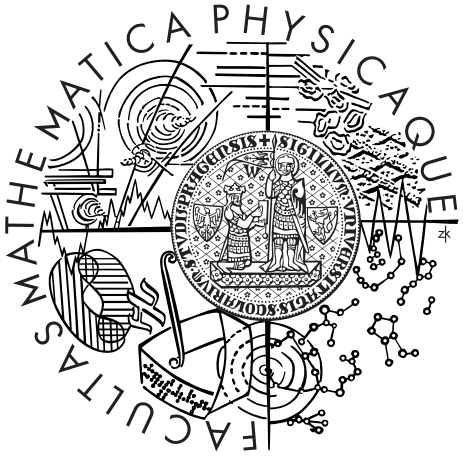
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁRSKA PRÁCA



Monika Sayedová

Nová varianta Diffie-Hellmanova problému

Katedra algebry

Vedúci bakalárskej práce:	doc. Mgr. Štěpán Holub, Ph.D.
Študijný program:	Matematika
Študijný odbor:	matematické metody informační bezpečnosti

Praha 2012

Touto cestou by som rada poďakovala všetkým, ktorí ma podporovali pri písaní tejto bakalárskej práci. Obzvlášť by som rada poďakovala môjmu vedúcemu práce, doc. Mgr. Štěpánovi Holubovi, Ph.D., za čas, odbornú pomoc a cenné rady, ktoré mi poskytol pri jej vypracovaní.

Čestne prehlasujem, že som túto bakalársku prácu vypracovala samostatne a výhradne s použitím citovaných prameňov, literatúry a ďalších odborných zdrojov.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb., autorského zákona v platnom znení, najmä skutočnosť, že Univerzita Karlova v Prahe má právo na uzavretie licenčnej zmluvy na použitie tejto práce ako školského diela podľa §60 odst. 1 autorského zákona.

V ..... dňa ..... Podpis autora

Názov práce: Nová varianta Diffie-Hellmanova problému

Autor: Monika Sayedová

Katedra: Katedra algebry

Vedúci bakalárskej práce: doc. Mgr. Štěpán Holub, Ph.D., Katedra algebry

Abstrakt: Diffie-Hellmanov (DH) problém je problém, o ktorom sa predpokladá, že je ťažký. Preto sa naň redukuje bezpečnosť mnohých kryptografických systémov. V tejto práci sa zoznámime s novou variantou DH problému — so zdvojeným DH problémom. Vytvoríme si metódu, ktorá nám dovolí simulovať rozhodovacie orákulum bez znalosti príslušného diskrétneho logaritmu daných prvkov. Ukážeme si zdvojené ElGamalovo šifrovanie a jeho bezpečnosť v modele náhodného orákula. ElGamalovo šifrovanie je bezpečné pri útoku vybraním zašifrovaného textu za predpokladu, že je proti tomuto útoku bezpečná aj príslušná symetrická šifra. Dokážeme si, že zdvojený DH protokol na neinteraktívnu výmenu kľúča je v modele náhodného orákula bezpečný proti aktívnym útokom. V oboch prípadoch stačí predpokladať platnosť DH predpokladu.

Kľúčové slová: zdvojené Diffie-Hellmanove predpoklady, zdvojené ElGamalovo šifrovanie, zdvojený Diffie-Hellmanov protokol, trapdoor test, asymetrická kryptografia

Title: New version of the Diffie-Hellman problem

Author: Monika Sayedová

Department: Department of Algebra

Supervisor: doc. Mgr. Štěpán Holub, Ph.D., Department of Algebra

Abstract: The Diffie-Hellman (DH) problem is a problem that is assumed to be difficult to do, hence the security of many cryptographic protocols is reduced to this problem. We show a new variant of the DH problem — the twin DH problem. We propose a method which allows us to simulate a decision oracle without knowing the discrete logarithms of the elements. We show twin ElGamal encryption and its security in a random oracle model. ElGamal is secure against chosen ciphertext attack when we assume that the symmetric encryption is secure against chosen ciphertext attack and the DH problem is hard. We prove that the DH non-interactive key exchange protocol is secure against an active attack in a random oracle model when the DH problem holds.

Keywords: twin Diffie-Hellman assumptions, twin Diffie-Hellman protocol, twin ElGamal encryption, trapdoor test, public key encryption

Obsah

Úvod

V novembri roku 1976 vyšla publikácia New Directions in Cryptography [7], v ktorej autori Whitfield Diffie a Martin E. Hellman predstavili Diffie-Hellmanov protokol na výmenu kľúča. Výsledkom protokolu je dohodnutie sa na spoločnom kľúči, ktorý slúži na symetrické šifrovanie. Protokol je založený na diskrétnom logaritme a je bezpečný pri nespoľahlivých kanáloch, kde má útočník možnosť odpočúvania. Diffie-Hellmanov protokol bol revolučným krokom v kryptografii. V roku 2009 vyšiel článok The Twin Diffie-Hellman Problem and Applications [4]. Autormi sú David Cash, Eike Kiltz a Victor Shoup. A práve tento článok je podnetom pre túto bakalársku prácu.

V prvej kapitole sa najprv zoznámime s pojmami symetrické šifrovanie, asymetrické šifrovanie a neinteraktívna schéma na výmenu kľúča. Pritom vychádzame z literatúr [2, 8, 4]. Popíšeme si jednotlivé schémy a následne si povieme niečo o modele ich bezpečnosti. Tieto poznatky sú čerpané z [8, 4, 3]. Pri bezpečnosti uvažujeme aktívneho útočníka, ktorý je schopný v nejakom smere meniť správanie účastníkov a zasahovať do siete. Pri symetrickom a asymetrickom šifrovaní je bezpečnosť založená na hre, pri ktorej útočník vkladá zašifrované správy podľa svojej voľby do siete, teda útočí pomocou vybrania zašifrovaného textu. Jeho úlohou je uhádnuť, ktorú z dvoch správ mu vyzývateľ zašifroval. Pri neinteraktívnej schéme na výmenu kľúča je bezpečnosť založená na hre s aktívnym útočníkom. Ten je v útoku úspešný, pokiaľ sa mu podarí odhaliť, či bit, ktorý si na začiatku útoku vyzývateľ zvolil, bol generovaný náhodne, alebo pomocou daného algoritmu. Bližšie a podrobnejšie sa s útočníkmi zoznámime v prvej kapitole.

Zadefinujeme si Diffie-Hellmanove predpoklady, ktoré budeme označovať DH predpoklady a zdvojené Diffie-Hellmanove predpoklady, ktoré budeme označovať 2DH predpoklady. Ako je už vyššie spomenuté, predpokladá sa, že DH problém je ťažký, preto sa naň redukuje bezpečnosť mnohých kryptografických systémov. Definície DH a 2DH predpokladov vychádzajú z kníh [5, 4]. Pri ich definovaní sa budeme snažiť postupovať intuitívne, zvolíme formu ako v [4]. Tieto definície dáme do súvislosti s hašovaným ElGamalovým šifrovaním. Ukážeme si, že 2DH predpoklad je len málo pozmenený DH predpoklad a je rovnako užitočný. Má rôzne zaujímavé vlastnosti. Výhodou je, že 2DH predpoklad zostáva ťažký, aj keď má útočník prístup do príslušného rozhodovacieho orákula. Pritom predpokladáme, že platí DH predpoklad.

Dôležitým dôsledkom zavedenia pojmu 2DH predpoklad je „trapdoor test“. Tento trapdoor test [4, 9] je technika, pomocou ktorej dokáže útočník s určitou pravdepodobnosťou „simulovať“ rozhodovacie orákulum. S akou, si povieme v tretej kapitole. Samozrejme predpokladáme, že útočník nepozná diskrétny logaritmus prvkov.

Aplikáciu [4] si ukážeme napríklad na zdvojenom ElGamalovom šifrovaní. Ukážeme si, že vďaka zdvojeniu je táto šifrovacia schéma bezpečná proti útoku vybraním zašifrovaného textu. Potrebujeme predpokladať, že príslušná symetrická šifra je tiež bezpečná. Predpokladajme platnosť DH predpokladu. Ďalšou aplikáciou, ktorú si podrobne rozoberieme, je Diffie-Hellmanov protokol. Ten slúži na neinteraktívnu výmenu kľúča medzi dvoma užívateľmi. Aj tentokrát nám pre zavedenie bezpečnosti proti aktívnemu útoku bude postačovať predpokladať,

že DH problém je ťažký. Možnosť aplikácie je oveľa širšia. Niektoré schémy sú popísané napríklad v [4]. Patria k nim nová varianta Cramer-Shoupovho šifrovania, nová varianta Boneh-Franklinovho šifrovania založeného na identite, protokol na výmenu kľúča založeného na autentifikácii heslom od Abdalla a Pointchevala, Shoupov Diffie-Hellmanov „samoopravovač“,...

1. Vybrané schémy a ich bezpečnosť

Predtým, než si popíšeme jednotlivé šifrovacie schémy, povedzme si niečo o našej predstave útočníka. Útočníkov môžeme podľa ich „schopností“ rozdeliť na dva základné typy — aktívnych a pasívnych. Pasívny útočník dokáže len odpočúvať, pričom pri aktívnom útočníkovi predpokladáme, že má okrem toho aj schopnosť vkladať správy do siete, či inak ovplyvňovať správanie účastníkov. V tejto práci sa budeme zaoberať práve tým silnejším — aktívnym — útočníkom. Vysporiadame sa s ním tak, ako Rackoff a Simon vo svojej práci [1]. Teda si zavedieme bezpečnosť proti prispôsobivému útoku vybraním zašifrovaného textu (po anglicky adaptive chosen ciphertext attack). Pre potreby tohto textu označme prispôsobivý útok vybraním zašifrovaného textu ako CCA.

CCA je interaktívny útok, pri ktorom útočník vkladá zašifrované správy do siete a je schopný vybrať čiastočnú informáciu o príslušnom otvorenom texte pomocou jeho interakcie s účastníkmi v sieti. Pri tomto modele útoku útočník získa dešifrovaný text podľa svojej voľby, tj. útočník má prístup do „dešifrovacieho orákula“. Pri cieľovej zašifrovanej správe chceme garantovať, že útočník o nej nemôže získať hocijakú čiastočnú informáciu. Aby sme to dosiahli, musíme nejako obmedziť útočníkove správanie, inak by mohol útočník jednoducho predložiť cieľový zašifrovaný text do dešifrovacieho orákula. Obmedzenie bude to najslabšie možné, útočník nebude mať povolené predložiť cieľový zašifrovaný text do orákula. Zato ale môže predložiť hocijakú inú zašifrovanú správu, vrátane správy, ktorá bude len málo pozmenená. S presným popisom tohto útočníka sa zoznámime nižšie.

1.1 Symetrické šifrovanie

Princíp symetrického šifrovania spočíva v tom, že odosielateľ a príjemca správy spolu zdieľajú spoločný tajný kľúč. Pred prvým posielaním správ sa musia na tomto spoločnom kľúči dohodnúť. To je možné napríklad pomocou bezpečného kanála, osobným stretnutím, použitím algoritmu na bezpečnú výmenu kľúča,... Predpokladajme, že pri útoku na takúto schému je útočník aktívny. Útočiť bude pomocou útoku typu CCA, ktorý sme popísali vyššie.

1.1.1 Model

Nech $\mathcal{P} = \{0,1\}^*$ označuje konečnú množinu otvorených správ, $\mathcal{C} = \{0,1\}^*$ konečnú množinu zašifrovaných správ a $\mathcal{K} = \{0,1\}^n$ množinu kľúčov pre $n \in \mathbb{N}$. Symetrická šifrovacia schéma je dvojica algoritmov (E, D).

Šifrovací algoritmus E je pravdepodobnostný polynomiálny algoritmus, ktorý má na vstupe kľúč $k \in \mathcal{K}$ a otvorený text $m \in \mathcal{P}$. Výstupom je zašifrovaný text $c = \mathsf{E}(k, m)$.

Dešifrovací algoritmus D je deterministický polynomiálny algoritmus, ktorý na vstupe prijme kľúč $k \in \mathsf{K}$ a domnelý zašifrovaný text $c \in \mathcal{C}$. Na výstupe vracia hodnotu $\mathsf{D}(k, c) \in \mathcal{P} \cup \{chyba\}$. Hodnota „chyba“ vyjadruje, že je domnelý

zašifrovaný text považovaný za neplatný, teda že nevznikol zašifrovaním žiadneho otvoreného textu. Požadujeme, aby

$$\forall m \in \mathcal{P}, k \in \mathcal{K} : \mathsf{D}(k, \mathsf{E}(k, m)) = m.$$

1.1.2 Bezpečnosť

Uvažujme o bezpečnosti proti útoku vybraním zašifrovaného textu (CCA) s útočníkom popísaným vyššie. Definujme ju nasledujúcou CCA „hrou“. V nej medzi sebou komunikujú vyzývateľ $\mathcal{CH}$ a útočník $\mathcal{A}$.

1. Vyzývateľ $\mathcal{CH}$ vygeneruje kľúč. Ten je tajný, nikam ho neposiela. Útočník $\mathcal{A}$ bude útočiť v dvoch fázach.

2. V prvej fáze, *fáze hľadania*, bude $\mathcal{A}$ klásť dešifrovacie otázky vyzývateľovi. To znamená, že sa útočník spýta na zašifrovaný text $\widehat{c}$ a vyzývateľ mu naň odpovie jeho dešifrovaním: $\mathsf{D}(k, \widehat{c})$. Otázky môžu byť kladené adaptívne, nie je nutné, aby správa, ktorú útočník predkladá, vznikla šifrovaním.

3. Konverzácia popísaná v druhom kroku prebieha, pokým sa $\mathcal{A}$ nerozhodne vyzývateľovi zaslať pár správ (m_0, m_1). Tým je prvá fáza ukončená. $\mathcal{CH}$ vypočíta $b \xleftarrow{R} \{0,1\}; c \xleftarrow{R} \mathsf{E}(k, m_b)$. Útočníkovi odpovie zaslaním výsledného zašifrovaného textu c.

4. Prichádza druhá fáza útočníka $\mathcal{A}$ — *fáza hádania*. Tak ako v druhom kroku, aj teraz bude $\mathcal{A}$ klásť dešifrovacie otázky vyzývateľovi. Tentokrát ale s podmienkou, že $\widehat{c} \neq c$. Tak ako predtým, otázky môžu byť kladené adaptívne, $\mathcal{A}$ môže vypočítať $\widehat{c}$ ako funkciu z c.

5. Fáza hádania sa ukončí odpoveďou $\mathcal{A}$. Odpovie $\widehat{b} \in \{0,1\}$.

Označme symetrické šifrovanie ako SE (z anglického symmetric encryption). Definujme si CCA výhodu útočníka $\mathcal{A}$ nad asymetrickým šifrovaním

$$\mathsf{AdvCCA}_{\mathcal{A},\mathsf{SE}} = |Pr[\widehat{b} = b] - \frac{1}{2}|.$$

Schéma je bezpečná, ak je výhoda všetkých efektívnych útočníkov zanedbateľná.

1.2 Asymetrické šifrovanie

Asymetrické šifrovanie je založené na verejnom a súkromnom kľúči. Teda jeho výhodou oproti symetrickému šifrovaniu je, že odosielateľ a príjemca správy spolu nemusia zdieľať spoločné tajomstvo. Tak ako pri symetrickom šifrovaní predpokladajme, že pri útoku na takúto schému je útočník aktívny. Útočiť bude pomocou útoku typu CCA, ktorý sme popísali vyššie.

1.2.1 Model

Nech $\mathcal{P} = \{0,1\}^*$ označuje konečnú množinu otvorených správ a $\mathcal{C} = \{0,1\}^*$ konečnú množinu zašifrovaných správ. Nech $\mathsf{PK} \subseteq \{0,1\}^*$ a $\mathsf{SK} \subseteq \{0,1\}^*$ sú množiny reťazcov. Asymetrická šifrovacia schéma je trojica algoritmov $(\mathsf{E}, \mathsf{D}, \mathsf{K})$.

Šifrovací algoritmus E je pravdepodobnostný polynomiálny algoritmus, ktorý má na vstupe verejný kľúč $pk \in \mathsf{PK}$ a otvorený text $m \in \mathcal{P}$. Výstupom je zašifrovaný text $c = \mathsf{E}(pk, m)$.

Dešifrovací algoritmus D je deterministický polynomiálny algoritmus, ktorý na vstupe prijme súkromný kľúč $sk \in \mathsf{SK}$ a domnelý zašifrovaný text $c \in \mathcal{C}$. Na výstupe vracia hodnotu $\mathsf{D}(sk, c) \in \mathcal{P} \cup \{chyba\}$. Ako predtým, hodnota „chyba“ vyjadruje, že je domnelý zašifrovaný text považovaný za neplatný, teda že nevznikol zašifrovaním žiadneho otvoreného textu.

Algoritmus K *na generovanie kľúča* je pravdepodobnostný polynomiálny algoritmus. Vygeneruje pár verejného/súkromného kľúča $(pk, sk) \in \mathsf{PK} \times \mathsf{SK}$. Požadujeme, aby

$$\forall m \in \mathcal{P}, (pk, sk) \in \mathsf{PK} \times \mathsf{SK} : \mathsf{D}(sk, \mathsf{E}(pk, m)) = m.$$

1.2.2 Bezpečnosť

Uvažujme o bezpečnosti proti útoku vybraním zašifrovaného textu (CCA) s útočníkom popísaným vyššie. Bezpečnosť popíšme nasledujúcou CCA „hrou“. V nej medzi sebou komunikujú vyzývateľ $\mathcal{CH}$ a útočník $\mathcal{A}$. Postupujeme analogicky, ako pri symetrickom šifrovaní.

1. Vyzývateľ $\mathcal{CH}$ spustí algoritmus K a vygeneruje pár verejného/súkromného kľúča: $(pk, sk) \xleftarrow{R} \mathsf{K}$. Verejný kľúč dá útočníkovi $\mathcal{A}$. Ten bude útočiť v dvoch fázach.

2. V prvej fáze, *fáze hľadania*, kladie $\mathcal{A}$ dešifrovacie otázky vyzývateľovi. To znamená, že sa útočník spýta na správu $\widehat{c}$ a $\mathcal{CH}$ na ňu odpovie $\mathsf{D}(sk, \widehat{c})$. Otázky môžu byť kladené adaptívne, nie je nutné, aby správa, ktorú útočník predkladá, vznikla šifrovaním.

3. Táto konverzácia prebieha, pokým sa $\mathcal{A}$ nerozhodne vyzývateľovi $\mathcal{CH}$ zaslať pár správ (m_0, m_1). Tým je prvá fáza ukončená. $\mathcal{CH}$ vypočíta $b \xleftarrow{R} \{0,1\}; c \xleftarrow{R} \mathsf{E}(pk, m_b)$. Vyzývateľ útočníkovi odpovie zaslaním výsledného zašifrovaného textu c.

4. Prichádza druhá fáza útočníka $\mathcal{A}$ — *fáza hádania*. Tak ako v druhom kroku, aj teraz bude $\mathcal{A}$ klásť dešifrovacie otázky vyzývateľovi. Tentokrát ale s podmienkou, že $\widehat{c} \neq c$. Tak ako predtým, otázky môžu byť kladené adaptívne, $\mathcal{A}$ môže vypočítať $\widehat{c}$ ako funkciu z c.

5. Fáza hádania sa ukončí odpoveďou $\mathcal{A}$. Odpovie $\widehat{b} \in \{0,1\}$.

Označme asymetrické šifrovanie ako PKE (z anglického public key encryption). Definujme si CCA výhodu útočníka $\mathcal{A}$ nad asymetrickým šifrovaním

$$\mathsf{AdvCCA}_{\mathcal{A},\mathsf{PKE}} = |Pr[\widehat{b} = b] - \frac{1}{2}|.$$

Teda táto schéma je bezpečná, ak je výhoda všetkých efektívnych útočníkov zanedbateľná.

1.3 Neinteraktívna schéma na výmenu kľúča

Pokiaľ chceme zašifrovať správu, či naopak dešifrovať prijatú správu, potrebujeme k tomu príslušný kľúč. Neinteraktívna schéma na výmenu kľúča slúži na to, aby si odosielateľ a príjemca správy vytvorili spoločné tajomstvo, v mojom prípade spoločný zdieľaný kľúč. Naďalej predpokladáme, že pri útoku na takúto schému je útočník aktívny. Útočiť bude pomocou aktívneho útoku, ktorý je popísaný nižšie.

1.3.1 Model

Neinteraktívna schéma na výmenu kľúčov je dvojica algoritmov (K, P).

Algoritmus K *na generovanie kľúčov* je pravdepodobnostný polynomiálny algoritmus, ktorého výstupom je pár verejného/súkromného kľúča.

Algoritmus P *na spárovanie kľúčov* dostane na vstupe jednu identitu, ktorá charakterizuje užívateľa, spolu s jej verejným kľúčom a druhú identitu spolu s jej súkromným kľúčom. Výstupom je zdieľaný kľúč pre dve identity. Identita užívateľa je uniformne náhodný reťazec.

1.3.2 Bezpečnosť

Aj tentokrát budeme bezpečnosť charakterizovať pomocou experimentu medzi vyzývateľom $\mathcal{CH}$ a útočníkom $\mathcal{A}$.

1. Vyzývateľ si ako vstup vezme bit b. Následne odpovedá na otázky útočníka $\mathcal{A}$.

2. Vyzývateľ odpovedá na nasledujúce typy otázok od útočníka:

   Zaregistrovanie dôveryhodného ID užívateľa. Útočník $\mathcal{A}$ chce zaregistrovať nejakú identitu. Napríklad nech zastupuje identitu id. Vyzývateľ spustí algoritmus K na generovanie kľúčov a vygeneruje pár verejného/súkromného kľúča $(\mathsf{pk}, \mathsf{sk})$. Uloží si do zoznamu štvoricu $(\text{dôveryhodný}, id, \mathsf{pk}, \mathsf{sk})$. Útočníkovi odpovie verejným kľúčom pk.

   Zaregistrovanie nedôveryhodného ID užívateľa. Tentokrát $\mathcal{A}$ zastupuje nielen identitu id, ale aj jej verejný kľúč pk. Vyzývateľ nič negeneruje, do zoznamu si uloží trojicu $(\text{nedôveryhodný}, id, \mathsf{pk})$.

   Získanie dôveryhodného spárovaného kľúča. $\mathcal{A}$ zastupuje dve identity: id, id'. Obe boli zaregistrované ako dôveryhodní užívatelia. Vyzývateľ použije bit b z prvého kroku. Ak $b = 0$, tak vyzývateľ spustí algoritmus P na spárovanie kľúčov. Vstupom do tohto algoritmu sú identity id, id', verejný kľúč identity id a súkromný kľúč identity id'. Výstup pošle útočníkovi. Pokiaľ $b = 1$, tak si vyzývateľ vygeneruje uniformne náhodný kľúč k a ten vráti útočníkovi. Aby sa zachovala konzistencia, vyzývateľ odpovie tento istý kľúč k, ak sa útočník spýta na spárovaný kľúč identít id, id' alebo identít id', id.

Získanie nedôveryhodného spárovaného kľúča. Ako predtým, útočník $\mathcal{A}$ zastupuje dve identity: id, id'. Tentokrát je ale id registrovaná ako nedôveryhodná identita a id' ako dôveryhodná. Vyzývateľ vygeneruje spárovaný kľúč pomocou algoritmu P a pošle ho útočníkovi. Vstupom do algoritmu sú identity id, id', verejný kľúč identity id a súkromný kľúč identity id'.

3. $\mathcal{A}$ odpovie bit $\widehat{b}$. Experiment vyhráva, pokiaľ $\widehat{b} = b$.

Označme neinteraktívnu schému na výmenu kľúča ako KE (z anglického non-interactive key exchange). Ďalej si označme aktívny útok útočníka ako AA (z anglického active attack). Definujme si AA výhodu útočníka $\mathcal{A}$ nad neinteraktívnou výmenou kľúča

$$\mathsf{AdvAA}_{\mathcal{A},\mathsf{KE}} = |Pr[\widehat{b} = b] - \frac{1}{2}|.$$

Teda táto schéma je bezpečná, ak je výhoda všetkých efektívnych útočníkov zanedbateľná.

Poznamenajme, že pri CCA experimente útočník vyhráva, pokiaľ uhádne, ktorá z dvoch správ bola zašifrovaná. Pri AA experimente útočník vyhráva, pokiaľ odhalí, či bola odpoveď vygenerovaná uniformne náhodne, alebo či pomocou algoritmu P.

2. Varianty Diffie-Hellmanových predpokladov

Motiváciou k pojmu Diffie-Hellmanov predpoklad je v tomto texte hašované ElGamalovo šifrovanie. Táto šifrovacia schéma je variantou ElGamalovho šifrovania a je popísaná o niečo nižšie. Je založená na Diffie-Hellmanovej výmene kľúča, čo si pozorný čitateľ určite hneď všimne. Preto nás ElGamalova šifrovacia schéma bude v rôznych variantách sprevádzať počas celej mojej práce. Predtým, než sa pustíme do tejto kapitoly, pripomeňme si, že pre uľahčenie budeme Diffie-Hellman označovať ako DH. Toto označenie aplikujme pre celý zvyšok práce.

Hašované ElGamalovo šifrovanie [4] je asymetrický šifrovací systém. Je definovaný nad konečnou cyklickou grupou $\mathbb{G}$ rádu q, kde q je prvočíslo. Generátorom tejto grupy je prvok $g \in \mathbb{G}$. Zaveďme označenie H pre hašovaciu funkciu a (E, D) pre symetrickú šifru. Keďže sa jedná o asymetrickú šifrovaciu schému, má verejný a súkromný kľúč, ktoré sú vygenerované pomocou algoritmu $\mathsf{K}{:}(X, x) \xleftarrow{R} \mathsf{K}$. Verejným kľúčom je prvok $X \in \mathbb{G}$ a príslušným súkromným kľúčom je x. Medzi nimi platí vzťah $X = g^x$.

Šifrovanie:
Šifrovací algoritmus asymetrickej šifry dostane na vstupe verejný kľúč X a správu m, ktorú chceme zašifrovať. Vyberme si uniformne náhodný prvok $y \in \mathbb{Z}_q$ a vypočítajme

$$Y := g^y,\ Z := X^y,\ k := \mathsf{H}(Y, Z),\ c := \mathsf{E}(k, m),$$

Výsledkom je zašifrovaný text (Y, c).

Dešifrovanie:
Dešifrovací algoritmus asymetrickej šifry dostane na vstupe súkromný kľúč x a zašifrovanú správu (Y, c). Dešifrovanie prebieha jednoducho. Vypočítame

$$Z := Y^x,\ k := \mathsf{H}(Y, Z),\ m := \mathsf{D}(k, c).$$

Všimnime si, že je tento systém bezpečný, iba ak nevieme vypočítať Z. Inak povedané, je „ťažké“ vypočítať Z, keď máme k dispozícii len hodnoty X a Y. A práve tento problém, problém vypočítania Z, si nazveme DH problémom.

2.1 DH predpoklady

Definícia. *Nech $\mathbb{G}$ je konečná cyklická grupa rádu q s generátorom $g \in \mathbb{G}$, kde q je prvočíslo. Nech $X = g^x$, $Y = g^y$ a $Z = g^{xy}$ pre $x, y \in \mathbb{Z}_q$ a $X, Y, Z \in \mathbb{G}$. Definujme $\mathsf{dh}(X, Y) := Z$. Problém vypočítania $\mathsf{dh}(X, Y)$, ak máme dané uniformne náhodné prvky $X, Y \in \mathbb{G}$, sa nazýva DH problém.*

DH predpoklad [4] tvrdí, že je tento problém ťažký, je založený na probléme diskrétneho logaritmu. Pripomeňme si definíciu diskrétneho logaritmu a jeho problému [5]:

Definícia. *Nech $\mathbb{G}$ je konečná cyklická grupa rádu n. Nech $\alpha \in \mathbb{G}$ je generátor grupy $\mathbb{G}$ a nech $\beta \in \mathbb{G}$. Diskrétny logaritmus β pri základe α, označme $\log_\alpha \beta$, je jednoznačné číslo x, $0 \leq x \leq n-1$, také, že $\beta = \alpha^x$.*

Definícia. *Problém diskrétneho logaritmu je nasledujúci: majme dané prvočíslo p, generátor $\alpha \in \mathbb{Z}_p^*$ a prvok $\beta \in \mathbb{Z}_p^*$, nájdime číslo x, $0 \leq x \leq p-2$, také, že $\alpha^x \equiv \beta \pmod{p}$.*

DH predpoklad sa zvykne nazývať aj *výpočtový* DH *predpoklad*. Označuje sa CDH (z anglického computational Diffie-Hellman assumption) [2].

Pozorovanie. Tento predpoklad nie je dostatočný na zabezpečenie hašovaného ElGamalovho šifrovania proti útoku typu CCA bez ohľadu na to, aké bezpečnostné vlastnosti má hašovacia funkcia H.

Predpokladajme útočníka, ktorý si uniformne náhodne zvolí prvky $\widehat{Y}, \widehat{Z} \in \mathbb{G}$. Vypočíta si kľúč $\widehat{k} := H(\widehat{Y}, \widehat{Z})$ a pomocou neho zašifruje ľubovoľnú správu $\widehat{m}$: $\widehat{c} := \mathsf{E}(\widehat{k}, \widehat{m})$. Ďalej predpokladajme, že útočník dá zašifrovaný text $(\widehat{Y}, \widehat{c})$ do „dešifrovacieho orákula“ a získa dešifrovanú správu m. Je veľmi pravdepodobné, že $\widehat{m} = m$ práve vtedy, keď $\widehat{Z} = \mathsf{dh}(X, \widehat{Y})$. Vidíme, že dešifrovacie orákulum môže byť útočníkom použité ako orákulum, ktoré zodpovie otázku: „Je $\mathsf{dh}(X, \widehat{Y}) = \widehat{Z}$?“ pre ľubovoľne zvolené $\widehat{Y}, \widehat{Z} \in \mathbb{G}$. Útočník nevie odpovedať na takúto otázku, takže mu dešifrovacie orákulum dáva nejaké informácie o súkromnom kľúči x. Tie môže použiť k prelomeniu šifrovacej schémy.

Preto, pokiaľ chceme zabezpečiť hašované ElGamalovo šifrovanie proti útoku typu CCA, potrebujeme silnejší predpoklad. To nás intuitívne vedie k tomu, aby sme si zaviedli pojem silný DH predpoklad. Predtým, než tak urobíme, zadefinujme si pre $X, \widehat{Y}, \widehat{Z} \in \mathbb{G}$ predikát

$$\mathsf{dhp}(X, \widehat{Y}, \widehat{Z}) := \mathsf{dh}(X, \widehat{Y}) \stackrel{?}{=} \widehat{Z}.$$

Definícia. *Nech $\mathbb{G}$ je konečná cyklická grupa rádu q s generátorom $g \in \mathbb{G}$, kde q je prvočíslo. Nech $X, Y \in \mathbb{G}$ a nech $\mathsf{dh}(X, Y)$ a $\mathsf{dhp}(X, ., .)$ sú definované ako vyššie. Problém vypočítania $\mathsf{dh}(X, Y)$ pri daných uniformne náhodných prvkoch X, Y a za predpokladu prístupu do rozhodovacieho orákula pre predikát $\mathsf{dhp}(X, ., .)$, ktorý na vstupe $(\widehat{Y}, \widehat{Z})$ vracia výstup $\mathsf{dh}(X, \widehat{Y}, \widehat{Z})$, sa nazýva silný* DH *problém.*

Silný DH predpoklad [4] tvrdí, že je tento problém ťažký. Pokiaľ by čitateľa zaujímal dôkaz bezpečnosti hašovaného ElGamalovho šifrovania proti útoku typu CCA, odporúčam literatúru [2, 3]. Je potrebné predpokladať nielen platnosť silného DH predpokladu, ale aj to, že symetrická šifra je sama o sebe bezpečná proti útoku typu CCA a že hašovacia funkcia H je modelovaná ako náhodné orákulum. V tejto kapitole sa tým dôkazom zaoberať nebudeme, pre nás bude oveľa zaujímavejší dôkaz bezpečnosti pre zdvojené ElGamalovo šifrovanie, ktoré si ukážeme neskôr.

Ďalším DH problémom je rozhodovací DH problém. Rozhodovací DH predpoklad tvrdí, že žiaden efektívny algoritmus nerozlíši medzi dvoma distribúciami $(X, Y, \mathsf{dh}(X, Y))$ a (X, Y, Z), teda sú výpočtovo nerozlíšiteľné pre uniformne náhodné prvky $X, Y, Z \in \mathbb{G}$. Alebo inak povedané, nie je efektívny pravdepodobnostný algoritmus, ktorý pre danú trojicu (X, Y, Z) dá výstup „1“, keď $\mathsf{dh}(X, Y) = Z$, inak vráti „0“.

Definícia. *Nech $\mathbb{G}$ je konečná cyklická grupa rádu q s generátorom $g \in \mathbb{G}$, kde q je prvočíslo. Nech X, Y sú uniformne náhodné prvky grupy $\mathbb{G}$. Nech $Z \in \mathbb{G}$ je buď $\mathsf{dh}(X, Y)$ alebo uniformne náhodný prvok, každé s polovičnou pravdepodobnosťou.*

Určenie, či $Z = \mathsf{dh}(X, Y)$*, alebo či je* Z *uniformne náhodné, je rozhodovací* DH *problém.*

Rozhodovací DH predpoklad [4] tvrdí, že je tento problém ťažký. Označuje sa DDH (z anglického decision Diffie-Hellman assumption) [2, 10, 11]. Prelomenie DDH implikuje konštrukciu polynomiálneho útočníka, ktorý dokáže rozlišovať medzi $Z = \mathsf{dh}(X, Y)$ a uniformne náhodným Z s nezanedbateľnou výhodou.

Zadefinujme si hašované varianty týchto dvoch predpokladov [4].

Definícia. *Nech* $\mathbb{G}$ *je konečná cyklická grupa rádu* q *s generátorom* $g \in \mathbb{G}$*, kde* q *je prvočíslo. Nech* $\mathsf{H} : \mathbb{G} \to \{0,1\}^{\mathcal{K}}$ *je hašovacia funkcia a nech* $X, Y \in \mathbb{G}$ *sú uniformne náhodné prvky. Nech* $k \in \{0,1\}^{\mathcal{K}}$ *je buď* $\mathsf{H}(\mathsf{dh}(X, Y))$ *alebo uniformne náhodný prvok, každé s polovičnou pravdepodobnosťou. Určenie, či* $k = \mathsf{H}(\mathsf{dh}(X, Y))$*, alebo či je* k *uniformne náhodné, je hašovaný* DDH *problém.*

Hašovaný DDH predpoklad tvrdí, že je tento problém ťažký. Silný hašovaný DDH predpoklad tvrdí, že je tento problém ťažký, aj keď máme prístup do orákula pre predikát $\mathsf{dhp}(X, ., .)$.

2.2 2DH predpoklady

2DH predpoklad je len slabo pozmenená verzia DH predpokladu. Hlavným dôsledkom je, že tento 2DH predpoklad sa dá využiť v rovnakých kryptografických schémach, kde by sme použili DH predpoklad a zároveň platí, že zostáva ťažký, aj keď má útočník prístup do príslušného rozhodovacieho orákula. Pripomeňme si, že zdvojené DH predpoklady označujeme 2DH predpoklady. Toto označenie aplikujme pre zvyšok tejto práce. Postupujme analogicky, ako pri obyčajných DH predpokladoch.

Definícia. *Nech* $\mathbb{G}$ *je cyklická grupa s generátorom* g*, prvočíselného rádu* q*. Nech* $X_1, X_2, Y \in \mathbb{G}$ *a nech* $\mathsf{dh}(., .)$ *je definované ako predtým. Definujme* 2DH *funkciu*

$$\begin{aligned} \mathsf{2dh} : \quad & \mathbb{G}^3 \to \mathbb{G}^2 \\ & (X_1, X_2, Y) \mapsto (\mathsf{dh}(X_1, Y), \mathsf{dh}(X_2, Y)). \end{aligned}$$

Problém vypočítania $\mathsf{2dh}(X_1, X_2, Y)$*, ak máme dané uniformne náhodné prvky* $X_1, X_2, Y \in \mathbb{G}$*, sa nazýva* 2DH *problém.*

2DH predpoklad [4] tvrdí, že je tento problém ťažký. Analogicky k DH predpokladu môžeme tento predpoklad označovať 2CDH. Je jasné, že DH predpoklad implikuje 2DH predpoklad. Príslušný 2DH *predikát* je:

$$\mathsf{2dhp}(X_1, X_2, \widehat{Y}, \widehat{Z}_1, \widehat{Z}_2) := \mathsf{2dh}(X_1, X_2, \widehat{Y}) \stackrel{?}{=} (\widehat{Z}_1, \widehat{Z}_2).$$

Definícia. *Nech* $\mathbb{G}$ *je konečná cyklická grupa rádu* q *s generátorom* $g \in \mathbb{G}$*, kde* q *je prvočíslo. Nech* $X_1, X_2, Y \in \mathbb{G}$ *a nech* $\mathsf{2dh}(X, Y)$ *a* $\mathsf{2dhp}(X_1, X_2, ., ., .)$ *sú definované ako vyššie. Problém vypočítania* $\mathsf{2dh}(X_1, X_2, Y)$ *pri daných uniformne náhodných prvkoch* X_1, X_2, Y *a za predpokladu prístupu do rozhodovacieho orákula pre predikát* $\mathsf{2dhp}(X_1, X_2, ., ., .)$*, ktorý na vstupe* $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$ *vracia výstup* $\mathsf{2dh}(X_1, X_2, \widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$*, sa nazýva silný* 2DH *problém.*

Silný 2DH predpoklad [4] tvrdí, že je tento problém ťažký.

Rozhodovací 2DH predpoklad tvrdí, že žiaden efektívny algoritmus nerozlíši medzi dvoma distribúciami $(X_1, X_2, Y, \mathsf{dh}(X_1, Y))$ a (X_1, X_2, Y, Z_1), teda sú výpočtovo nerozlíšiteľné pre uniformne náhodné prvky $X_1, X_2, Y, Z_1 \in \mathbb{G}$. Alebo inak povedané, nie je efektívny pravdepodobnostný algoritmus, ktorý pre danú štvoricu (X_1, X_2, Y, Z_1) dá výstup „1“, keď $\mathsf{dh}(X_1, Y) = Z_1$, inak vráti „0“.

Definícia. *Nech $\mathbb{G}$ je konečná cyklická grupa rádu q s generátorom $g \in \mathbb{G}$, kde q je prvočíslo. Nech X_1, X_2, Y sú uniformne náhodné prvky grupy $\mathbb{G}$. Nech $Z_1 \in \mathbb{G}$ je buď $\mathsf{dh}(X_1, Y)$ alebo uniformne náhodný prvok, každé s polovičnou pravdepodobnosťou. Určenie, či $Z_1 = \mathsf{dh}(X_1, Y)$, alebo či je Z_1 uniformne náhodné, je rozhodovací* 2DH *problém.*

Rozhodovací 2DH predpoklad [4] tvrdí, že je tento problém ťažký. Označuje sa 2DDH. Silný 2DDH predpoklad tvrdí, že je tento problém ťažký, aj keď máme prístup do rozhodovacieho orákula pre predikát $\mathsf{2dhp}(X_1, X_2, ., ., .)$. Tento predikát vracia na vstupe $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$ výstup $\mathsf{2dhp}(X_1, X_2, \widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$.

Zadefinujme si hašované varianty týchto dvoch predpokladov [4].

Definícia. *Nech $\mathbb{G}$ je konečná cyklická grupa rádu q s generátorom $g \in \mathbb{G}$, kde q je prvočíslo. Nech $\mathsf{H} : \mathbb{G} \to \{0,1\}^{\mathcal{K}}$ je hašovacia funkcia. Rozlíšenie dvoch distribúcií $(X_1, X_2, Y, \mathsf{H}(\mathsf{dh}(X_1, Y)))$ a (X_1, X_2, Y, k) pre uniformne náhodné $X_1, X_2, Y \in \mathbb{G}$ a $k \in \{0,1\}^{\mathcal{K}}$ sa nazýva zdvojený hašovaný* DDH *problém.*

Zdvojený hašovaný DDH predpoklad tvrdí, že je tento problém ťažký. Silný zdvojený hašovaný DDH predpoklad tvrdí, že je tento problém ťažký, aj keď máme prístup do orákula pre predikát $\mathsf{2dhp}(X_1, X_2, ., ., .)$. Poznamenajme, že (silný zdvojený) hašovaný DDH predpoklad sa zjednoduší na (silný zdvojený) DDH predpoklad, pokiaľ je H identita.

3. Trapdoor test

Motiváciou k trapdoor testu je nasledujúca veta.

Veta 1. *Obyčajný* DH *predpoklad platí práve vtedy, keď platí silný* 2DH *predpoklad.*

Implikácia z ľava do prava je jednoduchá. Opačná implikácia je už netriviálna. Aby sme ukázali, že obyčajný DH predpoklad implikuje silný 2DH predpoklad, musíme sa najprv zoznámiť so základným nástrojom, ktorý nazveme „trapdoor test“ [4]. Myšlienkou trapdoor testu je, že útočník dokáže s veľkou pravdepodobnosťou odpovedať na otázky rozhodovacieho orákula, pričom nepozná diskrétny logaritmus daných prvkov.

3.1 Trapdoor test

Ako som už spomenula vyššie, trapdoor test je metóda, na základe ktorej dokáže útočník s určitou pravdepodobnosťou „simulovať“ rozhodovacie orákulum. Samozrejme predpokladáme, že útočník je bez znalosti diskrétneho logaritmu prvkov. Cieľom útočníka je zredukovať silný 2DH predpoklad na DH predpoklad.

Popíšme si konštrukciu tejto metódy nasledovne: majme daný uniformne náhodný prvok $X_1 \in \mathbb{G}$, môžeme skonštruovať náhodný prvok $X_2 \in \mathbb{G}$ a tajnú informáciu — trapdoor — a to tak, že:

- X_1 a X_2 budú nezávislé náhodné premenné
- ak máme dané prvky $\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2 \in \mathbb{G}$, ktoré sú vypočítané ako funkcie z X_1 a X_2, tak potom môžeme pomocou trapdoor informácie efektívne ohodnotiť predikát $\mathsf{2dhp}(X_1, X_2, \widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$, pričom sa dopustíme chyby iba so zanedbateľnou pravdepodobnosťou.

Formálne povedané:

Veta 2 (Trapdoor test)**.** *Nech $\mathbb{G}$ je cyklická grupa rádu q, q je prvočíslo. Generátorom tejto grupy je prvok $g \in \mathbb{G}$. Predpokladajme, že X_1, r, s sú navzájom nezávislé uniformne náhodné premenné, kde X_1 má hodnoty v $\mathbb{G}$ a r, s sú uniformne rozdelené na $\mathbb{Z}_q$. Definujme náhodnú premennú $X_2 := g^s / X_1^r$. Ďalej predpokladajme, že $\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2 \in \mathbb{G}$ sú uniformne náhodné premenné, definované ako funkcie z X_1 a X_2. Potom platí:*

(i) X_2 *je uniformne rozdelené na* $\mathbb{G}$*;*

(ii) X_1 *a* X_2 *sú nezávislé;*

(iii) ak $X_1 = g^{x_1}$ *a* $X_2 = g^{x_2}$*, potom pravdepodobnosť, že pravdivostná hodnota*

$$\widehat{Z}_1^r \widehat{Z}_2 = \widehat{Y}^s \tag{3.1}$$

nie je zhodná s pravdivostnou hodnotou

$$\widehat{Z}_1 = \widehat{Y}^{x_1} \wedge \widehat{Z}_2 = \widehat{Y}^{x_2} \tag{3.2}$$

je najviac $1/q$*. Naviac, ak platí* (3.2)*, tak zrejme platí aj* (3.1)*.*

Dôkaz. Pri dokazovaní prvých dvoch bodov je dôležité si uvedomiť, že $s = rx_1 + x_2$. To si ukážeme nasledovne. Nech $X_1 = g^{x_1}$ a $X_2 = g^{x_2}$. Vieme, že $X_2 = g^s/X_1^r$. Z týchto poznatkov to už je jasné. Za X_1 si dosadíme g^{x_1} a za X_2 zase g^{x_2}. Dostávame $g^{x_2} = g^s/g^{rx_1}$. Odtiaľ vidíme, že $x_2 = s - rx_1$, čiže $s = rx_1 + x_2$. $X_2 = g^{x_2}$, teda $X_2 = g^{s-rx_1}$. Vieme, že r, s sú nezávislé a uniformne rozdelené na $\mathbb{Z}_q$. Z toho vyplýva, že aj $s - rx_1$ je uniformne rozdelené na $\mathbb{Z}_q$. Zo znalostí, že g je generátor grupy $\mathbb{G}$, ktorá je prvočíselného rádu q a x_2 je uniformne rozdelené na $\mathbb{Z}_q$ vyplýva, že X_2 je uniformne rozdelené na $\mathbb{G}$. Tým máme dokázaný prvý bod vety. Podobná úvaha platí aj pre dokazovanie druhého bodu. Vieme, že $s = rx_1 + x_2$, r, s sú nezávislé a uniformne rozdelené na $\mathbb{Z}_q$, teda aj rx_1 je uniformne rozdelené na $\mathbb{Z}_q$. Vidíme, že x_1 a x_2 sú nezávislé. Teda X_1 a X_2 sú nezávislé. Bod (iii) je trochu náročnejší. Podmienkou je, aby X_1 a X_2 boli pevné; r je uniformne rozložené na $\mathbb{Z}_q$; $x_1, x_2, \widehat{Y}, \widehat{Z}_1$ a $\widehat{Z}_2$ sú pevne volené.

Ak platia rovnice v (3.2), tak určite platí (3.1). Overme si to nasledovne. Predpokladáme, že platia rovnice $\widehat{Z}_1 = \widehat{Y}^{x_1}$ a $\widehat{Z}_2 = \widehat{Y}^{x_2}$. Najprv si prvú rovnicu umocníme na r a potom ju vynásobíme druhou rovnicou. Postupne nám vyjde, že $\widehat{Z}_1^r = \widehat{Y}^{rx_1}$ a $\widehat{Z}_1^r\widehat{Z}_2 = \widehat{Y}^{rx_1}\widehat{Y}^{x_2}$. Keďže $s = rx_1 + x_2$, tak sme tým dokázali, že $\widehat{Z}_1^r\widehat{Z}_2 = \widehat{Y}^s$, čo sme chceli.

Teraz uvažujme obrátene. Ak neplatia rovnice v (3.2), tak (3.1) platí s pravdepodobnosťou najviac $1/q$. Upravme si (3.1) na lepšiu podobu a to takto: $\widehat{Z}_1^r\widehat{Z}_2 = \widehat{Y}^s$ je ekvivalentné s $\widehat{Z}_1^r\widehat{Z}_2 = \widehat{Y}^{rx_1}\widehat{Y}^{x_2}$ a to je ekvivalentné s

$$(\widehat{Z}_1/\widehat{Y}^{x_1})^r = \widehat{Y}^{x_2}/\widehat{Z}_2. \tag{3.3}$$

Ak $\widehat{Z}_1 = \widehat{Y}^{x_1}$ a $\widehat{Z}_2 \neq \widehat{Y}^{x_2}$, tak je zrejmé, že (3.3) neplatí. Preto sa nám stačí zamerať na prípad, keď $\widehat{Z}_1 \neq \widehat{Y}^{x_1}$. Uvedomme si, že v tomto prípade máme na ľavej strane rovnice (3.3) uniformne náhodný prvok z grupy $\mathbb{G}$, pretože r je uniformne rozložené na $\mathbb{Z}_q$. Na pravej strane je pevný prvok z $\mathbb{G}$. Teda (3.3) platí s pravdepodobnosťou $1/q$. □

3.2 Veta 1

Vráťme sa k našej motivácii. Predtým, než sa pustíme do dokazovania vety, zaveďme si pojem „výhoda útočníka“. Majme útočníka $\mathcal{B}$, označme si jeho DH výhodu ako $\mathsf{AdvDH}_{\mathcal{B},\mathbb{G}}$. Je to pravdepodobnosť, že pri daných uniformne náhodných $X, Y \in \mathbb{G}$ dokáže $\mathcal{B}$ vypočítať $\mathsf{dh}(X, Y)$. Ďalej majme útočníka $\mathcal{A}$, ktorého silnú 2DH výhodu si označme $\mathsf{Adv2DH}_{\mathcal{A},\mathbb{G}}$. Je to pravdepodobnosť, že pri daných uniformne náhodných $X_1, X_2, Y \in \mathbb{G}$ dokáže $\mathcal{A}$ vypočítať $\mathsf{2dh}(X_1, X_2, Y)$. Útočník $\mathcal{A}$ má prístup do rozhodovacieho orákula pre predikát $\mathsf{2dhp}(X_1, X_2, ., ., .)$. Orákulum vracia pre vstup $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$ výstup $\mathsf{2dhp}(X_1, X_2, \widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$. Zovšeobecnime si Vetu 1 nasledovne:

Veta 3. *Predpokladajme útočníka $\mathcal{A}$. Nech $\mathcal{A}$ je silný* 2DH *útočník, ktorý má k dispozícii dešifrovacie orákulum, na ktoré kladie najviac Q_d otázok a beží v čase najviac τ. Potom existuje* DH *útočník $\mathcal{B}$, ktorý beží v čase τ plus $O(Q_d \log q)$. Ďalej pre útočníka $\mathcal{B}$ platí, že $\mathsf{Adv2DH}_{\mathcal{A},\mathbb{G}} \leq \mathsf{AdvDH}_{\mathcal{B},\mathbb{G}} + \frac{Q_d}{q}$. Ak $\mathcal{B}$ pobeží dokonca a dá výstup (teda nedôjde ku „zlyhaniu“), tak je výstup správny s pravdepodobnosťou aspoň $1 - \frac{1}{q}$.*

Dôkaz. Predpokladáme, že máme k dispozícii útočníka $\mathcal{A}$. Chceme dokázať existenciu útočníka $\mathcal{B}$ s vlastnosťami popísanými vyššie. Skonštruujme útočníka $\mathcal{B}$ nasledovne:

1. $\mathcal{B}$ dostane na vstupe dvojicu (X, Y). Jeho cieľom je výstup $Z = \mathsf{dh}(X, Y)$.
2. $\mathcal{B}$ si uniformne náhodne zvolí $r, s \in \mathbb{Z}_q$. Vypočíta $X_1 := X$ a $X_2 := g^s / X_1^r$ a pošle útočníkovi $\mathcal{A}$ trojicu (X_1, X_2, Y).
3. $\mathcal{A}$ dostal od $\mathcal{B}$ vstup (X_1, X_2, Y). Začne klásť najviac Q_d otázok $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$.
4. $\mathcal{B}$ sa snaží na základe trapdoor testu simulovať dešifrovacie orákulum. Každú otázku $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$, ktorú kladie $\mathcal{A}$, $\mathcal{B}$ spracuje tak, že overí, či platí $\widehat{Z}_1^r \widehat{Z}_2 = \widehat{Y}^s$. Na základe toho odpovie útočníkovi $\mathcal{A}$.
5. $\mathcal{A}$ po najviac Q_d otázok vráti výstup (Z_1, Z_2).
6. $\mathcal{B}$ testuje trojicu (Y, Z_1, Z_2) tak, že skontroluje, či platí $Z_1^r Z_2 = Y^s$. Pokiaľ nie, $\mathcal{B}$ vráti „zlyhanie“, v opačnom prípade vráti $Z := Z_1$.

Na základe prebehnutej komunikácie medzi útočníkmi $\mathcal{A}$ a $\mathcal{B}$ vidíme, že pokiaľ $\mathcal{A}$ beží v čase τ, tak potom časová zložitosť $\mathcal{B}$ je τ, pretože čaká na $\mathcal{A}$, plus $O(Q_d \log q)$ grupových operácií (časová zložitosť umocňovania pri Q_d otázkach). Ďalej vidíme, že výhoda $\mathcal{B}$ je ako výhoda $\mathcal{A}$, ale ešte musíme odčítať pravdepodobnosť, že sa $\mathcal{B}$ pri trapdoor teste pomýli. Pravdepodobnosť, že sa $\mathcal{B}$ v odpovedaní aspoň raz pomýli je $1 - (1 - \frac{1}{q})^{Q_d}$ (podľa vety o Trapdoor teste). Túto pravdepodobnosť môžeme zhora odhadnúť na $\frac{Q_d}{q}$. Teda máme, že

$$\mathsf{AdvDH}_{\mathcal{B},\mathbb{G}} \geq \mathsf{Adv2DH}_{\mathcal{A},\mathbb{G}} - \frac{Q_d}{q}.$$

Pokiaľ $\mathcal{B}$ nevráti „zlyhanie“, tak odpoveď bude správna s pravdepodobnosťou aspoň $1 - \frac{1}{q}$ (pravdepodobnosť, že sa pomýli pri poslednom overovaní je najviac $1/q$). □

Veta 3 je silnejším tvrdením Vety 1. Vzťah (hašovaného) DDH predpokladu a silného zdvojeného (hašovaného) DDH predpokladu vyjadruje nasledujúca veta.

Veta 4. *(Hašovaný)* DDH *predpoklad platí práve vtedy, keď platí silný zdvojený (hašovaný)* DDH *predpoklad. Konkrétne, predpokladajme útočníka $\mathcal{A}$. Nech $\mathcal{A}$ je silný zdvojený (hašovaný)* DDH *útočník, ktorý má k dispozícii dešifrovacie orákulum, na ktoré kladie najviac Q_d otázok a beží v čase najviac τ. Potom existuje (hašovaný)* DDH *útočník $\mathcal{B}$, ktorý beží v čase najviac τ plus $O(Q_d \log q)$. Ďalej pre útočníka $\mathcal{B}$ platí, že $\mathsf{Adv2DDH}_{\mathcal{A},\mathbb{G}} \leq \mathsf{AdvDDH}_{\mathcal{B},\mathbb{G}} + \frac{Q_d}{q}$.*

Táto veta je analogická k Vete 3. Dokazovať si ju nebudeme.

4. Zdvojené ElGamalovo šifrovanie

Zdvojené ElGamalovo šifrovanie je nová asymetrická šifrovacia schéma, ktorá je jednou z našich hlavných aplikácií 2DH problému. Pri hašovanom ElGamalovom šifrovaní sme si spomenuli, že je bezpečné proti útoku typu CCA v modele náhodného orákula, pokiaľ je symetrická šifra proti tomuto typu útoku bezpečná a za predpokladu, že platí silný DH predpoklad. Vďaka zdvojeniu ElGamalovho šifrovania vieme dokázať, že takto zdvojený šifrovací systém je bezpečný proti útoku typu CCA v modele náhodného orákula už za predpokladu platnosti obyčajného DH problému. Uvedomme si, že podľa Vety 1 máme ekvivalenciu medzi obyčajným DH problémom a silným 2DH problémom.

4.1 Definícia

Majme funkciu H a symetrickú šifru (E, D). Jedná sa o asymetrickú šifrovaciu schému, ktorá má verejný a súkromný pár kľúčov, ktoré sú vygenerované pomocou algoritmu K. Verejným kľúčom pre túto schému je pár (X_1, X_2), kde X_1 a X_2 sú uniformne náhodné prvky z grupy $\mathbb{G}$. K nim máme príslušný pár súkromných kľúčov (x_1, x_2), kde $X_i = g^{x_i}$ pre $i = 1, 2$.

Šifrovanie:
Šifrovací algoritmus asymetrickej šifry dostane na vstupe verejný pár kľúčov (X_1, X_2) a správu m, ktorú chceme zašifrovať. Uniformne náhodne si vyberieme $y \in \mathbb{Z}_q$ a vypočítame

$$Y := g^y,\ Z_1 := X_1^y,\ Z_2 := X_2^y,\ k := H(Y, Z_1, Z_2),\ c := \mathsf{E}(k, m).$$

Zašifrovaním správy m dostávame zašifrovaný text (Y, c).

Dešifrovanie:
Dešifrovací algoritmus asymetrickej šifry dostane na vstupe súkromný pár kľúčov (x_1, x_2) a zašifrovanú správu (Y, c). Dešifrovanie prebieha jednoducho. Vypočítame

$$Z_1 := Y^{x_1},\ Z_2 := Y^{x_2},\ k := H(Y, Z_1, Z_2),\ m := \mathsf{D}(k, c).$$

4.2 Bezpečnosť

Pripomeňme si, že CCA výhoda útočníka $\mathcal{A}$ nad asymetrickým šifrovaním sa označuje $\mathsf{AdvCCA}_{\mathcal{A},\mathsf{PKE}}$. Pokiaľ hašovaciu funkciu konštruujeme ako náhodné orákulum, tak výhodu útočníka v CCA hre budeme označovať $\mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{PKE}}$. V tom prípade majú v CCA hre vyzývateľ a aj útočník prístup do náhodného orákula. Analogicky to platí aj pre symetrickú kryptografiu a neinteraktívnu schému na výmenu kľúča z prvej kapitoly. CCA výhodu útočníka $\mathcal{A}$ nad symetrickým šifrovaním v modele náhodného orákula označme $\mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{SE}}$. AA výhodu útočníka $\mathcal{A}$ nad neinteraktívnou schémou na výmenu kľúča v modele náhodného orákula označme $\mathsf{AdvAA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{KE}}$.

Veta 5. *Nech platí:*

- *hašovacia funkcia* H *je modelované ako náhodné orákulum,*
- SE *je bezpečná proti* CCA *útoku,*
- *v grupe* $\mathbb{G}$ *platí* DH *predpoklad.*

Potom je $\mathsf{PKE}_{\mathsf{2dh}}$ *bezpečná proti útoku typu* CCA. *Nech* $\mathcal{A}$ *je útočník, ktorý realizuje útok* CCA *na* $\mathsf{PKE}_{\mathsf{2dh}}$ *v modele náhodného orákula.* $\mathcal{A}$ *beží v čase* τ *a spraví najviac* Q_h *hašovacích otázok a* Q_d *dešifrovacích otázok. Potom existuje útočník* $\mathcal{B}_{\mathsf{dh}}$ *proti* DH *problému a útočník* $\mathcal{B}_{\mathsf{sym}}$, *ktorý realizuje* CCA *útok na schému* SE. $\mathcal{B}_{\mathsf{dh}}$ *a* $\mathcal{B}_{\mathsf{sym}}$ *bežia v čase najviac* τ *plus čas na* $O((Q_h + Q_d)\log q)$ *grupových operácií. Platí, že*

$$\mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{PKE}_{\mathsf{2dh}}} \leq \mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \mathsf{AdvCCA}_{\mathcal{B}_{\mathsf{sym}},\mathsf{SE}} + \frac{Q_h}{q}.$$

Dôkaz. Postupujme pomocou postupností hier.

Hra 0 . Tento experiment nám bude predstavovať originálnu CCA hru pre PKE schému, ako je popísaná v sekcii o asymetrickom šifrovaní. Nech S_0 je udalosť, že sa v tejto hre $\widehat{b} = b$.

1. Komunikácia začne tým, že vyzývateľ vygeneruje tajný kľúč (x_1, x_2) a vypočíta korešpondujúci verejný kľúč (X_1, X_2), kde $X_i = g^{x_i}$, pre $i = 1, 2$. Verejný kľúč pošle útočníkovi. Zároveň si vyzývateľ implementuje náhodné orákulum a to použitím asociatívneho zoznamu, ktorý si označíme L. Tento zoznam bude indexovaný prvkami z $\mathbb{G}^3$. Inicializuje sa hodnotou $\perp$, ktorá nám bude označovať, že je zoznam nedefinovaný. Zoznam sa bude definovať postupne a to nasledovne:
   - kedykoľvek sa útočník spýta náhodného orákula na $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$, vyzývateľ odpovie buď $\mathsf{L}[\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2] = \widehat{k}$, pokiaľ je už táto trojica definovaná v zozname L, alebo odpovie uniformne náhodným symetrickým kľúčom $\widehat{k}$
   - pokiaľ odpovie uniformne náhodným symetrickým kľúčom $\widehat{k}$, do L pridá $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$ a k trojici priradí tento kľúč;
     poznamenajme, že $\mathsf{L}[\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2] = \widehat{k}$ intuitívne reprezentuje, že $H(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2) = \widehat{k}$
2. Začína fáza, v ktorej útočník kladie dešifrovacie otázky vyzývateľovi. Predpokladáme, že zašifrovaný text je tvaru $(\widehat{Y}, \widehat{c})$. Vyzývateľ ho dešifruje pomocou tajného kľúča (x_1, x_2). Teda vypočíta $\widehat{Z}_1 = \widehat{Y}^{x_1}$ a $\widehat{Z}_2 = \widehat{Y}^{x_2}$. Spýta sa na $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$ náhodného orákula. Orákulum mu odpovie buď $\mathsf{L}[\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2] = \widehat{k}$ alebo uniformne náhodné $\widehat{k}$ (ako je už popísané vyššie). Kľúč použije k dešifrovaniu správy a útočníkovi pošle $\mathsf{D}(\widehat{k}, \widehat{c})$.
3. Keď sa útočník rozhodne, že fáza hľadania skončila, pošle vyzývateľovi dve správy: m_0, m_1. Vyzývateľ si zvolí uniformne náhodné $y \in \mathbb{Z}_q$ a vypočíta $Y := g^y, Z_1 := X_1^y, Z_2 := X_2^y$. Spýta sa náhodného orákula na (Y, Z_1, Z_2), orákulum mu odpovie k. Ďalej si zvolí $b \in \{0, 1\}$ a vypočíta $c := \mathsf{E}(k, m_b)$. Útočníkovi pošle zašifrovaný text (Y, c).

4. V druhej fáze dešifrovacích otázok útočníka postupuje vyzývateľ rovnako, ako v druhom kroku.
5. Útočník odpovie $\widehat{b} \in \{0,1\}$. Tým je prvá hra ukončená. Vidíme, že

$$\mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{PKE}_{\mathsf{2dh}}} = |Pr[S_0] - \frac{1}{2}|. \tag{4.1}$$

Hra 1 Táto hra je rovnaká ako prvá až na jedno obmedzenie. Útočník sa ani v jednej fáze nesmie náhodného orákula spýtať na (Y, Z_1, Z_2). Pokiaľ sa tak stane, vyzývateľ komunikáciu ukončí. Túto udalosť označme F. Nech S_1 je udalosť, že sa v tomto experimente $\widehat{b} = b$. Vidíme, že tieto dva experimenty sú identické, pokiaľ nenastane udalosť F. Odtiaľ máme, že

$$|Pr[S_1] - Pr[S_0]| \leq Pr[F]. \tag{4.2}$$

Teraz chceme odhadnúť pravdepodobnosť udalosti F. Tvrdíme, že

$$|Pr[F]| \leq \mathsf{Adv2DH}_{\mathcal{B}_{\mathsf{2dh}},\mathbb{G}}, \tag{4.3}$$

kde $\mathcal{B}_{\mathsf{2dh}}$ je efektívny silný $\mathsf{2dh}$ útočník, ktorý spraví najviac Q_h rozhodovacích otázok na orákulum. $\mathcal{B}_{\mathsf{2dh}}$ hrá rolu vyzývateľa. Popíšeme ho a ukážeme, že tým získame výhodu, akú tvrdíme.

1. $\mathcal{B}_{\mathsf{2dh}}$ má na vstupe (X_1, X_2, Y). $\mathcal{B}_{\mathsf{2dh}}$ dá útočníkovi verejný kľúč. Poznamenajme, že jediným rozdielom medzi $\mathcal{B}_{\mathsf{2dh}}$ a vyzývateľom v druhej hre je, že $\mathcal{B}_{\mathsf{2dh}}$ nepozná súkromný kľúč. No aj napriek tomu bude vedieť odpovedať na dešifrovacie otázky útočníka. To si ukážeme za chvíľku. Pokiaľ sa útočník spýta $(\widehat{Y}, \widehat{Z}_1, \widehat{Z}_2)$ náhodného orákula, dochádza k rovnakému spracovaniu, ako pri druhej hre a ešte navyše $\mathcal{B}_{\mathsf{2dh}}$ pošle túto trojicu do jeho vlastného rozhodovacieho orákula. Označí si ju „dobrá“ alebo „zlá“ podľa toho, či $\mathsf{dh}(X_i, \widehat{Y}) = \widehat{Z}_i$ pre $i = 1, 2$.

2. $\mathcal{B}_{\mathsf{2dh}}$ spracováva dešifrovacie otázky bez znalosti súkromného kľúča: je daný zašifrovaný text $(\widehat{Y}, \widehat{c})$ a skontroluje, či už videl dobrú trojicu $(\widehat{Y}, ., .)$ v L. Ak áno, použije kľúč asociovaný s touto trojicou, ak nie, generuje uniformne náhodný kľúč a bude kontrolovať, či v budúcich otázkach neuvidí dobrú trojicu $(\widehat{Y}, ., .)$. Pokiaľ ju v budúcich otázkach uvidí, asociuje tento kľúč s tou trojicou, aby zachoval konzistenciu.

3. Útočník dáva po prvej fáze výstup (m_0, m_1). $\mathcal{B}_{\mathsf{2dh}}$ pozrie, či je tam dobrá trojica tvaru $(Y, ., .)$. Ak áno, skončí, ak nie, tak generuje uniformne náhodný kľúč k (bude dávať pozor, či sa v budúcich otázkach neobjaví dobrá trojica $(Y, ., .)$, asociuje tento kľúč s tou trojicou, aby sa zachovala konzistentnosť). Vypočíta $c := \mathsf{E}(k, m_b)$ a vráti zašifrovaný text (Y, c) útočníkovi.

4. Dešifrovacie otázky sú spracované ako v druhom kroku. Ak sa útočník pýta na dobrú trojicu $(Y, ., .)$, tak $\mathcal{B}_{\mathsf{2dh}}$ skončí.

5. Útočník odpovie $\widehat{b} \in \{0,1\}$.

Na konci hry sa $\mathcal{B}_{\mathsf{2dh}}$ pozrie, či videl dobrú trojicu $(Y, ., .)$. Ak áno, vráti posledné dva komponenty. Teda vidíme, že výhoda takéhoto útočníka zavisí od toho, či nastala udalosť F. Platí, že $|Pr[F]| \leq \mathsf{Adv2DH}_{\mathcal{B}_{\mathsf{2dh}},\mathbb{G}}$. Podľa Vety 3 máme, že

$$\mathsf{Adv2DH}_{\mathcal{B}_{\mathsf{2dh}},\mathbb{G}} \leq \mathsf{AdvDH}_{\mathcal{B}_{dh},\mathbb{G}} + \frac{Q_h}{q}. \tag{4.4}$$

Ešte si potrebujeme uvedomiť, že útočník v druhej hre vlastne hrá CCA hru proti SE. Súkromným kľúčom SE je v skutočnosti $k = \mathsf{L}[Y, Z_1, Z_2]$. Vyzývateľ odmieta čokoľvek prezradiť o tejto hodnote. Teda je zbytočné riešiť, či sa dá od Y dostať ku Z_1 a Z_2, pokiaľ je prechod ku k náhodný. Teda je tam efektívny útočník $\mathcal{B}_{\mathsf{sym}}$ taký, že

$$|Pr[S_1] - \frac{1}{2}| = \mathsf{AdvCCA}_{\mathcal{B}_{\mathsf{sym}},\mathsf{SE}} \tag{4.5}$$

Spojením vzťahov (4.2), (4.3) a (4.4) dostávame, že:

$$|Pr[S_1] - Pr[S_0]| \leq |Pr[F]| \leq \mathsf{Adv2DH}_{\mathcal{B}_{\mathsf{2dh}},\mathbb{G}} \leq \mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \frac{Q_h}{q}.$$

Teraz si upravme ľavú stranu predchádzajúcej nerovnosti a použime (4.1) a (4.5):

$$\begin{aligned}
&|Pr[S_1] - Pr[S_0]| = |Pr[S_0] - Pr[S_1]| = |Pr[S_0] - \frac{1}{2} + \frac{1}{2} - Pr[S_1]| = \\
&= |(Pr[S_0] - \frac{1}{2}) - (Pr[S_1] - \frac{1}{2})| \geq |Pr[S_0] - \frac{1}{2}| - |Pr[S_1] - \frac{1}{2}| = \\
&= \mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{PKE}_{\mathsf{2dh}}} - \mathsf{AdvCCA}_{\mathcal{B}_{\mathsf{sym}},\mathsf{SE}}.
\end{aligned}$$

Spojením posledných dvoch nerovností dostávame:

$$\mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{PKE}_{\mathsf{2dh}}} - \mathsf{AdvCCA}_{\mathcal{B}_{\mathsf{sym}},\mathsf{SE}} \leq \mathsf{AdvDH}_{\mathcal{B}_{dh},\mathbb{G}} + \frac{Q_h}{q}.$$

Teda

$$\mathsf{AdvCCA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{PKE}_{\mathsf{2dh}}} \leq \mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \mathsf{AdvCCA}_{\mathcal{B}_{\mathsf{sym}},\mathsf{SE}} + \frac{Q_h}{q}.$$

Pokiaľ $\mathcal{A}$ beží v čase najviac τ a spraví Q_h hašovacích otázok a Q_d dešifrovacích otázok, tak potom útočníci $\mathcal{B}_{\mathsf{dh}}$ a $\mathcal{B}_{\mathsf{sym}}$ bežia v čase ako $\mathcal{A}$, teda najviac τ a plus k nim treba pripočítať čas na spracovanie všetkých hašovacích a dešifrovacích otázok. Teda časová zložitosť týchto útočníkov je najviac τ plus čas na $O((Q_h + Q_d) \log q)$ grupových operácií. □

5. Zdvojený Diffie-Hellmanov protokol

Diffie-Hellmanov protokol predstavuje neinteraktívny protokol na výmenu kľúča. Komunikácia prebieha medzi dvoma užívateľmi, nazvime si ich Alica a Bob. Alica si vyberie uniformne náhodný prvok $x \in \mathbb{Z}_q$, vypočíta $X := g^x \in \mathbb{G}$. Zverejní pár (Alica, X) vo verejnom adresári. Analogicky si vyberie Bob uniformne náhodný prvok $y \in \mathbb{Z}_q$, vypočíta $Y := g^y \in \mathbb{G}$ a zverejní pár $(\mathsf{Bob},\ Y)$ vo verejnom adresári. Teraz sú Alica a Bob schopní vypočítať zdieľanú hodnotu $Z := g^{xy} \in \mathbb{G}$. Alica obnoví údaj z Bobového adresára a vypočíta $Z = Y^x$, zatiaľ čo Bob obnoví Alicin kľúč X a vypočíta $Z = X^y$. Spoločný kľúč na symetrickú šifru je $k := \mathsf{H}(\mathsf{Alica}, \mathsf{Bob}, Z)$. Bezpečnosť proti útoku typu CCA zostáva rovnaká, ako pri hašovanej ElGamalovej schéme, pokiaľ útočníkovi dovolíme ľubovolné vkladanie kľúča do verejných adresárov bez vyžadovania dôkazu, že má súkromný kľúč. Práve tomuto problému sa pri zdvojenom DH protokole vyhneme.

5.1 Definícia

V $\mathsf{2DH}$ protokole si Alica nevyberá len jeden prvok, ale dva uniformne náhodné prvky: $x_1, x_2 \in \mathbb{Z}_q$. Pre obe hodnoty, teda pre $i = 1, 2$, vypočíta $X_i := g^{x_i} \in \mathbb{G}$. Pár (X_1, X_2) tvorí verejný kľúč a (x_1, x_2) tvorí súkromný kľúč. Podobne postupuje aj Bob. Vyberie si dva uniformne náhodné prvky $y_1, y_2 \in \mathbb{Z}_q$. Pár (y_1, y_2) tvorí jeho súkromný kľúč. Pre $i = 1, 2$ vypočíta $Y_i := g^{y_i} \in \mathbb{G}$ a pár (Y_1, Y_2) tvorí príslušný verejný kľúč. Ich spoločný zdieľaný kľúč je

$$k := \mathsf{H}(\mathsf{Alica}, \mathsf{Bob}, \mathsf{dh}(X_1, Y_1), \mathsf{dh}(X_1, Y_2), \mathsf{dh}(X_2, Y_1), \mathsf{dh}(X_2, Y_2)),$$

kde H označuje hašovaciu funkciu. Alica vypočíta štvoricu prvkov v hašovacej funkcii ako $(Y_1^{x_1}, Y_2^{x_1}, Y_1^{x_2}, Y_2^{x_2})$. Bob ich zase vypočíta pomocou svojho páru súkromných kľúčov $(X_1^{y_1}, X_1^{y_2}, X_2^{y_1}, X_2^{y_2})$.

5.2 Bezpečnosť

Veta 6. *Nech je* H *modelované ako náhodné orákulum a nech platí* DH *predpoklad. Potom je* $\mathsf{KE}_{\mathsf{2dh}}$ *bezpečné proti útoku typu* AA. *Konkrétne,* $\mathcal{A}$ *je útočník, ktorý v modele náhodného orákula útočí na* $\mathsf{KE}_{\mathsf{2dh}}$. *Nech* $\mathcal{A}$ *beží v čase najviac* τ *a nech kladie najviac* Q *otázok všetkých typov na orákulum. Potom existuje* DH *útočník, označme ho* $\mathcal{B}_{\mathsf{dh}}$, *ktorý beží v čase najviac* τ *plus čas na* $O(Q \log q)$ *grupových operácií. Platí, že*

$$\mathsf{AdvAA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{KE}_{\mathsf{2dh}}} \leq 2\mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \frac{2Q}{q}.$$

Dôkaz. Budeme postupovať pomocou postupností hier.

Hra 0. Nech je táto hra originálny experiment útoku typu AA.

1. Vyzývateľ si ako vstup vezme bit b. Ním sa bude riadiť pri registrácii identít. Vytvorí si dva asociatívne zoznamy, L a K. Oba sú na začiatku prázdne, čo vyjadruje znak $\perp$. Postupne ich bude plniť tak, ako popíšem v druhom kroku.
2. Nasledujú otázky útočníka $\mathcal{A}$, na ktoré vyzývateľ odpovedá. Vyzývateľ si do L ukladá všetky útočníkove otázky na orákulum. Keď sa útočník spýta na spárovaný kľúč pre identity (id, id'), tak najprv si vyzývateľ dopočíta všetky časti do vstupu pre náhodné orákulum. To spraví pomocou súkromného kľúča dôveryhodnej identity. Nech je id dôveryhodná identita. Nech jej verejný kľúč je (X_1, X_2) a súkromný (x_1, x_2). Nech verejný kľúč identity id' je (Y_1, Y_2). Vyzývateľ si vypočíta

$$\mathsf{dh}(X_1, Y_1) = Y_1^{x_1},\ \mathsf{dh}(X_1, Y_2) = Y_2^{x_1},$$
$$\mathsf{dh}(X_2, Y_1) = Y_1^{x_2},\ \mathsf{dh}(X_2, Y_2) = Y_2^{x_2}.$$

   Napríklad, nech je tým vstupom $(id, id', Z_1, Z_2, Z_3, Z_4)$. Ak $b = 0$, tak vyzývateľ postupuje nasledovne. Ak L pre tento vstup je $k \neq \perp$, tak si uloží $\mathsf{K}[id, id'] := k$ a k vráti útočníkovi. Pokiaľ bolo L pre tento vstup prázdne, ešte nebolo nainicializované, tak si vyzývateľ vygeneruje uniformne náhodný kľúč k, uloží ho do $\mathsf{K}[id, id']$ a $\mathsf{L}[id, id', Z_1, Z_2, Z_3, Z_4]$ a odošle útočníkovi. Ak $b = 1$, tak vráti $\mathsf{K}[id, id']$, pokiaľ je nainicializované, pokiaľ nie je, nainicializuje uniformne náhodným kľúčom.
3. Útočník odpovie bit $\widehat{b}$. Nech S_0 je udalosť, že $\widehat{b} = b$.

$$\mathsf{AdvAA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{KE}_{\mathsf{2dh}}} = |Pr[S_0] - \frac{1}{2}|. \tag{5.1}$$

Hra 1. Táto hra je rovnaká, ako hra 0, až na to, že keď sa útočník spýta na spárovaný kľúč dôveryhodných identít (id, id'), tak vyzývateľ pri spracovávaní otázky ukladá kľúč len do K a nie aj do L. To má za dôsledok to, že pokiaľ sa útočník spýta náhodného orákula na korešpondujúci vstup s týmito identitami, tak sa vyzývateľ pozrie do L, zistí, že je prázdne a vygeneruje nový kľúč. Teda nepoužije ten, čo má uložený v K. Nech S_1 je udalosť, že $\widehat{b} = b$ v hre 1. Nech F je udalosť, že sa útočník spýta náhodného orákula práve na ten korešpondujúci vstup s tými identitami. Teda sa spýta na $(id, id', \widehat{Z}_1, \widehat{Z}_2, \widehat{Z}_3, \widehat{Z}_4)$, pričom je to korektný vstup pre tie identity. Je jasné, že

$$|Pr[S_1] - Pr[S_0]| \leq Pr[F]. \tag{5.2}$$

Vyzývateľ postupuje, akoby $b = 1$. Hodnota bitu b nemá vplyv na správanie sa vyzývateľa, teda

$$Pr[S_1] = \frac{1}{2}. \tag{5.3}$$

Tvrdíme, že $Pr[F]$ vieme odhadnúť nasledovne:

$$Pr[F] \leq 2\mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \frac{2Q}{q}. \tag{5.4}$$

$\mathcal{B}_{\mathsf{dh}}$ je efektívny DH útočník, ktorý v podstate simuluje vyzývateľa z hry 1.

1. $\mathcal{B}_{\mathsf{dh}}$ má na vstupe (X, Y). Vracia výstup $Z = \mathsf{dh}(X, Y)$. Vytvorí si dva asociatívne zoznamy, L a K. Oba sú na začiatku prázdne, čo vyjadruje znak $\perp$. Postupne ich bude plniť tak, ako popíšem v druhom kroku.

2. Nasledujú otázky útočníka $\mathcal{A}$, na ktoré vyzývateľ odpovedá. Keď sa zaregistruje dôveryhodná identita id, $\mathcal{B}_{\mathsf{dh}}$ vygeneruje uniformne náhodný bit b_{id} a uniformne náhodné $r_{id}, s_{id}, t_{id} \in \mathbb{Z}_q$. Ak sa $b_{id} = 0$, tak $\mathcal{B}_{\mathsf{dh}}$ vypočíta

$$X_1 := X g^{t_{id}},\ X_2 := g^{s_{id}} / X_1^{r_{id}}.$$

   Ak sa $b_{id} = 1$, tak $\mathcal{B}_{\mathsf{dh}}$ vypočíta

$$X_1 := Y g^{t_{id}},\ X_2 := g^{s_{id}} / X_1^{r_{id}}$$

   $\mathcal{B}_{\mathsf{dh}}$ vráti útočníkovi pár (X_1, X_2) ako verejný kľúč pre identitu id a uloží si bit b_{id}, trapdoor informáciu r_{id}, s_{id} a t_{id}. Keď sa zaregistruje nedôveryhodná identita id, $\mathcal{B}_{\mathsf{dh}}$ si ju len uloží spolu s jej verejným kľúčom.

   Keď sa útočník spýta na spárovaný kľúč pre identity id, id', tak sa $\mathcal{B}_{\mathsf{dh}}$ pozrie na $\mathsf{K}[id, id']$. Pokiaľ $\mathsf{K}[id, id'] = k \neq \perp$, tak $\mathcal{B}_{\mathsf{dh}}$ vráti útočníkovi k, pokiaľ $\mathsf{K}[id, id'] = \perp$, vygeneruje si uniformne náhodné k a ním inicializuje tento zoznam.

   Keď sa útočník spýta na orákulovú otázku $(id, id', \widehat{Z}_1, \widehat{Z}_2, \widehat{Z}_3, \widehat{Z}_4)$, tak $\mathcal{B}_{\mathsf{dh}}$ vráti $\mathsf{L}[id, id', Z_1, Z_2, Z_3, Z_4]$, ak je už táto hodnota nainicializovaná. Ak ešte nie je, tak $\mathcal{B}_{\mathsf{dh}}$ zistí, či je tento vstup správnym pre dané identity a pokiaľ je, tak túto položku v zozname L nainicializuje uniformne náhodným kľúčom. Ak sú identity v zlom poradí — inom, než predtým — tak v L bude iná hodnota, než je ich spárovaný kľúč, ktorý sa im už predtým pridelil. Správnosť tejto šestice bude overovať nasledovne. Budeme uvažovať dva prípady. Prvý je, keď je id dôveryhodná identita. Druhý prípad je, keď id' je dôveryhodná identita. Nech verejný kľúč pre id je (X_1, X_2) a pre id' je (Y_1, Y_2). Najprv uvažujme prvý prípad. id je dôveryhodná identita, teda si k nej $\mathcal{B}_{\mathsf{dh}}$ priradil nejakú trapdoor informáciu r_{id}, s_{id}. $\mathcal{B}_{\mathsf{dh}}$ ohodnotí predikáty

$$\mathsf{2dhp}(X_1, X_2, Y_1, \widehat{Z}_1, \widehat{Z}_3) \text{ a } \mathsf{2dhp}(X_1, X_2, Y_2, \widehat{Z}_2, \widehat{Z}_4)$$

   pomocou Vety 2. Teda oba predikáty sú ohodnotené na 1, ak $\widehat{Z}_1^{r_{id}} \widehat{Z}_3 = Y_1^{s_{id}}$ a $\widehat{Z}_2^{r_{id}} \widehat{Z}_4 = Y_2^{s_{id}}$, teda šestica je ohodnotená ako správna.

   Druhý prípad je analogický. id' je dôveryhodná identita, teda si k nej $\mathcal{B}_{\mathsf{dh}}$ priradil nejakú trapdoor informáciu $r_{id'}, s_{id'}$. $\mathcal{B}_{\mathsf{dh}}$ ohodnotí predikáty

$$\mathsf{2dhp}(Y_1, Y_2, X_1, \widehat{Z}_1, \widehat{Z}_2) \text{ a } \mathsf{2dhp}(Y_1, Y_2, X_2, \widehat{Z}_3, \widehat{Z}_4)$$

   pomocou Vety 2. Teda oba predikáty sú ohodnotené na 1, ak $\widehat{Z}_1^{r_{id'}} \widehat{Z}_2 = X_1^{s_{id'}}$ a $\widehat{Z}_3^{r_{id'}} \widehat{Z}_4 = X_2^{s_{id'}}$, teda šestica je ohodnotená ako správna.

3. Keď útočník skončí, $\mathcal{B}_{\mathsf{dh}}$ sa pozrie, či nie je v L dobrá šestica s dôveryhodnými identitami id, id' taká, že $b_{id} \neq b_{id'}$. Ak takú šesticu nájde, tak sa pozrie na verejné kľúče identít. Nech sú také, ako predtým, teda verejný kľúč id

je (X_1, X_2) a verejný kľúč id' je (Y_1, Y_2). Rozoberieme si dva prípady. Prvý prípad je, keď $b_{id} = 0, b_{id'} = 1$. $\mathcal{B}_{\mathsf{dh}}$ vypočíta výstup nasledovne.

$$Z_1 = g^{x_1 y_1} = g^{(x+t_{id})(y+t_{id'})} = g^{xy+xt_{id'}+yt_{id}+t_{id}t_{id'}}$$

Odtiaľ vidíme, že $Z_1 = ZX^{t_{id'}}Y^{t_{id}}g^{t_{id}t_{id'}}$. Teda $\mathcal{B}_{\mathsf{dh}}$ vypočíta výstup ako

$$Z := Z_1/(X^{t_{id'}}Y^{t_{id}}g^{t_{id}t_{id'}}).$$

Podobne postupujeme aj pri druhom prípade, keď $b_{id} = 1, b_{id'} = 0$. $\mathcal{B}_{\mathsf{dh}}$ vypočíta výstup nasledovne.

$$Z_1 = g^{x_1 y_1} = g^{(y+t_{id})(x+t_{id'})} = g^{xy+xt_{id}+yt_{id'}+t_{id}t_{id'}}$$

Odtiaľ vidíme, že $Z_1 = ZX^{t_{id}}Y^{t_{id'}}g^{t_{id}t_{id'}}$. Teda $\mathcal{B}_{\mathsf{dh}}$ vypočíta výstup ako

$$Z := Z_1/(X^{t_{id}}Y^{t_{id'}}g^{t_{id}t_{id'}}).$$

Uvedomme si, že verejné kľúče, ktoré sa dávajú útočníkovi sú uniformné a nezávislé (podľa Vety 2). $\mathcal{B}_{\mathsf{dh}}$ sa pri určovaní správnosti predikátov môže pomýliť s pravdepodobnosťou najviac $\frac{2Q}{q}$ (na každú otázku sa vyhodnocujú dva predikáty). Bity $b_{id}, b_{id'}$ sú z pohľadu útočníka nezávislé. Keď sa útočník spýta na dobrú šesticu, tak $\mathcal{B}_{\mathsf{dh}}$ vypočíta správne Z s pravdepodobnosťou $\frac{1}{2}$. Pravdepodobnosť, že $\mathcal{B}_{\mathsf{dh}}$ vypočíta správne Z je

$$\mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} \geq \frac{1}{2}(Pr[F] - \frac{2Q}{q}).$$

Z toho už vyplýva (5.4). Zo vzťahov (5.2), (5.4) dostávame

$$|Pr[S_1] - Pr[S_0]| \leq Pr[F] \leq 2\mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \frac{2Q}{q}$$

Upravme si nerovnicu (5.2) a skombinujme s (5.1), (5.3) nasledovne

$$|Pr[S_1] - Pr[S_0]| = |Pr[S_0] - \frac{1}{2} + \frac{1}{2} - Pr[S_1]| \geq |Pr[S_0] - \frac{1}{2}| - |Pr[S_1] - \frac{1}{2}| =$$
$$\mathsf{AdvAA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{KE}_{\mathsf{2dh}}} - |\frac{1}{2} - \frac{1}{2}| = \mathsf{AdvAA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{KE}_{\mathsf{2dh}}}.$$

Kombináciou posledných dvoch nerovníc dostávame

$$\mathsf{AdvAA}^{\mathsf{ro}}_{\mathcal{A},\mathsf{KE}_{\mathsf{2dh}}} \leq 2\mathsf{AdvDH}_{\mathcal{B}_{\mathsf{dh}},\mathbb{G}} + \frac{2Q}{q}.$$

$\mathcal{B}_{\mathsf{dh}}$ beží v čase najviac τ — ako útočník $\mathcal{A}$ — plus čas na $O(Q \log q)$ grupových operácií — pri každej otázke sa spraví konštantný počet operácií. □

Záver

Cieľom tejto práce bolo zoznámiť sa s novou variantou Diffie-Hellmanovho problému — so zdvojeným Diffie-Hellmanovým problémom. 2DH problém je len málo pozmenený DH problém. Dôsledkom je, že 2DH predpoklad sa dá použiť v mnohých kryptografických schémach, v ktorých by sme za bežných okolností použili DH predpoklad, bez toho, aby sa príliš znížila efektivita. Platí, že zostáva ťažký, aj keď má prístup do príslušného rozhodovacieho orákula. V tretej kapitole sme sa zoznámili s vetami, ktoré porovnávali DH a 2DH predpoklady. Veta 1 tvrdila, že obyčajný DH predpoklad (bez prístupu do príslušného rozhodovacieho orákula) platí práve vtedy, keď platí silný 2DH predpoklad. Veľmi podobné tvrdila aj Veta 4: (hašovaný) DDH predpoklad platí práve vtedy, keď platí silný zdvojený (hašovaný) DDH predpoklad.

Veta 1 bola zároveň aj motiváciou k zavedeniu tzv. „trapdoor testu“. Je to metóda, na základe ktorej dokáže útočník s pravdepodobnosťou $1 - \frac{1}{q}$ simulovať rozhodovacie orákulum, aj napriek tomu, že nepozná príslušné diskrétne logaritmy daných prvkov. Cieľom útočníka bolo zredukovať silný 2DH predpoklad na DH predpoklad. Trapdoor test nám spolu s 2DH predpokladom vytvára tzv. techniku zdvojenia. Na túto techniku sa môžeme pozerať ako na metódu, ktorá „vylepšuje“ protokoly, ktoré sú založené na platnosti silného DH predpokladu na protokoly, ktorých bezpečnosť je založená na DH probléme.

Vo štvrtej a piatej kapitole sme sa zoznámili s aplikáciami 2DH predpokladu. Konkrétne so zdvojeným ElGamalovým šifrovaním a zdvojeným Diffie-Hellmanovým protokolom na neinteraktívnu výmenu kľúča. Dokázali sme, že zdvojené Elgamalovo šifrovanie je CCA bezpečné v modele náhodného orákula za predpokladu, že symetrická šifra SE je CCA bezpečná a za predpokladu, že DH problém je ťažký. Taktiež sme dokázali, že zdvojený Diffie-Hellmanov protokol na neinteraktívnu výmenu kľúča je bezpečný proti aktívnemu útoku v modele náhodného orákula za predpokladu, že je DH problém ťažký. Ak by nedošlo ku zdvojeniu, tak by bezpečnosť proti útoku typu CCA zostala rovnaká, ako pri hašovanej ElGamalovej schéme, pokiaľ by sme útočníkovi dovolili ľubovolné vkladanie kľúča do verejných adresárov bez vyžadovania dôkazu, že má súkromný kľúč.

Ďalšie aplikácie [4]: nová varianta Cramer-Shoupovho šifrovania, nová varianta Boneh-Franklinovho šifrovania založená na identite, Shoupov DH „samoopravovač“, protokol na výmenu kľúča založeného na autentifikácii heslom PAKE [6].

Pokiaľ čitateľa táto práca zaujala, môžeme mu odporučiť aj zovšeobecnený DH problém na nDH problém. Predstavili ho autori Liqun Chen a Yu Chen v diele *The n-Diffie-Hellman Problem and its Applications* [9].

Zoznam použitej literatúry

[1] Rackoff, Charles, Simon, Daniel R. *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*: in Advances in Cryptology - CRYPT0 '91, ed. J. Feigenbaum. LNCS, vol. 576 Berlin: Springer-Verlag, 1992. ISBN 0-387-55188-3.

[2] Abdalla, Michel, Bellare, Mihir, Rogaway, Phillip. *The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES*: in Topics in Cryptology – CT-RSA 2001, ed. David Naccache. LNCS, vol. 2020 Berlin: Springer-Verlag, 2001. ISBN 3-540-41898-9.

[3] Kurosawa, Kaoru, Matsuo, Toshihiko. *How to Remove MAC from DHIES*: in Information Security and Privacy, ACISP 2004, eds. Huaxiong Wang, Josef Pieprzyk, Vijay Varadharajan, David Naccache. LNCS, vol. 3108 Berlin: Springer-Verlag, 2004. ISBN 3-540-22379-7.

[4] Cash, David, Kiltz, Eike, Shoup, Victor. *The Twin Diffie-Hellman Problem and Applications*: in Advances in Cryptology - EUROCRYPT 2008, ed. Nigel Smart. LNCS, vol. 4965 Berlin: Springer-Verlag, 2008. ISBN 3-540-78966-6.

[5] Menezes, Alfred J., Van Oorschot, Paul C., Vanstone, Scott A. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997. ISBN 0-8493-8523-7.

[6] Abdalla, Michel, Pointcheval, David. *Simple Password-Based Encrypted Key Exchange Protocols*: in Topics in Cryptology – CT-RSA 2005, ed. Alfred John Menezes. LNCS, vol. 3376 Berlin: Springer-Verlag, 2005. ISBN 978-3-540-24399-1.

[7] Diffie, Whitfield, Hellman, Martin E. *New Directions in Cryptography*: in IEEE Transactions on Information Theory. vol. IT-22, no. 6, 1976.

[8] Cramer, Ronald, Shoup, Victor. *Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack*: in SIAM Journal on Computing, 2003.

[9] Chen, Liqun, Chen, Yu. *The n-Diffie-Hellman Problem and its Applications*: in the Proceedings of the 14th Information Security Conference (ISC 2011). Information Processing Letters, 2011.

[10] MacKenzie, Philip. *More Effcient Password-Authenticated Key Exchange*: in Topics in Cryptology – CT-RSA 2001, ed. David Naccache. LNCS, vol. 2020 Berlin: Springer-Verlag, 2001. ISBN 3-540-41898-9.

[11] Boneh, Dan. *The Decision Diffie-Hellman Problem*: in Proceedings of the Third Algorithmic Number Theory Symposium. LNCS, vol. 1423 Berlin: Springer-Verlag, 1998.

Zoznam použitých skratiek

- *DH* — Diffie-Hellman
- *CDH* — výpočtový Diffie-Hellmanov predpoklad
- *DDH* — rozhodovací Diffie-Hellmanov predpoklad
- *2DH* — zdvojený Diffie-Hellman
- *2DDH* — zdvojený rozhodovací Diffie-Hellmanov predpoklad
- *CCA* — útok vybraním zašifrovaného textu
- *AA* — aktívny útok
- *SE* — symetrické šifrovanie
- *PKE* — asymetrické šifrovanie
- *KE* — neinteraktívny protokol na výmenu kľúča
- *PAKE* — protokol na výmenu kľúča založeného na autentifikácii heslom