УДК 519.179+519.87

Преобразования Murata в модели криптографического протокола Эль-Гамаля[1]

Е. А. Лукьянова, А. В. Дереза, А. И. Потапова
Крымский федеральный университет им. В. И. Вернадского,
e-mail: lukyanovaea@mail.ru, alena-dereza@mail.ru, alenaalena007@yandex.ru

Аннотация. В статье на модели Петри криптографического протокола Эль-Гамаля реализуются редуцирующие возможности компонентного моделирования и правил сокращения Murata.

Ключевые слова: сеть Петри, криптографический протокол Эль-Гамаля, редуцирование сети, правила сокращения Murata.

Murata Transformations in the model of the cryptographic protocol of El-Gamal

E. A. Lukyanova, A. V. Dereza, A. I. Potapova
V. I. Vernadsky Crimean Federal University.

Abstract. In the article, the reducing capabilities of component modeling and Murata reduction rules are realized on Petry's model of the El-Gamal cryptographic protocol.

Keywords: El-Gamal cryptographic protocol, network reduction, component modeling, Murata reduction rules.

MSC 2010: 34A34, 37C27, 37C80, 70F10

Введение

К основным графическим и математическим инструментам моделирования систем можно отнести моделирующий аппарат сетей Петри.

Сети Петри (СП) хорошо визуализируют связи моделируемой системы аналогично блок-схемам и сетям, при этом отражают динамику её функционирования и параллелизм. Инструмент сетей Петри успешно применяется для моделирования и анализа систем различной сложности, и позволяет получать математически строгое описание модели и проводить с помощью современной вычислительной техники её анализ. Активное применение сетей Петри, как в практических, так и теоретических исследованиях даёт возможность практикам получить от теоретиков информацию о том, как создать более реалистичные модели. При построении моделей Петри систем и объектов больших размеров приходиться решать проблему экспоненциального роста состояний модели.

В связи с этим применяются различные методы редукции, позволяющие осуществлять переход от исходной модели к адекватной ей, но имеющей размеры, позволяющие проводить анализ модели.

Цель настоящей работы: построить модель Петри для криптографического протокола Эль-Гамаля, реализовать редукции компонентного моделирования

[1]Настоящая работа выполнена при поддержке Программы развития ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского» на 2015-2024 годы в рамках реализации академической мобильности по проекту ФГАОУ ВО «КФУ им. В. И. Вернадского» «Поддержка академической мобильности работников университета на заявительной основе – ПМР» в ФГБОУ ВО «Липецкий государственный технический университет».

и правил сокращения Murata на модели криптографического протокола Эль-Гамаля.

1. Постановка задачи

Криптографический протокол Эль-Гамаля представляет собой алгоритмическую схему, которая позволяет при незащищенном от прослушивания канале связи, получать двум пользователям общий секретный ключ , предназначенный для обмена конфиденциальной информацией.

При этом сначала, первый из пользователей создает свой секретный ключ x и на его основе вычисляет открытый ключ $y = g^x \mod p$, где p и g – простые числа, известные обоим пользователям. Затем, второй пользователь создает свой секретный ключ k и помощью него вычисляет следующую пару чисел: $a = g^k \mod p$ и $b = My^k \mod p$, где y – полученный открытый ключ, M – общий секретный ключ, который должен получить в конечном итоге первый пользователь. После передачи вторым пользователем пары чисел (a, b), первым пользователем высчитывается итоговый ключ $M = ba^{p-1-x} \mod p$.

Построение модели данной алгоритмической схемы в виде сети Петри в работе осуществляется на основе компонентного моделирования [1], позволяющего ещё на этапе проектирования выделять группы одинаковых процессов и оформлять их в виде составных компонент модели. Для данной модели это будут компоненты-переходы [2]. Если же рассматривать модель алгоритмической схемы в виде полной сети Петри, где компоненты-переходы (участки полной сети Петри) изображаются своими представлениями в виде соответствующих сетей Петри, то эти участки правилами сокращения Murata [3] будут в итоге редуцированы в переходы, которые в предыдущей компонентной модели являются компонентами-переходами. В настоящей работе компонентное моделирование применяется для удобства построения модели Петри и компактности её представления.

2. Моделирование алгоритмической схемы

Модель схемы представляет собой тройку (S, W, M_0), где $S(P, T, F)$ – сеть, $W : F \to N$ – функция кратности дуг, (F – отношение инцидентности или зависимость между местами P и переходами T), M_0 – начальная разметка сети. Функция $M : P \to N$ – разметка сети S, которая описывает количество фишек $M(p)$, которые размещаются этой разметкой в каждое место $p \in P$. Пусть $I : (P \times T) \cup (T \times P \to N)$ – отношение инцидентности:

$$I(x, y) = \begin{cases} n, & \text{если } (x, y) \in F \wedge W(x, y) = n; \\ 0, & \text{если } (x, y) \notin F. \end{cases}$$

Если $P = p_1, \ldots, p_n$, то разметку M сети можно задать как вектор чисел $M = (m_1, \ldots, m_n)$ такой, что $m_i = M(p_i)$ для произвольного $i = 1, \ldots, n$.

Представим работу схемы Эль-Гамаля в виде некоторой последовательной программы, результат работы которой получение каждым из пользователей общего секретного ключа для дальнейшего обмена и шифрования информации:

begin
$input(p); input(g); input(x); input(k);$
$input(y); input(a); input(b); input(M);$
$y := g^x \mod p;$
$a := g^k \mod p;$
$b := My^k \mod p;$
$M := ba^{p-1-x} \mod p;$
$output(M);$
end.

Интерпретация данной программы для последующего построения модели Петри имеет вид:

$$input(x); input(y); input(M); input(p); input(g); \quad (t_1)$$
$$input(k); input(a); input(b); input(M); input(p); input(g); \quad (t_2)$$
$$y := g^x \mod p; \quad (t_3)$$
$$a := g^k \mod p; \quad (t_4)$$
$$b := My^k \mod p; \quad (t_5)$$
$$M := ba^{p-1-x} \mod p. \quad (t_6)$$

Соответствующая модель Петри показана на рис. 1. Эта сеть Петри представляется компонентной сетью Петри, в которой переходы t_3, t_4 и t_5, t_6 являются компонентами-переходами и моделируют процесс вычисления $g^x \mod p$.

Рассмотрим процесс вычисления $g^x \mod p$, как отдельную последовательную программу:
begin
$input(x); input(p);$
$input(g); input(s);$
$while(x > 0)do$
begin
$g := g * g;$
$x := x - 1;$
end;
$output(g);$
$while(g > p)do$
begin
$g := g - p;$
end;
$s := p - g;$
$output(s);$
end.

Интерпретация данной программы для последующего построения компоненты-

перехода имеет вид:

$$
\begin{aligned}
&\mathit{begin}\\
&\mathit{input}(p); \mathit{input}(x); \mathit{input}(g); \mathit{input}(s); && (t_1)\\
&x > 0? && (t_2)\\
&g := g * g; x := x - 1; && (t_3)\\
&\mathit{output}(g); && (t_4)\\
&g - p > 0? && (t_5)\\
&g := g - p; && (t_6)\\
&s := p - g; && (t_7)\\
&\mathit{output}(s). && (t_8)
\end{aligned}
$$

Сеть Петри, отвечающая данной последовательной программе показана на рис. 2.

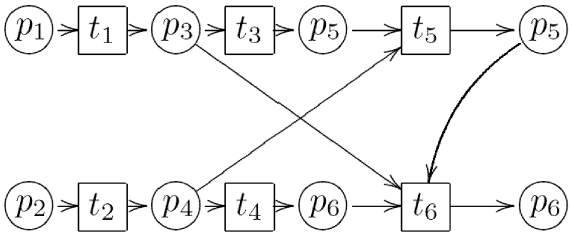

Рис. 1. Сеть Петри криптографического протокола Эль-Гамаля

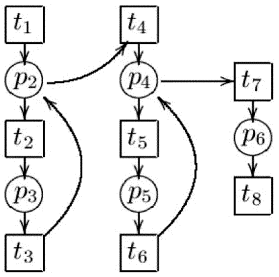

Рис. 2. Сеть Петри (компонента-переход), моделирующая процесс $g^x \mod p$

3. Правила сокращения Murata

В работе [3] предложены следующие шесть операций (правил сокращения Murata), редуцирующих сеть Петри. Это – преобразования, заключающиеся в слиянии мест, слиянии переходов, слиянии параллельных мест, слиянии параллельных переходов, в устранении петли мест, петли переходов. Указанные правила сокращения Murata показаны на рис. 3 – рис. 8.

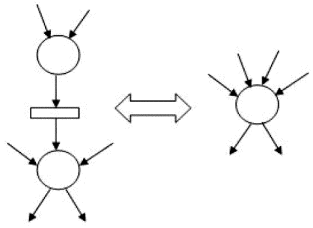

Рис. 3. Слияние серии мест СП

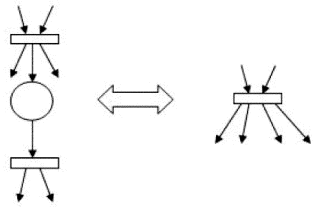

Рис. 4. Слияние серии переходов СП

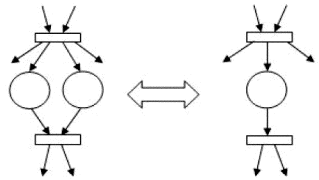

Рис. 5. Слияние параллельных мест СП

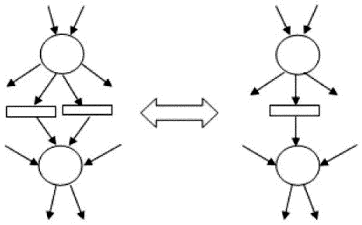

Рис. 6. Слияние параллельных переходов СП

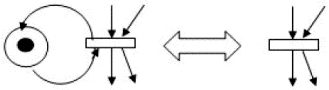

Рис. 7. Устранение петли мест СП

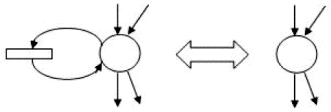

Рис. 8. Устранение петли переходов СП

Применим данные преобразования к сети Петри, показанной на рис. 2. После операции слияния серии мест будет получена сеть Петри, показанная на рис. 9. После операции устранения петли переходов будет получена сеть Петри, показанная на рис. 10. После операции слияния серии переходов сеть Петри, показанная на рис. 2, уже будет представлять один переход, являющийся компонентой-переходом (t_3, t_4 и t_5, t_6), в компонентной сети, показанной на рис. 1.

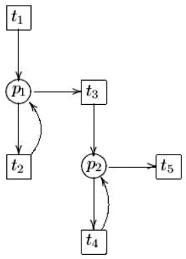

Рис. 9. СП после слияния серии мест

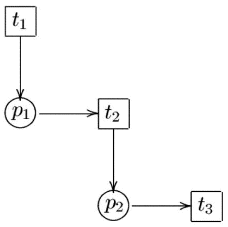

Рис. 10. СП после устранения петли переходов

Отметим, что полная СП или модель Петри криптографического протокола Эль-Гамаля в работе явно не показана в силу её громоздкости, но она представляет собой сеть Петри с рис. 1, в которой переходы t_3, t_4 и t_5, t_6, есть сети Петри с рис. 2. И так, имея изначально полную СП, моделирующую криптографический протокол Эль-Гамаля, и применяя к ней правила сокращения Murata, получим уменьшенную СП, показанную на рис. 1. Эта модель Петри является адекватной полной СП, т. к. согласно [3] правила сокращения Murata сохраняют важное и сильное свойство сетей Петри – живость, наличие которого в сети Петри определяет возможность срабатывания любого перехода при функционировании модели-

руемого объекта, отсутствие живости означает либо избыточность в моделируемой системе, либо возможность возникновения зацикливаний, тупиков, блокировок.

Заключение

Использование компонентного моделирования для построения модели рассматриваемого криптографического протокола позволило построить компактную модель по частям, сохраняющую отношения между частями построенной модели, а правила сокращения Murata подтверждают надёжность выводов о свойствах полной модели криптографического протокола Эль-Гамаля по его компонентной модели.

Список цитируемых источников

1. *Lukyanova E. A.* Component modeling: on connections of detailed Petri model and component model of parallel distributed system // ITHEA. – 2013. – Vol. 2, № 1. P. 15-22.
2. *Лукьянова Е. А.* О структурных элементах компонентной сети Петри // Проблеми програмування. – 2012. – № 2-3. – С. 25-32.
3. *Murata* T. Petri Nets: Properties, Analysis and Applications // Proceedings of the IEEE. – 1989. – Vol. 77. – № 4. – P. 541-580.