Základní principy kryptografických eskalačních protokolů

Jan Krhovják

Fakulta informatiky, Masarykova univerzita

xkrhovj@fi.muni.cz

Abstrakt

V tomto příspěvku budou představeny základní typy, principy a vlastnosti vybraných kryptografických eskalačních protokolů společně s problémy souvisejícími s jejich bezpečným návrhem. Dále budou prezentovány možnosti aplikace těchto protokolů v prostředí soudobých výpočetních systémů a počítačových sítí.

1 Úvod

Zcela zásadním problémem moderních kryptosystémů je obtížnost distribuce jejich šifrovacích klíčů. Protokoly umožňující vytváření a/nebo distribuci těchto klíčů (jako například známá Diffie-Hellmanova metoda) mohou být náchylné k útokům typu man-in-the-middle a vhodným protiopatřením se jeví až použití autentizovaných verzí těchto protokolů. Ty však paradoxně také vyžadují předem ustavené šifrovací klíče, které jsou pro jednotlivé uživatele prakticky nezapamatovatelné, a musí tedy být někde bezpečně uloženy. Přímé nahrazení těchto klíčů za snáze zapamatovatelné PINy či hesla vede u mnohých protokolů k snadné aplikaci off-line útoků hrubou silou (a tedy ke snadné kompromitaci PINu či hesla).

Kryptografické eskalační protokoly tvoří speciální třídu protokolů umožňujících autentizované ustavení kryptografických klíčů. Tyto protokoly jsou založeny na použití dat s nízkou entropií (jako například PINů či hesel) způsobem, který je nevystaví riziku off-line útoku hrubou silou (a tedy ani slovníkovému útoku). PINy i hesla jsou pro většinu uživatelů snadno zapamatovatelné a na straně klienta tedy není vyžadováno jejich uložení. Jednou z mála nevýhod všech „eskalačních“ protokolů je, že umožňují přímé on-line „hádání“ hesel – na straně serveru by tedy měla být vždy implementována protiopatření, která by těmto útokům zabránila.

Jako „eskalační“ označujeme tyto protokoly proto, že ačkoliv pro autentizované ustavení klíčů používají data s nízkou entropií, jsou výsledné klíče velmi kvalitním kryptografickým materiálem. Celý tento proces by se dal tedy nazvat „eskalací“ z málo kvalitního na velmi kvalitní kryptografický materiál, který již může být použit i jinými kryptografickými metodami jako je například symetrické šifrování apod.

2 Základní kryptografické eskalační protokoly

V této části si představíme základní typy kryptografických eskalačních protokolů. Během jejich popisu budeme předpokládat, že obě strany protokolu (tj. klient i server) mají již předem ustaveno společné tajné heslo (resp. u důmyslnějších protokolů na straně serveru nějakou z hesla „jednocestně“ odvozenou hodnotu).

Historicky první kryptografický eskalační protokol je označován jako *EKE (encrypted key exchange)* [BM92]. Jedná se o zcela originální kombinaci symetrické a asymetrické kryptografie, která inspirovala a ovlivnila návrhy mnoha dalších eskalačních protokolů. Sdílené tajné heslo zde slouží jako klíč symetrické blokové šifry, jehož pomocí je šifrován veřejný klíč klienta (který je společně se soukromým klíčem při zahájení protokolu jednorázově vygenerován). EKE může být použit se systémy umožňujícími distribuci veřejného klíče – obzvláště dobře funguje s Diffie-Hellmanovou (DH) metodou ustavení klíčů [DH76] (pak jej však nazýváme *DHEKE*), ale i s asymetrickými kryptosystémy (po vyřešení specifických problémů lze použít například RSA či ElGamal).

Z bezpečnostního hlediska je u tohoto protokolu zcela zásadní, aby zpráva, která má být pomocí hesla zašifrována (např. výše zmíněný veřejný klíč), byla (výpočetně) nerozlišitelná od náhodného čísla. V opačném případě (tj. kdyby zpráva měla určitou strukturu, kontrolní součet apod.) by bylo možné provést off-line útok hrubou silou. Rozšířením EKE, které nevyžaduje šifrování veřejných klíčů a ani opětovné (re)generování klíčových párů, je protokol *OKE (open key exchange)* resp. *RSA-OKE* [Luc97].

Nevýhodou protokolu EKE je, že jednotlivé strany si musí uchovávat svá sdílená hesla uložená v otevřené podobě. Protokol *AEKE (augmented encrypted key exchange)* [BM93] je takovým rozšířením a vylepšením protokolu DHEKE, které zajišťuje, že si server již uchovává hesla pouze jednocestně zašifrována – někdy je budeme označovat jako *verifikační hodnoty*. Útočník, který by získal přístup k souboru takto zašifrovaných hesel, by sice stále mohl vystupovat jako falešný server, ale nemohl by se jejich přímým použitím vydávat serveru za libovolného uživatele (nejprve by musel provést slovníkový útok). (A)EKE je vhodnou náhradou za Rivestův a Shamirův *interlock protocol* [RS84], který byl navržen tak, aby na komunikačním spoji detekoval aktivní útočníky. Davies a Price v [DP89] navrhli způsob jeho použití také k autentizaci, avšak později byl na něj v [BM94] popsán útok.

V [STW95] je popsána efektivnější varianta protokolu DHEKE, často označovaná jako *MEKE (minimal encrypted key exchange)*. Optimalizací došlo k redukci počtu zasílaných zpráv i prováděných kryptografických operací. Kromě popisu MEKE jsou zde diskutovány také kryptoanalytické útoky na (A)EKE a obrana proti nim. Jako podstatné je u (A)EKE zdůrazněno především bezpečné ustavení klíče sezení tak, aby jeho pozdější kompromitace neumožnila slovníkový útok na heslo. Proto by měl být výsledný klíč sezení raději vypočítán z původního klíče aplikací kryptografické hašovací funkce. Protokoly DHEKE i MEKE jsou proti podobnému typu útoku odolné. Další vylepšení, tentokráte již samotného protokolu MEKE, jsou představena v [LSH01].

I přes svůj precizní návrh jsou mnohé používané eskalační protokoly stále náchylné k útokům, které umožňují se znalostí současně používaného hesla získat všechna v budoucnu ustavená hesla – tzv. *password chaining attacks*. Zásadní problém většiny těchto protokolů totiž je, že používají své heslo také k ochraně zpráv, které jsou použity k ustavení nového hesla. Útočník, který zná původní heslo, tak může s jeho pomocí snadno dešifrovat zprávu obsahující nové heslo. Výsledkem odhalení byť jen jediného hesla je pak kompromitace veškeré komunikace daného uživatele. Protokol *DWEKE (dual-workfactor encrypted key exchange)* [Jas96] je vylepšenou variantou protokolu DHEKE a bez ztráty na rychlosti a efektivitě tomuto typu útoků zamezuje.

Protokol *SPEKE (simple password encrypted key exchange)* [Jab96] je svým návrhem a implementací velmi blízký protokolu DHEKE. I přes svou podobnost však mají tyto dva protokoly rozdílná omezení a nedostatky. První fáze SPEKE je založena na Diffie-Hellmanově metodě ustavení klíčů, ale namísto běžně používané fixní báze (generátoru) využívá SPEKE funkci, která na základě svého jediného parametru (hesla) vytvoří nějakou bázi pro umocňování (tedy ne nutně generátor příslušné grupy). SPEKE narozdíl od DHEKE v první fázi protokolu žádným způsobem nešifruje předávané zprávy, což útočníkovi dává možnost omezit prostor klíčů na malou množinu snadno předvídatelných hodnot – tzv. *subgroup confinement attack*. Použití bezpečných prvočísel počet malých podgrup pouze redukuje a jako protiopatření by tedy mělo být vždy testováno, zdali výsledný klíč do těchto podgrup nepatří.

Rozšíření EKE a SPEKE jsou představena v [Jab97] a podobně jako AEKE zajišťují, že si server uchovává hesla pouze jednocestně zašifrována. ASPEKE je přímočará aplikace technik použitých k vytvoření AEKE na protokol SPEKE. BEKE a BSPEKE nahrazuje poslední část AEKE a ASPEKE dalším kolem DH metody ustavení klíčů, které umožňuje serveru ověřit, že klient skutečně zná heslo. Ověření znalosti hesla je u tohoto typu protokolů zcela nezbytné, protože jejich původní část zůstává až na použití jednocestně zašifrované verifikační hodnoty namísto otevřeného hesla naprosto beze změn (klient si tuto verifikační hodnotu musí vždy ze zadaného hesla dopočítat) a přímá znalost hesla tedy není prokázána – kdokoliv, kdo zná verifikační hodnotu, by mohl vystupovat za klienta (resp. uživatele).

SRP (secure remote password) [Wu97] je zcela odlišný typ protokolu, který (stejně jako některé z předchozích protokolů) zajišťuje, že si server uchovává hesla pouze jednocestně zašifrována. Narozdíl od protokolů jako AEKE a ASPEKE (které jsou založeny na použití digitálních podpisů) či BEKE a BSPEKE (které využívají přidané kolo DH metody ustavení klíčů) je SRP založen na obecné konstrukci zvané *AKE (asymmetric key exchange)*. Tato konstrukce oproti EKE žádným způsobem nevyužívá symetrickou kryptografii, což činí výsledné protokoly jednodušší a mnohdy i bezpečnější (není již třeba řešit žádné problémy spjaté s používáním hesel jakožto symetrických šifrovacích klíčů). Protokol SRP je speciální instancí AKE, a nabízí navíc vyšší výkon než srovnatelné protokoly jako například AEKE či BSPEKE. Někdy je tento protokol nazýván SRP-3 a jeho vylepšená varianta SRP-6 [Wu02].

Posledním významným protokolem popsaným v této části je *PDM (password derived moduli)* [PK01a]. Tento protokol je opět založen na modifikaci DH metody ustavení klíčů, a jak již název napovídá, využívá heslo k vytvoření bezpečného prvočíselného modulu. Aby se předešlo redukci prostoru hesel, nesmí být žádná přenášená hodnota větší než jakákoliv modulo vytvořené na základě všech zkoušených hesel. V [PK99, PK01a] je navrženo několik protokolů, které jsou určeny pro bezpečné stahování citlivých informací (například soukromých klíčů). Ukázalo se však, že některé z metod uveřejněných v [PK99] mají určité bezpečnostní nedostatky [KKP99].

Mezi základní kryptografické eskalační protokoly řadíme také protokol založený na použití hašovacích funkcí bohatých na kolize [AL94] a sadu tří (od ostatních konstrukčně zcela odlišných) protokolů *S3P (strong secret sharing password)* [RCW98] založených výhradně na použití asymetrické kryptografie.

2.1 Shrnutí

V této části jsme se seznámili s protokolem EKE, který k ustavení klíče sezení využívá sdíleného hesla v kombinaci se symetrickou i asymetrickou kryptografií a poskytuje ochranu proti off-line útokům hrubou silou. Myšlenka tohoto zcela originálního protokolu se stala základem celé třídy nově vznikajících tzv. eskalačních protokolů. Oproti původnímu EKE zaručují rozšířené (tj. z EKE vycházející) protokoly DHEKE, DWEKE, MEKE či SPEKE navíc *dopřednou bezpečnost* (forward secrecy), což znamená, že kompromitace hesla neumožní útočníkovi získat klíče předcházejících sezení. Navíc začíná být také brán zřetel na to, aby případná kompromitace klíče sezení neumožňovala útoky vedoucí k získání hesla.

Největší problémem všech výše uvedených protokolů však stále zůstává nutnost uchovávat hesla na straně serveru v otevřené podobě. To jako první překonává protokol AEKE, který je rozšířením EKE a umožňuje serveru ukládat hesla jednocestně zašifrována. Nevýhodou této modifikace EKE je, že protokol už nezaručuje dopřednou bezpečnost. Protokol BSPEKE již podobnými nedostatky za cenu podstatného zvýšení výpočetní složitosti netrpí. Efektivnější řešení pak nabízejí protokoly SRP a PDM.

Velkým nedostatkem mnoha z těchto (a jim podobných) protokolů je, že nejsou prezentovány společně s důkazy, které by prokázaly jejich bezpečnost – na několik z nich již byly objeveny útoky (viz např. [Pat97, TM05]). Pokus o formální analýzu bezpečnosti byl proveden pouze u protokolu OKE [Luc97], na nějž byl však v [MPS00] popsán také útok.

3 Moderní kryptografické eskalační protokoly

Mnohé v předcházející části uvedené protokoly se do jisté míry staly základem pro vývoj moderních (a ve většině případů i mnohem složitějších) eskalačních protokolů, jejichž bezpečnost je již typicky nějakým způsobem formálně dokázána.

Prvním protokolem spadajícím do této kategorie je *SNAPI (secure network authentication with password identification)* [MS99]. Tento na RSA založený protokol vychází z OKE (jemuž je také velmi podobný) a jako první eskalační protokol je již představen společně s formálním důkazem jeho bezpečnosti. Jeho rozšířená verze *SNAPI-X (SNAPI-eXtended)* navíc využívá na straně serveru namísto hesel pouze verifikační hodnoty. Použití RSA činí SNAPI i SNAPI-X jen nepatrně pomalejší než SRP.

Na modifikaci DH metody ustavení klíčů je založen protokol *PAK (password-authenticated key exchange)* [BMP00], o němž je také formálně dokázáno, že je bezpečný. Stejně jako v případě SNAPI existuje i u PAK rozšíření *PAK-X (PAK-eXtended)*, zajišťující bezpečnost i v případě kompromitace citlivých informací uložených na straně serveru. V [BMP00] je také navržen poněkud odlišný avšak efektivnější protokol *PPK (password protected key exchange)*.

V [Mac01] je pak představeno několik vylepšení původních protokolů (včetně důkazů jejich bezpečnosti) rodiny PAK: *PAK-R (PAK reduced)*, vedoucí k dvojnásobnému zvýšení efektivity na straně klienta; oproti PAK-X koncepčně jednodušší *PAK-Y*; *PAK-EC* využívající eliptických křivek; a také *PAK-XTR* fungující nad speciálními XTR grupami. Zcela novou metodu zabezpečení citlivých informací na straně serveru využívá *PAK-Z* [Mac02], jehož jeden bezpečnostní nedostatek (společně s chybou v původním důkazu) odstraňuje PAK-Z^+ [GMZ05].

Jednoduchým a (oproti všem předcházejícím protokolům) mnohem efektivnějším protokolem je *AuthA* [BR00], založený opět na DH metodě ustavení klíčů a využívající také verifikačních hodnot na straně

serveru. Tento protokol je v podstatě opět pouze vylepšením klasického DHEKE. Formální důkazy bezpečnosti AuthA byly podány až v [BCP03, BCP04].

Podobné vlastnosti má i poměrně rozsáhlá rodina protokolů *AMP (authentication and key agreement via memorable password)* [Kwo00]. Ta kromě originálního protokolu AMP obsahuje také čtyři jeho základní varianty: AMP^{i}, AMP^{n}, AMP^{+}, AMP^{++}. AMP^{n} je založen pouze na použití hesel, zatímco ostatní varianty protokolu využívají na straně serveru z hesla odvozené verifikační hodnoty. AMP^{i} (podobně jako např. AEKE či SRP) umožňuje navíc (kvůli ztížení případných slovníkových útoků na kompromitovaný soubor s verifikačními hodnotami) využít také solení a AMP^{+} či AMP^{++} zase předcházejí některým specifickým (avšak pravděpodobně nijak kritickým) únikům informací při provádění protokolu. AMP^{i} a AMP^{n} jsou nepatrně efektivnější než AMP a naopak AMP^{+} a AMP^{++} jsou méně efektivní. Všechny tyto protokoly jsou však efektivnější než AuthA a jejich bezpečnost je také formálně dokázána. V [Kwo04] byl později navržen také protokol *TP-AMP (three-pass AMP)*, a v [Kwo05] byl popsán (a odstraněn) jeden bezpečnostní nedostatek protokolu AMP^{+}.

Stejně jako převážná většina předchozích protokolů je i protokol *EPA (efficient password-based protocol)* [HYL02] založen na modifikaci DH metody ustavení klíčů a i on na straně serveru využívá verifikačních hodnot. Za jeho poměrně vysokou efektivitou stojí použití dvou nezávislých generátorů prvočíselných podgrup a v případě protokolu EPA+ navíc i vylepšení mechanizmu výpočtu verifikačních hodnot. Bezpečnost těchto protokolů je také formálně dokazatelná.

PEKEP (password enabled key exchange protocol) [Zha04a] je podobně jako OKE či SNAPI založen na asymetrickém kryptosystému RSA. Oproti protokolu SNAPI, který umožňuje použití pouze veřejných prvočíselných exponentů větších než RSA modul, může navíc PEKEP používat i menší prvočíselné exponenty. Navíc na straně serveru již nevyžaduje provádění časově náročných prvočíselných testů, což jej činí efektivnějším než SNAPI. Jeho modifikace označovaná jako *CEKEP (computationally-efficient key exchange protocol)* umožňuje přidáním dvou přenosů mezi klientem a serverem zmírnit výpočetní zátěž jednotlivých komunikujících stran. Bezpečnost těchto protokolů je také formálně dokázána a jejich jedinou nevýhodou zůstává pouze nutnost uchovávat na straně serveru hesla v otevřené podobě (což platí i pro první eskalační protokol založený na použití kvadratických reziduí – QREKE [Zha04b]).

Svými vlastnostmi poněkud odlišným protokolem je *APAKE (anonymous password-based authenticated key exchange)* [VYT05], který (jak již z názvu plyne) umožňuje na hesle založené anonymní ustavení tajného klíče. Bezpečnost tohoto protokolu je také formálně dokázána.

3.1 Shrnutí

V této části jsme stručně popsali základní vlastnosti několika různých typů eskalačních protokolů, jejichž bezpečnost je již určitým způsobem formálně dokazatelná. Bohužel techniky dokazování (stejně tak jako použité předpoklady) jsou u různých protokolů mnohdy odlišné a pouhé konstatování oznamující existenci formálního důkazu ještě nezaručuje, že jsou všechny protokoly (či jejich instance) vždy skutečně bezpečné.

Například formální důkazy bezpečnosti protokolů SNAPI a SNAPI-X (ale i protokolů PEKEP a CEKEP) navíc, kromě předpokladu bezpečnosti RSA, využívají předpoklad, že se použité hašovací funkce chovají jako náhodné hašovací funkce – tj. využívají k dokazování tzv. *random-oracle model* (někdy též nazývaný *ideal-hash model*), podrobně popsaný v [BR93a]. Tento model je většinou použit tam, kde jsou k provedení důkazu nezbytné silné požadavky na náhodnost výstupu jednotlivých kryptografických hašovacích funkcí. S použitím takto idealizovaných hašovacích funkcí lze snáze dokázat, že je daný protokol bezpečný.

Random-oracle model je využit také při důkazech protokolů rodiny PAK [BMP00]. Tyto protokoly (které jsou postaveny na použití DH metody ustavení klíčů) jsou dokázány jako bezpečné za předpokladu *Decision Diffie-Hellman (DDH)*, což je mnohem silnější předpoklad než v některých jejich pozdějších důkazech použitý *Computational Diffie-Hellman (CDH)*. Za předpokladu DDH totiž nelze o DH metodou ustaveném klíči získat žádnou hodnotnou informaci (tj. nelze předpovědět ani jediný jeho bit). Přesné definice CDH i DDH jsou uvedeny v [Bon98]. Poznamenejme také, že některé důkazy protokolů rodiny PAK nevyžadují předpoklad ideální blokové šifry a jsou proto poměrně komplikované.

Protokol AuthA je za předpokladu CDH dokazatelný jak v random-oracle modelu, tak i ve velmi podobném tzv. *ideal-cipher modelu* (popsaném v [BPR00, BR93b, DP06]). V random-oracle modelu je dále za předpokladu DDH dokazatelných většina protokolů rodiny AMP a protokoly EPA/EPA+; za předpokladu CDH pak také protokol APAKE.

Ačkoliv jsou výše uvedené techniky formálního dokazovaní bezpečnosti pomocí idealizovaných modelů zcela jistě užitečné, může se v praxi stát, že po nahrazení idealizovaných funkcí reálnými funkcemi vznikne instance protokolu, která už bezpečná není. Typickým příkladem je protokol AuthA, který (i přesto že je v ideal-cipher modelu dokázán jako bezpečný) po nahrazení ideálních šifrovacích funkcí reálnými šifrovacími funkcemi (resp. algoritmy) může vykazovat určité bezpečnostní nedostatky umožňující aplikaci nejrůznějších útoků (více viz [ZDW05]). Nově vzniklým problémem nyní je, že (prozatím) neexistuje žádný způsob jak snadno rozlišit chybné (ne příliš bezpečné) instance protokolů od bezchybných (bezpečných) instancí.

4 Aplikace kryptografických eskalačních protokolů

Praktická aplikace kryptografických eskalačních protokolů pokrývá veškeré případy komunikace přes nezabezpečený kanál, kde by dlouhotrvající uchovávání kryptografických klíčů bylo nebezpečné či nepraktické.

Příkladem může být jejich nasazení v dnes poměrně rozšířeném autentizačním sytému Kerberos – analýza a možná integrace eskalačních protokolů do Kerbera je diskutována například v [BM01, Jas96, Wu99]. Dalším uplatněním může být také náhrada zastaralých internetových protokolů (umožňujících vzdálené přihlašování pomocí hesel zasílaných v otevřené podobě) či vylepšení stávajících protokolů. Začlenění eskalačních protokolů do IKE (internet key exchange) je navrženo v [PK01b] a podrobný popis integrace protokolu DHEKE do SSL/TLS protokolu je uveden v [Ste01].

Eskalační protokoly našly uplatnění také v mobilních výpočetních prostředích – zařízení spadající do této kategorie (jako například mobilní telefony, kapesní počítače, kryptografické čipové karty) mají nějakým způsobem omezené prostředky/zdroje (energii, paměť, výkon) a s ostatními (ne nutně pouze mobilními) zařízeními většinou komunikují prostřednictvím bezdrátových sítí. Protože eskalační protokoly jsou založené na použití hesla, které je snadno zapamatovatelné a nemusí být tedy nikde bezpečně uloženo, jsou pro implementaci v mobilních zařízeních naprosto ideální.

Příkladem toho může být vylepšení Bluetooth párovacího protokolu pomocí AMP$^+$ [WSC05] či vznik nových eskalačních protokolů integrovatelných do bezdrátových sítí bez jakékoliv modifikace IEEE 802.1X a EAP (extensible authentication protocol) [YS03]. Návrhy několika dalších eskalačních protokolů, vytvořených speciálně pro nasazení v mobilních zařízeních, zase přesouvají co největší část výpočtů na stranu serveru [WCZ05, ZWCY02]. Zajímavou aplikací může být také zabezpečení vzdáleného přístupu ke kryptografické čipové kartě s podporou technologie Java Card™ [IFH00].

5 Standardizace kryptografických eskalačních protokolů

Standardizací protokolů založených na použití hesla se zabývá pracovní skupina IEEE P1363 – viz draft IEEE P1363.2 [IEEE05]. Cílem tohoto právě vznikajícího dokumentu však není upřednostnění některých technik či protokolů před jinými, ale poskytnutí dostatečného množství různých metod, které se liší jak funkčností, tak také efektivitou. Podrobný popis jednotlivých metod pak slouží jakožto návod k jejich implementaci (a to jak na straně serveru, tak také na straně klienta). V současné době jsou do draftu zapracovány následující námi popsané protokoly: AMP, BSPEKE, PAK, PAK-Z, PPK, SPEKE, SRP3, SRP6. Bohužel, jako mnoho jiných, je i tento draft prozatím značně nepřehledný a bez důkladné znalosti jednotlivých technik a protokolů téměř nečitelný.

Odkazy a literatura

[AL94] R. J. Anderson and T. M. A. Lomas. *On Fortifying Key Negotiation Schemes With Poorly Chosen Passwords.* Electronics Letters, vol. 30, pp. 1040–1041, 1994.

[BCP03] E. Bresson, O. Chevassut, and D. Pointcheval. *Security proofs for an efficient password-based key exchange.* Proceedings of the 10th CCS, pp. 241–250, 2003.

[BCP04] E. Bresson, O. Chevassut, and D. Pointcheval. *New Security Results on Encrypted Key Exchange.* LNCS 2947, pp. 145–158, 2004.

[BM92] S. M. Bellovin and M. Merritt. *Encrypted Key Exchange: Password-based protocols secure against dictionary attacks.* Proceedings of IEEE CS SRSP, pp. 72–84, 1992.

[BM93] S. M. Bellovin and M. Merritt. *Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise.* Proceedings of the First ACM CCS, pp. 244–250, 1993.

[BM94] S. M. Bellovin and M. Merritt. *An attack on the Interlock Protocol When Used for Authentication.* IEEE Transactions on Information Theory, vol. 40, pp. 273–275, 1994.

[BMP00] V. Boyko, P. MacKenzie, and S. Patel. *Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman.* LNCS 1807, pp. 156–171, 2000.

[Bon98] D. Boneh. *The decision Diffie-Hellman problem.* Proceedings of the Third Algorithmic Number Theory Symposium, LNCS 1423, pp. 48–63, 1998.

[BPR00] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated Key Exchange Secure against Dictionary Attacks. LNCS 1807, pp. 139-155, 2000.

[BR00] M. Bellare and P. Rogaway. *The AuthA Protocol for Password-based Authenticated Key Exchange.* Contribution to the IEEE P1363 study group, 2000.

[BR93a] M. Bellare and P. Rogaway. Random oracles are practical. Proceedings of the 1st ACM conference on CCS, pp. 62–73, 1993.

[BR93b] M. Bellare and P. Rogaway. Entity Authentication and Key Distribution. Advances in Cryptology – CRYPTO '93, LNCS 773, pp. 232–249, 1993.

[DH76] W. Diffie and M. E. Hellman. *New Directions in Cryptography.* IEEE Transactions on Information Theory, vol. IT-22, pp. 644–654, November 1976.

[DP06] Yevgeniy Dodis and Prashant Puniya. On the Relation Between the Ideal Cipher and the Random Oracle Models. Accepted Paper for TCC 2006.

[DP89] D. W. Davies and W. L. Price. *Security for computer networks*. John Wiley & Sons, Inc., second edition, 1989.

[GMZ05] C. Gentry, P. MacKenzie, and Z. Ramzan. *PAK-Z+*. Contribution to the IEEE P1363 study group, 2005.

[HYL02] Y. Hwang, D. Yum, and P. Lee. *EPA: an efficient password-based. protocol for authenticated key exchange.* ACISP 2003, LNCS 2727, pp. 452–463, 2003.

[IEEE05] IEEE, Inc. *P1363.2/D22 (Draft version 22) – Standard Specifications for Password-based Public Key Cryptographic Techniques*, 2005.

[IFH00] N. Itoi, T. Fukuzawa, and P. Honeyman. *Secure Internet Smartcards.* LNCS 2041, pp. 73–89, 2000.

[Jab96] D. Jablon. *Strong password-only authenticated key exchange.* Computer Communication Review, vol. 26, pp. 5–26, ACM SIGCOMM, 1996.

[Jab97] D. Jablon. Extended *Password Key Exchange Protocols Immune to Dictionary Attacks.* Proceedings of WET-ICE '97, pp. 248–255, IEEE Computer Society, 1997.

[Jas96] B. Jaspan. *Dual-workfactor Encrypted Key Exchange: Efficiently Preventing Password Chaining and Dictionary Attacks.* Proc. of the 6th USENIX Sec. Symp., pp. 43–50, 1996.

[KKP99] S. Kim, B. Kim, and S. Park. *Comments on password-based private key download protocol of NDSS'99.* Electronics Letters, vol. 35, pp.1937-1938, 1999.

[Kwo00] T. Kwon. *Ultimate Solution to Authentication via Memorable Password.* Contribution to the IEEE P1363 study group for Future PKC Standards, 2000.

[Kwo04] T. Kwon. *Practical Authenticated Key Agreement Using Passwords.* LNCS 3225, pp. 1–12, 2004.

[Kwo05] T. Kwon. *Revision of AMP in IEEE P1363.2 and ISO/IEC 11770-4.* Contribution to the IEEE P1363 study group for Future PKC Standards, 2005.

[LSH01] Chun-Li Lin, Hung-Min Sun, and Tzonelih Hwang. *Efficient and Practical DHEKE Protocols.* ACM SIGOPS OS Review, vol. 35, pp. 41–47, 2001.

[Luc97] S. Lucks. *Open key exchange: How to defeat dictionary attacks without encrypting public keys.* Proceedings of the 5th IWSP, LNCS 1361, pp. 79–90, 1997.

[Mac01] P. MacKenzie. *More Efficient Password-Authenticated Key Exchange.* LNCS 2020, pp. 361–377, 2001.

[Mac02] P. MacKenzie. *The PAK suite: Protocols for Password-Authenticated Key Exchange.* Contribution to the IEEE P1363 study group, 2002.

[MPS00] P. MacKenzie, S. Patel, and R. Swaminathan. *Password-Authenticated Key Exchange based on RSA.* Asiacrypt 2000, LNCS 1976, pp. 599–613, 2000.

[MS99] P. MacKenzie and R. Swaminathan. *The PAK suite: Protocols for Password-Authenticated Key Exchange.* Contribution to the IEEE P1363 study group, 2000.

[Pat97] S. Patel. *Number theoretic attacks on secure password schemes.* IEEE Symposium on Security and Privacy, 1997.

[PK01a] R. Perlman and C. Kaufman. *PDM: A New Strong Password-Based Protocol.* Proceedings of the 10th USENIX Security Symposium, pp. 313–321, 2001.

[PK01b] R. Perlman and C. Kaufman. *Analysis of the IPSec Key Exchange Standard.* WET-ICE '01 – Enterprise Security, pp. 150-156, 2001.

[PK99] R. J. Perlman and C. Kaufman. Secure *Password-Based Protocol for Downloading a Private Key.* Proceedings of the Internet Society NDSS, 1999.

[RCW98] M. Roe, B. Christianson, and D. Wheeler. *Secure Password-Based Protocol for Downloading a Private Key.* TR 445, Univ. of Cambridge and Univ. of Hertfordshire, 1998.

[RS84] R. L. Rivest and A. Shamir. *How to Expose an Eavesdropper.* Communications of the ACM, vol. 27, pp. 393–395, 1984.

[Ste01] Michael Steiner. *Secure password-based. cipher suite for TLS.* ACM TISSEC, pp. 134–157, 2001.

[STW95] M. Steiner, G. Tsudik, and M. Waidner. *Refinement and Extension of Encrypted Key Exchange.* Operating Systems Review, vol. 29, pp. 22–30, ACM SIGOPS, 1995.

[TM05] Qiang Tang and Chris J. Mitchell. *On the security of some password-based key agreement schemes.* Cryptology ePrint Archive, Report 2005/156, 2005.

[VYT05] D. Q. Viet , A. Yamamura , H. Tanaka. *Anonymous Password-based Authenticated Key Exchange.* INDOCRYPT 2005, LNCS 3797, pp. 244–257, 2005.

[WCZ05] D. S. Wong, A. H. Chan, and F. Zhu. *Password Authenticated Key Exchange for Resource-Constrained Wireless Communications.* 2005.

[WSC05] F.-L. Wong, F. Stajano, and J. Clulow. *Repairing the Bluetooth pairing protocol.* Proceedings of 13th SPW 2006.

[Wu02] T. Wu. *SRP-6: Improvements and Refinements to the Secure Remote Password Protocol.* Submission to the IEEE P1363 Working Group, 2002.

[Wu97] T. Wu. *The Secure Remote Password protocol.* Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security, pp. 97–111, 1997.

[YS03] S. J. Yu and J. S. Song. *An Improved Password Authentication Key Exchange Protocol for 802.11 Environment.* LNCS 2668, pp. 201–209, 2003.

[ZDW05] Z. Zhao, Z. Dong, and Y. Wang. *Security analysis of a password-based authentication protocol proposed to IEEE 1363.* To appear in Theoretical Computer Science.

[Zha04a] M. Zhang. *New Approaches to Password Authenticated Key Exchange based on RSA.* ASIACRYPT '04, pp. 230–244, 2004.

[Zha04b] M. Zhang. *Password Authenticated Key Exchange Using Quadratic Residues.* LNCS 3089, pp. 233–247, 2004.

[ZWCY02] F. Zhu, D. S. Wong, A. H. Chan, and R. Ye. *Password authenticated key exchange based on RSA for imbalanced wireless networks.* LNCS 2433, pp. 150–161, 2002.