# ПРАКТИЧЕСКА РЕАЛИЗАЦИЯ НА ПОСТКВАНТОВИ МЕТОДИ ЗА ШИФРОВАНЕ НА ИНФОРМАЦИЯ

**Георги Т. Герасимов, Павел Г.Герасимов**

*office@g-92.com*

***Abstract.*** *In this article is presented and discussed different non-traditional approach in the sphere of practical realization of consummate low-budget encryption systems, that use automatically generated set of unique encryption keys, and blocks with variable length. The article also analyses the ressistance of such type encryption systems to brute-force attacks held by quantum computers.*

***Key word. s****low-budget encryption systems, defuzzification, delta conversion, unique super key, usk, object-relational encryption, ore, post-quantum cryptography, bs-6192,*

## Увод

*По дефиниция (Шенон) една криптосистема е съвършено сигурна тогава, когато независимо от това, че криптоаналитикът е запознат с алгоритъма на шифроване, вероятността да получи изходното (нешифровано) съобщение е равна на вероятността това съобщение да бъде открито в пространството на всички възможни съобщения*.

Съвършено сигурната криптосистема *престава да бъде такава, когато секретния ключ бива използван за повече от едно съобщение*. [1]

Съвършените криптосистеми са единствените доказано устойчиви на криптоатака, при която се използват високопроизводителни квантови компютри.

Целта на настоящия доклад е да се докаже възможността за *автоматично генерирае на набор от уникални секретни ключове за симетрични шифри, използващи блокове с променлива дължина.* Това е подход, доказал своята ефективност при изграждане на нискобюджетни съвършенни криптосистеми. [2]

## Квантов ефект на случайно събитие

При всички използвани към момента системи за генериране на секретен ключ съществуват два основни проблема както следва:

- Необходимост от логично доказване на тяхната устойчивост към криптоатаки;
- Количествената оценка, която се формира на база нивото на техническо развитие на апаратните и програмни средства към момента.

При използването на симетринчни алгоритми за шифроване с *общ секретен ключ* съществува и проблемът с *разпределение на ключовете между абонатите*.

*Основният тезис, върху който се основават по-нататъшните ни разглеждания е възможноста да бъде генериран общ секретен ключ в процеса на обмен на информация по открит канал за връзка*.

Според класическата теория докато абонатите не разполагат с общ секретен ключ те не са в състояние да обменят шифровани съобщения. Изхождайки от това следва, че те не са в състояние да обменят секретен ключ, защото не разполагат със секретен канал, който да гарантира конфеденциалният характер на обмена.

*От гледна точка на съвремения криптоанализ това твърдение е само частично вярно.*

Реално абонатите са в състояние да обменят или да генерират общ секретен ключ, *като използват открит канал за връзка*. Това е възможно при използване на явление, което в информатиката е познато с името „***квантов ефект на случайните събития***”.

По аналог с физиката, под *квантов ефект на случайно събитие* ние ще разбираме отклонение в обичайното поведение на обекта за всеки един от изграждащите го компоненти, което поражда *множество от случайни по своя характер събития*. [3]

За да бъде криптосистемата *максимално ефективна* е необходимо този механизъм да бъде прилаган към големи по обем информационни масиви, без това по някакъв начин да наруши устойчивостта ѝ към криптоатаки.

Съгласно законът за големите числа [4], според който при дадени общи условия, съвместното действие на случайни фактори води до *слабо зависещ от случайноста* резултат е в сила следната зависимост:

(1) $$P\left\{\left|\frac{\mu_n}{n}-\overline{p}\right|>\varepsilon\right\}\to 0$$

От тук следва, че при произволно $\varepsilon>0$ честотата на сбъдване клони по вероятност към *усреднената вероятност*.

Този закон е в сила само за обекти състоящи се от достатъчно голям брой елементи. [5]

Както всеки друг математически закон и тук практическата реализация *налага допускания*, които могат да бъдат изпълнени с *някаква степен на точност*. Например, последователно получените резултати не могат да се съхраняват безкрайно дълго с абсолютна точност[6][7].

За да се разбере по добре същността на цитирания закон ще си послужим с пример.

***Пример 1:***

За много малки стойности на ъгъл $\alpha$ функцията $\sin(\alpha)\approx\alpha$. С увеличаване на стойността на $\alpha$ ще се увеличава и различието между стойността на ъгъла и функцията $\sin(\alpha)$.

Описанието на механизма на квантов ефект на случайни събития е *много добре изучена материя*. Предлаганият механизъм за генерация на секретен ключ, се основава на използването на този ефект. Как точно се заражда квантовият ефект на случайни събития можем да бъде разбрано ако разгледаме използването на размита логика в системите за управление при изграждането на софтуерни приложения. [8][9]

В класическата математическа логика всяка една логическа функция може да бъде представена в дизюктивна или конюктивна нормална форма при използване на трите основни операции както следва: конюнкция (*или* – OR); дизюнкция (*и* – AND) и отрицание (*не* – NOT).

При размитата логика вместо традиционните, крайни стойности $[0,1]$ (*false*, *true*) се използва величината „***степен на истинност***" която може да приеме ***безкрайно много значения*** в ограничения интервал $\mu[0,1]$.

Прието е логическите операции в този случай да не се представят в табличен вид, а *като функции*.

- OR се представя като *max* функция $x_1 \vee x_2 \Rightarrow \max(x_1, x_2)$, при $x_1 > x_2$; $x_1 \vee x_2 \Rightarrow x_1 + x_2 - (x_1 \times x_2)$;
- AND се представя като *min* функция - $x_1 \vee x_2 \Rightarrow \min(x_1, x_2)$, при $x_1 > x_2$; $x_1 \vee x_2 \Rightarrow x_1 \times x_2$;
- NOT се представя като функция - $-x_1 = 1 - x_1$.

*Процесът при който се преминава от размита към класическа логика е сходен с процеса, които протича в една квантова система.*

Докато системата еволюира в съответствие с уравнението на Шрьофингер, нейното състояние се променя непрекъснато и детерменирано. *Всяко външно въздействие върху системата обаче предизвиква квантов скок и системата преминава в едно от дискретните си състояния*. Прието е преминаването от размита в реална стойност да се нарича „***дефъзифициране***" (*defuzzification*).

Изчисляването на реалната стойност на *дефъзираният сигнал* може да бъде изчислена както по максимална стойност, така и посредством изчисляване на тегловите суми за всички правила (*центроид*), което се извършва по формулата:

(2)
$$Z = \frac{\sum_{1}^{n} F_i S_i}{\sum_{1}^{n} F_i},$$

*където:*

$Z$ - Реална стойност на изходната променлива;

$F_i$ - Стойност на принадлежност към съответната изходна променлива;

$S_i$ - максимална стойност за съответната изходна променлива.

**Информационни маркери**

Липсата на секретен канал между абонатите не изключва възможността между тях да се предават открити съобщения. От това следва, че нищо не възпрепятства предаването на информация, която *не е критична и която не изисква съблюдаване на условието за конфеденциалност, но която може да послужи като елемент в процеса на генериране на секретен ключ*. [10]

Нека с $M$ означим открития текст, а с $K$ шифровъчния ключ. По дефиниция шифрованото съобщение $C$ ще бъде функция на $M$ и $K$, т.е. $C = f(M, K)$.

Да допуснем, че всеки открит текст може да бъде разглеждан като сума от символни блокове, с променлива дължина. Приемаме, че за всеки един блок може да бъде генериран секретен ключ така, че да бъде изпълнено условието:

(3)
$$L_{K_i} > L_{M_i},$$

където $L_{K_i}$ и $L_{M_i}$ са дължините на секретния ключ и прилежащия му блок, в условни единици.

На практика шифрованото съобщение ще се състои от $n$ на брой елементи, които *не е задължително да следват последователността на откритият текст*, като всяка една част ще бъде шифрована посредством уникален секретен ключ, т.е.

(4)
$$C = \sum_{1}^{n} C_i, \exists C_i = f(M_i, K_i) \neq C_{i+1} = f(M_{i+1}, K_{i+1}) \exists M_i \neq M_{i+1} \vee K_i \neq K_{i+1}$$

Очевидно е, че за всяко едно шифровано съобщение $C$ (*шифротекст*), критичната информация е тази, която има непосредствено отношение към използвания секретен ключ, *но не и тази, която е обвързана с открития текст*, при условие, че шифровъчният алгоритъм е известен.

*На практика шифротекстът може да бъде разглеждан като контейнер, в който се съхранява секретния ключ*.

Следващата стъпка е да определим начина, по който при подателя и реципиента ще бъдат формирани временни масиви (*функциониращи само и единствено в рамките на една конкретна сесия*) от уникални секретни ключове.

За да се реализира това ние ще използваме открит канал за връзка за да предадем „***информационни маркери***” от единия абонат на системата към другия.

Това, което е важно да се отбележи е, че „*маркерите*” (*времеви, обектни, друг вид*) *не са и по никакъв начин не могат да бъдат разглеждани като секретни ключове*. Тяхната роля е само и единствено да се задейства протоколът за автоматично генериране на уникални секретни ключове. *Друга тяхна характерна особеност е, че те по никакъв начин не могат да бъдат модифицирани, което позволява да се разглеждат като своеобразен индикатор за външна намеса в процеса на обмен между абонатите. Маркерите са динамични по своя характер. Това означава, че те могат да бъдат променяни в рамките на една сесия, което води до незабавна генерация на нов набор от секретни ключове, несъвпадащ с предхождащият го*.[11]

Процедурата за обмен на „маркери” между абонатите на криптосистемата се основава на използването на размита логика.

Изхождайки от гореизложеното можем да приемем, че ако имаме две открити съобщения $M_1$ и $M_2$, за които са изпълнени следните условия: дължината на $M_2$ е по-голяма от дължината на $M_1$ и $M_1$ се съдържа в някаква форма в $M_2$, то $M_2$ се явява „*контейнер*” за съобщението $M_1$.

От гледна точка на размитата логика (*fuzzy logic*) $M_1$, е типично размито множество, тъй като може да бъде представено като процентно съотношение от множеството $M_2$.

Нека илюстрираме така направените разглеждания със следния пример.

***Пример 2*:**

Нека са зададени следните символни низове както следва:

$M_1$ = „***допълнително проучване***”

$M_2$ = „Да се проведе ***допълнително проучване***.”

Изхождайки от принципите, върху които е изградена теорията на размитите множества, можем да твърдим, че $M_1$ е размито множество с всички, произтичащи от това последствия, тъй като за $M_1 \Rightarrow \mu \approx 0{,}5946$ или $M_1$ съставлява $\approx 60\%$ от $M_2$ и е в сила зависимостта:

$$\mu_{\tilde{M}} : M_2 \to [0,1].$$

Ако в $M_2$ бъде извършена *несанкционирана замяна* от вида: $M_2$ = „Да ***не*** се прове***жда допълнително проучване***.”, това би довело до следното изменение: $M_1 \Rightarrow \mu \approx 0{,}53653$, което означава, че $M_1$ вече ще бъде 54% от , $M_2$ и *че е била извършена външна манипулация* в рамер на 6% от оригиналния маркер. Това би довело до прекратяване на процеса или промяна в използвания протокол на обмен на данни.

Този тип *маркери* са изключително чувствителни към външна намеса, поради *малкия информационен излишък*.

**Алгоритъм за генериране на секретен ключ**

Въз основа на направените до момента разглеждания ще се опитаме да формираме алгоритъм за генериране на набор от уникални, секретни ключове при използване на маркери и открит канал за достъп.

Нека е нужно да генерираме набори (*множества*) от секретни ключове за всеки един от кореспондентите (*sender - S, recipient - R*), както следва: $K_S\left(K_1^S, K_2^S, K_3^S, \ldots, K_n^S\right)$ и $K_R\left(K_1^R, K_2^R, K_3^R, \ldots, K_n^R\right)$, които ще бъдат използвани в процеса на обмен на шифровани съобщения, за които е изпълнено условието:

(5) $$K_1^S \equiv K_1^R; K_2^S \equiv K_2^R; K_3^S \equiv K_3^R; \ldots, K_n^S \equiv K_n^R$$

Процесът на генериране на секретните ключове предхожда времево процесът на шифроване и обмен. Всеки един от тези процеси има начало и край, като с оглед на сигурността на обмена е редно всеки следващ процес да започва след като е установено, че предходният е бил успешно завършен.

Приемаме, че всеки един от двата абоната може да избере *случаен обект* (*реален или виртуален*), чиито параметри, биха могли да бъдат използвани като база за генериране на секретните ключове.

***С помощта на информационните маркери, при всеки един от абонатите на криптосистемата, локално и в рамките на текущата сесия се формира множеството от параметри, които ще бъдат използвани за генериране на секретните ключове.***

Всеки един от секретните ключове е обвързан със следните изисквания:

- Секретният ключ би следвало да има случайно, дискретно (*равномерно*) разпределение, описано с уравнението:
-

(6)
$$P_k(k)=\frac{1}{2^N}$$

където:

$P_k(k)$ - вероятност от случайно повторение на секретният ключ;
$k$ – секретен ключ;
$N$ – количество на бинарните символи, които се съдържат в ключа.

- Броят на символите в секретния ключ трябва да бъде по-голям от броя на символите, съдържащи се в асоцииранят блок (*блокът, който се шифрова със секретния ключ*).
- Всеки един секретен ключ се използва еднократно и се унищожава след приключване на сесията.

За да бъдат изпълнени тези условия всеки един от така избраните параметри се подлага на преобразуване.

Един от възможните вариантите на това преобразуване включва използване на цифров филтър с *безкрайна във времевата област импулсна характеристика*, който в най-общ вид може да бъде описан с уравнението:

(7)
$$y(n)=\sum_{i=0}^{P} b_i x(n-i)-\sum_{k=1}^{Q} a_k y(n-k),$$

където:

$x(n)$ - входяща информация;
$y(n)$ - изходяща информация;
$b_i$ - коефициент на входящата информация;
$a_i$ - коефициент на обратна връзка;
$P$ - разрядност на входящата информация;
$Q$ - разрядност на обратна връзка;

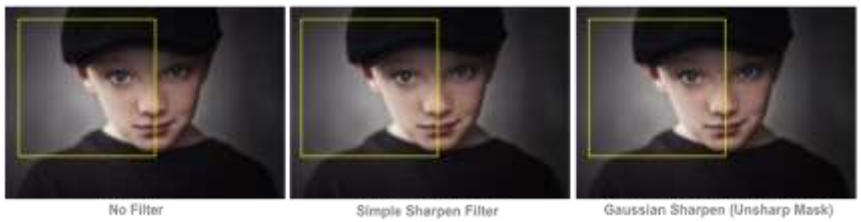
Стойностите за $y(n)$ са функционално зависими от стойностите на коефициентите $a_i$ и $b_i$, които са различни за всяка една итерация. На практика имаме *типична квантова система*, която функционира в съответствие с уравнението на Шрьодингер.

За да бъде разбран този процес ще си послужим с пример

***Пример 3*:**

Нека като случаен обект е избрано цифрово изображение, формат JPG, с размерност H=160 pix, W= 232 pix. Всеки един пиксел от изображението съдържа четири параметъра (*R, G, B, A*), всеки един от които с размерност 8 Bit.

На практика двоичното представяне на пикселите, изграждащи цифровото изображение, могат да бъдат интерпретирани като ***уникален супер ключ*** (***Unique Super Key, USK*** ) с дължина **1 187 840 Bit (*ключ с дължина един милион сто осемдесет и седем осемстотин и четиридесет бита*)**.




Фиг.1. Цифрови обекти, използвани за генериране на USK

Ако към изходното изображение приложим Simple Sharpen Filter, ще получим друго изображение, от което ще бъде генериран нов USK дължина 1 187 840 Bit, различаващ се съществено от предходния.

На практика всяко следващо повторение на тази процедура ще ни позволи да генерираме нов уникален секретен ключ.

В реалните шифросистеми обикновено се използва Gaussian Sharpen (*Unsharp Mask*) филтър, при който шировъчната система автоматично променя следните параметри: *Radius (R), Amount (A), Treshold (T).*

При обектно-релационното шифроване тази процедура се нарича *RAT-процес*. [12]

Тъй като за шифроване на блокове с променлива дължина не е нужно използването на USK, е прието да се използва малка област от избрания обект, което допълнително затруднява процеса на криптоанализ.

От така разглежданият пример могат да бъдат направени заключения, които ще ни позволят да изграждаме нискобюджетни приложения, устойчиви на криптоатаки, в т.ч. и такива, провеждани с квантови изчислителни средства.

На практика ние създадохме *съвършена система за генериране на супер дълги секретни ключове*, за която *нито един от кореспондентите няма достъп до основните елементи*, от *които е изграден шифровъчния процес*. В същото време самият процес може да бъде използван като ефективен метод за идентефикация на крайните кореспонденти, въпрос, който е тема на отделни разглеждания.

**Практическа реализация на шифровъчният модел**

В процеса на обмен на секретни съобщения, абонатите регулярно провеждат процедура за генерация на нов общ, секретен ключ, който заменя действащия. При този процес информацията, необходима за генериране на служебна информация се добавя към потока на полезна шифрована информация. Това се реализира или посредством периодични прекъсвания на потока, в рамките на една сесия (*режим на времеделение*) или при използване на няколко на брой канала за пренос. Това позволява секретните ключове да се обновяват многократно в рамките на една сесия.

Разбиването на потокът от полезна информация на достатъчно малки пакети (*делта информационни контейнери или просто* „***делти***"), в обектно-релационното шифроване се нарича „*делта преобразование*" (***delta conversion***).

Всеки един делта блок е с уникална дължина, *която не съвпада с дължината на шифрования блок*.

Процесът на обновяване на секретните ключове е пропорционален на броя на елементите, от които е изграден информационния поток.

От друга страна *служебната информация* създава предпоставки за допълнително натоварване на каналите за обмен на информация и изисква нейното времево или логично разделяне. Това налага създаване на процедура за *оптимизиране на информационният поток*.

Обменът на кратки съобщения не е решение, тъй като силно ограничава размерите на шифротекста. Много по-ефективно е използването на пакетен режим на обмен и цифров канал за връзка.

От така описаният механизъм за генериране на секретни ключове е ясно, че всяка двойка секретни ключове $\left[K_i^S, K_i^R\right]$ може да бъде едновременно (*синхроно*) генерирана при абонатите във всеки един момент $\tau_i$ от изпълнение на процедурата, тогава и само тогава, *когато използваните маркери са в допустимите граници на отклонение*.

**Заключение**

Предложенен е протокол и алгоритъм за синхронно *генериране на списъци от секретни* ключове между един или повече абонати за обмен на служебни съобщения при използване на открит канал за свръзка.

*Основното различие от класическите шифровъчни системи е, че в случая визираме процес на автоматично синхронно генериране (**Automatically Synchronized Generation, ASG**), а не за обмен. Този процес има своя специфика, която би следвало да бъде отчитана при бъдещи разглеждания.*

Друга характерна особеност е, че генерираните секретни ключове се съхраняват само и единствено в случай на необходимост. На практика обаче това не се прави. В реалните системи те се заменят с ключове от по-високо ниво, като действащите се унищожава автоматично. В резултат на тази процедура един или няколко секретени ключа не могат да бъдат откраднати или подменен както от злоумишленик така и от абонатите, защото *той съществува само и единствено в рамките на една конкретна работна сесия*.

Генерираните в рамките на сесията секретни ключове имат уникален характер. Това налага степента на надеждност на системата да бъде оценявана количествено въз основа на вероятността от прихващане на всички използвани секретни ключове, използвани от абонатите в рамките на една сесия или повече сесии.

Устойчивоста към криптоатаки при използване на този вид шифроване се обуславя не от липса на изчислителен ресурс от страна на криптоаналитика (*приемаме, че той разполага с неограничени ресурси*), а от невъзможноста да се получи необходимото количество служебна информация.

Дори когато криптоаналитикът е успял по някакъв начин да получи пълен достъп до служебната информация тя не би могла по никакъв начин да бъде обвързана с метода на провеждания криптоанализ.

На практика доказахме, че е възможно да бъде изградена нискобюджетна шифровъчна система, която в максимална степен се доближава по своите свойства до съвършенно секретните.

Въз основа на така направените теоретични разглеждания се пристъпи към практическа реализация на обектно-ориентирана система, за преобразуване на информацията, изпълняваща изискванията на съвършенна шифровъчна система.

Към настоящият момент проектът с работно наименование BS-6192A се използва успешно при надплатформени системи за обмен на критична оперативна информация (*продуктова група BeMail*) както и апаратно и програмно независими компоненти за защита на големи, информационни масиви.

Регистрирани са три международни патента. Работи се активно за реализиране на преход към *обемно-матрични системи*, използващи размита логика, които са с изключително широк спектър на приложение.

Предвижда се възможност за апаратна реализация, при която ще бъдат използвани на вероятностни процесори, базирани на PSBL (*Probability Synthesis to Bayesian Logic*).

**Използвана литература:**


1. Schneier, Bruce, „Applied Cryptography (Second Edition)”, John Wiley & Sons, Inc., 1996. ISBN 0-47111709-9.

2. Брассар, Жиль, „Современная криптология (*руководство*)”, М., Издательско-полиграфическая фирма ПОЛИМЕД, 1999. ISBN 5-8832-010-Ю. А. Розанов, „Случайные процессы”, М., изд-во „Наука”, 1971. УДК 519.2.

3. Холево А. С. Квантовая вероятность и квантовая статистика. Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления, 1991, 83, стр.5-132.

4. Feller, W. "Laws of Large Numbers." Ch. 10 in *An Introduction to Probability Theory and Its Applications, Vol. 1, 3rd ed.* New York: Wiley, pp. 228-247, 1968.

5. Feller, W. "Law of Large Numbers for Identically Distributed Variables." §7.7 in *An Introduction to Probability Theory and Its Applications, Vol. 2, 3rd ed.* New York: Wiley, pp. 231-234, 1971.

6. Колмогоров А. Н. Математика, ее содержание, методы и значение. — 1956. — С. 274-275.

7. Тутубалин В. Н. Теория вероятностей. — М.: Изд-во Московского университета, 1972. — 230 с. — С. 6-7

8. Parthasarathy K. R. An introduction to quantum stochastic calculus, Monographs in Mathematics, 85, Birkhäuser Verlag, Basel, 1992.

9. Meyer P. A. Quantum probability for probabilists, Lecture Notes in Mathematics. Vol. 1538. Springer-Verlag, Berlin, 1993.

10. Герасимов, Г. Т., Практически решения при използването на размити множества за представяне на цифрова информация, G-92 NGIT, Служебен бюлетин FFEB - 2013

11. Герасимов, Г. Т., Герасимов П.Г., Contemporary forms of information protection (*practical aspects of the object-relational encryption*), доклад.

12. Герасимов Г.Т., „Теоретични аспекти при разработването на специализирани хибридни системи”, Служебен бюлетин FFSA - 2017