Литература

1. Staszek, K. Theoretical Limits and Accuracy Improvement of Reflection-Coefficient Measurements in Six-Port Reflectometers [Text] / K. Staszek, S. Gruszczynski, K. Wincza // Microwave Theory and Techniques, IEEE Trans. on. 61. – 2013. – №8. – P.2966-2974.
2. Энген, Г. Ф. Успехи в области СВЧ-измерений [Text] / G. F. Engen // ТИИЭР. – 1978. –Т.66, №4. – С. 8-20.
3. Engen, G. F. The six-port reflectometer: an alternative network analyzer [Text] / G. F. Engen // IEEE Trans. Microwave Theory Tech. – 1977. – V. MTT-25, № 12. – P.1075-1080.
4. Кабанов, Д. А. Опыт разработки автоматических СВЧ цепей с 12-полюсными рефлектометрами [Текст] / Д. А. Кабанов, С. М. Никулин, С. В. Петров // Измерительная техника. – 1985. – №10. – С. 38 – 40.
5. Барташевский Е.Л. Векторный СВЧ-рефлектометр на основе четырехплечего делителя мощности [Текст] / Е. Л. Барташевский, В. А. Карлов // Электронная техника. Сер. 1, Электроника СВЧ. – 1989. – Вып. 1(415). – С.38 – 44.
6. А.С. СССР №1814076, кл. G 01 R 27/06. Устройство для измерения комплексного коэффициента отражения // Барташевский Е. Л., Борулько В. Ф., Карлов В. А., Лысоконь В. В., Славин И. В. – 1992.
7. Карлов, В. А. 30-ГГц крестообразный анализатор комплексного коэффициента отражения [Текст] / В. А. Карлов, К. К. Тарасов // 22-я Международная Крымская конференция “СВЧ техника и телекоммуникационные технологии”. – Севастополь, 2012. – С. 807-808.
8. Прохода, И. Г. Метод частичных пересекающихся областей для исследования волноводно-резонаторных систем сложной формы [Текст] / И. Г. Прохода, В. П. Чумаченко // Изв. вузов. Радиофизика. – 1973. – Т.16, № 10. – С. 1578-1581.
9. Морс, Ф. М. Методы теоретической физики [Текст] / Ф. М. Морс, Г. Фешбах. – Т.1. – М.: ИЛ, 1958. – 1960 с.
10. Karlov, V. Equivalent circuit of X-shaped converter of complex reflection coefficient analyzer [Text] / V. Karlov // Восточно-Европейский журнал передовых технологий. – 2013. – №4/9(64). – С. 8-11.
11. Karlov, V. A. Mathematical model of cross-formed transformer of vector reflectometer [Текст] / V.A. Karlov, V. S. Svyatsky // Proc. Int. Conf. on Actual Problems of Measuring Technique. – Kyiv, 1998. – pp.302 - 303.
12. Карлов, В. А. Крестообразный сумматор пятиплечего анализатора комплексного коэффициента отражения [Текст] / В. А. Карлов // 23-я Международная Крымская конференция “СВЧ техника и телекоммуникационные технологии”. – Севастополь, 2013. – Т.2.– С. 961-962.
13. Карлов, В. А. Разработка и создание сверхвысокочастотных виртуальных осциллографов комплексного коэффициента отражения на основе электродинамического подхода [Текст] / В. А. Карлов // 21-я Международная Крымская конференция “СВЧ техника и телекоммуникационные технологии”. – Севастополь, 2011. – Т.2.– С. 879 - 880.

Запропоновані криптографічні протоколи доказу із нульовим розголошенням знання на еліптичних кривих, що дозволяють встановити істинність твердження й при цьому не передавати якої-небудь додаткової інформації про саме твердження, а також значно зменшити розміри параметрів протоколу й збільшити криптографічну стійкість

Ключові слова: криптографічний протокол, еліптичні криві, ідентифікація, автентифікація, коректність, нульове розголошення

Предложены криптографические протоколы доказательства с нулевым разглашением знания на эллиптических кривых, позволяющие установить истинность утверждения и при этом не передавать какой-либо дополнительной информации о самом утверждении, а также значительно уменьшить размеры параметров протокола и увеличить криптографическую стойкость

Ключевые слова: криптографический протокол, эллиптические кривые, идентификация, аутентификация, корректность, нулевое разглашение

УДК 004.056.55:003.26

МОДИФИКАЦИЯ ПРОТОКОЛОВ ШНОРРА И ОКАМОТО НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

А. В. Онацкий
Кандидат технических наук,
старший преподаватель
Кафедра информационной безопасности и передачи данных
Одесская национальная академия связи им. А. С. Попова
ул. Кузнечная, 1, г. Одесса, Украина, 65029
E-mail: onatsky@mail.ru

1. Введение

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечение информационной безопасности при взаимодействии пользователей, является использование методов и средств, позволяющих одной

© А. В. Онацкий, 2013

(проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. В протоколах типа «запрос–ответ» (challenge–response) нарушитель, контролируя канал связи, может навязывать специально подобранные запросы и, анализируя ответы, получать информацию о секрете. Чтобы избежать этого, применяют протоколы доказательства знания, которые обладают дополнительным свойством нулевого разглашения секрета [1, 2].

2. Анализ исследований и публикаций

В криптографии доказательство с нулевым разглашением (zero-knowledge proof) – это интерактивный протокол, позволяющий одной из сторон (проверяющему, verifier) убедиться в достоверности какого-либо утверждения, не получив при этом никакой другой информации от второй стороны (доказывающего, prover) [3 – 5].

Цель доказывающего – убедить проверяющего в истинности некоторого утверждения. Проверяющий либо принимает, либо отвергает доказательство. В протоколах с нулевым разглашением доказательство имеет вероятностный характер. Если доказываемое утверждение, верно, то доказательство должно быть справедливым с вероятностью, стремящейся к единице при увеличении числа циклов протокола. Если же доказываемое утверждение ложно, то при увеличении числа циклов протокола вероятность правильности доказательства должна стремиться к нулю.

Широкое распространение при идентификации и аутентификации получили криптографические протоколы доказательства с нулевым разглашением на базе ассиметричного шифрования, наиболее известными являются: Фиата–Шамира, Шнорра, Окамото, Гиллоу–Кискатр, Брикелла–Мак-Карли, Фейга–Фиата–Шамира (табл. 1) [1 – 3, 5, 6].

Таблица 1

Криптографические протоколы с нулевым разглашением

Название протокола	Вычисление	Проверка
Фиата–Шамира (Fiat–Shamir)	1. A → B: certa, $\gamma \equiv r^2 \pmod n$; 2. A ← B: x; 3. A → B: $y \equiv r\,k^x \pmod n$.	$\gamma = (y^2\,Ya^x) \bmod n$
Шнорра (Schnorr)	1. A → B: certa, $\gamma \equiv \alpha^r \pmod p$; 2. A ← B: x; 3. A → B: $y \equiv (r + kx) \bmod q$.	$\gamma = (\alpha^y Y_a^{\,x}) \bmod p$
Окамото (Okamoto)	1. A → B: certa, $\gamma \equiv \alpha_1^{r_1}\,\alpha_2^{r_2} \pmod p$; 2. A ← B: x; 3. A → B: $y_1 \equiv (r_1 + k_1 x) \bmod q$; $y_2 \equiv (r_2 + k_2 x) \bmod q$.	$\gamma = (\alpha_1^{y_1}\,\alpha_2^{y_2}\,Y_a^{\,x}) \bmod p$
Гиллоу–Кискатр (Guillou–Quisquater)	1. A → B: certa, $\gamma \equiv r^e \pmod n$; 2. A ← B: x; 3. A → B: $y \equiv r\,k^x \pmod n$.	$\gamma = (Ya^x\,y^e) \bmod n$
Брикелла–Мак-Карли (Brickell–McCurley)	1. A → B: certa, $\gamma \equiv \alpha^r \pmod p$; 2. A ← B: x; 3. A → B: $y \equiv (r + k\,x) \bmod (p - 1)$.	$\gamma = (\alpha^y Y_a^{\,x}) \bmod p$
Фейга–Фиата–Шамира (Feige–Fiat–Shamir)	1. A → B: certa, $\gamma \equiv r^2 \pmod n$; 2. A ← B: $x_1, ..., x_k$; 3. A → B: $y \equiv r(k_1^{x_1} \cdot ... \cdot k_k^{x_k}) \bmod n$.	$\gamma = y^2(Y_{a_1}^{x_1} \cdot ... \cdot Y_{a_k}^{x_k}) \bmod n$

Корректность и стойкость представленных в табл. 1 протоколов определяется дискретным логарифмированием в простом конечном поле Z_n / Z_p, а также увеличением количества циклов аккредитации при разных случайных значениях r и x.

С развитием методов и средств криптоанализа, а также быстрого развития технологий и мощности вычислительных компьютерных систем, возникает необходимость увеличивать размеры общесистемных параметров протокола, вследствие чего увеличивается ресурсоемкость и сложность выполнения базовых операций в полях. Для уменьшения размера параметров протокола и увеличения криптографической стойкости целесообразно использовать эллиптические кривые.

Криптосистемы на эллиптических кривых ECC (Elliptic Curve Cryptography) [7 – 9] относятся к классу криптосистем с открытым ключом. Их безопасность, как правило, основана на трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой ECDLP (Elliptic Curve Discrete Logarithm Problem) [7, 10, 11]. Решение проблемы ECDLP является значительно более сложным, чем решение проблемы дискретного логарифмирования, на которой базируются криптографические протоколы, представленные в табл. 1.

Таблица 2

Размер ключей для ECC и RSA согласно NIST

ECC key, Bits	RSA key, Bits	Key ratio
163	1024	1 : 6
256	3072	1 : 12
384	7680	1 : 20
512	15360	1 : 30

Многочисленные исследования показали [10, 11], что криптосистемы на основе эллиптических кривых превосходят другие системы с открытым ключом по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при программной и аппаратной реализации.

Отсюда следует возможность применения более коротких ключей (табл. 2) [12].

3. Цель работы

Целью статьи является разработка криптографических протоколов доказательства с нулевым разглашением знания на эллиптических кривых, которые позволяют значительно уменьшить размер параметров протокола и увеличить криптографическую стойкость.

4. Протоколы доказательства с нулевым разглашением на эллиптических кривых

Протоколы идентификации можно рассматривать как вид интерактивного доказательства знания. Протокол доказательства знания (proof of knowledge protocol) – интерактивное доказательство, в котором доказывающий убеждает проверяющего в том, что он владеет секретной информацией.

Интерактивное доказательство (interactive proof) – понятие теории сложности вычислений, составляющее основу понятия доказательства с нулевым разглашением [4].

Протокол интерактивного доказательства должен учитывать возможность обмана со стороны обоих участников. Если участник А (доказывающий) на самом деле не знает доказываемого утверждения (либо от имени участника А выступает кто-либо другой), то участник В (проверяющий) должен обнаружить факт обмана.

Поэтому доказательство знания характеризуется тремя свойствами: полнотой, корректностью и нулевое разглашение [3, 4].

Протоколы доказательства выполняют в виде последовательности независимых циклов (раундов), каждый из которых состоит из трех шагов определенного вида:

1. $A \to B$: γ (заявка – witness);
2. $A \leftarrow B$: x (запрос – challenge);
3. $A \to B$: y (ответ – response).

После выполнения каждого такого цикла проверяющий принимает решение об истинности доказательства.

В работе предложены два протокола доказательства с нулевым разглашением знания на эллиптических кривых.

Модификация протокола Шнорра (рис. 1). Пусть Ep(a, b) – эллиптическая кривая, известная участникам информационного процесса, G – предварительно согласованная и опубликованная точка этой кривой. Абонент А выбирает секретное число k ($1 < k < n$) и вычисляет открытый ключ Y = kG, который передает абоненту В.

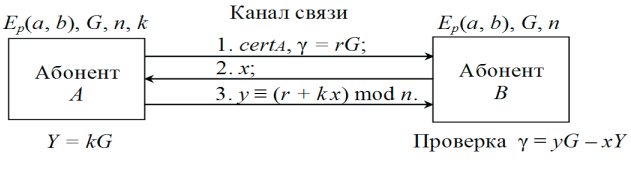


Рис. 1. Модификация протокола Шнорра

1. Абонент А выбирает случайное число r, $1 < r < n - 1$ и отправляет абоненту В число γ: $A \to B$: certa, $\gamma = rG$;

2. Абонент В отвечает случайным запросом x: $A \leftarrow B$: x;

3. Абонент А отправляет абоненту В число y: $A \to B$: $y \equiv (r + k x) \bmod n$.

Абонент В проверяет равенство $\gamma = yG - xY$.

Полнота. Доказывающий А знает значение k, поэтому он в состоянии ответить на запросы абонента В. При этом проверяющий В убеждается в справедливости соотношения

$$yG - xY = (r + kx)G - xkG = rG + k\,xG - xkG = rG = \gamma. \quad (1)$$

Пример 1. Пусть $E_{751}(-1, 188)$; G = (1, 375); n = 727, что соответствует кривой $y^2 = x^3 - x + 188$. Предположим, что пользователь А выбирает число k = 327, r = 619 и находит Y = 327(1, 375) = (354, 153).

1. $A \to B$: (354, 153), $\gamma = 619(1, 375) = (391, 564)$;
2. $A \leftarrow B$: x = 191;
3. $A \to B$: $y \equiv (619 + 191 \cdot 327) \bmod 727 \equiv 554$.

Абонент В выполняет проверку 554(1, 375) – – 191(354, 153) = (274, 422) + (62, 161) = (391, 564) = γ.

Модификация протокола Окамото (рис. 2). Пусть Ep(a, b) – эллиптическая кривая, известная участникам информационного процесса, G и Q – предварительно согласованные точки этой кривой. Абонент А выбирает секретные числа k_1 и k_2 ($1 < k_1, k_2 < n$) и вычисляет открытый ключ $Y = k_1G + k_2Q$, который передает абоненту В.

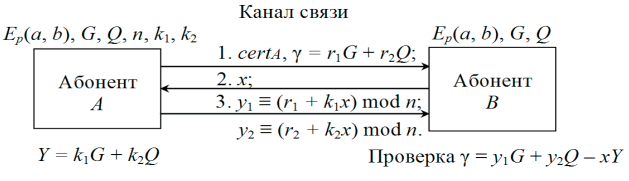


Рис. 2. Модификация протокола Окамото

1. Абонент А выбирает случайные числа r_1 и r_2, $1 < r_1, r_2 < n - 1$ и отправляет абоненту В число γ: $A \to B$: certa, $\gamma = r_1G + r_2Q$;

2. Абонент В отвечает случайным запросом x: $A \leftarrow B$: x;

3. Абонент А отправляет абоненту В значения y_1 и y_2: $A \to B$: $y_1 \equiv (r_1 + k_1x) \bmod n$, $y_2 \equiv (r_2 + k_2x) \bmod n$.

Абонент В проверяет равенство $\gamma = y_1G + y_2Q - xY$.

Полнота. В данном случае полнота протокола заключается в принятии доказательства от истинного участника и легко вытекает из равенств

$$y_1G + y_2Q - xY = (r_1 + k_1x)G + (r_2 + k_2x)Q - x(k_1G + k_2Q) = r_1G + k_1xG + r_2Q + k_2xQ - xk_1G - xk_2Q = r_1G + r_2Q = \gamma. \quad (2)$$

Пример 2. Пусть $E_{983}(-1, 188)$; G = (1, 257); Q = = (243, 1); n = 922.

Предположим, что пользователь А выбирает секретные числа $k_1 = 293$, $k_2 = 911$; случайные числа $r_1 = 193$, $r_2 = 499$ и вычисляет открытый ключ

$$Y = 293(1, 257) + 911(243, 1) = (103, 712) + (573, 116) = = (631, 928).$$

1. $A \to B$: (631, 928), $\gamma = 193(1, 257) + 499(243, 1) = =(902, 859)$;
2. $A \leftarrow B$: x = 613;
3. $A \to B$: $y_1 \equiv (193 + 293 \cdot 613) \bmod 922 \equiv 12$;
   $y_2 \equiv (499 + 911 \cdot 613) \bmod 922 \equiv 210$.

Абонент В выполняет проверку12(1, 257) + + 210(243, 1) – 613(631, 928) = (733, 666) + (492, 136) = (902, 859) = γ.

Для анализа предложенных протоколов на устойчивость к атакам противника был применен про-

граммный продукт AVISPA (Automated Validation of Internet Security Protocols and Applications) [13].

На рис. 3 и рис. 4 представлены спецификации протоколов Шнорра и Окамото на языке HLPSL (High-Level Protocol Specification Language) средствами пакета SPAN (Security Protocol Animator) [14] для AVISPA.

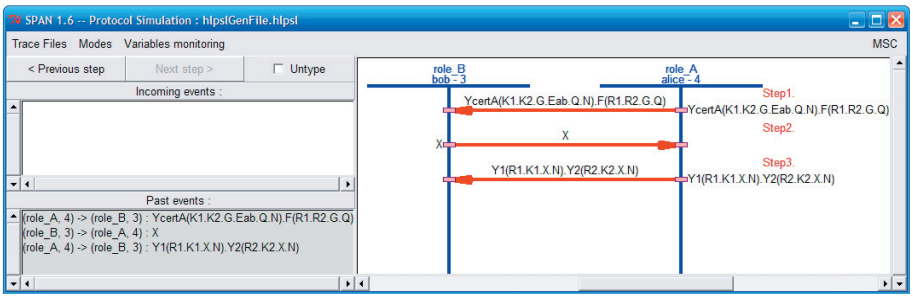
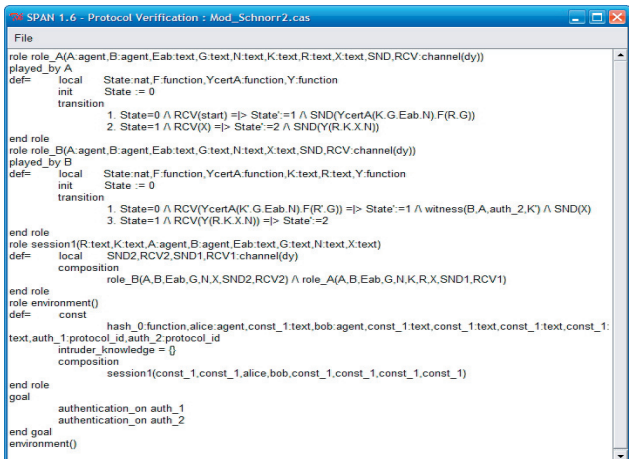
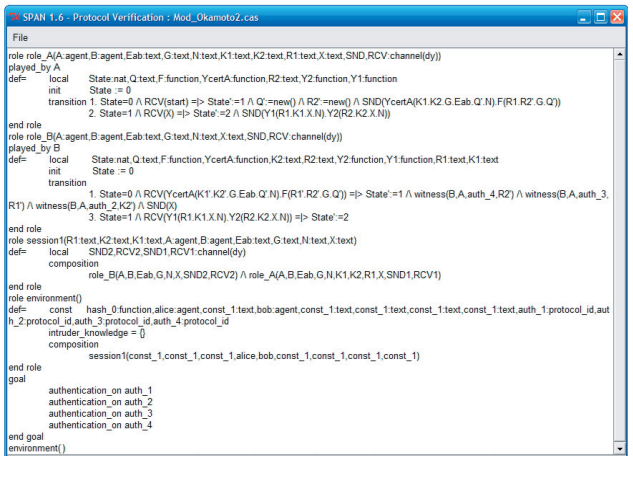


Рис. 6. Моделирование модификации протокола Окамото




```
role role_A(A:agent,B:agent,Eab:text,G:text,N:text,K:text,R:text,X:text,SND,RCV:channel(dy))
played_by A
def=        local       State:nat,F:function,YcertA:function,Y:function
            init        State := 0
            transition
                        1. State=0 /\ RCV(start) =|> State':=1 /\ SND(YcertA(K.G.Eab.N).F(R.G))
                        2. State=1 /\ RCV(X) =|> State':=2 /\ SND(Y(R.K.X.N))
end role
role role_B(A:agent,B:agent,Eab:text,G:text,N:text,X:text,SND,RCV:channel(dy))
played_by B
def=        local       State:nat,F:function,YcertA:function,K:text,R:text,Y:function
            init        State := 0
            transition
                        1. State=0 /\ RCV(YcertA(K'.G.Eab.N).F(R'.G)) =|> State':=1 /\ witness(B,A,auth_2,K') /\ SND(X)
                        3. State=1 /\ RCV(Y(R.K.X.N)) =|> State':=2
end role
role session1(R:text,K:text,A:agent,B:agent,Eab:text,G:text,N:text,X:text)
def=        local       SND2,RCV2,SND1,RCV1:channel(dy)
            composition
                        role_B(A,B,Eab,G,N,X,SND2,RCV2) /\ role_A(A,B,Eab,G,N,K,R,X,SND1,RCV1)
end role
role environment()
def=        const
                        hash_0:function,alice:agent,const_1:text,bob:agent,const_1:text,const_1:text,const_1:text,const_1:
text,auth_1:protocol_id,auth_2:protocol_id
            intruder_knowledge = {}
            composition
                        session1(const_1,const_1,alice,bob,const_1,const_1,const_1,const_1)
end role
goal
            authentication_on auth_1
            authentication_on auth_2
end goal
environment()
```

Рис. 3. Модификация протокола Шнорра на языке HLPSL




```
role role_A(A:agent,B:agent,Eab:text,G:text,N:text,K1:text,K2:text,R1:text,X:text,SND,RCV:channel(dy))
played_by A
def=        local       State:nat,Q:text,F:function,YcertA:function,R2:text,Y2:function,Y1:function
            init        State := 0
            transition 1. State=0 /\ RCV(start) =|> State':=1 /\ Q':=new() /\ R2':=new() /\ SND(YcertA(K1.K2.G.Eab.Q'.N).F(R1.R2'.G.Q'))
                        2. State=1 /\ RCV(X) =|> State':=2 /\ SND(Y(R1.K1.X.N).Y2(R2.K2.X.N))
end role
role role_B(A:agent,B:agent,Eab:text,G:text,N:text,X:text,SND,RCV:channel(dy))
played_by B
def=        local       State:nat,Q:text,F:function,YcertA:function,K2:text,R2:text,Y2:function,Y1:function,R1:text,K1:text
            init        State := 0
            transition
                        1. State=0 /\ RCV(YcertA(K1'.K2'.G.Eab.Q'.N).F(R1'.R2'.G.Q')) =|> State':=1 /\ witness(B,A,auth_4,R2') /\ witness(B,A,auth_3,
R1') /\ witness(B,A,auth_2,K2') /\ SND(X)
                        3. State=1 /\ RCV(Y(R1.K1.X.N).Y2(R2.K2.X.N)) =|> State':=2
end role
role session1(R1:text,K2:text,K1:text,A:agent,B:agent,Eab:text,G:text,N:text,X:text)
def=        local       SND2,RCV2,SND1,RCV1:channel(dy)
            composition
                        role_B(A,B,Eab,G,N,X,SND2,RCV2) /\ role_A(A,B,Eab,G,N,K1,K2,R1,X,SND1,RCV1)
end role
role environment()
def=        const   hash_0:function,alice:agent,const_1:text,bob:agent,const_1:text,const_1:text,const_1:text,const_1:text,auth_1:protocol_id,aut
h_2:protocol_id,auth_3:protocol_id,auth_4:protocol_id
            intruder_knowledge = {}
            composition
                        session1(const_1,const_1,const_1,alice,bob,const_1,const_1,const_1,const_1)
end role
goal
            authentication_on auth_1
            authentication_on auth_2
            authentication_on auth_3
            authentication_on auth_4
end goal
environment()
```

Рис. 4. Модификация протокола Окамото на языке HLPSL

Выполнена проверка моделей предложенных протоколов с помощью Protocol Simulation пакета SPAN (рис. 5, рис. 6).

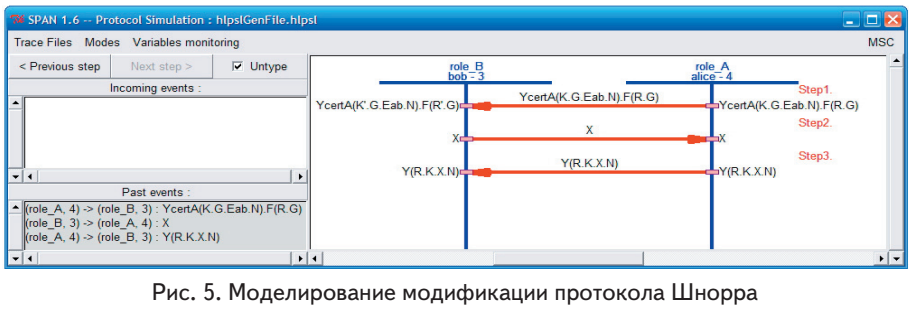


Рис. 5. Моделирование модификации протокола Шнорра

Программная верификация протоколов и устойчивость протоколов к атакам противника была выполнена с помощью программных модулей OFMC (On-the-Fly Model-Checker) и CLAtSe (CL-based Attack Searcher) AVISPA.

В результате проверки протоколов известных атак на протоколы не найдено.

5. Выводы

Криптографические протоколы, основанные на доказательстве с нулевым разглашением, позволяют произвести процедуры идентификации, обмена ключами и другие криптографические операции без утечки секретной информации в течение информационного обмена.

Для проверки протоколов на устойчивость к атакам противника были применены средства пакета SPAN для AVISPA.

В результате проверки протоколов известных атак на протоколы не найдено.

Противник может получить доступ к информации, только решив задачу ECDLP. Соответственно, при использовании криптографических протоколов на эллиптических кривых, позволяет значительно уменьшить размеры параметров протокола и увеличить криптографическую стойкость.

Литература

1. Menezes, A. Handbook of Applied Cryptography [Текст] / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М.: Триумф, 2002. – 816 с.
3. Соколов, А. В. Защита информации в распределенных корпоративных сетях и системах [Текст] / А. В. Соколов, В. Ф. Шань- гин. – М.: ДМК Пресс, 2002. – 656 с.
4. Погорелов, Б. А. Словарь криптографических терминов [Текст] / Б. А. Погорелов, В. Н. Сачков. – М.: МЦНМО, 2006. – 91 с.
5. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости [Текст] / А. В. Черемушкин. – М.: «Академия», 2009. – 272 с.

6. Запечников, С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности / С. В. Запечников. – М.: Горячая линия-Телеком, 2007. – 320 с.
7. Hankerson, D. Guide to Elliptic Curve Cryptography / D. Hankerson, A. Menezes, S. Vanstone. – Springer-Verlag, 2004. – 358 p.
8. Болотов, А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы [Текст] / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2006. – 328 с.
9. Болотов, А. А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых [Текст] / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2006. – 280 с.
10. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М.: МЦНМО, 2003. – 328 с.
11. Ростовцев, А. Г. Теоретическая криптография [Текст] / А. Г. Ростовцев, Е. Б. Маховенко. – М.: Профессионал, 2005. – 490 с.
12. An Elliptic Curve Cryptography (ECC). Primer why ECC is the next generation of public key cryptography. The Certicom 'Catch the Curve' White Paper Series, June 2004. – 24 c.
13. AVISPA. [Электронный ресурс]. – Режим доступа: http://www.avispa-project.org/.
14. Security Protocol Animator. [Электронный ресурс]. – Режим доступа: http://www.irisa.fr/celtique/genet/span/.

В статті описано алгоритм розробки програмно-апаратного комплексу визначення рівня емоційного напруження людини на основі даних шкірно-гальванічної реакції. В роботі реалізовано систему реєстрації динаміки змін шкірно-гальванічної реакції та аналізу даних з метою дослідження емоційного стану людини у відповідь на різні подразники

Ключові слова: емоційний стан, програмно-апаратний комплекс, шкірно-гальванічна реакція, NI LabVIEW, NI ELVIS

В статье описан алгоритм разработки программно-аппаратного комплекса определения уровня эмоционального напряжения человека на основе данных кожно-гальванической реакции. В работе реализована система регистрации изменений кожно-гальванической реакции и анализа данных с целью исследования эмоционального состояния человека в ответ на раздражители разного вида

Ключевые слова: эмоциональное состояние, программно-аппаратный комплекс, кожно-гальваническая реакція, NI LabVIEW, NI ELVIS

УДК 621.37

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС АНАЛІЗУ ЕМОЦІЙНОГО СТАНУ ЛЮДИНИ НА ОСНОВІ ШКІРНО-ГАЛЬВАНІЧНОЇ РЕАКЦІЇ

О. Г. Кисельова
Кандидат технічних наук, доцент*
E-mail: olga.mmif@gmail.com
Т. В. Сорока*
E-mail: Graisie@meta.ua
*Кафедра біобезпеки і відновної біоінженерії
Національний технічний університет України
«Київський політехнічний інститут»
пр. Перемоги, 37, м. Київ, Україна, 03056

1. Вступ

Перенапруга, важка робота, навчання та багато інших факторів викликають сильний стрес, який є причиною багатьох хвороб.

Дослідження зміни електричних властивостей шкіри при емоційній напрузі почалося ще у XIX столітті. Беручи за основу припущення Р. І. Тарханова [1] про те, що секреторна активність потових залоз впливає на електричний потенціал шкіри, на сьогоднішній день досліджується залежність динаміки шкірно-гальванічної реакції (ШГР) від таких факторів, як вагітність, розвиток ракової пухлини та ін.

Визначення шкірно-гальванічної реакції можливе двома способами:

• використовуючи зовнішній струм (метод Фере). В такому разі вимірюється опір шкіри [1];

• без використання зовнішнього струму (метод Тарханова). В такому разі вимірюються безпосередньо електричні потенціали шкіри [1].

Шкірно-гальванічна реакція може реєструватися з будь-якої ділянки тіла, але зазвичай використовуються пальці або кисті рук чи стопи [2].

Провідність шкіри залежить від кількості поту на ділянці, де прикріплені електроди. Деякі досліди використовують дану закономірність для діагностики

© О. Г. Кисельова, Т. В. Сорока, 2013