конференция
РусКрипто' 2015

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

СПбГПУ - ИБКС - 1997
OPE ET CONSILIO OPERA ET STUDIO

Система криптографических стандартов Республики Беларусь

Шенец Николай Николаевич
кандидат физ.-мат. наук

Санкт-Петербургский Политехнический университет Петра Великого
кафедра «Информационная безопасность компьютерных систем»

Информационные системы РБ и криптографические стандарты

ГосСУОК
(единая система управления открытыми ключами)

ЕСИФЮЛ
(массовая ID-карта)

форматы криптографических данных
сертификаты открытых ключей, CMS, OCSP, атрибутные сертификаты
СТБ 34.101.17,19,23,26,67

общие требования
программные СКЗИ
СТБ 34.101.27

криптографические протоколы	
протокол TLS 1.2 с дополнительными криптонаборами	формирование общего ключа, аутентификация
СТБ 34.101.65	СТБ 34.101.66

криптографические алгоритмы							
шифрование	имитозащита	хэширование	ЭЦП	транспорт	HMAC	PRNG	разделение секрета
СТБ 34.101.31			СТБ 34.101.45		СТБ 34.101.47		СТБ 34.101.60

*Алгоритмы разделения секрета СТБ 34.101.60-2014 (**BELS**)*

Решаемая задача:
Заданное секретное значение (*секрет*) $s \in S$ необходимо разделить между n пользователями таким образом, чтобы лишь определенные подмножества пользователей (*разрешенные*) могли совместно его восстановить, а остальные подмножества пользователей (*запрещенные*) не получали никакой информации о секрете. В стандарте разрешенными являются подмножества $A \subseteq \{1,\ldots,n\}$, $n \geq |A| \geq t$, ((t, n)-*пороговая схема разделения секрета*).

История развития:
2011 г. – предварительный стандарт СТБ П 34.101.60-2011, действовал 2 года.
2014 г. – стандарт СТБ 34.101.60-2014.

Аналоги в мире:
Интернет-драфт **draft-mcgrew-tss-03** (Cisco) – 2010, действовал полгода.
BSI-TR 02102-1 (раздел 8 – Secret Sharing) – Германия, январь 2013 г.

Алгоритмы разделения секрета СТБ 34.101.60-2014 (BELS)

Алгоритмы стандарта:

- **алгоритмы генерации открытых ключей** (генерация общего открытого ключа, генерация открытых ключей пользователей, генерация открытого ключа пользователя по идентификатору);
- **алгоритм разделения секрета**;
- **алгоритм восстановления секрета**.

Алгоритмы стандарта реализуют модулярную схему разделения секрета в кольце многочленов от одной переменной над двоичным полем, которая:

- *совершенна* (запрещенные подмножества пользователей не получают никакой дополнительной информации о секрете, кроме априорной);
- *идеальна* (размеры частичных секретов совпадают с размером основного секрета);
- *эффективна* в вычислительном плане.

Применение: ключ разблокировки корневого УЦ ГосСУОК хранится в разделенном виде между ответственными лицами; возможно применение в ЕСИФЮЛ; передача секретной информации в разделенном виде (или разделяется ключ шифрования).

Алгоритмы разделения секрета СТБ 34.101.60-2014 (BELS)

В схеме все параметры, кроме n и t, сопоставляются с двоичными многочленами. Секрет $s \in \{0,1\}^l$, где $l \in \{128,192,256\}$ – уровень стойкости. Открытые ключи пользователей $M_1,\ldots M_n \in \{0,1\}^l$, есть также общий открытый ключ $M_0 \in \{0,1\}^l$. Открытые ключи генерируются так, чтобы многочлены вида $x^l + M_i(x)$ были различными и неприводимыми над $\mathbf{F}_2$.

Разделение секрета:

1. Случайным образом сгенерировать одноразовый ключ $k \in \{0,1\}^{(t-1)l}$.
2. $C(x) = k(x)(x^l + M_0(x)) + s(x)$.
3. $S_i(x) = C(x) \bmod (x^l + M_i(x))$, $i = 1, 2,\ldots, n$.

Восстановление секрета:

1. Решить систему сравнений $C`(x) \equiv S_i(x) \bmod (x^l + M_i(x))$, $i \in A$.
2. Положить $s(x) = C`(x) \bmod (x^l + M_0(x))$.

Алгоритмы генерации псевдослучайных чисел СТБ 34.101.47-2012 (**BRNG**)

Решаемая задача:
Генерация псевдослучайных двоичных последовательностей.

История развития:
2003 г. – РД РБ 07040.1202-2003 (процедура выработки псевдослучайных данных с использованием секретного параметра).
2012 г. – стандарт СТБ 34.101.47-2012.

Список алгоритмов стандарта:
- генерация псевдослучайных чисел в режиме счетчика (РД РБ);
- выработка имитовставки по алгоритму HMAC (RFC 2104);
- генерация псевдослучайных чисел в режиме HMAC (RFC 5246 – TLS 1.2).

В алгоритмах используются *ключ* θ и *синхропосылка* S, а также функция хэширования $h:\{0,1\}^* \rightarrow \{0,1\}^l$.

Алгоритмы генерации псевдослучайных чисел СТБ 34.101.47-2012 (**BRNG**)

Генерация псевдослучайных чисел в режиме счетчика (θ, $S \in \{0,1\}^l$):

1. $s \leftarrow S$, $r \leftarrow S \oplus 1^l$.
2. Для $i = 1, 2, \ldots, n$ выполнить:
   2.1 $Y_i \leftarrow h(\theta \| s \| X_i \| r)$; - здесь X_i – дополнительные случайные данные (по умолч. 0^l);
   2.2 $s \leftarrow s+1 (\mathrm{mod} 2^l)$;
   2.3 $r \leftarrow r \oplus Y_i$.
3. Возвратить $Y = Y_1 \| Y_2 \| \ldots \| Y_n$.

Генерация псевдослучайных чисел в режиме HMAC не накладывает ограничений на длины ключа и синхропосылки, однако требуется, чтобы функция хэширования h была блочно-итерационной с длиной блока $b \geq l$ кратной 8.

В стандарте определены следующие идентификаторы алгоритмов:
`hmac-hspec`, `hmac-hbelt`, `brng-ctr-hspec`, `brng-ctr-hbelt`, `brng-ctr-stb1176`, `brng-hmac-hspec` и `brng-hmac-hbelt`.

Алгоритмы шифрования, имитозащиты и хэширования СТБ 34.101.31-2011 (BELT)

Решаемая задача:
Обеспечение конфиденциальности и контроль целостности данных.

История развития:
2001 г. – разработан алгоритм шифрования BELT.
2007 г. – предварительный стандарт СТБ П 34.101.31-2007.
2011 г. – стандарт СТБ 34.101.31-2011.
Наряду с ним в РБ действуют ГОСТ 28147-89 и СТБ 1176.1-99 (хэш), но они постепенно выводятся из практики использования внутри страны.

Список алгоритмов стандарта:
- шифрование блока, шифрование в режимах ECB, CBC, CFB, CTR;
- выработка имитовставки, хэширование;
- **шифрование и имитозащита данных;**
- **шифрование и имитозащита ключа;**
- расширение ключа и преобразование ключа (вспомогательные).

Алгоритмы шифрования, имитозащиты и хэширования СТБ 34.101.31-2011 (BELT)

Основные параметры:

ключ $\theta \in \{0,1\}^{256} = \theta_1 \| \theta_2 \| \ldots \| \theta_8$, синхропосылка $S \in \{0,1\}^{128}$,

имитовставка $T \in \{0,1\}^{64}$, хэш-значение $h \in \{0,1\}^{256}$,

длина блока $n_b = 128$, число тактов в режимах шифрования $d = 8$.

Используются:

-экспоненциальная подстановка $H: \{0,1\}^8 \to \{0,1\}^8$;

-операции $\oplus$, $\boxminus$, $\boxplus$ и циклические сдвиги;

-преобразования G_r ($r = 5, 13, 21$): $G_r = \mathrm{RotHi}^r(H(u_1)\|H(u_2)\|H(u_3)\|H(u_4))$;

-тактовые ключи $K_i = \theta_{(i-1)\bmod 8+1}$, $i = 1,2,\ldots,56$.

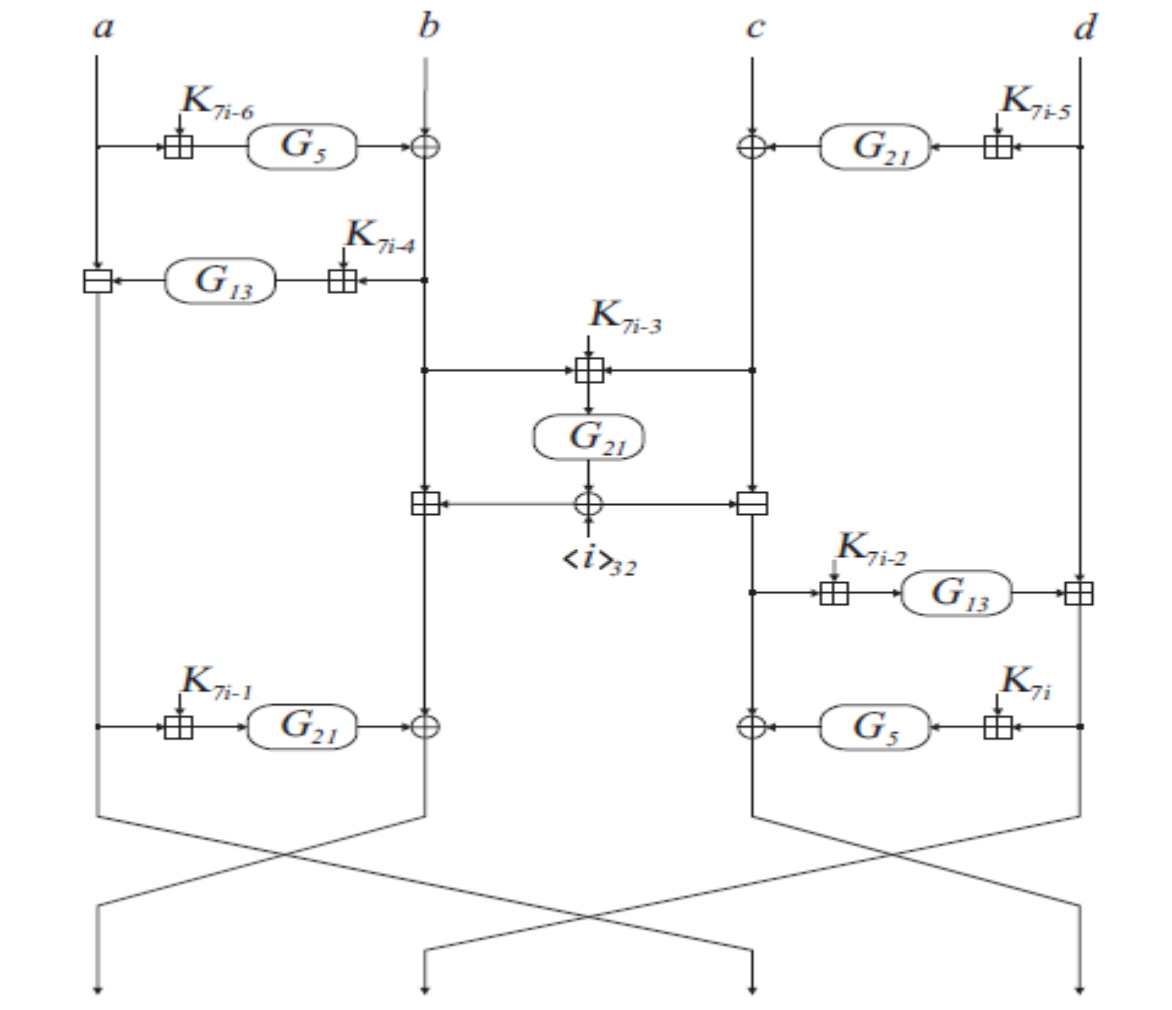
Особенности:

-ни SP-криптосистема, ни криптосистема Фейстеля;

-используются «неоднородные такты»: выбор подстановки i-го такта зависит не только от ключа, но и от номера такта;

-эффективная реализация (скорость шифрования сопоставима с AES).

Алгоритмы шифрования, имитозащиты и хэширования СТБ 34.101.31-2011 (BELT)



ЭЦП на эллиптических кривых СТБ 34.101.45-2013 (BIGN)

Решаемая задача:
Обеспечение подлинности и целостности сообщений; транспорт ключей.

История развития:
2011 г. – предварительный стандарт СТБ П 34.101.45-2011.
2013 г. – стандарт СТБ 34.101.45-2013.
Наряду с ним в РБ действует СТБ 1176.2-99 (схема Шнорра в простом поле), но он выводится из практики использования внутри страны.

Список алгоритмов стандарта:
- генерация и проверка параметров, генерация и проверка ключей;
- выработка/проверка подписи (схема Шнорра);
- **транспорт ключа (схема ЭльГамаля);**
- **выработка/проверка идентификационной ЭЦП;**
- **генерация одноразового ключа (ключ генератора определяется по личному ключу, синхропосылка - по сообщению);**
- **парольная защита ключа (дополнительно, PKCS#5 v.2.0).**

ЭЦП на эллиптических кривых СТБ 34.101.45-2013 (BIGN)

Параметры и ключи:

$l \in \{128,192,256\}$- длина личного ключа (уровень стойкости);

p – простой модуль, $2^{2l-1} < p < 2^{2l}$, $p \equiv 3 (\mathrm{mod}\ 4)$, определяет простое поле $\mathbf{F}_p$;

$a,b \in \mathbf{F}_p$- коэффициенты ЭК $E_{a,b}(\mathbf{F}_p)$: $y^2=x^3+ax+b$, $a \neq 0$, $\left(\frac{b}{p}\right)=1$,

$4a^3+27b^2 \not\equiv 0 (\mathrm{mod}\ p)$;

seed $\in \{0,1\}^{64}$ – случайное число для генерации b по a и p;

q – порядок группы точек ЭК: простое, $2^{2l-1} < q < 2^{2l}$, $q \neq p$, $q \nmid p^m-1$, $m = \overline{1,50}$

$G=(0,y_G) \in E_{a,b}(\mathbf{F}_p)$– базовая точка, причем $y_G = b^{(p+1)/4} (\mathrm{mod}\ p)$;

$d \in \{1,2,\ldots,q-1\}$ – личный ключ;

$Q \in E_{a,b}(\mathbf{F}_p)$ – открытый ключ, $Q=dG$;

$k \in \{1,2,\ldots,q-1\}$ – одноразовый личный ключ.

Используются:

h – хэш-функция длины $2l$ для предварительного хэширования сообщения;

OID(h) – идентификатор функции хэширования h;

hbelt – функция хэширования BELT.

ЭЦП на эллиптических кривых СТБ 34.101.45-2013 (BIGN)

Выработка ЭЦП	Проверка ЭЦП
1. $H \leftarrow h(X)$; 2. Случайно выбрать k; 3. $R \leftarrow kG$; 4. $S_0 \leftarrow <hbelt(\mathrm{OID}(h)\|\|<R>_{2l}\|\|H)>_l$; 5. $S_1 \leftarrow <(k-H-(S_0+2^l)d) \bmod q>_{2l}$; 6. $S = S_0\|S_1$.	1. Если $\|S\| \neq 3l$ – возвратить НЕТ; 2. $S = S_0\|S_1$, $S_0 \in \{0,1\}^l$, $S_1 \in \{0,1\}^{2l}$; 3. Если $S_1 \geq q$ – возвратить НЕТ; 4. $H \leftarrow h(X)$; 5. $R \leftarrow ((S_1+H) \bmod q)G+(S_0+2^l)Q$; 6. Если $R=O$ – возвратить НЕТ; 7. $t \leftarrow <hbelt(\mathrm{OID}(h)\|\|<R>_{2l}\|\|H)>_l$; 8. Если $t \neq S_0$– возвратить НЕТ; иначе ДА.

Сравнение операций:

Основные операции	Выработка ЭЦП	Проверка ЭЦП (без обрезки)	Проверка ЭЦП (с обрезкой)
Удвоение точек ЭК	$2l$	$2l$	$2l$
Сложение точек ЭК	l	$1{,}5l$	$1{,}25l$
Всего	$3l$	$3{,}5l$	$3{,}25l$

Протоколы на эллиптических кривых СТБ 34.101.66-2014 (BAKE)

Решаемая задача:
Выработка двумя и более сторонами общего секретного значения (ключа); выработка общего ключа на основе пароля.

История развития:
2003 г. – проект РД РБ «Банковские технологии. Протоколы формирования общего ключа» (Диффи-Хеллман);
2014 г. – стандарт СТБ 34.101.66-2014.

Список протоколов стандарта:

- протокол формирования общего ключа по схеме STS (BSTS);
- протокол формирования общего ключа по схеме MQV (BMQV);
- протокол формирования общего ключа на основе общего пароля (BPACE);
- преобразование двоичного слова в точку эллиптической кривой (доп.).

Длина формируемого ключа во всех протоколах равна 256 бит.

*Протоколы на эллиптических кривых СТБ 34.101.66-2014 (**BAKE**)*

BMQV	BSTS	BPACE
A:{hello$_A$}; B:{hello$_B$‖}{Cert(Id_B,Q_B)‖}$\langle V_B\rangle_{4l}$; A: {Cert(Id_A,Q_A)‖}$\langle V_A\rangle_{4l}$[‖T_A]; B: [T_B]. Общая секретная точка K: 1. $t \leftarrow \langle hbelt(\langle V_A\rangle_{2l}\|\langle V_B\rangle_{2l})\rangle_l$; 2. $s_{a,b} \leftarrow (u_{a,b} - (2^l+t)d_{a,b}) \bmod q$; 3. $K \leftarrow s_{a,b}(V_{b,a} - (2^l+t)Q_{b,a})$; 4. Если $K=O$, то $K=G$. На основе K и сообщений протокола вырабатывается пара ключей: общий ключ K_0 и служебный ключ K_1. Имитовставки сообщений 0^{128} и 1^{128} на ключе K_1 используются для подтверждения ключа K_0 сторонами.	A:{hello$_A$}; B:{hello$_B$‖}$\langle V_B\rangle_{4l}$; A: $\langle V_A\rangle_{4l}$‖Y_A‖T_A; B: Y_B‖T_B. Общая секретная точка K: $K=u_aV_B=u_bV_A$. На основе K и сообщений протокола вырабатываются 3 ключа: общий ключ K_0 и два служебных ключа K_1, K_2. На ключе K_2 зашифровываются сертификаты и подписи эфемерных личных ключей (u_A и u_B) сторон, обеспечивая анонимность сторон (сообщения Y_A и Y_B), а K_1 используется для вычисления имитовставок от Y_A и Y_B.	A:{hello$_A$}; B:{hello$_B$‖}Y_B; A: Y_A‖$\langle V_A\rangle_{4l}$; B: V_B[‖T_B]; A: [T_A]. Общая секретная точка K: $K=u_aV_B=u_bV_A$. На основе K и сообщений протокола вырабатывается пара ключей: общий ключ K_0 и служебный ключ K_1. Имитовставки сообщений 0^{128} и 1^{128} на ключе K_1 используются для подтверждения ключа K_0 сторонами. Общий пароль P используется для выработки ключа шифрования: $K_2 = hbelt(P)$, $Y_{A,B}=belt(R_{A,B}, K_2)$.

Во всех протоколах используются алгоритмы BELT и BIGN, а также возможно использование параметров ЭК из BIGN.

TLS 1.2, форматы данных

В этих стандартах отметим следующее:

1. Стандарты качественно переведены с учетом сложившейся в РБ терминологии.
2. Они адаптированы к белорусской криптографии, т.е. добавлены, где необходимо, ссылки на белорусские стандарты серии СТБ 34.101.* и описаны правила их использования. Например, сертификаты открытых ключей по СТБ 34.101.19 теперь можно однозначно формировать как для ключей СТБ 1176.2, так и для ключей СТБ 34.101.45.
3. В СТБ 34.101.65 (TLS) определены криптонаборы с белорусскими криптоалгоритмами.
4. Разработанные стандарты имеют общий стиль изложения и не содержат противоречивых или неоднозначных формулировок, хотя допускают гибкость их использования, которая заложена в соответствующих международных стандартах.

Достоинства и недостатки стандартов

Достоинства:

- *четкое, понятное изложение*: нет двусмысленных формулировок, имеются необходимые пояснения для разработчиков;
- *наличие справочного материала*: для всех алгоритмов и протоколов предусмотрены тестовые примеры;
- *самодостаточность*: для каждого алгоритма определены их идентификаторы и форматы данных, определены наборы стандартных параметров;
- *согласованность между собой*: алгоритмы и протоколы согласованы по используемым параметрам, текст стандартов написан в едином стиле;
- *гибкость и ориентация на практику*: стандарты разработаны с учетом потребностей современной криптографии, с учетом возможных изменений и появления других стандартов.

Недостатки:

- *недостаточная аргументация стойкости*: мало литературы и научных работ, обосновывающих стойкость принятых решений.

Что дальше?

В рамках межгосударственного сотрудничества Беларуси и России требуется, как минимум, взаимное принятие обеими странами криптографических стандартов. В этой связи возникают следующие вопросы, требующие осмысления и принятия решений:

1. Нужен ли глубокий анализ стандартов РБ в России? (следует ли проводить исследования в этой области?)
2. Следует ли заинтересованным организациям изучать стандарты РБ, получать аккредитацию на проведение испытаний с возможностью сертификации, или эти процедуры проводить строго только в РБ? (как это сейчас и делается)
3. В рамках взаимодействия ИОК двух стран в России необходим, как минимум, один УЦ, который будет использовать сертифицированные криптографические средства с белорусской криптографией. Какие шаги нужно предпринять, чтобы это осуществить?
4. ….

конференция
РусКрипто' 2015

САНКТ-ПЕТЕРБУРГСКИЙ
ПОЛИТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ
ПЕТРА ВЕЛИКОГО

Спасибо за внимание!