ОТЗЫВ

на автореферат диссертации
Бабуевой Александры Алексеевны
«Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля»,
представленной на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6.
Методы и системы защиты информации, информационная безопасность

Диссертационная работа Бабуевой А.А посвящена построению новых методов получения обоснованных оценок стойкости схем подписи вслепую. Криптографические механизмы такого типа являются специальным протоколом взаимодействия между подписывающей стороной (сервером) и стороной, запрашивающей подпись (клиентом). Выполнение протокола даёт клиенту подпись к сообщению, при этом без взаимодействия с сервером подписать сообщение нельзя – обеспечивается неподделываемость. Сервер же не получает какой-либо информации о сообщении или о подписи – обеспечивается свойство неотслеживаемости.

Рассматриваемая в диссертационной работе проблематика обладает высокой практической значимостью. Схемы подписи вслепую широко применяются на практике – в системах электронных платежей, в системах дистанционного электронного голосования, а также могут быть использованы при реализации классических схем подписи в условиях недоверенной вычислительной среды. Следует подчеркнуть, что результаты работы существенным образом использовались в общем процессе стандартизации криптографических механизмов в России – в части выбора и обоснования схемы подписи вслепую.

К достоинствам диссертационной работы безусловно следует отнести органичное сочетание конструктивных методов анализа (атак) и доказательного подхода к обоснованию стойкости, заключающегося в применении так называемого метода сведений. Доказательный подход подразумевает определение формальных моделей безопасности, включающих

описание свойств, которые должны обеспечиваться анализируемой схемой, а также перечень возможностей, используемых противником для атаки на схему.

Схемы подписи вслепую рассматриваются в диссертационной работе в рамках большого количества различных моделей, отражающих как свойство неподделываемости (UF, SEQ-UF, wUF, SA-UF, HBC-UF), так и свойство неотслеживаемости (Blind, HS-Blind). Разнообразие моделей позволяет адекватно учесть возможности противника, имеющие место в той или иной информационной системе. Как следствие такого рассмотрения, результаты диссертации позволяют обеспечить разумное сопоставление между конкретной схемой подписи и практическими условиями её применения, что также является достоинством работы.

Большое внимание уделено в работе определению базовых (вычислительно сложных) задач, достаточных для обеспечения стойкости схем подписи, сформулирована новая задача (SOMDL). Отметим, что все такие задачи (SDL, OMDL, SOMDL, REPR) определяются относительно стандартизированных групп точек эллиптических кривых и представляют собой нетривиальные вариации задачи дискретного логарифмирования.

Следует отдельно выделить следующие полученные в диссертации результаты.

1. Проанализированы свойства безопасности, (не)обеспечиваемые схемой слепой подписи Шаума-Педерсена. Построена атака с параллельными сеансами и тем самым продемонстрировано, что схема не обеспечивает свойство сильной неподделываемости (модель UF – атакующий предъявляет изменённую подпись к уже подписанному сообщению). Доказана стойкость схемы в модели wUF (слабая неподделываемость) за счёт сведения к задачам REPR и SOMDL, а также показана необходимость сложности задачи SDL для стойкости схемы.

2. Показана нестойкость ряда схем подписи вслепую на основе уравнений Эль-Гамаля. В частности, построены атаки на свойство неотслеживаемости (относительно пассивного нарушителя) для трёх существующих схем. Также определён класс схем, названный GenEG-BS, с помощью которого можно описать почти все известные к настоящему времени схемы подписи вслепую на основе уравнений Эль-Гамаля. Выполнена классификация схем, описываемых этим классом. Для всех криптоалгоритмов из класса GenEG-BS построены атаки, демонстрирующие нестойкость либо в модели UF, либо в модели Blind, либо в модели SEQ-UF.

3. Предложен способ использования схем подписи вслепую для реализации классического алгоритма подписи в условиях слабодоверенного вычислителя. Разработаны специальные модели угроз для схем подписи вслепую (SA-UF и HBC-UF), показана их связь с известными моделями. Для создания защищённой реализации предложено использовать схему подписи вслепую Камениша, в основе которой лежит такое же уравнение подписи, как в ГОСТ Р 34.10-2012. Доказано, что такая схема может обеспечить защиту ряда прикладных систем при единственном предположении, что отечественный алгоритм подписи обеспечивает свойство неподделываемости.

4. Разработана специальная модель угроз SUF-CMRA для классической схемы подписи, позволяющая учесть возможности противника по влиянию на процесс подписи. Предложена модификация схемы подписи Эль-Гамаля, позволяющая обеспечить защиту от использования в процессе подписи низкоэнтропийных случайных значений. Доказана стойкость такой модификации в модели SUF-CMRA.

Судя по автореферату и публикациям, диссертация Бабуевой А.А. по уровню выполнения, новизне и актуальности соответствует критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова для диссертаций на соискание ученой степени кандидата наук, а ее автор, Бабуева Александра

Алексеевна, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидат физико-математических наук,
главный специалист, ООО «СФБ Лаб» И.М. Арбеков

Контактные данные:

тел.:
e-mail: igor.arbekov@sfblaboratory.ru
почтовый адрес:
г. Москва,

Адрес места работы:

127273, Москва, ул. Отрадная, д. 2Б, стр. 1, тел: +7 495 645 44 38

Я, Арбеков Игорь Михайлович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

«21» октября 2025 г.

Подпись Арбекова И.М. удостоверяю.

Генеральный директор
ООО «СФБ Лаб» О.А. Залунин