УДК 004.056.53

САИДРЕЗА МАХМАЛИ

РЕАЛИЗАЦИЯ СХЕМЫ ИДЕНТИФИКАЦИИ FFSIS НА ОСНОВЕ УМНОЖЕНИЯ БЕЗ ПЕРЕНОСОВ

В статье представлен новый вариант реализации основанной на концепции нулевых знаний схемы идентификации Фейге-Фиата-Шамира (FFSIS), которая ориентирована на идентификацию абонентов многопользовательских систем или терминальный устройств. Предлагаемая модификация FFSIS состоит в использовании математической операции умножения без переносов на полях Галуа вместо модулярного умножения. Это позволяет повысить скорость выполнения процедуры идентификации как при программной, так и при аппаратной реализации. Изложена технология использования умножения без переносов для реализации FFSIS. Приведен численный пример реализации FFSIS с использованием умножения на полях Галуа. Выполнено аналитическое сравнение времени выполнения FFSIS для предложенного варианта реализации и известного, которое показало достигаемые преимущества.

In article the new variant of zero-knowledge FFSIS (Feige Fiat Shamir Identification Scheme) implementation fitted to identification of remote abonents of multiuser systems or tample-resistant devices is presented. The proposed FFSIS modification consist of using of mathematical operation of multiplication without carry on Galois fields instead of modular multiplication. It allows to speed up of identification process for software and hardware implementation. The technology of multiplication without carry using for FFSIS implementation is set forth clearly. A numerical example for FFSIS procedure based on Galois field multiplication is given. An analytical comparison of the FFSIS processing time of both the proposed and known variants is presented, that demonstrates the improvements attained.

Введение

В современных условиях, когда информационная интеграция становится одним из решающих факторов прогресса во всех областях человеческой деятельности, проблема быстрой и надежной идентификации удаленных абонентов многопользовательских систем приобретает большое практическое значение.

Эффективное решение этой проблемы позволяет разрешить противоречие между возможностью получения информации и ограничением доступа к ней. Действительно, с развитием компьютерных технологий расширяется доступ к информации, что позволяет заметно повысить эффективность принятия решения во всех сферах человеческой деятельности. С другой стороны, расширение возможностей доступа к информации не должно сказываться на соблюдении базовых прав охраны закрытых данных государства, личности и организаций. Значительная часть данных, по своей сути, является продуктом, на получение которого затрачены ресурсы и, соответственно, эти данные имеют определенную стоимость, что обуславливает необходимость ограничения доступа к ним.

В современных условиях быстрого развития информационного общества, происходит актуализация проблемы надежной и быстрой идентификации. Это обусловлено тем, что с расширением использования интегрированных систем хранения и обработки данных, возрастает ценность потенциально доступной информации, расширяется арсенал средств незаконного доступа к ней, в том числе, за счет побочного влияния на работу подсистемы идентификации. Расширение использования беспроводных каналов передачи данных создает предпосылки для прослушивания обмена идентификационными посылками и подмены легальных абонентов во время сеанса. Все эти факторы диктуют необходимость адекватного повышения надежности идентификации, что практически всегда связано с усложнением криптографических процедур, лежащих в ее основе. С другой стороны, рост числа абонентов, опережающий темпы увеличения производительности вычислительных средств, требует повышения скорости идентификации. Выход может быть найден только за счет создания новых методов и средств идентификации, позволяющих эффективно разрешать противоречие между надежностью и производительностью.

Часто в качестве терминальных устройств абонента выступают малоразрядные портативные микроконтроллеры (смарт-карты), для которых проблема вычислительной сложности процедур идентификации стоит особенно остро.

Таким образом, в современных условиях быстрого роста информационной интеграции, задача разработки новых и совершенствования известных методов идентификации является актуальной и важной для практики.

Идентификация на основе концепции нулевых знаний. Алгоритм FFSIS

В современных условиях объективно происходит расширение возможностей для несанкционированного доступа к закрытым информационным ресурсам интегрированных систем за счет нарушения процедур идентификации.

Как уже отмечалось выше, расширение использования беспроводных технологий передачи данных позволяет злоумышленнику активнее вмешиваться в процесс идентификации. В частности, в беспроводных линиях облегчается перехват злоумышленником пароля легального абонента, а также его подмена после проведения сеанса идентификации. Классическим средством противодействия подмене является периодическое повторное проведение сеансов идентификации в процессе взаимодействия системы с абонентом. Для этого процедура идентификации должна выполняться быстро.

Еще одним путем нарушения процессов идентификации является побочное направленное вмешательство в работу системы легальными пользователями, а также посредством вирусов или недобросовестного персонала. Для широкого класса коммерческих многоабонентных систем важным является исключение возможности имитации системой обращения пользователя.

Исходя из указанных обстоятельств, современные средства идентификации абонентов должны удовлетворять следующим требованиям [1]:

1) Идентифицирующая информационная посылка (пароль) должна меняться при каждом обращении к системе, при этом используемые пароли должны быть статистически независимыми;

2) Длина пароля должна полностью исключать возможность его подбора перебором;

3) Информация, хранящаяся в системе не должна быть достаточной для воспроизведения пароля абонента;

4) Процедура идентификации должна выполняться достаточно быстро.

В литературе [2] методы идентификации, удовлетворяющие первым трем из приведенных требований называют “строгими”, в противовес остальным, которые называются “слабыми”. К классу последних относится, например, процедура идентификации, используемая в операционной системе UNIX [2]. Эта процедура предусматривает сохранение в системе только хеш-образов паролей пользователей, что, при использовании необратимых хеш-преобразований, исключает возможность воспроизведение пароля системой; однако сами пароли не меняются, что позволяет достаточно просто их перехватить.

К классу “строгих” процедур относятся, большей частью, методы идентификации, в основе которых лежит концепция “нулевых знаний”. Наиболее известным из них является метод FFSIS (Feige Fiat Shamir Identification Scheme) [2]. FESIS представляет собой относительно простую и вместе с тем достаточно эффективную схему идентификации абонентов многопользовательских систем, на основе которой создано ряд имеющих практическое значение модификаций [3]. В плане практического использования основным недостатком FFSIS считается необходимость в большом числе обменов данными в процессе идентификации, что заметно нагружает линии передач.

Другие схемы идентификации, реализующие концепцию “нулевых знаний”, предложенные в [4,5] требуют существенно меньшего объема пересылок, но предусмотренные ими процедуры имеют большую вычислительную сложность, поскольку вместо операции возведения в квадрат, в них используются операции модулярного экспоненцирования.

Сущность FESIS состоит в следующем.

Посредник (абонент) выбирает два простых числа p и q, вычисляет модуль $m=p\cdot q$. Для генерации открытого и закрытого ключей посредник(абонент) выбирает число v, являющееся квадратичным вычетом по модулю m. Другими словами, выбирается v, для которого существует x такое, что $d^2 \bmod m = v$ и существует v^{-1} такое, что $v\cdot v^{-1} \bmod m = 1$. Затем вычисляется наименьшее s для которого выполняется: $s^2 \bmod m = v^{-1}$. Число v является открытым, а число s – закрытым ключом.

При регистрации абонент посылает в систему свой открытый ключ – число v.

В цикле идентификации абонент выбирает случайное число r и вычисляет значение $x = r^2 \bmod m$, вычисленное значение x отсылает в систему. Система инициирует выполнение t циклов аккредитации. В каждом цикле аккредитации выполняются следующие действия:

1) Система посылает абоненту случайный бит b.

2) Если b=0, то абонент посылает в систему число r, в противном случае, если b=1, то абонент вычисляет с использованием закрытого ключа s значение $y = r \cdot s \bmod m$ и отсылает его системе.

3) Если b=0, то система проверяет $x = r^2 \bmod m$, в противном случае, если b=1, проверяется, что $x = y^2 \cdot v \bmod m$, убеждаясь, что абонент знает $s = \sqrt{v^{-1}}$, поскольку,

$$y^2 \cdot v \bmod m = (r^2 \cdot (\sqrt{v^{-1}})^2 \cdot v) \bmod m =$$

$$= (r^2 \cdot v^{-1} \cdot v) \bmod m = r^2 \bmod m = x$$

Если злоумышленник знает открытый ключ v легального абонента, то он может подобрать любое g и вычислить $g^2 \cdot v \bmod m = \xi$; послать системе ξ в качестве x. Если посланный в ответ системой случайный бит b=1, то злоумышленник вместо y пересылает системе код g. Соответственно, система вычисляет $g^2 \cdot v \bmod m$, сравнивает с ξ, получая при этом положительный результат сравнения. Однако, при b=0 злоумышленник должен отправить системе код $g^2 \bmod m \neq \xi$, то есть выявить попытку подделки. Если злоумышленник пошлет в качестве x код $g^2 \bmod m$, то пройдет тест при b=0, но не пройдет при b=1.

Очевидно, что идентификация с положительным результатом достижима только в случае, если злоумышленник подобрал закрытый ключ s. Решение этой задачи эквивалентно отысканию значения v^{-1} по известному v.

Наиболее значительными недостатками описанного варианта схемы идентификации FFSIS являются: необходимость в нескольких циклах аккредитации и низкое быстродействие, обусловленное тем, что на каждом цикле аккредитации необходимо выполнять три операции модулярного умножения над многоразрядными числами. Особенно ощутимым этот недостаток становится, если в качестве терминальных устройств абонентов выступают портативные контроллеры (смарт-карты), в которых выполнение операции модулярного умножения занимают много времени.

Целью исследований является созданий модификации алгоритма FFSIS, обладающей меньшей вычислительной сложностью и позволяющей повысить скорость идентификации при программной и аппаратной реализации.

Реализация схемы идентификации FFSIS На основе алгебры полей Галуа

Существенное упрощение вычислений, связанных с реализацией схемы идентификации FFSIS может быть достигнуто за счет ее реализации в алгебре без межразрядных переносов и заемов. К числу последних относится алгебра полей Галуа. В последние годы эта алгебра широко используется в кодировании и защите информации. Одним из важных ее достоинств является то, что реализация ее базовых вычислительных операций: умножения, сложения и модулярной редукции выполняется существенно быстрее по сравнению с классическими операциями умножения, сложения и нахождением остатка.

В алгебре полей Галуа операция суммирования фактически соответствует логическому сложению (XOR). Операция умножения выполняется без межразрядных переносов и ниже обозначается знаком $\otimes$.

Произведение без межразрядных переносов $D=U \otimes V=\{d_{2 \cdot r},\ldots,d_3,d_2,d_1\}=d_1+2 \cdot d_2+4 \cdot d_3+\ldots+2^{2 \cdot r} \cdot d_{2 \cdot r}$, $\forall l \in \{1,..,2 \cdot r\}$: $d_l \in \{0,1\}$ двух r-разрядных чисел $U=\{u_r,\ldots,u_2,u_1\}=u_1+2 \cdot u_2+\ldots+2^r \cdot u_r$ и $V=\{v_r,\ldots,v_2,v_1\}=v_1+2 \cdot v_2+\ldots+2^r \cdot v_r$, $\forall i \in \{1,..,r\}$: $v_i,u_i \in \{0,1\}$ вычисляется следующим образом:

$$D = U \cdot v_1 \oplus (U \cdot v_2) << 1 \oplus \ldots \oplus (U \cdot v_r) << (r-1), \quad (1)$$

где $\cdot$ – операция логического умножения, $p<<q$ – операция логического сдвига числа p влево на q разрядов.

Сущность предлагаемой реализации схемы идентификации FFSIS в алгебре полей Галуа состоит в следующем.

На этапе регистрации абонентом (посредником) выполняется генерация открытого и закрытого ключей выбранной разрядности – n. Для этого выбирается простое в рассматриваемой алгебре (n+1)-разрядное число m. Например, если в порядке иллюстрации положить малую разрядность n=4, то можно выбрать в качестве модуля 5-разрядное $m=11001_2=25$.

Далее, абонент произвольно выбирает целое (n-1)-разрядное число η, после чего выполняется разложение (2·n-1)-разрядного числа $\eta \otimes m \oplus 1$ на n-разрядные множители d и s так, что $d \otimes s = \eta \otimes m \oplus 1$. Например, если η=4 и m=25, то $\eta \otimes m \oplus 1=101=9 \otimes 13$. Соответственно, d=9 и s=13. После этого вычисляются $v=d^2 \bmod m$ и $v^{-1} = s^2 \bmod m$; очевидно, что $v \cdot v^{-1} \bmod m = 1$. В рамках рас-

сматриваемого примера v=(9⊗9) mod m =14 и v^{-1} = (13⊗13) mod m = 7;

Число v является открытым, а число s – закрытым ключом.

При регистрации абонент посылает в систему свой открытый ключ – число v. v=14

При идентификации абонент случайным образом генерирует r, например, r=10; вычисляет d = (r^2) mod m и посылает вычисленное значение d в систему. Для примера d=10⊗10 mod 25 = 11. После этого вычисляет y=(r ⊗s) mod m и значение y также отсылает в систему. y=10⊗13 mod 25 = 15.

По получении указанных кодов, система, в соответствии со схемой FFSIS, инициирует выполнение t циклов аккредитации. В каждом цикле аккредитации выполняются следующие действия:

1) Система посылает абоненту случайный бит b.

2) Если b=0, то абонент посылает в систему число r, в противном случае, если b=1, то абонент вычисляет с использованием закрытого ключа s значение $y = r⊗s$ mod m и отсылает его системе.

3) Если b=0, то система проверяет справедливость $d = r^2$ mod m, в противном случае, если b=1, проверяется, что $d = y^2⊗v$ mod m, убеждаясь, что абонент знает $s = \sqrt{v^{-1}}$.

Например, пусть b=1 и абонент вычисляет значение y=(r ⊗s) mod m =10⊗13 mod 25 = 15 и значение y отсылает в систему. Система, получив, y = 15, вычисляет с использованием закрытого ключа v=14 z = 15⊗15⊗14 mod 25 =11. Поскольку z=11=d, то тест считается пройденным.

Если b=0, то абонент посылает в систему число r=10; $z = r^2$ mod m = 10⊗10 mod 25 = 11 и сравнивает его с ранее полученным значением d=11.

Таким образом, показано, что схема идентификации FFSIS работает при ее реализации в алгебре полей Галуа.

Оценка эффективности реализации FFSIS на полях Галуа

При программной реализации модулярного умножения n-разрядных чисел на w-разрядном процессоре, числа разбиваются на s фрагментов (s=n/w). Каждый фрагмент множителя умножается на каждый фрагмент множимого с формированием 2·w-разрядного произведения. Полученные произведения суммируются. Таким образом, при умножении n-разрядных чисел на w-разрядном процессоре общее число операций умножения w-разрядных чисел составляет s^2, а операций арифметического суммирования – $2 \cdot s^2$. Поскольку каждая из операций арифметического суммирования с вероятностью 0.5 сопровождается возникновением переноса, для учета которого необходимо повторно выполнять операцию инкрементирования (суммирования), то общее число операций сложения составляет $3 \cdot s^2$.

Нахождение остатка от деления n-разрядных чисел на w-разрядном процессоре выполняется весьма неэффективно: фактически n раз выполняется операция сравнения (вычитания) из произведения сдвигаемого модуля. При этом, в каждом из n циклов выполняется, в среднем, 1.5·s операций арифметического вычитания и s операций сдвига.

Таким образом, при программной реализации модулярного умножения на современных процессорах, время модулярного умножения $T_{мм}$ определяется следующим выражением:

$$T_{mm} = s^2 \cdot t_m + 1.5 \cdot s \cdot (2 \cdot s + n) \cdot t_a + n \cdot s \cdot t_S \qquad (2)$$

где t_m – время выполнения команды умножения, t_a – время выполнения команды арифметического сложения (вычитания), t_s – время выполнения команды сдвига. Согласно [6], команда умножения в современных процессорах занимает 10 тактов, арифметического сложения – 3 такта, сдвига – 1 такт, так, что формула (2) в оценочном плане может быть преобразована к виду:

$$T_{mm} \approx (19 \cdot s^2 + 5.5 \cdot s \cdot n) \cdot \tau \,, \qquad (3)$$

где τ – длительность такта.

При реализации операции умножения без переносов n-разрядных чисел на w-разрядном процессоре, числа также разбиваются на s фрагментов (s=n/w). Организуется поразрядная обработка n разрядов множителя, причем в каждом из n циклов выполняется логический сдвиг s фрагментов множимого и с половинной вероятностью осуществляется s операций логического суммирования. Нахождение остатка при полиномиальном делении полученного 2·n-произведения на образующий полином требует цикла последовательной обработки n старших разрядов полученного произведения. На каждом цикле выполняется операция сдвига кода образующего полинома и, с половинной вероятностью – s операций логического суммирования. Таким образом, время выполнения умно-

жения без переноса равно времени нахождения остатка (редуцирования), так, что суммарное время T_{mG} программной реализации умножения на поле Галуа над n-разрядных чисел на w-разрядном процессоре определяется формулой:

$$T_{mG} = 2 \cdot n \cdot s \cdot (0.5 \cdot t_X + t_S), \qquad (4)$$

где t_x – время выполнения команды логического сложения (XOR), которое согласно данным [6] занимает один такт, так, что в оценочном плане формула (4) может быть представлена в виде:

$$T_{mG} \approx 3 \cdot n \cdot s \cdot \tau. \qquad (5)$$

Сравнение выражений (4) и (5) свидетельствует о том, что время программной реализации операции умножения на поле Галуа, по меньшей мере, в 5.5/3 = 1.83 меньше времени модулярного умножения при одинаковой разрядности модуля и степени образующего полинома поля Галуа. Например, при n=1024 w=32 s=32 $T_{mm} = (19 \cdot 32^2 + 5.5 \cdot 32^3) \cdot \tau = 199680 \cdot \tau$, а $T_{\text{mG}} = 3 \cdot 32^3 \cdot \tau = 98304$, так, что соотношение времен программной реализации модулярного умножения и умножения на поле Галуа составляет:

$$h = \frac{T_{mm}}{T_{mG}} = \frac{199680}{98304} \approx 2 \qquad (6)$$

Ускорение программной реализации достигается за счет двух факторов: увеличении двое числа операций процессорного сложения из-за необходимости учета возникающих переносов; увеличения вдвое числа операций вычитания (сравнения).

При использовании в качестве терминальных устройств абонентов 8-разрядных смарт-карт, сокращение времени умножения при переходе к алгебре на полях Галуа получается еще более значительным. Так, при n=1024 w=8 s=128 $T_{mm} = (19 \cdot 128^2 + 5.5 \cdot 1024 \cdot 128) \cdot \tau = 1032192 \cdot \tau$, а $T_{\text{mG}} = 3 \cdot 1024 \cdot 128 \cdot \tau = 311296$, так, что соотношение времен программной реализации модулярного умножения и умножения на поле Галуа для смарт-карт составляет:

$$h = \frac{T_{mm}}{T_{mG}} = \frac{1032192}{311296} \approx 2.65. \qquad (7)$$

Практически, поскольку, при проведении цикла аккредитации выполняется две операции модулярного умножения, то переход к алгебре на полях Галуа позволяет примерно в 4 раза ускорить процесс идентификации. Проведенные экспериментальные исследования, в основном, подтвердили приведенные теоретические оценки. При аппаратной реализации, переход от модулярного умножения в традиционной алгебре к умножению на полях Галуа сопряжен с существенно большим выигрышем как в плане быстродействия, так в плане сложности схемы.

Базовой операцией модулярного умножения является арифметическое сложение, выполняемое над n-разрядными числами. Учет возникающего при сложении переноса выполняется путем выполнения еще одной операции сложения над n-разрядными числами, так, что каждое сложение реально требует выполнения, в среднем, 1.5 операций. При последовательном выполнении переноса время суммирования T_{as}, в оценочном плане, равно $1.5 \cdot t_3$, где t_3 – время срабатывания схемы 3-х входового сумматора; поскольку это время равно $t_3 = 3 \cdot t$, где t – время срабатывания двухвходового логического элемента, то, можно полагать, в первом приближении, что время суммирования равно $T_{as} = 4.5 \cdot n \cdot t$. Сложность (количество двухвходовых логических элементов) схемы последовательного арифметического суммирования S_{as} равна $S_{as} = n \cdot s_3$, где $s_3 = 6$ – число логических элементов, требующихся для реализации 3-х входового сумматора, соответственно, $S_{as} = 6 \cdot n$. При использовании схем ускоренного переноса, время арифметического суммирования T_{ap} определяется в виде: $T_{ap} = 1.5 \cdot (t_3 + t_c)$, где t_c – максимальное время формирования сигнала переноса, которое составляет $\log_2 n \cdot t$. таким образом, $T_{ap} \approx 1.5 \cdot \log_2 n$. При этом сложность схемы формирования переносов, в оценочном плане, определяется как $6 \cdot n^3$. Время T_L выполнения базовой операции умножения на полях Галуа – логического сложения равно t, а сложность S_L соответствующей схемы – n.

Сравнительные оценки времени выполнения и сложности аппаратной реализации базовой операции сложения в традиционной алгебре и на полях Галуа приведены в таблице 1.

Табл. 1. Соотношение времени выполнение и сложности схемы при аппаратной реализации арифметического и логического сложения.

	$\frac{T_a}{T_L}$	$\frac{S_a}{S_L}$
Последовательное формирование переноса	$4.5 \cdot n$ при n=1024 : 4608	6 при n=1024 : 6
Ускоренное формирование переноса	$1.5 \cdot \log_2 n$ при n=1024 : 15	$6 \cdot n^2$ при n=1024 : 6144

Выводы

Предложен способ реализации широко известной процедуры FFSIS строгой идентификации удаленных абонентов многопользовательских систем в рамках концепции “нулевых знаний” на основе операций без переносов на полях Галуа. Доказано, что использование таких операций не влияет на уровень защищенности, но позволяет существенно упростить и ускорить вычислительные процедуры FFSIS. Приведенная технология использования операций умножения на полях Галуа иллюстрирована примером. Доказано, что при программной реализации применение предложенного подхода позволяет, при практически используемых разрядностях чисел, примерно в 4 раза ускорить идентификации FFSIS.

Проведенными исследованиями показано, что при аппаратной реализации предложенный подход позволяет существенно ускорить процесс идентификации и заметно упростить схему. Так, если сравнивать предложенный вариант со схемой выполнения арифметических операций с последовательным переносом, предложенный подход позволяет ускорить процедуру идентификации в соответствии с FFSIS на три порядка. При сравнении со схемой с ускоренным переносом, предложенный вариант обеспечивает ускорение в 15 раз при том, что сложность схемы упрощается на 3 порядка.

Предложенный способ реализации процедуры FFSIS может быть использован для повышения эффективности идентификации как удаленных абонентов компьютерных сетей, так и для идентификации терминальный мобильных устройств (смарт-карт).

Список литературы

1. Bardis N., Doukas N. and Markovskyi O., Fast subscriber identification based on the zero knowledge principle for multimedia content distribution // International Journal of Multimedia Intelligence and Security.- 2010 - Vol.1.- № 4. - P. 363 - 377.
2. Feige U., Fiat A., Shamir. Zero Knowledge Profs of Identity // Journal of Cryptography.- 1988.- v.1- № 2.- P.77-94.
3. Micali S., Shamir A. An Improvement on the Feige-Fiat-Shamir Identification and Signature Schemes // Advances of Cryptology -Crypto-88. Proceeding.- Springer-Verlag.-190.- P. 244-247.
4. Guillou L.C., Quisquater J.-J. A Paradoxical Identity-Based Signature Schemes Resulting from Zero Knowledge // Advances of Cryptology -Crypto-88. Proceeding.- Springer-Verlag.-1990.- P. 216-231.
5. Cocks C. An identity based encryption schemes based on quadratic residues // Proceeding of the 6-th International Conference on Cryptography and Coding. - IMA.Press.-2001.- P.26-28.
6. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы. - СПб.: Изд-во “БХВ-Петрербург”.- 2005.- 1328 С.