УДК 681.3.06

Е.В. КОТУХ

К ВОПРОСУ ПРИМЕНЕНИЯ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ В РЕАЛИЗАЦИИ СХЕМ ДОКАЗУЕМО СТОЙКОЙ АУТЕНТИФИКАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Введение

Развитие рынка телекоммуникационных услуг неотъемлемо связано с совершенствованием технологий разработки программных продуктов, появлением широкого инструментария обслуживания пользователей, систем поддержки бизнеса (BSS). Основной тенденцией развития индустрии связи на современном этапе является использование конвергентных BSS решений [1], позволяющих обслуживать абонентов в режиме реального времени, быть ориентированным на нужды различных сегментов потребителей, осуществлять быструю реакцию на их запросы и выводить маркетинговые предложения, значительно расширить широкий спектр предлагаемых услуг [2]. С этой целью оператор использует весь арсенал возможных каналов связи со своим клиентом, среди которых CRM, каналы самообслуживания (USSD, Web, IOS/Android приложения), маркетинговые кампании посредством социальных медиа (SocialCRM) и т.д. Реализация программно-аппаратной архитектуры BSS системы телекоммуникационного оператора подразумевает взаимную межкомпонентную интеграцию (средствами SOAP, REST, XML-RPC), интеграцию с сетевыми интерфейсами транспортной сети и платформами предоставления услуг (SDP,VAS) посредством протоколов, реализующих методы вычислительно стойкой аутентификации (RADIUS/DIAMETER). Большое количество каналов обслуживания, платформ и решений приводит к большему проникновению корпоративных сетей и сервисов в сети с открытыми каналами передачи информации. В процессе жизненного цикла пользователя оператор получает огромное количество критической информации и персональных данных абонента. В данных условиях BSS среда, как место хранения подробной информации о потребителе услуг [1], становится инструментом реализации всей рыночной политики оператора и, очевидно, относится к классу критических информационно-телекоммуникационных систем (ИТС) с высокими требованиями к информационной безопасности.

Обзор современного состояния и цель работы

Для корпоративных ИТС операторов связи до недавнего времени была характерна модель, в которой нарушитель моделировался как внешний, по отношению к информационной системе, субъект. В процессе эволюции программного обеспечения возникает необходимость механизмов, гарантирующих обеспечение информационной безопасности в условиях взаимного недоверия между всеми участниками протокола, в условиях возможного сговора нескольких участников. Объем данных, передаваемых в корпоративных системах, который может быть доступным криптоаналитику в попытке реализовать модель нарушителя, напрямую влияет на эффективность дифференциального и частотного криптоанализа. Вследствие этого возникает одно из противоречий, когда в условиях стремительного возрастания объемов шифрованной информации, передаваемой по сетям, используемые на практике криптосистемы не позволяют обеспечивать требуемую стойкость к современным методам криптоанализа [3]. Согласно теории аутентификации [4] выделяют три уровня стойкости: вычислительная, доказуемая, безусловная стойкость. Основное противоречие доказуемо стойкой аутентификации состоит в том, что для обеспечения гарантированной вероятности обмана на уровне нижней границы размер ключа должен быть не меньше размера сообщения, а фиксирование размера ключа на нижней границе, определяемой мощностью пространства хешей, приводит к пропорциональному росту вероятности коллизии от длины данных.

В архитектуре современных BSS систем задачи проектирования механизмов аутентификации и авторизации между платформами различных вендоров решаются экспертным

путем, на основе знаний и опыта конкретных разработчиков с использованием рекомендованных стандартов, которые не всегда в полной мере удовлетворяют требованиям, предъявляемым к критическим ИТС. Наиболее распространенным решением задачи аутентификации является построение AAA инфраструктуры, как интерфейса взаимодействия с компонентами телекоммуникационной ИТС, посредством использования RADIUS (DIAMETER) протоколов. Принципы работы протоколов RADIUS/DIAMETER описаны в [5]. В решении задачи аутентификации широкое применение получил EAP фреймворк, позволяющий реализовать различные методы аутентификации [6]: EAP-SIM, EAP-AKA, LEAP, EAP-MD5, EAP-MSCHAP V2, EAP-TLS, EAP-SecureID.

Преимущество реализации EAP-реализации механизма аутентификации заключается в отсутствии необходимости аутентификатора понимать реализацию тех или иных специфичных особенностей различных методов аутентификации. Аутентификатор служит лишь передаточным звеном между клиентом и сервером аутентификации. В текущих реализациях методов аутентификации (рекомендованных EAP), не являющихся проприетарными, выявлен ряд уязвимостей, причиной которых является слабая вычислительная стойкость к коллизиям используемых криптографических примитивов, недостаточная длина ключей, возможность реализовать атаку изнутри, неудачная реализация клиентов.

Перспективным направлением является разработка библиотек, реализующих методы аутентификации с доказуемой и безусловной стойкостью. Целью данной статьи является:

- исследование возможностей универсального хеширования (*UH*) в целях построения доказуемо стойких схем аутентификации для телекоммуникационных систем;
- сравнительный анализ существующих подходов к построению универсальных хеш-функций на основе алгебраических кодовых конструкций, композиционных и каскадных схем, предложить рекомендации по использованию полученных результатов для реализации открытых библиотек;

Анализ предметной области

Решение задачи построения коллизионно-стойких функций хеширования, соответствующих международным требованиям гарантированной стойкости к атакам, сложности и скорости вычисления, характеристикам и реализациям алгоритма, возможно в теории доказуемо стойкой аутентификации. Основные положения теории аутентификации определены в [4]. Симмонс Г.Д. ввел понятие вероятности обмана и показал, что вероятность обмана имеет нижнюю границу $1/|B|$, где $|B|$ – мощность пространства кодов аутентификации [4]. Для доказуемо стойкой аутентификации ключевое пространство $|K|$ должно быть не меньше пространства сообщений $|D|$. Данное требование удовлетворяется в классе универсальных хеш функций. В методе универсального хеширования на основе скалярного произведения достигается $P_{кол}=1/|B|$, при условии, что $|K|=|D|$, а в методе полиномиального хеширования $P_{кол}\sim\log|D|$, $|K|=|B|$. Идеи универсальной аутентификации получили развитие с использованием строго универсального хеширования [13]. Основной результат строго универсального хеширования состоит в том, что вероятность коллизии $P_{кол}=1/|B|$ достигается при условии $|K|\geq|D|\cdot|B|$. Посредством применения слабосмещенных массивов для построения почти строго универсальных хеш функций удается снять ограничение на размер ключевого пространства $|K|\geq\cdot|B|^2$, но это предопределяет увеличение вероятности коллизии $P_{кол}>1/|B|$.

В работах [7, 8] рассматриваются практические аспекты реализации алгоритмов на основе универсального и строго универсального хеширования в приложении к задачам аутентификации в 3GPP/LTE. Сравнительный анализ свойств MAC-кодов с применением блочных шифров в режиме CBC-MAC (ISO/IEC 9797-1) и на основе без ключевых хэш-функций HMAC (ISO/IEC 9797-2) определил основные пути повышения коллизионных свойств и вычислительной скорости для практических схем реализации MAC-кодов [26]

Более широкое распространение получают идеи построения схем аутентификации на основе MAC-кодов с применением универсального класса хеш-функций. MAC-коды, основанные на универсальном хешировании, используют определение семейства хеш-функций [26].

Определение 1. H={h: D→R} есть семейство хэш-функций с общей областью определения D и конечным диапазоном значений R.

MAC коды являются отображением H: K×D→ R, где $h = H_K$: D→R – функция определенная для каждого $K \in$ K с заданным распределением на H [26].

Основные универсальные семейства хэш-функций имеют следующие представления:

1. H является универсальным семейством хэш-функций (ε-U) если для всех x≠y∈D,

$$Pr_{h\in H}[h(x)=h(y)]=\varepsilon,\ \varepsilon=1/\!/R/\!/.$$

2. H является Δ-универсальным семейством хэш-функций (ε-ΔU) если для всех x≠y∈D и всех a∈R,

$$Pr_{h\in H}[h(x)-h(y)=a]=\varepsilon,\ \varepsilon=1/\!/R/\!/.$$

3. H является почти Δ-универсальным семейством хэш-функций (ε-AΔU) если для всех x≠y∈D и всех a∈R,

$$Pr_{h\in H}[h(x)-h(y)=a]\le\varepsilon.$$

4. H является строго универсальным семейством хэш-функций (ε-SU) если для всех x≠y∈D и всех a,b∈R,

$$Pr_{h\in H}[h(x)=a,h(y)=b]=\varepsilon,\ \varepsilon=1/\!/R/\!/^2.$$

5. H является почти строго универсальным семейством хэш-функций (ε-ASU) если для всех x≠y∈D и всех a,b∈R,

$$Pr_{h\in H}[h(x)=a,h(y)=b]\le\varepsilon$$

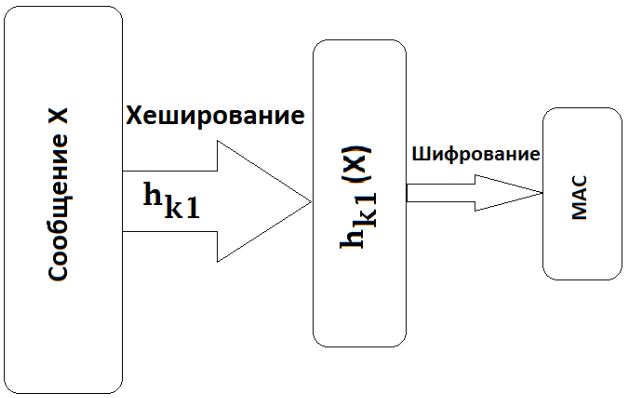
Практические схемы реализации MAC-кодов на основе алгебраического кодирования, почти универсального и строго универсального хеширования впервые предложено Картером и Вегманом [9, 10].

Основная идея заключается в хешировании сообщения X с использованием семейства универсальных хеш-функций для дальнейшего шифрования криптографическим примитивом для выработки аутентификатора:

$$MAC_K(X, N) = hK1(X) \oplus fK2(N), \qquad (1)$$

где *MAC* – код аутентификации, *X* – сообщение, *N* – случайный код; *K* – ключевое пространство, *K1*, *K2*∈*K*, *hK1* – хеш-функция семейства универсальных хеш-функций, *fK2* – блочное шифрование (рисунок).

Одним из конструктивных недостатков схем аутентификации на основе блочных шифров является невозможность построения алгоритмов с параллельными вычислениями. Схемы аутентификации на основе CW-MAC лишены данного недостатка и являются одними из наиболее производительных схем (первые решения на основе блочных шифров упирались в поток 2Gb/s, а схемы аутентификации на основе универсального хеширования позволяют увеличить этот предел до 10 Gb/s).



Общая схема построения CW-MAC

Основные положения универсального хеширование приведены в работах [9, 11, 12], уточнения и дополнения в [13]. Исследование вычислительных затрат в построении MAC-кодов на основе универсального класса хеш-функции и практические результаты по строго универсальному хешированию получены в [14]. Коллизионные свойства MAC кодов универсального хеширования MAC, коды универсального хеширования определяются массивами с известными статистическими и комбинаторными свойствами, что позволяет получить точные коллизионные границы.

Схемы построения MAC-кодов на основе универсального семейства хеш-функций и их свойства хорошо изучены для UMAC [18], криптографическая CRC [16], bucket-хеширование [16], MMH [17], GMAC [17]. Спецификация UMAC предложена в [18]. Схема имеет доказуемую стойкость. Использование универсальной хеш-функции позволило распараллелить вычисления и прийти к реализации с высокой пропускной способностью. Схема требует массива одноразовых случайных кодов (N) и обеспечения невозможности их переиспользования. Спецификация GMAC лежит в основе режима шифрования GCM. Полиномиальное хеширование в конечном поле GF (2^{128}). Реализация имеет ряд потенциальных уязвимостей, описанных в [15 – 17].

Принимая во внимание итоги конкурса NIST по SHA-3, выводы относительно коллизионной стойкости популярных криптографических хэш-функций (и MAC-кодов на основе этих функций), значительный прирост доступной криптоаналитику вычислительной мощности, обусловленной развитием GPGPU-технологий (General Purpose Graphic Processor Unit), можно предположить, что практические решения на основе методов универсального хеширования получат большее развитие и применение.

Таким образом, актуальной задачей является сравнительный анализ результатов универсального хеширования для практической реализации методов аутентификации и расширения возможностей открытых библиотек.

Возможности методов универсального хеширования. Основные результаты

Метод универсального хеширования на основе алгебраического кодирования предложен группой авторов в работе [19]. Основной результат состоит в том, что вероятность коллизии определяется параметрами алгебраического кода. Это позволило связать вероятность коллизии с длиной сообщения, ключа и полем вычисления хешей. Ключевое пространство определяется длиной кода. Выбор параметров алгебраического кода позволяет оптимизировать затраты на аутентификацию. Наилучшие результаты универсального хеширования по соотношению затрат на поле вычислений, размер ключевых данных при фиксированном значении вероятности коллизии достигается на алгебраических кривых с наибольшим отношением рода g к числу точек.

Параметры универсального хеширования по рациональным функциям наилучших алгебраических кривых оценки вероятности коллизии и сложности представлены в [19], универсальное хеширование по рациональным функциям алгебраической кривой представляется определением 1 [20].

Хеш-функция $h_{P_j}(m) \in F_q$ для сообщения $m = (m_1,..., m_k)$, $m_i \in F_q$ в точке P_j определяется выражением

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i , \qquad (2)$$

где $f_i \in F_q(\chi)$ с упорядоченными порядками полюсов $0 < \rho_1 < \rho_2 < ... < \rho_k$,.

Свойства универсального хеширования по рациональным функциям алгебраических кривых определяются утверждением.

Утверждение. Хеш-функция $h_{P_j}(m)$ определяет универсальный хеш-класс $\varepsilon - U(N, q^k, q)$, где N – число точек алгебраической кривой, q^k – объем пространства сообщений, q – объем пространства хеш кодов и вероятность коллизии, определяется выражением 3

$$\varepsilon = \rho_k / N , \qquad (3)$$

где ρ_k – значение полюса рациональной функций f_k. Граница вероятности коллизии для $\varepsilon - U(N, q^k, q)$ хеш класса, построенного по рациональным функциям плоских алгебраических кривых рода g над большим алфавитом и фиксированных $k \le g$ и q, имеет вид

$$1 - \frac{q^k (q-1)}{(q^k - 1)q} \le P_{кол} \le \varepsilon \le \frac{\sqrt{2k}}{q} + \frac{3\sqrt{2k}}{2q\sqrt{q}} . \qquad (4)$$

Параметры и основные результаты универсального хеширования обобщены в табл. 1. Верхняя асимптотическая граница вероятности коллизии лучше асимптотической границы для хеширования по алгебраическим кодам и уточняет границу для алгеброгеометрических кодов [20]. Асимптотические оценки вероятности коллизии универсального хеширования по рациональным функциям алгебраических кривых для фиксированного поле вычислений представлены в табл. 2.

Абсолютный результат реализуется для хеширования на кривой Сузуки. Вычисление по кривым Ферма и Сузуки является результативным для значений длины данных k, превышающих размерность поля [21]. В расширенном роле (табл. 3) достигаются наиболее интересные для практической реализации результаты *UH* по кривой Сузуки [23].

Несколько уступает по вероятности коллизии хеширование по кривой Ферма. Практические вычисления для вероятности коллизии $\varepsilon \sim 2^{-50}$ и меньше реализуются на модулях в 64 бит и больше для данных до нескольких гигабайт. Ключевые затраты на хеширование по кривым Сузуки и Ферма в два раза превышают по числу бит на хеширование по проективной прямой [21].

Безусловная аутентификация на основе композиционного хеширования является одним из подходов в решении задачи уменьшения ключевых затрат [20 – 22]. Композиционное хеширование эффективно снижает затраты на размер ключевых данных, допуская снижение секретности. Применение алгебраических кодов в композиционных схемах и основные оценки получены в [22, 25].

Как следует из анализа, лучшие результаты для строгой аутентификации достигаются на длинных алгебраических кодах. Коды Сузуки относятся к классу алгеброгеометрических кодов, определенных над полем рациональных функций ассоциированным с группой Сузуки,

что определяет актуальность построения теории универсального хеширования над полем рациональных функций алгебраических кривых.

Таблица 1

Параметры универсального хеширования

Уравнение кривой	Параметры универсального хеширования $\varepsilon - U(N, q^{2k}, q^2)$	Оценка вероятности коллизии ε, $k < g$	Оценка сложности вычислений	Асимптотическая оценка $\varepsilon_{q\to\infty}(k)$
$y^q + y = x^{q+1}$, F_{q^2}	$U(q^3, q^{2k}, q^2)$	$k/q^3 + s/q^2 - s(s-1)/(2q^3)$ $s = \lfloor (2k+1/4)^{1/2} - 1/2 \rfloor$	$k+s$	$\sqrt{2}k^{1/2}/q^2$
$y^q + y = x^d$, F_{q^2}, $d \mid q+1$	$U(q^2 + (d-1)(q-1)q, q^{2k}, q^2)$	$(iq + jd)/(q^2 + (d-1)(q-1)q)$ $s = \lfloor (2k/m + 1/4)^{1/2} - 1/2 \rfloor$, $t = \lfloor (k - m(s-1)s/2)/s \rfloor$. $m = (q+1)/d$, $ind = 0, -1$	$k+s$	$\sqrt{2(q+1)/d}$ $k^{1/2}/q^2$
$\sum_{i=1}^{t} y^{q/p^i} + \omega x^{q+1} = 0$ F_{q^2}, $q = p^t$ $\omega^{q-1} = -1$	$U(q^3/p, q^{2k}, q^2)$	$(i(q+1)p + jq)/q^3$ $s = \lfloor (2k/p + 1/4)^{1/2} - 1/2 \rfloor$, $t = \lfloor (k - p(s-1)s/2)/s \rfloor$, $ind = 0, 1$	$k+s$	$\sqrt{2p}k^{1/2}/q^2$
$x^{(q+1)/d} + x^{2(q+1)/d} + y^{q+1} = 0$ F_{q^2}, $q = 2 (\mathrm{mod} 3)$ $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$	$U((q^3 + 2q^2 + 4q + 3)/3, q^{2k}, q^2)$	$(3iq + 3j(q+1) + t \cdot 2(q+1))/$ $(q^3 + 2q^2 + 4q + 3)$ $s = \lfloor (2k/3 + 1/4)^{1/2} - 1/2 \rfloor$	$k+s+3$	$\sqrt{6}k^{1/2}/q^2$
$\omega x^{(q-1)/d} - y x^{2(q-1)/d} + y^q = 0$ F_{q^2}, $\omega^{q-1} = -1$ $q \equiv 1 (\mathrm{mod} 3)$ $\alpha^{(q+1)/2} x^{(q-1)/3} +$ $\alpha^{(q^2-1)/2} x^{2(q-1)/3} y + y^q = 0$	$U((q^3 + 2q^2 - q - 2)/3, q^{2k}, q^2)$	$(3iq + 3j(q+1) + t \cdot (2q+1))/$ $(q^3 + 2q^2 - q - 2)$ $s = \lceil (2k/3 + 1/4)^{1/2} - 1/2 \rceil$	$k+s+3$	$\sqrt{6}k^{1/2}/q^2$
$y^q - y = x^{q_0}(x^q - x)$ F_q, $q = 2q_0^2$, $q_0 = 2^s$	$U(q^2, q^k, q)$	$(i(q+2q_0) + j(q+2q_0+1) +$ $t(q+q_0) + rq)/q^2$ $s = (3k)^{1/3}$	$k + s^3/3 +$ $s^2/2 + 2s - 1$	$(3k)^{1/3}/q$
$X + Y + Z = 0$, F_q	$U(q, q^k, q)$	k/q	k	k/q
$X^{(q-1)/3} + Y^{(q-1)/3} +$ $Z^{(q-1)/3} = 0$ F_q, $q \equiv 1 (\mathrm{mod} 3)$	$U(2(q-1)^2/9, q^k, q)$	$s = \lceil (2k+1/4)^{1/2} - 1/2 \rceil$ $3\lceil (2k+1/4)^{1/2} - 1/2 \rceil/(2(q-1))$	$k+s$	$3/\sqrt{2}k^{1/2}/q$
$X^{q^2+q+1} + Y^{q^2+q+1} +$ $Z^{q^2+q+1} = 0$ F_{q^3}	$U((q-2)(q^2+q+1)^2$ $2(q^2+q+1), q^{3k}, q^3)$	$s = \lceil (2k+1/4)^{1/2} - 1/2 \rceil$ $\lceil (2k+1/4)^{1/2} - 1/2 \rceil/$ $((q-2)(q^2+q+1)+2)$	$k+s$	$\sqrt{2}k^{1/2}/q^3$

Таблица 2

Оценки вероятности коллизии *UH* по алгебраическим кривым над полем F_q

Тип кривой	Оценки вероятности коллизий $\varepsilon_{q\to\infty}(k)$ для k слов данных			
	$k=1$	$k=\sqrt{q}$	$k=q$	$k=q^{3/2}$
Проективная прямая	$1/q$	$1/q^{1/2}$	1	1
Кривая Эрмита	$1/q$	$\sqrt{2}/q^{3/4}$	$\sqrt{2}/q^{1/2}$	1
Максимальные кривые второго рода	$1/q$	$2/q^{3/4}$	$2/q^{1/2}$	1
Максимальные кривые третьего рода	$1/q$	$\sqrt{6}/q^{3/4}$	$\sqrt{6}/q^{1/2}$	1
Кривые Ферма с большим числом точек	$1/q$	$3/(\sqrt{2}q^{3/4})$	$3/(\sqrt{2}q^{1/2})$	$3/(\sqrt{2}q^{1/4})$
Кривая Сузуки	$1/q$	$\sqrt[3]{3}/q^{5/6}$	$\sqrt[3]{3}/q^{2/3}$	$\sqrt[3]{3}/q^{1/2}$

Таблица 3

Оценки параметров *UH* для расширенного поля

Параметры конечного поля F_q, $p=2^m$	Уравнение кривой	Размер пространства ключей (бит)	Вероятность коллизии для данных размером L бит			Размер хеш кода (бит)
			1Кбт	1Мбт	1Гбт	
$q=2^{32}$	$X+Y+Z=0$	32	2^{-24}	2^{-14}	2^{-4}	32
$q=2^{31}$	$y^q-y=x^{q_0}(x^q-x)$	62	$2^{-27,79}$	$2^{-24,46}$	$2^{-21,13}$	31
$q=2^{32}$	$x^{(q-1)/3}+x^{(q-1)/3}+1=0$	64	$2^{-26,89}$	$2^{-21,91}$	$2^{-17,5}$	32
$q=2^{64}$	$X+Y+Z=0$	63	2^{-57}	2^{-47}	2^{-37}	64
$q=2^{63}$	$y^q-y=x^{q_0}(x^q-x)$	126	$2^{-60,13}$	$2^{-56,8}$	$2^{-53,47}$	63
$q=2^{64}$	$x^{(q-1)/3}+x^{(q-1)/3}+1=0$	128	$2^{-59,41}$	$2^{-54,41}$	$2^{-49,41}$	64

Выводы

1. Развитие подходов к построению универсальных хеш-функций на основе алгеброгеометрических кодовых конструкций, композиционных и каскадных схем позволяет реализовать схему доказуемо стойкой и безусловной аутентификации для критических ИТС.

2. Актуальные исследования обосновали возможность уменьшения сложности вычислений без увеличения вероятности коллизии посредством решения задачи минимизации сложности вычислений при хешировании заданного числа слов данных и заданной вероятности коллизии за счет оптимизации выбора базисных функций и размерности функционального пространства.

3. Полученные результаты обосновывают применение каскадного хеширования, позволяющего получить наименьшую вероятность коллизии, сложность вычислений хешей для фиксированного объема данных и размерности конечного поля, что дает возможность эффективно увеличить размер хешируемых данных и выравнивает вероятность коллизии с изменением длины данных.

4. Эти и другие результаты предопределяют появление нового поколения хеш-функций и стандартов для построения схем аутентификации в критических ИТС, а также их практическое применение и разработку современных методов для решения задачи аутентификации посредством EAP фреймворка.

Список литературы: 1. http://wemove.technology . 2. *Orga* Systems and Astelit deliver fast end-to-end BSS transformation project for BeST Belarus // Press release, www.orga-systems.com, 2014. 3. *Авдошин С.М., Савельева А.А.* Криптоанализ: современное состояние и перспективы развития: материал технической информации // ИТ : Прилож. к журналу "Информационные технологии". – 2007. – N3. – С. 1 – 32. 4. *Simmons, G. J.* Authentication theory/coding theory // Aduances in Cryptology, Proc. CRYPT0 84, Lecture Notes in Computer Science, No. 196. G. R. Blakley and D. Chaum, Eds. New York: Springer, 1985, pp. 411-431. 5. *Гольдштейн Б.С., Елагин В.С., Сенченко Ю.Л.* Протоколы AAA: RADIUS и Diameter. Сер. «Телекоммуникационные протоколы». Кн. 9. – СПб. : БХВ&Петербург, 2014. – 352 с. 6. *Extensible* Authentication Protocol [online]. 7. *ETSI/SAGE* Specification. Specification of the 3GPP Confidentiality and Integrity Algorithms. Document 2: Kasumi Algorithm Specification. ETSI/SAGE, 2011. 8. *Ju-Sung Kang, Sang Uk Shin, Dowon Hong, and Okyeon Yi.* Provable security of KASUMI and 3GPP encryption mode f8. In Colin Boyd, editor, ASIACRYPT, volume 2248 of Lecture Notes in Computer Science, pages 255{271. Springer, 2001. 9. *Carter L., Wegman, M. N.* Universal Classes of Hash Functions //Journal of CSS, 1979. 10. *Carter L., Wegman M. N.* New hash functions and their use in authentication and set equality // Journal of Computer and System Sciences. – 1981. – Vol. 22. 11. *Stinson D.R.* Combinatorial techniques for universal hashing / D.R.Stinson // Journal of Computer and Systems Science. – 1994. – V.48. – P.337 – 346. 12. Stinson D.R. Universal hashing and authentication codes / D.R.Stinson // Designs, Codes and Cryptography. – 1994. – N. 4. – P.369–380. 13. *Халимов Г.З.* Аутентификация и универсальное хеширование / Г.З.Халимов, А.А.Кузнецов // Радиотехника. – 2001. – Вып. 119. – С. 88 – 94. 14. *Халимов Г.З.* Строго универсальное хеширование // Прикладная радиоэлектроника. – 2013. – Т. 12. № 2. – С. 220–224. 15. *Helena* Handschuh and Bart Preneel. Key-recovery attacks on universal hash function based MAC algorithms // International Crytology Conference – CRYPTO , pp. 144-161, 2008. 16. *Procter G. and Cid C.* On weak keys and forgery attacks against polynomial-based MAC schemes // Fast Software Encryption, Lecture Notes in Computer Science, page To appear. Springer, 2013. 17. *Markku-Juhani* Olavi Saarinen. Cycling attacks on GCM, GHASH and other polynomial MACs and hashes // Anne Canteaut, editor, FSE, volume 7549 of Lecture Notes in Computer Science, pages 216{225. Springer, 2012. 18. *John Black, Shai Halevi, Hugo Krawczyk, Ted Krovetz and Phillip Rogaway*. Advances in Cryptology ."UMAC: Fast and Secure Message Authentication" // CRYPTO '99. Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999, pp. 216 – 233. 19. *Bierbrauer, J.* On families of hash functions via geometriccodes and concatenation. / Bierbrauer J., Johansson T., Kabatianskii G., Smeets B. // Advances in Cryptology-CRYPTO'93 Proceedings. – Springer-Verlag, 1994. – P. 331–342. 20. *Халимов Г.З.* Каскадное универсальное хеширование с использованием АГК кодов / Халимов Г.З., Иохов А.Ю. // Восточно-европейский журнал передовых технологий. – Х., 2005. – Вып. 2/2(14). – С. 111–119. 21. *Халимов Г.З.* Каскадное универсальное хеширование по рациональным функциям алгебраическихкривых / Г.З. Халимов // Радиотехника. – 2011. – Вып 166. – С.218 – 225. 22. *Халимов Г.З.* Универсальное хеширование по кривой Сузуки / Г.З. Халимов, Е.В. Котух // Прикладная радиоэлектроника. – 2011. – Т.10, № 2. – С.80 – 86. 23. *Котух Е.* Универсальное хеширование с ограничением функционального поля алгебраических кривых / Е. В. Котух. – Радиотехника. – 2011. – Вып 171. – С. 109 – 115. 24. *Котух Е.* Метод универсального хеширования по алгебраическим кривым / Е. Котух, Г. Халимов, А. Бойко, А. Герцог // XV Юбилейная Междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах». Тезисы докладов – Киев : Гос. служба специальной связи и защиты информации Украины, 2012. – С. 36. 25. *Котух Е.* Многокаскадное универсальное хеширование по рациональным функциям максимальной кривой третьего рода / А. Г. Корченко, Е. В.Котух, А.А.Бойко // Радиотехника. – 2011. – №166. – С. 44 – 49. 26. Халимов, Г. Высокоскоростной UMAC алгоритм / Геннадий Халимов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. – Вип. 11. – С. 167-173.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 12.02.2015