ностью этой процедуры объясняется и значительно больший разброс значений выборки относительно регрессионной линии.

Заключение. В работе предложена система аутентификации в мобильном приложении на основе разделенного хранения ключа ECDSA при помощи (2, 2)-пороговой полиномиальной модулярной СРС. С целью повышения стойкости алгоритмы разделения секрета и генерации ключей были модифицированы, что позволило реализовать защиту мобильного приложения наиболее эффективным образом. Система интегрирована с безопасным протоколом передачи защищенных документов мобильного приложения BuzzTalk Reader. Продемонстрировано использование системы и проанализированы результаты тестирования системы.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. American National Standard X9.62-1999, Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA) / Accredited Standards Committee X9. – 1999. – P. 16.
2. Asmuth, C.A. A modular approach to key safeguarding / C.A. Asmuth, J. Bloom // IEEE Transactions on Information Theory. – 1983. – Vol. 29. – P. 156–169.
3. Heuberger, C. Prodinger Hamming Weight of the Non-Adjacent-Form under Various Input Statistics / C. Heuberger, H. Prodinger // Periodica Mathematica Hungarica. – Volume 55. – Issue 1: сб. науч. ст. – 2007. – P. 81–96.
4. Common Vulnerabilities and Exposures. The Standard for Information Security Vulnerability Names – Режим доступа: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3860. – Дата доступа: 06.11.2015.
5. Elenkov, N. Android Security Internals: An In-Depth Guide to Android's Security Architecture / Nikolay Elenkov. – San Francisco: No Starch Press, 2014. – P. 268–277.
6. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets // Proc. of SYNASC'08. – IEEE Comp. soc. press, Los Alamitos – 2009 – P. 197-200.
7. J. A. Muir D. R. Stinson On the low weight discrete logarithm problem for nonadjacent representations / J. A. Muir D. R. Stinson // Applicable Algebra in Engineering, Communication and Computing Volume 16 Issue 6: сб. науч. ст. – 2006. – P. 461–472.
8. Schirokauer, O. The number field sieve for integers of low weight / Oliver Schirokauer // Mathematics of computation. – Volume 79. – Number 269: сб. науч. ст. – 2009. – P. 583–602.
9. Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters / Certicom Research. – 2010. – P. 13–26.
10. Информационные технологии и безопасность. Алгоритмы разделения секрета: СТБ 34.101.60-2014 – Минск: БГУ, 2014. – Режим доступа: http://apmi.bsu.by/assets/files/std/bels-spec29.pdf. – Дата доступа: 06.11.2015.

VISSIYA H.E.M.R., GALIBUS T.V., GAFUROV S.V., KAGANOVICH D.M. Mobile device authentication system based on the secret sharing scheme

In this paper, we propose a novel approach to the mobile authentication systems based on the secret sharing scheme.

The proposed approach provides a secure way to store a private key on a mobile device. In order to improve the functionality of the authentication system, we suggest a modification of ECDSA private key generation algorithm. We discuss the specifics of implementation and its integration into a secure transport protocol. We demonstrate the workflow of the production ready mobile application using the proposed protocol. Finally, we provide the results of mobile application testing along with analysis.

УДК 004.75

Цаволык Т.Г., Яцкив В.В.

МЕТОД ИСПРАВЛЕНИЯ ОШИБОК НА ОСНОВЕ МОДУЛЯРНЫХ КОРРЕКТИРУЮЩИХ КОДОВ

Введение. С развитием и широким использованием беспроводных технологий задача обеспечения высокой надежности передачи данных приобретает все более важное значение. В настоящее время для повышения надежности передачи данных разработаны и используются различные помехоустойчивые коды [1]. При выборе помехоустойчивых кодов необходимо учитывать сложность алгоритмов кодирования / декодирования, аппаратные ограничения устройств с автономным питанием, а также использование нелицензионного диапазона частот, что повышает вероятность искажения информационных символов.

Для повышения надежности передачи данных в беспроводных сенсорных сетях предложены модулярные корректирующие коды [2]. Данные коды сохраняют преимущества корректирующих кодов системы остаточных классов, но в отличие от последних обрабатывают входные данные, представленные в позиционной системе счисления (двоичной, десятичной), что значительно упрощает процедуры кодирования / декодирования и расширяет область их применения. В [3] разработан метод и алгоритм исправления многократных ошибок на основе модулярных корректирующих кодов с использованием двух проверочных символов.

Модулярные корректирующие коды. В данной работе разработан метод исправления ошибок в двух информационных символах с использованием одного проверочного символа. Значение контрольного символа в модулярных корректирующих кодах вычисляется по формуле [3]

$$x_{k+1} = \left|(v_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + v_i \cdot x_i + \ldots + v_k \cdot x_k)\right|_P, \quad (1)$$

где x_i – информационные символы, v_i – коэффициенты взаимно простые с P, $|\bullet|_P$ – операция получения остатка по модулю P.

Декодер по принятым данным $\left(x_1^{'}, x_2^{'}, \ldots, x_i^{'}, \ldots, x_k^{'}\right)$ вычисляет значение контрольного символа:

$$x_{k+1}^{'} = \left|(v_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + v_i \cdot x_i^{'} + \ldots + v_k \cdot x_k)\right|_P. \quad (2)$$

Для определения ошибки вычислим синдром, представляющий разницу между проверочным символом полученным и проверочным символом вычисленным на приемной стороне (в декодере):

$$\delta = \left|x_{k+1}^{'} - x_{k+1}\right|_P, \quad (3)$$

уравнение (3) можно записать в виде

Цаволык Тарас Григорьевич, *аспирант Тернопольского национального экономического университета.*

Яцкив Василий Васильевич, *к.т.н., доцент кафедры специализированных компьютерных систем Тернопольского национального экономического университета.*

Украина, 46009, г. Тернополь, Тернопольская область, ул. Львовская, 11.

$$\delta = \left| v_1 \cdot (x_1^{'} - x_1) + v_2 \cdot (x_2^{'} - x_2) + \right.$$
$$\left. + \ldots + v_i \cdot (x_i^{'} - x_i) + \ldots + v_k \cdot (x_k^{'} - x_k) \right|_P , \quad (4)$$

если синдром равен нулю $\delta = 0$, то ошибки нет, так как при отсутствии ошибки $x_i^{'} = x_i$, следовательно $x_{k+1}^{'} = x_{k+1}$, если $\delta \neq 0$ – имеется ошибка, соответственно $x_i^{'} \neq x_i$ и, как следствие, $x_{k+1}^{'} \neq x_{k+1}$.

Для исправления ошибок в одном информационном символе необходимо и достаточно, чтобы значение синдрома δ было уникальное для всех возможных вариантов ошибки. Для выполнения данного условия необходимо, чтобы выполнялось условие $P > 2 \cdot n \cdot (2^m - 1)$, где n – количество информационных символов, m – разрядность информационных символов.

Рассмотрим возможность исправления ошибок в двух информационных символах. Предположим, что ошибки произошли в двух символах, так как при отсутствии ошибки $x_i^{'} - x_i = 0$, то уравнение (4) примет вид:

$$\left| v_i \cdot (x_i^{'} - x_i) + v_{i+1} \cdot (x_{i+1}^{'} - x_{i+1}) \right|_P = \delta , \quad (5)$$

выполнив преобразования, получим

$$\left| v_i \cdot x_i + v_{i+1} \cdot x_{i+1} \right|_P = \left| v_i \cdot x_i^{'} + v_{i+1} \cdot x_{i+1}^{'} - \delta \right|_P . \quad (6)$$

Обозначим правую часть уравнения (6) через c, получим диофантовое уравнение с двумя неизвестными:

$$v_i \cdot x_i + v_{i+1} \cdot x_{i+1} = \left| c \right|_P . \quad (7)$$

С помощью расширенного алгоритма Евклида находим одно из решений уравнения (7). Расширенный алгоритм Евклида по заданным коэффициентам v_i, v_{i+1} находит их наибольший общий делитель $g = \gcd(v_i, v_{i+1})$, а также коэффициенты x_g, x_{g+1}, такие, что

$$v_i \cdot x_g + v_{i+1} \cdot x_{g+1} = g .$$

Так как коэффициенты v_i, v_{i+1} взаимно простые числа то $g = \gcd(v_i, v_{i+1}) = 1$, следовательно, c делится на g, соответственно диофантовое уравнение (7) имеет решение, и одним из таких решений являются числа:

$$\begin{cases} x_{0i} = x_g \cdot c \\ x_{0i+1} = x_{g+1} \cdot c \cdot \end{cases}$$

Все решения уравнения (7) вычисляются по формуле:

$$\begin{cases} x_i = \left| x_{0i} - k \cdot v_{i+1} \right|_P , \\ x_{i+1} = \left| x_{0i+1} + k \cdot v_i \right|_P , \end{cases} \text{ при } k \in P . \quad (8)$$

Учитывая ограничения, которые накладываются на x_i, в частности $0 \le x_i < 2^m$, только одно из решений будет соответствовать диапазону представления информационных символов. Таким образом, найденные решения уравнения (7) и будут правильные значения информационных символов. Для выявления ошибок необходимо проверить все пары информационных символов и при наличии ошибки исправить их приведенным выше методом.

Алгоритм обнаружения и исправления ошибок. Алгоритм обнаружения и исправления ошибок состоит из следующих шагов:

1. Вычисление проверочного символа x'_{k+1} по принятым данных.
2. Вычисления по формуле (3) синдрома δ.
3. Если $\delta = 0$ – ошибки нет. Конец.
4. Иначе вычисления выражения $f_j = \left| v_i * e_j \right|_P$.
5. Сравнение значения синдрома δ и f_j.
6. Если $\delta = f_j$ – ошибка обнаружена.
7. Исправление ошибки по формуле $x_i = \left| x'_i \pm e_j \right|$.
8. Если $\delta \neq f_j$ ошибка присутствует в более чем в одном символе.
9. Предполагаем, что ошибки есть в символах x_i, x_j, $i \neq j$.
10. С использованием расширенного алгоритмом Евклида находим одно из решений уравнения (5).
11. По формуле (8) находим все решения уравнения (7).
12. Проверяем, есть ли среди множества решений такие, которые находятся в диапазоне информационных символов, если да, то ошибки выявлены и найденные решение и есть правильные значения информационных символов. Конец.
13. Иначе, выбираем следующую пару символов x_i, x_j, $i \neq j$.
14. Повторяем пункты 10–13 до тех пор, пока не будут проверены все комбинации информационных символов. Конец.

Рассмотрим корректирующий код, который состоит из восьми информационных и одного проверочного символа и обеспечивает исправление ошибок в любых двух информационных символах. Разрядность информационных символов 4 бита. Кортеж данных, которые необходимо передать, имеет вид: $X = (5, 8, 10, 3, 7, 14, 12, 1)$.

Выбираем проверочный модуль $P = 1021$ и взаимно простые коэффициенты для вычисления проверочного символа: $v_1 = 13$, $v_2 = 17$, $v_3 = 19$, $v_4 = 23$, $v_5 = 29$, $v_6 = 31$, $v_7 = 37$, $v_8 = 43$.

Значение проверочного символа находим по формуле (1):

$$x_{k+1} = \left| 13 \cdot 5 + 17 \cdot 8 + 19 \cdot 10 + 23 \cdot 3 + 29 \cdot 7 + \right.$$
$$\left. + 31 \cdot 14 + 37 \cdot 12 + 43 \cdot 1 \right|_{1021} = 563.$$

В результате искажения данных получили кортеж: $X = (5, 4, 6, 3, 7, 14, 12, 1)$, ошибки есть во втором и третьем информационных символах.

Вычисляем проверочный символ по принятым данным по формуле (2):

$$x_{k+1}^{'} = \left| 13 \cdot 5 + 17 \cdot 4 + 19 \cdot 6 + 23 \cdot 3 + \right.$$
$$\left. + 29 \cdot 7 + 31 \cdot 14 + 37 \cdot 12 + 43 \cdot 1 \right|_{1021} = 419.$$

Вычисляем синдром:

$$\delta = \left| x_{n+1}^{'} - x_{n+1} \right|_P = \left| 419 - 563 \right|_{1021} = 877.$$

Так как синдром δ не равен нулю, это означает наличие ошибки.

Предположим, что ошибка в информационных символах x_2 и x_3. После подстановки числовых значений уравнение (7) примет вид:

$$\left| 17 \cdot (4 - x_2) + 19 \cdot (6 - x_3) \right|_{1021} = 877 ,$$

проведя вычисления, получим:

$$\left| 17 \cdot x_2 + 19 \cdot x_3 \right|_{1021} = 326 . \quad (9)$$

С использованием расширенного алгоритма Евклида находим коэффициенты $x_{g2} = 9$, $x_{g3} = -8$, и значение $x_{02} = 892$, $x_{03} = 455$.

Подставив значения x_{02}, x_{03} в формулу (8), находим все решения уравнения (9):

$$\begin{cases} x_2 = \left| 892 - k \cdot 19 \right|_P , \\ x_3 = \left| 455 + k \cdot 17 \right|_P . \end{cases} \text{ при } k \in P .$$

Множество решений уравнения (9) приведено на рис. 1 (кривая *Error:x2, x3*), из которого видно, что только одно решение ($x_2 = 8$,

$x_3 = 10$) соответствует диапазону представления информационных символов, которые соответствуют правильным значениям информационных символов. Если только в одном из двух выбранных символов, например (x_2, x_4), есть ошибка, то среди множества решений не будет правильного, то есть такого, что соответствует диапазону представления информационных символов (рис. 1, кривая *Error:x2, x4*).

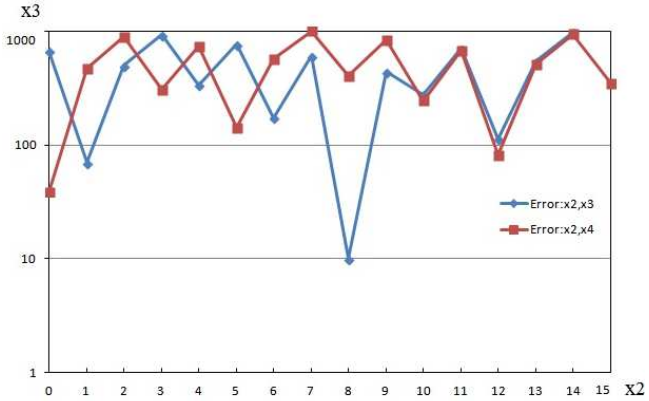

Рис. 1. Множество решений диофантового уравнения (9)

Скорость кода вычисляется по формуле $R = \frac{k}{n}$, где k – разрядность данных, n – общая длина кода. Для рассматриваемого примера: $k = 32$ бит (восемь четырех разрядных символов), $n = 32 + \lceil \log_2 1021 \rceil = 42$, $R = 0.76$. При использовании двух проверочных символов $n = 32 + 2 \cdot \lceil \log_2 1021 \rceil = 52$, $R = 0.62$. Таким образом, использование разработанного метода позволяет примерно на 20% повысить скорость кода.

Разработанный метод обеспечивает исправление ошибок в двух информационных символах с использованием одного проверочного символа и тем самым позволяет увеличить скорость кода примерно на 20%, соответственно уменьшить избыточность модулярного корректирующего кода.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Howard, S.L. Error control coding in low-power wireless sensor networks: When is ECC energy-efficient? / S.L.Howard, C. Schlegel, K. Iniewski // EURASIP Journal on Wireless Communications and Networking. – 2006. – № 2. – P. 29.
2. Яцків, В.В. Модифіковані коректуючі коди системи залишкових класів та їх застосування / В.В. Яцків // Інформаційні технології та комп'ютерна інженерія. – 2013. – № 2. – С. 39–45.
3. Yatskiv, V. Multiple Error Detection and Correction Based on Modular Arithmetic Correcting Codes / V. Yatskiv, T. Tsavolyk, Hu Zhengbing // Proceedings of the 8-th 2015 IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS'2015. – Warszawa. – 2015. – Volume 2. – P. 850–854.

Материал поступил в редакцию 09.12.15

TSAVOLYK T.G., YATSKIV V.V. Error-correcting method based on modular correcting codes

In this paper we proposed correcting codes - based on modular arithmetic - to improve the data transmission robustness in wireless sensor networks. We developed a new method and algorithm for the detection and correction of multiple errors. The codes are characterized by high correction characteristics as well as the simplified coding procedure. These codes provide the possibility to improve adaptively the reliability of data transmission in wireless sensor networks without changing the coding principle.

УДК 004.032.26

Савицкий Ю.В., Хвещук В.И., Савицкий А.Ю.

МОДИФИКАЦИЯ АЛГОРИТМА BPE ДЛЯ АДАПТИВНОГО ОБУЧЕНИЯ СИГМОИДАЛЬНЫХ НЕЙРОНОВ В АРХИТЕКТУРЕ МНОГОСЛОЙНОЙ НЕЙРОННОЙ СЕТИ

Введение. В последнее время в мире активизировались исследования в области глубокого обучения многослойных нейронных сетей. Это связано с определенными успехами в данной области, достигнутыми рядом исследователей [1, 2], а также высокой практической значимостью сильно-многослойных нейронных сетей (СМНС). Так, ряд разработчиков интеллектуального программного обеспечения (корпорации Google, Microsoft и др.) с успехом применяют технологии глубоких нейронных сетей в различных своих приложениях. При этом перспективным считается подход к предобучению (pretraining) СМНС не только с помощью ограниченной машины Больцмана (RBM), но и с применением нейросетевых автоэнкодеров (Autoencoder). Каждый такой нейросетевой автоэнкодер представляет собой трехслойный персептрон архитектуры *N→M→N*, где параметр *N* соответствует количеству входов текущего предобучаемого слоя, *M* – количеству нейронов указанного слоя сильно-многослойной нейросетевой архитектуры. Последовательное (начиная с входного слоя СМНС) обучение совокупности таких автоэнкодеров на входной обучающей выборке позволяет получить наборы весовых коэффициентов для финальной настройки синаптических связей всей СМНС (fine-tuning). При этом, для обучения как нейросетевых автоэнкодеров, так и СМНС, как правило, применяется алгоритм обратного распространения ошибки (Back Propagation Error, BPE) [3]. Очевидно, что эффективность алгоритма BPE напрямую определяет эффективность (точность обучения, обобщающие свойства) результирующей модели СНМС в целом.

В данной работе предлагается методика точного обучения нейронных элементов (НЭ) сигмоидального типа в составе многослойной нейронной сети (с целью последующего использования для обучения нейроросетевых автоэнкодеров и СНМС); основные результаты сформулированы в теореме 1 и утверждении 1; выполняется анализ особенностей предложенных решений.

1. Обобщенная архитектура нейронной сети. На рисунках 1 и

***Савицкий Юрий Викторович**, к.т.н., доцент кафедры «Интеллектуальные информационные технологии» Брестского государственного технического университета.*

***Хвещук Владимир Иванович,** к.т.н., профессор кафедры «Интеллектуальные информационные технологии» Брестского государственного технического университета.*

***Савицкий Антон Юрьевич,** студент 4 курса специальности «Автоматизированные системы обработки информации» факультета электронно-информационных систем Брестского государственного технического университета.*

Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.