

PASSWORD AUTHENTICATED KEY EXCHANGE: FROM TWO PARTY METHODS TO GROUP SCHEMES

STEPHEN MELCZER, TARAS MYCHASKIW AND YI ZHANG

ABSTRACT. This project investigates group password authenticated key exchange methods (GPAKEs). In particular, we detail the so-called ‘fairy ring dance’ method recently described by Hao et. al. [4] which allows for the extension of two party password authenticated key exchange methods (PAKEs) with explicit key confirmation to a group setting with an arbitrary number of users without increasing round complexity (the computational complexity, of course, increases with the number of users). This paper presents two new GPAKEs constructed through these means, based on the Dragonfly and PAK/PPK two party protocols, and includes timings comparing them to previous GPAKEs of Hao et. al. [4].

1. INTRODUCTION

Since their introduction in the 1990s, password-authenticated key exchange (PAKE) methods – also known as password-authenticated key agreement methods – have become popular for their ability to allow agents sharing a (typically low entropy) password to securely establish shared cryptographic keys (see Bellovin and Merritt [1] or Jablon [6] for early examples, and Hao and Ryan [3] for a more recent paper). Although they have been around for decades, most research on PAKEs has focused on key establishment between two parties. For our project, we have studied the problem of establishing Group PAKEs (GPAKEs) – that is, using a low entropy password shared between many agents to set up cryptographic keys. This has modern applications with the rise of the so-called ‘Internet of Things’, where many consumer devices connected through a local Internet connection wish to securely communicate (such schemes would allow, for instance, secure communication between a smart television, DVD player, and cable box after their owner inputs a short shared password into each upon purchase).

The major issue in designing an efficient GPAKE is to minimize the number of rounds of communication between the agents involved, as the latency of such a protocol is determined by the slowest responder in each round. A recent pre-print of Hao et. al. [4] proposes a construction which allows for the extension of any secure two-party PAKE to a multi-party PAKE with explicit key confirmation without adding any extra rounds of communication. The authors continue on to give two explicit schemes following from this template: SPEKE+ (using two rounds of communication, adapted from the SPEKE [6] protocol) and J-PAKE+ (using three rounds of communication, adapted from the J-PAKE [3] protocol).

The structure of this document is as follows: Section 2 begins by giving a survey of classical two-party PAKEs – including explicit descriptions of the PAKEs which will be extended into the group setting and background information on the zero knowledge proof protocols these use. Section 3 starts with a description of the theoretical methodology developed by Hao et. al. [4] to extend two-party PAKEs into a group setting. After this theoretical background, we give two explicit GPAKEs (SPEKE+ and J-PAKE+) constructed by Hao et. al. using this methodology, followed by two explicit GPAKEs which we have derived through the same means (a group variant of the IEEE 802.11-2012 standard Dragonfly protocol [5], and a variant of the PAK/PPK protocol [2]); the security of these new GPAKEs are proven using realistic attack models, when one assumes the underlying two party PAKE protocols are secure. In Section 4 we test the practical efficacy of our new methods against the Java implementations of SPEKE+ and J-PAKE+ given by Hao et. al. [4]. Section 5 concludes with an overview of these results and possible directions for future work.

The main original contributions found in this project come from the two new group PAKEs we have constructed (see sub-Sections 2.3 and 2.4), including the proofs of their security and timings to compare

against SPEKE+ and J-PAKE+. We have also fleshed out the security proofs of SPEKE+ and J-PAKE+, include the relevant background material on Zero Knowledge Proofs needed to explicitly specify all aspects of these protocols, and fixed some minor Java implementation errors which could cause the timings in Hao et. al. [4] to be slightly inaccurate.

2. TWO PARTY PASSWORD-AUTHENTICATED KEY EXCHANGE (PAKE)

[The background information in this section, and details about SPEKE and J-PAKE, are based on the presentation in Hao and Ryan [3]. The information on the Dragonfly protocol was taken from Harkins [5]. The sub-section about PAK/PPK is based on work of [2].]

The genesis of password-authenticated key exchange is widely credited to the 1992 work of Bellovin and Merrit [1], whose protocol (known as Encrypted Key Exchange – or EKE, for short) came to be known as the first PAKE. All PAKEs aim for two main goals: to require their users to provide a zero knowledge proof of a short password known to both parties *a priori* (that is, before the protocol has begun) and to leverage knowledge of this password to facilitate an authenticated key exchange. As password are assumed to be low entropy – for instance, they are often assumed to be human memorable passwords (typically assumed to be approximately 20-30 bits of entropy) – if the passwords themselves were broadcast they would need to be protected, for instance using SSL. This would require Public Key Infrastructure, which can be expensive, hence the use of zero knowledge proofs.

Indeed, it is somewhat miraculous that PAKEs – which transform a low entropy shared secret into a much larger and more complicated shared key – exist at all. Although the EKE protocol of Bellovin and Merrit was later shown to have weaknesses (see Jaspan [6], for example) its great contribution was to show that such schemes can be achieved. Due to its historical significance, we outline the Diffie-Hellman variant of the method here (an RSA variant, also by Bellovin and Merrit, was later shown to be insecure). Given a symmetric encryption function $[\cdot]_s$ which uses a password s shared by agents Alice and Bob as a key, the algorithm does the following: [Do we want a better way of writing protocols?][Yi: Probably...]

Setup: Let α be a primitive root of \mathbb{Z}_p

Alice: Pick $x_a \in \mathbb{Z}_p \setminus \{0\}$ randomly
Send Bob $[\alpha^{x_a}]_s$

Bob: Pick $x_b \in \mathbb{Z}_p \setminus \{0\}$ randomly
Send Alice $[\alpha^{x_b}]_s$

At the end, both Alice and Bob share the key $K = \alpha^{x_a \cdot x_b}$. The weakness of the algorithm comes from an issue discussed above: as the password has low entropy in order for the scheme to be secure the input into $[\cdot]_s$ must essentially look like a random number. But a 1024 bit number modulo p is not random, and a passive attacker can try candidate passwords to decipher $[\alpha^{x_a}]_s$ and immediately rule out any passwords giving a result in the range $[p, 2^{1024} - 1]$.

Although EKE has this (and other) weaknesses, it was extremely influential and its general characteristics are reflected in many of the more advanced protocols we outline below. Before giving these methods, we must outline what constitutes a good measure of security for a PAKE. In the modern literature, a full proof of security for a two party PAKE typically consists of proving each of the following four properties:

(Offline dictionary attack resistance)

The PAKE does not leak any information to a passive or active attacker which can be used by the attacker to determine the password through a brute force search (the protocol cannot reveal a hash of the password, for instance).

(Forward secrecy for established keys)

If the password is disclosed, past session keys cannot be computed by an attacker. This implies that a *passive* attacker who knows the password he cannot learn a session key by observing communication between Alice and Bob (of course, an active attacker could establish a shared key with one of the participants as he would have access to all of their secret information).

(Known session security)

If an attacker learns all secrets of a protocol in progress, it does not reveal any information about other established sessions.

(Online dictionary attack resistance)

An active attacker can only test one password per protocol execution (this is the best that we can reasonably assume, as any attacker can randomly guess a password and run the protocol – at some point the key must be confirmed, either explicitly through the PAKE or when the key is used in some other protocol, and the attacker will know whether or not his guess was correct).

These properties are illustrated in sub-Section 2.2 when we outline proofs of these properties for the J-PAKE protocol. Some PAKEs satisfy the additional requirement that an attacker not be allowed to impersonate other users to some fixed target after obtaining (through illicit means) password verification files for those users which were stored by the target. The schemes with this additional property are known as augmented PAKEs, although some (for instance, Hao et. al. [4]) have argued that such a requirement is not useful as the low entropy of the password means that it will soon be discovered through an offline dictionary attack on the verification files. Nevertheless, augmented variants exist for a number of balanced PAKEs (for example Augmented-EKE for EKE, B-SPEKE for SPEKE and PAK-Z for PAK/PPK).

2.1. SPEKE. Info about SPEKE

2.2. J-PAKE. We start this protocol by describing the Password Authenticated Key Exchange by Juggling (J-PAKE) method of Hao and Ryan [3]. Let G be a subgroup of $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ with prime order q , where the Decision Diffie-Hellman (DDH) problem is considered intractable. Let $g \in G$ be a generator of the subgroup and $s \in [1, q-1]$ be the shared password between Alice and Bob, where $[a, b]$ is notation meaning the elements of \mathbb{Z}^* between a and b : $[a, b] := \{a, a+1, \dots, b\}$.

The protocol consists of a setup round followed by two rounds of communication (for details on zero knowledge proofs see sub-Section 2.5 – in our implementation detailed later the XXX ZKP is used [Which? Schnorr?]): *

Setup Alice picks $x_1 \in [0, q-1]$ and $x_2 \in [1, q-1]$ randomly
 Bob picks $x_3 \in [0, q-1]$ and $x_4 \in [1, q-1]$ randomly

Round 1 Alice sends g^{x_1}, g^{x_2} and zero knowledge proofs of x_1 and x_2 to Bob
 Bob sends g^{x_3}, g^{x_4} and zero knowledge proofs of x_3 and x_4 to Alice
 [Alice and Bob verify the knowledge proofs and that $g^{x_2}, g^{x_4} \neq 1$]

Round 2 Alice sends $A = g^{(x_1+x_3+x_4)x_2 \cdot s}$ and a zero knowledge proof of x_2s
 Bob sends $B = g^{(x_1+x_2+x_3)x_4 \cdot s}$ and a zero knowledge proof of x_4s

At this point, both are able to determine

$$K = \underbrace{(B/g^{x_2x_4s})^{x_2}}_{\text{Computable by Alice}} = g^{(x_1+x_3)x_2x_4s} = \underbrace{(A/g^{x_2x_4s})^{x_4}}_{\text{Computable by Bob}}.$$

The shared session key is then taken to be $\kappa = H(K)$, where H is a hash function. [Why do they hash here?] Note that this scheme has implicit key confirmation: each of Alice and Bob believe only the other can calculate the shared key; an explicit key confirmation can then be performed if desired (which will increase the number of rounds of communication by at least one). *

We now show that the J-PAKE protocol satisfies the four properties required to be considered a secure PAKE, in order to illustrate the properties and the methods by which they can be proven: without loss of generality we may assume that Alice is honest, and let $x_a := x_1 + x_3 + x_4$.

Lemma 2.1. *With high probability (approximately 2^{-160} for q a 160-bit prime) the element $g_a := g^{x_a}$ is a generator for the subgroup G , and Alice can verify this.*

Proof. Since $|G| = q$ is prime, it is sufficient to prove that $g_a \neq 1$ (any non-identity element generates G) with high probability. As Alice verifies that x_3 and x_4 are known to Bob due to his zero knowledge proofs in round 1, and x_1 is chosen randomly by Alice, x_a must be a random value from Bob's perspective. In other words, $x_a \neq 0$ with high probability, even if Bob is an active adversary. Alice can verify that g_a is a generator for g as she knows the value of x_a . \square

An analogous proof shows that when Bob is honest the element $g_b := g^{x_1+x_2+x_3}$ is a generator of G with high probability. We first show resistance to an offline attack with an active adversary.

Theorem 2.2 (Offline resistance to active attack). *Under the DDH assumption, when g_a is a generator of G any attacker Oscar cannot distinguish Alice's ciphertext from a random non-identity element in the subgroup G .*

Proof. Suppose that Alice communicates with Oscar, who does not know the password. After the protocol is run, Oscar knows

$$g^{x_1}, g^{x_2}, A = g_a^{x_2s}, \text{ and ZKPs of the exponents } x_1 \text{ and } x_2.$$

By definition, with high probability the zero knowledge proofs reveal only one bit of information: that Alice knows the values of the exponents. As argued in the proof of the last lemma, with high probability g_a is a (random) generator of the group G . Furthermore, as x_2 is chosen randomly it follows that $x_2s \in [1, q-1]$ is random and thus unknown to Oscar. Thus, the only way to distinguish A from a random non-identity element would be for Oscar to solve an instance of the Decision Diffie-Hellman problem. \square

The result in the case of a passive attacker follows in a straightforward manner (note that this case must be proven separately as above the active attacker does not know the password s , but when he passively observes a session Alice is communicating with Bob, who does know s).

Theorem 2.3 (Offline resistance to passive attack). *Under the DDH assumption, given that g_a and g_b are generators of G , the ciphertexts*

$$A = g_a^{x_2s} \text{ and } B = g_b^{x_4s}$$

do not leak information for password verification.

Proof. Our above work shows that the value A looks random to Bob, and analogously that B looks random to Alice. Thus, both must look random to a passive adversary, who has less information about the protocol's secrets than either Alice or Bob. \square

Next we show forward secrecy under the assumption that the Square Computational Diffie-Hellman problem is hard (this problem, which has been shown to be equivalent to the Computational Diffie-Hellman problem, asks one to compute g^{a^2} given the value g^a with a some unknown value). Since the zero-knowledge proofs imply that Alice and Bob know the values of x_1 and x_3 , with high probability $x_1 + x_3 \neq 0$ in \mathbb{Z}_q – which implies $K = g^{(x_1+x_3)x_2x_4s} \neq 1$ with high probability, even if one of Alice or Bob is an active adversary.

Theorem 2.4 (Forward Secrecy). *Under the Square Computational Diffie-Hellman assumption, when $K \neq 1$, past session keys derived from the protocol remain incomputable even when s is later disclosed.*

Proof. Knowing s , the attacker wants to compute $\kappa = H(K)$ given

$$\{g^{x_1}, g^{x_2}, g^{x_3}, g^{x_4}, g^{(x_1+x_3+x_4)x_2}, g^{(x_1+x_2+x_3)x_4}\}.$$

Suppose the attacker can compute K , and thus $g^{(x_1+x_3)x_2x_4}$ from the above information – we show how he can act as an oracle to solve the Square Computational Diffie-Hellman problem. Let $x_5 = x_1 + x_3 \bmod q$ (which is non-zero when $K \neq 1$). Then ... \square

[To be continued]

2.3. **Dragonfly**. Info about Dragonfly

2.4. **PAK/PPK**. Info about PPK. Yi's first update.

2.5. **Zero-Knowledge Proof Protocols**. Info about Schnorr and XXX

3. GROUP PASSWORD-AUTHENTICATED KEY EXCHANGE (GPAKE)

Background info from paper

3.1. **SPEKE+ and J-PAKE+**. Info about SPEKE+ and J-PAKE+

3.2. **Dragonfly+**. Our extensions of Dragonfly (and others?)

3.3. **PPK+**. Our extension of PPK

4. IMPLEMENTATION RESULTS

Our implementation results

5. CONCLUSION

The conclusion

REFERENCES

- [1] S. M. Bellare and M. Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *1992 IEEE Computer Society Symposium on Research in Security and Privacy Proceedings*, pages 72–84. IEEE, 1992.
- [2] V. Boyko, P. MacKenzie, and S. Patel. Provably secure password-authenticated key exchange using diffie-hellman. In *LNCS 1807, Springer-Verlag, Berlin*, pages 156–171. Eurocrypt 2000, 2000.
- [3] F. Hao and P. Ryan. J-PAKE: Authenticated key exchange without PKI. *Transactions on Computational Science XI, Lecture Notes in Computer Science*, 6480:192–206, 2010.
- [4] F. Hao, X. Yi, L. Chen, and S. F. Shahandashti. The fairy-ring dance: Password authenticated key exchange in a group. Cryptology ePrint Archive, Report 2015/080, 2015. <http://eprint.iacr.org/2015/080>.
- [5] D. Harkins. Dragonfly key exchange – internet research task force internet draft, 2015. http://datatracker.ietf.org/doc/draft-irtf-cfrg-dragonfly/?include_text=1.
- [6] B. Jaspán. Dual-workfactor encrypted key exchange: efficiently preventing password chaining and dictionary attacks. In *Proceedings of the Sixth Annual USENIX Security Conference*, pages 43–50, July 1996.