Особенности криминалистического анализа некоторых смартфонов на базе чипсетов Qualcomm

Чиликов А.А., к.ф.-м.н., доцент кафедры «Информационная безопасность», МГТУ им.Баумана, Passware Inc.

Хоруженко Г.И., Passware Inc.

2019 г.

Актуальность

Версия ОС Android	Функция вычисления ключа из пароля (KDF)	Решение для перебора без участия телефона (offline)
4.3 (JellyBean) и ниже	PBKDF2	+
4.4 (KitKat)	scrypt	+
5 (Lollipop) и выше	**scrypt + keymaster**	**?**

Предположения об объекте исследования

- **Установлена последняя версия ПО** – Android 5 и выше
- **FRP: ON** – нет штатной возможности загрузить неподписанный образ boot.img/recovery.img
- **Шифрование: включено**
- **Secure Startup: ON** – ключ шифрования вычисляется на основе пароля пользователя

Moto G4

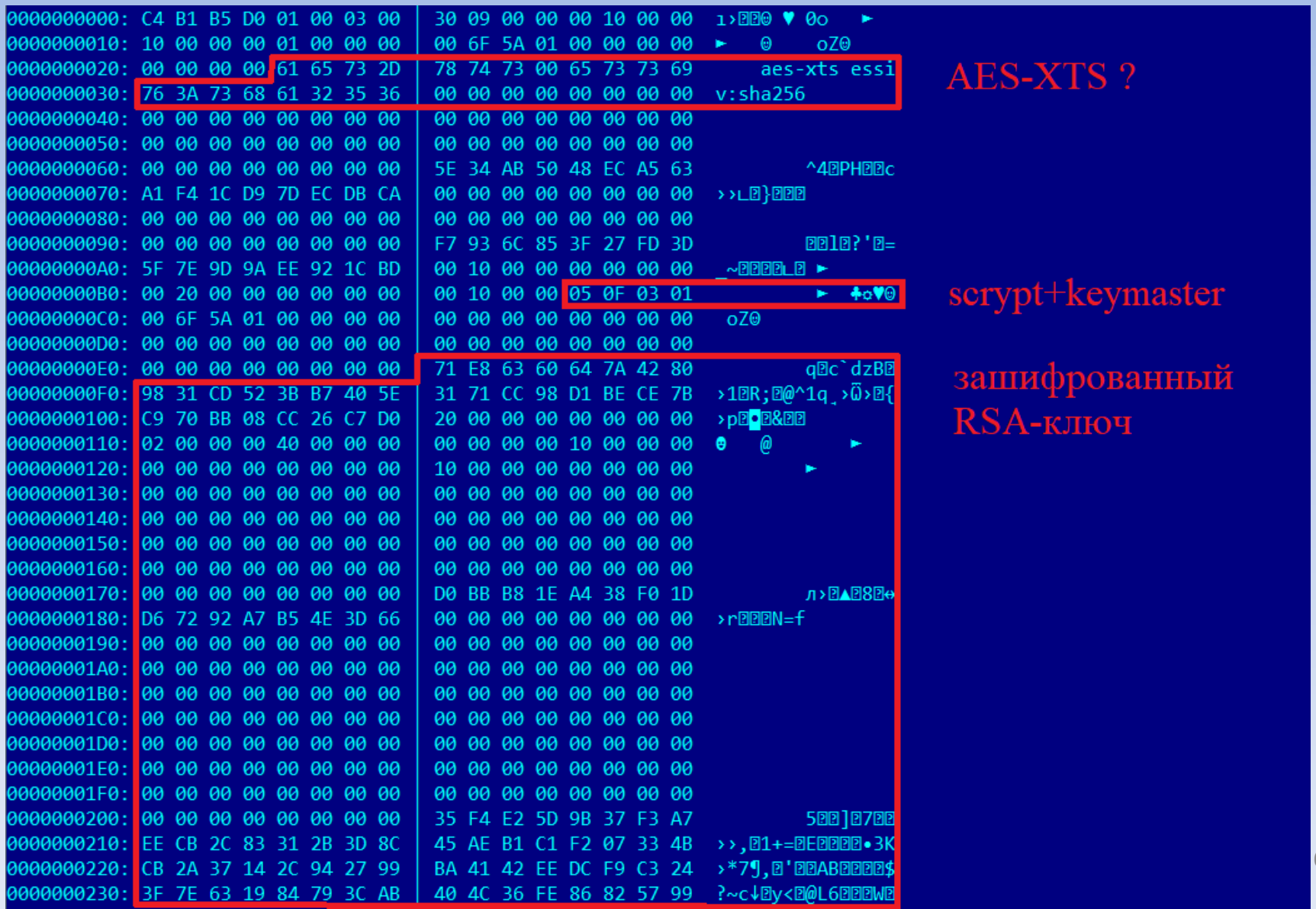
Год выпуска: **2016**
Чипсет: **Qualcomm MSM8952**

*https://www.gsmarena.com/motorola_moto_g4-pictures-8103.php

Moto G4: подходы

1. **chip-off/ISP** ?

Moto G4: crypto footer



Moto G4: подходы

1. ~~**chip-off/ISP**~~ – scrypt+keymaster
2. **custom recovery (TWRP, …)** ?

Moto G4: подходы

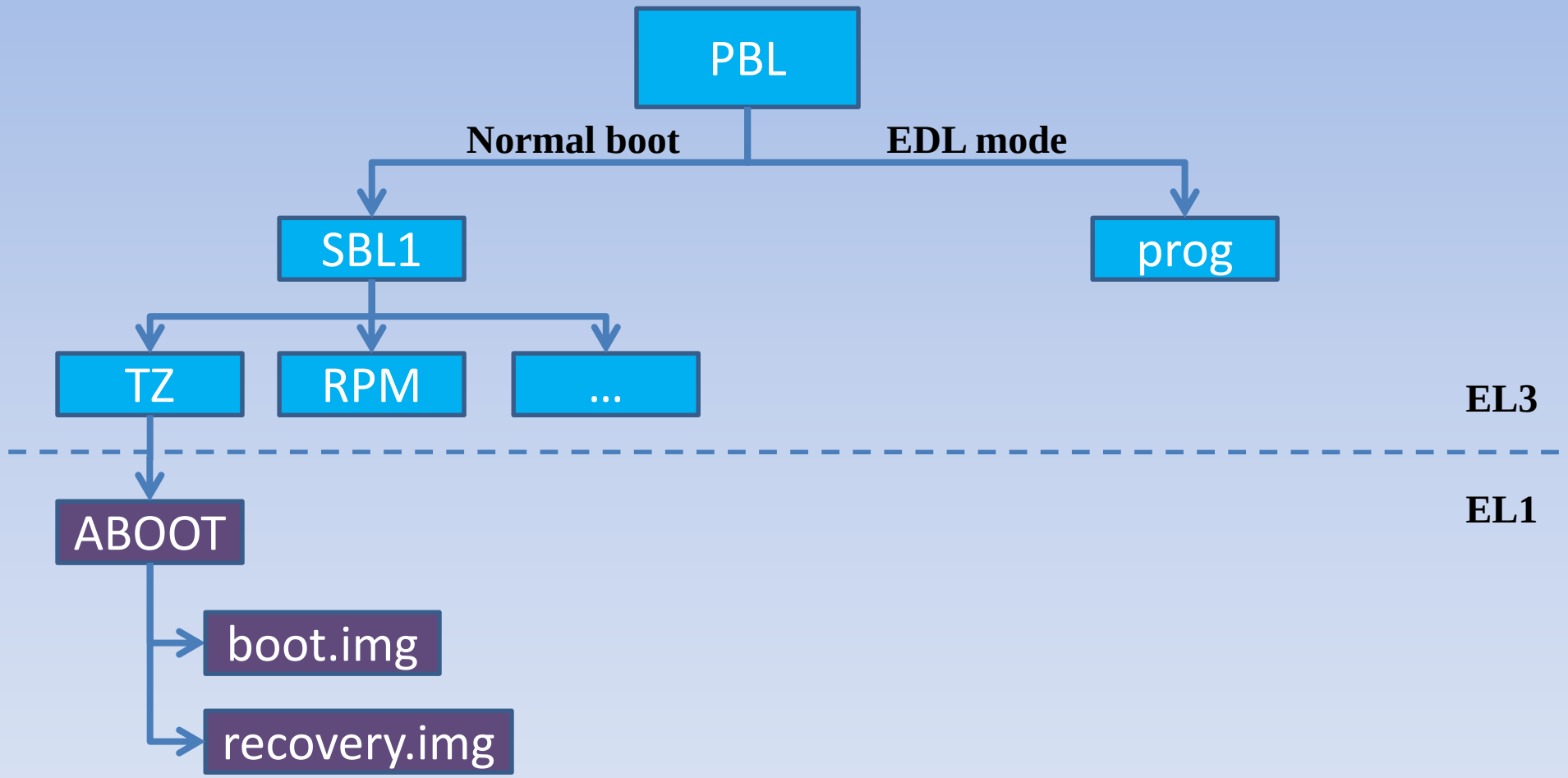
1. ~~**chip-off/ISP**~~ – scrypt+keymaster
2. ~~**custom recovery (TWRP, …)**~~ **–** включен FRP
3. **kernel cmdline injection (CVE-2016-10277)** ?

Moto G4: подходы

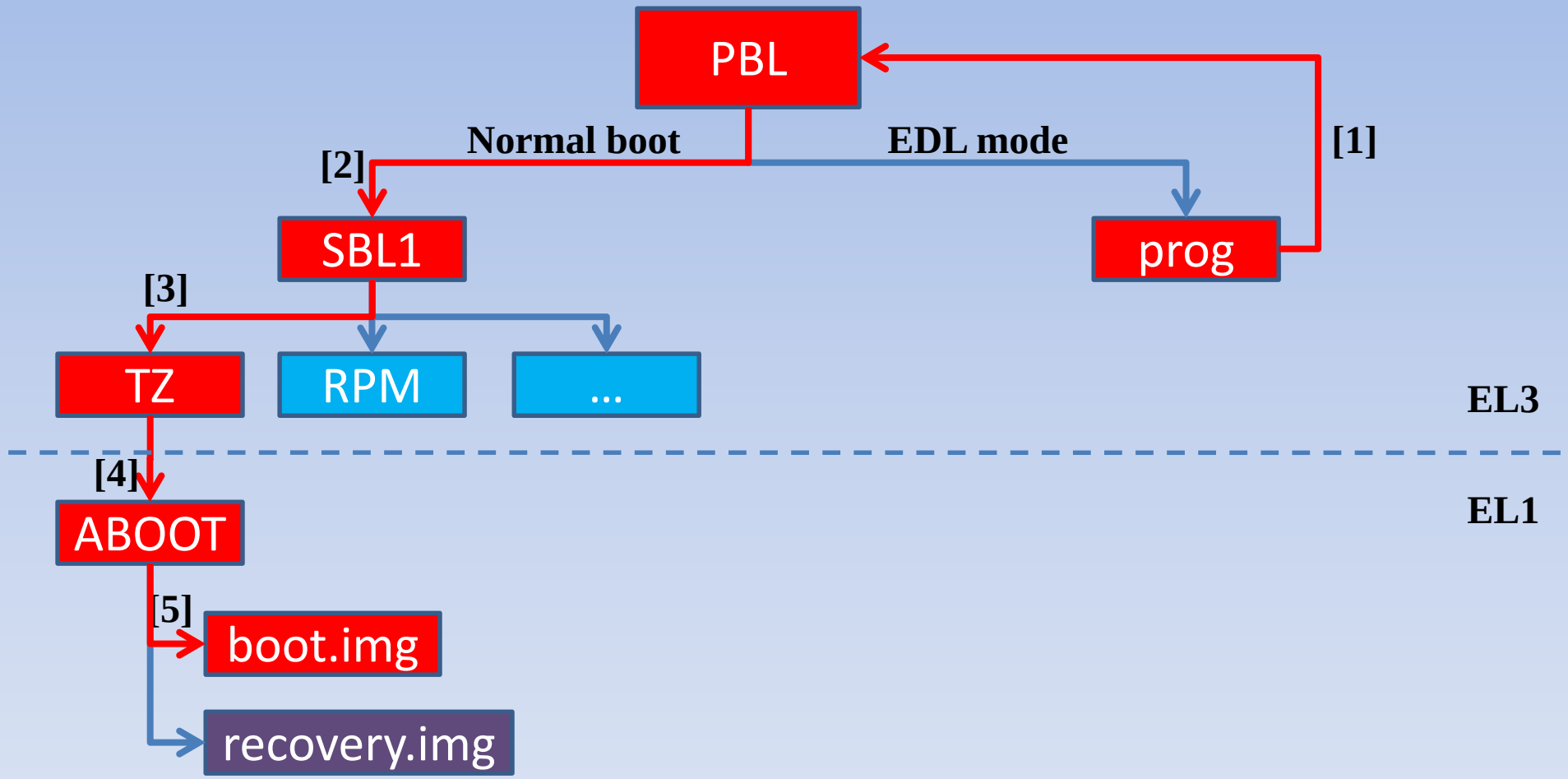
1. ~~**chip-off/ISP**~~ – scrypt+keymaster
2. ~~**custom recovery (TWRP, …)**~~ **–** включен FRP
3. ~~**kernel cmdline injection (CVE-2016-10277)**~~ – есть патч
4. **EDL mode: peek/poke (QPSIIR-909)*** ?

*https://alephsecurity.com/vulns/aleph-2017028

Описание QPSIIR-909 (1)



Описание QPSIIR-909 (2)



Описание QPSIIR-909 (3)

Необходимые условия:

1. Наличие **prog-**файла для данной модели
2. **prog-**файл выполняется с наивысшими привилениями (**EL3** в терминах **aarch64**)
3. Учтены особенности аппаратной платформы
4. Реализованы и доступны функции **peek/poke**

Moto G4: подходы

1. ~~**chip-off/ISP**~~ – scrypt+keymaster
2. ~~**custom recovery (TWRP, …)**~~ **–** включен FRP
3. ~~**kernel cmdline injection (CVE-2016-10277)**~~ – есть патч
4. ~~**EDL mode: peek/poke (QPSHR-909)***~~ – команды peek/poke недоступны
5. **Уязвимость в PBL MSM8952**** ?

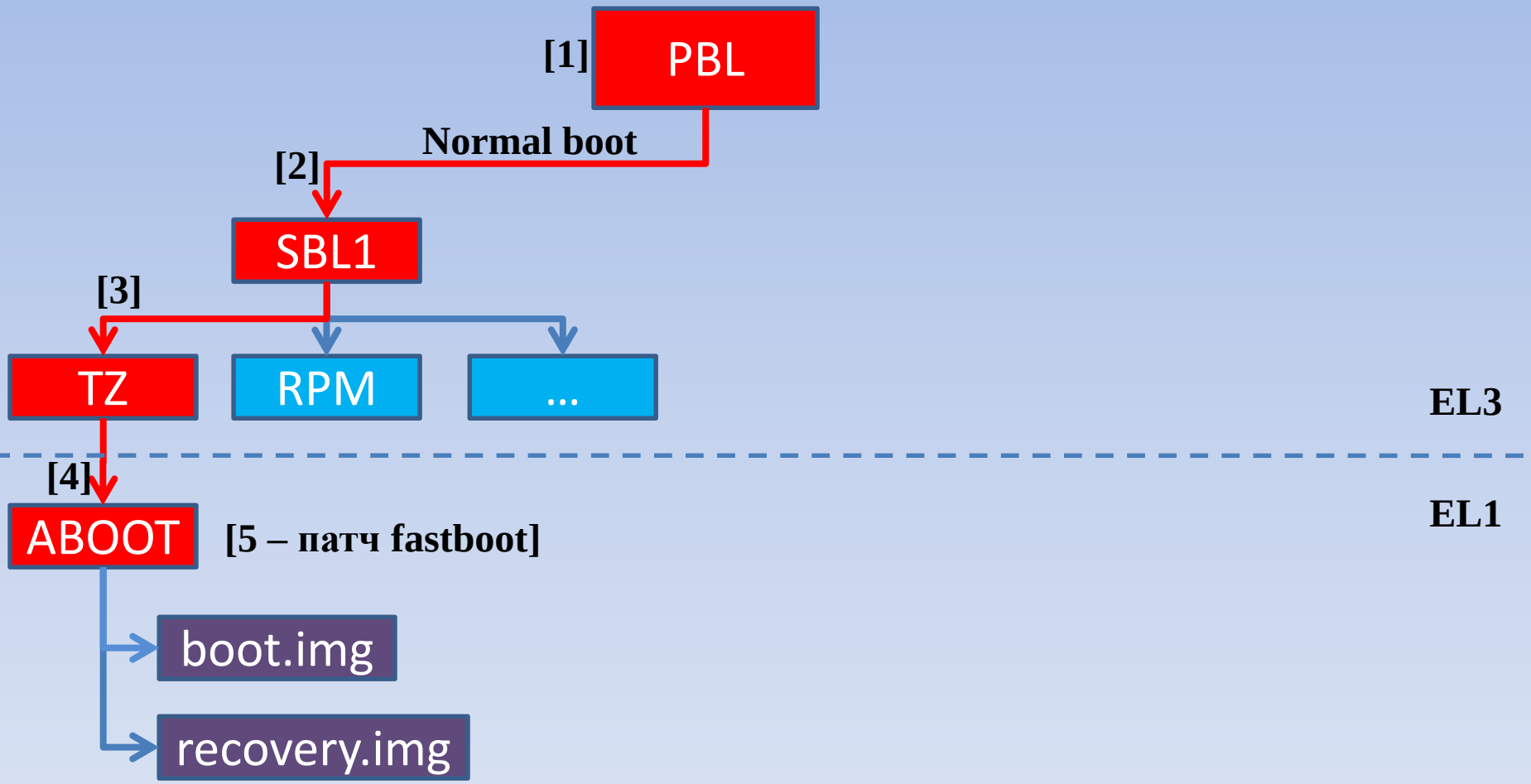
*https://alephsecurity.com/vulns/aleph-2017028

**https://www.bluehatil.com/2018/files/Terrorist2%20Phone%20Unlocking%20101%20-%20BlueHat%20IL%202018.pdf

Уязвимость в PBL MSM8952 (1)

- Устройство – **ZTE Zmax Pro (MSM8952)**
- Доклад:
  - Общее описание работы в режиме **EDL**
  - Никаких деталей об уязвимости/шифровании

Уязвимость в PBL MSM8952 (2)



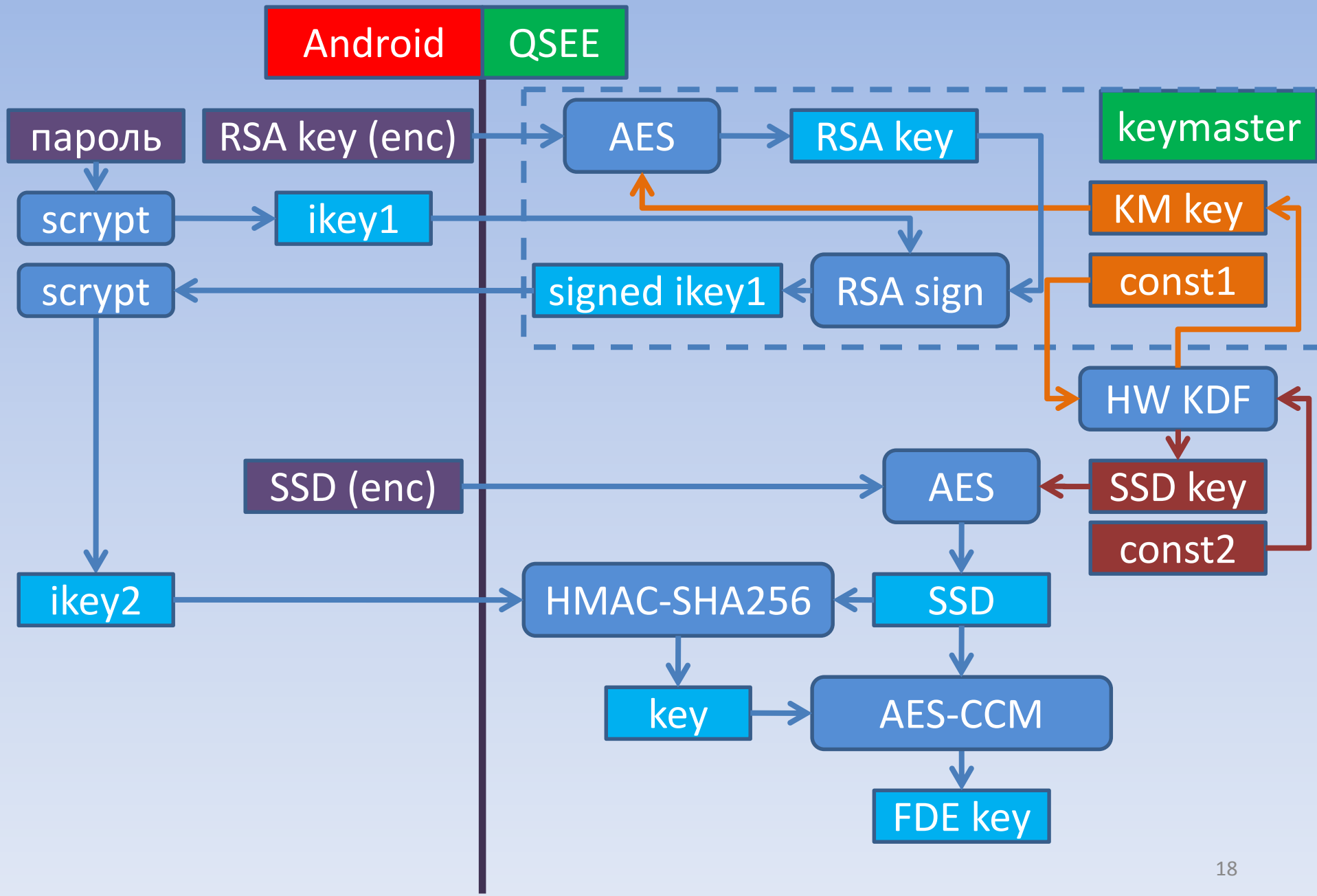
Уязвимость в PBL MSM8952 (3)

Необходимые условия:

1. Чипсет – **MSM8952**
2. Устройство должно быть переведено в режим **EDL** (программно/аппаратно)

Moto G4: перевод в режим EDL

Moto G4: схема FDE



Moto G4: итоги

1. Возможна компрометация **Secure Boot** через уязвимость в **PBL** (**MSM8952**)
2. Перебор **offline** возможен путём извлечения пары ключей (**KM key**, **SSD Key**)
3. Алгоритм перебора состоит из нескольких этапов:

- **scrypt + RSA-sign + scrypt**
- итеративный **HMAC-SHA256**
- **AES-CCM**

Moto G3

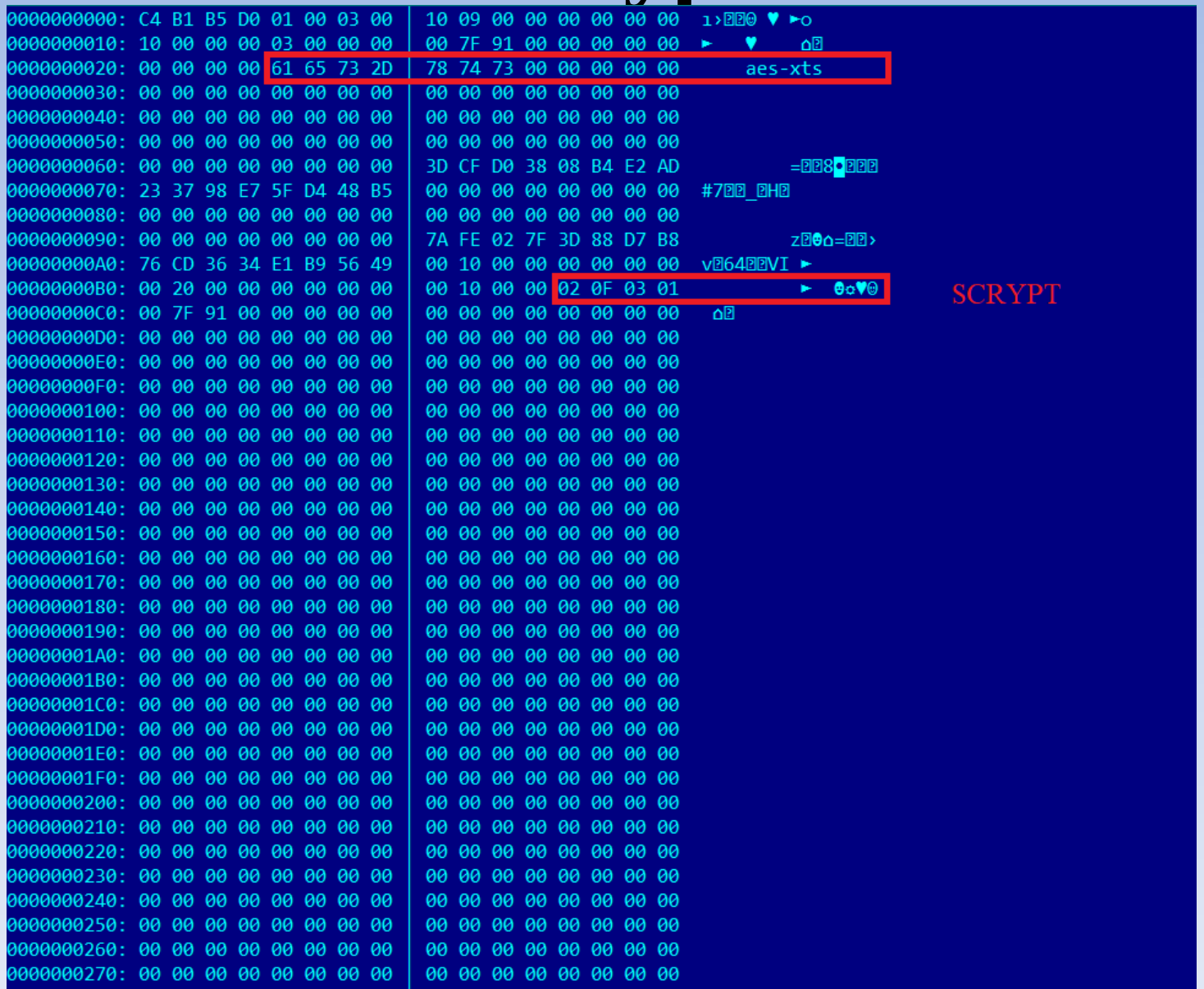
Год выпуска: **2015**
Чипсет: **Qualcomm MSM8916**

*https://www.gsmarena.com/motorola_moto_g_(3rd_gen)-pictures-7247.php

Moto G3: подходы

1. **chip-off/ISP** ?

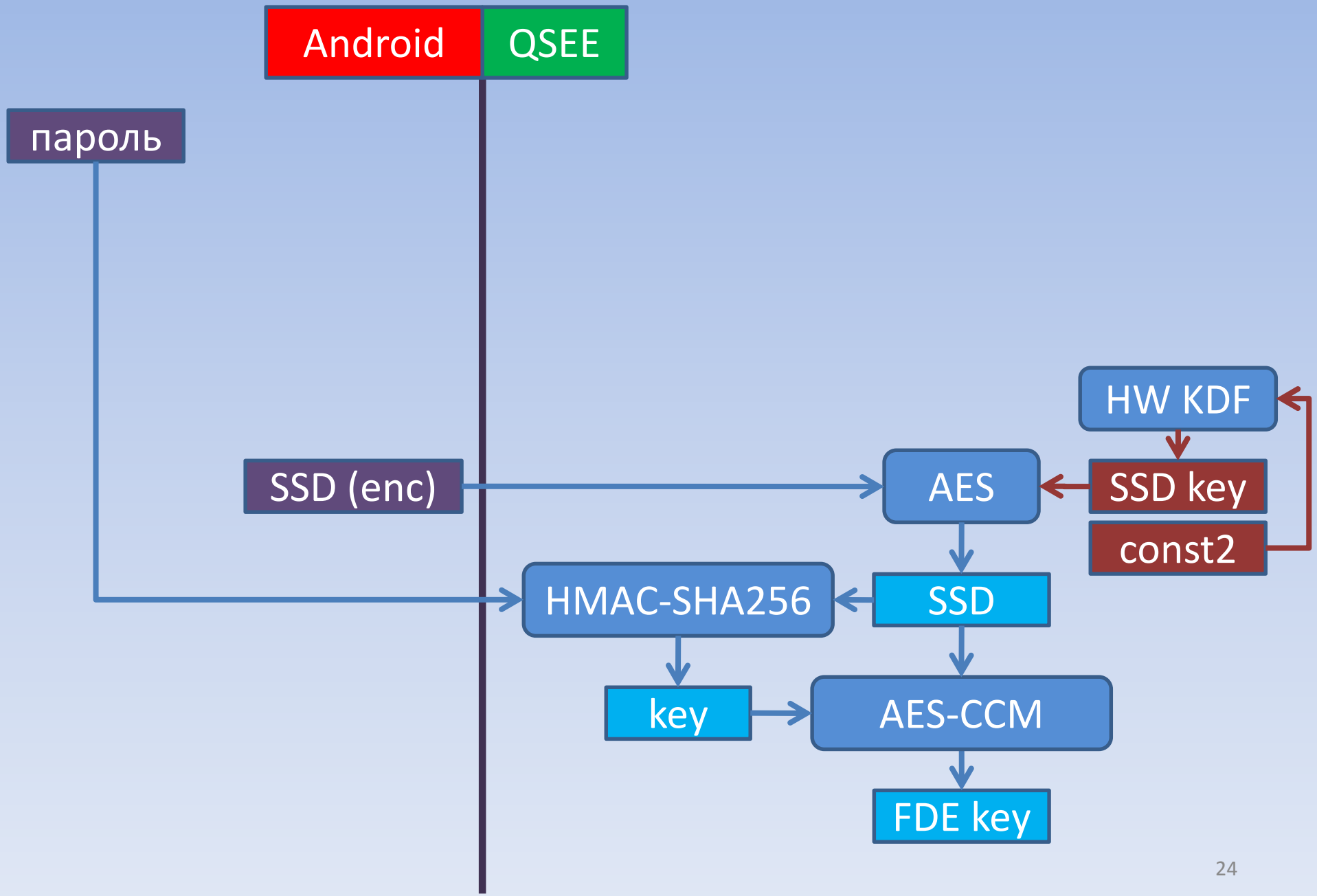
Moto G3: crypto footer



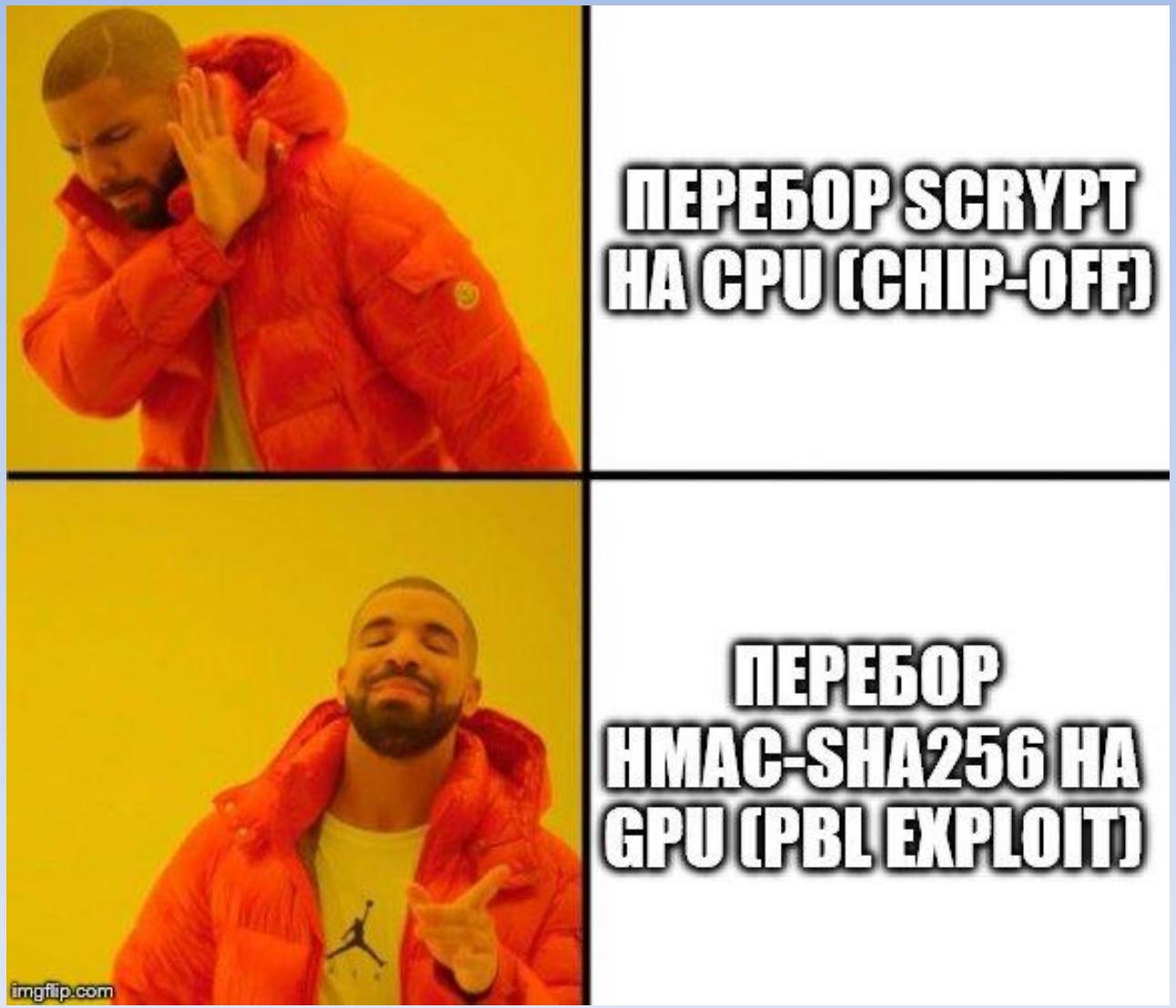
Moto G3: подходы

1. ~~**chip-off/ISP**~~ – scrypt, но aes-xts
2. ~~**custom recovery (TWRP, …)**~~ **–** включен FRP
3. ~~**kernel cmdline injection (CVE-2016-10277)**~~ – есть патч
4. ~~**EDL mode: peek/poke (QPSHR-909)**~~ – нет prog-файла
5. **Уязвимость в PBL MSM8916** ?

Moto G3: схема FDE



Moto G3: scrypt VS hmac-sha256



Moto G3: итоги

1. Возможна компрометация **Secure Boot** через уязвимость в **PBL** (**MSM8952**)
2. Перебор **offline** возможен путём извлечения ключа **SSD Key**
3. Алгоритм перебора состоит из нескольких этапов (возможно ускорение на **GPU**):

- итеративный **HMAC-SHA256**
- **AES-CCM**

Samsung J5 (2016)

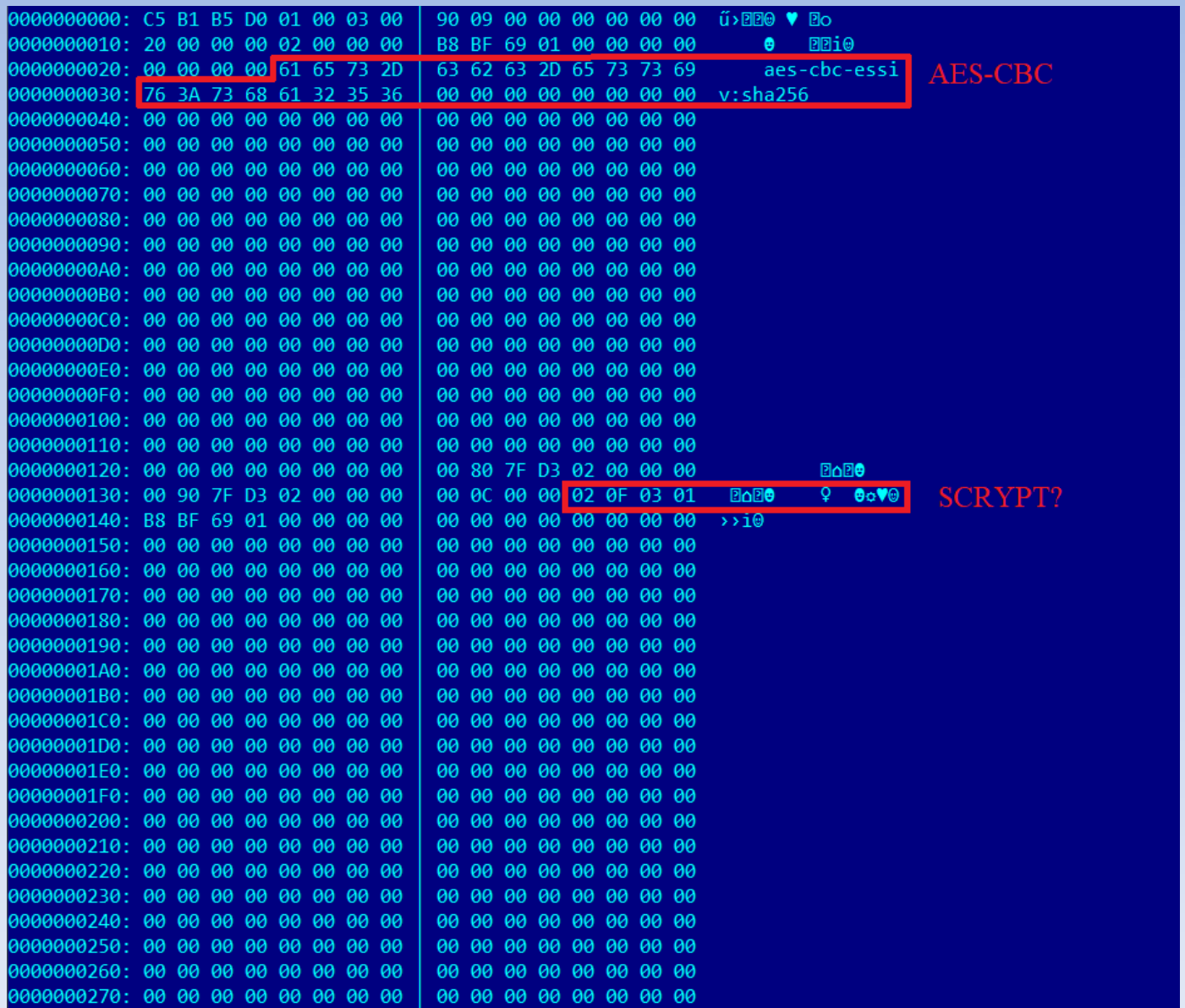
Год выпуска: **2016**
Чипсет: **Qualcomm MSM8916**

*https://www.gsmarena.com/samsung_galaxy_j5_(2016)-pictures-7869.php

Samsung J5 (2016): подходы

1. **chip-off/ISP** ?

Samsung J5 (2016): footer (1)



Samsung J5 (2016): footer (2)

зашифрованный RSA-ключ

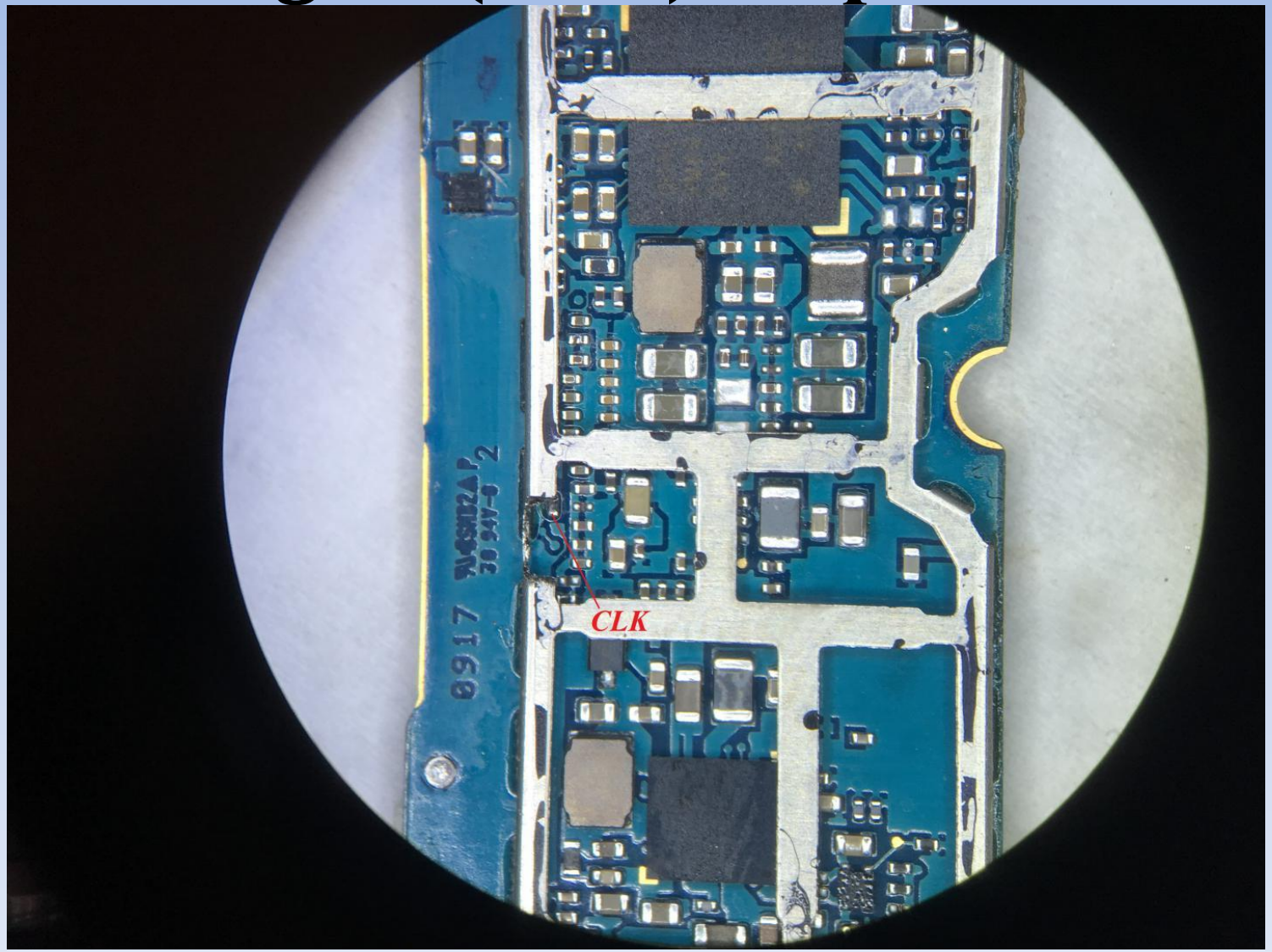
Samsung J5 (2016): подходы

1. ~~**chip-off/ISP**~~ – scrypt+keymaster
2. ~~**custom recovery (TWRP, …)**~~ **–** включен FRP
3. **engboot** ?

Samsung J5 (2016): подходы

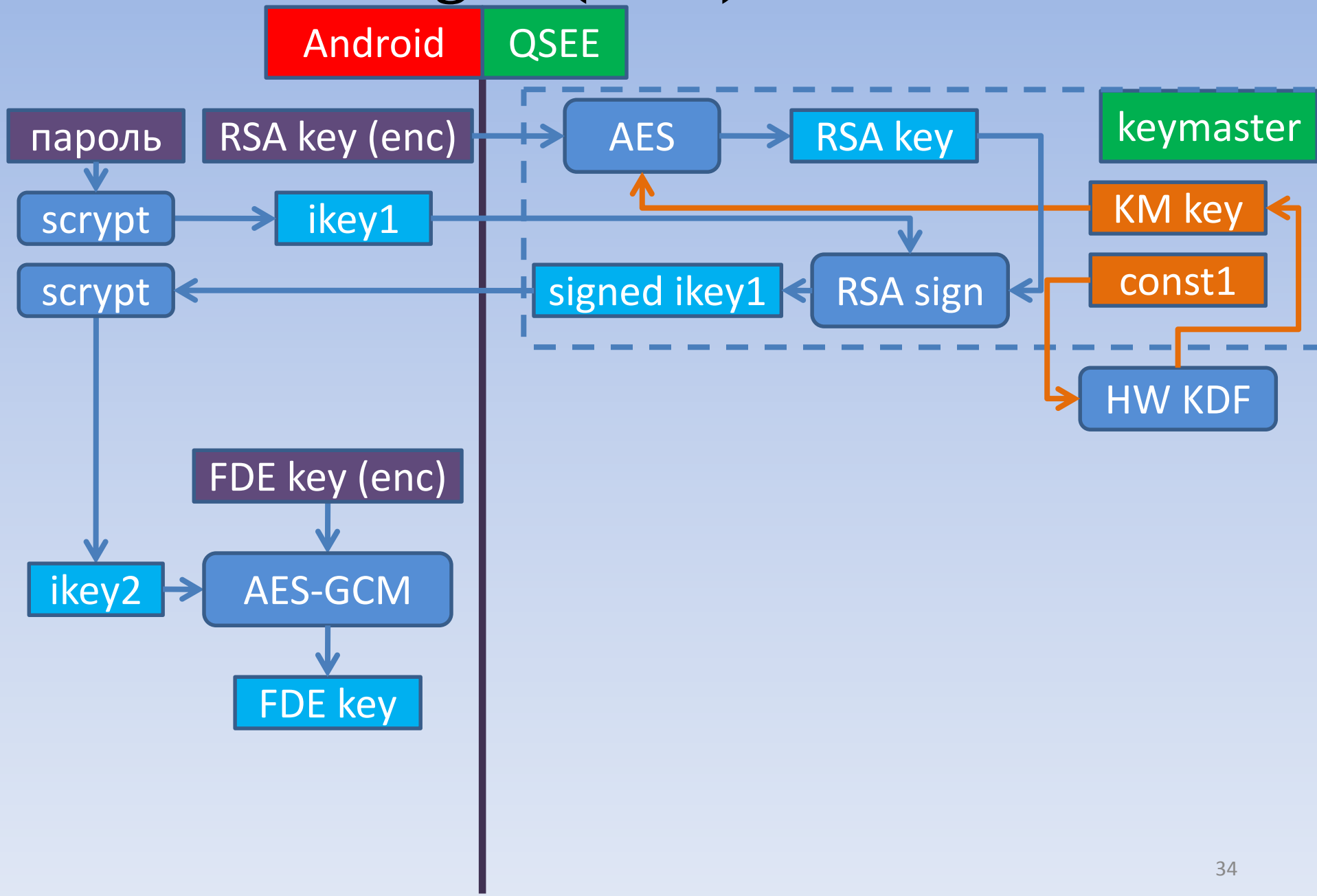
1. ~~**chip-off/ISP**~~ – scrypt+keymaster
2. ~~**custom recovery (TWRP, …)**~~ **–** включен FRP
3. ~~**engboot**~~ – есть только для Android 6 (актуальная версия – 7)
4. ~~**EDL mode: peek/poke (QPSHR-909)**~~ – нет prog-файла
5. **Уязвимость в PBL MSM8916**

Samsung J5 (2016): перевод в EDL



*http://www.gsmforum.ru/threads/305154-Samsung-SM-J510FN-JTAG-unsupported-device?p=1329075

Samsung J5 (2016): схема FDE



Samsung J510F: итоги

1. Возможна компрометация **Secure Boot** через уязвимость в **PBL** (**MSM8952**)
2. Перебор **offline** возможен путём извлечения ключа **KM key**
3. Алгоритм перебора состоит из нескольких этапов:

- **scrypt + RSA-sign + scrypt**
- **AES-GCM**

Результаты работы

- Обнаружены слабости криптографических схем вычисления ключа шифрования для **FDE** в телефонах **Moto G4**, **Moto G3**, **Samsung J5 2016,** приводящие к возможности **offline-**перебора пароля и расшифрования раздела **userdata**.

Спасибо за внимание!