К вопросу описания слабых параметров схемы цифровой подписи «Шиповник»

Григорий Маршалко

Параметризуемые криптографические механизмы

Исключение слабых параметров

- перечисление условий, обеспечивающих отсутствие или минимизацию вероятности появления слабых параметров, как, например, в разделе 5.2 стандарта ГОСТ Р 34.10-2012 «Процессы формирования и проверки электронной подписи»;
- доказуемо псевдослучайная выработка параметров с использованием криптографической однонаправленной функции и известных начальных параметров такой выработки Р 132356.1.024-2019 «Параметры эллиптических кривых для криптографических алгоритмов и протоколов»

Параметры схемы «Шиповник»

- n – длина кода в битах;
- k – размерность кода в битах;
- ω – кодовое расстояние в битах;
- матрица H' с элементами из $GF(2)$ размера $(n-k) \times (n-k)$, такая, что матрица $H = (H'|I_{n-k})$ – проверочная матица кода;
- хэш-функция $h() : V_\infty \to V_{512}$
- δ – длина подписи в битах.

Секретным ключом схемы является вектор $s = s_L||s_T$ длины n, открытым – вектор $y = H's_L^T \oplus s_R^T$ длины $n-k$.

Задача синдромного декодирования

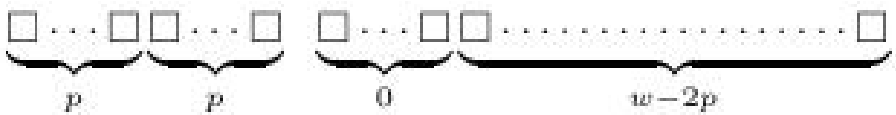
Зная y, H, ω найти $s, ||s|| \leq \omega$

Задача синдромного декодирования

Алгоритм Штерна

- произвольным образом выбирается подмножество из $n - k - l$ столбцов, проверяется максимальность ранга полученного минора и он приводится к единичному виду;
- из оставшихся произвольным образом выбирется k столбцов, проверяется максимальность ранга получившегося минора и для построенного минора производится поиск кандидатов ключа методом согласования;
- полученные кандидаты проверяются на истинность и если ключ не найден происходит переход к следующему шагу 1.

Stern's algorithm



Задание матрицы H

При псевдослучайном выборе матрицы H'

- максимальный ранг с вероятностью 0,2888[a];
- существуют матрицы H с матрицей H' не максимального ранга, в которых ни при каком варианте выбора столбцов невозможно получить два минора максимального ранга (для единичной матрицы и для информационного множества), что не позволяет применить алгоритм Штерна;

[a] И.Н. Коваленко, О распределении линейного ранга случайной матрицы

Примеры матриц H

Пример матрицы с нулевым столбцом/строкой

$$\begin{matrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

- при нулевых столбцах – уменьшение эффективно длины кода
- при нулевых строках – раскрытие бита секретного ключа s_R^T

Примеры матриц H

Пример матрицы с дублирующимися столбцами столбцами/строками

$$\begin{matrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

невозможность исправления кодом всех одиночных ошибок[a]

[a] Теорема 1.31, Э. Берлекэмп, Алгебраическая теория кодирования

При практическом использовании

Эффект

- при случайном выборе вероятность появления вероятность принебрежимо мала
- возможность навязывания слабых параметров схемы

Противодействие

- явное изучение и описание в спецификациях слабых классов параметров схемы (аналогично ГОСТ Р 34.10-2012)
- доказуемо псевдослучайная генерация параметров схемы (аналогично Р 132356.1.024-2019)
- проверка конкретных выработанных параметров схемы на принадлежность слабым классам[a]

[a] E.K. Alekseev, V.D. Nikolaev, S.V. Smyshlyaev, On the security properties of Russian standardized elliptic curves