Федюкович В.Е.

Восстановление анонимности при использовании протоколов DAA

Исследовался обмен информацией в процессе удаленной проверки целостности платформы пользователя в Trusted Computing. Анализировались механизмы защиты персональной информации. Был предложен альтернативный алгоритм проверки экземпляра подписи Пользователя, допускающий некорректные экземпляры подписи Эмитента. Было предложено дополнительное уравнение проверки, позволяющее Пользователю обнаружить попытку нарушения анонимности.

Интерактивная система (протокол), вероятность успешного завершения. Свойства полноты (completeness) и корректности (soundness).

Доказательство и аргумент, безусловность и зависимость корректности от некоторой сложной задачи.

Алгоритм экстрактор и свойство знания.

Моделирующий алгоритм и свойство нулевого разглашения. Нулевое разглашение с честным Проверяющим и схема подписи Фиат-Шамира.

Протоколы с двоичными запросами и эффективные протоколы.

Модель с ’наблюдателем’, имеющим ограниченные документированные возможности взаимодействия с платформой Пользователя: “Wallet Databases with Observers”, Chaum, Pedersen, Crypto 1992.

Обзор и библиография: “Rethinking Public Key Infrastructures and Digital Certificates”, Brands, 2001.

Brickell, Camenisch, Chen, IACR 2004/205.

Публичная информация Эмитента: $(N, g, h, Z, S, R_0, R_1)$; факторизация N известна Эмитенту.

Информация Пользователя: (f_0, f_1, v'), $U = R_0^{f_0} R_1^{f_1} S^{v'}$, подпись Эмитента: (e, A, v'').

$$A^e U S^{v''} = \bar{Z} \pmod{N}, \qquad \bar{Z} \neq Z \tag{1}$$

$$SPK\{(\dots) : \quad \bar{Z} = T_1^e R_0^{f_0} R_1^{f_1} S^v h^{-ew} \quad \dots\} \tag{2}$$

$$c \stackrel{?}{=} H(\dots N_V || \bar{T}_1 || \hat{T}_2 \dots) \tag{3}$$

$$\bar{T}_1 = \bar{Z}^{-c} T_1^{s_e + c2^{l_e - 1}} R_0^{s_{f0}} R_1^{s_{f1}} S^{s_v} h^{-s_{ew}} \tag{4}$$

Спасибо за внимание!

Предложена дополнительная проверка для протокола DAA Join, снижающая риски нецелевого использования (возможно) персональных данных Пользователей.

IACR 2008/277

Федюкович Вадим Евгеньевич

Протоколы аргумента для демонстрации справедливости утверждений о множествах, графах, строках, искаженном кодовом слове кода Гоппы.

МаБИТ'08 и 2008/363; ИТиС'08 и 2008/357; 2008/359.

`http://vf.org.ua/`