ПОЛОЖЕНИЕ
об Открытом конкурсе научных работ
по исследованию хэш-функции ГОСТ Р 34.11-2012

1 Общие положения

1.1 Российский Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) при участии Академии криптографии Российской Федерации и при организационной и финансовой поддержке ОАО «ИнфоТеКС» проводит открытый конкурс научно-исследовательских работ, посвященных анализу криптографических качеств хэш-функции, определенной в национальном стандарте ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

1.2 Настоящее положение (далее – Положение) определяет цели, задачи, условия участия, организационное и финансовое обеспечение и порядок проведения конкурса научно-исследовательских работ (далее – Конкурс) и порядок определения его победителей и их награждения.

1.3 Основными целями и задачами Конкурса являются:

- привлечение внимания российской и международной научной общественности к отечественным криптографическим алгоритмам и протоколам;
- стимулирование и поощрение научных исследований по оценке криптографических качеств алгоритмов и протоколов, включенных в национальные стандарты Российской Федерации;
- популяризация и повышение привлекательности отечественных решений в области криптографической защиты информации.

1.4 Организатором Конкурса выступает ОАО «ИнфоТеКС».

1.5 Финансовое обеспечение Конкурса осуществляется за счет средств Организатора.

1.6 Информационная поддержка Конкурса осуществляется силами Организатора и Технического комитета ТК26.

1.7 Сроки проведения Конкурса: с 21 октября 2013 года по 15 декабря 2014 года.

1.8 Рабочими языками проведения Конкурса являются русский и английский языки.

2 Порядок организации Конкурса

2.1 Для проведения Конкурса Организатор формирует Оргкомитет и Конкурсную комиссию.

2.2 Оргкомитет Конкурса:

- подготавливает информационные материалы о Конкурсе;
- организует оповещение о проводимом Конкурсе путем:
  - публикации информации о Конкурсе в профильных печатных изданиях и в материалах профильных конференций и симпозиумов;
  - размещения информации о Конкурсе на публичных информационных ресурсах Интернета, профильных новостных и аналитических сайтах;
  - рассылки информационных материалов о конкурсе по электронной почте в научные организации математического и технического профиля, учреждения, входящие в Учебно-методическое объединение высших

учебных заведений России по образованию в области информационной безопасности, и организации, разрабатывающие средства криптографической защиты;

- производит сбор заявок на участие в конкурсе и материалов научно-исследовательских работ;
- передает в Конкурсную комиссию представленные работы в обезличенном виде для проведения независимой экспертизы;
- осуществляет информационную поддержку Конкурса на всех этапах его проведения;
- осуществляет иные функции в соответствии с настоящим Положением по организационной и технической поддержке проведения Конкурса.

2.3 Конкурсная комиссия формируется из ведущих специалистов в области криптографии и математики: докторов и кандидатов физико-математических и технических наук, профессорско-преподавательского состава кафедр ведущих образовательных учреждений высшего профессионального образования по информационной безопасности и экспертов по криптографии научных институтов и других научно-технических организаций.

- Состав Конкурсной комиссии и ее Председатель согласовывается с Техническим комитетом ТК26 и с Академией криптографии Российской Федерации. Состав Конкурсной комиссии публикуется Организатором до окончания приема заявок на Конкурс.
- Конкурсная комиссия:
  - определяет порядок работы Комиссии;
  - вырабатывает критерии оценки работ, поступивших на Конкурс;
  - организует на условиях анонимности проведение научной экспертизы представленных на Конкурс работ собственными членами и путем привлечения внешних экспертов;
  - определяет победителей и призеров Конкурса;
  - осуществляет иные функции в соответствии с настоящим Положением.
- Конкурсная комиссия принимает решения простым большинством голосов. В случае равенства голосов, голос Председателя комиссии является решающим.
- Конкурсная комиссия представляет в Оргкомитет результаты проведенной экспертизы научно-исследовательских работ участников и список победителей и призеров Конкурса.

2.4 Церемония награждения победителей и призеров Конкурса проводится Техническим комитетом ТК26 и Организатором Конкурса.

3 Порядок проведения Конкурса

3.1 Конкурс проводится в 2 этапа: промежуточный и заключительный.

3.2 Первый (промежуточный) этап Конкурса проводится в период с 21 ноября 2013 года по 31 марта 2014 года. Заявки на участие в первом этапе Конкурса принимаются Оргкомитетом до 28 февраля 2014 года включительно.

- В первом этапе Конкурса могут принять участие завершенные, не публиковавшиеся ранее в рецензируемых изданиях работы, подготовленные для данного Конкурса одним автором либо авторским коллективом.
- Экспертиза работ осуществляется методом «слепого» рецензирования не менее, чем двумя экспертами.

- По результатам экспертизы Конкурсная комиссия выносит решение о составе победителей первого этапа Конкурса в количестве до 8 работ. Протокол заседания Конкурсной комиссии с подведением итогов первого этапа Конкурса передается в Оргкомитет Конкурса для награждения победителей первого этапа Конкурса.
- Объявление результатов первого этапа Конкурса производится до 31 марта 2014 года на сайте Организатора, сайте Технического комитета ТК26, на общедоступных новостных и профильных ресурсах Интернета, рассылкой по электронной почте. Оргкомитет Конкурса гарантирует сохранность авторских прав на интеллектуальную собственность участников Конкурса и третьих лиц при публикациях информационных материалов о ходе Конкурса.
- Оповещение победителей первого этапа Конкурса осуществляется Оргкомитетом заказным письмом и по электронной почте в соответствии с сообщенными ими контактными данными. При этом победителям предоставляются:
  - анонимные отзывы экспертов, рецензировавших работу;
  - отзыв-рекомендация в журналы «Математические вопросы криптографии» и «Дискретная математика» на публикацию работы;
  - приглашение на представление работы на симпозиуме CTCrypt-2014 «Современные тенденции в криптографии».
- Победителям (одному представителю от авторского коллектива, указанному в заявке) первого этапа выплачивается вознаграждение в размере 70000 рублей, предназначенное для организации публикации представленных на Конкурс работ в материалах профильных рецензируемых международных конференций и симпозиумов, а также общедоступных периодических изданиях. Список конференций и изданий, в которых рекомендуется публикация результатов, согласуется победителем первого этапа и Организатором индивидуально. Примерный перечень мероприятий и изданий для публикации работ приведен в Приложении 3 к настоящему Положению.

3.3 Второй (заключительный) этап Конкурса проводится в период с 1 апреля 2014 года по 15 декабря 2014 года. Заявки на участие во втором этапе Конкурса принимаются Оргкомитетом до 30 ноября 2014 года включительно.

- Во втором этапе Конкурса могут принять участие работы:
  - принимавшие участие в первом этапе Конкурса и опубликованные или принятые к публикации на момент подачи заявки;
  - опубликованные на момент подачи заявки работы по тематике Конкурса, не участвовавшие в первом этапе.
- Оценку научной значимости выдвинутых работ производит Конкурсная комиссия с учетом мнения широкой научной общественности, сложившегося после публикации результатов. Ранжирование представленных работ осуществляется каждым экспертом Конкурсной комиссии независимо.
- По результатам индивидуальных оценок Конкурсная комиссия вырабатывает согласованное решение о присуждении первых и вторых премий призерам всего Конкурса. Всего может быть присуждено не более 2-х первых премий и не более 2-х вторых. Протокол заседания Конкурсной комиссии с утвержденным списком призеров Конкурса передается в Оргкомитет Конкурса для организации награждения.
- Размер первой и второй премии установлен в 500 000 (пятьсот тысяч) рублей и 300 000 (триста тысяч) рублей соответственно.

- В случае присуждения премии авторскому коллективу денежное вознаграждение выплачивается авторам пропорционально личному творческому вкладу, указанному в соглашении, прилагаемому к заявке на участие в Конкурсе.
  В случае отсутствия соглашения о личном творческом участии между соавторами денежное вознаграждение делится поровну между соавторами.
  В случае отказа одного из соавторов участвовать в Конкурсе денежное вознаграждение распределяется среди соавторов, участвующих в Конкурсе, пропорционально их творческому вкладу.
  В случае смерти автора или кого-либо из соавторов, причитающееся ему денежное вознаграждение выплачивается его наследникам.
- Выплата премий осуществляется путем перечисления денежных средств на лицевые счета, открытые в кредитных учреждениях на имя призеров.
- Объявление результатов Конкурса производится до 15 декабря 2014 года на сайте Организатора, сайте Технического комитета ТК26, на общедоступных новостных и профильных ресурсах Интернета, рассылкой по электронной почте.
- Оповещение призеров Конкурса осуществляется Оргкомитетом заказным письмом и по электронной почте в соответствии с сообщенными ими контактными данными.

4 Правила участия в Конкурсе

4.1 К участию в конкурсе принимаются оригинальные завершенные работы на русском или английском языке.

4.2 В Конкурсе могут участвовать индивидуальные и коллективные научно-исследовательские работы. Количество соавторов в работе не ограничивается. Количество представленных работ от одного автора/соавтора не ограничивается.

4.3 Сотрудники Организатора Конкурса и члены коллектива разработчиков ГОСТ Р 34.11-2012 не могут принимать участие в Конкурсе в качестве авторов или соавторов работ.

4.4 Содержание работы, представляемой на Конкурс, должно соответствовать тематике Конкурса. Перечень направлений исследований приведен в Приложении 2 к настоящему Положению. Решение о соответствии темы работы тематике Конкурса принимает Конкурсная комиссия.

4.5 Работы, не соответствующие условиям настоящего Положения о Конкурсе, представленные с нарушением порядка оформления или поступившие после установленных сроков, Конкурсной комиссией не рассматриваются.

4.6 В первом этапе Конкурса могут принять участие только не публиковавшиеся ранее в рецензируемых изданиях работы. Краткие тезисы и уже опубликованные работы в первом этапе Конкурса не участвуют.

- Работы, предоставляемые на первый этап Конкурса, не должны содержать сведений, составляющих государственную и/или иную охраняемую законом тайну, и нарушать авторские права на интеллектуальную собственность третьих лиц.
- Выдвигаемые на первый этап Конкурса работы должны быть оформлены по общепринятым для научных публикаций правилам.
- Работы на первый этап Конкурса предоставляются в печатном или электронном виде (файлы формата PDF). Работы, написанные от руки, на Конкурс не принимаются.

4.7 Во втором этапе Конкурса могут принять участие только работы, опубликованные или принятые к публикации в общедоступных профильных рецензируемых изданиях, включая электронные, не ранее 2010 года.

- Для работ, принимавших участие в первом этапе Конкурса, допускается доработка публикуемых материалов согласно требованиям организаторов конференций и симпозиумов и издателей. Если работа не опубликована, но принята к публикации, авторы должны предоставить Организатору соответствующее подтверждение.
- В качестве выдвигаемых работ, не участвовавших в первом этапе, могут быть заявлены монографии, статьи или циклы опубликованных статей в общедоступных периодических рецензируемых изданиях, или публикации в материалах международных конференций и симпозиумов.
- В случае наличия публикации только краткой версии (тезисов) работы, для участия во втором этапе Конкурса необходимо представить полную версию работы.
  При этом полная версия работы должна быть предоставлена в печатном или электронном виде (файлы формата PDF). Допускается, что тезисы и сама работа могут быть оформлены на разных языках (одно - на русском, другое – на английском).
- Несмотря на опубликование в общедоступных источниках Оргкомитет имеет право потребовать от авторов предоставление текста конкурсной работы.

4.8 Направленные на конкурс материалы не возвращаются. Рецензия на работу предоставляется только победителям первого этапа Конкурса.

4.9 Гражданство участников Конкурса не имеет значения.

4.10 Участие можно принимать по выбору как в обоих этапах Конкурса, так и в отдельных этапах.

4.11 Участие в любом этапе Конкурса не ограничивает авторов в возможности публикации их работ по собственному усмотрению.

4.12 Для участия в любом из этапов Конкурса необходимо зарегистрироваться на сайте Конкурса и заполнить электронную заявку и приложить соответствующие документы не позднее даты окончания приема заявок соответствующего этапа.

4.13 Допускается подача письменной заявки с работой в печатном и электронном виде и иными сопутствующими материалами. Такая заявка должна быть отправлена в адрес Организатора по почте заказным письмом не позднее даты окончания приема заявок соответствующего этапа. В случае отправки материалов по почте дата подачи заявки определяется по почтовому штемпелю отправления.

4.14 Для коллективных работ форма заявки должна быть заполнена каждым соавтором.

4.15 К коллективной заявке может быть приложено соглашение о доли личного творческого вклада каждого из соавторов в свободной форме. При отсутствии такого соглашения личный творческий вклад всех соавторов считается одинаковым.
Если выдвигаемая работа выполнена одним автором, соглашения о его творческом вкладе не требуется.

5 Авторские права и персональные данные

5.1 Интеллектуальные и иные права на результаты исследований остаются за авторами подаваемых на Конкурс работ.

5.2 В соответствии с Федеральным законом от 27.07.2006 года «О персональных данных» № 152-ФЗ авторам конкурсных работ гарантируется конфиденциальность персональных данных. Организатор Конкурса принимает необходимые

организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

К персональным данным относятся:

- паспортные данные;
- информация о месте работы и должности;
- сведения о научных степенях и званиях;
- данные о личном творческом вкладе (для работ в соавторстве);
- номера банковских счетов призеров Конкурса;
- контактная информация (номера домашних и мобильных телефонов, адреса личной электронной почты и т.д.), добровольно сообщаемая участниками.

5.3 Подачей заявки на участие в Конкурсе авторы подтверждают:

- принятие условий Конкурса, описанных в настоящем Положении;
- отсутствие сведений, составляющих государственную и иную охраняемую законом тайну, в предоставляемых материалах на Конкурс;
- что их участие в Конкурсе не нарушает авторские права на интеллектуальную собственность третьих лиц.

6 Контакты

Организатор конкурса – Открытое акционерное общество «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Почтовый адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1.

Телефоны/Факс: +7-(495)-737-61-92, 737-6193 / 737-72-78.

Интернет-адреса: www.streebog.info, www.infotecs.ru, www.tc26.ru.

Контактное лицо: Сериков Игорь Анатольевич.

E-mail: serikov@infotecs.ru.

Приложения

Приложение 1. Оргкомитет Конкурса

Председатель Оргкомитета: Чапчаев А. А.

Члены Оргкомитета:
Гусев Д. М.;
Звейник Е. В.;
Иванов А. Г.;
Лунин А. В.;
Науменко А. П.;
Сериков И. А.;
Смирнов Н. В.;
Степанович С. В.;
Уривский А. В.

Приложение 2. Перечень тем исследований

К участию в Конкурсе принимаются работы на русском или английском языке, посвященные решению хотя бы одной из следующих задач для хотя бы одной из следующих функций $f(IV, M)$ со значениями в V_n.

Функции

1. Функции хэширования, определяемые ГОСТ Р 34.11-2012. В этом случае $n = 256$ или $n = 512$, значения $IV \in V_{512}$ фиксированы и определены в п. 5.1 стандарта, если не оговорено противное, и $M \in V^*$.
2. Функции хэширования, определяемые ГОСТ Р 34.11-2012, без завершающих или одного из завершающих преобразований (шаги 3.3.-3.6). В этом случае, так же, как в предыдущем, $n = 256$ или $n = 512$, значения $IV \in V_{512}$ фиксированы и определены в п. 5.1 стандарта, если не оговорено противное, и $M \in V^*$.
3. Функции сжатия функций хэширования, определяемых ГОСТ Р 34.11-2012. В этом случае $n = 512$, значение $IV \in V_{512}$ произвольно и фиксировано, если не оговорено противное, и $M \in V_{512}$.
4. Усечённые (round-reduced) варианты указанных выше функций, т.е. соответствующие использованию в преобразовании $E(K, m)$ меньшего числа преобразований $LPSX$, чем определено в ГОСТ Р 34.11-2012.

Задачи

1. Обращение (построение прообраза, preimage attack). По заданному значению $h \in V_n$ найти значение M такое, что $f(IV, M) = h$.
2. Построение коллизии. Найти два различных значения M и M' такие, что $f(IV, M) = f(IV, M')$.
3. Построение второго прообраза (second preimage attack). По заданному значению M найти отличное от M значение M' такое, что $f(IV, M) = f(IV, M')$.
4. Построение псевдо-прообраза (pseudo-preimage attack). По заданному значению $h \in V_n$ найти значения IV и M такие, что $f(IV, M) = h$.
5. Построение условно-свободной коллизии (collision attack for different IV, semi-free-start collision attack). Найти значение IV и два различных значения M, M' такие, что $f(IV, M) = f(IV, M')$.
6. Построение псевдо-коллизии (pseudo-collision attack, free-start collision attack). Найти два значения IV, IV' и два различных значения M, M' такие, что $f(IV, M) = f(IV', M')$.
7. Построение второго псевдо-прообраза (second pseudo-preimage attack, free-start target attack). По заданному значению M найти значение IV' и отличное от M значение M' такие, что $f(IV, M) = f(IV', M')$.
8. Построение мульти-коллизии (построение *r*-коллизии). Найти попарно различные значения $M_1, \ldots, M_r$ такие, что $f(IV, M_1) = \ldots = f(IV, M_r)$
9. Построение мульти-прообраза (построение *r*-прообраза). По заданному значению $h \in V_n$ найти попарно различные значения $M_1, \ldots, M_r$ такие, что $f(IV, M_1) = \ldots = f(IV, M_r) = h$.

10. Построение второго мульти-прообраза (построение второго *r*-прообраза). По заданному значению M найти отличные от M и попарно различные значения $M_1,\ldots,M_r$ такие, что $f(IV,M_1)=\ldots=f(IV,M_r)=f(IV,M)$.
11. Построение почти-прообраза. По заданному значению $h\in V_n$ найти значение M такое, что сумма $f(IV,M)\oplus h$ имеет небольшой вес Хэмминга.
12. Построение почти-коллизии (near-collision attack). Найти два различных значения M и M' такие, что сумма $f(IV,M)\oplus f(IV,M')$ имеет небольшой вес Хэмминга.
13. Построение второго почти-прообраза. По заданному значению M найти отличное от M значение M' такое, что сумма $f(IV,M)\oplus f(IV,M')$ имеет небольшой вес Хэмминга.
14. Расширение сообщения (length-extension attack, только для функций хэширования и их усеченных вариантов). По заданным значениям $|M|$, $f(IV,M)$ найти некоторое значение M', для которого вычислить $f(IV,M\|M')$.
15. Построение прообраза при заданном префиксе сообщения и заранее выбранном значении функции (chosen target force prefix, CTFP, Nostradamus attack, только для функций хэширования и их усеченных вариантов). Задача состоит из двух этапов. На первом этапе требуется построить и предъявить некоторое значение $h\in V_n$. На втором этапе по заданному значению *M*, выбираемому из некоторого заранее известного множества значений, требуется найти такое значение M', что $f(IV,M\|M')=h$.
16. Построение алгоритма различения (distinguishing attack). Построить алгоритм, позволяющий отличить функцию $f(IV,M)$ от случайно и равновероятно выбранной функции.

Приложение 3. Примерный перечень профильных конференций, симпозиумов и периодических изданий для публикации работ

Мероприятия:

- Российско-Белорусская конференция «Комплексная защита информации»;
- CRYPTO - International Cryptology Conference;
- EUROCRYPT - International Conference on the Theory and Applications of Cryptographic Techniques;
- ASIACRYPT - International Conference on the Theory and Application of Cryptology and Information Security;
- FSE - Fast Software Encryption;
- CHES - Cryptographic Hardware and Embedded Systems;
- PKC - International Conference on Practice and Theory in Public Key Cryptography;
- SAC – Selected Areas in Cryptography;
- IEEE Symposium on Security and Privacy;
- IEEE Symposium on the Foundations of Computer Science (FOCS);
- ACM-STOC – ACM Symposium on Theory of Computing;
- ACM-CCS – ACM Computer and Communication Security;
- ESORICS – European Symposium on Research in Computer Security;
- ACISP – Australasian Conference on Information Security and Privacy;
- FC – Financial Cryptography and Data Security;
- ICISC – International Conference on Information Security and Cryptography;
- LATINCRYPT – International Conference on Cryptology and Information Security in Latin America;
- INDOCRYPT – International Conference on Cryptology;
- AFRICACRYPT – International Conference on the Theory and Applications of Cryptology;
- INSCRYPT – China International Conference on Information Security and Cryptology;
- CECC – Central European Conference on Cryptology;
- SECRYPT – International Conference on Security and Cryptography;
- TCC – Theory of Cryptography Conference;
- CBC – Code-based Cryptography;

Периодические издания:

- Springer Journal of Cryptology;
- Springer Cryptography and Communications;
- Springer Designs, Codes and Cryptography;
- Springer International Journal of Information Security;
- Springer Combinatorica;
- Elsevier Discrete Applied Mathematics;
- Elsevier Journal of Computer and System Sciences (JCSS);

- Elsevier Journal of Discrete Algorithms;
- Elsevier Computer Communications;
- Elsevier Information and Computation;
- Journal of the ACM;
- Communications of the ACM;
- IEEE Transactions on Information Theory;
- IEEE Transactions on Computers;
- IEEE Security & Privacy;
- IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences;
- IEICE Transactions on Information and Systems;
- SIAM Journal on Computing.