Биометрическое личностное шифрование

А. В. Поляков

В данной статье представлен протокол шифрования, в котором биометрические данные пользователя используются для генерации открытого ключа посредством нечеткого экстрактора. Это схема устойчива к адаптивной атаке с выбранным открытым текстом и обладает шифртекстом постоянного размера. определена модель безопасности и показано, что безопасность протокола основана на Билинейной задаче принятия решения Диффи-Хеллмана. Сравнительный анализ показывает большую устойчивость и безопасность предложенной схемы перед аналогами.

Введение

Асимметричная криптография стала элегантным решением задачи распределения ключей. Однако этот подход стало причиной возникновения другой проблемы. А именно, открытый ключ, в силу математических свойств асимметричных криптоалгоритмов, является набором случайных бит, не содержащих никакой информации о владельце, поэтому он не может служить средством аутентификации. Этот недостаток стал причиной появления иерархической системы сертификации открытых ключей. В настоящее время аутентификация пользователей происходит следующим образом:

1. Пользователь Алиса проходит процедуру проверки в удостоверяющем центре и получает сертификат;
2. Алиса посылает свой сертификат Бобу;
3. Боб получает сертификат удостоверяющего центра;
4. С помощью полученных сертификатов Боб производит аутентификацию Алисы.

Личностное шифрование впервые было предложено А. Шамиром [2] в 1984 году, которое возникло как идея упрощения этой схемы. Шамир предположил, что если бы появилась возможность использовать в качестве открытого ключа имя или почтовый адрес Алисы, то это лишило бы сложную процедуру аутентификации всякого смысла.

Под личностным шифрованием подразумевается криптосистема с открытым ключом, в которой пользователю разрешено выбрать адрес своей электронной почты либо телефонный номер в качестве открытого ключа вместо генерации случайным образом пары открытого и секретного ключей. Генератор секретного ключа вычисляет секретный ключ пользователя по личным данным пользователя и секретный мастер-ключ, после чего передает пользователю его секретный ключ.

Долгое время идея Шамира оставалась всего лишь красивой криптографической головоломкой, главным недостатком подобной схемы долгое время была невозможность использования биометрии в этой системе в силу ее изменчивости.

Однако в 2005 году в статье [3] была предложена концепция нечеткого личностного шифрования, в которой личностные характеристики были представлены набором атрибутов, а не строкой символов. В 2007 в статье [4] была предложена концепция цифровой подписи, основанной на пользовательской биометрии. В ней была предложена идея использования биометрических данных для создания открытого ключа, но не было предложено конкретной схемы. В 2008 году в статье [5] был впервые предложен протокол биометрического личностного шифрования. В 2010 году в статье [6] были предложены общие схемы биометрического личностного шифрования.

Однако протоколы, описанные в этих статьях, обладают следующими ограничениями: размер шифртекста линеен по пользовательским данным и требует большого количества операций при расшифровании. Целью настоящего исследования является устранение этих ограничений. В этой статье представлен новый протокол биометрического личностного шифрования, удовлетворяющий следующим свойствам:

- Постоянный размер шифртектста;
- Быстрый алгоритм генерации ключей;
- Эффективный алгоритм расшифрования. Представленный алгоритм расшифрования требует всего две операции спаривания, что

лучше, чем количество операций в аналогичных алгоритмах (линейное число от параметра, определяющего допустимое количество ошибок);

- Сводимость к билинейной задаче распознавания Диффи-Хеллмана. Сложность этой задачи считается выше сложности билинейной инверсионной задачи Диффи-Хеллмана, на которой основаны схемы [5], [6];

- Безопасность протокола. Протокол обладает стойкостью к атаке на основе адаптивно подобранных выбранной идентифицирующей информации и шифртекста (в то время как аналогичные схемы обладают устойчивостью только к атаке с выбранным открытым текстом).

Предварительные сведения и определения

Определение 1. *Пусть* $\mathbb{G}$ *и* $\mathbb{G}_1$ *- две мультипликативные циклические группы простого порядка* p*. Пусть* g *— порождающий элемент* $\mathbb{G}$*. Билинейным отображением называется отображение* $f : G \times G \to G_1$ *со следующими свойствами:*

1) билинейность: $f(u^a, v^b) = f(u, v)^{ab}$ $\forall u, v \in G, \forall a, b \in \mathbb{Z}_p$

2) невырожденность: $f(g, g) \neq 1_{\mathbb{G}_1}$

3) эффективная вычислимость: существует эффективный алгоритм, который вычисляет $f(u, v)$ $\forall u, v \in \mathbb{G}$*.*

Примерами таких отображений служат модифицированное спаривание Вейля и спаривание Тейта [7].

Определение 2. *(Билинейная задача распознавания Диффи-Хеллмана) Пусть дана группа* G *простого порядка* p*,* g *— порождающий элемент этой группы,* $g^a, g^b, g^c \in G$ *для некоторых случайным образом выбранных* $a, b, c \in \mathbb{Z}_p$*. Пусть дан* $Z \in \mathbb{G}_1$*, требуется выяснить, равен ли* Z *величине* $f(g, g)^{abc}$ *или нет.*

Определение 3. *Скажем, что алгоритм* $A(\varepsilon)$*, где* $\varepsilon-$ *параметр алгоритма* A*, на выходе которого может быть получено значение* $\{0, 1\}$*, имеет преимущество* ε *в решении задачи распознавания Диффи-Хеллмана, если*

$$P(A(f(g, g)^{a,b,c}, g, g^a, g^b, g^c) = 1) - P(A(Z, g, g^a, g^b, g^c) = 1) \geq \varepsilon$$

Здесь $P(B)-$ частота события B. Частота вычисляется при условии, что бит на выходе алгоритма A является случайным.

Определение 4. *Будем говорить, что если не существует алгоритма, который с преимуществом ε за время t может решить билинейную задачу распознавания Диффи-Хеллмана, то выполняется предположение $(t, e)-$ безопасности.*

Определение 5. *Статистическим расстоянием между двумя вероятностными распределениями A и B называется величина*

$$SD(A, B) = \frac{1}{2} \sum_{v} (|P(A = v) - P(B = v)|).$$

Определение 6. *Мин-энтропией случайной величины A называется называется величина*

$$H_{\infty}(A) = -\log(\max_{a}(P(A) = a)).$$

Определение 7. *Функция $f(x) : \mathbb{Z} \to \mathbb{R}$ называется пренебрежимо малой, если для каждого полинома $p(x)$ существует такая константа N_p, что $f(x) \leq \frac{1}{p(x)}$ $\forall x \geq N_p$.*

Схема разделения секрета Шамира

В 1979 г. А. Шамир предложил схему разделения секрета между n сторонами [8] таким образом, что для восстановления секрета достаточно не менее k частей, и никакие (k-1) частей не дают никакой информации о секрете.

Пусть требуется разделить секрет S между n участниками так, чтобы восстановить его смогли $k \leq n$ человек.

Для этого выбирается простое число $p > S$. Оно задает конечное поле порядка GF(p). Над этим полем строится многочлен степени k-1:

$$F(x) = S + \sum_{i=1}^{k-1} a_i x^i \ mod \ p$$

В схеме разделения секрета Шамира ключ секрет делится на несколько частей, которые впоследствии передаются d различным участникам. Для восстановления секрета требуется определенное количество частей.

Здесь $S-$ разделяемый секрет, а коэффициенты $a_1, \ldots, a_{d-1} \in GF(p)$ выбираются случайным образом.

Для всех $i \in \{1, \ldots, n\}$, каждому участнику P_i ставится в соответствие уникальный элемент $\alpha_i \in GF(p)$, после чего ему посылается его доля секрета: $S_i = F(\alpha_i)$.

Любая группа участников M численностью не менее k может восстановить секрет, вычислив

$$F(x) = \sum_{P_i \in M} l_i(x) S_i,$$

где

$$l_i(x) = \prod_{p_j \in S, i \neq j} \frac{x - \alpha_i}{\alpha_i - \alpha_j} \; mod \; p$$

С другой стороны, никакая группа участников численностью меньше k не сможет восстановить секрет S.

Нечеткие экстракторы

Современная криптография базируется на использовании независимых равномерно распределенных случайных строк для создания секретных ключей. Строки, не обладающие свойствами случайности и не являющиеся воспроизводимыми (а именно такими строками являются биометрические шаблоны: действительно, отпечаток пальца, радужка глаза, лицо не является ни случайным, ни точно воспроизводимым при повторных измерениях), кажутся не столь привлекательными для криптографических целей. Тем не менее, в [1] предложен строгий и теоретически обоснованный подход использования таких строк в криптографических приложениях. Он базируется на использовании нового криптографического примитива: нечеткого экстрактора. Нечеткий экстрактор определяется следующим образом.

Пусть $\mathcal{M} = \{0,1\}^n-$ метрическое пространство с метрикой $\rho : \mathcal{M} \times \mathcal{M} \to \mathbb{Z}^+$.

Каждая точка метрического пространства представляет собой биометрический шаблон, метрика - расстояние между шаблонами $T, T' \in \mathcal{M}$.

Определение 8. *Нечетким экстрактором называется пара рандомизированных функций (Gen,Rep) со следующими свойствами:*

1) Функция $Gen : \mathcal{M} \to \{0,1\}^l \times P$ *получает на вход биометрический шаблон* $T \in \mathcal{M}$ *и возвращает строку* $R \in \{0,1\}^l$ *и вспомогательную информацию* $P \in \{0,1\}^*$*;*

2) Функция $Rep : \mathcal{M} \times \{0,1\}^* \to \{0,1\}^l$ *получает на вход элемент* $T' \in \mathcal{M}$ *и битовую строку* $P \in \{0,1\}^*$. *Свойство корректности нечетких экстракторов гарантирует, что если* $\rho(T,T') < t$ *и пара* (R,P) *является образом* $Gen(T)$, *то* $Rep(T',P) = R$. *Если* $\rho(T,T') \geq t$, *то значение Rep(T',P) не определено.*

3) Свойство безопасности гарантирует, что для любого распределения W *на* $\mathcal{M}$ *с мин-энтропией m, выход функции Gen близок к равномерному распределению даже при условии обладания информацией P, а именно, если* $Rep(W) \to (R,P)$, *то* $SD((R,P),(U_l,P)) \leq \varepsilon$.

Будем говорить, что нечеткий экстрактор эффективен, если функции *Rep* и *Gen* вычислимы за полиномиальное время.

Нечеткий экстрактор характеризуется работой с неравномерными распределениями строк и устойчивостью к ошибкам. Он надежно извлекает случайную строку R от входа T устойчивым к ошибкам способом. Если вход незначительно меняется по метрике ρ, то выход экстрактора R остается тем же. Для восстановления R по T' экстрактор использует публичные данные — строку P, однако R остается случайной при известном P.

В [1] приведен конкретный пример нечеткого экстрактора, построенного в пространстве $\mathcal{M} = \{0,1\}^n$ с метрикой Хэмминга и криптографической хэш-функцией $H : \{0,1\}^n \to \{0,1\}^l$.

Функция *Gen* принимает на вход биометрический шаблон T, возвращает $ID = H(T)$ и публичную строку $P = T \oplus C_e(ID)$, где C_e- функция кодирования. Функция *Rep* получает на вход публичную строку P и биометрический шаблон T' и вычисляет $ID' = C_d(T' \oplus P) = C_d(T' \oplus T \oplus C_e(ID)) = e' \oplus C_e(ID)$, где $e' = T' \oplus T$.

Тогда, если $\rho(T,T') < t$, то $ID = ID'$. Здесь C_d- функция декодирования, исправляющая до t ошибок.

Обработка биометрических данных

Обработка биометрических данных производится в четыре этапа:

1) Биометрия пользователя сканируется посредством оптического сенсора. Получается изображение биометрической модальности.

2) С помощью экстрактора из изображения выделяется вектор признаков (атрибутов).Каждый i-й атрибут связан с уникальным $\mu_i \in \mathbb{Z}_p^*$. Тогда личность моделируется набором биометрических атрибутов $(\mu_1, ..., \mu_n)$, где n- количество биометрических модальностей.

3) Каждый признак, формирующий вектор признаков, преобразуется в бинарную строку для генерации биометрического шаблона.

4) Нечеткий экстрактор используется для генерации уникальной строки ID посредством кодов, исправляющих ошибки, из биометрического шаблона b таким образом, что разрешается допустить t ошибок. То есть если $\rho(b, b') < t$, то $ID(b) = ID(b')$.

Определение биометрического личностного шифрования

Система личностного биометрического шифрования состоит из 4-х алгоритмов: установка, экстракция, шифрование, расшифрование.

Установка: дан параметр безопасности k и порог d, алгоритм порождает генерирует секретный мастер-ключ MK и множество публичных параметров PK системы.

Экстракция: дан биометрический шаблон T и секретный мастер-ключ MK, алгоритм возвращает конфиденциальный ключ пользователя K_T.

Шифрование: даны PK, биометрический шаблон T', сообщение M, алгоритм возвращает шифртекст C.

Расшифрование: дан секретный ключ K_T и шифртекст C, зашифрованный посредством биометрического шаблона T'. алгоритм возвращает текст M в случае, если $|T \cap T'| > d$, и останавливает работу в противном случае.

Модель угрозы

Определение 9. *Биометрическое личностное шифрование устойчиво к атаке с выбранным шифртекстом, если не существует алгоритма A, имеющего не пренебрежимо малое преимущество в следующей игре:*

Инициализация. Противник A генерирует биометрический шаблон T'.

Подготовительный этап. Претендент B запускает алгоритм установки и посылает публичные данные PK противнику A.

Первый этап. Противник A посылает запросы экстракции и расшифрования секретным ключом.

1. Запросы экстракции. A посылает запросы для личности γ_j такой, что $|\gamma_j \cap T'| < d$. B ответ на запрос B запускает алгоритм экстракции с целью получить секретный ключ K_{γ_j} и отправляет его A.

2. Запросы дешифрования. A отправляет запросы расшифрования на шифртекст C и биометрию γ_j, где $|\gamma_j - T'| \geq d$. B ответ, B запускает алгоритм экстракции с целью получить секретный ключ γ_j и затем запускает алгоритм расшифрования, чтобы получить открытый текст M, который отправляет A.

Задача: Противник A отправляет 2 сообщения M_0, M_1 B. B случайно выбирает число $\beta \in \{0, 1\}$ и шифрует текст M_β биометрией T'. Шифртекст отправляется к A.

Второй этап. A отправляет запросы экстракции и расшифрования как аналогично первому этапу.

Догадка: противник A случайно угадывает число $\beta' \in \{0, 1\}$ и побеждает, если $\beta' = \beta$. Преимущество противника A в этой игре определяется следующим образом:

$$Adv_A = |P(\beta' = \beta) - \frac{1}{2}|.$$

Определение 10. *Скажем, что биометрическая личностная система шифрования $(t, \varepsilon, q_E, q_D)-$ безопасна, если за время t противник посылает не более q_E запросов экстракции, q_D запросов расшифрования, и получает преимущество в игре не более ε.*

Система биометрического личностного шифрования

В данном разделе приводится список обозначений и описание системы биометрического личностного шифрования. У системы есть три участника: Генератор секретных ключей (Мерлин), Передатчик (Алиса) и Приемник (Боб). На этапе шифрования Алиса получает биометрию от Боба и публичный параметр P. Алиса выделяет из биометрии вектор признаков и вычисляет биометрическую строку с помощью нечеткого экстрактора. На этапе дешифрования предложенная система устойчива к ошибкам, возникающих из-за изменчивости биометрической информации.

Будем считать, что если $|T \cap T'| > d$, то $|b - b'| < t$ и $ID = ID'$. В этом случае Алиса может расшифровать текст, зашифрованный с помощью T', используя секретный ключ, соответствующий T, если b и b' находятся на расстоянии не более t друг от друга.

Список обозначений

$G-$ мультипликативная группа простого порядка p.

G_1- мультипликативная группа простого порядка p.

$g-$ порождающий элемент группы G.

$f : G \times G \to G_1-$ билинейное упорядочение

$M-$ сообщение C_e- функция кодирования кода, исправляющего ошибки

C_d- функция декодирования кода, исправляющего ошибки

$d-$ пороговое значение параметра устойчивости к ошибке, которое представляет собой расстояние между двумя биометрическими шаблонами для успешного расшифрования сообщения.

H_1 - криптографическая хэш-функция, $H_1 : \mathbb{Z}_p^* \times \{0,1\}^* \to \mathbb{Z}_p^*$

Подготовительный этап

Пусть k_0- параметр безопасности, Мерлин генерирует две мультипликативные группы G и G_1 простого порядка $p > 2^{k_0}$ и выбирает порождающий элемент $g \in G$. После этого Мерлин выбирает случайный элемент $g_1 \in G, s \in \mathbb{Z}_p^*$ и вычисляет $g_2 = g^s$ и выбирает порог ошибок $d \in \mathbb{Z}^+$.

После этого Мерлин публикует параметры $\{g, g_1, g_2, d\}$, мастер-ключ s он держит в секрете.

Экстракция

Сначала создается вектор признаков Боба $T = (\mu_1, ..., \mu_n)$ из изображения, полученного со сканера посредством алгоритма выделения признаков, входящего в состав любой биометрической системы. Каждый $\mu_i \in \mathbb{Z}_p^*, i \in \{1, ..., n\}$. Далее вычисляется $ID = H(b)$ от биометрического шаблона b.

Пусть дан вектор признаков T и ID, Мерлин создает секретный ключ следующим образом:

1) выбирается случайный полином степени $(d-1)$:

$$p(x) = a_0 + a_1 x + ... + a_{d-1} x^{d-1}$$

такой, что $p(0) = a_0 = s$.

2) Для $\mu_i \in T$ вычислить $d_{i,1} = (g_1 g^{H_1(T,ID)})^p(\mu_i)$, $d_{i,2} = g^p(\mu_i)$, $P = Gen(b, ID)$

3) Мерлин передает конфиденциальным образом ключ $\{d_{i,1}, d_{i,2}\}_{mu_i \in T}$ пользователю Бобу и публикует P.

Шифрование

Алиса получает биометрические данные Боба и публичные данные P. Алиса по ним извлекает T' и вычисляет $ID' = Rep(b', P)$. При $\rho(b, b') < t$ имеем $ID = ID'$.

При данном ID', T' и сообщении M Алиса делает следующее:

1) Выбирает случайное число $r \in \mathbb{Z}_p^*$ и вычисляет следующие величины:

$$C_1 = g^r$$

$$C_2 = (g^{H_1(T', ID')})^r$$

$$C_3 = f(g_1, g_2)^r M$$

и отправляет шифртекст $C = (T', C_1, C_2, C_3)$ Бобу.

Расшифровка

Дан шифртекст $C = (T', C_1, C_2, C_3)$, Боб расшифровывает C своим закрытым ключом K_T следующим образом:

1) если $|T \cap T'| < d$, то расшифровка прерывается;

2) если $|T \cap T'| \geq d$, то Боб выбирает любое подмножество $S \subseteq T \cap T'$, $|S| = d$ и вычисляет

$$M = C_3 \frac{f(C_2, \prod_{\mu_j \in S} d_{i,2}^{l_i(0)})}{f(C_1, \prod_{\mu_j \in S} d_{i,1}^{l_i(0)})}$$

Лемма 1. *Пусть M-открытый текст, в указанных выше обозначениях величины $C_1 = g^r$, $C_2 = (g^{H_1(T', ID')})^r$, $C_3 = f(g_1, g_2)^r M$,*

$d_{i,1} = (g_1 g^{H_1(T, ID)})^p(\mu_i)$,

$d_{i,2} = g^p(\mu_i)$,

тогда справедливо равенство

$$M = C_3 \frac{f(C_2, \prod_{\mu_j \in S} d_{i,2}^{l_i(0)})}{f(C_1, \prod_{\mu_j \in S} d_{i,1}^{l_i(0)})}$$

Доказательство: *Действительно,*

$$C_3\frac{f(C_2,\prod_{\mu_j\in S}d_{i,2}^{l_i(0)})}{f(C_1,\prod_{\mu_j\in S}d_{i,1}^{l_i(0)})}=f(g_1,g_2)^rM\frac{f((g^{H_1(T',ID')})^r,\prod_{\mu_j\in S}d_{i,2}^{l_i(0)})}{f(g^r,\prod_{\mu_j\in S}d_{i,1}^{l_i(0)})}=$$

$$=\frac{f((g^{H_1(T',ID')})^r,g^s)}{f(g^r,(g_1g^{H_1(T,ID)})^s)}Mf(g_1,g_2)^r=\frac{f((g^{H_1(T',ID')})^r,g^s)}{f((g^{H_1(T,ID)})^s,g^r)f(g_1,g^r)^s}Mf(g_1,g_2)^r=$$

$$=\frac{f((g^{H_1(T',ID')})^r,g^s)}{f((g^{H_1(T,ID)})^s,g^r)f(g_1,g^r)^s}Mf(g_1,g_2)^r=$$

$$\frac{f((g^h)^r,g^s)}{f((g^h)^s,g^r)f(g_1,g^r)^s}Mf(g_1,g_2)^r=M.$$

Здесь $h=H_1(T',ID')=H_1(T,ID)$ *в силу того, что* $ID=ID'$, *т.к.* $T\cap T'>d$ *и* $\rho(b,b')<t$.

Лемма доказана

Анализ безопасности

Теорема 1. *Пусть* $G-$*мультипликативная группа,* $|G|=p$, *где* $p-$ *простое, и для* G *выполняется* (t',ε') $--$*предположение безопасности. Тогда построенная система биометрического личностного шифрования* $(t,\varepsilon,q_E,q_D)-$ *безопасна, где* $\varepsilon=\varepsilon'$, $t=t'-d(t_{MULT}+t_{EXP})q_E$, *где* $t_{MULT}-$*время, требующееся на умножение,* $t_{EXP}-$*время на возведение в степень,* $d-$ *порог устойчивости системы к ошибкам,* q_E- *количество запросов экстракции.*

Доказательство: *Пусть существует* $(t,e,q_E,q_D)-$*противник Ева. Тогда может быть построен алгоритм* C, *решающий билинейную задачу распознавания Диффи-Хеллмана за время* t' *с вероятностью* ε'. *Под алгоритмом будем понимать кортеж* (g,g^a,g^b,g^c,Z) *из формулипровки билинейной задачи распознавания Диффи-Хелммана, где* Z *либо равно* $f(g,g)^{abc}$ *либо случайный элемент из* G_1.

Далее игра развивается следующим образом.

1. Инициализация. Евой выбирается биометрическая личность $T^*=(\mu_1^*,...,\mu_n^*)$.

2. Подготовительный этап. Ева на вход алгоритму C *устанавливает параметры* $g_1=g^a$, $g_2=g^b$ *и параметр ошибки* $d\in\mathbb{Z}^+$.*Алгоритм на выходе возвращает Еве публичные параметры* $P=(g,g_1,g_2,d)$

3.Хэш-запросы: будем считать, что Ева может посылать хэш-запросы на любом этапе игры. При получении запроса T_i, если в хэш-таблице существует (T_i, α_i, g_i^h), возвращается g^{h_i}. Если $T_i = T^*$, выбрать случайно $\alpha^* \in \mathbb{Z}_p$ и положить $g^{h^*} = g^{\alpha^*}$. В противном случае выбрать случайным образом $\alpha_i \in \mathbb{Z}_p$ и вычислить $g^{h_i} = \frac{g^{l_i}}{g_1}$.

Этап 1. на данном этапе Ева посылает запросы экстракции и запросы расшифрования секретного ключа.

1) Запросы экстракции. При получении запроса секретного ключа для $\gamma_j = (\mu_1, ..., \mu_n)$, где $|\gamma_j \cap T^*| < d$, алгоритм C устанавливает $\Gamma = \gamma_j \cap T'$ и пусть $\Gamma'-$ любое множество, удовлетворяющее следующим условиям: $\Gamma \subseteq \Gamma' \subseteq \gamma_j$, $|\Gamma'| = d - 1$.

Пусть $S = \Gamma' \cup \{0\}$. запустить указанный выше запрос для получения $(\gamma_j, \alpha_j, g^{h_j})$ из хэш-таблицы.

а) Для каждого $\mu_i \in \Gamma'$, выберем случайным образом $\lambda_i \in \mathbb{Z}_p$ и вычислим $(d_{i,1}, d_{i,2}) = ((g_1 g^{h_j})^{\lambda_i}, g^{\lambda_i})$. Для случайного полинома $p(x) \in \mathbb{Z}_p[x]$, $deg(p(x)) = d - 1$, $p(0) = b$, определим $\lambda_i = p(\mu_i)$. Таким образом, алгоритм C может успешно построить $(d_{i,1}, d_{i,2})$ для $\mu_i \in \Gamma'$.

б) Для каждого $\mu_i \in \gamma_j \setminus \Gamma'$, $i \in \{1, ..., n\}$, вычислить:

$$d_{i,1} = g_2^{l_0(\mu_i)\alpha_j} \prod_{\mu_k \in \Gamma'} (g_1 g^{h_j})^{l_k(\mu_i)\lambda_k},$$

$$d_{i,2} = g_2^{l_0(\mu_i)} \prod_{\mu_k \in \Gamma'} (g)^{l_k(\mu_i)\lambda_k}.$$

Заметим, что $g_1 g^{h_j} = g^{l_j}$, если $\gamma_j \neq T^*$.

Тогда

$$d_{i,1} = g^{\alpha_j l_0(\mu_i) b} g^{\alpha_j (\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k))} = g^{\alpha_j (l_0(\mu_i) p(0) + (\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k)))} =$$

$$= g^{l_j p(\mu_i)} = g^{l_j p(\mu_i)} = (g_1 g^{h_j})^{p(\mu_i)} = (g_1 g^{h_j})^{p(\mu_i)} =$$

$$(g_1 g^{H_1(\gamma_j, ID)})^{p(\mu_i)}$$

$$d_{i,2} = g^{l_0(\mu_i) b} g^{(\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k))} = g^{l_0(\mu_i) p(0) + (\sum_{\mu_k \in \Gamma'} l_k(\mu_i) p(\mu_k))} = g^{p(\mu_i)}.$$

Таким образом, алгоритм C может успешно имитировать секретный ключ пользователя $\gamma_j = (mu_1, ..., \mu_n)$.

2. Запросы расшифрования

Для дешифровки запроса $C = (\gamma'_j, C_1, C_2, C_3)$ *пользователя* γ_j, *где* $|\gamma'_j \cap \gamma_j| \geq d$, *алгоритм* C *работает следующим образом:*

а) C *запускает указанный выше алгоритм экстракции секретного ключа для создания ключа* $K_{\gamma_j} = (d_{i,1}, d_{i,2})_{\mu_i \in \gamma_j}$;

б) C *выбирает любое множество* S, *удовлетворяющее условиям:* $S \subseteq \gamma_j \cup \gamma'_j$ *и* $|S| = d$. *После этого* C *вычисляет открытый текст* M *по лемме 1 и отправляет его Еве.*

Попытка взлома:

Противник Ева генерирует два сообщения M_0 *и* M_1. *Алгоритм* C *случайно выбирает* $\beta \in \{0,1\}$ *и шифрует* M_β *с помощью* T^*, *который получен от* b^*. *Шифртекст возвращается к Еве:*

$C^* = (T^*, C_1^*, C_2^*, C_3^*) = (T^*, g^c, (g^c)^{\alpha^*}, ZM_\beta)$

Если $Z = f(g,g)^{abc}$, *то* C^*- *корректная шифровка сообщения* M_β, *так как* $C_1^* = g^c$, $C_2^* = (g^c)^{\alpha^*} = (g^{\alpha^*})^c = (g^{h^*})^c = (g^{(T^*, ID)})^c$,

$C_3^* = ZM_\beta = f(g,g)^{abc} M_\beta = f(g_1, g_2)^c M_\beta$

2. Если Z *равномерно на* G_1, C_3^* *не зависит от* M_β. *Поэтому* C^* *не зависит от* β *с точки зрения Евы.*

Этап 2. Ева посылает запросы экстракции ключа и дешифрования как на этапе 1.

Предположение: Ева делает предположении о значении $\beta' \in \{0,1\}$. *Алгоритм* C *завершает игру следующим образом. Если* $\beta' = \beta$, *то* C *возвращает 1, что означает* $Z = f(g,g)^{abc}$. *В противном случае* C *возвращает 0, что означает, что* Z *выбрано случайным образом в* G_1.

Вероятностный анализ:

1) если $Z = f(g,g)^{abc}$, *то* $|P(\beta' = \beta) - \frac{1}{2}| \geq \varepsilon$

2) если $Z-$ *случайный элемент* G_1, *то* $P(\beta' = \beta) = \frac{1}{2}$

3)Отсюда

$$|P(C(f(g,g)^{abc}, g, g^a, g^b, g^c)) = 0| - P(C(Z, g, g^a, g^b, g^c)) = 0| \geq |(\frac{1}{2} \pm \varepsilon) - \frac{1}{2}| = \varepsilon$$

Временной анализ:

Время работы системы определяется умножением и возведением в степень на этапе запросов экстракции. Отсюда $t' = t + d(t_{MULT} + t_{EXP})q_E$.

Теорема доказана

Сравнение с существующими нечеткими системами личностного шифрования

Таблица 1: Сравнительный анализ

Система	Sahai [3]	Sarier [5]	Предложенная система
Размер открытого ключа	$u\|G\| + G_1$	$2\|G\|$	$3\|G\|$
Размер секретного ключа	nG	nG	$2n\|G\|$
Размер шифртекста	$n\|G\| + \|G_1\|$	$n\|G\| + \|M\|$	$2\|G\| + \|G_1\|$
Сложность генерации ключа	nt_{EXP}	nt_{EXP}	$2nt_{EXP}$
Сложность шифрования	$(n+1)t_{EXP}$	$t_{pair} + nt_{EXP}$	$3t_{EXP}$
Сложность расшифрования	dt_{PAIR}	dt_{PAIR}	$2t_{PAIR}$
Связанная задача	МБДХ	k-ИБДХ	БРДХ

Размер открытого и секретного ключей в [5] меньше, чем в предложенной схеме. При этом сложность генерации ключа на n (количество биометрических модальностей) операций возведения в степень больше, чем в [5]. Размер шифртекста в [6] равен $n|G| + |M|$, где $|M|-$ размер шифртекста. В предложенной схеме шифртекст имеет постоянный размер.

Сложность шифрования и дешифрования в предложенной схеме ниже, чем в [5].

При этом предложенная система основана на билинейной задаче распознавания Диффи-Хеллмана (БРДХ), в то время как в [5] система основана на задаче k-инверсной билинейной задаче диффи-Хеллмана, трудность которой ниже, чем БРДХ.

таким образом, предложенная схема обладает большей вычислительной эффективностью и более сильной безопасностью, чем [5]

Сравнительный анализ приведен в таблице 1.

Заключение

В этой главе была описана новая биометрическая система личностного шифрования, которая отличается от ближайших аналогов постоянным

размером шифртекста, меньшей сложностью шифрования и расшифрования и сводится к более трудной задаче, чем аналоги.

Список литературы

[1] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in Proc. Eurocrypt, 2004, pp. 523–540.

[2] Shamir, A., 1984. Identity-Based Cryptosystems and Signature Schemes. Proc. Crypto, p.47-53.

[3] Sahai, A., Waters, B., 2005. Fuzzy Identity-Based Encryption. Proc. EUROCRYPT, p.457-473

[4] Burnett, A., Byrne, F., Dowling, T., Duffy, A., 2007. A biometric identity based signature scheme. Int. J.Network Secur., 5(3):317-326

[5] Sarier, N.D., 2008. A New Biometric Identity Based Encryption Scheme. Proc. ICYCS, p.2061-2066

[6] Sarier, N.D., 2010. Generic Constructions of Biometric Identity Based Encryption Systems. Proc. WISTP, p.90-105.

[7] Boneh, D., Franklin, M.K., 2001. Identity-Based Encryption from the Weil Pairing. Proc. CRYPTO, p.213-229.

[8] Shamir A. How to share a secret // Commun. ACM — New York City: ACM, 1979. — Vol. 22, Iss. 11. — P. 612-613.

[9] Cheon, J.H., 2006. Security Analysis of the Strong Diffie-Hellman Problem. Proc. EUROCRYPT, p.1-11