ПОВЫШЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ОБЩЕГО СЕКРЕТА, СФОРМИРОВАННОГО С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Радюкевич М. Л., Голиков В. Ф.

Формирование общего секрета между абонентами A и B

Выбираем такое d, *чтобы* $P(t_{AB} \le d) \ge P_{\text{тр}}$

где
t_{AB}
A и
$P_{\text{тр}}$ требуемая вероятность синхронизации

Если $\vec{W}^A(d) = \vec{W}^B(d)$, то общий секрет $S^{AB} = \vec{W}^A(d) = \vec{W}^B(d)$

$\vec{W}^A(0)$ и $\vec{W}^B(0)$ выбираются случайным образом A и B
$\vec{W}^A(d)$ и $\vec{W}^B(d)$ фиксируются не оглашаясь A и B после d тактов синхронизации

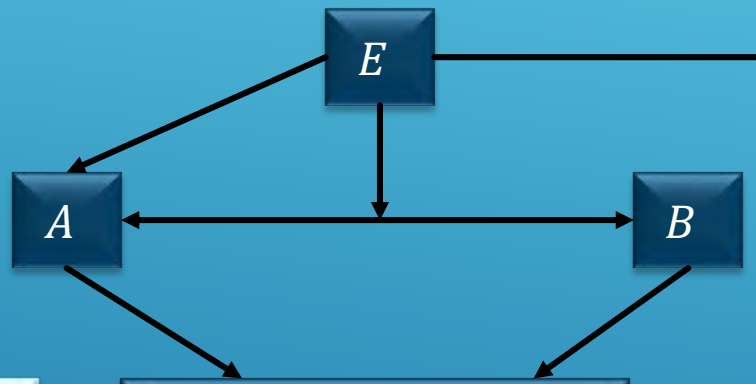
$\vec{W}^A(d) = \vec{W}^B(d)$

да

S^{AB}

Модель поведения криптоаналитика

Криптоаналитик E синхронизирует свою сеть, например, с сетью A



E проверяет совпадение, либо предполагает, что $\vec{W}^E(d) == \vec{W}^A(d)$

A и B достигли синхронизации

$\vec{W}^A(d) = \vec{W}^B(d)$

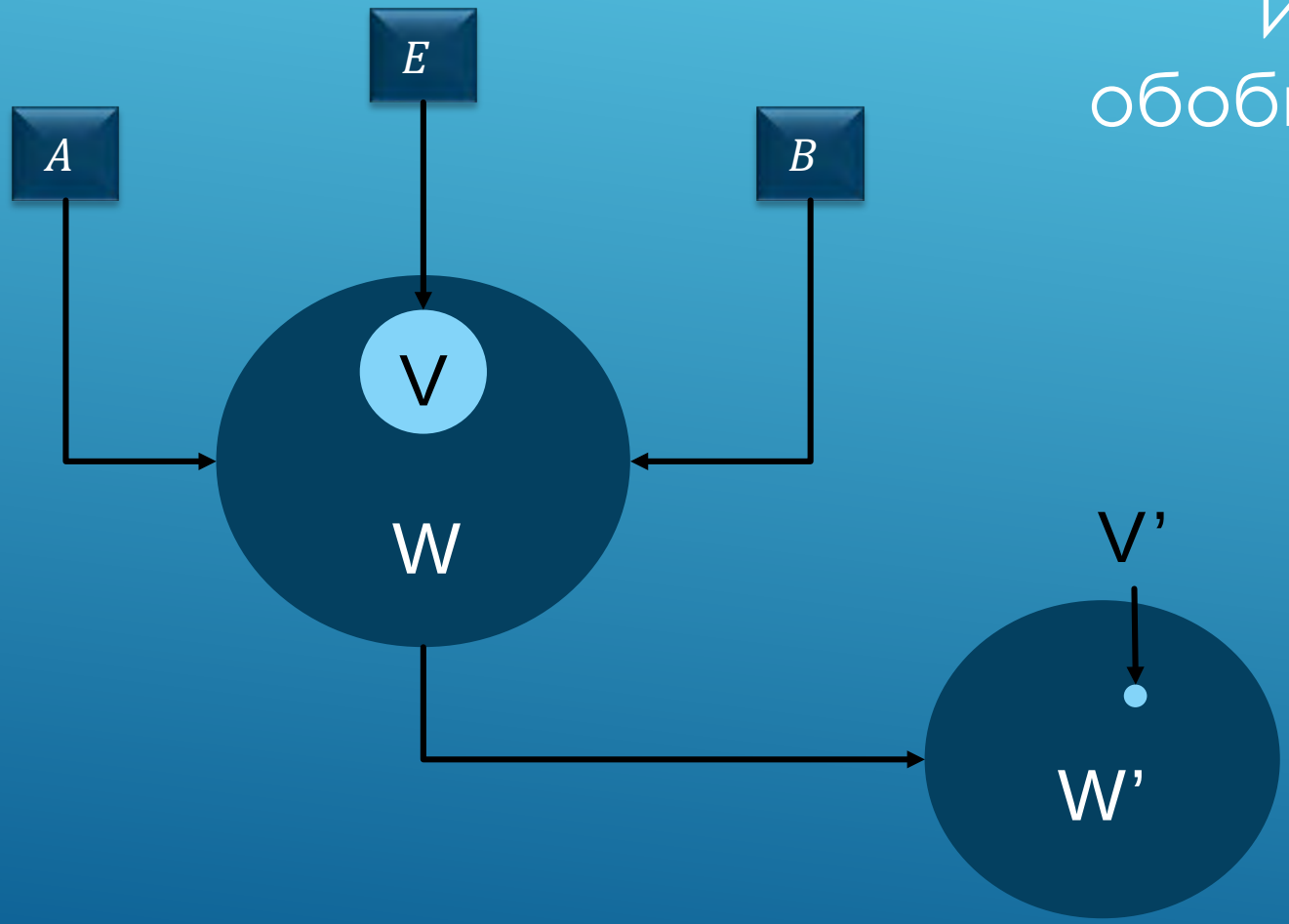
$\vec{W}^E(d) == \vec{W}^A(d)$

$P_{EA} = P(t_{EA} \leq d)$

P_{EA} - вероятность совпадения

Повышение конфиденциальности

Идея метода в обобщенном виде



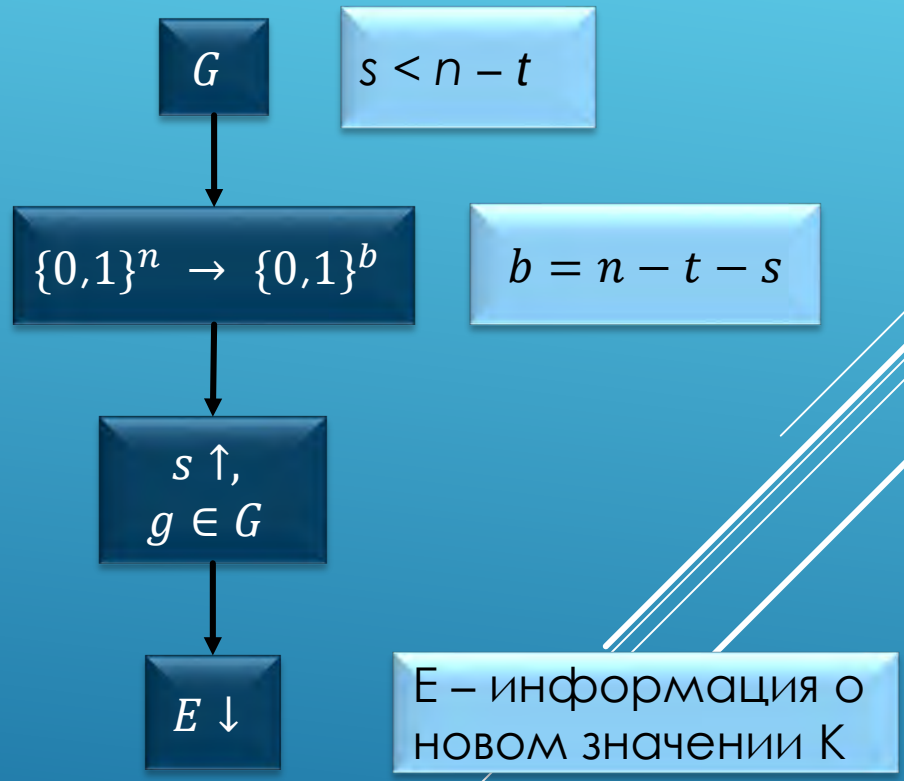
Задача повышения конфиденциальности

Сформирован абонентами A и B в виде битовой строки размером n

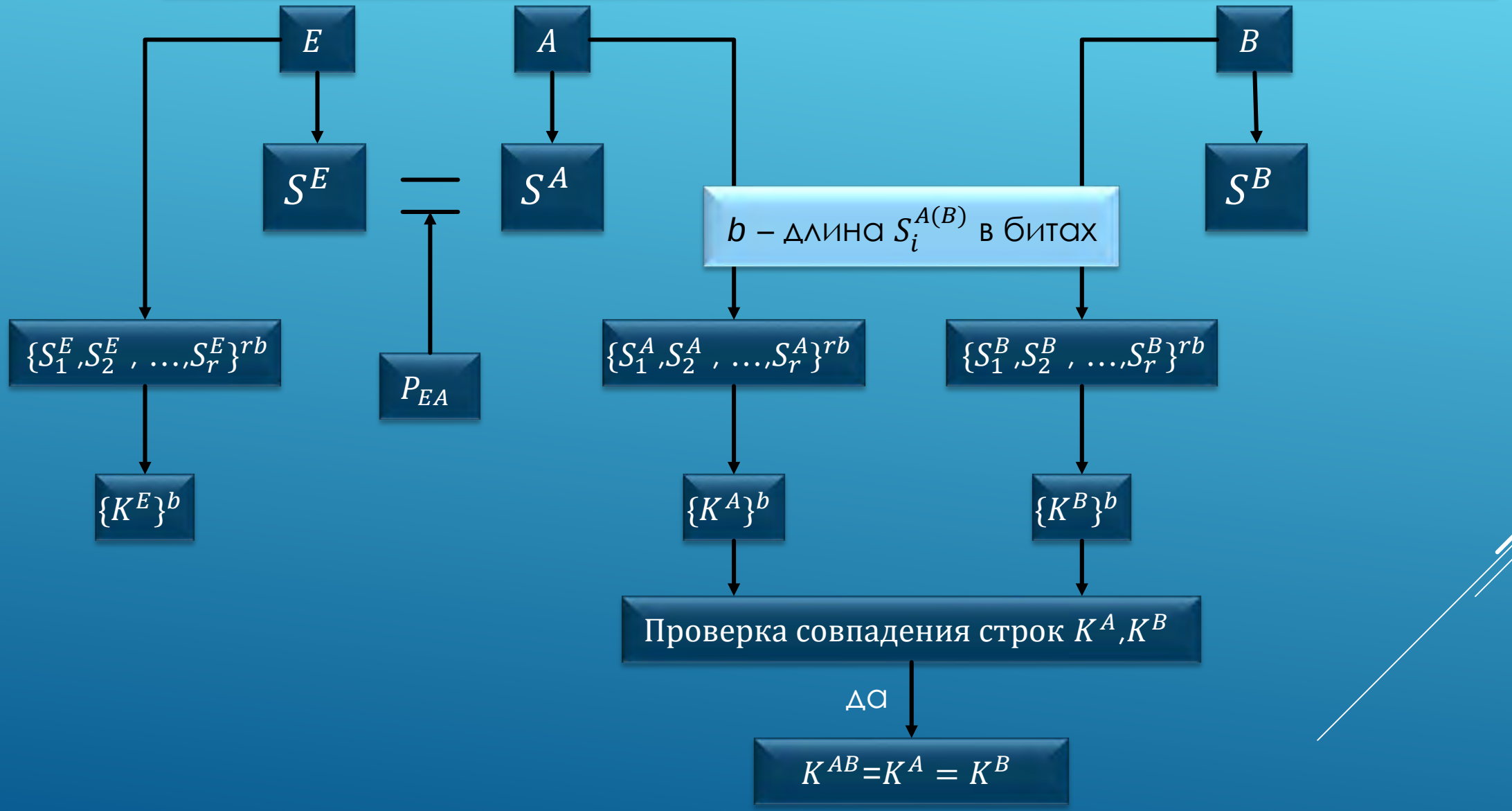
Криптоаналитик *E* имеет информацию *V*, коррелированную с *W* и дающую знание *t* бит из *n*

A и *B* хотят публично выбрать функцию сжатия *g*

Частичная информация *E* о *W* и ее полная информация о *g* должны дать мало информации о *K*



Задача повышения конфиденциальности



Анализ безопасности сформированного секрета

$$P_{AB,r} = \prod_{i=1}^{r} P_{ABi} = (P_{AB})^r$$

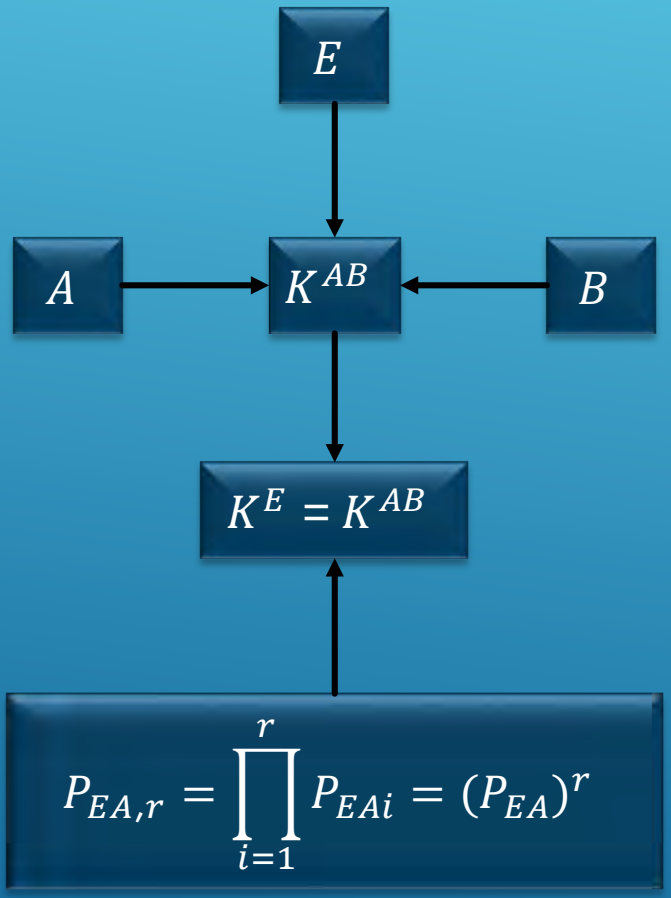
Согласно данному варианту формирования общего секрета $P_{AB,r} \geq P_{\text{тр}}$

$$m_{AB,r} \geq \frac{\ln(1 - P_{\text{тр}})}{\ln(1 - P_{AB,r})}$$

Количество сеансов синхронизации A и B при различных значениях r для обеспечения необходимых значений вероятностей

r P_{AB}	**0,8**	**0,90**	**0,95**	**0,99**
5	8	4	3	1
10	27	7	4	2
20	259	24	7	2
50	209 895	580	38	4

Анализ безопасности сформированного секрета



Вероятность совпадения значения K^E с K^{AB} при разных значениях P_{EA} и r

P_{EA} r	5	10	20	50
0,01	$1{,}0*10^{-10}$	$1{,}0*10^{-20}$	$1{,}0*10^{-40}$	$1{,}0*10^{-100}$
0,05	$3{,}1*10^{-7}$	$9{,}7*10^{-14}$	$9{,}5*10^{-27}$	$8{,}8*10^{-66}$
0,10	$1{,}0*10^{-5}$	$1{,}0*10^{-10}$	$1{,}0*10^{-20}$	$1{,}0*10^{-50}$
0,20	$3{,}2*10^{-4}$	$1{,}0*10^{-7}$	$1{,}0*10^{-14}$	$1{,}1*10^{-35}$

Анализ безопасности сформированного секрета

$P_{EA,r}$ зависит от r экспоненциально и может быть выбрана сколь угодно малой увеличением r

для A и B вероятность успешного сеанса поддерживается за счет увеличения m_{AB}

При этом описанный эффект будет иметь место, если

$$P_{EA,r} \ll 1$$

$$P_{AB,r} \approx 1$$

Свертка

$K = g(S_1, S_2, \ldots, S_r)$

Преобразование, свертывающее множество размером *rb* в *b*, при котором выходная величина зависит от всех битов входной

Хеш-функции

Обладают стандартными размерами выходных величин, которые будут ограничивать размер сформированного секрета

Свертка побитовым сложением по (mod 2) всех битов множества $\{S_i\}$

$$K^{A(B)} = \sum_{i}^{r} S_i^{A(B)} \text{ (mod 2)}$$

Бинарная последовательность длиной b, в которой каждый бит – сумма битов по модулю 2 из r слагаемых

Отклонение вероятности от равномерного распределения

j_i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
$j_{i\text{исх}}$	0	1	2	3	4	5	6	7
Δ, %	–0,04	–0,17	0,26	0,34	–0,26	0,21	–0,27	–0,08
j_i	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
$j_{i\text{исх}}$	8	–1	–2	–3	–4	–5	–6	–7
Δ, %	–0,03	–0,42	0,35	0,41	–0,16	0,03	–0,03	0,38

$$\Delta_i = \frac{(f_i - f_0)}{f_0} \cdot 100,$$

где f_i – частота i-го значения,

f_0 – частота при равномерном распределении $f_0 = \frac{1}{L_2 - L_1 + 1}$,

j_i – значение чисел из диапазона $[L_1, L_2]$.

Заключение:

Для решения задачи повышения конфиденциальности формируемого общего секрета предлагается использовать функцию сжатия g

Вероятность успеха криптоаналитика ($P_{EA,r}$) зависит от *r* экспоненциально и может быть выбрана сколь угодно малой увеличением *r*

Для *A* и *B* вероятность успешного сеанса поддерживается за счет увеличения *m*

Закон распределения сформированного ключа после функции сжатия близок к равномерному, при чем равномерность возрастает с ростом *r*

СПАСИБО ЗА ВНИМАНИЕ!

Радюкевич Марина Львовна

Государственное предприятие «НИИ ТЗИ»

Начальник испытательной лаборатории по требованиям безопасности информации

тел.+375 17 294-01-71

факс +375 17 285-31-86