УДК 004.056

Д. А. Ковалев, С. В. Беззатеев

ЗАЩИТА ПРОТОКОЛОВ УЛЬТРАЛЕГКОЙ АУТЕНТИФИКАЦИИ ОТ АТАК НА LSB

Предложен подход к улучшению версии протокола взаимной аутентификации LMAP++ путем замены стандартной операции сложения по модулю 2^m на операцию сложения по модулю 2^m–1 и использованием только простейших арифметических операций. Проведено сравнение сложности предложенной версии со сложностью известных методов повышения надежности протокола LMAP++.

Ключевые слова: *RFID, ультралегкие протоколы, LMAP++, аутентификация.*

Введение. Ультралегкие протоколы аутентификации для RFID построены на простейших арифметических операциях. Такие протоколы предназначены для сфер, требующих массового использования RFID-меток.

Ультралегкая RFID-метка имеет существенные ограничения по вычислительным возможностям и памяти, поэтому такие распространенные криптографические решения по обеспечению безопасности, как RSA, DES, AES, не могут быть реализованы в криптографических функциях, используемых в ультралегких протоколах, в них применяется следующий набор операций [1]:

— $\oplus$ XOR — поразрядная операция ИСКЛЮЧАЮЩЕГО ИЛИ,

— $\vee$ OR — поразрядное логическое ИЛИ,

— $\wedge$ AND — поразрядное логическое И,

— + — сложение m-битных чисел с игнорированием переполнения (сложение по модулю 2^m).

Несмотря на существенные ограничения по вычислительным возможностям, к безопасности ультралегких RFID-меток предъявляются достаточно высокие требования:

— анонимность метки,

— взаимная аутентификация между RFID-считывателем и меткой при минимальном числе сообщений, которыми они обмениваются.

В ультралегких протоколах можно выделить следующие основные этапы.

1. Считыватель посылает некоторую, инициализирующую протокол, команду метке. На этот запрос RFID-метка всегда отвечает своим динамическим идентификатором.

2. Считыватель находит в базе ключи и статический идентификатор метки по полученному динамическому идентификатору. Далее считыватель генерирует случайные числа и использует их и ключ метки для создания сообщения, которое на следующем шаге будет использоваться для взаимной аутентификации.

3. Считыватель и метка обмениваются сообщениями аутентификации.

4. Обновляются ключи и динамический идентификатор на считывателе и метке.

В 2006 г. P. Peris-Lopez предложил несколько ультралегких протоколов взаимной аутентификации — LMAP [2], EMAP [1], M2AP [3], но в них было обнаружено множество уязвимостей [4, 5]. В 2007 г. Li и Wang предложили улучшенную версию протокола LMAP: SLMAP, в которой также были найдены слабые места [6, 7]. В 2008 г. Tieyan Li улучшил свой протокол и назвал его LMAP++ [8], улучшенная версия также имела недостатки [9, 10].

Основные уязвимости протоколов аутентификации ультралегких радиочастотных идентификаторов. Большинство атак на ультралегкие протоколы используют идентичность операции сложения по модулю 2^m и операции XOR ($\oplus$) для наименее значимых битов (LSB)

$$[a+b]_0 = a_0 \oplus b_0,$$
$$[a-b]_0 = a_0 \oplus b_0.$$

Для представления старших битов используется следующая формула:

$$[a+b]_i = a_i \oplus b_i \oplus s(a,b,i-1),$$
$$[a-b]_i = a_i \oplus b_i \oplus t(a,b,i-1),$$

где $0 \le i < m$, а $s(a,b,i) = ([a]_i \wedge [b]_i) \vee ([a]_i \oplus [b]_i \wedge s(a,b,i-1))$ определяет, происходит ли перенос единицы в старший бит при сложении a_i и b_i, $s(a,b,i) = 1$ означает наличие переноса единицы из младших битов в старшие.

Аналогичным образом определяется параметр $t(a,b,i)$ — заем единицы из старших битов при вычитании a_i из b_i.

На такой особенности соотношения операций арифметического сложения и сложения по модулю два построено большинство атак на ультралегкие протоколы. Эти атаки приводят к рассинхронизации информации, хранящейся на считывателе и метке, раскрытию секретной информации о метке, а также к возможности отслеживать метку даже после ее успешной аутентификации на считывателе.

Способы противодействия атакам, использующим уязвимости LSB. Для предотвращения проведения атак, построенных на уязвимости LSB, в некоторых протоколах предлагается использовать следующие операции. В протоколе ULAP [11], Gossamer [12] предлагается использовать легкую хэш-функцию MixBits. В ULAP динамический идентификатор передается не в открытом виде, а в виде хэш-функции от него. Для этого считыватель генерирует случайное число и отсылает его метке вместе с сообщением, которое служит командой инициализации протокола. Метка отвечает значением IDS_{ULAP} (рис. 1), вычисляемым по алгоритму:

```
IDS_ULAP=IDS;
for(i=0;i<32;i++)
{
  IDS_ULAP = (IDS_ULAP >>1) + IDS_ULAP + IDS_ULAP +n;
}
```

где IDSULAP >>1 — сдвиг вектора IDSULAP на 1 бит вправо.

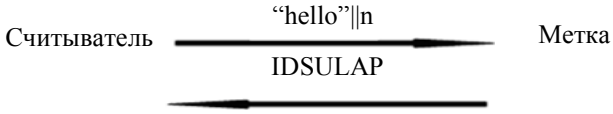

Рис. 1

В протоколах UMA-RFID [13], SASI [14], SULMA [15] при создании сообщений для взаимной аутентификации используется операция Rot(**x**,**y**), т.е. циклический сдвиг влево вектора **x**, на wt(**y**) позиций, где wt — вес Хемминга.

В протоколе RAPP [16] при создании сообщений используется операция перестановки Per(**x**,**y**) битов в векторе **x** в соответствии со значениями битов в векторе **y**.

Перестановка Per(**x**,**y**) выполняется следующим образом. Предположим, что **x** и **y** — два 96-битных числа, где

$$x = x_0 x_2 ... x_{95},\ x_i \in \{0,1\},\ i = 0,1,2,...,95,$$
$$y = y_0 y_2 ... y_{95},\ y_i \in \{0,1\},\ i = 0,1,2,...,95,$$

и вес Хемминга вектора **y** равен m ($0 \le m \le 95$), при

$$y_{k_1} = y_{k_2} = ... = y_{k_m} = 1, y_{k_m} = y_{k_{m+1}} = ... = y_{k_{95}} = 0,$$

где $0 \le k_1 < k_2 < ... < k_m \le 95$ и $0 \le k_{m+1} < k_{m+2} < ... < k_{95} \le 95$. Тогда перестановка Per(**x**,**y**)= $= x_{k_1}\ x_{k_2}\ ...\ x_{k_m}\ x_{k_{95}}\ ...\ x_{k_{m+2}}\ x_{k_{m+1}}$.

В протоколе EMAP [1] при обновлении ключей и динамического идентификатора метки используется операция Fp(**a**) при m=96, вектор **a** будет разбит на 24 блока по 4 бита, и для каждого блока будет вычисляться бит четности.

Пусть $\mathbf{a} = a_0, a_1, a_2, \ldots, a_{95}$, тогда

$$\mathrm{Fp}(\mathbf{a}) = (a_0 \oplus a_1 \oplus a_2 \oplus a_3, a_4 \oplus a_5 \oplus a_6 \oplus a_7, \ldots, a_{92} \oplus a_{93} \oplus a_{94} \oplus a_{95}).$$

Использование операции сложения по модулю 2^m–1. Для устранения возможности проведения атак, построенных на уязвимости LSB, предлагается заменить операцию сложения по модулю 2^m на операцию сложения по модулю 2^m–1. Реализовать эту операцию можно с помощью элементарных арифметических операций и архитектуры сумматора (рис. 2).

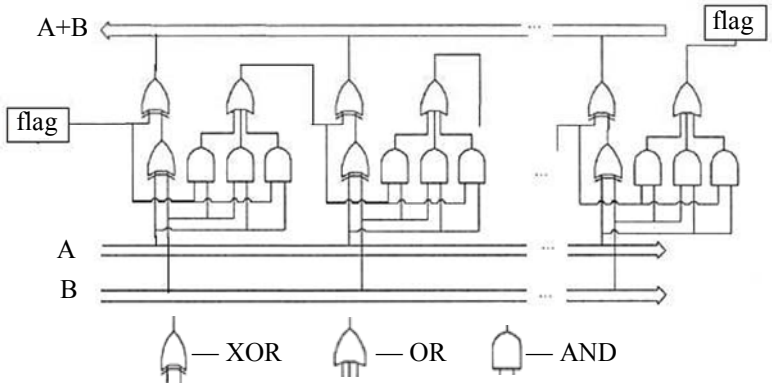

Рис. 2

Сложение по модулю 2^m –1 для чисел A и B можно провести за 5 шагов.

Шаг 1. C' =A+B mod 2^m, flag=1 если A+B > 2^m–1 и flag=0 — в противном случае.

Шаг 2. C'=C'+0+flag mod 2^m.

Шаг 3. D=C mod 2^m.

Шаг 4. D=D+1 mod 2^m, flag=1, если D=2^m–1, и flag=0 — в противном случае.

Шаг 5. C=C'+0+flag mod 2^m.

Таким образом, результатом сложения чисел A и B по модулю 2^m–1 будет число C.

При использовании операции сложения по модулю 2^m–1 исключаются уязвимости, существовавшие ранее вследствие идентичности операций сложения по модулю 2^m и XOR для LSB, так как равенства $[a+b]_0 = a_0 \oplus b_0$ и $[a-b]_0 = a_0 \oplus b_0$ не выполняются для операций арифметического сложения и вычитания по модулю 2^m–1.

В таблице сравниваются параметры операций, использовавшихся для предотвращения атаки по LSB.

Операции	Сложность в логических вентилях при m=96
MixBits	8120
Rot (**x**,**y**)	480
Permutation	~45794
Fp	468
Сложение по mod 2^m–1	173

Выводы. Предложена операция, предотвращающая атаки LSB, которая менее требовательна к вычислительным возможностям RFID-метки, чем предлагавшиеся ранее операции.

СПИСОК ЛИТЕРАТУРЫ

1. *Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A.* EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags // OTM Federated Conf. and Workshop: IS Workshop (IS'06). Montpellier, France: Springer-Verlag, 2006. Vol. 4277 of LNCS. P. 352—361.

2. *Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A.* LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags // Workshop on RFID Security (RFIDSec'06). Graz Austria, 2006.

3. *Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A.* M2AP: A Minimalist mutual authentication protocol for low-cost RFID tags // 3rd Intern. Conf. on Ubiquitous Intelligence and Computing (UIC'06). 2006. Vol. 4159. P. 912—923.

4. *Barasz M., Boros B., Ligeti P., Loja K., Nagy D. A.* Breaking LMAP // Proc of RFIDSec. 2007. P. 11—16.

5. *Li T., Wang G., Deng R. H.* SecurityAnalysisona Family of Ultra-lightweight RFID Authentication Protocols // J. of Software. 2008. Vol. 3. P. 1—10.

6. *Safkhani M., Bagheri N., Naderi M., Sanadhya S. K.* Security Analysis of LMAP++, an RFID Authentication Protocol // 6th Intern. Conf. Internet Technology and Secured Transactions. 2011. P. 689—694.

7. *Hernandez-Castro J. C., Tapiador J. E., Peris-Lopez P., Clark J. A., Talbi E.* Metaheuristic Traceability Attack against SLMAP, an RFID Lightweight Authentication Protocol // Intern. J. Foundations of Computer Science. 2009. P. 543—553.

8. *Li T.* Employing Lightweight Primitiveson Low-Cost RFID Tags for Authentication // Vehicular Technology Conf. 2008. P. 770—776.

9. *Wangand S.-H., Zhang W.-W.* Passive Attack on RFID LMAP++ Authentication protocol // CANS. 2009. P. 185—193.

10. *Hernandez-Castro J. C., Tapiador J. E., Peris-Lopez P., Clark J. A., Talbi E.* Metaheuristic Traceability Attackagainst SLMAP, an RFID Lightweight Authentication Protocol // IPDPS'09. Proc. of the 2009 IEEE Intern. Symp. Parallel & Distributed Processing. 2009. P. 1—5.

11. *Tanenbaum A. S.* Structured Computer Organization. 2001.

12. *Barasz M., Boros B., Ligeti P., Loja K., Nagy D. A.* Breaking EMAP // SecureComm. 2007. P. 514—517.

13. *Li T., Wang G.* Security Analysis of Two UltraLightweight RFID Authentication Protocols // IFIPSEC'07. 2007. P. 109—120.

14. *Yu H.* SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity // Dependable and Secure Computing. IEEE Transact. on Date of Publication. 2007.

15. *Kianersi M., Gardeshi M., Arjmand M.*SULMA: A Secure Ultra Light-Weight Mutual Authentication Protocol for Lowcost RFID Tags // Intern. J. of UbiComp. 2011. Vol. 2. P. 17.

16. *Peris-Lopez P., Hernandez-Castro J. C., Tapiador J. M. E., Ribagorda A.* Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol // Workshop on Information Security Applications. 2008. Vol. 5379. P. 56—68.

Сведения об авторах

Данил Александрович Ковалев — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра технологий защиты информации; E-mail: iostreamawm@gmail.com

Сергей Валентинович Беззатеев — д-р техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра технологий защиты информации; заведующий кафедрой; E-mail: bsv@aanet.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.