Об особенностях применения криптографических механизмов в системе маркировки товаров различных торговых групп

Ежегодная международная научно-практическая конференция
«РусКрипто'2022»

Антон Гуселев,
Академия криптографии Российской Федерации

Цели внедрения системы маркировки товаров

Маркировка товаров – инструмент противодействия обороту контрафактных товаров

Краткое введение в систему маркировки

Маркировка товаров осуществляется **средствами идентификации**, которые представляется в виде двумерного штрихового кода в **формате Data Matrix** и содержит **код маркировки**, включающий в себя 4 группы данных:

- первая и вторая группы образуют код идентификации
- третья группа содержит ключ проверки, который генерируется оператором системы
- четвертая группа содержит код проверки – *последовательность символов (цифр, строчных и прописных букв латинского алфавита, а также специальных символов), сформированная в результате криптографического преобразования кода идентификации*

Товары, подлежащие маркировке

Код проверки 88 символов

- обувные товары
  (Постановление Правительства РФ от 5 июля 2019 г. N 860)

Код проверки 44 символа

- лекарственные препараты для медицинского применения
  (Постановление Правительства РФ от 14 декабря 2018 г. N 1556)
- ...

Код провери 4 символа*

- табачная и никотинсодержая продукция
  (Постановление Правительства РФ от 28 февраля 2019 г. N 224)
- ...

Реализация

4 символа и нет ключа проверки $\Rightarrow$ имитовставка $\Rightarrow$
$\Rightarrow$ см. документы национальной системы стандартизации

44 символа (256 бит) + ключ проверки $\Rightarrow$ цифровая подпись $\Rightarrow$??

88 символов (≥ 512 бит) + ключ проверки $\Rightarrow$ цифровая подпись $\Rightarrow$
$\Rightarrow$ ГОСТ Р 34.10-2012

Реализация

4 символа и нет ключа проверки $\Rightarrow$ имитовставка $\Rightarrow$
$\Rightarrow$ см. документы национальной системы стандартизации

44 символа (256 бит) + ключ проверки $\Rightarrow$ цифровая подпись $\Rightarrow$??

88 символов (≥ 512 бит) + ключ проверки $\Rightarrow$ цифровая подпись $\Rightarrow$
$\Rightarrow$ ГОСТ Р 34.10-2012

Реализация

4 символа и нет ключа проверки $\Rightarrow$ имитовставка $\Rightarrow$
$\Rightarrow$ см. документы национальной системы стандартизации

44 символа (256 бит) + ключ проверки $\Rightarrow$ цифровая подпись $\Rightarrow$??

88 символов (≥ 512 бит) + ключ проверки $\Rightarrow$ цифровая подпись $\Rightarrow$
$\Rightarrow$ ГОСТ Р 34.10-2012

Может быть подпись по ГОСТ?

Схема цифровой подписи ГОСТ Р 34.10-2012 (вариант $q \sim 2^{256}$)

- цифровая подпись $(\bar{r} \| \bar{s})$ $(r, s \in \mathbb{Z}_q)$ имеет длину 512 бит
- подделка подписи требует выполнения порядка 2^{128} операций

!!! Подпись «не уместится» в допустимое поле

А можно ли уместить?

- сократим размер подписи (пропорционально)
- хотим, чтобы $|\bar{r}| = |\bar{s}| = 128$
- для этого используем $q \sim 2^{128}$
- *подделка подписи потребует выполнения порядка 2^{64} операций*

Может быть подпись по ГОСТ?

Схема цифровой подписи ГОСТ Р 34.10-2012 (вариант $q \sim 2^{256}$)

- цифровая подпись $(\bar{r}\|\bar{s})$ $(r, s \in \mathbb{Z}_q)$ имеет длину 512 бит
- подделка подписи требует выполнения порядка 2^{128} операций

!!! Подпись «не уместится» в допустимое поле

А можно ли уместить?

- сократим размер подписи (пропорционально)
- хотим, чтобы $|\bar{r}| = |\bar{s}| = 128$
- для этого используем $q \sim 2^{128}$
- *подделка подписи потребует выполнения порядка 2^{64} операций*

Может быть подпись по ГОСТ?

? Достаточно ли стойкости, чтобы удовлетворить «Требованиям к шифровальным (криптографическим) средствам защиты информации, действующим в отношении шифровальных (криптографических) средств, предназначенных для проверки кодов маркировки»?

? Если ли другая схема подписи, способная обеспечить более высокий уровень стойкости?

Другие варианты схем цифровой подписи

Схема на основе билинейных отображений

подпись x-координата точки эллиптической кривой $\Rightarrow$
$\Rightarrow$ длина зависит от выбранного базового поля

Существует способ выбора параметров, при котором подделка подписи потребует выполнения порядка 2^{105} операций

Однако

- ! исследования все еще активно ведутся...
- ? как правильно выбрать функции спаривания?
- ? как правильно выбрать эллиптическую кривую?
- ? как правильно отобразить (хэшировать) сообщение в точку кривой?

Другие варианты схем цифровой подписи

Вариант схемы Шнорра

- цифровая подпись $(\bar{r}\|\bar{s})$ ($\bar{r} \in \{0,1\}^l$, $s \in \mathbb{Z}_q$, $l = \log_2 q$) длины 512 бит (при $q \sim 2^{256}$)
- есть возможность «непропорционального» сокращения длины компонент подписи
- можно получить подпись вида $(\bar{r}\|\bar{s})$, где $\bar{r} \in \{0,1\}^{\frac{l}{2}}$, $s \in \mathbb{Z}_q$
- чтобы уместить подпись в 256 бит используем $q \sim 2^{170}$
- подделка подписи требует порядка 2^{85} операций

Нетрудно заметить, что $85 > 64$

Другие варианты схем цифровой подписи

Вариант схемы Шнорра

- цифровая подпись $(\bar{r}\|\bar{s})$ ($\bar{r} \in \{0,1\}^l$, $s \in \mathbb{Z}_q$, $l = \log_2 q$) длины 512 бит (при $q \sim 2^{256}$)
- есть возможность «непропорционального» сокращения длины компонент подписи
- можно получить подпись вида $(\bar{r}\|\bar{s})$, где $\bar{r} \in \{0,1\}^{\frac{l}{2}}$, $s \in \mathbb{Z}_q$
- чтобы уместить подпись в 256 бит используем $q \sim 2^{170}$
- подделка подписи требует порядка 2^{85} операций

Нетрудно заметить, что $85 > 64$

Описание схемы

- ключ подписи d
- ключ проверки подписи $Q = dP$

Процедура формирования подписи

Вход: (d, Msg)

Выход: подпись $\bar{r}\|\bar{s}$

1: $k \xleftarrow{\mathcal{U}} \{1, 2, \ldots, q-1\}$.
2: $r \leftarrow x_{kP} \pmod q$
3: $s_0 \leftarrow \mathsf{H}(\bar{r}\|\bar{x}_Q\|\mathrm{Msg})$
4: $s_1 \leftarrow k + s_0 d \pmod q$
5: **return** $\bar{s}_0\|\bar{s}_1$

Процедура проверки подписи

Вход: $(Q, \mathrm{Msg}, \bar{s}_0\|\bar{s}_1)$

Выход: $\{0, 1\}$

1: $R \leftarrow s_1 P - s_0 Q$
2: $r \leftarrow x_R \pmod q$
3: $\bar{s}'_0 \leftarrow \mathsf{H}(\bar{r}\|\bar{x}_Q\|\mathrm{Msg})$
4: **if** $s'_0 \neq s_0$ **then**
5: **return** 0 ▷ Подпись невалидна
6: **else**
7: **return** 1 ▷ Подпись валидна