



Московский институт электроники
и математики им. А.Н. Тихонова

Кафедра информационной
безопасности киберфизических
систем

Москва 2025

Модификация Cascade

Проект 1476
Горелов С. Ю.



Процесс BINARY в Cascade

Алиса

индексы: 16 17 18 19

parity = 1

1	0	1	1
---	---	---	---

Боб

индексы: 16 17 18 19

parity = 0

1	1	1	1
---	---	---	---

Записи блоков

...
[16 17 18 19]
...



Процесс BINARY в Cascade

Алиса

индексы: 16 17 18 19

parity = 1



1.

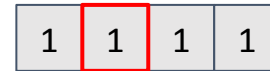


parity = 1

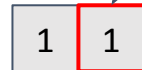
Боб

индексы: 16 17 18 19

parity = 0



1.



parity = 0

Записи блоков

...
[16 17 18 19]
...



Процесс BINARY в Cascade

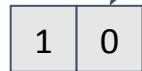
Алиса

индексы: 16 17 18 19

parity = 1



1.



parity = 1

2.

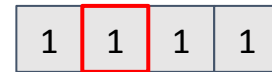


parity = 1

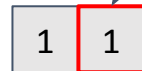
Боб

индексы: 16 17 18 19

parity = 0



1.



parity = 0

2.



parity = 1

Записи блоков

...
[16 17 18 19]
...



Процесс BINARY в Cascade

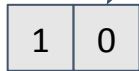
Алиса

индексы: 16 17 18 19

parity = 1



1.



parity = 1

2.

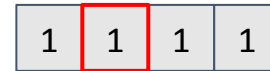


parity = 1

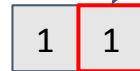
Боб

индексы: 16 17 18 19

parity = 0



1.



parity = 0

2.



parity = 1

3.



Записи блоков

...
[16 17 18 19]
...

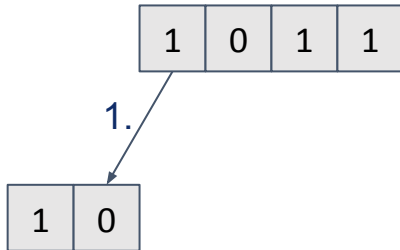


Модификация BINARY

Алиса

индексы: 16 17 18 19

parity = 1

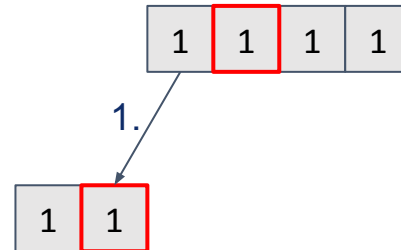


parity = 1

Боб

индексы: 16 17 18 19

parity = 0



parity = 0

Записи блоков

init: ...
 [16 17 18 19]
 ...
 ...
1 шаг: ~~[16 17 18 19]~~
 [16 17] [18 19]
 ...



Модификация BINARY

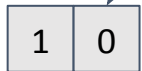
Алиса

индексы: 16 17 18 19

parity = 1



1.



parity = 1

2.

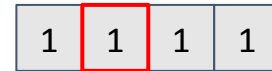


parity = 1

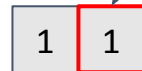
Боб

индексы: 16 17 18 19

parity = 0



1.



parity = 0

2.



parity = 1

Записи блоков

init: ...
[16 17 18 19]

...

1 шаг: ...
~~[16 17 18 19]~~
[16 17] [18 19]

...

2 шаг: ...
~~[16 17]~~ [18 19]
[16] [17]

...



Модификация BINARY

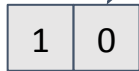
Алиса

индексы: 16 17 18 19

parity = 1



1.



parity = 1

2.

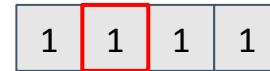


parity = 1

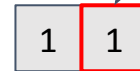
Боб

индексы: 16 17 18 19

parity = 0



1.



parity = 0

2.



parity = 1

3.



Записи блоков

init: [16 17 18 19]

1 шаг: [16 17 18 19]
[16 17] [18 19]

2 шаг: [16 17] [18 19]
[16] [17]



Модификация параметров Cascade

После 3 прохода: $k_i = \frac{N}{2}$

Table 2 Number of remain errors after each pass of
Cascade
(key length $N = 10000$, result is average value of 100
experiments)
 $\alpha = 0.5$

ϵ	initial	pass 1	pass 2	pass 3	pass 4
0.01	102.41	38.08	0.44	0	0
0.05	494.61	171.12	0.44	0.04	0
0.1	1001.27	326.10	0.42	0	0
0.15	1497.90	403.06	0.34	0	0
0.2	2001.07	401.30	0.06	0	0
0.25	2498.07	623.02	0.22	0	0

$\alpha = 1.0$

ϵ	initial	pass 1	pass 2	pass 3	pass 4
0.01	99.02	56.0	2.44	0.02	0
0.05	501.81	282.48	1.80	0.02	0
0.1	994.37	545.18	2.08	0	0
0.15	1494.68	836.42	2.20	0	0
0.2	2008.04	1082.86	1.28	0	0
0.25	2497.39	1323.94	1.28	0	0

$\alpha = 1.5$

ϵ	initial	pass 1	pass 2	pass 3	pass 4
0.01	98.99	66.62	5.56	0.04	0
0.05	501.17	341.72	8.42	0.04	0
0.1	996.76	674.06	6.40	0.02	0
0.15	1499.67	1013.28	6.98	0	0
0.2	1999.09	1382.58	8.64	0	0
0.25	2498.73	1674.68	4.16	0	0



Результаты экспериментов

Параметры new protocol:

$$\alpha = 0.8, \beta = 5$$

с 3 прохода: $k_i = \frac{N}{2}$

Параметры original CASCADE:

$$\alpha = 0.73, \beta = 2$$

$$\text{efficiency} = 1 - \frac{|E|}{N}$$

$$\text{theoretical limit} = 1 - H(\epsilon)$$

