СИСТЕМЫ ЦИФРОВОЙ ПОДПИСИ И НАПРАВЛЕННОГО ШИФРОВАНИЯ НА ИДЕНТИФИКАТОРАХ

Козулин А.А.
научный руководитель – д.т.н., проф. Горбенко И.Д.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. БИТ, тел. (057) 702-14-25)

This work is devoted applications of bilinear pairings in cryptography and contains basic concepts and ideas of the use of the id-based systems.

Система ЭЦП Украины построена на основе стандартной модели инфраструктуры открытых ключей ДСТУ ISO/IEC 9594-8:2006, главным недостатком которой является необходимость в изготовлении и обслуживании сертификатов пользователей данной системы. Система ЭЦП основанная на математике билинейного отображения, которая позволяет вместо сертификата открытого ключа использовать открытый идентификатор пользователя.

Основными отличиями системы на идентификаторах являются: в качестве открытого ключа пользователя используется открытая информация – идентификатор; все секретные ключи изготовляет уполномоченный на генерацию; утерянный секретный ключ может быть легко восстановлен; каждый незарегистрированный пользователь по сути уже является членом системы, так как ему нет необходимости в изготовлении сертификата; поддерживается офф-лайн обмен.

Недостатком системы является: необходимость в доверии к уполномоченному на генерацию; сложная политика безопасности; сложность интеграции и использование в больших (реальных) системах.

Что бы использовать достоинства двух моделей, предлагается дополнение к стандартной модели инфраструктуры открытых ключей – комбинированная система.

Суть взаимодействия двух систем состоит в надстройке традиционной инфраструктуры. Она заключается в том, что сертификат, выданный в центре сертификации ключей, может выступать гарантом целой подсистемы на идентификаторах, для этого достаточно подписать некоторые открытые и закрытые параметры уполномоченного на генерацию ключей, и обеспечить аутентичность ведения корреспонденции пользователей двух разных подсистем, что можно достичь благодаря иерархической системе центров сертификации.

Исследования, проведенные в ЗАО «ИИТ» и на кафедре БИТ ХНУРЭ, дали перспективы для дальнейшего развития комбинированной модели инфраструктуры открытых ключей и разработанной системы на идентификаторах.