Обоснование выбранного прототипа для разработки алгоритма электронной цифровой подписи на основе алгебры параметров

Ахмедова О.П., к.т.н. (ГУП «UNICON.UZ»)

В данной статье формированы основные критерия для выбора алгоритма в качестве прототипа и обоснован выбор трех прототипов для разработки алгоритма электронной цифровой подписи на эллиптических кривых.

Мазкур мақолада алгоритмни прототип сифатида танлаш учун асосий мезонлар шакллантирилган ва эллиптик эгри чизиқларга асосланган электрон рақамли имзо алгоритмини ишлаб чиқиш учун танланган учта прототип асосланган.

This article form the main criterion for the selection algorithm as a prototype and substantiated choice of three prototypes for the development of digital signature algorithm for elliptic curves.

В настоящее время передовые страны мира в области информационной безопасности имеют криптографические алгоритмы электронной цифровой подписи (ЭЦП) на базе эллиптических кривых (ЭК), принятые на уровне государственных и международных стандартов. Примерами таких стран являются Соединенные Штаты Америки (EC-DSA) [1], Южная Корея (EC-KCDSA) [2] и Федеративная Республика Германии (EC-GDSA) [3]. В Российской Федерации, где с 2001 года успешно используется ГОСТ Р 34.10-2001 [4], ведутся работы по получению статуса международного стандарта алгоритму ЭЦП на основе ЭК. Алгоритмы ЭЦП лежат в основе систем электронного документооборота и играют ключевую роль в алгоритмическом и программном обеспечении системы электронного правительства любого государства.

В [5] отмечалось, что основным критерием выбора прототипа является стойкость и эффективность программной, аппаратной и аппаратно-программной реализации операций сложения и скалярного умножения в процессах генерации и проверки ЭЦП, которые главным образом зависят от используемой алгебраической структуры и выбранных системных параметров, в том числе ЭК, степени учета требований, направленных на обеспечение стойкости и быстродействия.

В принципе, прототипом могут являться все известные, используемые в настоящее время алгоритмы ЭЦП на ЭК. Среди них следует отдать предпочтение в первую очередь алгоритмам, которые приемлемы для встраивания дополнительного секрета, и отнесены к категории государственных, международных стандартов, и успешно эксплуатируются в течение большого промежутка времени.

В предлагаемом алгоритме будет исследованы пути встраивания новых секретов в одностороннюю функцию на ЭК с целью определения новых

вычислительно-сложных проблем. Таким образом, основными критериями для выбора алгоритма в качестве прототипа являются:

1) признак пригодности к встраиванию дополнительного секрета в уравнение ЭК;

2) категория (статус) алгоритма;

3) оценка стойкости;

4) производительность процедур определения порядка подгруппы группы точек ЭК;

5) влияние процессов генерации и проверки ЭЦП на стойкость.

По первому критерии. Как отмечалось в [5-6], в эллиптической криптографии в основном используются ЭК следующих видов:

- над полем *F(p),* где простое число *p>3,* и над расширением простого поля $F(p^m)$;

- *несуперсингулярная* ЭК над полем $F(2^m)$;

- *суперсингулярная* ЭК над полем $F(2^m)$.

Во всех случаях необходимо быть уверенным в существовании в группе элементов большого порядка [5-6].

Как отмечалось в [5-6] в целях уменьшения вычислительной сложности преобразований в группах точек ЭК иногда используются специфичные кривые, например кривые Коблица. Коэффициенты кривых Коблица над $F(2^m)$ принадлежат полю *F(2).* Так как $b \neq 0$, то существуют два вида таких кривых:

$$ЭК_0: y^2+xy=x^3+1, \quad (1)$$
$$ЭК_1: y^2+xy=x^3+x^2+1, \quad (2)$$

которые позволяют ускорить вычисление скалярных произведений, доминирующих в процессах генерации и верификации ЭЦП на ЭК.

Имея в виду, что разрабатываемый алгоритм на ЭК будет базироваться на алгебре параметров с секретным параметром *R,* будет исключен из списка кандидатур в прототипы *несуперсингулярные и суперсингулярные* ЭК над полем $F(2^m)$, кривые Коблица вида *(1),(2).* Причиной этому служит то обстоятельство, что коэффициенты уравнения таких ЭК принимают значения *0* или *1* и в засекречивании их нет смысла. В работе ЭК над полем $F(2^m)$, отличающиеся от кривых Коблица также исключены из рассмотрения.

Таким образом, в списке кандидатов в прототипы остаются только ЭК над полем *F(p),* где простое число *p>3* и над расширением простого поля $F(p^m)$. Среди них и осуществляется выбор прототипов на основе критериев 2-5.

По второму критерию. Можно включить в список кандидатур алгоритмы ЭЦП на ЭК, имеющие категорию государственного, международного стандарта: ГОСТ Р 34.10-2001, EC-DSA-2000, EC-KCDSA, EC-GDSA и ДСТУ 4145-2002, и над простым полем *F(p),* и над расширением простого поля $F(p^m)$, анализированные в [5]. Анализ показал, что ДСТУ 4145-2002 имеет лишь одно отличие от ГОСТ Р 34.10-2001, заключающееся в использовании характеристики расширенного конечного поля Галуа. Данный алгоритм из списка кандидатур в прототипы исключается.

Как отмечалось в [5] на страницах Интернет [7] описана возможность подмены подписанного документа из-за имеющейся ошибки в EC-DSA-2000. Эта ошибка, по мнению А.В. Кобеца, вызвана равенством *x* координат противоположных точек ЭК $G_x == -G_x$, что приводит к тождествам

$$r_1=[k]G==r_2=[(q-1)k]G==r.$$

Если злоумышленнику необходимо подобрать одинаковую ЭЦП для хэш-значений e_1 и e_2 двух различных документов, то достаточно из равенства пары

уравнений для компоненты s определить личный ключ d, на основе которого формируются одинаковые ЭЦП для разных документов. Однако исправить эту ошибку несложно. Например, достаточно обеспечить доказательную генерацию личного ключа. Но тем не менее, данному алгоритму присущ еще один недостаток. В алгоритме используется операция обращения, как в процессе генерации, так и в процессе подтверждения подлинности ЭЦП, что не свойственно другим стандартам, из-за снижения производительности выполнения операций за счет этого. По этим двум причинам EC-DSA-2000 исключается из списка кандидатур в прототипы. Таким образом, для дальнейшего анализа в списке кандидатур в прототипы остаются ГОСТ Р 34.10-2001, EC-KCDSA, EC-GDSA.

По третьему критерию. Стойкость используемых алгоритмов определяется сложностью решения проблемы дискретного логарифма эллиптической кривой (ECDLP) на основе криптоанализа, которая зависит от длины в битах конечного поля, над которым задана ЭК. При этом предполагается, что системные параметры ЭЦП на ЭК успешно верифицированы. В таблице 1 приведены данные по сложностям криптоанализа ЭК.

Таблица 1 - Данные по сложностям криптоанализа

Длина модуля преобразований, bit	Сложность криптоанализа ЭК
192	$2^{95,82} \approx 10^{29,21}$
256	$2^{127,82} \approx 10^{39}$
512	$2^{255,82} \approx 10^{78}$
1024	$2^{511,82} \approx 10^{156}$

Следовательно, по третьему критерию (оценка стойкости) сравниваемые все три кандидатуры в прототипы имеют равные шансы.

По четвертому критерию. Определение числа точек на ЭК над конечным полем является важной составляющей процесса генерации системных параметров. Согласно [2-8] для того, чтобы предотвратить атаки на ECDLP Полиг-Хеллмана и Полларда, $rho \# PE(F_p)$ порядок группы точек должен быть делимым на достаточно большое простое число $n>2^{160}$. Тем самым $\# PE(F_p)$ станет равным hn, где n простое число, $h \in \{1,2,3,4\}$.

Для противостояния к изоморфным атакам должно соблюдаться неравенство $p \neq \# PE(F_p)$.

При этом, необходимо учесть, что соблюдение условия $n>4\sqrt{p}$ гарантирует существование уникальной подгруппы порядка n потому, что согласно теореме Хассе [2-8] $\# PE(F_p) \leq (\sqrt{p}+1)^2$ и n^2 не делит $\# PE(F_p)$. Вследствие этого существует только целое $h=\lfloor(\sqrt{p}+1)^2\rfloor$ в интервале Хассе.

Известный наивный алгоритм, заключающийся в вычислении для каждой x координаты точки числа решений для соответствующей y координаты точки уравнения ЭК, не приемлем для реальных ЭК над конечным полем, применяемых в эллиптической криптографии. Поэтому, эффективней пользоваться алгоритмами генерации ЭК с заданным порядком.

В эллиптической криптографии в основном используются следующие три метода для выбора ЭК с заданным порядком [5]:

1) метод кривых подполя;

2) метод Аткин-Морина (комплексного умножения конечных полей);

3) вычисление точек (Скуфф-Элкис-Аткина).

На основе известных методов, например, метода Аткин-Морина возможно генерировать на рабочей станции в течение одной минуты криптографически приемлемые ЭК. Следовательно, по четвертому критерию (производительность процедур определения порядка подгруппы группы точек ЭК) сравниваемые кандидатуры в прототипы имеют равные шансы.

По пятому критерию. В результате сравнительного анализа схем алгоритмов предпочтение было отдано стандарту международной категории EC-KCDSA, разработанному учеными Южной Кореи. При этом учитывались следующие отличительные особенности EC-KCDSA:

1) введение хэш-кода владельца ЭЦП в конкатенации с подписываемым сообщением при вычислении хэш-значения существенно снижает вероятность положительного исхода успешной экзистенциальной атаки;

2) компонента *r* ЭЦП вычисляется как значение хэш-функции точки *[k]G,* что повышает стойкость алгоритма ЭЦП за счет стойкости используемой хэш-функции;

3) в процессах генерации ЭЦП и проверки подлинности ЭЦП не используется трудоёмкая операция обращения чисел;

4) в алгоритме генерации ЭЦП содержится лишь один шаг возврата к шагу генерации случайного числа.

Остальные два кандидата в прототипы этими особенностями, положительно влияющими на стойкость и производительность алгоритма ЭЦП не обладают. Каждый из кандидатов EC-GDSA и ГОСТ Р 34.10-2001 содержит операцию обращения и два шага возврата к шагу генерации случайного числа, и имеют равные уровни по стойкости и производительности.

Анализ схем алгоритмов ЭЦП на базе ЭК показывает, что формальная замена прежних схем ЭЦП (в основном, модификаций схем Эль Гамаля) новыми произошла на основе двух алгебраических структур - конечной аддитивной группы точек ЭК и конечного поля *F(q),* где *q* - порядок группы для базовой (порождающей) точки *G* ЭК. При этом, алгебраическая операция возведения в степень определенной над элементом конечной мультипликативной группы поля заменена алгебраической операцией скалярного умножения (многократного сложения) элементов (точек) в конечной аддитивной группе точек ЭК. В схемах ЭЦП операции над элементами конечного поля оставались без изменений.

При одинаковой стойкости прежних и новых схем ЭЦП (соответственно, при прежних и новых размерностях характеристик полей), основной выигрыш состоит в повышении быстродействия и снижении требуемого объема памяти криптографического модуля, благодаря замене медленных операций возведения в степень быстродействующими операциями скалярного умножения точки на целое число и замене длинных ключей короткими ключами.

Следует отметить, что самая сложная в вычислительном отношении операция в формулах сложения – вычисление обратного элемента. Используя так называемое проективное представление точек ЭК, можно избавиться от этой операции за счет некоторого увеличения числа других операции.

Криптографические алгоритмы на ЭК строятся вполне аналогично алгоритмам на простых конечных полях. Фактически надо только возведение в степень по модулю заменить на скалярное произведение точки ЭК на целое число. При этом заменяется:

- порождающий элемент конечного поля *g* на порождающую (базовую) точку *G* ЭК;

- порядок порождающего элемента *q* на порядок порождающей точки *G* ЭК;

- личный ключ d на личный ключ d;

- открытый ключ $y=g^d \pmod p$, являющийся элементом конечного поля, на открытый ключ $Q = [d]G$, представляющий собой точку на ЭК.

Процесс составления алгоритма схемы ЭЦП на базе ЭК начинается со спецификации системных параметров и завершается схемами алгоритмов генерации и проверки ЭЦП.

При составлении схем ЭЦП в алгебре параметров за прототип можно выбрать:

1) прототип на ЭК без изменений;

2) прототип на ЭК с модификацией;

3) прототип не переведенный на эллиптический вариант.

При переходе на схемы на базе алгебры параметров процессы генерации и верификации ЭЦП можно осуществить в следующих вариантах:

- на основе неявной формы уравнения ЭК;

- на основе сокрытия или шифрования параметра, с использованием явной формы уравнения ЭК.

В данной статье для построения алгоритма ЭЦП на ЭК в алгебре параметров использована идея [9] по введению дополнительного секрета, а именно, параметра R в уравнение ЭК. В результате таких преобразований уравнение ЭК приобретает неявную форму из-за секретности параметра R, вследствие чего уровень стойкости алгоритмов увеличивается на несколько порядков.

В традиционных криптосистемах эллиптической криптографии коэффициенты уравнения ЭК являются открытыми и их засекречивание не оказывает ощутимого влияния на стойкость алгоритма. Данное обстоятельство становится возможным в связи с тем, что число открытых параметров в форме точек на ЭК станет равным числу коэффициентов уравнения ЭК, вследствие чего определение засекреченных коэффициентов уравнения ЭК не представляет никаких трудностей.

Например, при использовании уравнения ЭК в форме $y_0^2 \equiv x_0^3+ax_0+b \pmod p$ с засекреченными коэффициентами a, b и объявлении двух точек (x_{01}, y_{01}) и (x_{01}, y_{01}), одна из которых является базовой точкой, вторая - открытым ключом, коэффициенты a, b легко определяются из следующих сравнений:

$$a \equiv (y_{02}^2 - x_{02}^3 - y_{01}^2 + x_{01}^3)(y_{02}^2 - y_{01}^2)^{-1} \pmod p,$$

$$b \equiv -ax_{01} + y_{01}^2 - x_{01}^3 x_{01}^3 \pmod p.$$

В конечной коммутативной группе точек ЭК с параметром $(PE(F_n); +^{\backslash})$, благодаря закрытому параметру R, засекреченность коэффициентов a, B приводит к повышению стойкости криптосистемы по сравнению с традиционными криптосистемами.

Определение 1. Эллиптические кривые с закрытой тройкой параметров (R,a,B) называются неявными ЭК.

Проблема параметра неявной ЭК определяется следующим образом.

Определение 2. Если в группе $(PE(F_p); +^{\backslash})$ точек неявной ЭК (с закрытой тройкой параметров (R, a, B)) заданы порядок подгруппы группы точек q, базовая точка $G=(x_1, y_1)$ и x координата x_2 открытого ключа $Q=(x_2,y_2)$, удовлетворяющего равенству $Q=d*^{\backslash}G$, тогда найти d и тройку параметров (R, a, B), где уравнение ЭК с параметром имеет вид $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \pmod p$.

В настоящее время эффективный алгоритм решения данной проблемы отсутствует. Естественно предположить уровень сложности данной проблемы гораздо более высоким по сравнению с проблемой ECDLP.

Стойкость алгоритмов, основанных на использовании неявных ЭК, реализованных в виде аппаратного криптографического модуля (АКМ) [10], определяется сложностью решения проблемы параметра неявной ЭК.

Выводы:

1. Прототипами для построения алгоритмов ЭЦП на эллиптических кривых в алгебре параметров могут являться все известные, используемые в настоящее время алгоритмы. Среди них следует отдать предпочтение в первую очередь алгоритмам, которые отнесены к категории государственных, международных стандартов, успешно эксплуатируемым в течение длительного промежутка времени, которые обладают высокой степенью стойкости, производительностью процедур определения порядка подгруппы группы точек ЭК и процессов генерации и проверки ЭЦП.

2. В традиционных криптосистемах эллиптической криптографии коэффициенты уравнения ЭК являются открытыми, и их засекречивание не оказывает ощутимого влияния на стойкость алгоритма. В конечной аддитивной коммутативной группе точек ЭК с параметром $(PE(F_n); +^{\backslash})$, благодаря закрытому параметру R, засекреченность коэффициентов a,B приводит к повышению стойкости криптосистемы по сравнению с традиционными криптосистемами.

3. Стойкость алгоритмов, основанных на использовании неявных ЭК, реализуемых в виде АКМ определяется сложностью решения проблемы параметра неявной ЭК. В настоящее время эффективный алгоритм решения данной проблемы отсутствует. Естественно предположить уровень сложности данной проблемы гораздо более высоким по сравнению с проблемой дискретного логарифмирования на ЭК.

Литература

1 ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

2 D. Hankerson, A. Menezes, S. Vanstone Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.

3 ISO/IEC 15946-2:2002. Information technology – Security techniques – Cryptographic techniques based on elliptic curves.

4 ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

5 Отчет о НИР «Разработка алгоритма электронной цифровой подписи на эллиптических кривых на основе алгебры параметров», 2-этап, ГУП «UNICON.UZ», 2009.

6 Ахмедова О.П. Принципы построения алгоритмов электронной цифровой подписи на базе эллиптических кривых Ахбороткоммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №2, 2013.

7 Кобец А.М. Подмена подписанного документа в новом американском стандарте ЭЦП ECDSA// http: www.bugtrag/ru.

8 Алгоритмические основы эллиптической криптографии // Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А. – Москва МЭИ, 2000.

9 Хасанов Х.П. Криптографические системы на базе эллиптических кривых с параметром. Ахбороткоммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №4, 2008.

10 Патент РУз IAP 04445 «Способ создания аппаратного криптографического модуля» Приоритет от 14.05.2008 г. 30.11.2011, Бюл., №11. // Хасанов П.Ф., Махмудов М.М., Исаев Р.И., Хасанов Х.П., Ахмедова О.П., Расулов О.Х., Мукимов Ж.Д.