ЗАЩИЩЕННАЯ СХЕМА ДОВЕРЕННОЙ ЦИФРОВОЙ ПОДПИСИ С ПОЛНОМОЧИЯМИ НА ОСНОВЕ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Еленевич Р. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

В современных системах всё острее становится проблема информационной безопасности. Основными угрозами являются перехват данных закрытого характера, фальсификации передаваемой информации, уничтожение данных с целью нарушения нормальной работы системы. Использование криптографии – основной метод защиты информации. Электронная цифровая подпись наилучшим образом гарантирует целостность данных, а также позволяет решать проблемы аутентификации и неотрицания авторства.

Традиционные протоколы ЭЦП были предложены довольно давно, но зачастую их свойств оказывается недостаточно для решения современных проблем, поэтому предлагаются новые модификаций цифровой подписи, например, слепая, групповая, кольцевая цифровая подпись.

Важную группу составляют схемы доверенной цифровой подписи: частичное делегирование, делегирование с полномочиями, частичное делегирование с полномочиями, пороговое делегирование и другие модификации. Доверенная цифровая подпись может быть применена для широкого круга задач, например, в электронной коммерции, распределенных системах и в электронном документообороте. Была исследована и реализована защищенная схема доверенной цифровой подписи с полномочиями на основе алгоритма цифровой подписи Эль-Гамаль.

На рисунке 1 приведена схема, поясняющая принципы работы защищенной доверенной цифровой подписи с полномочиями:

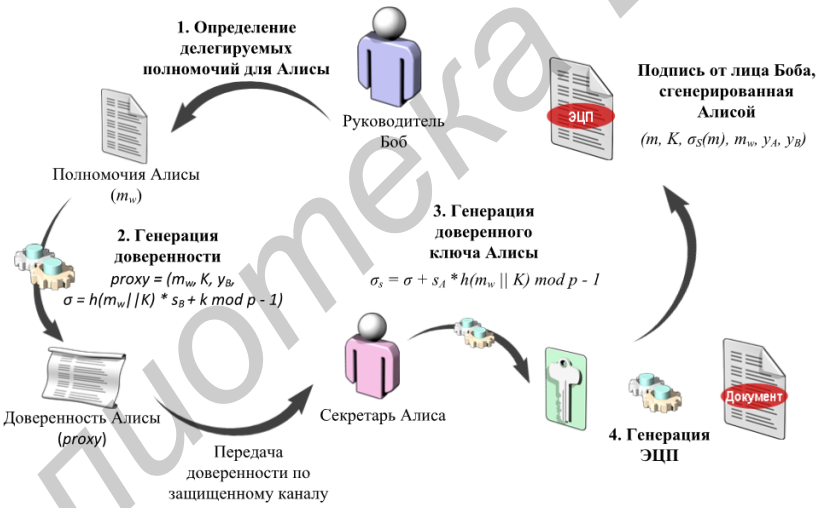

Рис. 1 – Принципы работы защищенной доверенной цифровой подписи с полномочиями

Одним из главных шагов данного алгоритма доверенной цифровой подписи является генерация личного ключа доверенной стороны Алисы на основе ключевой информации доверителя Боба и делегируемых полномочий, определенных на стороне доверителя:

$$\sigma = h(m_w||K) * s_B + k \bmod p - 1,$$

где h - алгоритм криптографического хеширования, m_w – информация о полномочиях, s_B – личный ключ доверителя, k – сгенерированное случайное число, p – большое простое число.

После генерации секретного значения и передачи его по защищенному каналу доверенной стороне происходит вычисление подстановочного секретного ключа доверенной стороны Алисы, который и определяет свойства защищенной схемы доверенной цифровой подписи с полномочиями:

$$\sigma_s = \sigma + s_A * h(m_w||K) \bmod p - 1,$$

где s_A – секретный ключ доверенной стороны Алисы.

После получения доверенной стороной конечного подстановочного секретного ключа может быть сгенерированна защищенная доверенная цифровая подпись с полномочиями. Электронная цифровая подпись имеет структуру $(m_p, s_{\sigma_p}(m_p), K, m_w)$, где m_p – передаваемое сообщение, $s_{\sigma_p}(m_p)$ – электронная цифровая подпись сообщения.

При получении сообщения с защищенной доверенной цифровой подписью проверяющая сторона

выполняет проверку электронной цифровой подписи в два шага. На первом этапе вычисляет значение открытого ключа на основе открытой ключевой информации доверителя Боба и доверенной стороны Алисы:

$$y_p = (y_A \cdot y_B)^{h(m_W||K)} \cdot K \bmod p,$$

где y_A – открытый ключ доверенной стороны, y_B – открытый ключ доверителя.

На втором этапе происходит проверка цифровой подписи по алгоритму Эль-Гамаль с использованием открытого ключа y_p. В результате проверки доверенной цифровой подписи проверяющая сторона может убедиться в целостности переданного документа, однозначно идентифицировать доверителя и доверенную сторону.

На основе приведенных выше вычислений можно сделать следующие выводы: доверенная сторона не может сгенерировать подпись идентичную оригинальной подписи доверителя, доверитель не может сгенерировать защищенную доверенную подпись от лица доверенной стороны, доверительно может наложить ограничения на сферу возможного применения цифровой подписи с использованием полномочий, результирующая электронная цифровая подпись однозначно идентифицирует доверителя и доверенную сторону.

Для реализации математической модели использовался язык программирования Java и криптографическая библиотека с открытым исходным кодом Bouncy Castle. Корректное функционирование было проверено с использованием модульных тестов.

Таким образом, была разработана и реализована математическая модель защищенной доверенной цифровой подписи с полномочиями. Рассматриваемая модель за счет использования генерируемого секретного значения позволяет избежать передачи ключевой информации доверителя, однозначно идентифицировать доверителя и доверенную сторону, исключает возможность доверителю выдать себя за доверенную сторону, а также дает возможность ограничить применение доверенной подписи за счет использования полномочий. Эти свойства выделяют данную схему по сравнению с другими алгоритмами доверенной цифровой подписи.

Список использованных источников:

1. Mambo, M. Proxy Signatures: Delegation of the power to sign Foundation / M. Mambo, K. Usuda, and E. Okamoto // IEICE Trans. Fundamentals Volume E79-A, Number 9, Sep 9, - 1996. – P. 1338-1354.
2. Sattar, A. A practical proxy signature scheme / A. Sattar, Y. Sufian // IJDIWC – 2012. – P. 27 – 35.
3. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. ElGamal // IEEE Trans. On Information Theory, Vol. IT-31, No. 4 – 1985 - P 86-91
4. Толюпа, Е.А. Некоторые протоколы доверенной цифровой подписи / Е.А. Толюпа – Математические методы криптографии №1(11) - 2011 – с 70-78.
5. Kim, S. Proxy signatures, revisited // Information and Communications / S. Kim, S. Park, D. Won // Security (ICICS'97). 1997. LNCS. V. 1334, P. 223–232
6. Lee, B. Strong proxy signature and its applications / B. Lee, H. Kim, K. Kim // Proc. of the 2001 Symposium on Cryptography and Information Security (SCIS'01), Oiso, Japan, Jan. 23–26, 2001. V. 2/2. P. 603–608

МЕТОДЫ ПОСТРОЕНИЯ И СИНХРОНИЗАЦИИ КРИПТОГРАФИЧЕСКИХ СИСТЕМ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Плехова Т. В.

Ярмолик В. Н. – д.т.н., профессор

Из-за процесса постоянного роста вычислительных мощностей современных компьютеров, а также технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически нераскрываемыми. Таким образом возникает актуальность в поиске новых подходов к построению криптографических систем. Примером такого подхода является построение криптографических систем на основе нейронных сетей.

Нейронные сети не программируются в привычном смысле этого слова, они обучаются. Возможность обучения — одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. Технически обучение заключается в нахождении коэффициентов связей между нейронами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение. Это значит, что, в случае успешного обучения, сеть сможет вернуть верный результат на основании данных, которые отсутствовали в обучающей выборке, а также неполных и/или «зашумленных», частично искаженных данных.

В криптоанализе используется способность нейронных сетей исследовать пространство решений. Также имеется возможность создавать новые типы атак на существующие алгоритмы шифрования, основанные на том, что любая функции может быть представлена нейронной сетью. Взломав алгоритм, можно найти решение, по крайней мере, теоретически. При этом используются такие свойства нейронных сетей,