

Об угрозе UKS и влиянии на ее реализуемость

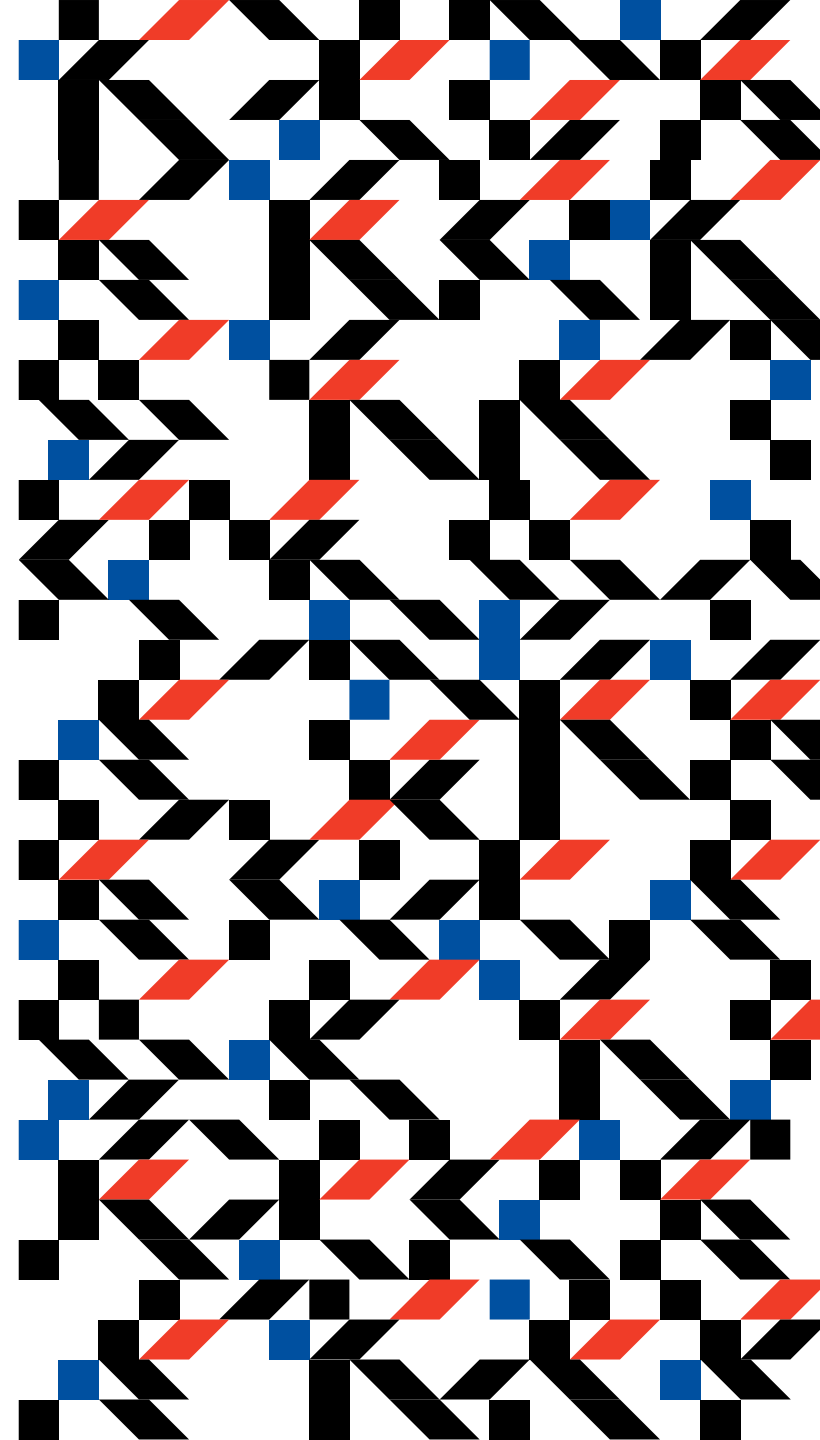
**возможности получения и навязывания
будущих эфемерных ключей
честных сторон**

Алексеев Евгений Константинович

Кяжин Сергей Николаевич

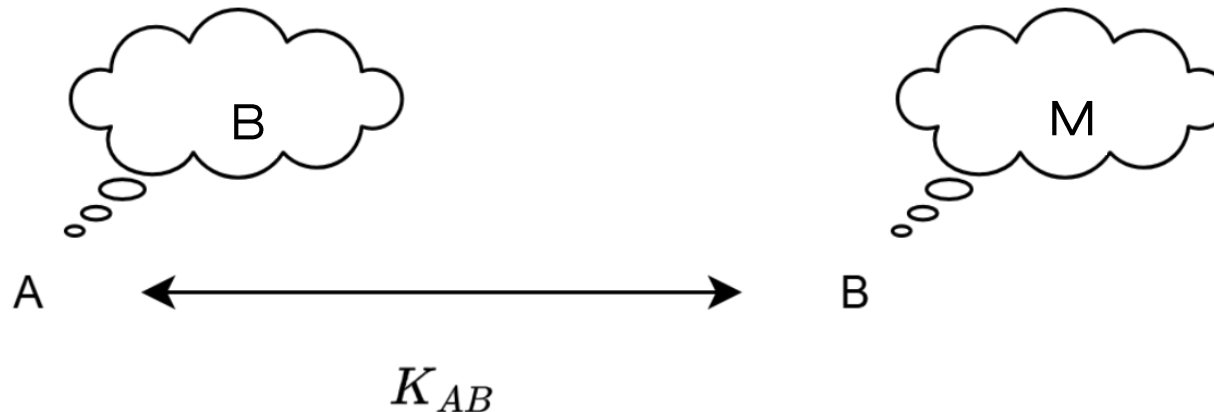
Мухортова Алена Андреевна

Смышляев Станислав Витальевич



Угроза UKS

- Угроза **Unknown Key Share (UKS)** – две честные стороны А и В успешно выработали общий сеансовый ключ K , который не известен нарушителю М, причем А думает, что выработал его с В, но В думает, что выработал его с М.
- Впервые рассмотрена в 1992 году: работа Diffie W., Van Oorschot P. C., Wiener M. J. «Authentication and authenticated key exchanges», 1992.
- Актуальность:
 - ✓ А – отличник, сдающий экзамен проверяющему В, а М – двоечник. Ущерб: если М реализовал UKS, то результаты А будут зачтены М.
 - ✓ А – честный клиент банка В, а М – злонамеренный клиент банка В. Ущерб: если М реализовал UKS, то деньги, внесенные А, поступят на счет М.



Причины и цели исследования?

- «Probing the security landscape for authenticated key establishment protocols» (CTCrypt 2023):
 - ✓ «ландшафт защищенности»
 - ✓ подход к систематизированному выявлению угроз и возможностей нарушителя
- «Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей» (CTCrypt 2024):
 - ✓ рассмотрена новая возможность нарушителя
 - ✓ предложен ряд атак и методов противодействия
- Угрозы, которые реализуются в результате атак из работы 2024 года:
 - ✓ ложная аутентификация
 - ✓ нарушение секретности сеансового ключа
 - ✓ KCI

Нет ни одной атаки, в результате которой реализуется угроза UKS!

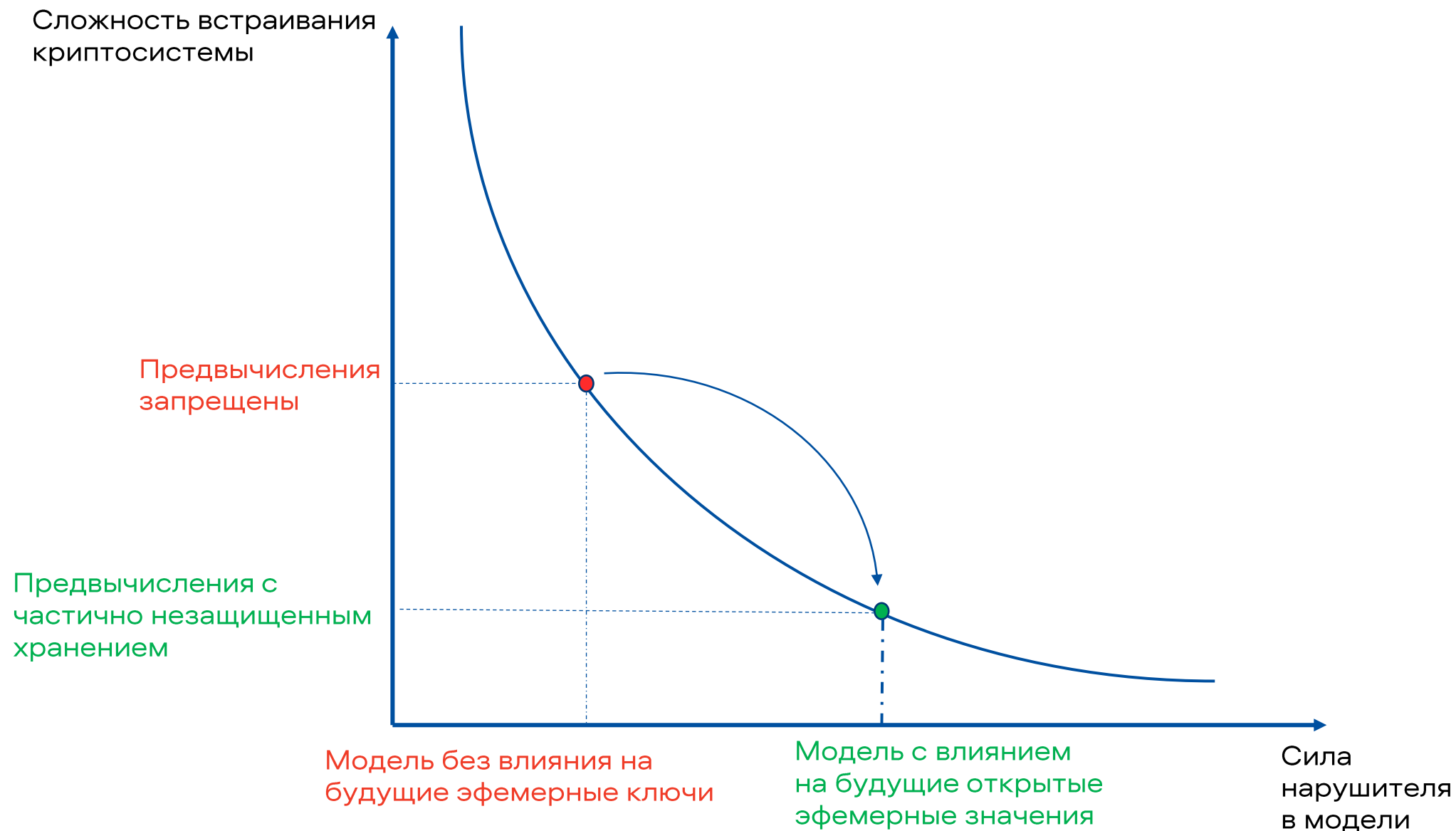
- Цель настоящего исследования: **оценить влияние возможности навязывания будущих открытых эфемерных ключей на реализуемость угрозы UKS**



Возможность навязывания будущих открытых эфемерных ключей

- Впервые рассмотрена: CTCrypt 2024 («Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей», ПДМ, №66, 2024)
- Усиление идеи компрометации будущих открытых эфемерных ключей, предложенной в работе Seye P. B. and Sarr A. P. «Enhanced modelling of authenticated key exchange security», 2017.
- Мотивация: возможность предвычислений с частично незащищенным хранением (актуально для низкоресурсных устройств (IoT) и постквантовой криптографии)

Возможность навязывания будущих открытых эфемерных ключей

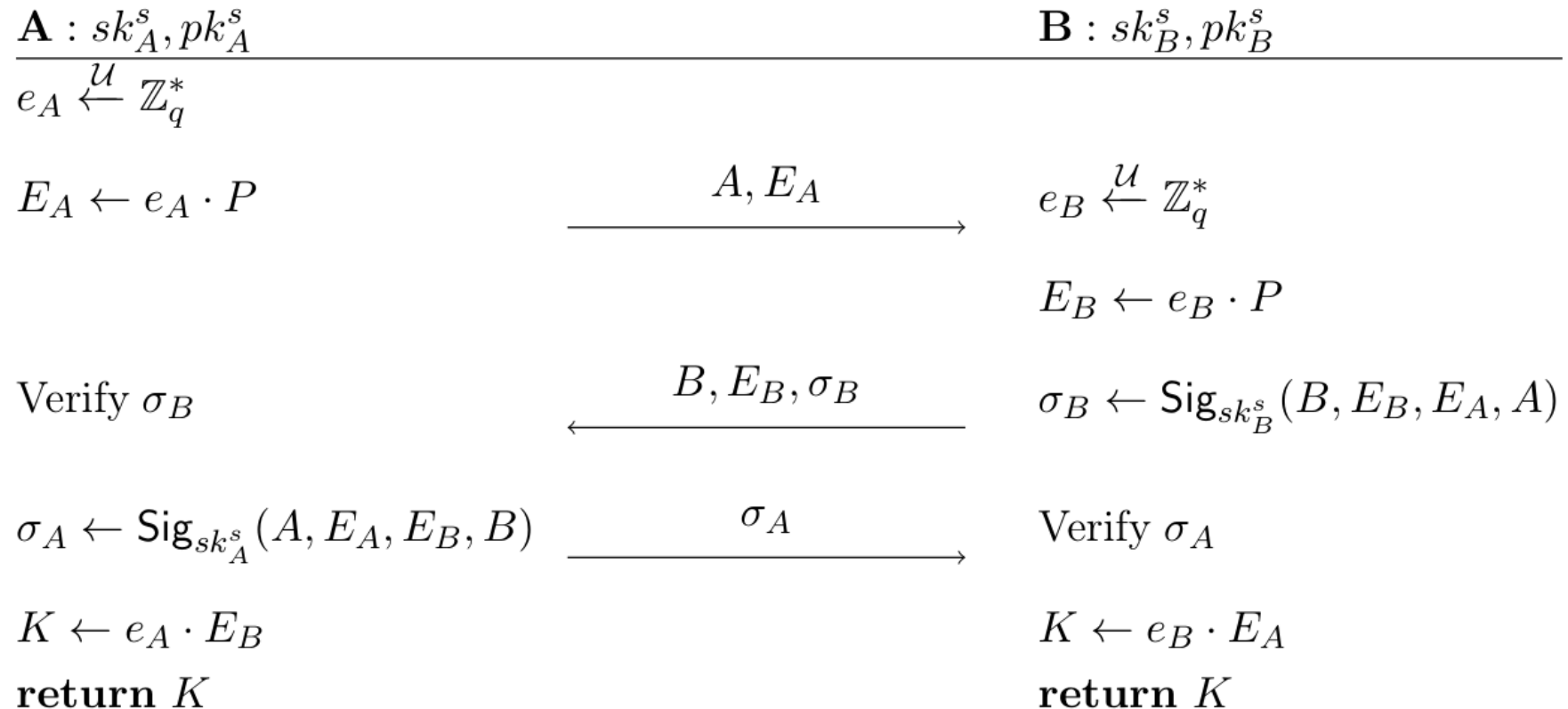


Полученные результаты

- Предложен новый подход к построению UKS-атак
- Выявлена связь между классической угрозой ложной аутентификации и UKS
- Построена новая атака, приводящая к реализации угрозы ложной аутентификации, на протокол SIGMA
- Выделено 27 типов угроз UKS (углублена существующая классификация)
- Построены новые UKS-атаки на некоторые протоколы, в частности, HMQV

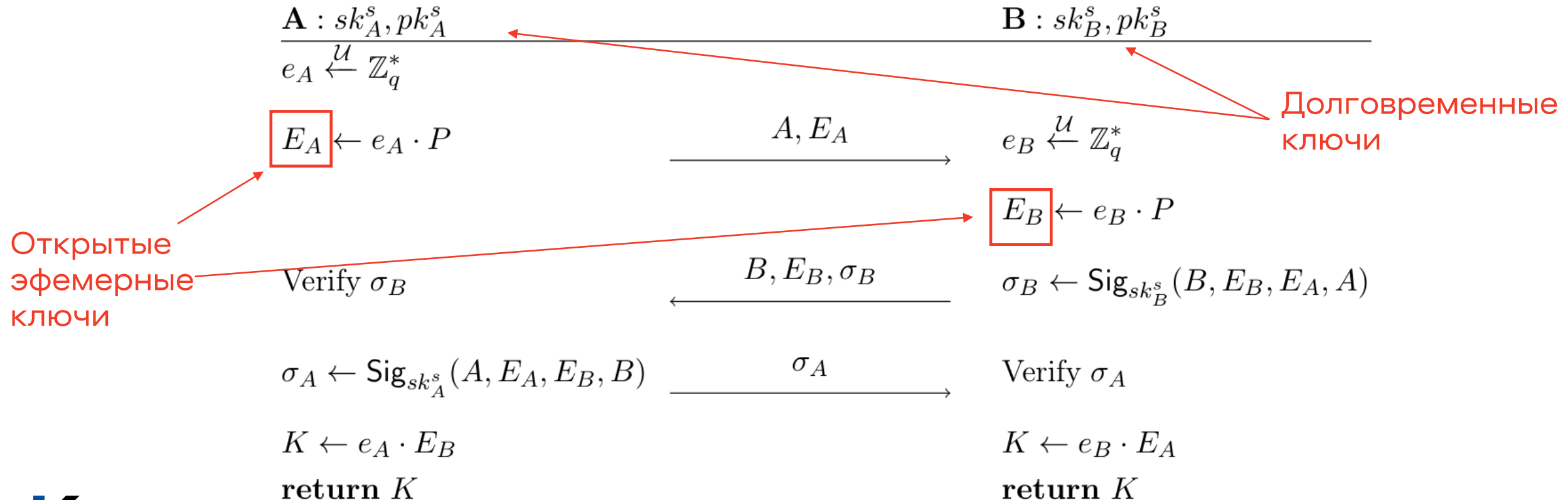
UKS-атака на протокол SIG-DH

- Протокол SIG-DH (Canetti R., Krawczyk H. «Analysis of key-exchange protocols and their use for building secure channels», 2001)
- Обозначения в соответствии с «AKE Zoo: 100 two-party protocols (to be continued)», 2023.



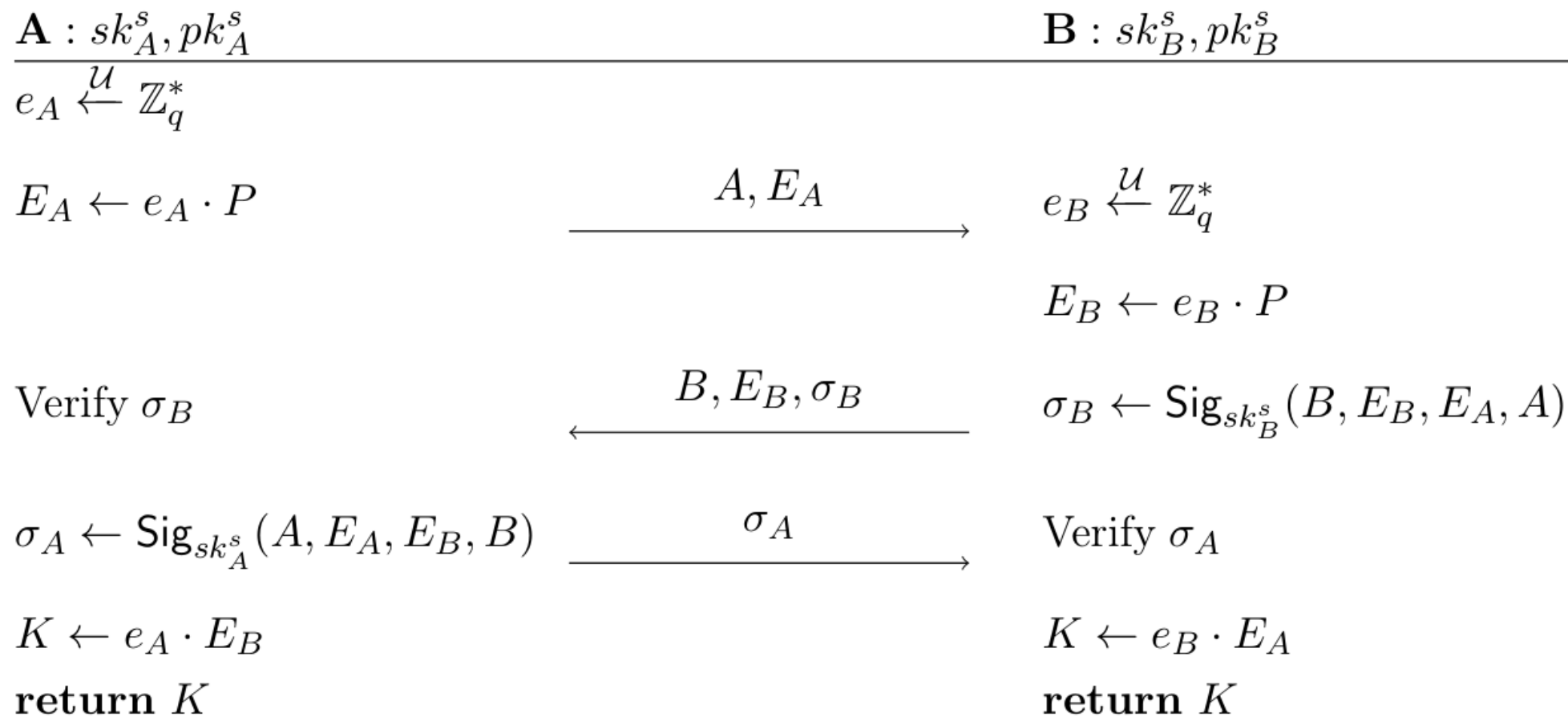
UKS-атака на протокол SIG-DH

- Протокол SIG-DH (Canetti R., Krawczyk H. «Analysis of key-exchange protocols and their use for building secure channels», 2001)
- Обозначения в соответствии с «AKE Zoo: 100 two-party protocols (to be continued)», 2023.



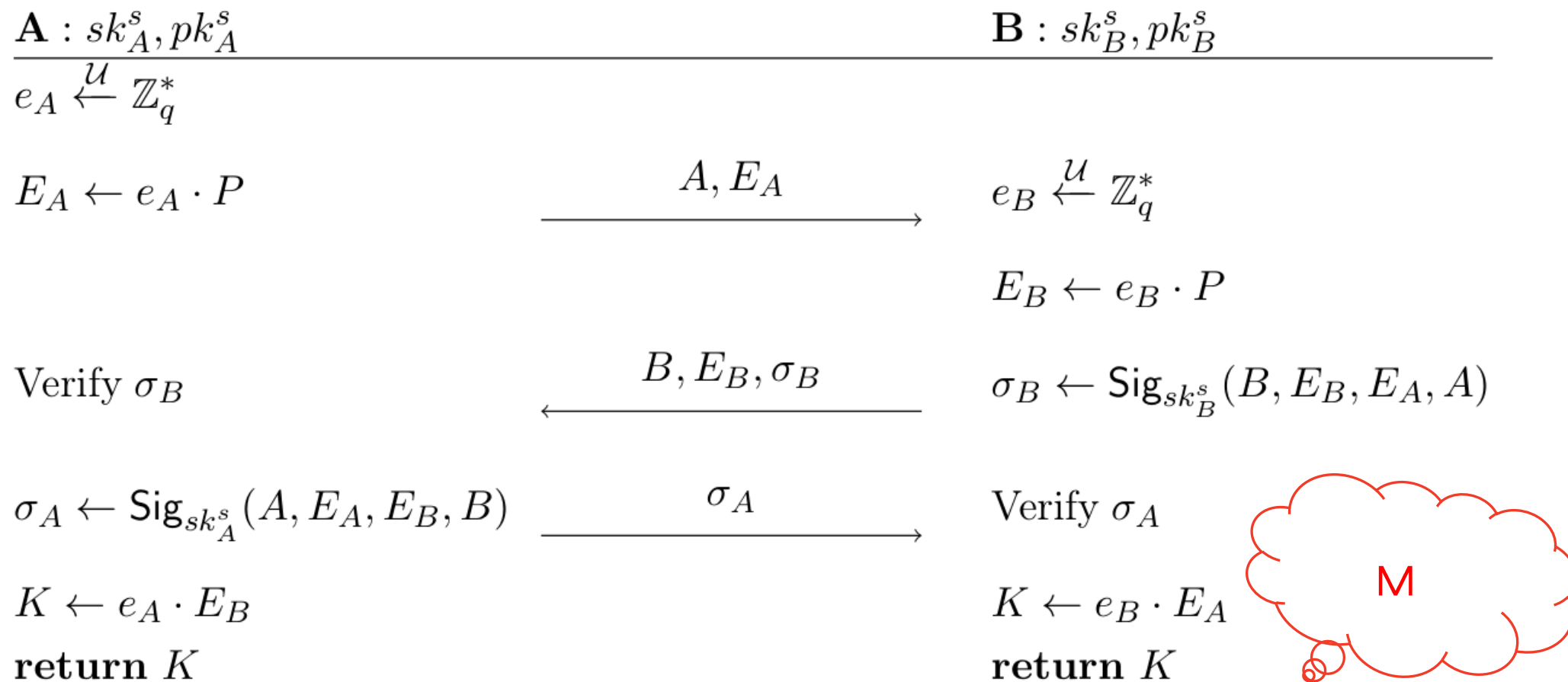
UKS-атака на протокол SIG-DH

- Почему не получается реализовать UKS без дополнительных возможностей



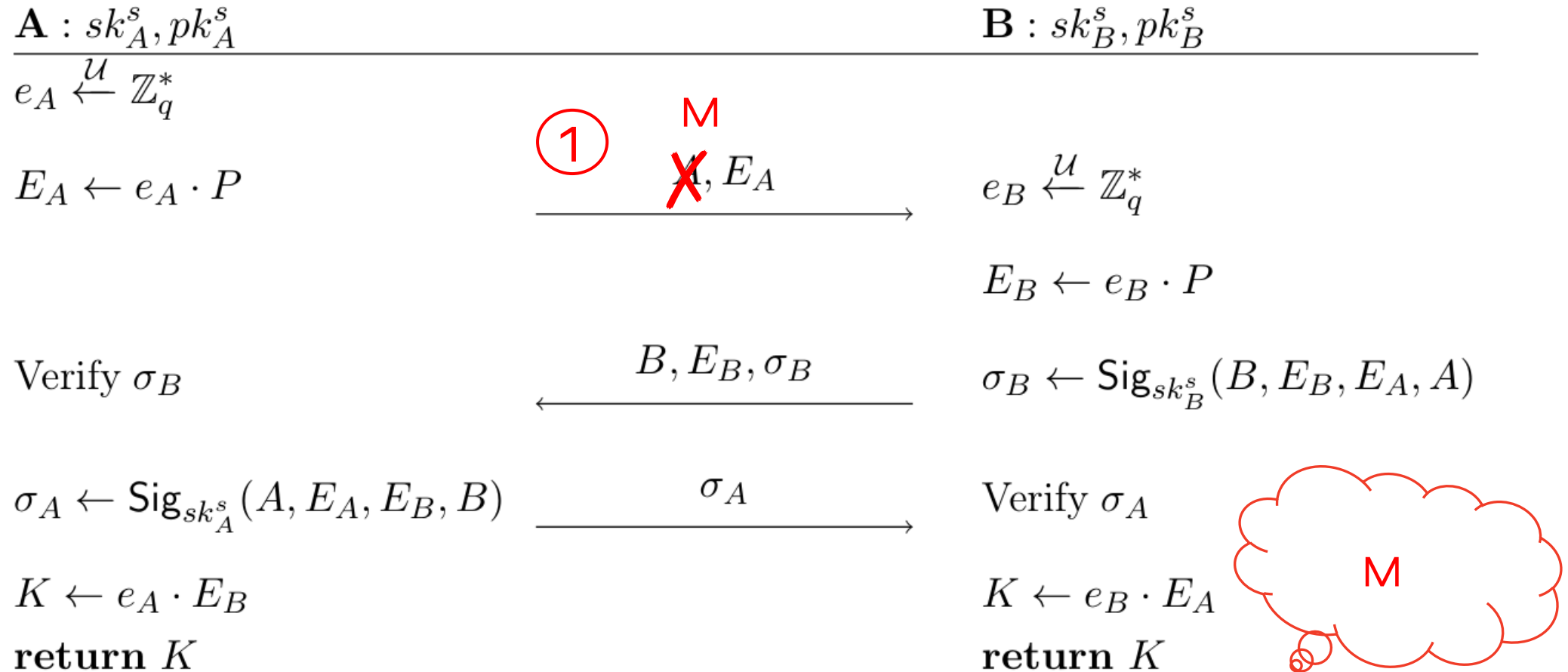
UKS-атака на протокол SIG-DH

- Почему не получается реализовать UKS без дополнительных возможностей



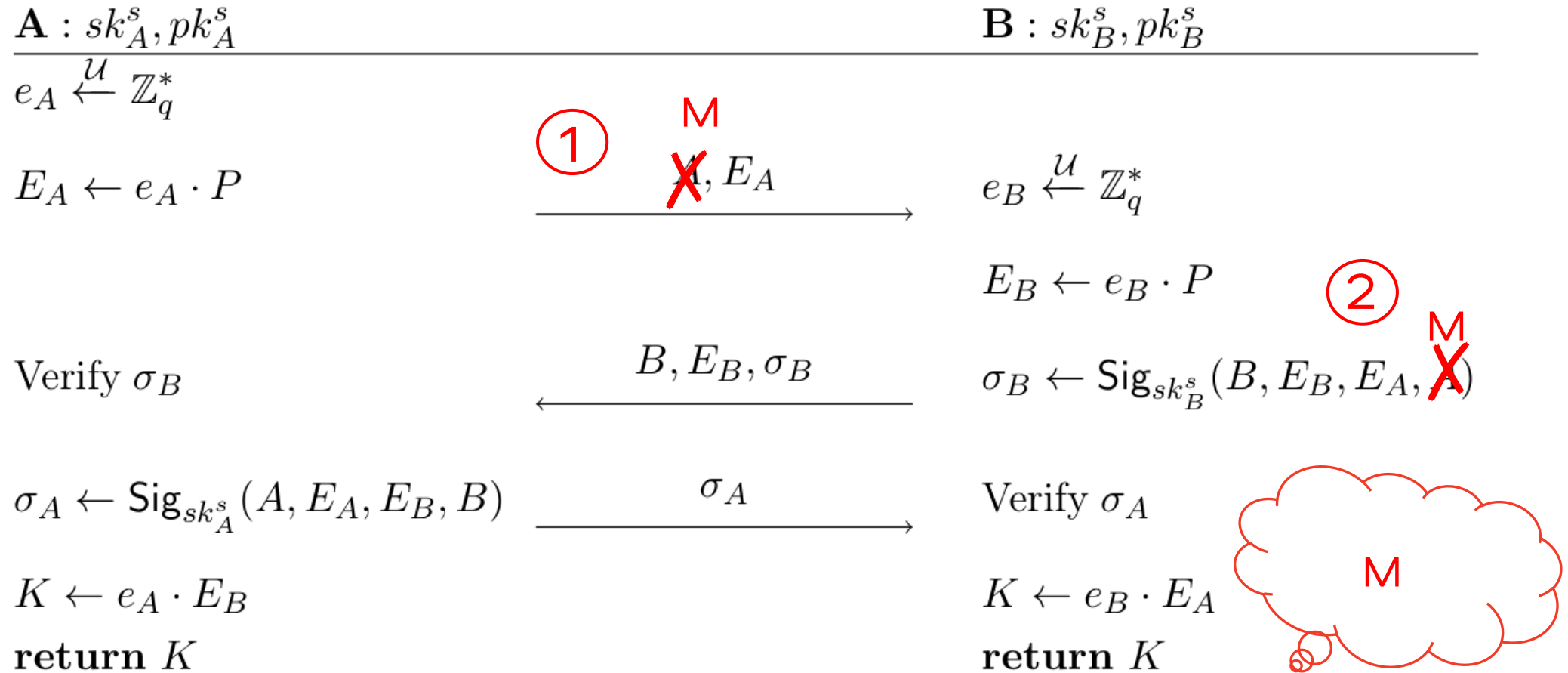
UKS-атака на протокол SIG-DH

- Почему не получается реализовать UKS без дополнительных возможностей



UKS-атака на протокол SIG-DH

- Почему не получается реализовать UKS без дополнительных возможностей



UKS-атака на протокол SIG-DH

- Почему не получается реализовать UKS без дополнительных возможностей

A : sk_A^s, pk_A^s

$e_A \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$E_A \leftarrow e_A \cdot P$

Проверка завершится неудачей, т.к.
сторона A будет проверять подпись под
строкой со своим идентификатором

Verify σ_B

$\sigma_A \leftarrow \text{Sig}_{sk_A^s}(A, E_A, E_B, B)$

$K \leftarrow e_A \cdot E_B$

return K

B : sk_B^s, pk_B^s

$e_B \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$E_B \leftarrow e_B \cdot P$

$\sigma_B \leftarrow \text{Sig}_{sk_B^s}(B, E_B, E_A, \text{M})$

Verify σ_A

$K \leftarrow e_B \cdot E_A$

return K

1

M

~~A~~, E_A

2

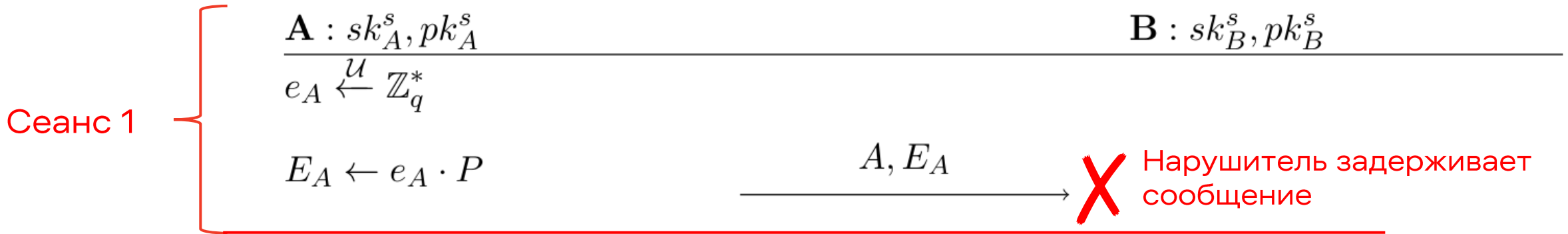
M

~~A~~

M

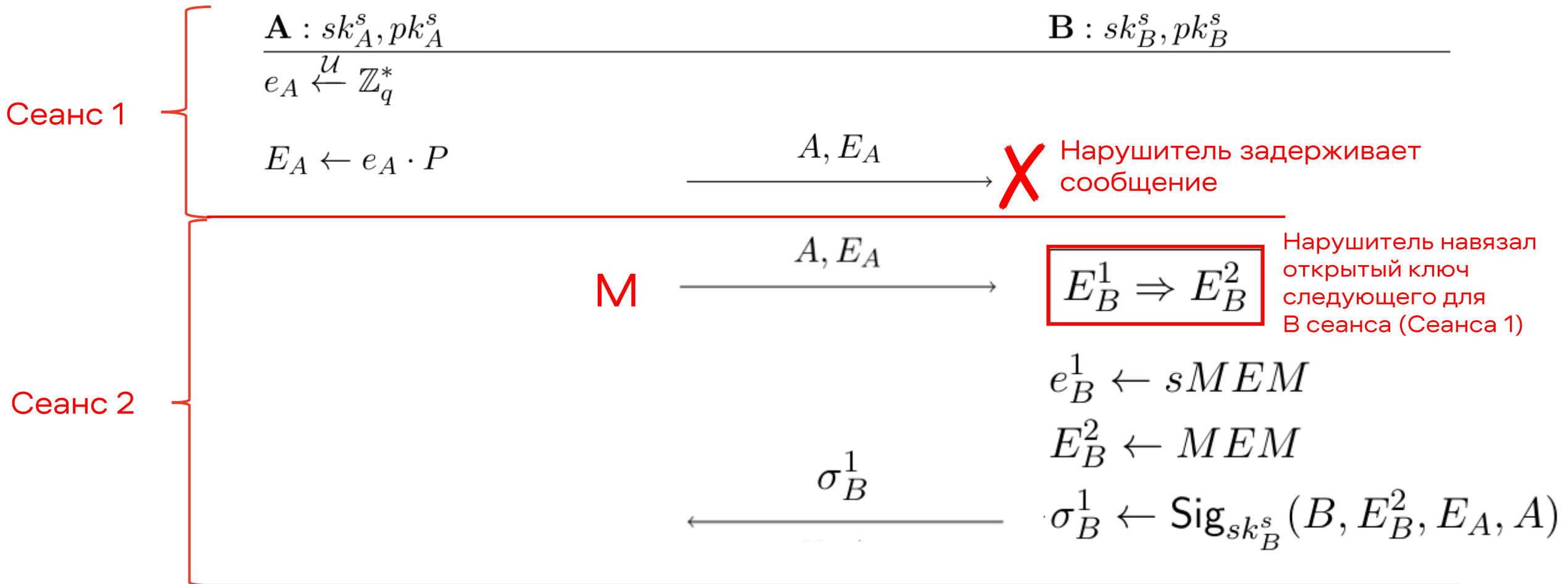
UKS-атака на протокол SIG-DH

- Идея атаки: узнав открытые эфемерные ключи стороны В, заготовленные для **двух** следующих сеансов, заменить первый на второй, чтобы получить подпись, которая пройдет Verify на стороне А.



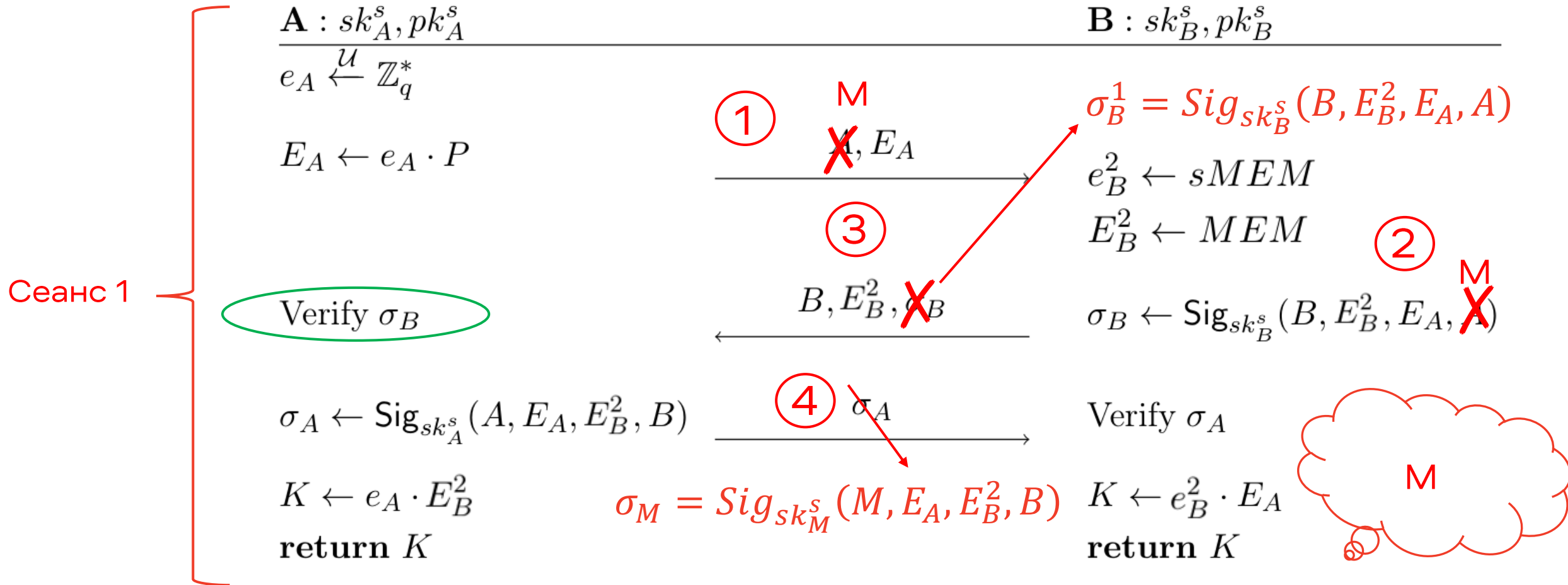
UKS-атака на протокол SIG-DH

- Идея атаки: узнав открытые эфемерные ключи стороны В, заготовленные для **двух** следующих сеансов, заменить первый на второй, чтобы получить подпись, которая пройдет Verify на стороне А.



UKS-атака на протокол SIG-DH

- Идея атаки: узнав открытые эфемерные ключи стороны В, заготовленные для **двух** следующих сеансов, заменить первый на второй, чтобы получить подпись, которая пройдет Verify на стороне А.

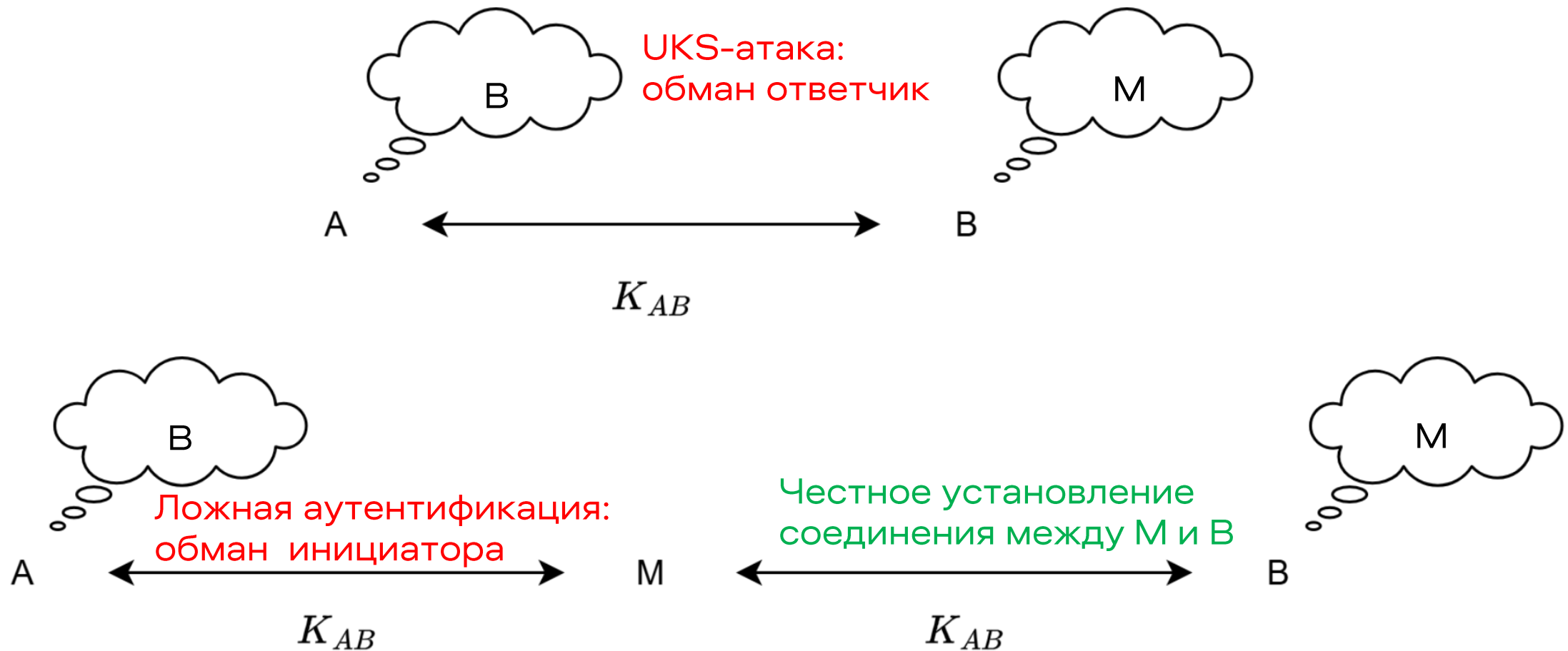


UKS-атака на протокол SIG-DH

- **Идея атаки:** узнав открытые эфемерные ключи стороны В, заготовленные для **двух** следующих сеансов, заменить первый на второй, чтобы получить в первом сеансе подпись, которая пройдет Verify на стороне А во втором сеансе.
- Описанная идея также применима для построения UKS-атак на следующие протоколы:
 - ✓ SIG-DH+
 - ✓ *mSTS-MAC-6*
 - ✓ *ISO93-KE*
 - ✓ *TS3*
 - ✓ *TS3-1*
 - ✓ *DHKE*

Связь между угрозой ложной аутентификации и UKS

- Угроза ложной аутентификации на инициатора/ответчика «эквивалентна по ущербу» угрозе UKS для случая, когда неверное представление о партнере создается у ответчика/инициатора



Атака ложной аутентификации на ответчика для протокола SIGMA

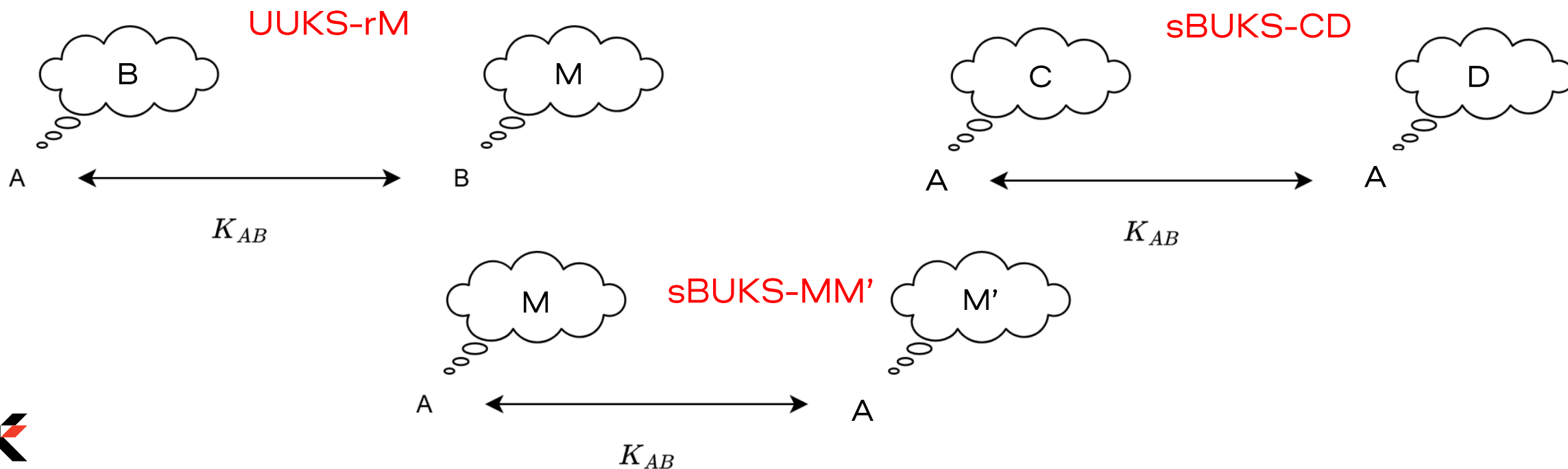
- Протокол SIGMA предложен в 2003 году Хьюго Кравчиком в классической работе «SIGMA: The ‘SIGn-and-MAC’ Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols».
- Главный АКЕ-протокол современного Интернета:
 - ✓ Основа TLS 1.3
 - ✓ Основа IKEv2
- Неизвестно атак в стандартных моделях
- **Атака ложной аутентификации на инициатора** при возможности навязывания будущих открытых эфемерных ключей представлена на **CTCrypt 2024** в докладе «Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей»
- **Результат, полученный в настоящей работе:** построена **атака ложной аутентификации на ответчика** в предположении, что честные участники используют одну и ту же долговременную ключевую пару для взаимодействия по протоколу в разных ролях (инициатор/ответчик).

Расширенная классификация угроз UKS

- В изначальной работе 1992 года рассматривалось только 2 типа угроз UKS: два честных участника вырабатывают общий ключ, а о партнере заблуждается либо только инициатор, либо только ответчик
- В 2007 году в работе Chen L., Tang Q. «Bilateral Unknown Key-Share Attacks in Key Agreement Protocols» предложено расширение угрозы UKS на случай, когда относительно своего партнера заблуждаются обе стороны:
 - ✓ Когда заблуждается одна сторона – Unilateral Unknown Key Share (UUKS)
 - ✓ Когда заблуждаются обе стороны – Bilateral Unknown Key Share (BUKS)
- **В настоящей работе** предложена классификация, дополнительно основанная на следующих факторах:
 - ✓ одинаковы ли идентификаторы участников, которые выработали друг с другом общий ключ
 - ✓ кого обманутая сторона предполагает в качестве своего партнера

Расширенная классификация угроз UKS

- Принцип наименования:
 - ✓ UUKS/BUKS – обманута **одна/две** честные стороны
 - ✓ есть/нет префикс 's' – ключ выработали стороны с **одинаковыми/разными** идентификаторами
 - ✓ XY – навязанные идентификаторы партнеров для BUKS
 - ✓ xY – роль (x) обманутой стороны и идентификатор (Y) предполагаемого ей партнера
 - ✓ Идентификаторы:
 - A, B, C, D – честные стороны
 - M, M' – нарушители



Расширенная классификация угроз UKS

- 4 подтипа: UUKS-XY, sUUKS-XY, BUKS-XY, sBUKS-XY
- Перебирая возможные X,Y,x: 27 конкретных вариантов угроз
- Примеры:
 - ✓ Selfie-атака на TLS 1.3 – **sBUKS-CC** (ключ выработал A с A, но инициатор думает, что выработал его с другим честным C)
 - ✓ Атака на SIG-DH из этой работы – **UUKS-rM** (ключ выработали A и B, но B думает, что выработал его с нарушителем M)
 - ✓ Атака Seye-Sarr на HMQV – **BUKS-MM'** (ключ выработали A и B, но A думает, что выработал его с M, а B думает, что выработал его с M')

Новые UKS-атаки в стандартных моделях нарушителя

- Предложена новая атака, реализующая угрозу **BUKS-MM'** на протокол HMQV:
 - ✓ Атака, реализующая такую же угрозу ранее уже была известна (Seye P. B., Sarr A. P. «Enhanced Modelling of Authenticated Key Exchange Security»), но в настоящей работе атака построена в несравнимой по возможностям модели нарушителя;
 - ✓ В атаке Seye-Sarr требовалась компрометация будущих открытых эфемерных ключей обеих сторон;
 - ✓ В предложенной атаке компрометации открытых эфемерных ключей НЕ требуется, но требуется возможность динамической регистрации в сети без доказательства знания закрытых ключей;
 - ✓ Отдельное спасибо А.М. Гуселеву за подсказку, позволившую избавиться от необходимости использования одной лишней возможности при построении этой атаки.
- Предложена новая атака, реализующая угрозу **BUKS-MM** на протокол BKM-KK, описанный в работе Boyd C., Kock B. Millerjord L. «Modular Design of KEM-Based Authenticated Key Exchange», 2023.

Спасибо за внимание! Вопросы?

