ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

СТОЙКОСТЬ К КРИПТОГРАФИЧЕСКИМ АТАКАМ СИСТЕМ РАДИОЧАСТОТНОЙ АУТЕНТИФИКАЦИИ

К. А. Акула

Белорусский государственный университет, г. Минск;
Ksenea1@gmail.com
науч. рук.: А. В. Сидоренко, д-р техн. наук, проф.

Рассматриваются системы радиочастотной аутентификации (RFID-системы) при использовании в мобильной коммерции. При формировании ключа предложено использовать хаотические отображения: логистическое, тент-отображение и кусочно-линейное отображение. Приводятся результаты оценки вероятностей успешных атак злоумышленника при использовании протоколов м-коммерции.

Ключевые слова: радиочастотная аутентификация; атаки; протоколы; отображения, динамический хаос.

ВВЕДЕНИЕ

В системах радиочастотной аутентификации (RFID-системах), широко применяемых в мобильной коммерции (м-коммерции) для автоматизации бизнес-процессов и электронных платежей, актуальна проблема обеспечения защиты информации.

На основании проведенного анализа установлено, что в RFID-системах основными видами атак являются следующие: раскрытие секрета (ат. 1), обезличивание считывателя (ат. 2), десинхронизация (ат. 3), обезличивание метки (ат. 4), клонирование метки (ат. 5) [1].

Цель данной работы – определение основных атак злоумышленников в (RFID-системах) и анализ успешного проведения атак при формировании ключа с использованием хаотических отображений.

МЕТОДИКА И РЕЗУЛЬТАТЫ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА

При использовании радиочастотной аутентификации для реализации их функций необходимо определение стандартов или правил, оформленных в виде протоколов. Для мобильной коммерции используются протоколы ULRAS и ULRAS1, далее обозначается как Prot1 и Prot2.

В данной работе для оценки количественных параметров возможных атак проведен вычислительный эксперимент и определены вероятности успешного проведения каждой из этих атак. С этой целью было модифициро-

вано программное обеспечение протоколов Prot1 и Prot2 путем введения блока, предназначенного для оценки вероятности проведения этих атак.

Для обеспечения снижения вероятностных параметров проведения вышеназванных атак в данной работе при формировании ключа применены различные хаотические отображения:

логистическое отображение

$$x_{n+1} = f(x_n) = r_n(1 - x_n),$$

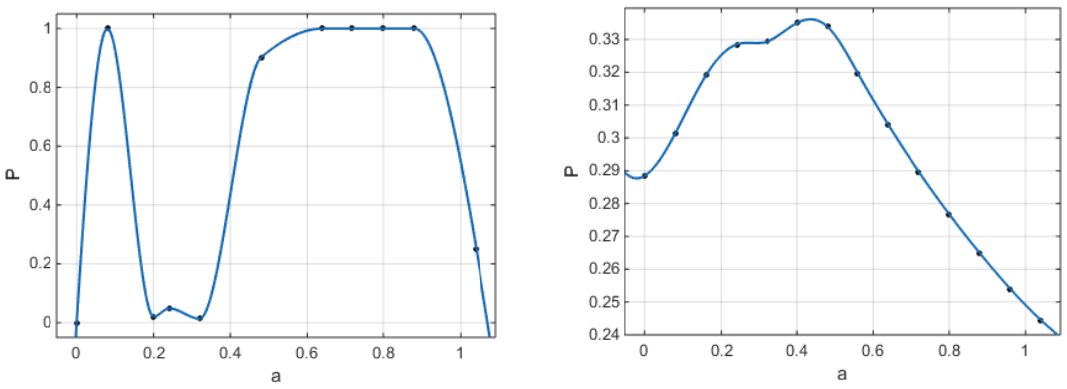
тент отображение

$$x_i = \begin{cases} x_i a^{-1}, & 0 < x_i < a \\ (1 - x_i)(1 - a)^{-1}, & a < x_i \le 1 \end{cases}$$

и кусочно-линейное отображение

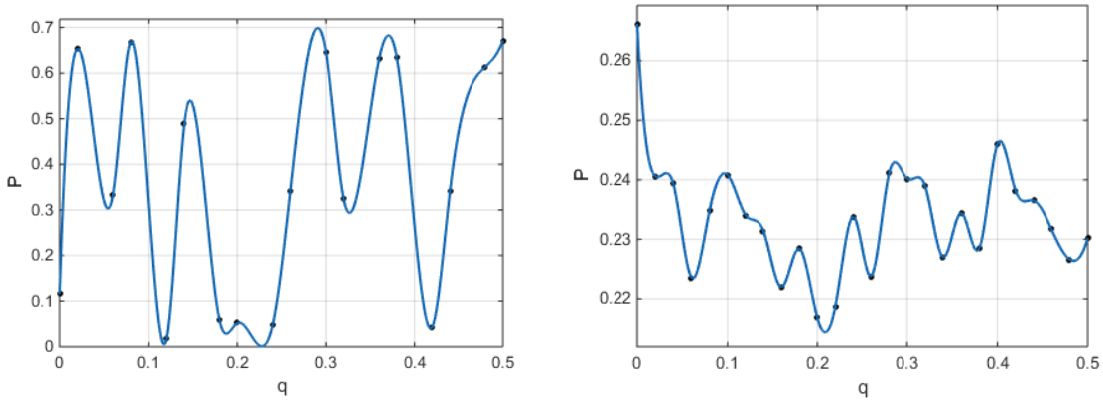
$$x_i = F(x_i, q) = \begin{cases} x_i q^{-1}, & x_i < q \\ (x_i - q)(0{,}5 - q)^{-1}, & q \le x_i \le 0{,}5 \\ F(1 - x_i, q), & x_i > 0{,}5 \end{cases}$$

Результаты вычислительного эксперимента приведены в графическом виде на рис. 1 – 3. В таблице представлено сравнение оценок (вероятностей) успешного проведения атак с использованием трех типов хаотического отображения.



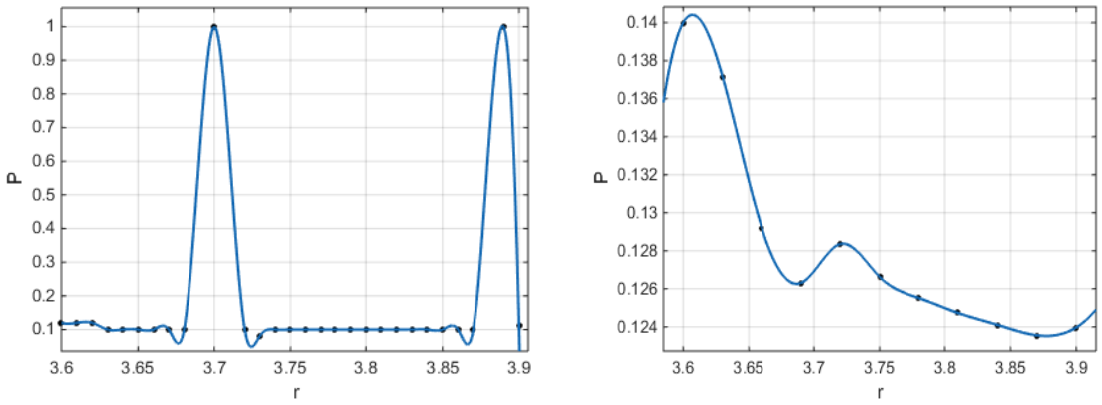
а *б*

Рис. 1. Графики зависимости вероятности успеха ат.1 с использованием тент отображения от параметра a: Prot1 (*а*) и Prot2 (*б*)



а *б*

Рис. 2. Графики зависимости вероятности успеха ат.2 с использованием кусочно-линейного отображения от параметра *q*: Prot1 (а) и Prot2(б)



а *б*

Рис. 3. Графики зависимости вероятности успеха ат.3 с использованием логистического отображения от параметра *r*: Prot1 (*а*) и Prot2 (*б*)

Таблица

Вероятности успешного проведения атак с использованием трех типов хаотического отображения

		Данные, приведенные в научной литературе [2]			Результаты вычислительного эксперимента			
Протокол	Тип отображения	Ат. 1	Ат. 2	Ат. 4	Ат. 1	Ат. 2	Ат. 3	Ат. 4
Prot1	Логистическое	+	+	-	0.4432 ± 0.0376	0.3481 ± 0.0266	0.1598 ± 0.0823	0.0090± 0.0025
	Кусочно-линейное	+	+	-	0.4288 ± 0.1172	0.3422 ± 0.0778	0.1427 ± 0.0500	0.0012± 1.0482e-04

окончание табл.

		Данные, приведенные в научной литературе [2]			Результаты вычислительного эксперимента			
	Тент-отображение	+	+	-	0.7203 ± 0.0775	0.4871 ± 0.1305	0.1252 ± 0.0016	0.0009± 5.6713e-05
	Нет	+	+	-	0.8356 ± 0.1603	0.5625 ±0.0056	0.4127 ± 0.0013	0.0115± 9.0602e-04
	Логистическое	-	-	-	0.3033 ± 0.1329	0.2486 ± 0.0903	0.1279 ± 0.0018	0.0071± 6.4658e-04
Prot2	Кусочно-линейное	-	-	-	0.3346 ± 0.0029	0.2745 ± 0.0099	0.1387 ± 0.0015	0.0053± 0.0013
	Тент-отображение	-	-	-	0.2986 ± 0.0057	0.2481 ± 0.0065	0.0707 ± 0.0199	0.0044± 1.6490e-04
	Нет	-	-	-	0.5275 ± 0.0962	0.3664 ± 0.0056	0.2048 ± 0.0306	0.0116± 1.6105e-04

ЗАКЛЮЧЕНИЕ

В процессе выполнения работы получены следующие результаты:

1. Проанализированы и определение основные виды атак в системах радиочастотной аутентификации мобильной коммерции.

2. Проведена модификация программ, используемых в мобильной коммерции протоколов ULRAS и ULTRAS1, введением блока, определения параметров оценки при наличии атак.

3. При формировании ключа в системах радиочастотной аутентификации предложено использовать хаотические отображения: логистическое, кусочно-линейное и тент-отображение.

4. Установлено, что использование хаотических отображений позволяет снизить вероятность успешной атаки на систему. При формировании ключа целесообразно использовать кусочно-линейное отображение и тент-отображение.

Библиографические ссылки

1. *Акула К. А.* Атака «клонирование меток» при радиочастотной аутентификации // Матер. 74 научной конференции студентов и аспирантов БГУ. – 2017 г., с. 178.
2. SeyedFarhadAghili, Hamid Mala Security Analysis of an Ultra-lightweight RFID Authentication Protocol for M-commerce/ SeyedFarhadAghili, Hamid Mala Security // IACR Cryptology ePrint Archive – 2017. – Vol. 2017, № 1. – p. 547.