УДК 519.17 + 512.54 + 004.056

Коды, исправляющие ошибки, и криптосистемы с открытым ключом.

Н.Д. Зюляркина

Рассмотрен класс задач для построения криптосистем с открытым ключом. Для построения ассиметричных криптосистем используется метод, основанный на использовании линейных кодов, исправляющих достаточно большое число ошибок.

Ключевые слова: криптосистемы с открытым ключом, линейные коды, исправление ошибок.

Введение.

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» У. Диффи и М. Хеллмана, опубликованной в 1976 году ([1]).

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования, при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах и стандартах цифровой подписи.

Для построения криптосистемы с открытым ключом выбирается класс задач, для которого в произвольном случае не известен эффективный алгоритм решения и .в этом классе выделяется подзадача, для которой такой алгоритм существует. Выбранную задачу маскируют под задачу общего вида и на основе ее выбирают ключ шифрования. В качестве секретного ключа используется информация, позволяющая перевести выбранную задачу в исходный вид.

Наиболее распространенными в настоящее время являются криптосистемы, основанные на задаче факторизации (RSA) и задаче нахождения дискретного логарифма (Схема Эль-Гамаля) [2]. Но усовершенствование технических средств требует постоянного изменения параметров систем, основанных на задаче факторизации, что приводит к определенным сложностям при их использовании. Ввиду этого актуальность приобретают альтернативные методы построения ассиметричных криптосистем, использующие задачи, не связанные с факторизацией.

Одним из таких методов является метод, описанный Г.Нидеррайтером ([3]), основанный на использовании линейных кодов, исправляющих достаточно большое число ошибок.

Заметим, что линейные коды над конечными полями это подпространства конечномерных векторных пространств над этими полями. Существуют различные способы построения подпространств, удовлетворяющих ряду условий, связанных с характеристиками надежности. Особого внимания заслуживает метод, основанный на действии группы автоморфизмов пространства, в котором строится код. Для построения требуемого кода выбирается некоторая подгруппа группы автоморфизмов и некоторое подмножество из исходного пространства и строится инвариантное замыкание этого множества с помощью выбранной подгруппы. Отметим, что выбранная подгруппа должна обладать рядом специальных свойств. обеспечивающих надежность построенного кода. Кроме того, абелевы подгруппы группы автоморфизмов, имеющие элементы достаточно большого порядка, представляют интерес в связи с тем, что они могут быть использованы для построения криптосистемы на основе схемы Эль-Гамаля.

Ввиду сказанного особое внимание уделяется изучению подгрупп с заданными свойствами в классических группах, которые являются группами автоморфизмов конечномерных векторных пространств над конечными полями.

Подгруппы специального вида в классических группах и связанные с ними графы.

Для построения в заданной группе подгруппы с “разреженным” строением можно использовать так называемые TI-подгруппы. Подгруппу A группы G будем называть TI-подгруппой, если $A \cap A^g=1$ для любого элемента $g \notin N_G(A)$. Группы, содержащие TI-подгруппу, являющуюся 2-группой, активно изучались, и для классических групп имеется описание строения циклических подгрупп такого типа ([4]). Заметим, циклический случай можно свести к рассмотрению ситуации, когда данная подгруппа имеет порядок 4. В дальнейшем будем считать, что A является циклической подгруппой порядка 4 в группе $G=XA$, где $X=F^*(G)$ классическая группа над полем нечетной характеристики, a_0 это инволюция из A. Для изучения групп с заданными свойствами можно исследовать связанные с ними комбинаторные объекты (графы, схемы, геометрии и др.) Одним из таких объектов является граф коммутирования. Пусть G -- группа, A - TI-подгруппа группы G. Определим граф коммутирования $\Gamma_G(A)$ следующим образом: вершинами графа $\Gamma_G(A)$ являются подгруппы,

сопряженные с A, и две вершины смежны тогда и только тогда, когда они различны и коммутируют. Кликой будем называть полный граф, то есть граф, в котором любые две различные вершины смежны. Максимальной кликой графа Г будем называть подграф Г, являющийся кликой и не вкладывающийся в клику с большим числом вершин. Наибольшей кликой назовем максимальную клику с наибольшим числом вершин. Заметим, что максимальным кликам в графе коммутирования будут соответствовать абелевы подгруппы из $<A^G>$, и для оценки порядка таких подгрупп необходимо иметь информацию о порядке этих клик. Для случая классических групп над полями нечетной характеристики ответ на этот вопрос дают следующие теоремы.

Теорема 1. Пусть X-это частное $SL_n(q)$ по центральной подгруппе порядка d, q – нечетно. Тогда будут справедливы следующие утверждения:

(1) $q \equiv 1(4)$, a_0 соответствует инволюции типа k из $GL_n(q)$, $k \neq n/2$ или d нечетно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность C_n^k

(2) $q \equiv 1(4)$, a_0 соответствует инволюции типа k из $GL_n(q)$, $k=n/2$ и d нечетно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность $C_n^k/2$

(3) $q \equiv -1(4)$, a_0 соответствует инволюции типа 0 из $GL_n(q)$. Тогда $n=2m$, d - четно и любая максимальная клика из $\Gamma_G(A)$ имеет размерность 2^{m-1}.

Теорема 2. Пусть X-это частное $SU_n(q)$ по центральной подгруппе порядка d, q – нечетно. Тогда будут справедливы следующие утверждения:

(1) $q \equiv -1(4)$, a_0 соответствует инволюции типа k из $U_n(q)$, $k \neq n/2$ или d нечетно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность C_n^k

(2) $q \equiv -1(4)$, a_0 соответствует инволюции типа k из $U_n(q)$, $k=n/2$ и d нечетно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность $C_n^k/2$

(3) $q \equiv 1(4)$, a_0 соответствует инволюции типа 0 из $GU_n(q)$ или $q \equiv -1(4)$, a_0 соответствует инволюции из $GU_n(q) \backslash U_n(q)$ Тогда $n=2m$, d - четно и любая максимальная клика из $\Gamma_G(A)$ имеет размерность 2^{m-1}

Теорема 3. Пусть X-это частное $Sp_{2m}(q)$ по центральной подгруппе, q – нечетно. Тогда a_0 соответствует либо полуинволюции

типа 0 из $Sp_{2m}(q)$ если $q-1 \equiv -1(4)$, либо инволюции типа m из $GSp_{2m}(q) \backslash Sp_{2m}(q)$, если $q-1 \equiv 1(4)$.В любом из этих случаев максимальные клики из $\Gamma_G(A)$ имеют размерность 2^{m-1}.

Теорема 4. Пусть X-это частное $\Omega_n(q)$ по центральной подгруппе,n>6 q – нечетно, a_0 соответствует инволюции типа 2 из $\Omega_n(q)$, ε - тип группы $\Omega_n(q)$ в случае четного n. Тогда будут справедливы следующие утверждения:

(1) n=2m, ε =+1 и либо $q \equiv 1(4)$, либо m четно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность m

(2) n=2m, ε =+1 $q \equiv -1(4)$ и m нечетно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность m-1

(3) n=2m, ε =-1 и либо $q \equiv 1(4)$, либо m четно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность m-1

(4) n=2m, ε =-1 $q \equiv -1(4)$ и m нечетно. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность m.

(5) n=2m+1. Тогда любая максимальная клика из $\Gamma_G(A)$ имеет размерность m.

Литература:

1.Diffie W, Hellman M.E. New Directions in Cryptography. // IEEE Transactions on Information Theory ,V. TI-22,1977, pp 644-654.

2. ElGamal, T. A Public – Key Cryptosystem and Signature Scheme based on discrete logarithms. // IEEE Transactions on Information Theory 31(4), 1985, pp 469-472.

3. Niederreiter H. Knapsack – type cryptosystems and algebraic coding theory //Prob. Contr. Inform. Theory V.15(2), 1986, pp 157 – 166.

4. Зюляркина Н.Д. Циклические TI - подгруппы порядка 4 в классических группах Шевалле нечетной характеристики. // Вопросы алгебры и логики. Труды ИМ СО РАН, 1996, С.89 --- 110.

Codes that correct errors, and cryptosystems with an open key.

N. D. Zyulyarkina

The class of tasks for creation of cryptosystems with an open key is considered. The method based on use of the linear codes correcting rather large number of errors is used for creation of asymmetric cryptosystems.

Keywords: cryptosystems with an open key, linear codes, correction of mistakes.

References

1.Diffie W, Hellman M.E. New Directions in Cryptography. *IEEE Transactions on Information Theory*,V. TI-22,1977, pp. 644-654.

2. ElGamal, T. A Public – Key Cryptosystem and Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4), 1985, pp. 469-472.

3. Niederreiter H. Knapsack – Type Cryptosystems and Algebraic Coding Theory. *Prob. Contr. Inform. Theory*, V.15(2), 1986, pp. 157–166.

4. Zyulyarkina N. D. [Cyclic TI - Subgroups about 4 in Classical Groups of Chevalley of the Odd Characteristic]. *Questions of Algebra and Logic. Works THEM of the Siberian Branch of the Russian Academy of Science*, 1996, pp. 89–110. (in Russ.)