in the t^{th} attempt where $t \leq k$ or fails in all k attempts as seen in Table IV. Then to discourage the intruder from attacking the protocol, this inequality must hold:*

$$\alpha > \frac{\epsilon U^+ + (1-\epsilon)U^-}{U}$$

We summarise the intruder's accumulative payoff and probability of success and failure in Table IV.

Proof: When an intruder attacks a protocol up to k runs, from Table III, the expected (or average) number of runs the intruder intervenes in this protocol is:

$$\begin{aligned}
N &= \epsilon + 2\epsilon(1-\epsilon) + \cdots + k\epsilon(1-\epsilon)^{k-1} + k(1-\epsilon)^k \\
&= 1 + (1-\epsilon) + (1-\epsilon)^2 + \cdots + (1-\epsilon)^{k-1}
\end{aligned}$$

The second equality holds because for any integer $t \geq 1$ we have $(1-\epsilon)^t = t(1-\epsilon)^{t-1}\epsilon + (t+1)(1-\epsilon)^t - t(1-\epsilon)^{t-1}$.

[4]We note that our protocol transformation of Table I and the analysis of this section also apply to other manual authentication protocols, including schemes of Vaudenay [26] and Čagalj et al. [6], which do not use a universal hash function.

No. of attempts	Outcome	Probability	Payoff of intruder
1	Succeed	ϵ	U^+
2	Succeed	$\epsilon(1-\epsilon)$	$U^- + U^+$
3	Succeed	$\epsilon(1-\epsilon)^2$	$2U^- + U^+$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
t	Succeed	$\epsilon(1-\epsilon)^{t-1}$	$(t-1)U^- + U^+$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	Succeed	$\epsilon(1-\epsilon)^{k-1}$	$(k-1)U^- + U^+$
k	Fail	$(1-\epsilon)^k$	kU^-

Table IV
A SUMMARY OF THE GAME AGAINST A MANUAL AUTHENTICATION PROTOCOL.

The expected accumulative payoff of the intruder's multiple-run attack can be computed as follows

$$\begin{aligned} P &= \epsilon U^+ + \epsilon(1-\epsilon)(U^- + U^+) + \cdots + \\ &\quad \epsilon(1-\epsilon)^{k-1}((k-1)U^- + U^+) + (1-\epsilon)^k kU^- \\ &= U^+\epsilon\left[1 + (1-\epsilon) + \cdots + (1-\epsilon)^{k-1}\right] + \\ &\quad U^-(1-\epsilon)[\epsilon + 2\epsilon(1-\epsilon) + \cdots + \\ &\quad (k-1)\epsilon(1-\epsilon)^{k-2} + k(1-\epsilon)^{k-1}] \\ &= U^+\epsilon N + U^-(1-\epsilon)N \\ &= N\left[U^+\epsilon + U^-(1-\epsilon)\right] \end{aligned}$$

Since the payoff an intruder gets from following this protocol in each run is αU, in order to discourage the intruder from attacking a protocol in multiple runs, we must have:

$$\begin{aligned} \alpha U N &> P \\ \alpha &> \frac{\epsilon U^+ + (1-\epsilon)U^-}{U} \end{aligned}$$

■

V. CONCLUSIONS AND FUTURE RESEARCH

We have introduced the use of ideas from game theory to redesign two families of authentication protocols, namely password-based authentication and manual authentication protocols, to make them resilient against a powerful and rational intruder. In these protocols, only the intruder and dishonest parties are self-interested and all other trustworthy protocol participants should incorporate to complete a protocol run successfully, since this is in their mutual interest to agree on the same data.

It is also worth to point out that our strategy in transforming these protocols does not require the presence of a trusted third party or a dealer (whether on- or off-line) at any stage of a protocol as usually required in rational secret sharing schemes. All communication channels are public, and there is no need for any assumption on simultaneous broadcast.

While we have explored the notion of rational and powerful intruder in two types of authentication protocols, our work reported here opens the way to a number of new problems. The first set of questions consists of direct extension of the results presented here. For example, the kind of rational intruder considered here might not be present in some applications, and hence can one formally define and model a weaker intruder so that the probability that honest nodes need to behave irrationally can be reduced further? We note that there is no need to use the protocol transformation of Table I in every scenario, instead one can switch it on or off depending on the anticipated level of threat, risk or presence of a powerful intruder in each application. And how relevant the notion of a rational intruder is to other types of authentication protocols which are based on PKIs or long private keys. The second set of questions is more open-ended. As a rational and powerful intruder exists in hostile environment, can one transform other families of cryptographic protocols to make them more resilient against this kind of intruder? Since our protocol transformation works best when protocols are immune to (off-line) searching, can it be relaxed or modified to accommodate a wider variety of possible attacks that are relevant to other cryptographic primitives, including message authentication codes?

REFERENCES

[1] *Simple Pairing White Paper*. See: `www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf`

[2] M. Bellare, D. Pointcheval, and P. Rogaway. *Authenticated Key Exchange Secure against Dictionary Attacks*. Advances in Cryptology – Eurocrypt 2000 LNCS (Springer-Verlag) 1807.

[3] S.M. Bellovin and M. Merritt. *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks*. Proceedings of the IEEE Symposium on Research in Security and Privacy (Oakland): 72.

[4] V. Boyko, P. MacKenzie, and S. Patel. *Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman*. Advances in Cryptology – Eurocrypt 2000, LNCS (Springer-Verlag) 1807: 156.

[5] L. Buttyán, Jean-Pierre Hubaux, and S. Čapkun. *A Formal Analysis of Syverson's Rational Exchange Protocol*. Proceedings of the 15th IEEE workshop on Computer Security Foundations, 2002.

[6] M. Čagalj, S. Čapkun and J. Hubaux. *Key agreement in peer-to-peer wireless networks*. Proceedings of the IEEE Special Issue on Security and Cryptography, vol. 94, no. 2, pp. 467-478, 2006.

[7] J.L. Carter and M.N. Wegman. *Universal Classes of Hash Functions.* Journal of Computer and System Sciences, vol. 18 (1979), pp. 143-154.

[8] Y. Dodis and T. Rabin. *Cryptography and Game Theory*.

[9] G. Fuchsbauer, J. Katz and D. Naccache. *Efficient Rational Secret Sharing in Standard Communication Networks*. TCC 2010: 419-436

[10] C. Gehrmann, C. Mitchell and K. Nyberg. *Manual Authentication for Wireless Devices.* RSA Cryptobytes, vol. 7, no. 1, pp. 29-37, 2004.

[11] S.D. Gordon and J. Katz. *Rational secret sharing, revisited*. In Proceedings of Security and Cryptography for Networks. Lecture Notes in Computer Science, 2006, Volume 4116/2006, 229-241.

[12] J. Halpern and V. Teague. *Rational Secret Sharing and Multiparty Computation.* In Proceedings of the thirty-sixth annual ACM symposium on Theory of computing STOC '04. Pages 623-632, 2004.

[13] J. Katz. *Bridging Game Theory and Cryptography: Recent Results and Future Directions*. In the Proceeding of 5th Theory of Cryptography Conference (TCC) 2008.

[14] S. Laur and K. Nyberg. *Efficient Mutual Data Authentication Using Manually Authenticated Strings.* LNCS vol. 4301, pp. 90-107, 2006.

[15] S. Laur and S. Pasini. *SAS-Based Group Authentication and Key Agreement Protocols.* Public Key Cryptography, PKC, 197-213 (2008).

[16] A.Y. Lindell. *Comparison-based key exchange and the security of the numeric comparison mode in Bluetooth v2.1*. In Proceedings of the Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology, Lecture Notes in Computer Science, Vol. 5473, M. Fischlin, ed., Springer, 2009, pp. 66-83.

[17] L.H. Nguyen (editor), second edition. ISO/IEC 9798-6 (2010): *Information Technology – Security Techniques – Entity authentication – Part 6: Mechanisms using manual data transfer*.

[18] L.H. Nguyen and A.W. Roscoe. *Authenticating ad hoc networks by comparison of short digests.* Information and Computation 206 (2008), 250-271.

[19] L.H. Nguyen and A.W. Roscoe. *Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey.* Journal of Computer Security (to appear).

[20] L.H. Nguyen and A.W. Roscoe. *Efficient group authentication protocol based on human interaction.* Proceedings of Workshop on Foundation of Computer Security and Automated Reasoning Protocol Security Analysis (FCS-ARSPA), pp. 9-31, 2006.

[21] L.H. Nguyen and A.W. Roscoe. *Separating two roles of hashing in one-way message authentication.* Proceedings of Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (FCS-ARSPA-WITS) 2008, pp. 195-210.

[22] L.H. Nguyen and A.W. Roscoe *On the construction of digest functions for manual authentication protocols.* Submitted for publication. See: `http://www.comlab.ox.ac.uk/files/3812/digest.pdf`

[23] S. Pasini and S. Vaudenay. *SAS-based Authenticated Key Agreement.* Public Key Cryptography - PKC 2006: The 9th international workshop on theory and practice in public key cryptography, LNCS vol. 3958, pp. 395-409.

[24] D.R. Stinson. *Universal Hashing and Authentication Codes.* Advances in Cryptology - Crypto 1991, LNCS vol. 576, pp. 74-85, 1992.

[25] P. Syverson. *Weakly secret bit commitment: Applications to lotteries and fair exchange.* In Proceedings of the IEEE Computer Security Foundations Workshop, pages 2-13, 1998.

[26] S. Vaudenay. *Secure Communications over Insecure Channels Based on Short Authenticated Strings*. Advances in Cryptology - Crypto 2005, LNCS vol. 3621, pp. 309-326.

[27] J. Valkonen, N. Asokan and K. Nyberg. *Ad Hoc Security Associations for Groups.* In Proceedings of the Third European Workshop on Security and Privacy in Ad hoc and Sensor Networks 2006. LNCS vol. 4357, pp. 150-164.