PROTECTION OF CARDIOLOGICAL DATA IMPLEMENTED USING CRYPTOGRAPHY METHODS

Miroslav Dechev
miroslav.dechev@gmail.com

Abstract. With the transformation of digital health services and e-health, technologies for protecting patient data are increasingly vulnerable to attacks, unauthorized access, and theft. This article describes the application of cryptography in the protection of cardiology databases. Information security systems in e-health must ensure the implementation of certain requirements included in government regulations to protect health information from attacks, disclosure, unauthorized use, and destruction. The improvement of digital health infrastructure has brought to the forefront modern means of protecting both personal and research data in the healthcare industry, as well as effective interactions between healthcare and patients.
Keywords: digital health, cryptography, information security systems

Въведение.

С трансформацията на цифровите здравни услуги и електронното здравеопазване, технологиите за защита на данните на пациентите са все по-уязвими от атаки, неправемерен достъп и кражби. Тази статия описва приложението на криптографията в защитата на кардиологични бази от данни.

Въпросите относно използването на криптиране остават на дневен ред. През декември 2020 г. Европейската комисия и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност определиха криптирането като ключов метод за защита на индивидуалните права и гарантиране на сигурността на лицата [1].

Системите за информационна сигурност в електронното здравеопазване трябва да осигурят изпълнението на определени изисквания, включени в държавни нормативни документи с цел защита на здравната информация от атаки, разкриване, неправомерно използване и унищожаване.

Стотици са заплахите и все повече сигурността на информацията зависи от добре обезпечената сигурност, освен на потребителите, и на системите в организациите. Киберсигурността се базира на: информационната сигурност, сигурността на приложенията, мрежовата сигурност и сигурността на Интернет, като на стълбове на своя фундамент [2].

Усъвършенставането на дигиталната здравна инфраструктура поствя на преден план съвременните средства за защита, както на личните, така и на изследователските данни в здравната индустрия, също и на ефективните взаимодействия между здравеопазването и пациентите.

Тази статия представя резултатите, свързани с три вида кардио данни: ФПГ, ЕКГ и Холтер записи. Формата на вълната на кардио сигнала, записана от Холтер апарат, е идентична с тази на ЕКГ сигналите, записани с електрокардиограф; разликата е, че Холтер апаратът е проектиран да записва непрекъснати ЕКГ данни (2x10min). Всички данни, върху които се прилагат тестовете, са получени от кардио записи, което е особено важно за реалистичността на резултатите. Предварителна обработка беше приложена към трите вида данни от изследването, която включва намаляване на интерференцията [1], откриване на максималните отклонения в сигналите (QRS комплексите са Q, R, S-характерни точки в ЕКГ сигнала, с максимално отклонение на амплитудата в точката R и локализация на P пика при PPG сигнала [1].

Постоянно развиващите се технологии като роботика, изкуствен интелект, генетика, синтетична биология, нанотехнологиите, триизмерния печат и виртуалната реалност дават все по-голямо отражение върху света ни, но те са придружени и от безброй заплахи за сигурността на информацията. За да бъде гарантирана тя се изисква изграждане на модел за сигурност в една организация [3].

1. Инструменти за защита с Криптография.

Криптографските ключове и дигиталните сертификати са средства, с които нашите данни и използваните технологии следва да са защитени и обезопасени [3]. Често към получените данни се добавя воден знак /алгоритъм за защита на електронни документи използвайки воден знак [8]/, за да се защитят от неоторизиран достъп, преди да се извърши криптография, използвайки подходящо подбран алгоритъм за криптиране.

В [1] е представен и анализиран алгоритъм, който включва защита с помощта на криптография с публичен и симетричен ключ.

Предложеният софтуерен алгоритъм е изпълнен върху реални електрокардиографски, фотоплетизмографски и Холтер кардио данни. Осигуряването на защитата и сигурността на няколко реални сигнала, използвани в ежедневието на хората, от злонамерена намеса, неоторизиран достъп, фалшифициране и сериозни атаки е възможно днес благодарение на създаването на математически базирани софтуерни решения [1].

Техническото обезпечаване и събирането на повече информация води до необходимост от използване на все повече устройства от медицинския персонал, но с бума на мобилните технологии в последните години това препятствие е значително по-лесно за преодоляване [6].

Добрата защита на една информационна система от база здравни данни трябва да бъде и добре управлявана от администраторите на здравни заведения. Специалисти по

проектиране на програмното обезпечаване са задължителни длъжности в изграждането на административната база на лечебните институции.

Осигуряването защитата на информацията започва още с проектирането и изграждането на бъдещата информационна система за защита на кардиологичните данни. Това става с конфигурирането на оборудването и програмното обезпечаване. Важен е анализът на информационните потоци и контрола на взаимната съвместимост. Когато този етап завърши се преминава към разработването на мерките за сигурност [4].

Сигурността на данните трябва да бъде гарантирана при предаване на записана медицинска информация и лични данни. Използването на технология за криптиране е един от най-ефективните начини за поддържане на сигурността на биомедицинските сигнали. Поради тази причина, въпросите, свързани с удостоверяването и поверителността, са заложени на карта в телемедицината, като се гарантира, че само оторизирани потребители имат достъп до медицинските и личните данни на пациентите. В същото време качеството на оригиналните сигнали трябва да бъде запазено до необходимата степен, за да не се нарушат диагностичните свойства на данните [1].

1.1.Криптографски приложения

Използваните методи и процеси в защитната архитектура на моделите за сигурност са: *Криптографията, Автентикацията, Упълномощаването, Проверки, Инфраструктура на публичния ключ, Цифрови сертификати.*

Криптографията е наука за шифриране и дешифриране на данни. Обикновено данните съществуват в своя суров вид и могат да бъдат четени от всеки. Такива данни не са защитени, тъй като хакерите могат да пробият защитата и да ги прочетат. Ако маскирате данните по някакъв начин, който ги прави да изглеждат безсмислени, вие сте ги криптирали успешно [5].

Така нареченият шифрован текст остава неразбираем за хората, които не знаят по какъв начин данните са криптирани. Т.е. декриптирането, превръщането на данните в първоначалния им изглед е механизъм познат само на избрани потребители и би бил труден да бъде проследен от хакери. Криптирането се осъществява посредством математически алгоритъм (шифър), който криптира и декриптира данните.

Конвенционалната криптография използва понятието криптиране със симетричен ключ (symmetric key encryption). При такова криптиране се използва само един ключ както за криптиране, така и за декриптиране на данните. Пример за конвенционална криптография е „Цезаровото писмо”, което използва метода „отместване с три”. При този

метод всяка буква се замества с буквата на трето място в азбуката след заместваната буква [7].

За да декриптирате текста, трябва да използвате същия метод, само че наопаки – отмествате с три букви назад. Съществуват много стандарти за криптиране. Такъв е стандартът за криптиране на данни DES (Data Encryption Standard), който използва многократно по-сложен механизъм. Ако използвате симетрично криптиране, човекът, който ще чете информацията трябва да разполага с ключа за декриптиране. Докато пазите ключовете на сигурно място, обменът на информация между вас е сравнително сигурен [5].

Съществува и криптиране с публичен ключ, което изисква два ключа, наречено асиметрично криптиране. Единият /публичен/ ключ служи за криптиране, а другият /часният/ - за декриптиране на данните. При този метод веднъж изпратената информация вече не може да се прочете от криптиралия я с публичен ключ, а само от получателя с неговия частен ключ, докато при криптирането със симетричен ключ е необходима размяна на един ключ. Анализирайки заплахите и риска задачите относно защитата на данните в информационните системи става все по-сложна. Тя трябва да обхване освен физическото опазване и специализирания софтуер. Криптирането е един от начините за осигуряването на цялостност при предаването на данните.

Смисълът на една шифрова (криптографска) система е преобразуването на някакъв таен текст, така че неговото съдържание да бъде разбираемо само за посветени в тайната хора и неразбираемо за всички останали [7].

Основната цел на криптирания текст е защитата му, невъзможността да бъде разчетен от трето лице, освен от този, който го изпраща и този, който го получава. Криптографските преобразувания се осъществяват по точно определен алгоритъм, като той може да се реализира апаратно/хардуерно/ или изпълнен на универсален компютър, но винаги програмно.

Най-важната разлика между тези два типа е в начинът на съхраняване на ключовете. При апаратното криптиране ключовете се пазят в специално устройство и до тях няма програмен достъп [7].

Под понятието „програмно криптиране” ще разбираме такова криптиране, при което криптиращата последователност се получава, чрез програмни средства, изпълнявани на универсален компютър, а ключовете на криптографската система се пазят върху стандартните му запомнящи устройства [7].

Апаратното криптиране има няколко характеристики, сред които се нареждат сигурното съхранение на ключа, слабата адаптивност, висока цена и променливи параметри на апаратурата. При програмното особеностите са обратни – ниска цена и проблемно съхранение на ключовете. Разликите обуславят и появата на смесени реализации между програмно и апаратно криптиране. Двата основни елемента на процедурите при криптографията са алгоритъмът и ключът. Крипртираният текст трябва да е устойчив на атаките. В този смисъл криптографските алгоритми са от изключително значение.

Криптографският алгоритъм е система от краен брой указания и правила, задаващи реда на изпълнение на елементарни действия над явния и криптирания текст и над ключа с цел ефективно криптографско преобразуване [7].

Последователността от битове, думи или байтове, които потребителят е избрал при използване на криптографската система определя криптографския ключ. Криптографските алгоритми са много и разнообразни според криптографските преобразования. Те могат да бъдат симетрични, поточни, блокови, на публичните ключове, комбинирани, за еднопосочни хеш функции, за електронни подписи, за автентикация на съобщенията, за криптографски протоколи и др.

Автентикацията е процес, при който се използва име на акаунт и парола за идентифициране на потребител [*5*].

Типовете на автентикация са различни. Могат да се използват пароли и потребитески имена или биометрични данни. Упълномощаването представлява най-общо оторизирането на потебителите за достъп и дава определени права на използване на системата.Проверките на потребителите изискват записването им в системата и тяхното проследяване.

Инфраструктура на публичния ключ е сбор от технологии и средства, чрез която се постига сигурна комуникация. Отговаря за проверка на поверителността и автентичността на информацията, обменяна между две точки. Инфраструктурата на публичния ключ използва следните три криптографски технологии за генериране на компонентите на сигурността: шифри на симетричните ключове, шифри на асиметричните ключове, еднопосочни хеш-функции [5].

Целта тук е след създаването на акаунта и паролата хеш-функцията да ги криптира и запише. При всяко влизане в системата хеш-функциите сравняват криптираната парола и чак тогава се осигурява достъп в системата за потребителя. Цифрови сертификати се

базират на уникален цифров подпис. Автенчтичността на потребителя се установява след неговия електронен подпис /отпечатък/.

Голяма част от данните не са криптирани или са зле защитени. Публикувано през юли 2014 г. проучване на „Хюлет Пакард" установява, че 90% от устройствата, свързани с интернет, събират лични данни, 70% от които се изпращат без никаква форма на криптиране [3].

Естествено некриптираните данни са изложени на риска да бъдат разбрани или прочетени от всеки, за който са достъпни. Особено опасно е когато здравна институция или финансова компания не криптира данните за платежните документи на клиентите си, което за хакерите е благодатна почва за източване на лична информация, а чрез нея и средства. Такъв е случаят с компанията „Хоум депо", от която хакери извлекли номерата на кредитни карти на 55 милиона клиенти. Google, например, обръща внимание на това и все повече криптира кореспонденцията между потребителите и сървърите си.

Съвременните компютърни операционни системи притежават безплатни вградени инструменти за криптиране на твърдия диск, само че те не са включени по подразбиране и много малка част от потребителите ги използват. Всъщност повечето клиенти дори не подозират за съществуването на тези протоколи за сигурност [3].

Емблематичен за предизвикателствата, пред които сме изправени, е големият пропуск в протоколите за криптиране, открит още в началото на 2014 г., известен с името „Хартблийд" [3].

Както стана ясно по-горе криптографските алгоритми се използват за кодиране и декодиране на изпращаната информация. Един от най-използваните протоколи за криптиране са Secure Sockets Layer/SSL/ и Transport Layer Security/TLS/.

Една от версиите на SSL, така наречения „отворен" SSL, отговаря за защитата на над две трети от трафика в интернет [3].

Безспорно една от защитите при електронното общуване е идентификацията. Хилядите измами с документи, фалшиви самоличности, пари, паспорти и визи са неоспоримо доказателство, че проблемите в тази област на защита са много сериозни и налице. Често банковата институция например не може да установи, че лицето, което тегли пари, прехвърля по сметки или извършва транзакции е нейн клиент, най-малкото защото по електронен път той няма как да бъде разпознат като такъв, ако не представи необходимата идентификация. С технологичния напредък все по-често започват да се използват образите, гласовете и отпечатъците, паролите и електронните сертификати.

Идентификацията често се извършва с криптографски подходи. При обмен на криптирани съобщения основният идентификатор е притежаването на необходимия ключ [7].

Паролите са най-често използваното средство за идентификация. Изборът на пароли често е съобразен с личното усещане на потребителя, което определя и сигурността. Доказано е, че потребителите избират пароли, които са близки до личността им символи или психологически усещания, което понякога крие риск от разкриваемостта им. Слабо място се оказва и съхраняването на паролата, тъй като уязвимите места в Интернет пространството постоянно се променят и нарастват. Друг е моментът, че въведени в дадена система те задължително са криптирани и могат да бъдат изисквани от потребителите при тяхното евентуално забравяне. Други възможности за идентификация са електронния подпис, който е автентичен и категорично доказва подписания документ от изпращача и автентификацията на файловете и съобщенията, която дава възможност получателят да е сигурен, че получва оригиналния документ и като цяло оригиналната информация.

За изработването на код за автентичност се използват така наречените хеш функции, които са клас от еднопосочни функции [7].

Това са функции, които на входа си получават низ с произволна дължина, от когото на изхода си изграждат низ с постонна такава. Хубаво е винаги криптирането да е допълнено от автентифициране, което прави добре защитена една криптографска система.

1.2. Гарантиране на защитата на информационни системи в здравеопазването с криптиране.

При внедряването на информационни системи в здравните администрации и услуги е необходимо да се гарантира надеждност, безопасност и сигурност.

Прилагането на криптографски алгоритми, независимо от конкретния метод на внедряване (публичен ключ, секретен ключ или хибридни алгоритми), е много важно за сигурността на предаваната информация. Използването на протоколи за обмен на ключове, цифрови подписи и вграждане на воден знак са ефективни инструменти за защита на данни, сигнали и изображения. Изборът на най-подходящия алгоритъм за криптиране играе съществена роля в процеса на проектиране на схемата за защита на предаваната информация [1].

1.3. Математически метод в процеса на криптиране.

Често използван математически метод за процеса на криптиране е криптографията с елиптични криви, подход за осигуряване на криптиране с публичен ключ, който се основава на алгебричната структура на елиптични криви върху крайни полета [1]. Използването на криптография в биомедицински приложения е метод, който гарантира поверителността на медицинските данни на лицата. Методът, който представя това изследване за прилагане на криптография за защита на видовете кардиологични данни обхваща данните: ЕКГ, фотоплетизмографски сигнал (ФПГ) и Холтер. Процедурата за криптиране се извършва след компресиране на изследваните данни и извършване на вейвлет трансформация (ВТ) върху получената последователност.

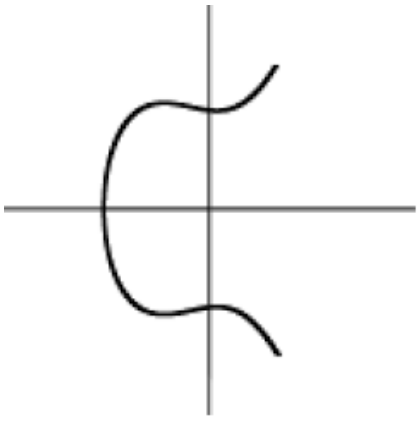
Алгоритъмът за криптиране е приложен въз основа на реални кардиологични данни от ЕКГ и FIG сигнали, получени чрез PPG устройство, позволяващо едновременно записване на два PPG сигнала и един ЕКГ сигнал. Паралелно е извършен Холтер запис, с помощта на устройство за Холтер мониторинг, поставено върху изследваното лице. Холтерът може непрекъснато да записва сърдечни данни до 72 часа [1].

Проективно пространство и елиптични криви Дефиниция:

Нека *F* е поле. Елиптична крива *E(F)* над *F* (зададена с уравнение на Вайерщрас в обобщена форма) наричаме съвкупността от всички точки (*x, y)* на равнина *F2* , които удовлетворяват:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{F},$$

и една специална точка O, наричана безкрайна точка [10].



Фиг. 1. Elliptic Curves Calculator /приложение/

Предложената процедура за криптиране има за цел да осигури добра защита на трите вида кардио сигнали при създаване на архив от използваните ЕКГ, ФПГ и Холтер записи, получени при изследване на кардио записи от пациенти с различни сърдечно-съдови

заболявания и здрава контролна група. Създаденият алгоритъм е реализиран софтуерно в среда за програмиране на Microsoft Visual C++ като стандартно софтуерно приложение [1].

Извършени са математически анализи на проведените изследвания и са определени характеристики за оценка.

Това изследване анализира ефективността на отделните стъпки при прилагането на приложената процедура за защита на кардиологични данни (използвайки параметри за оценка на ефективността на използваните в процедурата алгоритми) и сравнява стойностите на параметрите на изходния сигнал с тези на входния сигнал за всичките три типа кардио данни.

2. Методи за защита на кардиологични данни.

Предимството на защитата на кардио сигналите е, че те са относително по-малко податливи на измами поради уникалния си характер. От друга страна, ЕКГ и ФПГ сензорите генерират постоянно голям брой отчети, които трябва да се обработват в реално време.

Електрокардиографията и фотоплетизмографията са съвременни, несложни инструменти за изучаване на здравословното състояние на субектите, предоставящи информация за състоянието на сърдечно-съдовата система, активността на автономната нервна система и други.

2.1. Процедура за защита на кардио данни.

Математически базираният метод за защита на кардио данни, предложен и изследван в тази статия, се състои от някои от следните стъпки: На първо място: *Прилагане на дискретна трансформация; Прилагане на оптимизирана компресия, базирана на ефективност на енергийното опаковане, на получената последователност; Вграждане на воден знак в редуцираните WT коефициенти; Процедура за криптиране с помощта на хибриден криптографски алгоритъм; Прилагане на обратна дискретна уейвлет трансформация на получената последователност; Определяне на изследваните параметри за оценка на използваните алгоритми.*

2.2. Стъпки на математически базиран метод за защита на кардио данни.

Прилагане на дискретна трансформация;

Дискретизацията/квантизацията често е ключова стъпка когато искаме да приложим **дискретни** (integer-valued) механизми за поверителност (напр. *geometric/discrete Laplace*, *discrete Gaussian*), или когато комбинираме

диференциална поверителност (DP) с криптография (HE/SMPC) или федеративно обучение.

Неправилна оценка води до липса на реална защита или ненужно голям шум, за това е необходимо измерване с точност чувствителността на определяне на шума. Не е уместно неограничено комбиниране на множество DP-операции без privacy accounting — записа на ε сумарно расте (composition). Използва се advanced composition или moments accountant. Запазването на клинична валидност и тестване дали важни клинични открития (напр. детекция на аритмия) оцеляват след защита е задължителна стъпка. Нужно е документиране [11].

Прилагане на оптимизирана компресия, базирана на ефективност на енергийното опаковане, на получената последователност;

Разработването на метода за компресия и защита на кардиологични сигнали (напр. ЕКГ), включва: оптимизирана енергийна трансформация (напр. чрез въллетно, Фурие или дискретно косинусово преобразуване); компресията се управлява според ефективността на опсковане на енергията (energy encapsulation efficiency, EEE) — тоест колко добре основната енергия на сигнала се концентрира в малък брой коефициенти и върху компресираните (дискретни) коефициенти се прилага математически метод за защита — например дискретен механизъм на диференциална поверителност (geometric или discrete Gaussian).

Така се постига двойна цел:

1.Намаляване на излишната информация чрез компресия с висока енергийна ефективност;

2.Осигуряване на поверителност чрез дискретен шум, добавен в пространството на компресираните коефициенти, където чувствителността е по-ниска.

Вграждане на воден знак в редуцираните WT коефициенти - процедура за

Дизайн-принципи/изисквания:

- Невидимост (imperceptibility): вграденото изменение да не разрушава клинично значимите характеристики (R-пикове, HRV и т.н.). Оценка чрез PRD / PSNR + клинични метрики.

- Робустност: водният знак трябва да оцелява на типични трансформации (компресия, шум, филтриране, частично премахване).

- **Криптографска сигурност**: използване на ключ (seed) за избора на коефициенти и/или генерация на битовата последователност.

- Съвместимост с редукцията/DP: вграждането трябва да работи при вече намален набор коефициенти; ако след това при прилагане на DP-шум (дискретен).

Процедура за криптиране с помощта на хибриден криптографски алгоритъм;

Хибридният подход комбинира асиметрична криптография (за защитено прехвърляне/обмен на ключ) и симетрична автентифицирана шифрация (за самите данни). Често се формулира като KEM (Key Encapsulation Mechanism) + DEM (Data Encapsulation Mechanism). Асиметричната криптография е удобна за сигурно споделяне на ключове, но бавна за големи блокове данни. Симетричните AEAD алгоритми (напр. AES-GCM) са бързи и дават интегритет/автентичност. Хибридът дава най-доброто от двата свята.

Процедура

A. Генериране /подготовка ключове (еднократно/по нужда): Получателят генерира дълготраен асиметричен ключ.
B. Шифрриране - KEM + DEM
C. Дешифриране: Получателят прочита header, извлича EncapsulatedKey(epk или RSA_encrypted_key).

Таблица.1
Процедура за криптиране с помощта на хибриден криптографски алгоритъм

За постигането на компресирани WT коефициенти е необходимо да се шифрират **след** вграждането на воден знак и след евентуална дискретизация/DP (ако DP е част от pipeline трябва да бъде включен, определена поредността внимателно — обикновено: извличане фичъри → вграждане watermark → компресия/редукция → (ако е централно) DP → шифроване за съхранение/транзит).

Заключение:

Усъвършенставането на дигиталната здравна инфраструктура поствя на преден план съвременните средства за защита, както на личните, така и на изследователските данни в здравната индустрия, също и на ефективните взаимодействия между здравеопазването и пациентите. Предложеният софтуерен алгоритъм е изпълнен върху реални електрокардиографски, фотоплетизмографски и Холтер кардио данни. Осигуряването на защитата на няколко реални сигнала от злонамерена намеса, неоторизиран достъп, фалшифициране и сериозни атаки е възможно благодарение на създаването на математически базирани софтуерни решения. Техническото обезпечаване и събирането на огромна база от данни създава трайна необходимост от използване на все повече устройства от медицинския персонал, което налага дбрата защита на една информационна система от здрани данни да бъде и добре управлявана от администраторите на здравни заведения.

ИЗТОЧНИЦИ:

[1] Georgieva-Tsaneva, G., Galina Bogdanova, Evgeniya Gospodinova. Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography, Mathematics, 2022, 10, 390 4 от 18; file:///C:/Users/User/Downloads/mathematics-10-00390.pdf

[2] Denchev, Senior, Information and Security, University of Library Science and Information Technologies, Sofia, 2019, https://www.unibit.bg/files/opismeneh-digital/Information%20and%20Security.pdf

[3] Goodman M 2016 Future Crimes Anchor Book Press

[4] Дизайн на система за защита на кардиологични данни

[5] Pritam, VV, NIIT, Firewalls and Internet Security, 2005

[6]Съвременните технологии и техника променят облика на здравеопазването: https://digitalk.bg/internet/2013/05/10/3474077_suvremennite_tehnologii_i_tehnika_promeniat_oblika_na/

[7] Petrov, R., Information protection in computers and networks. Sofia, 2002

[8] НАУЧНИ ТРУДОВЕ НА РУСЕНСКИЯ УНИВЕРСИТЕТ - 2011, том 50, серия 3.2 - 75 - Подход за защита на електронни документи срещу несанкциониран достъп Георги Върбанов, Гео Кунев

[9] Elliptic Curves Calculator /приложение/

[10]https://store.fmi.uni-sofia.bg/fmi/algebra/lect_notes_manev/NumbTh10.pdf, Елиптични криви и криптография. СУ „Св. Климент Охридски”, Глава 10.

[11] Clément L. Canonne, Gautam Kamath, Thomas Steinke,The Discrete Gaussian for Differential Privacy, Computer Science > Data Structures and Algorithms,[Submitted on 31 Mar 2020 (v1), last revised 18 Nov 2024 (this version, v6)], [2004.00010] The Discrete Gaussian for Differential Privacy.