Password-based Authenticated Key Exchange

David Pointcheval

ENS, Paris, France [⋆]

Abstract. *Authenticated Key Exchange* protocols enable several parties to establish a shared cryptographically strong key over an insecure network using various authentication means, such as strong cryptographic keys or short (*i.e.*, low-entropy) common secrets. The latter example is definitely the most interesting in practice, since no additional device is required, but just a human-memorable password, for authenticating the players.
After the seminal work by Bellovin and Merritt, many settings and security notions have been defined, and many protocols have been proposed, in the two-user setting and in the group setting.

1 Introduction

Key exchange protocols are cryptographic primitives used to provide several users (two or more), communicating over a public unreliable channel, with a secure session key. This thus allows establishment of virtual secure channels over insecure networks, which is one of the main practical applications of cryptography. Bellare and Rogaway gave the first foundations in [13, 14], but password-based authentication required more work: in this setting, where the authentication means is a short secret chosen from a small set of possible values (a four-digit pin, for example), the brute-force method which consists in trying all the possible values in the dictionary succeeds after a rather small number of attempts. This attack is called *on-line dictionary attack* and is unavoidable. But its damages can be limited by a policy that invalidates or blocks the use of a password if a certain number of failed attempts has occurred, unless failures are undetectable [27].

This paper presents a brief survey on Password-based Authenticated Key Exchange (PAKE) protocols, with a presentation of some security models in Section 2, and relations to practice. Section 3 deals with some practical constructions.

2 Security Models

Bellare, Pointcheval and Rogaway [12], and Boyko, MacKenzie and Patel [16] first formalized security of Password-based Authenticated Key Exchange, in two different frameworks.

[⋆] CNRS – UMR 8548 and INRIA – EPI Cascade

2.1 Game-based Security

The former model [12], the so-called *Find-then-Guess* scenario, is in the indistinguishability-based framework where an adversary should not be able to get an advantage significantly greater than q_S/N (or at most $\mathcal{O}(q_S)/N$ for some technicality reasons) in distinguishing a random session key from a real session key, if q_S is the number of active attacks and N the size of the dictionary. It has thereafter been improved to the *Real-or-Random* scenario [7]. More precisely, the adversary is given access to oracles: Execute-queries model passive attacks, Send-queries model active attacks, Corrupt-queries model corruptions with the leakage of long-term secrets, Reveal-queries model bad uses of session keys and thus the leakage of ephemeral secrets, and Test-queries model the semantic security of the session key with a real or random answer. In the Find-then-Guess scenario, only one Test-query can be asked, whereas in the Real-or-Random scenario many Test-queries can be asked with either always-real or always-random answers. The latter is clearly at least as strong as the former. But while both scenarios were known to be equivalent for encryption schemes [11], a linear loss in the number of Test-queries makes them quite different for PAKE, where the advantage should remain in $\mathcal{O}(q_s)/N$, whatever the number of Test-queries. We have then showed [7] that in this Real-or-Random scenario, Reveal-queries are not useful anymore, hence simplifying the security games.

2.2 Simulation-based Security

The latter model [16] is in the simulation-based framework, with an ideal functionality in which the adversary is allowed to check one password per session. This models on-line dictionary attacks. Excepted this test instance password, no information is leaked about the passwords and the session keys.

2.3 Universal Composability

In both above models, one formalized the fact that, with an active attack, the adversary can basically test one password, whereas passive eavesdropping does not (computationally) leak any information. The goal is essentially to rule out *off-line dictionary attacks* in which the adversary makes some active and passive attacks, and then makes an off-line brute-force attack on the dictionary. On-line brute-force attacks, which are unavoidable, should be the only possible way to have some information about the session keys, and thus many interactions with a real player are required.

However, there were still some limitations on the password distributions and for composition with other protocols, which were overcome by Canetti, Halevi, Katz, Lindell and MacKenzie [24]. They indeed provided an ideal functionality in the Universally Composable (UC) security framework [23], see Figure 1. This functionality also models on-line dictionary attacks with a TestPwd-query that can be asked once to each user in sessions. An important property is that passwords are chosen by the environment which then hands them to the parties

The functionality $\mathcal{F}_{\mathsf{PAKE}}$ is parameterized by a security parameter k. It interacts with an adversary $\mathcal{S}$ and a set of parties $P_1, \ldots, P_n$ via the following queries:

- P_i asks for a **$(\mathsf{NewSession}, \mathsf{sid}, P_i, P_j, pw)$**: Send $(\mathsf{NewSession}, \mathsf{sid}, P_i, P_j)$ to $\mathcal{S}$. If this is the first NewSession-query, or if this is the second NewSession-query and there is a record (P_j, P_i, pw'), then record (P_i, P_j, pw) and mark this record fresh.
- $\mathcal{S}$ asks for a **$(\mathsf{TestPwd}, \mathsf{sid}, P_i, pw')$**: If there is a record of the form (P_i, P_j, pw) which is fresh, then do:
  - If $pw = pw'$, mark the record compromised and reply with "correct guess";
  - If $pw \neq pw'$, mark the record interrupted and reply with "wrong guess".
- $\mathcal{S}$ asks for a **$(\mathsf{NewKey}, \mathsf{sid}, P_i, sk)$**: If there is a record of the form (P_i, P_j, pw), and this is the first NewKey-query for P_i, then:
  - If this record is compromised, or either P_i or P_j is corrupted, then output (sid, sk) to player P_i;
  - If this record is fresh, and there is a record (P_j, P_i, pw') with $pw' = pw$, and a key sk' was sent to P_j, and (P_j, P_i, pw) was fresh at the time, then output (sid, sk') to P_i;
  - In any other case, pick a new random key sk' of length k and send (sid, sk') to P_i.

  Either way, mark the record (P_i, P_j, pw) as completed.

Fig. 1. The PAKE Ideal Functionality $\mathcal{F}_{\mathsf{PAKE}}$

as inputs. This guarantees security even in the case where two honest players execute the protocol with two different passwords: the environment can emulate any distribution, mistypes of passwords and related passwords. Also note that allowing the environment to choose the passwords guarantees forward secrecy. This functionality mimics quite well some concrete requirements, but still, some leakage of information is not modeled, and could be exploited by a real-life adversary, whereas the ideal functionality does not allow it to the ideal-world adversary.

Explicit Authentication. With the above functionality, if neither party is corrupted, then they both end up with a uniformly-distributed session key, either the same key if the passwords are the same (success), or independent keys if the passwords are different (failure). Furthermore, the adversary learns nothing about the keys and the passwords, and even nothing about the status of the session (success or failure), but the users either. *Explicit authentication*, or mutual authentication modeled in [5], provides the players with a session key if and only if the passwords are the same, informing the adversary of success or not. This is an interesting additional feature, which is also more relevant in practice. In the real life, the adversary anyway learns whether the protocol succeeded or not, since in the latter case the communication stops.

Combined with the split functionality [10], it also allows to remove the TestPwd-query since the NewKey-query would reveal to the adversary whether the passwords are the same or not, by leaking the success or failure status. The split functionality allows the adversary to split a session between users Alice and Bob into two sessions, one between Alice and the adversary trying to impersonate Bob, and a second one between Bob and the adversary trying to impersonate Alice. When the adversary plays with Alice, in case of success, this means it has guessed Alice's password, which is similar to the $\mathsf{TestPwd}$-query.

Contributiveness. In the $\mathcal{F}_{\mathsf{PAKE}}$ functionality, if one party is corrupted, or if the adversary successfully guessed the player's password, the adversary is granted the right to fully determine the session key. Note that as soon as a party is corrupted, the adversary anyway learns the key, so one can think that nothing is lost by allowing it to fully determine it. But this is precisely the difference between *key agreement* and *key distribution* protocols.

In case of groups, this makes a huge difference. Hence the more recent functionality proposed by Abdalla, Catalano, Chevalier and Pointcheval [4] which

The functionality $\mathcal{F}_{\mathsf{GPAKE}}$ is parameterized by a security parameter k, and the parameter t of the contributiveness. It interacts with an adversary $\mathcal{S}$ and a set of parties $P_1, \ldots, P_n$ via the following queries:

- P_i asks for a $(\mathsf{\textbf{NewSession}}, \mathsf{\textbf{sid}}, \mathsf{\textbf{Pid}}, \boldsymbol{P_i}, \boldsymbol{pw_i})$: If this is the first $\mathsf{NewSession}$-query for P_i, where Pid is a set of at least two distinct identities containing P_i, record $(\mathsf{sid}, \mathsf{Pid}, P_i, pw_i)$, mark it fresh, and send $(\mathsf{sid}, \mathsf{Pid}, P_i)$ to $\mathcal{S}$. Ignore any subsequent $\mathsf{NewSession}$-queries with a different Pid set. If all the players involved in Pid have submitted their $\mathsf{NewSession}$-queries, then record $(\mathsf{sid}, \mathsf{Pid}, \mathsf{ready})$ and send it to $\mathcal{S}$.
- $\mathcal{S}$ asks for a $(\mathsf{\textbf{TestPwd}}, \mathsf{\textbf{sid}}, \mathsf{\textbf{Pid}}, \boldsymbol{P_i}, \boldsymbol{pw'})$: If there exists a record of the form $(\mathsf{sid}, \mathsf{Pid}, P_i, pw_i)$ which is fresh:
  - If $pw_i = pw'$, mark the record $\mathsf{compromised}$ and reply with "correct guess";
  - If $pw_i \neq pw'$, mark the record $\mathsf{interrupted}$ and reply with "wrong guess".
- $\mathcal{S}$ asks for a $(\mathsf{\textbf{NewKey}}, \mathsf{\textbf{sid}}, \mathsf{\textbf{Pid}}, \boldsymbol{sk})$: If there is a record of the form $(\mathsf{sid}, \mathsf{Pid}, \mathsf{ready})$, then, denote by n_c the number of corrupted players, and
  - If all $P_i \in \mathsf{Pid}$ have the same passwords and $n_c < t$, choose $sk' \in \{0,1\}^k$ uniformly at random and store $(\mathsf{sid}, \mathsf{Pid}, sk')$.
  - If all $P_i \in \mathsf{Pid}$ have the same passwords but $n_c \geq t$, store $(\mathsf{sid}, \mathsf{Pid}, sk)$.

  In both cases, for all $P_i \in \mathsf{Pid}$, mark the record $(\mathsf{sid}, \mathsf{Pid}, P_i, pw_i)$ $\mathsf{completed}$. In any other case, store $(\mathsf{sid}, \mathsf{Pid}, \mathsf{error})$, and for all $P_i \in \mathsf{Pid}$, mark the record $(\mathsf{sid}, \mathsf{Pid}, P_i, pw_i)$ error. When the key is set, report the result (either error or $\mathsf{completed}$) to $\mathcal{S}$.
- $\mathcal{S}$ asks for a $(\mathsf{\textbf{SendKey}}, \boldsymbol{b}, \mathsf{\textbf{sid}}, \mathsf{\textbf{Pid}}, \boldsymbol{P_i})$: If $P_i \in \mathsf{Pid}$ and there is a recorded tuple $(\mathsf{sid}, \mathsf{Pid}, \alpha)$ where $\alpha \in \{0,1\}^k \cup \{\mathsf{error}\}$, send $(\mathsf{sid}, \mathsf{Pid}, \alpha)$ to P_i if $b = 1$ or $(\mathsf{sid}, \mathsf{Pid}, \mathsf{error})$ if $b = 0$.
- $\mathcal{S}$ asks for a $(\mathsf{\textbf{Corrupt}}, \mathsf{\textbf{sid}}, \mathsf{\textbf{Pid}}, \boldsymbol{P_i})$: If there is a recorded tuple $(\mathsf{sid}, \mathsf{Pid}, P_i, pw_i)$, then reveal pw_i to $\mathcal{S}$. If there also is a recorded tuple $(\mathsf{sid}, \mathsf{Pid}, sk)$, that has not yet been sent to P_i, then send $(\mathsf{sid}, \mathsf{Pid}, sk)$ to $\mathcal{S}$.

Fig. 2. The Contributory GPAKE Ideal Functionality $\mathcal{F}_{\mathsf{GPAKE}}$

provides the *contributiveness* property to Group Password-based Authenticated Key Exchange (GPAKE), see Figure 2. PAKE is a particular case of GPAKE with groups of size 2. The latter property allows the adversary to fully determine the session key only if it has corrupted enough players, more than a threshold. This threshold can even be maximal: as soon as a player is honest, if a common key is generated, it is uniformly distributed in an unpredictable way. This means that no player has a more important role, and so there is no player to corrupt in priority for the adversary. As explained above, and as done in [5], one can even remove TestPwd-queries, allowing the adversary to split the group into several subgroups, with sub-session-IDs, where the adversary plays the role of the other users.

3 Constructions

3.1 Two-Party Password-based Authenticated Key Exchange

Bellovin and Merritt [15] proposed the first scheme, the so-called Encrypted Key Exchange (EKE), see Figure 3 for a sketch of the protocol, where $\mathcal{E}$ is assumed to be an encryption scheme onto the group $\mathbb{G}$, sometimes modeled as an ideal cipher. A first security analysis has been provided in the indistinguishability-based framework, in the ideal-cipher model [12], followed by several proofs of variations [8, 18, 19], trying to reduce the need of ideal models but still keeping the initial efficiency of EKE. EKE has also been studied in the simulation-based framework, in the random-oracle model [16], followed by studies in the UC framework [3] with security against adaptive corruptions, but still in ideal models. Our "simple PAKE" protocols [8] are definitely the most efficient, with a random oracle only for extracting the session key, with a security analysis in the Find-then-Guess scenario, under the CDH assumption.

Katz, Ostrovsky and Yung [33] proposed the first practical scheme, but still less efficient than above schemes, in the standard model with a common reference string, followed by a generalization from Gennaro and Lindell (GL) [28, 29], using the power of smooth-projective hash functions [26], in the Find-then-Guess

$$\begin{array}{rcl}
A^{\;pw} & & B^{\;pw}\\
x \overset{R}{\leftarrow} \{1,\ldots,|\mathbb{G}|\} & & \\
X \leftarrow g^x, X' \leftarrow \mathcal{E}_{pw}(X) & \xrightarrow{\quad A\|X' \quad} & y \overset{R}{\leftarrow} \{1,\ldots,|\mathbb{G}|\}\\
 & \xleftarrow{\quad \mathcal{E}_{pw}(g^y) \quad} & Y \leftarrow g^y, Y' \leftarrow \mathcal{E}_{pw}(Y)\\
Y \leftarrow \mathcal{D}_{pw}(Y') & & X \leftarrow \mathcal{D}_{pw}(X')\\
Z \leftarrow Y^x & & Z \leftarrow X^y\\
\multicolumn{3}{c}{sk \leftarrow H(A\|B\|X\|Y\|Z)}
\end{array}$$

Fig. 3. Encrypted Key Exchange

scenario. Many variations [6, 24, 31, 34, 35] have thereafter been proposed, to get security in the UC framework, to improve round efficiency, or to rely on new assumptions.

Whereas the huge majority of the protocols rely on Diffie-Hellman assumptions, some efficient schemes have also been proposed on factoring-related assumptions [25, 30, 36, 37]. Besides the Secure Remote Password (SRP) protocol [39] and the Simple Password Exponential Key Exchange (SPEKE) protocol [32] that have been standardized, EKE-like and GL-like schemes are the two main streams, with security analyses in the UC framework.

3.2 Group Password-based Authenticated Key Exchange

For groups, while the first proposals were extensions of the group Diffie-Hellman key exchange [17, 20, 38], the Burmester and Desmedt construction [21, 22] became more appropriate, because of its constant number of rounds, independently of the size of the group. Several group password-based authenticated key exchange protocols have then been proposed [1, 2, 5, 9], essentially combining a two-party PAKE with the Burmester and Desmedt methodology.

Acknowledgments

I would like to thank Céline Chevalier for her valuable comments, and all my other co-authors on this quite active and interesting area: Michel Abdalla, Mihir Bellare, Emmanuel Bresson, Dario Catalano, Olivier Chevassut, Pierre-Alain Fouque, Louis Granboulan, Thomas Pornin, Jean-Jacques Quisquater and Phil Rogaway.

References

1. Michel Abdalla, Jens-Matthias Bohli, Maria Isabel Gonzalez Vasco, and Rainer Steinwandt. (Password) authenticated key establishment: From 2-party to group. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 499–514. Springer, February 2007.
2. Michel Abdalla, Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Password-based group key exchange in a constant number of rounds. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *PKC 2006: 9th International Conference on Theory and Practice of Public Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 427–442. Springer, April 2006.
3. Michel Abdalla, Dario Catalano, Céline Chevalier, and David Pointcheval. Efficient two-party password-based key exchange protocols in the UC framework. In Tal Malkin, editor, *Topics in Cryptology – CT-RSA 2008*, volume 4964 of *Lecture Notes in Computer Science*, pages 335–351. Springer, April 2008.

4. Michel Abdalla, Dario Catalano, Céline Chevalier, and David Pointcheval. Password-authenticated group key agreement with adaptive security and contributiveness. In Bart Preneel, editor, *AFRICACRYPT 09: 2nd International Conference on Cryptology in Africa*, volume 5580 of *Lecture Notes in Computer Science*, pages 254–271. Springer, June 2009.
5. Michel Abdalla, Céline Chevalier, Louis Granboulan, and David Pointcheval. Contributory password-authenticated group key exchange with join capability. In Aggelos Kiayias, editor, *Topics in Cryptology – CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 142–160. Springer, February 2011.
6. Michel Abdalla, Céline Chevalier, and David Pointcheval. Smooth projective hashing for conditionally extractable commitments. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 671–689. Springer, August 2009.
7. Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval. Password-based authenticated key exchange in the three-party setting. In Serge Vaudenay, editor, *PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 65–84. Springer, January 2005.
8. Michel Abdalla and David Pointcheval. Simple password-based encrypted key exchange protocols. In Alfred Menezes, editor, *Topics in Cryptology – CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 191–208. Springer, February 2005.
9. Michel Abdalla and David Pointcheval. A scalable password-based group key exchange protocol in the standard model. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 332–347. Springer, December 2006.
10. Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 361–377. Springer, August 2005.
11. Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th Annual Symposium on Foundations of Computer Science*, pages 394–403. IEEE Computer Society Press, October 1997.
12. Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 139–155. Springer, May 2000.
13. Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In Douglas R. Stinson, editor, *Advances in Cryptology – CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249. Springer, August 1994.
14. Mihir Bellare and Phillip Rogaway. Provably secure session key distribution: The three party case. In *27th Annual ACM Symposium on Theory of Computing*, pages 57–66. ACM Press, May / June 1995.
15. Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *1992 IEEE Symposium on Security and Privacy*, pages 72–84. IEEE Computer Society Press, May 1992.
16. Victor Boyko, Philip D. MacKenzie, and Sarvar Patel. Provably secure password-authenticated key exchange using Diffie-Hellman. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 156–171. Springer, May 2000.

17. Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Group Diffie-Hellman key exchange secure against dictionary attacks. In Yuliang Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 497–514. Springer, December 2002.
18. Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Security proofs for an efficient password-based key exchange. In Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors, *ACM CCS 03: 10th Conference on Computer and Communications Security*, pages 241–250. ACM Press, October 2003.
19. Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. New security results on encrypted key exchange. In Feng Bao, Robert Deng, and Jianying Zhou, editors, *PKC 2004: 7th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 145–158. Springer, March 2004.
20. Emmanuel Bresson, Olivier Chevassut, David Pointcheval, and Jean-Jacques Quisquater. Provably authenticated group Diffie-Hellman key exchange. In *ACM CCS 01: 8th Conference on Computer and Communications Security*, pages 255–264. ACM Press, November 2001.
21. Mike Burmester and Yvo Desmedt. A secure and efficient conference key distribution system (extended abstract). In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 275–286. Springer, May 1994.
22. Mike Burmester and Yvo Desmedt. A secure and scalable group key exchange system. *Information Processing Letters*, 94(3):137–143, May 2005.
23. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science*, pages 136–145. IEEE Computer Society Press, October 2001.
24. Ran Canetti, Shai Halevi, Jonathan Katz, Yehuda Lindell, and Philip D. MacKenzie. Universally composable password-based key exchange. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 404–421. Springer, May 2005.
25. Dario Catalano, David Pointcheval, and Thomas Pornin. IPAKE: Isomorphisms for password-based authenticated key exchange. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 477–493. Springer, August 2004.
26. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, April / May 2002.
27. Yun Ding and Patrick Horster. Undetectable on-line password guessing attacks. *SIGOPS Oper. Syst. Rev.*, 29:77–86, October 1995.
28. Rosario Gennaro. Faster and shorter password-authenticated key exchange. In Ran Canetti, editor, *TCC 2008: 5th Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 589–606. Springer, March 2008.
29. Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 524–543. Springer, May 2003. `http://eprint.iacr.org/2003/032.ps.gz`.
30. Craig Gentry, Philip D. Mackenzie, and Zulfikar Ramzan. Password authenticated key exchange using hidden smooth subgroups. In Vijayalakshmi Atluri, Catherine Meadows, and Ari Juels, editors, *ACM CCS 05: 12th Conference on Computer and Communications Security*, pages 299–309. ACM Press, November 2005.

31. Adam Groce and Jonathan Katz. A new framework for efficient password-based authenticated key exchange. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 10: 17th Conference on Computer and Communications Security*, pages 516–525. ACM Press, October 2010.
32. David P. Jablon. Strong password-only authenticated key exchange. *SIGCOMM Comput. Commun. Rev.*, 26(5):5–26, October 1996.
33. Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient password-authenticated key exchange using human-memorable passwords. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 475–494. Springer, May 2001.
34. Jonathan Katz and Vinod Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 636–652. Springer, December 2009.
35. Jonathan Katz and Vinod Vaikuntanathan. Round-optimal password-based authenticated key exchange. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 293–310. Springer, March 2011.
36. Stefan Lucks. Open key exchange: How to defeat dictionary attacks without encrypting public keys. In *Workshop on Security Protocols*, École Normale Supérieure, 1997.
37. Philip D. MacKenzie, Sarvar Patel, and Ram Swaminathan. Password-authenticated key exchange based on RSA. In Tatsuaki Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 599–613. Springer, December 2000.
38. Michael Steiner, Gene Tsudik, and Michael Waidner. Diffie-Hellman key distribution extended to group communication. In *ACM CCS 96: 3rd Conference on Computer and Communications Security*, pages 31–37. ACM Press, March 1996.
39. Thomas D. Wu. The secure remote password protocol. In *ISOC Network and Distributed System Security Symposium – NDSS'98*. The Internet Society, March 1998.