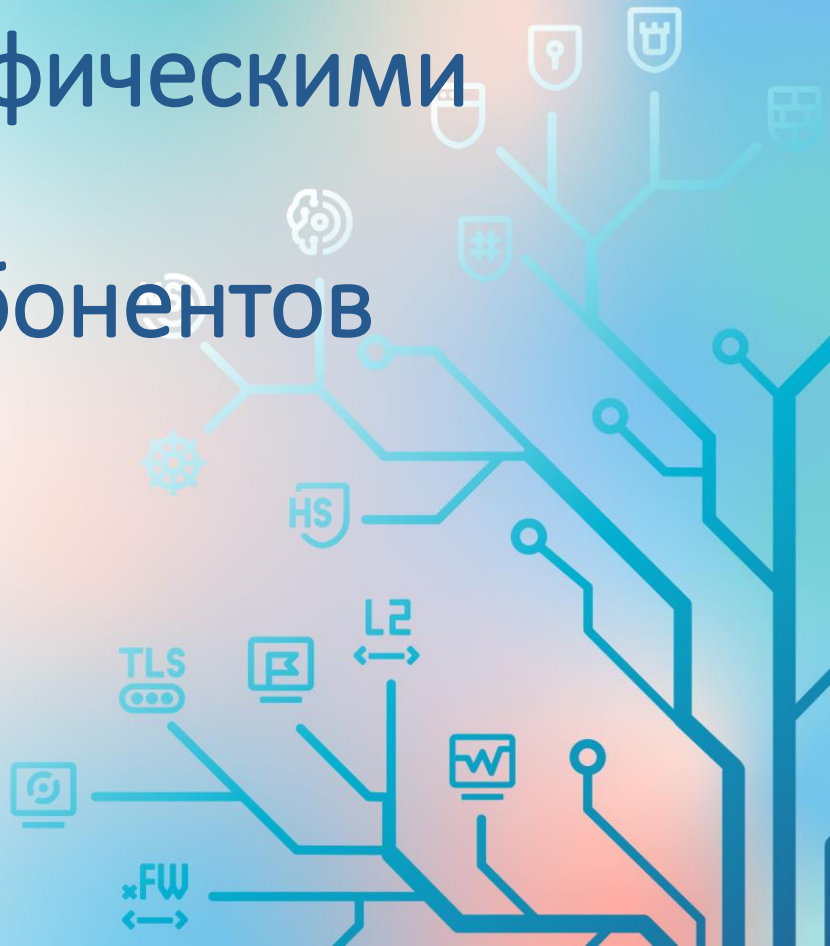


Управление криптографическими ключами для больших динамических групп абонентов

Бородин Михаил Алексеевич
Старший исследователь

 инфотекс

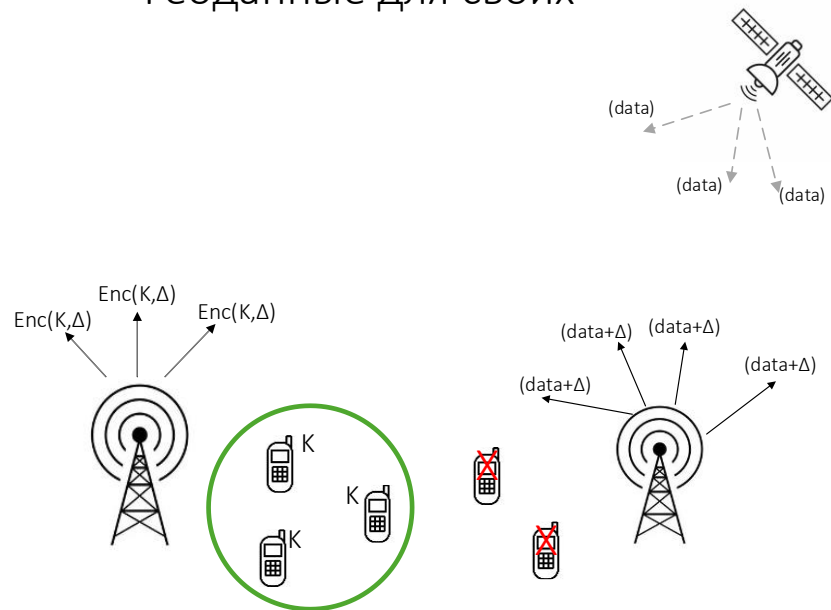
CTCrypt Минск 2026



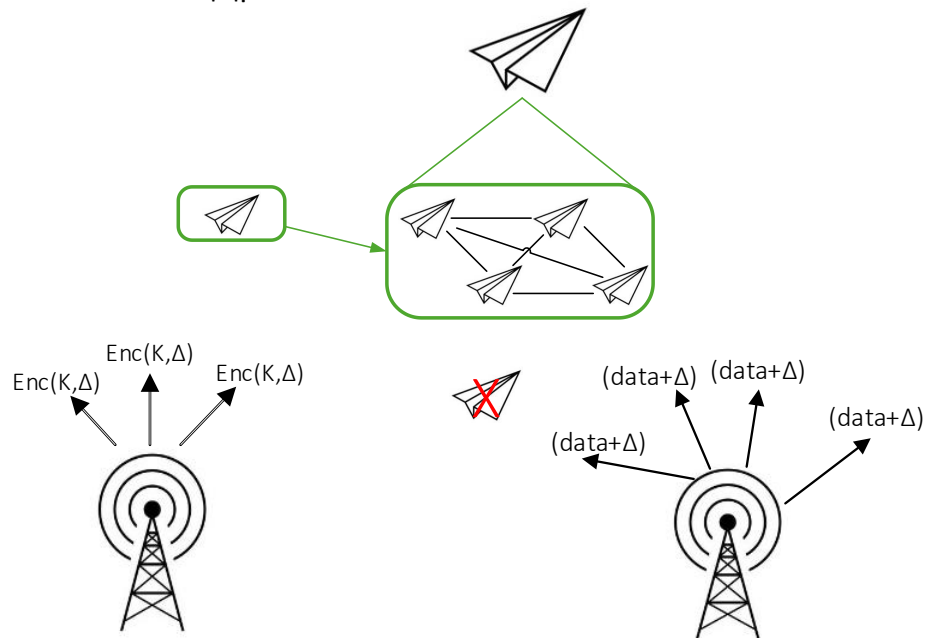
Рассматриваемые задачи

Рассмотрим две задачи:

- Геоданные для своих



- Рой дронов



Геоданные для СВОИХ

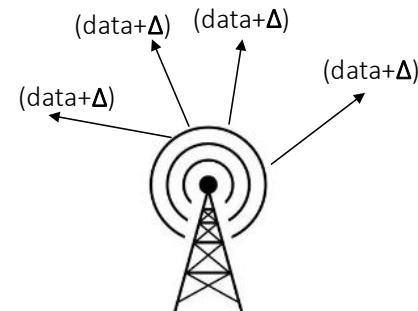
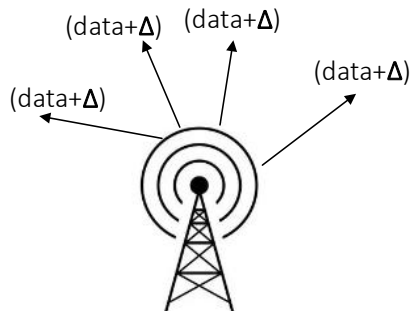
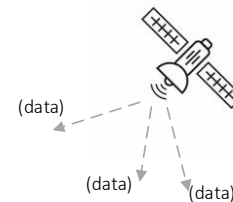
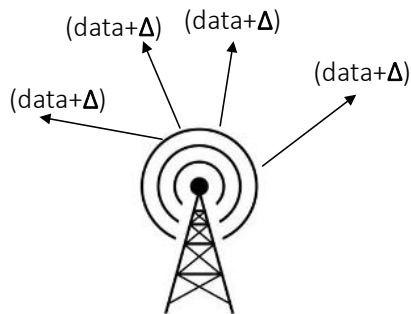


Геоданные для своих

Существует несколько способов трансляции ложных геоданных для чужих устройств и правильных данных для **своих**. Рассмотрим один из них.

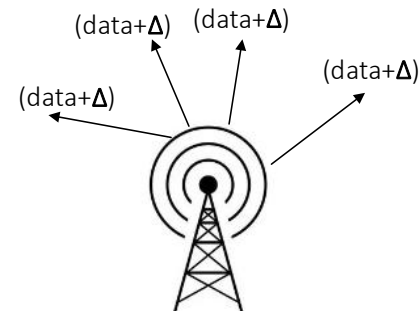
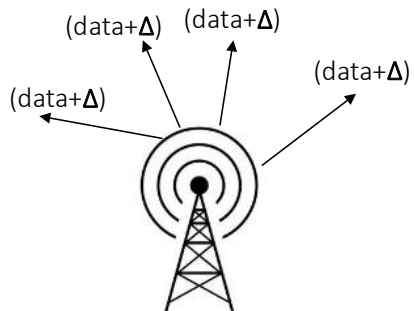
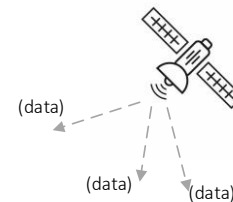
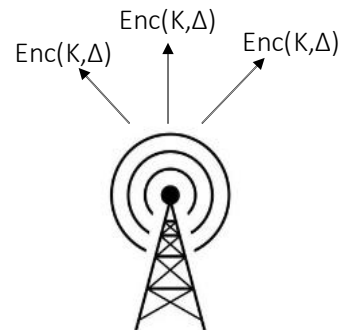
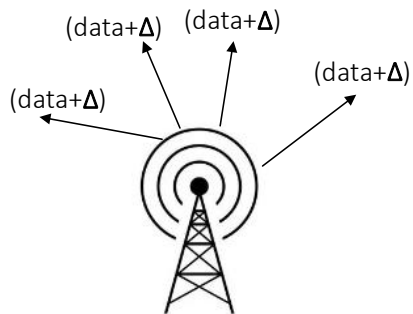
Геоданные для своих

В обозначенном месте устанавливаются «мощные» станции, которые транслируют геоданные со «смещением» ($\text{data} + \Delta$). «Смещение» Δ время от времени меняется.



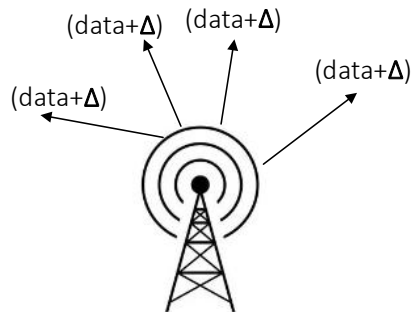
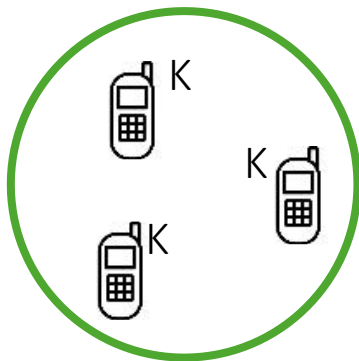
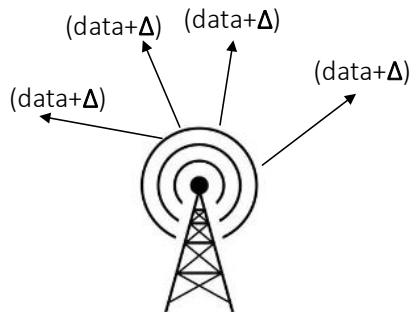
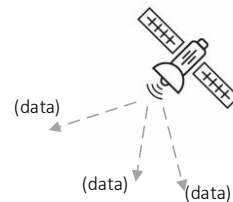
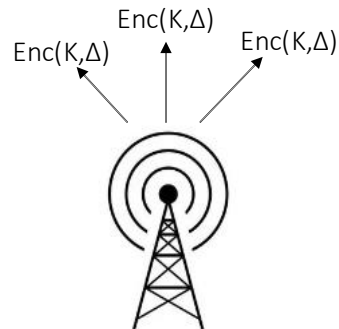
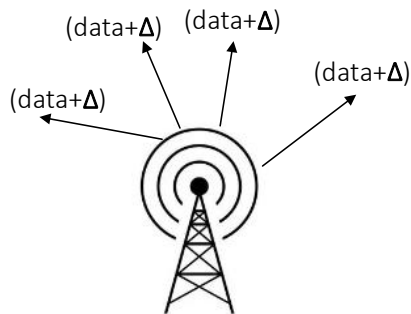
Геоданные для своих

В том же месте транслируется величина «смещения» Δ в защищенном виде: $\text{Enc}(K, \Delta)$.



Геоданные для своих

Свои устройства знают о смещении и обладают ключом K , поэтому они способны вычислить правильные геоданные. Остальные устройства не могут.



Геоданные для своих

Особенности:

1. Геоданные транслируются чаще, чем происходит смена величины «смещения».

Геоданные для своих

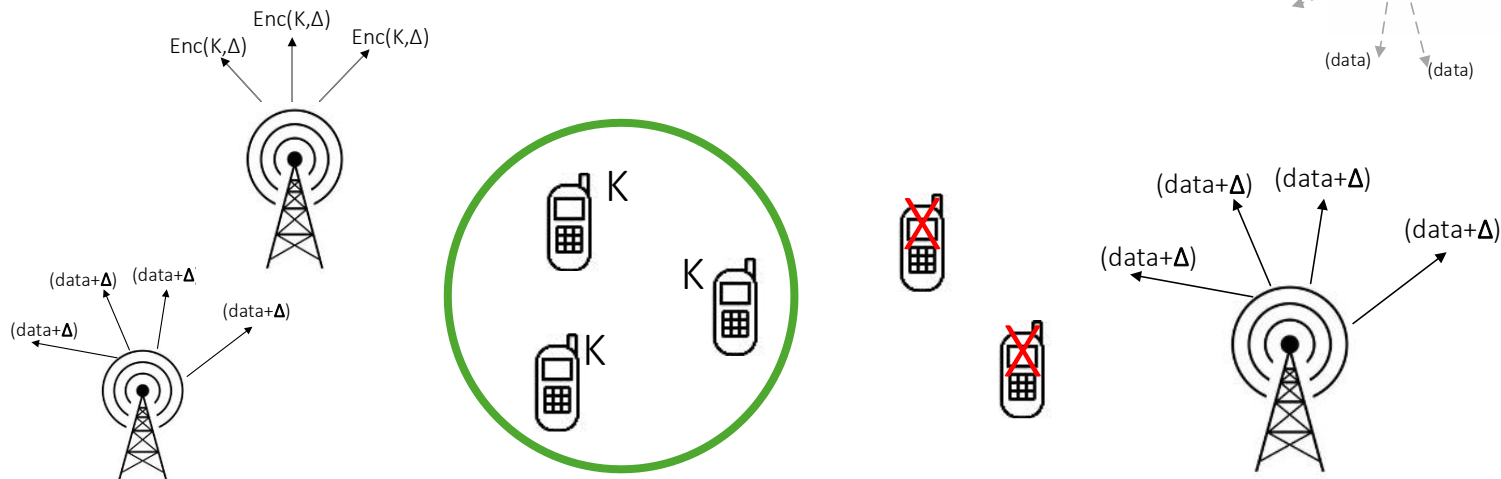
Особенности:

1. Геоданные транслируются чаще, чем происходит смена «смещения».
2. Список «своих» на момент трансляции «смещения» известен. Этот список может как расширяться, путем добавления новых устройств, так и сужаться путем удаления из него некоторых устройств. Более того, после удаления устройство снова может быть возвращено в этот список.

Геоданные для своих

Некоторые «размерности»:

1. Объем геоданных (data).
2. Частота смены «смещения» Δ .
3. Число устройств, находящихся в списке «свои».
4. Число отозванных устройств (удаленных из списка «свои»).



Геоданные для своих

Про безопасность:

1. Нарушитель может иметь сколько угодно отозванных устройств, но он не должен получать правильные геоданные.



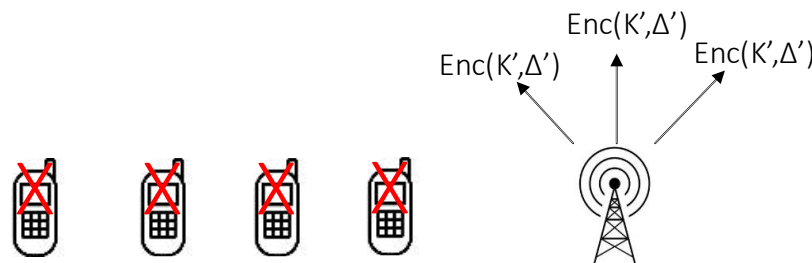
Геоданные для своих

Про безопасность:

1. Нарушитель может иметь сколько угодно отозванных устройств, но он не должен получать правильные геоданные.



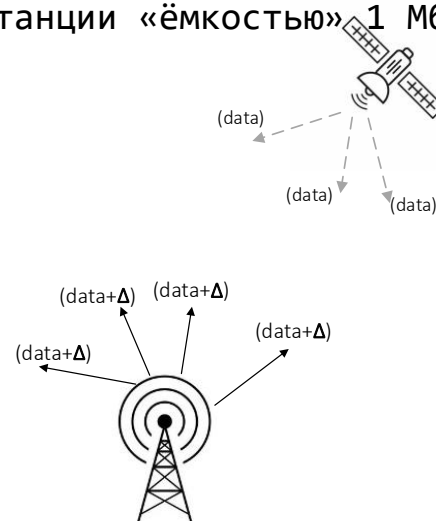
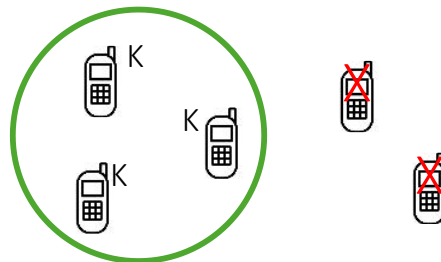
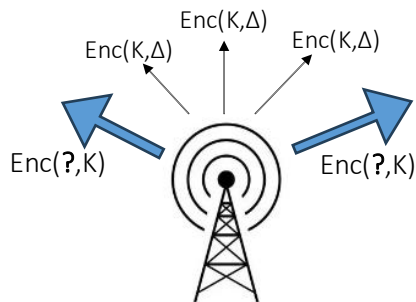
2. Защита от навязывания геоданных не является обязательной, но приветствуется. Можно рассматривать нарушителя, владеющего отозванными устройствами и собственной станцией трансляции.



Геоданные для своих

Пример:

- Общее число устройств: 10^6 .
- Динамика списка «своих»: ± 100 .
- Размер ключа шифрования + идентификатор: $32 + 4 = 36$ байт.
- Скорость **трансляции** геоданных: 50-1000 бит/с, полный кадр 1500 бит.
- Связь с устройствами: ключи транслируются через станции «ёмкостью» 1 Мбит/с.



Геоданные для своих

Пример:

- Общее число устройств: 10^6 .
- Динамика списка «своих»: ± 100 .
- Размер ключа шифрования + идентификатор: $32 + 4 = 36$ байт.
- Скорость **трансляции** геоданных: 50-1000 бит/с, полный кадр 1500 бит.
- Связь с устройствами: ключи транслируются через станции «ёмкостью» 1 Мбит/с.

Реализация системы защиты через парно-выборочные связи или PKI будет или низкопроизводительной, или потребует использовать мощную иерархическую инфраструктуру с делением устройств на группы и обслуживанием каждой из групп выделенным «сервером»/станцией. (Это можно обсудить).

Геоданные для своих

Пример:

- Общее число устройств: 10^6 .
- Динамика списка «своих»: +/- 100.
- Размер ключа шифрования + идентификатор: $32 + 4 = 36$ байт.
- Скорость **трансляции** геоданных: 50-1000 бит/с, полный кадр 1500 бит.
- Связь с устройствами: ключи транслируются через станции «ёмкостью» 1 Мбит/с.

Реализация системы защиты через парно-выборочные связи или PKI будет или низкопроизводительной, или потребует использовать мощную иерархическую инфраструктуру с делением устройств на группы и обслуживанием каждой из групп выделенным «сервером»/станцией. (Это можно обсудить).

Альтернатива - использовать подходы **широковещательного шифрования** (broadcast encryption).

Геоданные для своих

Широковещательное шифрование, некоторые работы:

-  NAOR D., NAOR M., LOTSPIECH J. REVOCATION AND TRACING SCHEMES FOR STATELESS RECEIVERS, CRYPTO 2001
-  BHATTACHERJEE S., SARKAR P. TREE BASED SYMMETRIC KEY BROADCAST ENCRYPTION, 2013
-  BHATTACHERJEE S., SARKAR P. REDUCING COMMUNICATION OVERHEAD OF THE SUBSET DIFFERENCE SCHEME, 2014
-  КИРЮХИН В.А, ПРОТОКОЛ ДОСТАВКИ КЛЮЧЕЙ «БУРУНДУК», РусКрипто 2026

Геоданные для своих

Основной принцип:

K - ключ защиты Δ , распространяется широковещательным сообщением:

$$(Id_1, Enc(H_1, K)) || (Id_2, Enc(H_2, K)) || \dots || (Id_x, Enc(H_x, K)),$$

где H_i - ключ, известный некоторой группе «своих» устройств.

Геоданные для своих

Основной принцип:

K - ключ защиты Δ , распространяется широковещательным сообщением:

$$(Id_1, Enc(H_1, K)) || (Id_2, Enc(H_2, K)) || \dots || (Id_x, Enc(H_x, K)),$$

где H_i - ключ, известный некоторой группе «своих» устройств.

Как распределить ключи H_i между устройствами?

Геоданные для своих

Основной принцип:

K - ключ защиты Δ , распространяется широковещательным сообщением:

$$(Id_1, Enc(K, H_1)) || (Id_2, Enc(K, H_2)) || \dots || (Id_x, Enc(K, H_x)),$$

где H_i - ключ, известный некоторой группе «своих» устройств.

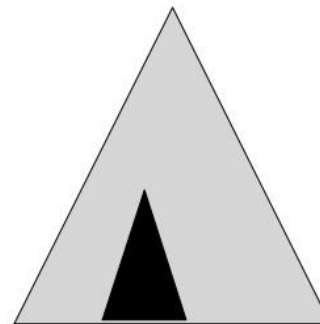
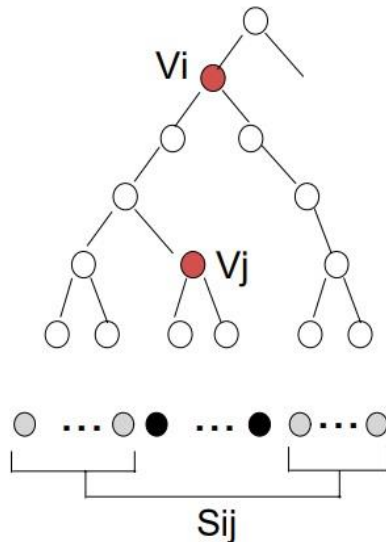


*Рисунок из работы NAOR D., NAOR M., LOTSPIECH J. REVOCATION AND TRACING SCHEMES FOR STATELESS RECEIVERS

Геоданные для своих

Параметры:

- Число участников: N .
- Число отзывов: r .
- Длина ключа: $|K|$.
- Объем данных в канале в битах: M .
- Число хранимых ключей на устройстве: T .

В предложенных условиях:

- $N = 10^6$.
- $r = 100$.
- $|K| = 256$ бит.
- $\log_2(N) < 32$.

На примере «БУРУНДУКА»:

$M = c \cdot r \cdot (|K| + \log_2(N))$, где $c \leq 2$.

$$T \approx \frac{1}{2} (\log_2(N))^2.$$

В предложенных условиях:

- $M < 2 \cdot 100 \cdot (290 \text{ бит});$
 $M < 58 \text{ Кбит или } 7,25 \text{ Кбайт.}$
 $T \approx 200 \text{ ключей.}$

Геоданные для своих

Фрагмент ключевой системы:

- В ключевом центре строится древо ключей (H_i). Размер дерева может быть выбран с запасом.
- Ключи распределяются по устройствам (личная явка / доверенная доставка / *место для Industrial PKI*).
- При формировании широковещательного сообщения:
 - вычисляется подходящее подмножество (H_i);
 - формируется широковещательное сообщение $(Id_1, Enc(H_1, K)) || (Id_2, Enc(H_2, K)) || \dots || (Id_x, Enc(H_x, K))$.
- В случае отзыва какого-нибудь устройства:
 - меняется «смещение» и меняется ключ защиты;
 - вычисляется новое подмножество (H_i) и формируется новое широковещательное сообщение.

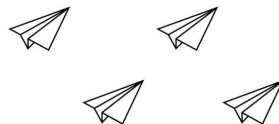
Рой дронов



Рой дронов

Рой дронов:

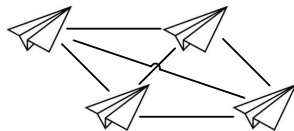
- группа дронов, выполняющая совместное задание.



Рой дронов

Рой дронов:

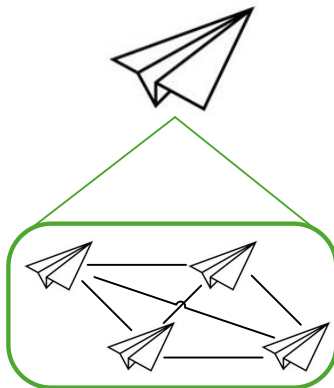
- группа дронов, выполняющая совместное задание.
- в группе между дронами должны быть парные связи.



Рой дронов

Рой дронов:

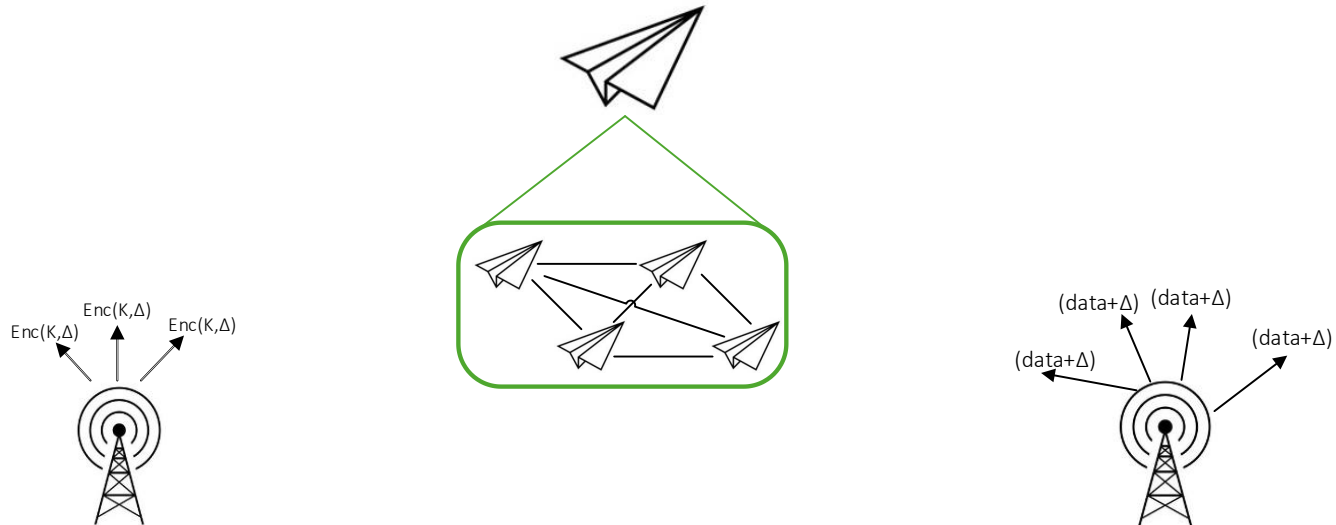
- группа дронов, выполняющая совместное задание.
- в группе между дронами должны быть парные связи.
- в группе может быть «материнский» дрон – это выделенный член группы, осуществляющий управление группой.



Рой дронов

Рой дронов:

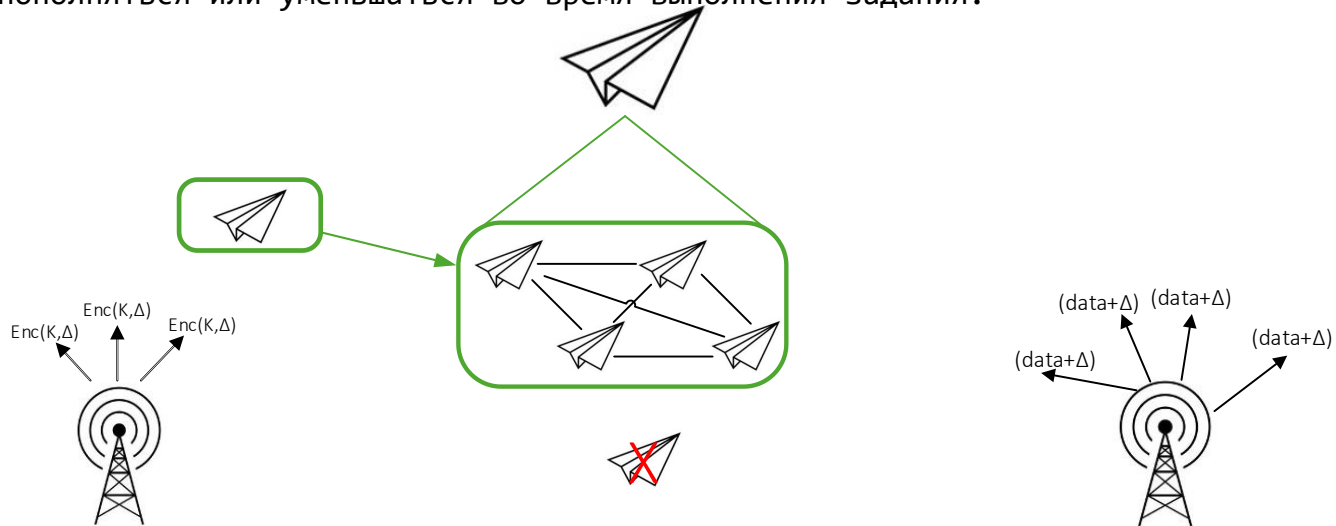
- группа дронов, выполняющая совместное задание.
- в группе между дронами должны быть парные связи.
- в группе может быть «материнский» дрон – это выделенный член группы, осуществляющий управление группой.
- группа и каждый дрон в отдельности может иметь связь с узлами наземной инфраструктуры.



Рой дронов

Рой дронов:

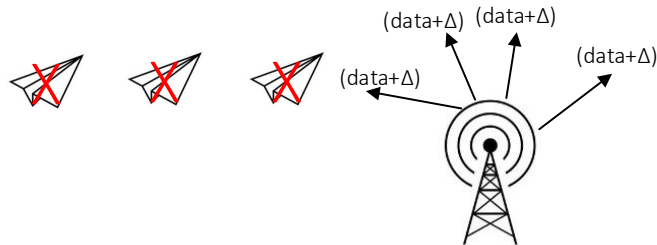
- группа дронов, выполняющая совместное задание.
- в группе между дронами должны быть парные связи.
- в группе может быть «материнский» дрон – это выделенный член группы, осуществляющий управление группой.
- группа и каждый дрон в отдельности может иметь связь с узлами наземной инфраструктуры.
- группа может пополняться или уменьшаться во время выполнения задания.



Рой дронов

Про безопасность:

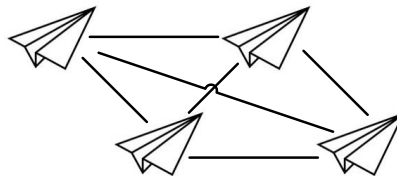
- Активный нарушитель обладает **некоторым количеством** отозванных дронов и своими узлами наземной инфраструктуры.
- Компрометация материнского дрона не рассматривается. Попытку подмены сигнала материнского дрона можно рассматривать как ложный сигнал с наземной инфраструктуры.
- Цели: нарушить конфиденциальность связи, внедрить ложное сообщение.



Рой дронов

Как реализовать:

- в группе между дронами должны быть парные связи.



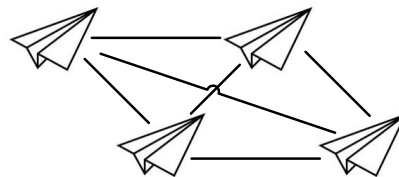
Предложение,

для парных связей можно использовать схему Блома (есть пример использования Р 1323565.1.028–2019).

Рой дронов

Как реализовать:

- в группе между дронами должны быть парные связи.



Предложение,

для парных связей можно использовать схему Блома (есть пример использования Р 1323565.1.028–2019).

Или симметричные ключи, или Industrial PKI?

Рой дронов

	Схема Блома	«Симметрия»	I_PKI
Хранение	Вектор размера ($u+1$), ID дрона	N ключей, ID дрона	Сертификат и закрытый ключ
Вычисления	Хэш и значение полинома степени u	-	Д.-Х., подпись
Обмен	Отправить ID, получить ID	-	Д.-Х. с сертификатом
Добавление	Добавить в список «своих» / проверить отзыв	Добавить в список «своих» / проверить отзыв	Добавить в список «своих» / проверить отзыв
Удаление	Удалить ID из списка «своих» ИЛИ проверить отзыв	Добавить в список «своих» / проверить отзыв	Добавить в список «своих» / проверить отзыв
Особенность	Параметр безопасности u	Ограничение на число участников: не больше N.	• Не PQC. • Защищенность от чтения назад. • Нормативные документы?

Рой дронов

Как реализовать:

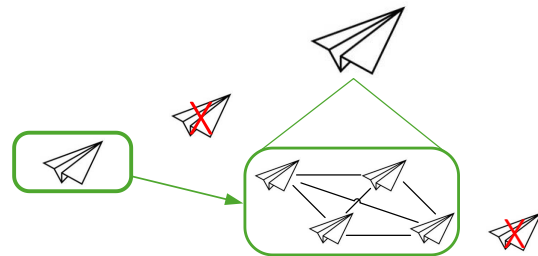
- в группе может быть «материнский» дрон – это выделенный член группы, осуществляющий управление группой.

Предложение,

для групповой рассылки можно использовать широковещательное шифрование, центр – материнский дрон.

Индивидуальная связь возможна как с использованием схемы Блома, так и частный случай широковещательного шифрования.

Защита от навязывания скомпрометированных ключей: подписи, цепочки временных ключей («Бурундук» обеспечивает защиту от навязывания).



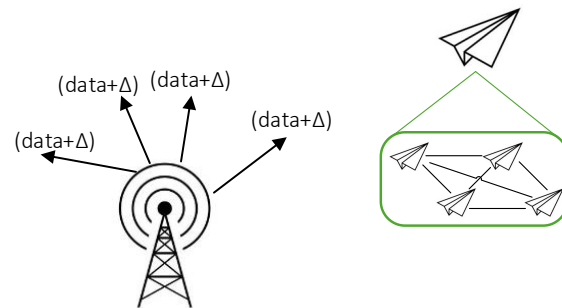
Рой дронов

Как реализовать:

- группа и каждый дрон в отдельности может иметь связь с узлами наземной инфраструктуры.

В зависимости от задачи узел наземной инфраструктуры можно рассматривать и как узел схемы Блома, и как центр широковещательного шифрования.

Альтернативы для схемы Блома: симметричные ключи или Industrial PKI.



Заключение

- Широковещательное шифрование востребовано в промышленном интернете вещей (ПИВ):
 - В ПИВ довольно много задач, требующих обеспечить защищенную массовую рассылку, к примеру: «Трансляция дорожной обстановки», «Мгновенная остановка конвейера», «Обновление информации в умных счётчиках» и т.д.
 - Использование в этих задачах именно широковещательного шифрования может быть как минимум **дешево** и **удобно**, а порой **безальтернативно** с учетом доступных вычислительных ресурсов.
 - Ввиду изложенного, было бы полезно иметь некоторое описание механизма широковещательного шифрования в виде нормативного документа.

Заключение

- Широковещательное шифрование востребовано в промышленном интернете вещей (ПИВ):
 - В ПИВ довольно много задач, требующих обеспечить защищенную массовую рассылку, к примеру: «Трансляция дорожной обстановки», «Мгновенная остановка конвейера», «Обновления информации в умных счётчиках» и т.д.
 - Использование в этих задачах именно широковещательного шифрования может быть как минимум **дешево** и **удобно**, а порой **безальтернативно** с учетом доступных вычислительных ресурсов.
 - Ввиду изложенного, было бы полезно иметь некоторое описание механизма широковещательного шифрования в виде нормативного документа.
- Вопрос к аудитории: «Какие перспективы по внедрению PQS в индустриальный PKI?»



Спасибо за внимание!

