МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Факультет
вычислительной математики
и кибернетики

# ТРУДЫ

## VIII МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ

# «ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

**Москва**

**6–9 апреля 2009 г.**

**МОСКВА**

**2009**

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Факультет вычислительной математики и кибернетики

# ТРУДЫ

## VIII МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ

# «ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

Москва

6–9 апреля 2009 г.

МАКС ПРЕСС

МОСКВА – 2009

УДК 510.5+519.71
ББК 22.12:22.18
Д48

*Печатается по решению Редакционно-издательского совета факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова*

Отв. ред. *В.Б. Алексеев, В.А. Захаров*

Д48 **Дискретные модели в теории управляющих систем:** VIII Международная конференция. Москва, 6–9 апреля 2009 г.: Труды/ Отв. ред. В.Б. Алексеев, В.А. Захаров. – М.: Издательский отдел факультета ВМиК МГУ им. М.В. Ломоносова (лицензия ИД N 05899 от 24.09.2001 г.); МАКС Пресс, 2009. – 380 с.
ISBN 978-5-89407-366-8
ISBN 978-5-317-02847-3

В сборнике представлены труды VIII Международной конференции «Дискретные модели в теории управляющих систем», проведенной факультетом ВМК Московского государственного университета имени М.В. Ломоносова. Тематика конференции включает вопросы теории функциональных систем, теории синтеза и анализа управляющих систем, теории графов, теории сложности вычислений, теории кодирования, теории автоматов, криптографии, математической логики, теории программирования, гибридного математического моделирования.

Конференция организована кафедрой математической кибернетики факультета ВМК МГУ имени М.В. Ломоносова при финансовой поддержке Российского Фонда Фундаментальных исследований (грант 09-01-06017).

УДК 510.5+519.71
ББК 22.12:22.18

**ISBN 978-5-89407-366-8**
**ISBN 978-5-317-02847-3**

# Конструкции, контролирующие ошибки, на основе действующих криптографических стандартов

О. А. Финько*, Д. В. Самойленко

г. Краснодар

Законодательные ограничения, накладываемые на исследования в области криптографии, создают непреодолимые трудности при решении задач совершенствования криптографической обработки информации в ближайшей перспективе. Предлагается способ построения новых избыточных криптографических конструкций, обладающих новыми полезными свойствами, однако построенных на основе действующих в настоящее время (или в перспективе) криптографических стандартов. Суть идеи заключается в рассмотрении множества криптограмм как элементов избыточного кода. На основе этого множества вычисляются избыточные цифры кода, которые в свою очередь могут быть зашифрованны. Полученный таким образом код позволяет контролировать ошибки любой кратности в масштабе отдельных криптограмм, то есть и в случае их искажения (вплоть до стирания). При этом имитация обнаруживается как ошибка кода, а коррекция ошибки трактуется как восстановление истинного содержания имитированного сообщения [4].

Будем рассматривать $n$-канальную систему шифрования:

$$\begin{cases} C^{(1)} = \mathrm{E}_{k^{(1)}}\left(M^{(1)}\right) \pmod{m^{(1)}}, \\ C^{(2)} = \mathrm{E}_{k^{(2)}}\left(M^{(2)}\right) \pmod{m^{(2)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C^{(n)} = \mathrm{E}_{k^{(n)}}\left(M^{(n)}\right) \pmod{m^{(n)}}; \end{cases} \tag{1}$$

$$\begin{cases} M^{(1)} = \mathrm{D}_{k^{(1)}}\left(C^{(1)}\right) \pmod{m^{(1)}}, \\ M^{(2)} = \mathrm{D}_{k^{(2)}}\left(C^{(2)}\right) \pmod{m^{(2)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ M^{(n)} = \mathrm{D}_{k^{(n)}}\left(C^{(n)}\right) \pmod{m^{(n)}}; \end{cases} \tag{2}$$

где

$M^{(1)}, M^{(2)}, \ldots, M^{(n)}$ — открытые тексты,

$C^{(1)}, C^{(2)}, \ldots, C^{(n)}$ — криптограммы,

$k^{(1)}, k^{(2)}, \ldots, k^{(n)}$ — ключи (системы ключей).

На вход приемника поступят криптограммы, которые в канале связи могут подвергнуться искажениям (преднамеренным или непреднамеренным): $C^{*(1)}, C^{*(2)}, \ldots, C^{*(n)}$.

*ofinko@yandex.ru; http://www.mathnet.ru/rus/person/40004

Процедура расшифрования (2) примет вид:

$$\begin{cases} M^{*(1)} = \mathrm{D}_{k^{(1)}}\left(C^{*(1)}\right) \pmod{m^{(1)}}, \\ M^{*(2)} = \mathrm{D}_{k^{(2)}}\left(C^{*(2)}\right) \pmod{m^{(2)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ M^{*(n)} = \mathrm{D}_{k^{(n)}}\left(C^{*(n)}\right) \pmod{m^{(n)}}, \end{cases} \tag{3}$$

где $M^{*(1)}$, $M^{*(2)}$, …, $M^{*(n)}$ — открытые тексты, которые могут содержать ошибки.

Пусть: $\gcd(m_i, m_j) = 1$, где $i, j = 1, 2, \ldots, n$. Тогда система сравнений (1) в соответствии с Китайской теоремой об остатках имеет единственное решение $0 \le \mathcal{C} < \prod_{i=1}^{n} m^{(i)}$.

Дополним систему модулей $m^{(1)}, m^{(2)}, \ldots, m^{(n)}$ избыточными $r$ модулями $m^{(n+1)}, \ldots, m^{(n+r)}$ такими, что $\gcd(m_i, m_j) = 1$, где $i, j = 1, 2, \ldots, n + r$. Потребуем $m^{(n+1)} < \ldots < m^{(n+r)}$. Тогда получим *расширенную* систему криптограмм: $C^{(1)}, C^{(2)}, \ldots, C^{(n)} \ldots, C^{(n+r)}$, где $C^{(n+1)} = \mathcal{C} \pmod{m^{(n+1)}}$, $\ldots$, $C^{(n+r)} = \mathcal{C} \pmod{m^{(n+r)}}$.

Систему (3) перепишем в виде:

$$\begin{cases} M^{*(1)} = \mathrm{D}_{k^{(1)}}\left(C^{*(1)}\right) \pmod{m^{(1)}}, \\ M^{*(2)} = \mathrm{D}_{k^{(2)}}\left(C^{*(2)}\right) \pmod{m^{(2)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ M^{*(n)} = \mathrm{D}_{k^{(n)}}\left(C^{*(n)}\right) \pmod{m^{(n)}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ M^{*(n+r)} = \mathrm{D}_{k^{(n+r)}}\left(C^{*(n+r)}\right) \pmod{m^{(n+r)}}. \end{cases} \tag{4}$$

Расширенная система криптограмм есть расширенный модулярный $R$-код, контролирующий ошибки [1, 2, 5, 6, 7]. При этом $t$-кратная ошибка — произвольное искажение $t$-криптограмм. Известно, что $R$-код обнаруживает все одиночные ошибки, если $r \ge 1$ и исправляет $t$ или менее ошибок, если $2t \le r$ [1, 2].

Признак обнаруживаемой ошибки — выполнение условия [1, 2] $\mathcal{C}^* \ge \prod_{i=1}^{n} m^{(i)}$, где $\mathcal{C}^*$ — решение системы сравнений для криптограмм $C_i^*$ $(i = 1, \ldots, n+r)$ для системы модулей $m^{(i)}$ $(i = 1, \ldots, n+r)$. Пример $n$-канальной системы с одним избыточным каналом представлены на рис. **1**.

Отметим, что после процедуры исправления ошибок над кодовым словом $(C^{*(1)}, \ldots, C^{*(n+r)})$ мы получим криптограммы: $C^{**(1)}, \ldots, C^{**(n)}$ и исправленные открытые тексты: $M^{**(1)}, \ldots, M^{**(n)}$. Две звездочки ** указывают на вероятностный характер исправления ошибки.

Достоинства рассмотренной системы:

- возможность обнаружения (исправления) любых искажений в передаваемых криптограммах, если количество искаженных криптограмм не превышает обнаруживающих (исправляющих) возможностей $R$-кода;
- система с новыми свойствами может быть построена на основе действующих криптографических стандартов, основанных на модулярных криптографических функциях.

Для имитации криптограммы или цифровой подписи злоумышленнику придется иметь дело со всей совокупностью информационных криптограмм для того, чтобы модифицировать избыточные криптограммы. Но при шифровании избыточных цифр $C^{(n+1)}, \ldots, C^{(n+r)}$ (избыточных цифровых подписей) и такая возможность устраняется.

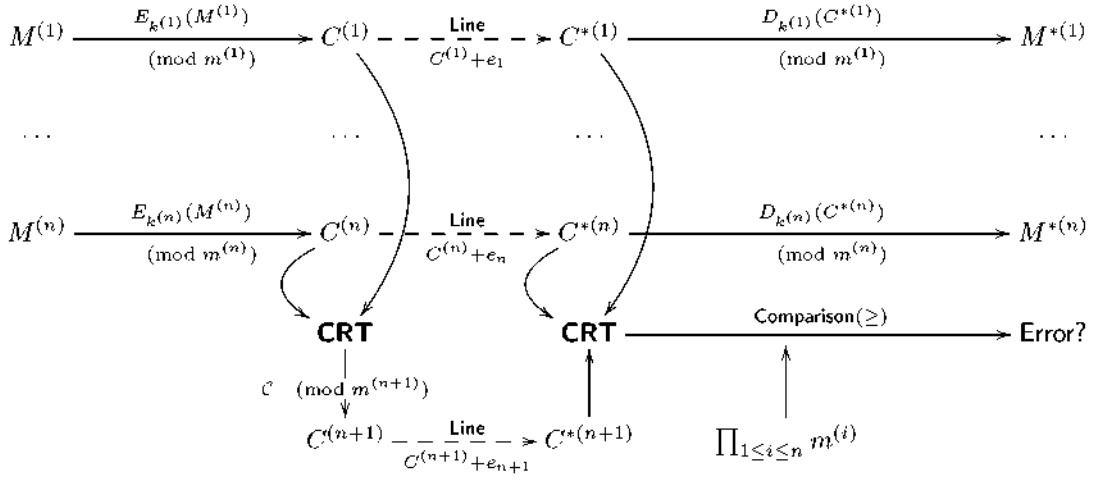


Рис. 1: Многоканальная система с обнаружением однократных ошибок

## Список литературы


[1] *Амербаев В. М.* Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 324 с.

[2] *Боляринов И. М.* Помехоустойчивое кодирование числовой информации. — М.: Наука, 1983. — 196 с.

[3] *Финько О. А.* Восстановление числа в системе остаточных классов с минимальным количеством оснований // Электронное моделирование. — 1998. — Т. 20, № 3. — С. 56–61.

[4] *Финько О. А.* Групповой контроль ассиметричных криптосистем методами модулярной арифметики // XIV Междунар. школа-семинар «Синтез и сложность управляющих систем». Н. Новгород, 27 окт. — 1 нояб. 2003. Сб. тр./ Под ред. акад. РАН О. Б. Лупанова. — Н. Новгород: Изд-во Нижегород. пед. ун-та, 2003. — С. 85–86.

[5] *Mandelbaum D. M.* Error correction in residue arithmetic // IEEE Trans. Comput. — 1972. — Vol. 21, № 6. — P. 538–545.

[6] *Mandelbaum D. M.* On a class of arithmetic codes and a decoding algorithm // IEEE Trans. On Information Theory. — 1976. — № 21. — P. 85–88.

[7] *Mandelbaum D. M.* Further results on decoding arithmetic residue codes // IEEE Trans. On Information Theory. — 1978. — № 24. — P. 643–644.