Справка за оригиналните научни приноси

на ас. д-р Тодорка Александрова

в трудовете, представени за участие в конкурс за доцент по професионално направление 4.6. Информатика и компютърни науки, научна специалност „Информатика“ (Взаимодействие човек – компютър), обявен в ДВ, бр.52/02.07.2019г.

Общият списък на научните публикации на кандидата съдържа 51 заглавия. За участие в конкурса са представени 22 научни публикации, номерирани от 1 до 22 в списъка на научните публикации за участие в конкурса, като настоящата справка използва същата номерация на публикациите. Статиите са излезли от печат през 2010 - 2016 г. след придобиване на образователна и научна степен „доктор“. Нито една от статиите за участие в настоящия конкурс не е участвала в предишни процедури.

Представените за участие в конкурса статии са публикувани както следва:

- в научни списания с импакт фактор (IF): статии 1, 2, 16 (три);
- в научни списания с импакт ранг (SJR): статии 9, 11, 12, 13, 15 (пет);
- в материали на конференции, реферирани и индексирани в Scopus: статии 3, 4, 5, 6, 7, 8, 10, 17, 18, 19, 21, 22 (дванадесет);
- в материали на конференции, реферирани и индексирани в ACM Digital Library: статии 14, 20 (две).

Общият импакт фактор (IF) на представените за участие в конкурса трудове е 3.457, а импакт ранг (SJR) е 1.063. Общият брой цитирания, индексирани в Scopus, на всички статии за участие в конкурса към 16.08.2019г. е 161 (без автоцитати), а 20 са цитиранията (без автоцитати), представени за участие в конкурса, като всички от тях са индексирани в Scopus.

Представените за участие в конкурса публикации могат да се разделят по тематика в следните три групи:

I. **Насърчаване на човешкото поведение чрез подобряване на реалния свят с помощта на информационни технологии/Navigating human behavior by enhancing the real world with information technologies**

II. **Използване на краудсорсинг за търсене и обмен на знания/Using crowdsourcing for knowledge search and exchange**

III. **Приложения на схеми за разпределяне на тайната/Secret sharing schemes' applications**

I. **Насърчаване на човешкото поведение чрез подобряване на реалния свят с помощта на информационни технологии**

Статиите в тази група са 1, 2, 3, 4, 7, 8, 9, 11, 12, 13, 14, 15, 17 от списъка на научните публикации за участие в конкурса.

Съвременните информационни технологии драматично променят ежедневието на хората. По-конкретно, повсеместните компютърни технологии и социалните медии предлагат различни нови възможности за подобряване на начина и качеството на живот. Когато се прилагат информационни технологии в подкрепа на ежедневните дейности, не е достатъчно да бъдат взети предвид само функционалните аспекти на използваните технологии, но трябва да бъдат добре обмислени начини за поддържане на човешкото благополучие (well-being), което включва пет фактора, необходими за просперитета на хората: положителни емоциии, ангажираност, взаимоотношения, смисъл и постижения. Целта на нашите изследвания е да насочим хората към благополучие и да повлияем на техните емоции и поведение, обогатявайки значението на реалния свят и подобрявайки го с помощта на информационни технологии като игри, виртуални форми, виртуални герои и геймификация/игровизация (gamification).

За да осъществим тази цел, разработваме два примера/казуса, които илюстрират и анализират използването на тези похвати, а именно включването на виртуални обекти в реалния свят. Единият е допълнената компютърна игра с колекционерси карти, наречена Augmented Trading Card Game, а другият е платформата за мобилен краудосрсинг, наречена Micro-Crowdfunding, която цели да мотивира хората да участват в постигането на устойчиво общество (sustainable society), като допринасят в поддържането на обществените блага.

Заобикалящите ни интелигентни технологии (Ambient intelligence technologies) правят ежедневието ни все по-виртуално, което води до постепенното размиване на границата между реалния и виртуалния свят. Компютърните игри често се играят в интернет, което позволява на хората да се наслаждават на игра с други хора, дори когато те самите не се намират на едно и също място. Trading Card Game (TCG) е популярна и извън Япония игра с колекционерски Yu-Gi-Oh! карти и има две версии: настолна и компютърна. Компютърната версия на TCG позволява да се играе дистанционно и има редица подобрения, като например визуализация на въображаеми ефекти върху виртуалните карти. Въпреки това много играчи все още предпочитат настолната версия на Trading Card Game (TCG) пред компютърната, тъй като комптърната не успява да замести пълноценно някои от характеристиките на настолната, като например удоволствието от колекционирането и попълването на тестета от Yu-Gi-Oh! карти, усещането за допир на хартиените карти, размяната на хартиени карти или комуникацията с реален опонент и

други. В публикации [1] и [7] се анализират двете версии на Trading Card Game (TCG) и се обсъжда изгубеното чувство за реалност и удоволствие при игра на компютърната версия на TCG в сравнение с настолната. Твърдим, че компютърните технологии могат да разрешат проблемите, причинени от виртуалността в дадена игра, като се използват техники на допълнена реалност (augmented reality). Като пример за това предлагаме Augmented Trading Card Game (Augmented TCG), в която играчите могат да използват колекциите си от хартиени карти, които да бъдат допълнени с виртуална информация. За да се изследват по-нататъшни перспективи относно влиянието на виртуалността в TCG, са проведени и анализирани експерименти с Augmented Trading Card Game, в които истинският противник е заменен с виртуален играч. Резултатите показват, че усещането за реалност е от съществено значение за успеха при използването на интегрирана виртуалност. Изследвани са потенциалните трудности, които се появяват като резултат от добавянето на виртуалност в TCG чрез анализ на базата на сценарии, фокусирани върху личността на играча. Тъй като играчите с различни личности се фокусират върху различни функционалности и се наслаждават на различни аспекти на играта, е важно да се анализират ефектите от различните реализации на играта върху различни личности. Описаният в статиите анализ, базиран на личността на играчите, е полезен за анализиране на човешките социални взаимоотношения в различни игри и социални медии, както и за изясняване на възможните причини за неудовлетворение при използване на социални медии и игра на компютърни игри за различните типове личност.

Напоследък някои игрови концепции могат да бъдат приложени при обогатяването на реалния свят, като от изключителна важност е да се изследва влиянието на виртуалността, въведена чрез игрите. Тъй като бъдещото социално взаимодействие ще включва виртуалност, основана на различни игрови концепции, описаните в статиите идеи ще бъдат полезни за успешното разработването на бъдещи игрови социални взаимодействия.

Статии [9] и [12] представят разработената от нас Augmented Trading Card Game, в която дистанционната компютърна игра с колекционерски карти Yu-Gi-Oh! Trading Card Game (TCG) е подобрена чрез добавянето на емпатични виртуални герои, добре познати от фантастичните истории на популярни анимации и игри. Виртулните герои са използвани да представят противниковия играч в играта, като действията и поведението им е синхронизирано с поведението на реалния противник, както и да насърчават и окуражават играчите в играта за победа. Описани са наблюдения за начина, по който играчите използват системата, реализираща играта, както и техните впечатления за системата на базата на проведените експерименти. В публикация [8] тези изследвания са доразширени и експериментите показват, че използването на добре познати виртуални герои е обещаващ подход за въздействие върху отношението и поведението на играчите, тъй като такива герои провокират по-лесно емпатията в хората и за тях също така е

лесно да си спомнят лайтмотива на техните фантастични истории. Така положителните елементи и идеологии в историите на героите водят до увеличаване на позивитизма в самите играчите, както и до положителни промени в поведението и отношението им.

В Япония е популярно да се използват известни виртуални герои от анимации и игри в различни сфери, като това е основна дейност на някои бизнес компании. В реалния свят ежедневието се състои от различни социални дейности, а виртуалните герои предлагат възможност за подобряване и обогатяване на тези дейности. Например, настоящите социални дейности могат да бъдат игровизирани чрез заместване на непознатите хора в тях с любимите ни виртуални герои и по този начин да бъдат обогатени с техните истории. Получените резултати са изключително полезни при обмислянето на възможностите за използването на емпатични виртуални герои в дейности от реалния свят за бъдещи информационни услуги. Работите обсъждат начина, по който предложеният подход може да бъде разширен, за да бъде създаден нов тип трансмедийно разказване (transmedia storytelling), като разглеждаме Augmented Trading Card Game като една от формите на трансмедийното разказване.

Виртуализацията на реалния свят чрез включването на различни изчислителни устройства в заобикалящата ни среда има много предимства и позволява използването на аспекти като геймификация с цел насърчаването на мотивацията на потребителите в ежедневието, но все още остава предизвикателството как „успешно“ и „хармонично“ да бъде проектиран виртуализирания реален свят.

В статия [17] са разгледани три примера/казуса и въз основа на опита от експериментите с тях са предложени идеи за това как да бъде запазена или възстановена реалността във виртуализирания реален свят, тъй като в противен случай потребителят може да не успее да намери правилната семантика на средата и да загуби усет за това как да се държи и реагира в съответната среда. Дискусията в статията е много важна за обсъждане на дизайна на бъдещите кибер-физически системи.

Компютърните технологии позволяват да подобрим и направим по-ценни предметите от ежедневието, като добавим виртуални форми към тях. Виртуалните форми представляват динамично генерирани визуални образи, съдържащи информация, която влияе на поведението и мисленето на потребителя и обикновено се реализират чрез добавяне на дисплей, който показва визуални изрази или чрез проектиране на информация върху предметите. В [13] и [15] са представени примери, които илюстрират добавянето на виртуални форми към съществуващи обекти. Първият пример е Virtual Aquarium, който предлага виртуален аквариум, отразяващ процеса на миене на зъбите на потребителя с цел стимулиране на правилния начин на миене и насърчаване към здравословен начин на живот. Вторият казус е Augmented Go, който проектира допълнителна информация

върху игралната дъска на Go, подпомагайки по-добрите игрови ходове на играча. Третият случай е Augmented Trading Card Game, който добавя виртуални герои и специални ефекти към картите на играта с цел да насърчи и провокира по-социална игра. На базата на опита ни с трите примера, които подобряват традиционните обекти с виртуални форми, извличаме шест ценности/стойности (values), които играят важна роля в проектирането и създаването на виртуални форми, подобряващи традиционни предмети. Тези шест стойности са: естетична (aestheetic value), като важен фактор за привлекателността и красотата на ежедневните предмети; емпатична (empathic value), която провокира емпатията в потребителите; убеждаваща (persuasive value), която предлага външна мотивация (extrinsic motivation) на потребителите с цел промяна на тяхното поведение и отношение; инфомативна (informative value), която предлага допълнителна информация и помага взимането на по-добри решения; икономическа (economic value), която представя желанието на потребителя да закупи/размени/спечели допълнителни ефекти или атрибути и идеологическа (ideological value), представляваща метафората, която показва например мечтите, убежденията или очакванията на потребителя. Описаните стойности са полезни първо за идентифициране на основните стойности на традиционните обекти и второ за това как да бъдат добавени допълнителни стойности към обектите, за да да бъдат обогатени и направени по-приятни и ценни за потребителите. Вярваме, че тези стойности биха били полезни при подобряването на каквито и да било обекти с виртуални форми.

Статия [2] е продължение и обобщение на предишните статии и цели да бъдат разработени интелигентни артефакти, подсилени с виртуални форми, които да влияят на човешкото поведение. За да предложим подходящи начини за разработване на такива артефакти, които хармонично да интегрират виртуални форми, въз основа на опита с описаните три казуса, предлагаме основана на шестте ценности концептуална рамка за анализ (value-based analysis framework), която позволява да обсъдим и разгледаме някои правилни подходи за дизайн на подобрени интелигентни артефакти. Резултатът от експериментите показва, че включването на фантастични елементи е обещаваща посока за създаване на интелигентни артефакти с идеологически послания, които да влияят на отношението и поведението на хората.

Съвременните технологии позволяват да бъдат геймифицирани (gamify) ежедневните дейности, като се вграждат компютри в заобикалящата ни среда. В [11] е предложена базирана на ценности концептуална рамка за геймификация (value-based gamification framework), която цели увеличаването на вътрешната мотивация в ежедневието. Като пример е показано използването на тези ценности в създаването на Augmented Trading Card.

Статии [3] и [4] предлагат нов подход за мотивиране на хората да участват в постигането

на устойчиво общество. Методът се нарича Micro-Crowdfunding и насърчава хората, живеещи в градовете, да подкрепят и допринесат за устойчивостта на малки общи блага, като обществени мивки, тоалетни, рафтове, офис площи и други. Micro-Crowdfunding се основава на концепцията за краудфъндинг (crowdfunding) и използва идеята за местна валута (local currency) като инструменти на социалния механизъм, за да повиши информираността на хората за това как да участват в поддържането на устойчивостта на общите блага. Предложеният подход има за цел да поддържа устойчивостта на общите ресурси с малки усилия от страна на хората. При този подход организаторът въвежда нова мисия за поддържане на устойчивостта на даден ресурс и инвеститорите го финансират. В резултат, изпълнителят довежда докрай мисията с минимални усилия, постигайки устойчивост на ресурса. Описани са експериментални резултати от системата, които показват как икономическият и социален фактор влияят върху поведението и отношението на индивида и общността. Изследването би било полезно и при проектирането на други социални медии, основани на краудфъндинг, когато се разглежда баланса между използването на икономически и социални стимули.

Публикация [14] предлага нов подход в технологиите за убеждаващо въздействие (persuasive technology), основан на взаимодействието между деца и родители, който е имплементиран в приложение за мобилни устройства. Целта на подхода е да подпомогне проблема с потреблението на природни ресурси, не само чрез повишаване на информираността, но и чрез насърчаване на информирани решения относно тяхното използване. Проведено е проучване, за да се види кои природни ресурси са по-важни за японското общество и е създаден атрактивен мултимедиен инструмент, като се има предвид семейното взаимодействие, което използва еко-визуализации, разказ и герои от анимационни филми. При успех, по този начин може да бъде постигната по-добре информирана консумация на храна и други природни ресурси, засилвайки положителните нагласи в семейството.

II. **Използване на краудорсинг за търсене и обмен на знания**

Статиите в тази група са 5, 6, 16, 18, 19, 20 от списъка на научните публикации за участие в конкурса.

Краудсорсингът се превръща в популярен и успешен подход за решаване на задачи, свързани с търсене и споделяне на знания и информация, тъй като все още съществуват голям брой задачи от този тип, с които настоящите компютри и машинни алгоритми не могат да се справят толкова добре колкото самите хора. По-голяма част от съществуващите краудсорсинг системи не успяват да се адаптират към мобилния контекст, където потребителите изискват лесен начин на въвеждане на задачи и очакват бърза/незабавна реакция и отговор. Освен това повечето съществуващите системи използват модела за платен краудсорсинг, което означава, че възложителите трябва да плащат определена

сума пари на работниците, които извършват задачите, за да изпълнят всяка задача. В нашите изследвания твърдим, че за някои видове задачи съществуващите платформи за социални медии могат да осигурят безплатен набор от работници, които да участват в създаването, търсенето и предоставянето на знания при поискване в реално време.

Освен това, със зараждането на идеята за повсеместните изчисления (ubiquitos computing/ UbiComp) едно от ключовите предизвикателства е как да бъде извлечена контекстна информация от физическата среда. Без подобна информация, UbiComp приложенията не могат да предоставят истински контекстно ориентирани услуги. Обичайният подход е използването на сензори и сензорни мрежи. Капацитетът на тези машинни сензори обаче все още е ограничен до събиране на физически данни на ниско ниво, като например скорост, температура и налягане, но за приложенията, които са контекстно ориентирани, е важно да има информация от по-високо ниво, като например локални знания, човешка дейност, социална среда, групови емоции на маса хора, състояние на неелекронни обекти и т.н. Освен това, тези знания често са чувствителни във времето, което означава, че много трудно могат да бъдат използвани повторно и стойността им намалява с течение на времето. В нашите изследвания разглеждаме възможността хората, използващи съществуващи социални медийни услуги, да бъдат използвани като сензори (Human as Sensors) за извличане на информация, която е чувствителна спрямо времето и мястото с помощта на преносими устройства. Използвайки такъв подход, системата може да събира информация, която е трудно (ако не и невъзможно) да се получи от машинни сензори, като по този начин предлага възможност за генериране на по-богат контекстуален модел.

В статии [16], [19], [20] е представена мобилна краудсорсинг платформа, наречена UbiAsk, която е изградена върху социални медии и предлага в реално време социално/културно търсене и превод на чужденци в Япония, които срещат затруднения в използването, четенето и писането на йероглифи и поради тази причине не могат да използват джобни речници или онлайн услуги за превод, за да разберат менюта, карти, знаци и друга важна информация, тъй като не могат да въведат текста, който виждат. Решенията на базата на оптично разпознаване на символи предлагат много ограничени възможности в реални ситуации (т.е. сложен фон, тъмна среда, замъглени снимки, нестандартни шрифтове, размер или формати) и в случай на сложни писмени символи като йероглифи. С помощта на местните хора (local crowd), използвайки социални медии, приложението UbiAsk помага на чуждестранни посетители в Япония, като отговаря своевременно на техните въпроси, базирани на изображения. Голям брой хора, използващи мобилни терминали, участват доброволно в разпознаване на изображения и отговор на конкретни въпроси, и превод, свързани с тях. В сравнение с чисто техническите решения, подходът за използването на хора за извършване на такива дейности позволява не само чист превод, но и предоставянето на контекстна и нетекстова информация и по този начин

предоставянето на информация от по-високо ниво на крайния потребител. Резултатите от експериментите показват, че именно такива контекстни знания са от много по-голям интерес за потребителите в сравнение с чист превод на текст и могат да бъдат получени от хора много по-ефективно, отколкото чрез настоящите машинни алгоритми. Описани са и резултати от проведен контролиран експеримент с приложението в продължение на 6 седмици с 55 участника. На базата на този експеримент е установено, че мобилният краудсорсинг модел демонстрира надеждна ефективност по отношение на скоростта на отговаряне и количеството на отговорите за даден въпрос: на половината от запитванията е отговорено в рамките на 10 минути, на 75% от запитванията е отговорено в рамките на 30 минути, а на всяко запитване е имало средно по 4,2 отговора. По-конкретно в следобедните часове, вечер и през нощта, почти 88% от запитванията са получили отговор в рамките на 10 минути и средно с повече от 4 отговора на запитване. Допълнително са изследвани видовете информация, която е интересна за потребителите и възможните нематериални стимули за локалните експерти, за да участват активно в платформата като геймификация и социални стимули. По отношение на мотивацията за участие от страна на локалните експерти, които са отговаряли на запитванията, е установено, че най-активно отговарящите хора са били подтикнати да участват предимно от вътрешни мотиви, а не от проектираните външните стимули, като геймификация и социални стимули.

Статия [18] изследва специално възможностите за прилагане на геймификация при проектирането на интелигентни среди с цел подобряването на цялостната ангажираност на потребителите. За да бъде разбрана по-добре ефективността на игровизирането на интелигентните системи са представени два примера: мобилното краудсорсинг приложение UbiAsk; и приложение с насърчаващо въздействие, което мотивира потребителите да участват в намаляването на емисиите на въглероден двуокис, наречено EcoIsland. На базата на експериментите с приложенията е установено, че за да бъдат ефективни игровите стимули, те трябва да бъдат създадени много внимателно: дизайнерите трябва да са наясно, че основните функционалности на системата имат много по-голямо въздействие от допълнителните игрални компоненти, а желаното потребителско поведение изисква цялостен игрови опит, който е подкрепен не само от игрова структура (“game structure”), но и от игрова визия (“game-look”). След публикуването си статията има висок брой цитирания и е популярна в областта на геймификацията.

Статия [6] представя възможността хората да бъдат използвани като най-подходящите сензори за извличане на контекстна информация, която е чувствителна спрямо времето и мястото. Работата описва предложената услуга MoboQ, внедрена в Китай, за отговор на социални/обществени въпроси в реално време, базирани на местоположение. Използвайки MoboQ, хората могат да задават времеви или гео-чувствителни въпроси, като

например колко време се чака на опашка в момента за даден популярен бизнес и след това да получат отговор от други потребители, които се намират на същото място в момента. За да получи отговори на въпросите, системата анализира на живо потока от обществената микроблог услуга Sina Weibo, за да идентифицира хората, които най-вероятно в момента са на мястото, асоциирано с въпроса, и им изпраща въпроса чрез услугата микроблог, в която са били идентифицирани. MoboQ е внедрена в Китай от началото на 2012 г. до октомври същата година, като е използвана за задаване на 15 224 въпроса от 35 214 регистрирани потребители и е събрала 29 491 отговора; 74.6% от въпросите са получили поне един отговор, 28% са получили първи отговор в рамките на 10 минути, а 51% от въпросите са получили първи отговор в рамките на 20 минути. Като цяло 91% от въпросите успешно са намерили поне един отговор като те са изпратени до 162,954 микроблог потребители. Анализират се моделите на използване и поведението на крайните потребители в реалния свят, обсъжда се натрупания опит и се очертават бъдещите направления и възможните бъдещи приложения, които могат да бъдат направени на базата на MoboQ. Доказва се, че използването на хората като сензори за такава информация е много по-ефективно от използването на платформи, които се базират само на машинни алгоритми.

Като допълнително изследване в статия [5] е разгледан проблемът за намаляването на възможността за споделяне на информация между различните типове хора с развитието на Web 2.0, което прави проектирането на системи, които да подпомогнат информационният поток сред различни обществени групи с различни мнения или вкусове сериозно предизвикателство за дигиталните дизайнери. В статията е представено текущо проучване за изследване на система, базирана на тълпи (crowd), за улесняване на естествения информационен поток сред различни типове хора. Проведено е проучване от типа Wizard-of-OZ, в което хората получават неочаквани и непоискани мнения и препоръки от други хора, което цели да разбере как реагират участниците при получаване на неочаквана информация. Въз основа на констатациите, е създадено и внедрено уеб приложение за насърчаване на различни типове хора да обменят информация по метода всеки с всеки (peer-to-peer).

III. **Приложения на схеми за разпределяне на тайната**

Статиите в тази група са 10, 21, 22 от списъка на научните публикации за участие в конкурса. Тези работи представят няколко приложения на схеми за разпределяне на тайната и са продължение на изследванията от дисертацията ми, в която са изследвани теоритично прагови схеми за разпределяне на тайната.

Схемите за разпределяне на тайната (secret sharing schemes) са важен инструмент в съвременната сигурност на информацията и имат голямо приложение в областта на компю-

търните мрежи. Те са метод за разделяне на тайна s на n части, наречени тайни части, и разпределянето им между n потребители по такъв начин, че само определени квалифицирани подмножества от потребители могат да възстановят тайната, като комбинират своите тайни части.

Реализирането на анонимност в съвременните Peer-to-Peer (P2P) мрежите е важен проблем. Статии [10] и [21] предлагат методи за реализиране на анонимност в P2P мрежи, използвайки схеми за разпределяне на тайните.

В статия [21] е предложен двустранно анонимен (mutually anonymous) протокол за децентрализирани Peer-to-Peer (P2P) мрежи, който реализа анонимността на инициатора и на респондента, както и на тяхната комуникация. Протоколът е комбинация между двустранно анонимен протокол, базиран на схеми за разпределяне на тайната, наречен Secret-Sharing-Based Mutual Anonymity Protocol (SSMP), и техника за „нарязване“ на информацията, наречена information slicing technique. Използването на концепцията на схемите за разпределяне на тайната играе съществена роля за реализирането на анонимността и защитата на предаваната информация между инициатора и респондента. Използването на техниката за нарязване на информация осигурява устойчивостта на протокола към динамично присъединяване и напускане на пиъри, както и позволява той да бъде реализиран без използването на инфраструктура на публичен ключ (PKI), т.е. с по-ниски криптографски разходи. Направена е оценка на анонимността на P2P системата от вероятностна гледна точка. Резултатите показват, че предложеният двустранно анонимен протокол осигурява по-добра анонимност от предложените до сега методи.

Устойчивостта на Peer-to-Peer (P2P) мрежите към неспособността на дадени върхове от мрежата да изпълняват задълженията си за кодиране и/или препращане на информацията (churn resielnce) поради динамичното присъединяване/напускане на мрежата от пиъри с или без предупреждение, мрежови/хардуерни грешки или целенасочено злонамерено действие на противник, което води до загуба, корупция, дублиране на съобщения, е важен проблем за съвременните мрежи. Статия [10] подобрява вече съществуващ дизайн на анонимна P2P мрежа, правейки я устойчива в описания по-горе смисъл. Това се постига чрез използване на свойствата на праговите схеми за разпределяне на тайната.

В статия [22] е описано приложение на схемите за разпределяне на тайната за постигането на сигурността на изображения. Предложен е метод за реализиране на (t, n) схема за разпределяне на тайни изображения. Предложеният алгоритъм за разпределяне на тайни изображения се реализира чрез прилагане на схеми за разпределяне на множество тайни (multi-secret sharing schemes), базирани на еднопосочни функции на две променливи (two-variable one-way functions) и схемите на Шамир за разпределяне на тайната. В предложените схеми при възстановяване на тайните изображения участниците трябва

да обединят само своите псевдо-тайни части, вместо да разкриват истинските си тайни части. По този начин всеки участник може да участва в разпределянето на множество тайни изображения, като притежава само една тайна част. Освен това дължината на всяка тайна част не зависи от размера на тайното изображение и това е важно свойство за по-нататъшния процес на разпределяне на изображението. Предложеният метод е схема за многократна употреба, която може да се използва в различни сесии за разпределяне на тайни без да е необходимо преразпределяне на тайните части на участниците. В сравнение с други техники за разпределяне на тайни изображения друго основно предимство на предложения метод е, че той не генерира изображения за тайни части, които са трудни за използване и администриране.

21.08.2019 г. Подпис: .....

/Тодорка Александрова/