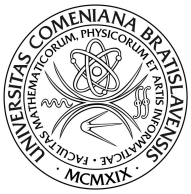


Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

RNDr. Michal Rjaško

Autoreferát dizertačnej práce

Cryptographic Hash Functions

(Kryptografické hašovacie funkcie)

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

Bratislava 2012

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

Predkladateľ: RNDr. Michal Rjaško
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 ..... 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, ...

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

1 Úvod

V rámci kryptografie existuje veľké množstvo oblastí, ktoré využívajú kryptografické hašovacie funkcie: digitálne podpisy, ochrana hesiel, autentifikácia správ, atď. Každá aplikácia kryptografických hašovacích funkcií má svoje vlastné nároky na použitú hašovaciu funkciu. Veľké množstvo aplikácii však vyžaduje veľké množstvo rôznych vlastností, ktoré sa od kryptografických hašovacích funkcií očakávajú.

Kryptografické hašovacie funkcie zobrazujú binárne reťazce (takmer) ľubovoľnej dĺžky na reťazce pevnej dĺžky – zvyčajne 128 až 512 bitov. Výstup hašovacej funkcie nazývame haš alebo obraz. Vstupné reťazce voláme správy. Každá aplikácia má svoje vlastné nároky na použitú hašovaciu funkciu. Existuje však niekoľko vlastností, ktoré by mala spĺňať každá hašovacia funkcia:

- *odolnosť voči nájdeniu vzoru* - pre daný obraz y je ťažké nájsť správu m, ktorej haš je y.
- *odolnosť voči nájdeniu 2. vzoru* - pre danú správu m je ťažké nájsť inú správu m', ktorá ma rovnaký obraz ako m.
- *odolnosť voči kolíziám* - je ťažké nájsť dve správy s rovnakým obrazom.

Hašovacia funkcia by sa mala správať dostatočne "náhodne" a musí byť zároveň aj výpočtovo efektívna.

V posledných rokoch bolo objavených niekoľko útokov na najpoužívanejšie hašovacie funkcie MD5 a SHA-1. Útoky na hašovaciu funkciu MD5 [25, 44] je možné vykonať v reálnom čase. Útoky na SHA-1 [43] nie sú prakticky vykonateľné, avšak ich zložitosť je menšia ako by sa očakávalo od "ideálnej" hašovacej funkcie. Z tohto dôvodu americký inštitút NIST (National Institute for Standards and Technology) vyhlásil v roku 2007 verejnú súťaž na nový hašovací štandard SHA-3. Súťaž je momentálne v jej poslednom kole, bolo vybraných 5 finalistov, z ktorých bude do konca roka 2012 vybraný víťaz.

V tejto práci sme sa sústredili na návrh a analýzu konštrukcií, ktoré dokázateľne spĺňajú dôležité vlastnosti hašovacích funkcií, analýzu vlastností hašovacích funkcií a vzťahov medzi týmito vlastnosťami.

V prvej časti práce sa venujeme tzv. robustným kombinátorom. Sú to konštrukcie spájajúce viacero hašovacích funkcií do jednej funkcie, ktorá je bezpečná (v zmysle nejakej vlastnosti), ak je bezpečná aspoň jedna z čiastkových hašovacích funkcií. Dokázali sme, že robustné kombinátory s krátkou dĺžkou výstupu pre odolnosť voči nájdeniu prvého a druhého vzoru neexistujú. Výsledky z tejto časti práce nadväzujú na výsledky

Boneha, Boyena a Pietrzaka [8, 35, 36] o neexistencii robustných kombinátorov s krátkou dĺžkou výstupu pre odolnosť voči kolíziám.

V druhej časti práce prezentujeme niekoľko konštrukcií, ktoré zabezpečujú spĺňanie viacerých vlastností jednou hašovacou funkciou. Ide o kombináciu aspoň dvoch hašovacích funkcií, kde jednotlivé funkcie spĺňajú isté vlastnosti a výsledná hašovacia funkcia spĺňa všetky vlastnosti.

Ďalšia časť práce obsahuje návrh novej vlastnosti hašovacích funkcií, tzv. black-box vlastnosť. Ambíciou pri návrhu black-box vlastnosti bolo navrhnúť „univerzálnu“ vlastnosť, ktorá bude zabezpečovať spĺňanie väčšiny z vlastností hašovacích funkcií. V práci dokazujeme niekoľko základných výsledkov súvisiacich s touto vlastnosťou, okrem iného aj ekvivalenciu medzi black-box vlastnosťou kombinovanou so pseudo-náhodnosťou a vlastnosťou pseudo-náhodného orákula.

Veľa kryptografických schém využívajúcich hašovacie funkcie má dôkaz bezpečnosti v tzv. modeli s náhodným orákulom, kde je hašovacia funkcia nahradená náhodnou funkciou. Dôkaz bezpečnosti je tak oveľa jednoduchší, avšak v skutočnosti nezaručuje bezpečnosť systému po inštancovaní náhodnej funkcie reálnou hašovacou funkciou [9]. Takýto dôkaz poskytuje iba heuristické garancie, že ak je hašovacia funkcia dostatočne “náhodná”, potom bude aj výsledná schéma bezpečná. Existuje niekoľko vlastností, ktoré sa snažia zabezpečiť “náhodné” správanie hašovacej funkcie. Jedna z nich je aj vlastnosť pseudo-náhodného orákula (Pro). V poslednej časti práce analyzujeme variant tejto vlastnosti – vlastnosť pseudo-náhodného orákula s verejnými obrazmi (Img-Pro), kde má útočník prístup ku všetkým obrazom, ktoré boli vyprodukované hašovacou funkciou. Dokázali sme, že vlastnosť Img-Pro je ekvivalentná vlastnosti Pro.

2 Hlavné výsledky práce

2.1 Robustné kombinátory

Vo všeobecnosti, (k, l)-robustný kombinátor pre l hašovacích funkcií $F_1, \ldots, F_l$, kde $F_i : \{0,1\}^* \to \{0,1\}^v$, $i = 1, \ldots, l$ je dvojica algoritmov (C, P), kde

- $C : \{0,1\}^m \to \{0,1\}^y$ je algoritmus ktorý kombinuje hašovacie funkcie $F_1, \ldots, F_l$, ku ktorým má orákulovský prístup. Algoritmus C dostane na vstupe správu M, počas svojho behu sa môže ľubovoľne veľa krát spýtať dotaz na $F_1, \ldots, F_l$. Nakoniec C vráti obraz správy M.

- P poskytuje dôkaz bezpečnosti pre C. Je to algoritmus, ktorý transformuje

schopnosť útočiť (v zmysle nejakej vlastnosti) na C na schopnosť útočiť na k z l čiastkových hašovacích funkcií.

V prípade robustných kombinátorov pre odolnosť voči kolíziám je úlohou algoritmu P transformovať kolíziu v C na kolízie v aspoň k čiastkových funkciách. Uvažujme napr. nasledovný $(1, 2)$-robustný kombinátor pre odolnosť voči kolíziám:

$$C^{F_1,F_2}(M) := F_1(M)||F_2(M).$$

Ak máme dve správy M a M', ktoré kolidujú v C, tak potom tieto dve správy kolidujú v obidvoch funkciách F_1 aj v F_2. Nevýhodou tohto kombinátora je jeho veľká dĺžka výstupu, ktorá je dvojnásobkom dĺžky výstupu čiastkových hašovacích funkcií.

V prípade odolnosti voči nájdeniu vzoru je P súčasťou nasledovnej hry. Nech f je funkcia, ktorá pre daný obraz Y vráti správu M, pričom $C^{F_1,\ldots,F_l}(M) = Y$. Ak taká správa M neexistuje, potom f vráti $\perp$. (Funkciu f môžeme chápať ako "zariadenie" (čiernu skrinku), ktoré je schopné hľadať vzory k obrazom z $C^{F_1,\ldots,F_l}$.)

Hra Pre-Comb^f:

1. Náhodne sa vyberie správa w a vypočíta sa $y_1 = F_1(w), \ldots, y_l = F_l(w)$. Obrazy $y_1, \ldots, y_l$ sú odoslané na vstup do P.
2. P s orákulovským prístupom k $F_1, \ldots, F_l$ vráti obraz $Y \in \{0,1\}^y$.
3. Správa $M = f(Y)$, kde $C^{F_1,\ldots,F_l}(M) = Y$, je odoslaná do P. Ak $f(Y) = \perp$ tak hra končí a P neuspelo.
4. P pokračuje v behu, nakoniec vráti vektor $\mathbf{W} = (w'_1, \ldots, w'_l)$.

Nech

$$\mathbf{Adv}_P^{\mathrm{PreComb}[k]}[(F_1, \ldots, F_l), (y_1, \ldots, y_l), f]$$

označuje pravdepodobnosť, že P uspeje, t.j. aspoň pre k indexov $i = 1, \ldots, l$ platí $F_i(w'_i) = y_i$.

Algoritmus P kombinátora pre odolnosť voči nájdeniu druhého vzoru hrá nasledovnú hru. Nech f je funkcia, ktorá pre danú správu M vráti inú správu M' takú, že $C^{F_1,\ldots,F_l}(M) = C^{F_1,\ldots,F_l}(M')$. Ak taká správa M' neexistuje, potom f vráti $\perp$.

Hra Sec-Comb^f:

1. Náhodne sa vyberie správa w a pošle sa na vstup do P.
2. P s orákulovským prístupom k $F_1, \ldots, F_l$ vráti správu $M \in \{0,1\}^m$.

3. Správa $M' = f(M)$, kde $M' \neq M$ and $C^{F_1,\ldots,F_l}(M) = C^{F_1,\ldots,F_l}(M')$, je odoslaná do P.
4. P pokračuje v behu, nakoniec vráti vektor $\mathbf{W} = (w'_1, \ldots, w'_l)$.

Nech

$$\mathbf{Adv}_P^{\mathrm{SecComb}[k]}[(F_1, \ldots, F_l), w, f]$$

označuje pravdepodobnosť, že P uspeje, t.j. aspoň pre k indexov $i = 1, \ldots, l$ platí $F_i(w'_i) = F_i(w)$.

Hlavným výsledkom tejto časti práce sú nižšie uvedené výsledky o neexistencii kombinátorov s krátkou dĺžkou výstupu pre odolnosť voči nájdeniu prvého a druhého vzoru. Dodatočné bezpečnostné garancie, ktoré robustné kombinátory poskytujú, sú teda len za cenu väčšej dĺžky výstupu.

Veta 1. *Nech (C, P) je (k, l)-robustný kombinátor pre odolnosť voči nájdeniu vzoru, ktorý kombinuje l hašovacích funkcií $F_1, \ldots, F_l : \{0,1\}^* \to \{0,1\}^v$. Predpokladajme, že C urobí najviac q_C dotazov na svoje orákulá $F_1, \ldots, F_l$. Ďalej predpokladajme, že pre dĺžku výstupu y algoritmu C platí*

$$y < (v - \lg(q_C))(l - k + 1) - l.$$

Potom existujú obrazy $y_1, \ldots, y_l$ a hašovacie funkcie $F_1, \ldots, F_l$ a f, pre ktoré je

$$\mathbf{Adv}_P^{\mathrm{PreComb}[k]}[(F_1, \ldots, F_l), (y_1, \ldots, y_l), f]$$

zanedbateľná.

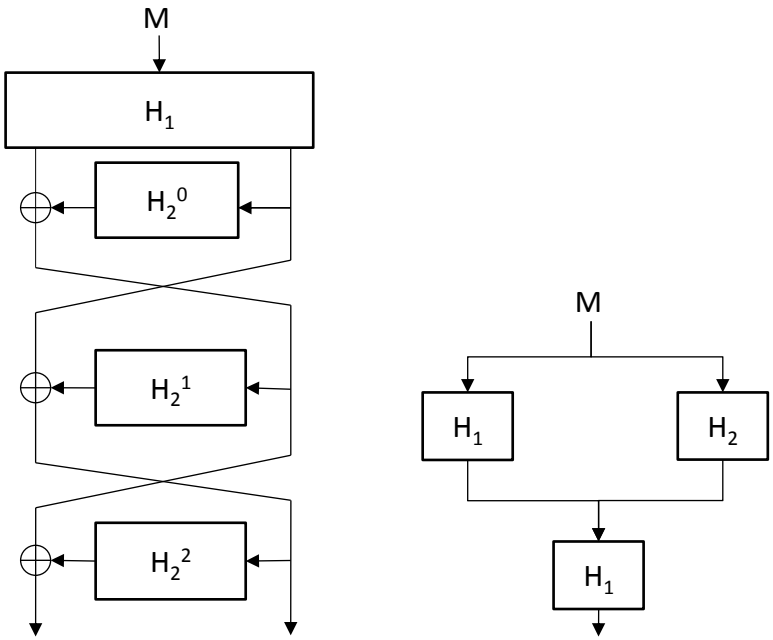
Veta 2. *Nech (C, P) je (k, l)-robustný kombinátor pre odolnosť voči nájdeniu druhého vzoru, ktorý kombinuje l hašovacích funkcií $F_1, \ldots, F_l : \{0,1\}^* \to \{0,1\}^v$. Predpokladajme, že C urobí najviac q_C dotazov na svoje orákulá $F_1, \ldots, F_l$. Ďalej predpokladajme, že pre dĺžku výstupu y algoritmu C platí*

$$y < (v - \lg(q_C))(l - k + 1) - l + 1.$$

Potom existuje správa w a hašovacie funkcie $F_1, \ldots, F_l$ a f, pre ktoré je

$$\mathbf{Adv}_P^{\mathrm{SecComb}[k]}[(F_1, \ldots, F_l), w, f]$$

zanedbateľná.



Obr. 1: Konštrukcie kombinátorov vlastností pre pseudo-náhodnosť a odolnosť voči kolíziám (vľavo) a všade odolnosť voči nájdeniu vzoru a odolnosť voči kolíziám (vpravo).

2.2 Kombinátory vlastností

V tejto kapitole sme zaviedli pojdem "kombinátor vlastností", čo je konštrukcia kombinujúca niekoľko vlastností z rôznych hašovacích funkcií do jednej hašovacej funkcie. Navrhli sme dve konštrukcie kombinátorov vlastností C_1 a C_2 (obr. 1). Konštrukcia C_1 (obr. 1 vľavo) kombinuje dve rodiny hašovacích funkcií H_1, H_2, pričom ak H_1 je pseudo-náhodná (Prf) a H_2 odolná voči kolíziám (Coll), tak C_1 je Prf a zároveň Coll. Konštrukcia je postavená na trojkolovej Feistelovskej permutácii aplikovanej na funkciu odolnú voči kolíziám.

Konštrukcia C_2 (obr. 1 vpravo) je Coll a všade odolná voči nájdeniu vzoru (ePre), ak H_1 je Coll a H_2 ePre. Kombinátory vieme zároveň skombinovať do konštrukcie $C_1^{H_1,C_2^{H_2,H_3}}$, ktorá je Prf, Coll a ePre, ak H_1 je Prf, H_2 je Coll a H_3 ePre.

2.3 Black-box vlastnosť

Hra $G^{O,A}$ je efektívny pravdepodobnostný algoritmus, ktorého výstup je jeden bit $b \in \{0,1\}$. Ak $b = 1$ tak hovoríme, že útočník A uspel v hre G proti orákulu O.

Ak $b = 0$ tak hovoríme, že A prehral hru G proti orákulu O. Neformálne povedané, netriviálna hra je taká, ktorú je ťažké vyhrať ak O je náhodné orákulum.

Nech $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ je rodina hašovacích funkcií, G je ľubovoľná hra a A je útočník. Uvažujme nasledovný experiment:

Experiment HashBB(H, G, A, S)

1. choose $K \xleftarrow{\$} \{0,1\}^k$
2. run $G^{H_K, A^K} \to b$
3. run $G^{H_K, S^{H_K}} \to b'$
4. if $b \neq b'$ return 1
5. otherwise return 0

Definícia 1. *Hovoríme, že rodina hašovacích funkcií $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ má black-box vlastnosť, ak pre všetky netriviálne hry G a všetkých útočníkov A existuje polynomiálny algoritmus S (nazývaný simulátor) pre ktoré je pravdepodobnosť*

$$\Pr\left[\text{HashBB}(H, G, A, S) = 1\right]$$

zanedbateľná

Ak ma rodina hašovacích funkcií H black-box vlastnosť a zároveň je pseudo-náhodná, hovoríme, že H je Prf-BB.

Transformácia rozširujúca doménu je konštrukcia, ktorá z "kompresnej" funckie f s fixnou dĺžkou vstupu vytvorí funkciu s ľubovoľnou dĺžkou vstupu. Hovoríme, že transformácia zachováva určitú vlastnosť P, ak výsledná hašovacia funkcia spĺňa vlastnosť P za predpokladu spĺňania vlastnosti P kompresnou funkciou. V práci sme ukázali, že známa Merkle-Damgårdova iteratívna konštrukcia nezachováva Prf-BB vlastnosť. Naopak, konštrukcia HMAC ju zachováva. Hlavným výsledkom tejto časti práce je dôkaz, že každá transformácia, ktorá zachováva Prf-BB vlastnosť, zachováva aj vlastnosť Pro a naopak. Prf-BB je teda v istom zmysle ekvivalentnou vlastnosťou k vlastnosti Pro. Vlastnosť Prf-BB je na rozdiel od Pro vlastnosti definovaná v štandardnom modeli (vlastnosť Pro má definíciu iba v modeli s náhodným orákulom).

Veta 3. *Nech H je tranformácia rozširujúca doménu kompresnej funkcie f. Potom H je Prf-BB práve vtedy keď H je Pro.*

2.4 Pseudo-náhodné orákulum s verejnými obrazmi

Vlastnosť pseudo-náhodného orákula (Pro) je vlastnosť transformácii rozširujúcich doménu postavená na pojme nerozpoznateľnosti. Hašovacia funkcia H^f postavená na kompresnej funkcii f má vlastnosť Pro, ak je nerozpoznateľná od náhodného orákula.

Je ľahké nahliadnuť, že Merkle-Damgårdova (MD) konštrukcia nemá vlastnosť Pro. Existuje však veľké množstvo aplikácií, ktoré využívajú hašovacie funkcie postavené na MD konštrukcii, no doteraz na nich nebol nájdený žiaden útok. Z tohto dôvodu Dodis a kol. [13] definovali tzv. vlastnosť verejne používaného pseudo-náhodného orákula (Pub-Pro), ktorá je dostatočne silná na to, aby bolo možné dokázať bezpečnosť niektorých krytpografických systémov a zároveň dostatočne slabá na to, aby ju MD konštrukcia zachovávala.

Veľa aplikácií (napr. digitálne podpisy) počíta haš iba zo správ, ktoré sú verejne dostupné, t.j. nie sú tajné. Bezpečnosť takýchto aplikácií nie je ohroznená, ak sú všetky zahašované správy dostupné aj pre potenciálnych útočníkov. Vlastnosť Pub-Pro je vhodná pre takéto aplikácie. Pub-Pro zabezpečuje nerozpoznateľnosť hašovacej funkcie od verejne dostupného náhodného orákula. Ide o náhodné orákulum, ktoré si pamätá všetky zahašované správy a na požiadanie ich sprístupní komukoľvek. Dodis a kol. [13] ukázali, že MD konštrukcia zachováva vlastnosť Pub-Pro.

V tejto časti práce analyzujeme vlastnosť pseudo-náhodného orákula s verejnými obrazmi (Img-Pro), ktorá je niekde medzi vlastnosťami Pro a Pub-Pro. Vlastnosť Img-Pro predpokladá verejnú dostupnosť iba obrazov zahašovaných správ, samotné správy zostávajú tajné. Ukázali sme, že vlastnosť Img-Pro je ekvivalentná vlastnosti Pro. Prístup iba k obrazom zahašovaných správ teda nepridáva útočníkovi na sile.

Veta 4. *Nech H je tranformácia rozširujúca doménu kompresnej funkcie f. Potom H je Pro práve vtedy keď H je Img-Pro.*

3 Zoznam použitej literatúry

[1] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 1–18, London, UK, UK, 2001. Springer-Verlag.

[2] M. Bellare, R. Canneti, and H. Krawczyk. Keying Hash Functions for Message Authentication. In *Advances in Cryptology – Crypto 96, LNCS vol. 1109*, pages 1–15. Springer, 1996.

[3] M. Bellare and T. Ristenpart. Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms. In *International Colloquim on Automata, Languages, and Progamming, LNCS vol. 4596*, pages 399–410. Springer, 2006.

[4] M. Bellare and T. Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. In *Advances in Cryptology - ASIACRYPT 2006, LNCS vol. 4284*, pages 299–314. Springer, 2006.

[5] M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM, 1993.

[6] M. Bellare and P. Rogaway. Collision-Resistant hashing: Towards making UOWHFs practical. In *Advances in Cryptology - CRYPTO '97, LNCS vol. 1294*, pages 470–484. Springer, 1997.

[7] E. Biham and O. Dunkelman. A framework for iterative hash functions: Haifa. In *Proceedings of Second NIST Cryptographic Hash Workshop*, 2006.

[8] D. Boneh and X. Boyen. On the Impossibility of Efficiently Combining Collision Resistant Hash Functions. In *Advances in Cryptology - CRYPTO 2006, LNCS vol. 4117*, pages 570–583. Springer, 2006.

[9] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Journal of the ACM, vol. 51, issue 4*, pages 557–594. ACM, 2004.

[10] R. Canetti, R. Rivest, M. Sudan, L. Trevisan, S. Vadhan, and H. Wee. Amplifying Collision Resistance: A Complexity-Theoretic Treatment. In *Advances in Cryptology - Crypto 2007, LNCS vol. 4622*, pages 264–283, 2007.

[11] J.S. Coron, Y. Dodis, C. Malinaud, and P. Puniya. Merkle-Damgård Revisited: How to Construct a Hash Function. In *Advances in Cryptology – CRYPTO 2005, LNCS vol. 3621*, pages 430–448. Springer, 2005.

[12] I. Damgard. A design principle for hash functions. In *Advances in Cryptology – CRYPTO '89, LNCS vol. 435*, pages 416–427. Springer, 1989.

[13] Y. Dodis, T. Ristenpart, and T. Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In *Advances in Cryptology - EUROCRYPT '09, LNCS vol. 5479*, pages 371–388. Springer, 2009.

[14] M. Fischlin and A. Lehman. Security-Amplifying Combiners for Collision-Resistant Hash Functions. In *Advances in Cryptology - CRYPTO 2007, LNCS vol. 4622*, pages 224–243. Springer, 2007.

[15] M. Fischlin and A. Lehman. Multi-property Preserving Combiners for Hash Functions. In *Theory of Cryptography, LNCS vol. 4948*, pages 375–392. Springer, 2008.

[16] M. Fischlin, A. Lehmann, and K. Pietrzak. Robust Multi-property Combiners for Hash Functions Revisited. In *Automata, Languages and Programming, LNCS vol. 5126*, pages 655–666, 2009.

[17] E. Fleischmann, M. Gorski, and S. Lucks. Some observations on indifferentiability. In *Proceedings of the 15th Australasian conference on Information security and privacy*, ACISP'10, pages 117–134, Berlin, Heidelberg, 2010. Springer-Verlag.

[18] Oded Goldreich. *Computational complexity - a conceptual perspective*. Cambridge University Press, 2008.

[19] S. Halevi and H. Krawczyk. Strengthening Digital Signatures Via Randomized Hashing. In *Advances in Cryptology - CRYPTO 2006, LNCS vol. 4117*, pages 41–59. Springer, 2006.

[20] A. Herzberg. Folklore, practice and theory of robust combiners. In *Journal of Computer Security, vol. 17, issue 2*, pages 159–189. IOS Press, 2009.

[21] J. J. Hoch and A. Shamir. On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak. In *Automata, Languages and Programming, LNCS vol. 5126*, pages 616–630. Springer, 2009.

[22] A. Joux. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. In *Advances in Cryptology – CRYPTO 2004, LNCS vol. 3152*, pages 306–316. Springer, 2004.

[23] J. Kelsey and T. Kohno. Herding Hash Functions and the Nostradamus Attack. In *Advances in Cryptology – EUROCRYPT 2006, LNCS vol. 4004*, pages 183–200. Springer, 2006.

[24] J. Kelsey and B. Schneier. Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work. In *Advances in Cryptology – EUROCRYPT 2005, LNCS vol. 3494*, pages 474–490, 2005.

[25] V. Klima. Tunnels in Hash Functions: MD5 Collisions Within a Minute. Technical report, Cryptology ePrint Archive, Report 2006/105, 2006.

[26] A. Lehmann and S. Tessaro. A modular design for hash functions: Towards making the mix-compress-mix approach practical. In *Advances in Cryptology -*

ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings, pages 364–381, 2009.

[27] M. Liskov. Constructing an ideal hash function from weak ideal compression functions. In *Proceedings of the 13th international conference on Selected areas in cryptography*, SAC'06, pages 358–375, Berlin, Heidelberg, 2007. Springer-Verlag.

[28] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. In *SIAM Journal on Computing*, volume 17, pages 373–386, 1988.

[29] S. Lucks. A failure-friendly design principle for hash functions. In *Proceedings of the 11th international conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'05, pages 474–494, Berlin, Heidelberg, 2005. Springer-Verlag.

[30] U. Maurer, R. Renner, and C. Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In *Theory of Cryptography, LNCS vol. 2951*, pages 21–39. Springer, 2004.

[31] R. Merkle. One way hash functions and DES. In *Advances in Cryptology – CRYPTO '89, LNCS vol. 435*, pages 428–446. Springer, 1989.

[32] M. Mitrengová. Kombinátory hašovacích funkcií. Master's thesis, FMFI UK, Bratislava, 2011.

[33] M. Naor and M. Yung. Universal One-Way Hash Functions and their Cryptographic Applications. In *21st annual ACM Symposium on Theory of Computing*, pages 33–43. ACM, 1989.

[34] NIST Website for SHA-3 Competition. `http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`.

[35] K. Pietrzak. Non-Trivial Black-Box Combiners for Collision-Resistant Hash-Functions don't Exist. In *Advances in Cryptology - EUROCRYPT 2007, LNCS vol. 4515*, pages 23–33. Springer, 2007.

[36] K. Pietrzak. Compression from Collisions, or Why CRHF Combiners Have a Long Output. In *Advances in Cryptology 2008, LNCS vol. 5157*, pages 413–432. Springer, 2008.

[37] T. Ristenpart, H. Shacham, and T. Shrimpton. Careful with composition: Limitations of the indifferentiability framework. In Kenneth G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 487–506. Springer, 2011.

[38] T. Ristenpart and T. Shrimpton. How to build a hash function from any collision-resistant function. In *Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security*, ASIACRYPT'07, pages 147–163, Berlin, Heidelberg, 2007. Springer-Verlag.

[39] M. Rjaško. Properties of Cryptographic Hash Functions. *Cryptology ePrint Archive, Report 2008/527*, 2008.

[40] P. Rogaway. Formalizing Human Ignorance: Collision-Resistant Hashing without the Keys. In *Progress in Cryptology - VIETCRYPT 2006, LNCS vol. 4341*, pages 211–228. Springer, 2006.

[41] P. Rogaway and T. Shrimpton. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In *Fast Software Encryption, LNCS vol. 3017*, pages 371–388. Springer, 2004.

[42] D. R. Simon. Finding Collisions on a One-Way Street: Can secure hash functions be based on general assumptions? In *Advances in Cryptology - EUROCRYPT'98, LNCS vol. 1403*, pages 334–345. Springer, 1998.

[43] X. Wang, Y. L. Yin, and H. Yu. Finding Collisions in the Full SHA-1. In *Advances in Cryptology – CRYPTO 2005, LNCS vol. 3621*, pages 17–36, 2005.

[44] X. Wang and H. Yu. How to Break MD5 and Other Hash Functions. In *Advances in Cryptology - EUROCRYPT 2005, LNCS vol. 3494*, pages 19–35, 2005.

[45] H. Yu, G. Wang, G. Zhang, and X. Wang. The Second-Preimage Attack on MD4. In *Cryptology and Network Security, LNCS vol. 3810*, pages 1–12, 2005.

4 Zoznam publikovaných prác autora so vzťahom ku skúmanej problematike

[1] M. Rjaško. On existence of robust combiners for cryptographic hash functions. In *ITAT 2009 Information Technologies - Applications and Theory, Seňa : PONT*, pages 71–76, 2009.

[2] M. Rjaško. Combining properties of cryptographic hash functions. Technical report, Cryptology ePrint Archive, Report 2010/524, 2010.

[3] M. Rjaško. Black-box Property of Cryptographic Hash Functions. In *Foundations and Practice of Security, LNCS vol. 6888*, pages 181–194. Springer, 2012.

Summary

Cryptographic hash functions are used in many different areas in cryptography: digital signatures, password protection, message authentication, etc. Each application of cryptographic hash function has its own expectations on the hash function. This leads to a large number of various properties which cryptographic hash functions should satisfy.

The thesis gives a general description of cryptographic hash functions including their properties. The main results are impossibility results regarding output length of robust combiners, some novel constructions which combines several properties together, analysis of a black-box property of cryptographic hash functions, it's relationship to a pseudo-random oracle property, and proof of equivalence between the pseudo-random oracle property and it's variant with public images.