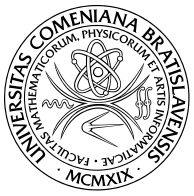
Fakulta matematiky, fyziky a informatiky
Univerzity Komenského v Bratislave



RNDr. Peter Gaži

Autoreferát dizertačnej práce

Methods in Provable Security

(Metódy v dokázateľnej bezpečnosti)

na získanie vedecko-akademickej hodnosti philosophiæ doctor
v odbore doktorandského štúdia: 9.2.1. informatika

Bratislava 2010

Dizertačná práca bola vypracovaná v internej forme doktorandského štúdia na Katedre informatiky Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave.

Predkladateľ: RNDr. Peter Gaži
Katedra informatiky
Fakulta matematiky, fyziky a informatiky
Univerzity Komenského
Mlynská dolina
842 48 Bratislava

Školiteľ: Doc. RNDr. Martin Stanek, PhD.
Katedra informatiky FMFI UK
Bratislava

Oponenti: .....

.....

.....

Obhajoba dizertačnej práce sa koná dňa ..... o ..... h.
pred komisiou pre obhajobu dizertačnej práce v odbore doktorandského štúdia vymenovanou predsedom odborovej komisie dňa .....

v študijnom odbore 9.2.1. informatika

na Fakulte matematiky, fyziky a informatiky UK, Mlynská dolina, miestnosť .....

Predseda odborovej komisie:
Prof. RNDr. Branislav Rovan, PhD.
Fakulta matematiky, fyziky a informatiky
Univerzity Komenského
Mlynská dolina
842 48 Bratislava

1 Úvod

Táto práca sa zaoberá skúmaním metód používaných v oblasti kryptológie známej ako dokázateľná bezpečnosť, ich rozširovaním a aplikáciou na konkrétne problémy.

Keďže moderná kryptológia sa vyvinula do podoby veľmi širokej vednej disciplíny s množstvom oblastí, používané techniky naprieč týmito oblasťami sú tiež veľmi odlišné. Jedným z hlavných atribútov každého modelu používaného na analýzu bezpečnosti kryptografických konštrukcií je, či sú dosahované bezpečnostné garancie výpočtové alebo informačno-teoretické. My v práci prezentujeme výsledky z oboch týchto oblastí, spolu s použitými metódami.

V oblasti výpočtovej bezpečnosti sme sa sústredili na otázky bezpečnosti asymetrických šifrovacích schém. V tejto oblasti už existuje niekoľko zaužívaných a všeobecne akceptovaných kritérií bezpečnosti a sú známe vzťahy medzi nimi. Má však zmysel uvažovať o ďalších užitočných bezpečnostných kritériach, ktoré by mohla asymetrická šifrovacia schéma dosahovať. V práci definujeme bezpečnostné kritérium nerozpoznateľnosti šifrového textu (ciphertext undetectability, CUD). Schéma má túto vlastnosť, ak žiaden efektívny útočník nedokáže (so znalosťou verejného kľúča) odlíšiť náhodný platný šifrový text od náhodného prvku nejakej jednoducho popísateľnej vlastnej nadmnožiny platných šifrových textov. Takto definované bezpečnostné kritérium uvažujeme ako želanú doplnkovú vlastnosť šifrovacej schémy popri klasickej bezpečnosti. Skúmame preto vzťahy CUD k etablovaným bezpečnostným kritériam a generické konštrukcie, ktoré šifrovacej schéme túto vlastnosť dodajú bez straty iných bezpečnostných záruk. Ukážeme tiež, že niektoré existujúce schémy túto vlastnosť dosahujú aj bez ďalších úprav.

V druhej časti práce sa venujeme informačno-teoretickej kryptografii. Predstavíme Maurerovu teóriu náhodných systémov, slúžiacu na analýzu interakcií diskrétnych systémov v informačno-teoretickom scenári. Prezentujeme tiež vlastný príspevok k tejto teórii, ktorý sa ukáže byť užitočným pri aplikácii tejto teórie na analýzu bezpečnosti kaskádového šifrovania.

Úroveň bezpečnosti dosahovaná kaskádovým šifrovaním je intenzívne skúmaným problémom s praktickými dôsledkami. My v práci analyzujeme túto konštrukciu v informačno-teoretickom modeli s ideálnou šifrou. Zovšeobecnením predchádzajúcich analýz ukážeme, že voľne povedané, pre blokové šifry s kratšou dĺžkou kľúča ako dĺžkou bloku (napríklad DES) bezpečnosť kaskádového šifrovania rastie s dĺžkou kaskády.

2 Základné pojmy a označenia

V tejto sekcií definujeme niekoľko pojmov z oblasti dokázateľnej bezpečnosti, ktoré budeme neskôr potrebovať pri popise našich výsledkov.

Funkciu $f\colon \mathbb{N} \to \mathbb{R}$ budeme nazývať zanedbateľnou (negligible) ak pre každú konštantu $c \geq 0$ existuje prirodzené číslo k_c také, že $f(k) \leq k^{-c}$ pre všetky $k \geq k_c$. Usporiadanú k-ticu prvkov z množiny $\mathcal{U}$ budeme označovať ako $u^k = (u_1, \ldots, u_k)$ a množinu všetkých k-tic prvkov $\mathcal{U}$ budeme označovať $\mathcal{U}^k$.

2.1 Asymetrické šifrovacie schémy

Asymetrická šifrovacia schéma je trojica $S = (G, E, D)$, kde G je pravdepodobnostný polynomiálny algoritmus generovania kľúčov, E je pravdepodobnostný polynomiálny šifrovací algoritmus a G je deterministický polynomiálny dešifrovací algoritmus. Algoritmus G dostane na vstupe bezpečnostný parameter k v unárnom kódovaní a vráti pár (pk, sk): verejný a prislúchajúci súkromný kľúč. Tento pár definuje *inštanciu* šifrovacej schémy S; je nimi určená aj množina všetkých otvorených a šifrových textov pre túto inštanciu, a to nasledovne. Množina všetkých otvorených textov sa značí $\mathcal{P}(pk)$, teda $\mathcal{P}(pk) = Dom(E_{pk})$, pričom predpokladáme, že so znalosťou pk možno generovať náhodné prvky $\mathcal{P}(pk)$ aj rozhodovať príslušnosť do tejto množiny efektívne. Symbol $\mathcal{C}(sk)$ označuje množinu $Dom(D_{sk})$ prvkov, ktoré môžu byť vstupom dešifrovacieho algoritmu (aj keď môžu prípadne viesť k špeciálnemu symbolu zlyhania dešifrovania $\perp$). Pre každý súkromný kľúč sk budeme označovať $\mathcal{C}_v(sk)$ množinu všetkých platných šifrových textov pre tento kľúč, teda $\mathcal{C}_v(sk) = \{c \in \mathcal{C}(sk) \mid D_{sk}(c) \neq \perp\}$.

2.2 Teória náhodných systémov

Teória náhodných systémov predstavená v [Mau02] definuje formalizmus na popis interakcie diskrétnych systémov. Správanie každého takéhoto systému $\mathbf{F}$ je určené postupnosťou podmienených pravdepodobnostných distribúcií $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1})$ (pre $i \geq 1$) získania výstupu $y_i \in \mathcal{Y}$ ako odpovede na vstup $x_i \in \mathcal{X}$, za predpokladu predchádzajúcich $i-1$ vstupov $x^{i-1} = (x_1, \ldots, x_{i-1}) \in \mathcal{X}^{i-1}$ a k nim prislúchajúcich výstupov $y^{i-1} = (y_1, \ldots, y_{i-1}) \in \mathcal{Y}^{i-1}$.

Útočník (distinguisher) $\mathbf{D}$ je, neformálne povedané, náhodný systém, ktorý inému systému kladie otázky a dostáva odpovede; na základe takejto interakcie sa potom snaží uhádnuť, s ktorým z dvoch vopred určených systémov

interagoval. Je teda popísaný podmienenými distribúciami $\mathsf{p}^{\mathbf{D}}_{X_i|X^{i-1}Y^{i-1}}$ pre všetky $i \geq 1$. Po istom počte otázok q útočník dá na výstup bit W_q. Ak pre útočníka $\mathbf{D}$ a systémy $\mathbf{F}$ a $\mathbf{G}$ označíme $\mathbf{DF}$ (resp. $\mathbf{DG}$) experiment, v ktorom $\mathbf{D}$ interaguje s $\mathbf{F}$ (resp. $\mathbf{G}$), potom *výhoda* $\mathbf{D}$ pri rozlišovaní $\mathbf{F}$ a $\mathbf{G}$ na q otázok je definovaná ako $\Delta^{\mathbf{D}}_q(\mathbf{F},\mathbf{G}) = \left|\mathsf{P}^{\mathbf{DF}}(W_q = 1) - \mathsf{P}^{\mathbf{DG}}(W_q = 1)\right|$ a $\Delta_q(\mathbf{F},\mathbf{G})$ označuje maximum cez všetkých (výpočtovo neohraničených) útočníkov $\mathbf{D}$.

3 Ciele dizertačnej práce

Ako už bolo uvedené, súčasný výskum v oblasti dokázateľnej bezpečnosti sa odohráva naprieč mnohými oblasťami a využíva množstvo veľmi odlišných metód a prístupov. Cieľom tejto práce je demonštrovať niektoré z týchto prístupov na autorom dosiahnutých výsledkoch. V práci prezentujeme nástroje a výsledky z oboch hlavných oblastí kryptografie: výpočtovej aj informačno-teoretickej.

V rámci sveta výpočtovej bezpečnosti sa zaoberáme bezpečnostnými kritériami pre asymetrické šifrovacie schémy. Ide o pomerne prirodzenú voľbu, keďže asymetrické šifrovanie tak ako ho poznáme nevyhnutne vyžaduje prijať predpoklady o zložitosti nejakého výpočtového problému. Podobné prístupy ako demonštrujeme sa však využívajú aj pri analýze výpočtovej bezpečnosti ďalších konštrukcií (symetrické šifrovanie, digitálne podpisy, MAC).

Dôkazy informačno-teoretickej bezpečnosti kryptografických konštrukcií často spočívajú v analýze interakcií diskrétnych systémov bez obmedzení na ich výpočtovú silu, typicky s cieľom ukázať neodlíšiteľnosť reálneho systému od ideálneho. V práci preto predstavíme všeobecný nástroj na formálne uchopenie takejto analýzy: Maurerovu teóriu náhodných systémov. Zovšeobecníme jeden z jej základných nástrojov a následne ho využijeme pri analýze bezpečnosti kaskádového šifrovania v modeli s ideálnou šifrou.

4 Hlavné výsledky a ich význam

4.1 Výpočtová bezpečnosť

V oblasti výpočtovej bezpečnosti sa venujeme oblasti bezpečnostných kritérií pre asymetrické šifrovacie schémy. Zavádzame pojem nerozpoznateľnosti šifrového textu a skúmame jeho vlastnosti.

4.1.1 Nerozpoznateľnosť šifrového textu.

Neformálne povedané, asymetrická šifrovacia schéma má vlastnosť nerozpoznateľnosti šifrového textu (ciphertext undetectability, CUD), ak žiaden výpočtovo efektívny útočník nie je schopný odlíšiť (so znalosťou verejného kľúča) náhodný platný šifrový text od náhodného prvku nejakej jednoducho popísateľnej vlastnej nadmnožiny platných šifrových textov.

Nerozpoznateľnosť šifrového textu v schéme S definujeme za pomoci experimentu. Nech A je pravdepodobnostný polynomiálny útočník pracujúci v dvoch fázach. V prvej ("ask") fáze A dostane k dispozícii verejný kľúč pk a v závislosti od útočného modelu atk môže mať prístup k dešifrovaciemu orákulu. Výstupom prvej fázy je stavová informácia s. Potom sa na základe uniformne náhodne vygenerovaného bitu b zvolí výzva pre útočníka: jedná sa buď o platný alebo o neplatný šifrový text z množiny $\overline{\mathcal{C}}(pk)$, ktorá je nadmnožinou množiny $\mathcal{C}_v(sk)$ všetkých platných šifrových textov. Táto výzva je spolu so stavovou informáciou s poskytnutá útočníkovi v jeho druhej fáze ("guess") a jeho úlohou je uhádnuť hodnotu bitu b. Experiment je sformalizovaný nasledovne, symbol $\mathbf{C}$ označuje systém množín $\overline{\mathcal{C}}(sk)$ pre každú inštanciu schémy S.

```
Experiment Expt^{cud−atk−b}_{S,C,A}(k)
  (pk, sk) ← G(1^k);
  s ← A^{D1}(ask,pk);
  if b = 1 then y ←$ C_v(sk)
    else y ←$ C̄(pk) \ C_v(sk);
  b′ ← A^{D2}(guess,y,s);
  return b′;
```

útočný model	D_1	D_2
CPA	$\perp$	$\perp$
CCA1	D_{sk}	$\perp$
CCA2	D_{sk}	D_{sk}

Tu platí $b \in \{0,1\}$, $atk \in \{CPA, CCA1, CCA2\}$ a orákulá D_1 a D_2 sú zvolené v závislosti od útočného modelu podľa tabuľky vpravo. Ak $atk = CCA2$, útočníkovi nie je umožnené použiť v druhej fáze dešifrovacie orákulum priamo na dešifrovanie výzvy y. Výhodu (advantage) útočníka A (vzhľadom na $\mathbf{C}$) definujeme ako

$$\mathbf{Adv}^{\mathrm{cud-atk}}_{S,\mathbf{C},A}(k) = \Pr[\mathbf{Expt}^{\mathrm{cud-atk-1}}_{S,\mathbf{C},A}(k) = 1] - \Pr[\mathbf{Expt}^{\mathrm{cud-atk-0}}_{S,\mathbf{C},A}(k) = 1].$$

a túto kvantitu použijeme na definíciu nerozpoznateľnosti šifrového textu nasledujúcim spôsobom:

Definícia 1. *Asymetrická schéma $S = (G, E, D)$ je CUD-atk bezpečná ($atk \in \{CPA, CCA1, CCA2\}$), ak existuje systém $\mathbf{C}$ množín $\overline{\mathcal{C}}(pk)$ pre každú inštanciu (pk, sk) schémy S taký, že platí:*

1. $\mathcal{C}_v(sk) \subsetneq \overline{\mathcal{C}}(pk)$,

2. *existuje deterministický polynomiálny algoritmus, ktorý na vstupe* (pk, c) *akceptuje práve vtedy, keď* $c \in \overline{\mathcal{C}}(pk)$,

3. *pre každého pravdepodobnostného polynomiálneho útočníka* A *je výhoda* $\boldsymbol{Adv}^{\mathrm{cud-atk}}_{S,\mathbf{C},A}(k)$ *zanedbateľná vzhľadom na* k.

Pri skúmaní vlastností pojmu nerozoznateľnosti šifrového textu dospejeme v práci k nasledujúcim výsledkom:

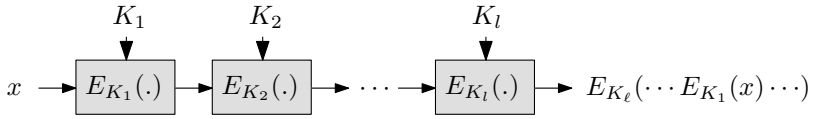
- Ukážeme separáciu tried CUD-CPA/CCA1/CCA2. Navyše demonštrujeme nezávislosť pojmu nerozlíšiteľnosti šifrového textu od zaužívaných kritérií bezpečnosti pre asymetrické šifrovacie schémy: ukážeme separáciu pojmov CUD-atk a IND-CPA/CCA1/CCA2, PA-RO.

- Ukážeme separáciu CUD-*atk* a štandardného pojmu pseudonáhodnosti šifrového textu (ciphertext pseudorandomness, CPR), používaného pri skúmaní steganografických vlastností šifrovacích schém. Ukážeme ale tiež, že za istých prirodzených podmienok je nerozoznateľnosť šifrového textu implikovaná pseudonáhodnosťou šifrového textu.

- Prezentujeme a analyzujeme rôzne spôsoby modifikácie asymetrických šifrovacích schém, pomocou ktorých tieto schémy získajú vlastnosť nerozpoznateľnosti šifrového textu bez straty iných bezpečnostných garancií.

- Ukážeme, že niektoré existujúce asymetrické šifrovacie schémy majú vlastnosť nerozpoznateľnosti šifrového textu aj bez potreby akejkoľvek modifikácie. Menovite, ukážeme, že schémy Cramer-Shoup lite, DEG (Damgård ElGamal) a plnohodnotný Cramer-Shoup dosahujú CUD-CPA za predpokladu obtiažnosti rozhodovacieho Diffie-Hellmanovho problému (DDH) v príslušnej grupe. Tiež ukážeme, že schémy Cramer-Shoup lite a DEG dosahujú CUD-CCA1 za predpokladov DDH a takzvanej Diffie-Hellman Knowledge Assumption (DHK1).

Význam výsledkov: Hlavný prínos tejto časti práce spočíva vo formálnom zavedení pojmu nerozpoznateľnosti šifrového textu. Jedná sa o vlastnosť, ktorú, ako neskôr ukážeme, dosahujú rôzne existujúce šifrovacie schémy, no dosiaľ nebola formálne skúmaná. Keďže ukážeme, že táto vlastnosť je nezávislá od štandardných bezpečnostných kritérií uvažovaných pre asymetrické šifrovacie schémy, je možné ju vnímať ako želanú netriviálnu dodatočnú vlastnosť schém. Preto má zmysel skúmať spôsoby, ako túto vlastnosť dosahovať bez straty iných bezpečnostných garancií.



Obr. 1: Kaskádové šifrovanie dĺžky l, aplikujúce blokovú šifru E postupne s kľúčmi $K_1, \ldots, K_l$.

Ukáže sa tiež, že nerozpoznateľnosť šifrového textu možno za istých podmienok považovať za zoslabenie pojmu pseudonáhodnosti šifrového textu. Ak teda nevieme určitú schému priamo modifikovať tak, aby dosahovala CPR, môžeme použiť niektorý zo skúmaných postupov aspoň na dosiahnutie CUD bezpečnosti.

4.2 Informačno-teoretická bezpečnosť

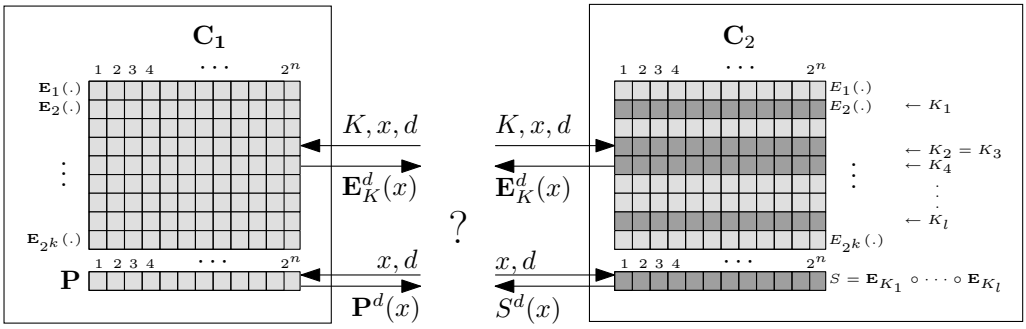
4.2.1 Teória náhodných systémov.

Kľúčovým nástrojom pri aplikácii teórie náhodných systémov na dokazovanie nerozlíšiteľnosti systémov je lema prezentovaná v [Mau02]. Táto lema, neformálne povedané, hovorí, že ak sú dva systémy ekvivalentné pokým je v jednom z nich splnená nejaká presne definovaná podmienka, potom maximálna výhoda pri rozlišovaní týchto dvoch systémov je zhora ohraničená maximálnou dosiahnuteľnou pravdepodobnosťou porušenia tejto podmienky. Toto pozorovanie bolo neskôr formulované aj v špeciálnom prípade formalizmu hrania hier (game-playing scenario) ako Fundamental lemma of game-playing [BR06b] a stalo sa dôležitým a používaným nástrojom v tomto formalizme (viď napr. [BR06a, BN08]).

My v našej práci túto lemu zovšeobecňujeme na prípad, ak rozlišované systémy nie sú ani za dodržania uvažovaných podmienok úplne ekvivalentné, ale rozdiely v ich správaní za dodržania týchto podmienok môžu byť ľahšie kvantifikované. Toto zovšeobecnenie sa ukáže užitočné v ďalej popísanej aplikácii.

4.2.2 Kaskádové šifrovanie.

V záverečnej časti práce aplikujeme dosiahnuté rozšírenia teórie náhodných systémov na analýzu bezpečnosti kaskádového šifrovania v modeli s ideálnou šifrou. Kaskádové šifrovanie je jednoduchá a praktická metóda ako zväčšiť priestor kľúčov blokovej šifry bez nutnosti prechodu na novú šifru. Spočíva v opakovanej aplikácii šifry s nezávisle zvolenými kľúčmi (pozri obr. 1).



Obr. 2: Rozlišovanie náhodnej permutácie (vľavo) od kaskády (vpravo) s možnosťou prístupu k podkladovej blokovej šifre. V oboch prípadoch je útočníkovi umožnené klásť otázky v oboch smeroch ($d \in \{-1, 1\}$).

Model s ideálnou šifrou (ideal cipher model) pozostáva z predpokladu, že bloková šifra použitá v analyzovanej konštrukcií je ideálna: pre každý kľúč realizuje nezávislú, uniformne náhodne zvolenú permutáciu na množine blokov.

Bezpečnosť kaskádového šifrovania teda (v nadväznosti na predchádzajúcu analýzu [BR06b]) formulujeme ako úlohu rozoznávania dvoch systémov: oba obsahujú ideálnu blokovú šifru a permutáciu. V prvom prípade je permutácia uniformne náhodne zvolená, nezávislá od príslušnej blokovej šifry, v druhom prípade je permutácia kaskádou postavenou z tejto šifry (teda zložením permutácií zodpovedajúcich niekoľkým náhodne zvoleným kľúčom). Útočník má možnosť klásť otázky na blokovú šifru i permutáciu v obidvoch smeroch (teda šifrovať aj dešifrovať) a jeho úlohou je zistiť, či interaguje so systémom naľavo alebo napravo. Tento scenár je zobrazený na obr. 2.

Hlavným výsledkom v tejto časti práce je nasledovné tvrdenie zhora ohraničujúce výhodu, ktorú môže ľubovoľný (výpočtovo neobmedzene silný) útočník dosiahnuť vo vyššie popísanom scenári, ak položí najviac q otázok.

Veta 1. *Pre systémy* $\mathbf{C}_1$, $\mathbf{C}_2$ *popísané vyššie platí*

$$\Delta_q(\mathbf{C}_1, \mathbf{C}_2) \leq 2l\alpha^{\lfloor l/2 \rfloor} \frac{q^{\lceil l/2 \rceil}}{(2^k)_l} + 1.9 \left(\frac{lq}{2^{k+n/2}} \right)^{2/3} + \frac{l^2}{2^{k+1}},$$

kde n *popisuje veľkosť bloku,* k *je dĺžka kľúča,* l *je dĺžka kaskády a* $\alpha = \max\{2e2^{k-n}, 2n + k\lfloor l/2 \rfloor\}$.

Význam výsledkov: Otázka posilnenia neodlíšiteľnosti (indistinguishability amplification) dosahovanej kaskádovým šifrovaním je intenzívne skúmaný problém s praktickým významom. V informačno-teoretickom scenári

bol špeciálny prípad trojitého šifrovania skúmaný v práci [BR06b], kde autori ukázali, že trojité šifrovanie je bezpečné, ak útočník nemá možnosť položiť aspoň $2^{k+\frac{1}{2}\min\{n,k\}}$ otázok a zároveň poukázali na bezpečnosť dlhších kaskád ako na zaujímavý otvorený problém. My tento otvorený problém čiastočne vyriešime, keďže náš výsledok implikuje, že kaskádové šifrovanie dĺžky l je bezpečné až po hranicu (veľmi približne) $2^{k+\min\{n/2,k\}}$ otázok. To znamená, že pre blokové šifry s kratším kľúčom ako dĺžkou bloku (napríklad DES) bezpečnosť kaskády rastie s jej dĺžkou až po istú hranicu.

5 Zoznam použitej literatúry

[3DE98] ANSI X9.52: Triple Data Encryption Algorithm Modes of Operation, 1998.

[3DE99] FIPS PUB 46-3: Data Encryption Standard (DES). National Institute of Standards and Technology, 1999.

[3DE04] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. National Institute of Standards and Technology, Special Publication 800-67, 2004.

[ABCV98] William Aiello, Mihir Bellare, Giovanni Di Crescenzo, and Ramarathnam Venkatesan. Security amplification by composition: The case of doubly-iterated, ideal ciphers. In *CRYPTO '98: Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, volume 1462 of *Lecture Notes in Computer Science*, pages 499–558. Springer-Verlag, 1998.

[AH04] L. Ahn and N. Hopper. Public-key steganography. In *Advances in Cryptology — EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 322–339. Springer-Verlag, 2004.

[AM09] Divesh Aggarwal and Ueli Maurer. Breaking RSA Generically is Equivalent to Factoring. In A. Joux, editor, *Advances in Cryptology - EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 36–53. Springer-Verlag, April 2009.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[BC04] Michael Backes and Christian Cachin. Public-key steganography with active attacks. In *Theory of Cryptography Conference Proceedings*, volume 3378 of *Lecture Notes in Computer Science*, pages 210–226. Springer-Verlag, 2004.

[BDJR97] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of the 38th Symposium on Foundations of Computer Science*, pages 394–403, 1997.

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology — CRYPTO 1998*, Lecture Notes in Computer Science, pages 26–45. Springer-Verlag, 1998.

[BFM88a] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the* 20^{th} *Annual Symposium on the Theory of Computing*, pages 103–112, 1988.

[BFM88b] Manuel Blum, Paul Feldman, and Silvio Micali. Proving security against chosen ciphertext attacks. In *Advances in Cryptology - CRYPTO 1988*, Lecture Notes in Computer Science, pages 256–268. Springer-Verlag, 1988.

[BKR94] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of cipher block chaining message authentication code. In *CRYPTO '94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology*, Lecture Notes in Computer Science, pages 341–358. Springer-Verlag, 1994.

[BL96] Dan Boneh and Richard J. Lipton. Algorithms for black-box fields and their application to cryptography. In *Advances in Cryptology - CRYPTO 1996*, Lecture Notes in Computer Science, pages 283–297. Springer-Verlag, 1996.

[Ble98] Daniel Bleichenbacher. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1. In *Advances in Cryptology - CRYPTO 1998*, Lecture Notes in Computer Science, pages 1–12. Springer-Verlag, 1998.

[BN08] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *J. Cryptology*, 21(4):469–491, 2008.

[Bon98] Dan Boneh. The Decision Diffie-Hellman Problem. In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer-Verlag, 1998.

[BP04] Mihir Bellare and Adriana Palacio. Towards plaintext-aware public-key encryption without random oracles. In *Advances in Cryptology - ASIACRYPT 2004*, Lecture Notes in Computer Science, pages 48–62. Springer-Verlag, 2004.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

[BR94] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In *Advances in Cryptology — EUROCRYPT 1994*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer-Verlag, 1994.

[BR06a] Mihir Bellare and Thomas Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. In *Advances in Cryptology - ASIACRYPT 2006*, pages 299–314. Springer-Verlag, 2006.

[BR06b] Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. In *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 409–426. Springer-Verlag, 2006. Full version at `http://eprint.iacr.org/2004/331`.

[Bro05] Daniel R. L. Brown. Breaking RSA May Be As Difficult As Factoring. Cryptology ePrint Archive, Report 2005/380, 2005. http://eprint.iacr.org/.

[BV98] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA May Not Be Equivalent to Factoring. In *Advances in Cryptology — EUROCRYPT 1998*, Lecture Notes in Computer Science, pages 59–71. Springer-Verlag, 1998.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *STOC '98: Proceedings of the*

thirtieth annual ACM symposium on Theory of computing, pages 209–218. ACM, 1998.

[CK78] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[CPS08] Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin. The random oracle model and the ideal cipher model are equivalent. In *CRYPTO 2008: Proceedings of the 28th Annual conference on Cryptology*, volume 5157 of *Lecture Notes in Computer Science*, pages 1–20. Springer-Verlag, 2008.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Advances in Cryptology - CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer-Verlag, 1998.

[CS04] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, 2004.

[Dam92] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, volume 576 of *Lecture Notes in Computer Science*, pages 445–456. Springer-Verlag, 1992.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 542–552. ACM, 1991.

[Den06] Alexander W. Dent. The Cramer-Shoup Encryption Scheme Is Plaintext Aware in the Standard Model. In *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 289–307. Springer-Verlag, 2006.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[DH77] W. Diffie and M. E. Hellman. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10(6):74–84, 1977.

[EG85a] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology - CRYPTO 1984*, Lecture Notes in Computer Science, pages 10–18. Springer-Verlag, 1985.

[EG85b] S. Even and O. Goldreich. On the power of cascade ciphers. *ACM Trans. Comput. Syst.*, 3(2):108–116, 1985.

[EM91] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In *Journal of Cryptology*, pages 151–161. Springer-Verlag, 1991.

[Gaž07] Peter Gaži. Using ElGamal in the OAEP+ scheme. *Journal of Electrical Engineering*, 58(7/s):7–10, 2007.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC '82: Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 365–377. ACM, 1982.

[GM09] Peter Gaži and Ueli Maurer. Cascade encryption revisited. In M. Matsui, editor, *Advances in Cryptology — ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 37–51. Springer-Verlag, December 2009.

[GM10] Peter Gaži and Ueli Maurer. Free-start distinguishing: Combining two types of indistinguishability amplification. In K. Kurosawa, editor, *The 4th International Conference on Information Theoretic Security - ICITS 2009*, volume 5973 of *Lecture Notes in Computer Science*, pages 28–44. Springer-Verlag, 2010.

[Gol00] Oded Goldreich. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, New York, NY, USA, 2000.

[GS08] Peter Gaži and Martin Stanek. On ciphertext undetectability. *Tatra Mountains Mathematical Publications*, 41(7/s):133–151, 2008.

[HGS99] Chris Hall, Ian Goldberg, and Bruce Schneier. Reaction attacks against several public-key cryptosystems. In *ICICS '99: Proceedings of the Second International Conference on Information and Communication Security*, volume 1726 of *Lecture Notes in Computer Science*, pages 2–12. Springer-Verlag, 1999.

[JQY01] Marc Joye, Jean-Jacques Quisquater, and Moti Yung. On the Power of Misbehaving Adversaries and Security Analysis of the Original EPOC. In *CT-RSA 2001: Proceedings of the 2001 Conference on Topics in Cryptology*, volume 2020 of *Lecture Notes in Computer Science*, pages 208–222, London, UK, 2001. Springer-Verlag.

[Mau92] Ueli Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[Mau93] Ueli Maurer. Secret key agreement by public discussion. *IEEE Transactions on Information Theory*, 39(3):733–742, May 1993.

[Mau94] Ueli Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. In Yvo Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 271–281. Springer-Verlag, August 1994.

[Mau99] Ueli Maurer. Information-theoretic cryptography. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 47–64. Springer-Verlag, August 1999.

[Mau02] Ueli Maurer. Indistinguishability of random systems. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 110–132. Springer-Verlag, May 2002.

[Mau05] Ueli Maurer. Abstract models of computation in cryptography. In Nigel Smart, editor, *Cryptography and Coding 2005*, volume 3796 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, December 2005.

[Mau09] Ueli Maurer. Abstraction in cryptography. In Shai Halevi, editor, *Advances in Cryptology — CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, page 459. Springer-Verlag, August 2009.

[MM93] Ueli Maurer and James L. Massey. Cascade ciphers: The importance of being first. *Journal of Cryptology*, 6(1):55–61, 1993.

[Möl04] Bodo Möller. A public-key encryption scheme with pseudorandom ciphertexts. In *Proceedings of ESORICS 2004*, volume 3193 of *Lecture Notes in Computer Science*, pages 335–351. Springer-Verlag, 2004.

[MOPS06] Ueli Maurer, Yvonne Anne Oswald, Krzysztof Pietrzak, and Johan Sjödin. Luby-Rackoff ciphers from weak round functions? In *Advances in Cryptology — EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 391–408. Springer-Verlag, May 2006.

[MP04] Ueli Maurer and Krzysztof Pietrzak. Composition of random systems: When two weak make one strong. In Moni Naor, editor, *Theory of Cryptography Conference — TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 410–427. Springer-Verlag, February 2004.

[MPR07] Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *Advances in Cryptology — CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer-Verlag, August 2007.

[MR09] Ueli Maurer and Renato Renner. Abstract cryptography. Manuscript, 2009.

[MT07] Ueli Maurer and Stefano Tessaro. Domain extension of public random functions: Beyond the birthday barrier. In Alfred Menezes, editor, *Advances in Cryptology — CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 187–204. Springer-Verlag, August 2007. Full version available from http://eprint.iacr.org/2007/229.

[MW99] Ueli Maurer and Stefan Wolf. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. *SIAM Journal on Computing*, 28(5):1689–1721, April 1999.

[NY90] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC '90: Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 427–437. ACM, 1990.

[OP01] Tatsuaki Okamoto and David Pointcheval. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. In *CT-RSA 2001: Proceedings of the 2001 Conference on Topics in Cryptology*, volume 2020 of *Lecture Notes in Computer Science*, pages 159–175. Springer-Verlag, 2001.

[Poi05] D. Pointcheval. Contemporary Cryptology – Provable Security for Public Key Schemes. Advanced Courses CRM Barcelona, 2005.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. Springer-Verlag, 1992.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28(4):656–715, 1949.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in Cryptology - EUROCRYPT 1997*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer-Verlag, 1997.

[Sho01] Victor Shoup. OAEP Reconsidered. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, volume 2139 of *Lecture Notes in Computer Science*, pages 239–259. Springer-Verlag, 2001.

[Vau00] Serge Vaudenay. Adaptive-attack norm for decorrelation and super-pseudorandomness. In *SAC '99: Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography*, Lecture Notes in Computer Science, pages 49–61. Springer-Verlag, 2000.

[Wol98] Stefan Wolf. Unconditional security in cryptography. In Ivan Damgård, editor, *Lectures on Data Security: Modern Cryptology in Theory and Practice*, volume 1561 of *Lecture Notes in Computer Science*, pages 217–250. Springer-Verlag, July 1998.

[Wyn75] Aaron D. Wyner. The Wire-tap Channel. *Bell Systems Technical Journal*, 54(8):1355–1387, January 1975.

6 Zoznam publikovaných prác autora so vzťahom ku skúmanej problematike

[Gaž07] Peter Gaži. Using ElGamal in the OAEP+ scheme. *Journal of Electrical Engineering*, 58(7/s):7–10, 2007.

[GS08] Peter Gaži and Martin Stanek. On ciphertext undetectability. *Tatra Mountains Mathematical Publications*, 41(7/s):133–151, 2008.

[GM09] Peter Gaži and Ueli Maurer. Cascade encryption revisited. In M. Matsui, editor, *Advances in Cryptology — ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 37–51. Springer-Verlag, December 2009.

[GM10] Peter Gaži and Ueli Maurer. Free-start distinguishing: Combining two types of indistinguishability amplification. In K. Kurosawa, editor, *The 4th International Conference on Information Theoretic Security - ICITS 2009*, volume 5973 of *Lecture Notes in Computer Science*, pages 28–44. Springer-Verlag, 2010.

7 Ohlasy na prácu

Cituje [GM09]:

[BR08] Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive, Report 2004/331, version 3.0, 2008. The proceedings version appeared in Advances in Cryptology - Eurocrypt 2006.

[Tes10] Stefano Tessaro. Security Amplification for the Cascade of Arbitrarily Weak PRPs: Tight Bounds via the Interactive Hardcore Lemma. Submitted manuscript, available at `http://www.crypto.ethz.ch/publications/`, January 2010.

Cituje [GM10]:

[Tes10] Stefano Tessaro. Security Amplification for the Cascade of Arbitrarily Weak PRPs: Tight Bounds via the Interactive Hardcore Lemma. Submitted manuscript, available at `http://www.crypto.ethz.ch/publications/`, January 2010.

8 Summary

This thesis is focusing on understanding the typical methods used in the area of provable security, extending them and applying them to certain cryptographic problems.

Modern cryptography has evolved into a broad research field with a lot of areas, hence the techniques used across these areas are very different. One of the main attributes of each model used for analyzing cryptographic constructions is whether the security guarantees obtained are computational or information-theoretic. In this thesis we present results from both these domains along with the methods used to obtain them.

In the area of computational security, we concentrate on the security of public-key encryption schemes. There are several established notions of security in this area and the relationships among them are known. However, it turns out to be useful to consider additional, special-purpose properties of encryption schemes that are not implied by the usual security notions. We define and analyze the notion of ciphertext undetectability (CUD). Loosely speaking, an encryption scheme satisfies this property if no efficient adversary can distinguish (given the public key) a randomly chosen valid ciphertext from a randomly chosen element of some easily recognizable superset of all valid ciphertexts. This notion is presented as a desirable additional property of an encryption scheme when coupled with some classical security notion. Therefore, we investigate relationships between CUD and the established notions, and generic modifications of existing encryption schemes such that they acquire the ciphertext undetectability property without loosing their original security guarantees. We also prove some existing schemes to satisfy the CUD property without any modifications.

In the second part of the thesis we focus on information-theoretic cryptography. We introduce Maurer's theory of random systems, a tool for analyzing interactions of discrete systems in the information-theoretic scenario. We also present our own contribution to this framework, which turns out to be useful when employing the framework in an analysis of the security of cascade encryption.

The security amplification achieved by cascade encryption is a well-studied problem with practical implications. We analyze this construction in the information-theoretic scenario, using the ideal cipher model. Our result implies that, loosely speaking, for blockciphers with smaller key length than block length (e.g. DES) the security increases with the length of the cascade.