Об усложнении дискретного логарифмирования в полях характеристики 2

Валерий М. Максимов, Эдуард А. Применко

***Аннотация* — В реальных практических задачах, связанных с проблемами защиты информации, вычисления часто проводятся в полях характеристики 2. Современные вычислительные технологии, в частности, применение суперкомпьютеров, позволяют проводить вычисления для достаточно больших значений $m = 128, 256, 512$. С развитием вычислительной техники и разработкой новых методов анализа систем защиты информации приходится увеличивать параметр m. Кроме того, важно, чтобы вычисления, необходимые для обеспечения защиты информации легальным участникам информационного обмена, выполнялись за ограниченное время. В то же время для гипотетического злоумышленника, обладающего современными вычислительными ресурсами, взлом системы защиты должен быть невозможен за ограниченное время.**

Для построения циклических групп большого порядка, широко применяемых при синтезе криптографических протоколов, предлагается строить башни квадратичных расширений полей характеристики два. Устанавливается сложность построения таких расширений в зависимости от степени поля. В работе даётся метод построения квадратичного расширения полей $\mathcal{F}_2(m)$ со сложностью построения порядка $c \cdot m^4$, где c не зависит от m. Метод основан на построении двумерной алгебры с единицей над полем. Этот процесс удвоения степени поля можно продолжать и строить поля каждый раз в 2 раза большей степени. При этом не требуется строить неприводимые многочлены высших степеней.

***Ключевые слова* — DLP, задача дискретного логарифмирования, квадратичное расширение поля, примитивный элемент.**

I. Введение

В реальных практических задачах, связанных с проблемами защиты информации, вычисления часто проводятся в полях $GF(2^m) = \mathcal{F}_2(m)$, т.е. в полях характеристики 2. Современные вычислительные технологии, в частности, применение суперкомпьютеров, позволяют проводить вычисления для достаточно больших значений $m = 128, 256, 512$. С развитием вычислительной техники и разработкой новых методов анализа систем защиты информации приходится увеличивать параметр m. Так, например, в стандарте шифрования DES (1976 год) $m = 64$, а в ныне действующем стандарте шифрования $m = 128, 256$.

Кроме того, важно, чтобы вычисления, необходимые для обеспечения защиты информации легальным участникам информационного обмена, выполнялись за ограниченное время. В то же время для гипотетического злоумышленника, обладающего современными вычислительными ресурсами, взлом системы защиты должен быть невозможен за ограниченное время.

Для разрешения этой проблемы мы будем использовать важное условие на число m допускающим, что обладая вычислительными ресурсами для вычислений в поле $\mathcal{F}_2(m) = GF(2^m)$, например, для реализации задачи DLP (задача дискретного логарифмирования), предполагается невозможность эффективно реализовывать криптоалгоритмы в поле $\mathcal{F}_2(m \cdot (1 + \varepsilon)),\ \varepsilon > \varepsilon_0 > 0$.

В работе даётся метод построения квадратичного расширения полей $\mathcal{F}_2(m)$ со сложностью построения порядка $c \cdot m^4$, где c не зависит от m. Метод основан на построении двумерной алгебры с единицей над полем $\mathcal{F}_2(m)$. Эта алгебра будет полем $\mathcal{F}_2(2m)$, если для некоторого базисного элемента e, $e \neq \lambda \mathbb{1}$, где $\mathbb{1}$ – единица алгебры, $\lambda \in \mathcal{F}_2(m)$ с условием $e^2 = e + \alpha \mathbb{1}$, $\alpha \in \mathcal{F}_2(m)$, и многочлен $f = e^2 + e + \alpha$ неприводим над полем $\mathcal{F}_2(m)$. Этот процесс удвоения степени поля можно продолжать и строить поля степени $2^k \cdot m$. При этом не требуется строить неприводимые многочлены высших степеней.

В качестве примера рассмотрим задачу дискретного логарифмирования, на которой основаны современные стандарты ЭЦП.

Пусть G — группа, $a \in G$ и $ord(a) = N$. Возведение a в степень $n \leqslant N$ требует не более $T \leqslant 2\lfloor \log_2 N \rfloor$ групповых операций. Так, если $N = 2^{1000}$, то $T \leqslant 2000$. В то же время нет общего алгоритма решения задачи дискретного логарифмирования, т.е. решения уравнения $a^x = b$ в группе G, кроме полного перебора [3],[4],[8], за исключением специальных групп, например, группы точек эллиптической кривой, где есть более эффективные алгоритмы, чем полный перебор.

Современные криптографические стандарты построены на основе мультипликативной группы конечного поля или на основе группы точек эллиптической кривой над конечным полем. В работах [1],[2] исследовалась возможность построения некоммутативных групп большого порядка на основе конечных алгебр. В данной работе исследуется возможность построения групп большого порядка на основе квадратичного расширения конечного поля $GF(2^m) = \mathcal{F}_2(m)$. При таком подходе можно значительно усложнить решение задачи

Статья получена 15 августа 2018.

В.М. Максимов, Российский университет дружбы народов (РУДН), Российский государственный гуманитарный университет (РГГУ).
Э.А. Применко, Московский государственный университет имени М.В.Ломоносова.

дискретного логарифмирования для злоумышленника. Так, например, пусть $G = \mathcal{F}_2^*(2m) = GF^*(2^{2m})$, $a \in G,\ \mathrm{ord}(a) = 2^{2m} - 1$, т.е. a — примитивный элемент поля $\mathcal{F}_2(2m)$.

В этом случае, если злоумышленник может эффективно решать задачу дискретного логарифмирования в поле $\mathcal{F}_2(m)$, то решение этой задачи в поле $\mathcal{F}_2(2m)$ будет значительно сложнее. Например, если $p|(2^{2m}-1)$ и p — большое простое число, то эта задача практически неразрешима.

II. Построение алгебры $\mathcal{A}$ размерности 2 над полем

Рассмотрим алгебру $\mathcal{A}_2(m,\ \alpha)$ размерности 2 над полем $\mathcal{F}_2(m)$ с базисом $\mathbb{1}$ (единица поля $\mathcal{F}_2(m)$) и e, удовлетворяющему условию

$$e^2 = \alpha \cdot \mathbb{1} + e, \quad \alpha \in \mathcal{F}_2(m). \text{ (1)}$$

Таким образом,

$$\mathcal{A}_2(m,\ \alpha) = \{x\mathbb{1} + ye \mid x,\ y \in \mathcal{F}_2(m)\}.$$

Из (1) следует, что

$$\begin{cases} (x_1\mathbb{1} + y_1 \cdot e) + (x_2\mathbb{1} + y_2 \cdot e) = (x_1 + x_2)\mathbb{1} + (y_1 + y_2)e, \\ (x_1\mathbb{1} + y_1 e) \cdot (x_2\mathbb{1} + y_2 e) = \\ = (x_1x_2 + \alpha y_1y_2)\mathbb{1} + [x_1y_2 + y_1(x_2 + y_2)]e. \end{cases} \quad (2)$$

Выясним при каких условиях элемент $a = x_1\mathbb{1} + y_1 e \neq 0$ обратим в $\mathcal{A}_2(m,\ \alpha)$. Из (2) следует, что для этого необходимо и достаточно, чтобы выполнялись условия

$$\begin{cases} x_1x_2 + \alpha y_1y_2 = \mathbb{1}, \\ y_1x_2 + (x_1 + y_1)y_2 = 0. \end{cases} \quad (3)$$

Если $y_1 = 0,\ x_1 \neq 0$, то (3) будет иметь вид:

$$\begin{cases} x_1 \cdot x_2 = \mathbb{1}, \\ x_1 \cdot y_2 = 0. \end{cases}$$

Следовательно, $y_2 = 0,\ x_2 = x_1^{-1}$. Если $y_1 \neq 0$, то определитель D системы (3) равен:

$$D = x_1^2 + x_1y_1 + \alpha y_1^2.$$

Так как $y_1 \neq 0$, то $D = 0$, тогда и только тогда, когда

$$\left(\frac{x_1}{y_1}\right)^2 + \left(\frac{x_1}{y_1}\right) + \alpha = 0.$$

Это значит, что $t_0 = \frac{x_1}{y_1} = x_1y_1^{-1}$ является корнем многочлена $f(t) = t^2 + t + \alpha$. Т.е. этот многочлен приводим над полем $\mathcal{F}_2(m)$.

Таким образом, если $f(t) = t^2 + t + \alpha$ неприводим над полем $\mathcal{F}_2(m)$, то любой элемент алгебры $\mathcal{A}_2(m,\ \alpha)$ отличный от 0 обратим. Т.е. алгебра $\mathcal{A}_2(m,\ \alpha)$ является полем, изоморфным полю $GF(2^{2m})$.

III. Поиск элемента, порождающего неприводимый многочлен

Найдём элемент $\alpha \in \mathcal{F}_2(m)$, порождающий неприводимый многочлен $f(t) = t^2 + t + \alpha$. Легко видеть что отображение $\psi(t) = t^2 + t$ поля $\mathcal{F}_2(m)$ в поле $\mathcal{F}_2(m)$, является линейным и $\ker(\psi) = \{0,\ 1\} = GF(2)$.

Поэтому $A = F_m(\psi) = \{\psi(t) \mid t \in \mathcal{F}_2(m)\}$ является аддитивной подгруппой (подпространством) $\mathcal{F}_2(m)$ и $|A| = 2^{m-1}$.

Поле $\mathcal{F}_2(m)$ как аддитивная группа разбивается относительно подгруппы A на два смежных класса:

$$\mathcal{F}_2(m) = A + B,\ B = \alpha + A,\ \alpha \notin A.$$

A — можно рассматривать как линейное пространство размерности $m-1$ над полем $GF(2)$, т.е. поле из двух элементов 0 и $\mathbb{1}$. Из изложенного выше, следует справедливость следующего утверждения:

Утверждение 1. Для того, чтобы алгебра $\mathcal{A}_1(m,\ \alpha)$ была полем, необходимо и достаточно, чтобы $\alpha \in B$.

IV. Алгоритм поиска элемента $\alpha \in B$

Линейное подпространство A имеет размерность $m-1$. Если $a_1,\ \ldots,\ a_{m-1}$ базис A, а элемент $\alpha \notin A$, то $\alpha \in B$. Поэтому можно предложить следующий алгоритм поиска элемента $\alpha \notin B$.

1. Случайно выбираем $t_1 \in \mathcal{F}_2(m),\ t_1 \neq 0$ и вычисляем $a_1 = t_1^2 + t_1$.
2. Проверяем условие: $t_1 = 0$.
3. Если ДА, то переходим к п.1.
4. Выбираем случайно $t_2 \in \mathcal{F}_2(m),\ t_2 \neq t_1,\ t_2 \neq 0$ и вычисляем $a_2 = t_2^2 + t_2$.
5. Проверяем линейно зависимы ли векторы $a_1,\ a_2$.
6. Если ДА, то переходим к п.3.
7. Если мы определили систему линейно независимых элементов $a_1,\ \ldots,\ a_k,\ (2 \leqslant k < m)$ из A, то выбираем $a_{k+1} \in A$. (2)
8. Проверяем на линейную независимость систему из векторов $a_1,\ \ldots,\ a_k,\ a_{k+1}$. Если эта система линейно зависима, возвращаемся к п.5.
9. При $k = m-1$ процесс выбора базиса группы A заканчивается. Базис $a_1,\ \ldots,\ a_{m-1}$ группы A найден.

Далее для поиска элемента $\alpha \in B$ применяем следующую естественную процедуру; а именно:

Выбираем случайно $\alpha \in \mathcal{F}_2(m)$ и проверяем на линейную независимость систему элементов $a_1,\ \ldots,\ a_{m-1},\ \alpha$.

Если эта система линейно независима, то $\alpha \in B$.

Так как время нахождения элементов базиса A зависит от случайного выбора и сложности вычислений, то возникает проблема экспериментального определения времени решения этой задачи - т.е. время нахождения элемента α. Работа в этом направлении будет продолжена в дальнейшем.

V. Об экспериментальной оценке предложенного алгоритма

Оценка времени нахождения базы группы A требует точных оценок всех встречающихся алгоритмов и учета времени их выполнения.

Поэтому удобнее время нахождения базы рассматривать как случайную величину, возникающую в условиях вычислений. Проводя независимо нахождение базы A достаточно большое число раз получим экспериментальные распределения времени его нахождения.

Если уже выбран базис из k элементов, то $k+1$ базисный элемент не принадлежит подпространству, натянутому на k базисных векторов. Такое пространство состоит из 2^k элементов. Таким образом, выбор $k+1$-го базисного элемента происходит из множества,

состоящего из $2^{m-1}-2^k$ элементов. При равновероятном выборе, вероятность выбора k-го базисного элемента равна $\frac{2^{m-1}-2^k}{2^{m-1}}=1-\frac{1}{2^{m-1-k}}$. Так как $k<m-1$, то эта вероятность не меньше $\frac{1}{2}$. Поэтому за небольшое число выборов мы угадаем $k+1$-ый базисный элемент. Время выбора элемента α из B, смежного класса группы A.

Если уже все базисные элементы A известны, то мы производим случайный равновероятный выбор из всего множества $\mathcal{F}_2(m)$. Так как $|A|=|B|$, то вероятность выбора α равна $\frac{1}{2}$. Вероятность того, что элемент α не будет выбран за l испытаний равна $\frac{1}{2^l}$. Если T_0 — время проверки принадлежности выбранного элемента множеству A, то время ожидания появления α не превосходит суммы $T_0\frac{1}{2}+T_0\frac{1}{2^2}+T_0\frac{1}{2^3}+\cdots=T_0(\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\dots)=T_0$. Если T — время появления α, то это случайная величина и экспериментально можно найти её распределение.

Оценка сложности алгоритма установления линейной независимости векторов $a_1,\dots,a_k$ на основе алгоритма Гаусса очевидно не превосходит k^3. Поскольку k не превосходит $m-1$, и алгоритм Гаусса применяется для каждого $k, k=1,2,\dots,m-1$, то общая сложность не превосходит m^4.

Поскольку каждый выбор элемента a_k связан со случайным выбором, как это описано выше, то в оценке сложности m^4, может появиться константа C, которая не зависит от числа m, но зависит от уровня вероятности, при котором мы считаем выбор a_k достоверным.

VI. Специальные случаи построения неприводимых квадратичных полиномов

Если $m=2k+1$, то для поиска $\alpha\in B$, т.е. построения неприводимого над полем $\mathcal{F}_2(m)$ многочлена $f(t)=t^2+t+\alpha$ нужно вычислить $Tr(\alpha)=\alpha+\alpha^2+\cdots+\alpha^{2^{m-1}}\in\{0,\ 1\}$.

Если $Tr(\alpha)=1$, то $\alpha\in B$. Поскольку $\mathbb{P}(Tr(a)=1)=\frac{1}{2}$, то за l экспериментов с вероятностью $p=1-\frac{1}{2^l}$, мы найдем элемент $\alpha\in B$.

Замечание. Если $m=2k+1$, то $Tr(\mathbb{1})=\mathbb{1}$ и многочлен $t^2+t+\mathbb{1}$ неприводим над полем $\mathcal{F}_2(m)$.

Утверждение 2. Пусть $m=2^k\cdot s$, НОД$(2^{2^k}+1,\ 2^m-1)=$ НОД$(s,2)=1$, $\theta_0\in\mathcal{F}_2^*(2^k)\subset\mathcal{F}_2^*(m)$. Тогда многочлен $f(t)=t^2+t+\theta_0$ неприводим над полем $\mathcal{F}_2(m)$ тогда и только тогда, когда многочлен $f(t)$ неприводим над полем $\mathcal{F}_2(2^k)$.

Доказательство. Необходимость очевидна. Допустим, что $f(t_0)=t_0^2+t_0+\theta_0=0,\ t_0\in\mathcal{F}_2(m)$, т.е. $f(t)$ — приводимый. Следовательно,

$t_0^2+t_0=\theta_0$. (4)

Докажем достаточность. Из (4) следует, что

$t_0^{2^{2^i}}=t_0^4=t_0+\theta_0^2+\theta_0$

Индукцией по i легко установить, что

$$t_0^{2^{2^i}}=t_0+\sum_{j=0}^{2^i-1}\theta_0^{2^j}. \quad (5)$$

При $i=k$ из (5) следует:

$$t_0^{2^{2^k}}=t_0+\sum_{j=0}^{2^k-1}\theta_0^{2^j}=t_0+Tr(\theta_0). \quad (6)$$

Возможны случаи

1. $Tr(\theta_0)=0$.

Тогда из (6) вытекает, что $t_0^{2^{2^k}-1}=\mathbb{1}$. Это значит, что $ord(t_0)\mid(2^{2^k}-1)$, т.е. $t_0\in\mathcal{F}_2^*(2^k)$, и, следовательно, многочлен $f(t)$ приводим над подполем $\mathcal{F}_2(2^k)$. Пришли к противоречию с условием утверждения.

2. $Tr(\theta_0)=\mathbb{1}$.

В этом случае из (6) следует, что

$t_0^{2^{2^k}}=t_0+\mathbb{1}$.

Возводя обе части последнего равенства в степень 2^{2^k}, получим:

$t_0^{2^{2^{k+1}}}=t_0^{2^{2^k}}+\mathbb{1}=t_0+\mathbb{1}+\mathbb{1}=t_0$.

Таким образом,

$$t_0^{2^{2^{k+1}}-1}=t_0^{(2^{2^k}-1)(2^{2^k}+1)}=\mathbb{1}. \quad (7)$$

Так как, по условию, НОД$(2^{2^k}+1,\ 2^m-1)=1$, то из (7) следует, что $ord(t_0)\mid(2^{2^k}-1)$. Это означает, что $t_0\in\mathcal{F}_2^*(2^k)$. Снова пришли к противоречию с условием. Тем самым справедливость утверждения 2 полностью доказана.

Пример 1. Пусть $m=2^2\cdot 7=28,\ \mathcal{F}_2(28)=GF(2^{28})$. НОД$(2^{2^2}+1,\ 2^{28}-1)$ = НОД$(17,\ (2^{14}-1)(2^{14}+1))=1$. Следовательно, если $\theta_0\in\mathcal{F}_2(28)$ и $ord(\theta_0)=3$, то многочлен $f(t)=t^2+t+\theta_0$ неприводим над полем $GF(2^{28})$.

Пример 2. Пусть $m=2^3\cdot 11=88,\ \mathcal{F}_2(88)=GF(2^{88})$. НОД$(2^{2^3}+1,\ 2^{88}-1)$ = НОД$(257,\ (2^{88}-1))=d$. Вычислим

$$b=2^{88}-1\ (\mathrm{mod}\ 257)=(2^8)^{11}-1$$
$$(\mathrm{mod}\ 257)=(-1)^{11}-1\equiv-2\ (\mathrm{mod}\ 257)$$

Таким образом, $d=1$. Следовательно, многочлен $f(t)=t^2+t+\theta_0$, где $ord(\theta_0)=2^{2^3}-1=255$.

VII. О гипотезах для элементов больших порядков алгебры $\mathcal{A}_2(m)$

Поскольку алгебра $\mathcal{A}_2(m)$ является полем порядка 2^{2m}, то для практического приложения (например, построения открытых ключей) важно указать какой-нибудь примитивный элемент этого поля или элемент большого порядка $>2^{m(1+\varepsilon)}$. К сожалению, мы не можем сказать, что элемент e, или $\mathbb{1}+e$, или другой конкретный элемент, которые были бы примитивными, т.е. образующими мультипликативной группы этого поля или элементы большого порядка. Поэтому встает вопрос об оценке порядка таких конкретных элементов. Для усложнения дискретного логарифмирования основанного на элементах поля $\mathcal{F}_2(m)$ нам достаточно выбрать элемент алгебры $\mathcal{A}_2(m)$ с порядком большим чем $2^{(1+\varepsilon)m}$, где $\varepsilon>\varepsilon_0>0$. Действительно, если элемент $a\in\mathcal{A}_2(m)$ имеет порядок больший чем $2^{(1+\varepsilon)m}$,

то все степени $a,\ a^2, \ldots, a^{2^{(1+\varepsilon)m}}$ различны и мы можем применить процесс дискретного логарифмирования для a^n, где n — любое, $2^m < n < 2^{(1+\varepsilon)m}$.

Идея усиления дискретного логарифмирования состоит в том, что при порядке элемента a равного 2^m реализация алгоритма нахождения дискретного логарифма ещё возможна, в то время как при порядке $2^{(1+\varepsilon)m}$ уже практически нереализуема при ε больше некоторого $\varepsilon_0,\ \varepsilon_0 > 0$. Поэтому если порядок элементов $e,\ \mathbb{1} + e,\ \xi + e$, где ξ примитивный элемент $\mathcal{F}_2(m)$ больше чем $2^{(1+\varepsilon)m}$, то нахождение их порядков практически нереализуемо.

Допустим гипотезу, что элементы $e,\ \mathbb{1} + e,\ \xi + e$, а также некоторые другие имеют порядки $2^{(1+\varepsilon)m} - 1$ при любых m. Если эту гипотезу можно было бы подтвердить или опровергнуть, то её можно было бы подтвердить для всех $m' \leqslant m$, так как можно считать, что задача нахождения дискретного логарифма реально решается для 2^{128} элементов. Тогда в случае её справедливости возникает возможность “бесконечного” увеличения сложности дискретного логарифмирования. В условиях выбора m нам достаточно лишь одно удвоение.

Как отмечалось выше, мы начинаем искать квадратичные расширения поля $\mathcal{F}_2(m)$, т.е. искать некоторый элемент $\alpha_2 \in \mathcal{F}_2(m)$, для которого алгебра $\mathcal{A}_2(m)$ является полем. Это поле определяется соотношением $e_1^2 = \alpha + e_1$, где элементы $\mathbb{1}_1$ (единица) и e_1 являются базой алгебры $\mathcal{A}_2(m)$ над полем $\mathcal{F}_2(m)$. Тогда элемент e_1 берем как образующий мультипликативной группы поля $\mathcal{A}_2(m)$ порядка $2^{2m} - 1$. Так как поля с одинаковым числом элементов изоморфны, то поле $\mathcal{A}_2(m)$ можно обозначить $\mathcal{F}_2(2m)$. Аналогично можно найти квадратичные расширения поля $\mathcal{F}_2(2m)$ и его примитивный элемент.

При этом, если в первом случае потребовалось Cm^4 операций (константа C от m не зависит), то при нахождении квадратичного расширения $\mathcal{F}_2(2m)$ потребуется не более $16Cm^4$ операций. Таким образом, реально находится элемент $\alpha_2 \in \mathcal{F}_2(2m)$ и берутся элементы $\mathbb{1}_2$ (единица) и e_2, образующие базу алгебры $\mathcal{A}_2(2m)$, при этом $e_2^2 = \alpha_2 + e_2$. Если элемент e_2 является образующим мультипликативной группы поля $\mathcal{A}_2(2m)$, то его можно обозначить $\mathcal{F}_2(4m)$. Для элемента e_2, сложность дискретного логарифмирования равна $C2^{4m}$. Таким образом, процесс квадратичного расширения можно было бы продолжать сколь угодно долго, так как на каждом шаге расширение вновь полученного поля реально возможно.

Таким образом, предложенные в работе методы позволяют сделать вывод о возможности проведения дальнейших исследований с использованием компьютерных технологий. Авторы предполагают продолжение этой работы в направлении экспериментальных вычислений на базе высокопроизводительного вычислительного кластера Российского университета дружбы народов (РУДН).

Библиография

[1] А. С. Кузьмин, В. Т. Марков, А. А. Михалев, А. В. Михалев, А. А. Нечаев. Криптографические алгоритмы на группах и алгебрах. Фундаментальная и прикладная математика, 2015, том 20, №1, с. 205–222.

[2] N. Moldovyan, A. Moldovyan. Vector Finite Groups on Primitives for Fast Digital Signature Algorithms. Information Fusion and Geographic Information Systems. Lecture Notes in Geo–information and Cartography, Springer–Verlag Berlin, Heidlberg, 2009, p. 317-330.

[3] Н. Коблиц. Курс теории чисел и криптографии. — М.: Научное издательство ЋТВПЛ, 2001.

[4] L. Adleman and J. DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. In D. Stinson, editor, Proceedings of CRYPTO’93, volime 773 of Lecture Notes in Comput. Sci., pages 147-158. Springer, 1993.

[5] Гашков С. Б., Сергеев И. С. О сложности и глубине булевых схем для умножения и инвертирования в конечных полях характеристики 2. Дискретная математика, том 25, вып. 1, 2013.

[6] Cryptology ePrint Archive: Report 2013/095. A new index calculus algorithm with complexity L(1/4+o(1)) in very small characteristic. Antoine Joux

[7] Herlestam T., Johannesson R. On computing logarithms over GF(2p) // BIT. 1981. V. 21. P. 326—336

[8] ElGamal T. On computing logarithm over finite fields // Advances in cryptology — CRYPTO’85 (Santa Barbara, Calif., 1985). 1986. (Lect. Notes in Comput. Sci.; V. 218). P. 396—402.

[9] Coppersmith D. Fast evaluation of discrete logarithms in fields of characteristic two. IEEE Trans // Inform. Theory. 1984. V. 30 (4). P. 587—594.

[10] ThomДe E. Computation of discrete logarithms in GF(2607) // Advances in Cryptology — AsiaCrypt’2001. 2001. (Lect. Notes in Comput. Sci.; V. 2248). P. 107—124.

[11] ThomДe E. Discrete logarithms in GF(2607). e-mail to the NMBRTHRY mailing list, February 2002. http://listserv.nodak.edu/archives/nmbrthry.html

[12] Petit C., Quisquater JJ. (2012) On Polynomial Systems Arising from a Weil Descent. In: Wang X., Sako K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg

[13] I. Semaev. New algorithm for the discrete logarithm problem on elliptic curves. Report 2015/310.

[14] C. Petit and J.-J. Quisquater. On Polynomial Systems Arising from a Weil Descent. In: Wang X., Sako K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg.

The complication of discrete logarithms in fields of characteristic 2

Valerij M. Maksimov, Eduard A. Primenko

Annotation **- In real practical problems relating to the issue of information security calculations are frequently carried out in the fields of characteristic 2. In modern computing technologies, particularly, the usage of supercomputers, allow us to conduct calculations for quite large values $m = 128, 256, 512$. By developing computer technology and exploitation of new methods for analysis of information security systems, the parameter m should be increased.**

In order to construct a cyclical group of a large order, which is widely used in the synthesis of cryptographic protocols, it is proposed to construct towers of quadratic extensions fields in characteristic 2. The complexity of constructing such extensions depending on the degree of the field is established. The paper provides a method for constructing a quadratic extension field $\mathcal{F}_2(m)$ with the complexity of constructing an order $c \cdot m^4$,where it does not depend on m. The method is based on the construction of a two-dimensional algebra with one over the field. This process of doubling the degree of the field can be proceeded and construct the field every time, 2 times greater. In addition, It is not required to construct irreducible polynomials of higher degrees.

Keywords**—DLP, discrete logarithm problem, field extension, prime element.**

Manuscript received August 15, 2018.

V.M. Максимов is with RUDN University and Russian State University for the Humanities.

E.A. Primenko is with Lomonosov Moscow State University.