

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

Moto G4: подходы

1. chip-off/ISP ?

Moto G4: crypto footer

```
000000000: C4 B1 B5 D0 01 00 03 00 | 30 09 00 00 00 10 00 00 | 1>P@ ♥ 0o ▶
000000010: 10 00 00 00 01 00 00 00 | 00 6F 5A 01 00 00 00 00 | ▶ @ oZ@
000000020: 00 00 00 00 61 65 73 2D | 78 74 73 00 65 73 73 69 | aes-xts essi
000000030: 76 3A 73 68 61 32 35 36 | 00 00 00 00 00 00 00 00 | v:sha256
000000040: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000050: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000060: 00 00 00 00 00 00 00 00 | 5E 34 AB 50 48 EC A5 63 | ^4PH@c
000000070: A1 F4 1C D9 7D EC DB CA | 00 00 00 00 00 00 00 00 | >>L}
000000080: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000090: 00 00 00 00 00 00 00 00 | F7 93 6C 85 3F 27 FD 3D | ?1?'=-
0000000A0: 5F 7E 9D 9A EE 92 1C BD | 00 10 00 00 00 00 00 00 | ~L ▶
0000000B0: 00 20 00 00 00 00 00 00 | 00 10 00 00 05 0F 03 01 | ▶ +o♥
0000000C0: 00 6F 5A 01 00 00 00 00 | 00 00 00 00 00 00 00 00 | oZ@
0000000D0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000000E0: 00 00 00 00 00 00 00 00 | 71 E8 63 60 64 7A 42 80 | qc`dzB
0000000F0: 98 31 CD 52 3B B7 40 5E | 31 71 CC 98 D1 BE CE 7B | >1R;@^1q_>D>{
000000100: C9 70 BB 08 CC 26 C7 D0 | 20 00 00 00 00 00 00 00 | >p&&
000000110: 02 00 00 00 40 00 00 00 | 00 00 00 00 10 00 00 00 | @ @ ▶
000000120: 00 00 00 00 00 00 00 00 | 10 00 00 00 00 00 00 00 | ▶
000000130: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000140: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000150: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000160: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000170: 00 00 00 00 00 00 00 00 | D0 BB B8 1E A4 38 F0 1D | л>▲8+
000000180: D6 72 92 A7 B5 4E 3D 66 | 00 00 00 00 00 00 00 00 | >rN=f
000000190: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001A0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001B0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001C0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001D0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001E0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001F0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000200: 00 00 00 00 00 00 00 00 | 35 F4 E2 5D 9B 37 F3 A7 | 5]7
000000210: EE CB 2C 83 31 2B 3D 8C | 45 AE B1 C1 F2 07 33 4B | >>,1+=E•K
000000220: CB 2A 37 14 2C 94 27 99 | BA 41 42 EE DC F9 C3 24 | >*7, 'AB$
000000230: 3F 7E 63 19 84 79 3C AB | 40 4C 36 FE 86 82 57 99 | ?~c↓y<@L6W
```

AES-XTS ?

script+keymaster

зашифрованный
RSA-ключ

Moto G4: подходы

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

Moto G4: подходы

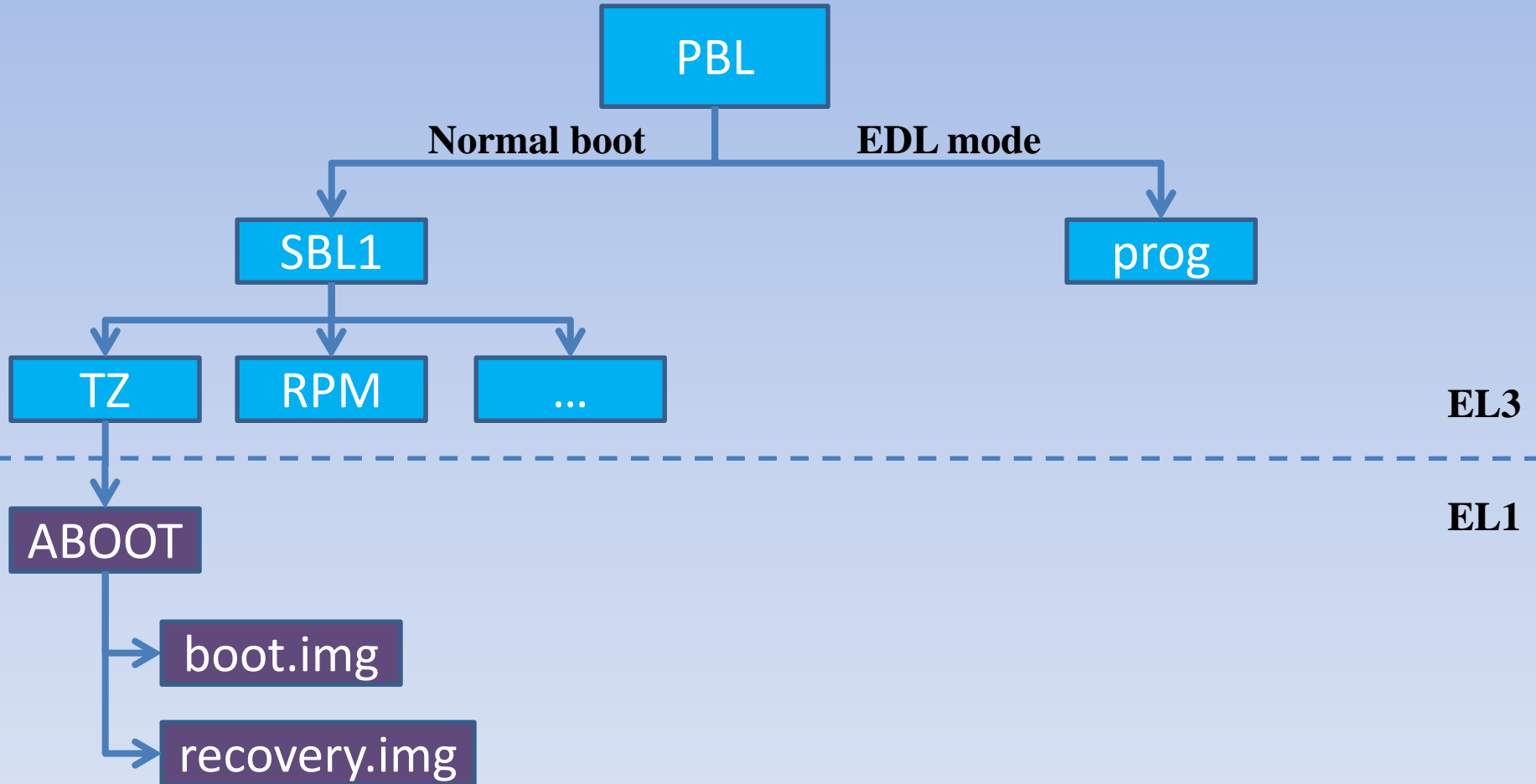
- ~~1. chip-off/ISP~~ – scrypt+keymaster
- ~~2. custom recovery (TWRP, ...)~~ – включен FRP
3. kernel cmdline injection (CVE-2016-10277) ?

Moto G4: подходы

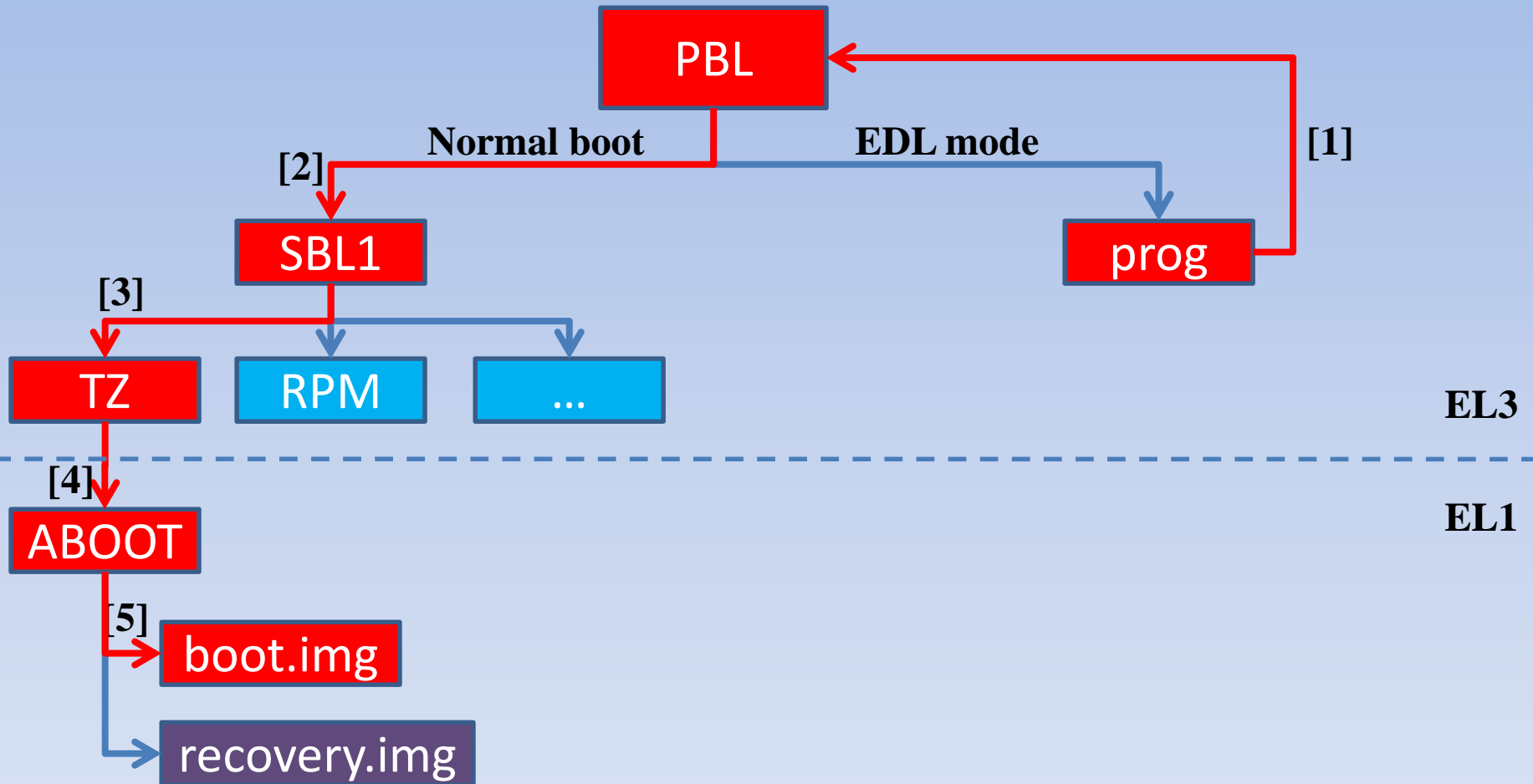
- ~~1. chip-off/ISP – scrypt+keymaster~~
- ~~2. custom recovery (TWRP, ...) – включен FRP~~
- ~~3. kernel cmdline injection (CVE-2016-10277) –
есть патч~~
4. EDL mode: peek/poke (QPSIIR-909)* ?

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

Описание QPSIIR-909 (1)



Описание QPSIR-909 (2)



Описание QPSIR-909 (3)

Необходимые условия:

1. Наличие **prog**-файла для данной модели
2. **prog**-файл выполняется с наивысшими привилегиями (**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 (QPSIR-909)* – команды
peek/poke недоступны~~
5. Уязвимость в PBL MSM8952** ?

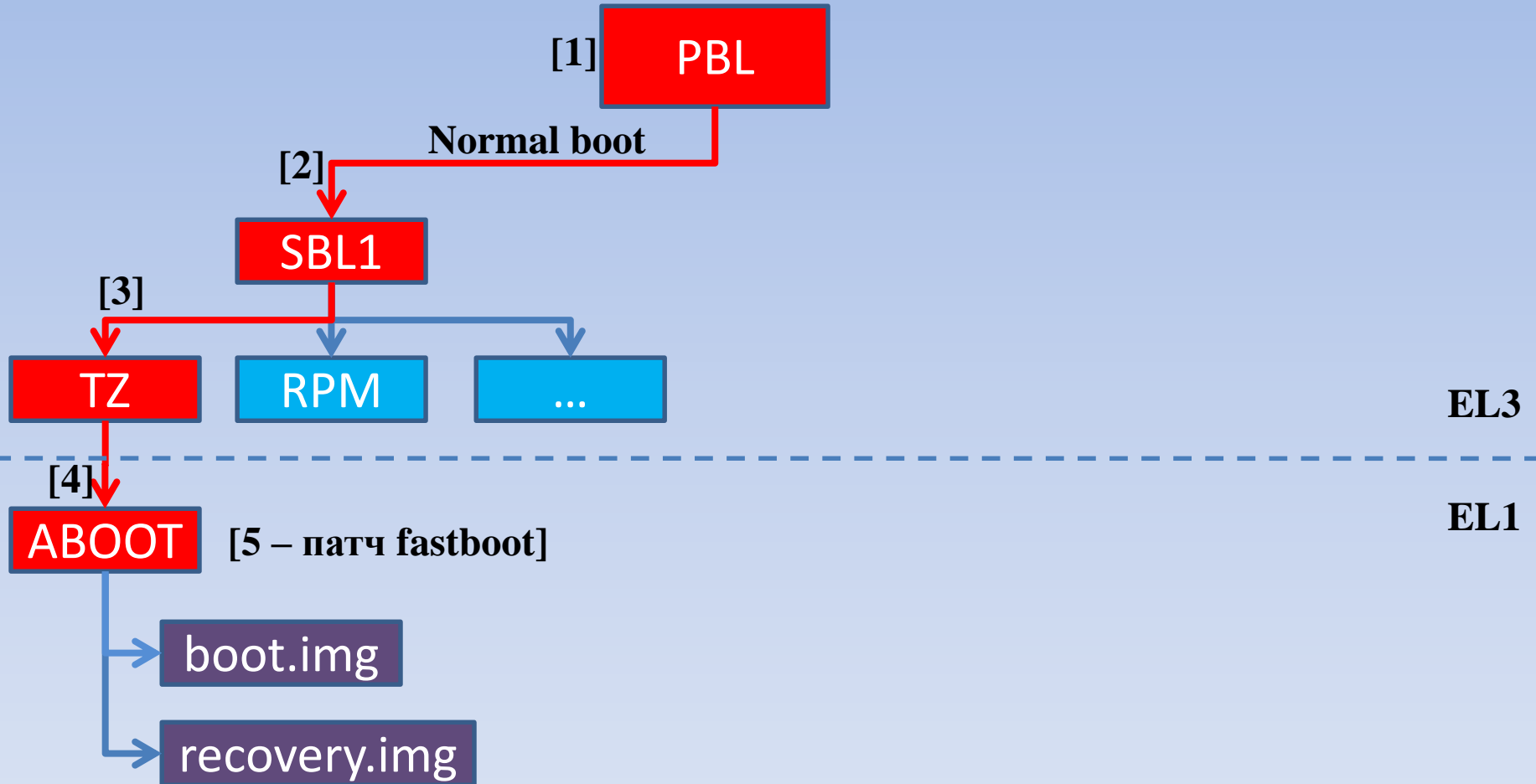
*<https://alephsecurity.com/vulns/aleph-2017028>

**<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)

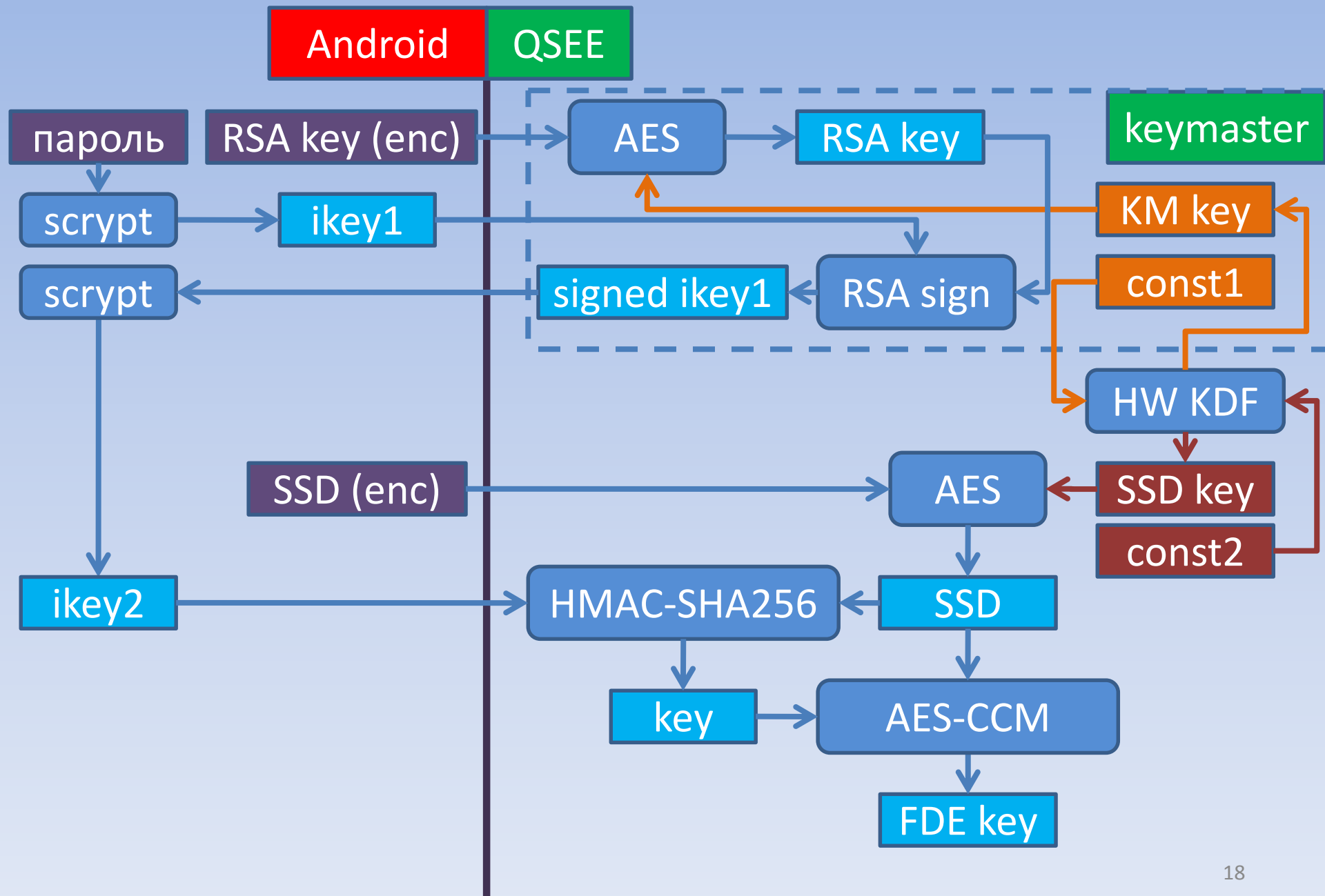
Необходимые условия:

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**



Moto G3: подходы

1. chip-off/ISP ?

Moto G3: crypto footer

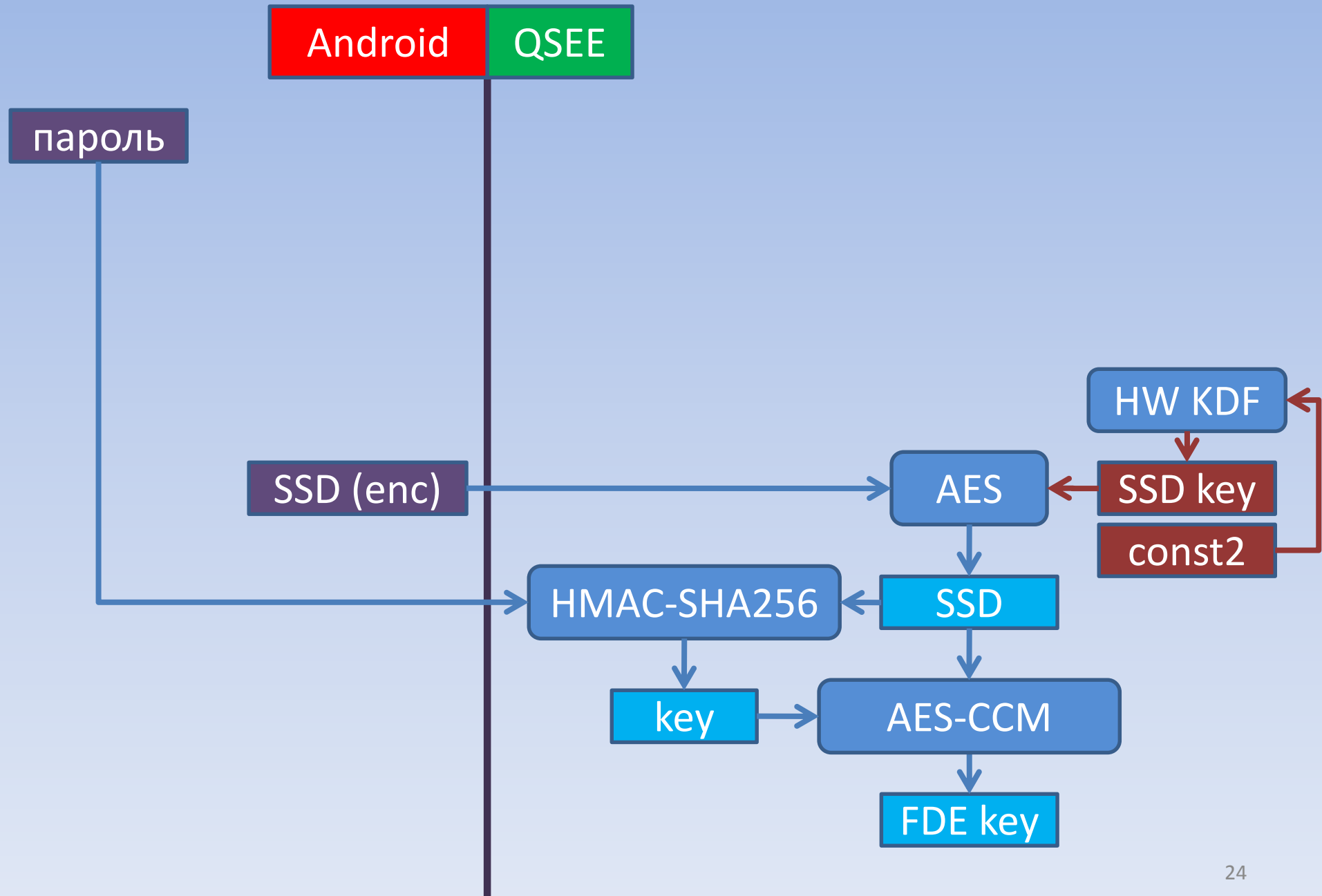
```
000000000: C4 B1 B5 D0 01 00 03 00 | 10 09 00 00 00 00 00 00 | i> 000 000 000
000000010: 10 00 00 00 03 00 00 00 | 00 7F 91 00 00 00 00 00 | 000 000 000
000000020: 00 00 00 00 61 65 73 2D | 78 74 73 00 00 00 00 00 | aes-xts
000000030: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000040: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000050: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000060: 00 00 00 00 00 00 00 00 | 3D CF D0 38 08 B4 E2 AD | =008 000
000000070: 23 37 98 E7 5F D4 48 B5 | 00 00 00 00 00 00 00 00 | #700_0H0
000000080: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000090: 00 00 00 00 00 00 00 00 | 7A FE 02 7F 3D 88 D7 B8 | z00=00>
0000000A0: 76 CD 36 34 E1 B9 56 49 | 00 10 00 00 00 00 00 00 | v0640EVI
0000000B0: 00 20 00 00 00 00 00 00 | 00 10 00 00 02 0F 03 01 | 000000
0000000C0: 00 7F 91 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | 000
0000000D0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000000E0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000000F0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000100: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000110: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000120: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000130: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000140: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000150: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000160: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000170: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000180: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000190: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001A0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001B0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001C0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001D0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001E0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
0000001F0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000200: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000210: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000220: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000230: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000240: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000250: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000260: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
000000270: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |
```

SCRIPT

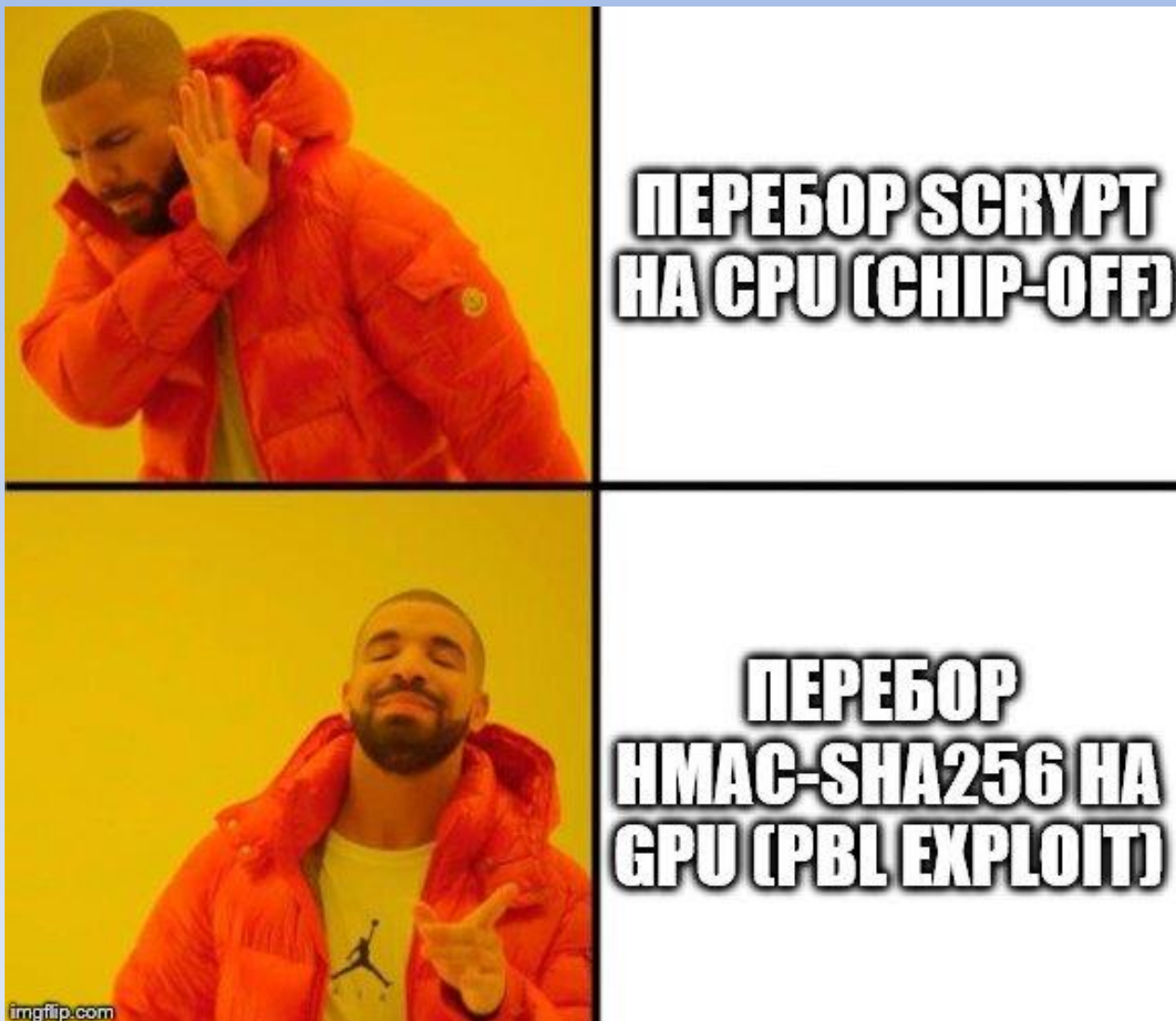
Moto G3: подходы

- ~~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 (QPSIR-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**

Samsung J5 (2016): подходы

1. chip-off/ISP ?

Samsung J5 (2016): footer (1)

```
000000000: C5 B1 B5 D0 01 00 03 00 90 09 00 00 00 00 00 00  ũ>  ♡  ♪o
000000010: 20 00 00 00 02 00 00 00  B8 BF 69 01 00 00 00 00  ♀  ♪i@
000000020: 00 00 00 00 61 65 73 2D 63 62 63 2D 65 73 73 69  aes-cbc-essi  AES-CBC
000000030: 76 3A 73 68 61 32 35 36 00 00 00 00 00 00 00 00  v:sha256
000000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000120: 00 00 00 00 00 00 00 00 00 80 7F D3 02 00 00 00  ♪i@
000000130: 00 90 7F D3 02 00 00 00 00 0C 00 00 02 0F 03 01  ♪i@  ♀  ♪i@  ♪i@  SCRYPT?
000000140: B8 BF 69 01 00 00 00 00 00 00 00 00 00 00 00 00  >>i@
000000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000230: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Samsung J5 (2016): footer (2)

0000003200: 00 00 00 01 0C 00 00 00	11 10 00 00 00 00 30 00	0♀ ← 0
0000003210: 0E 00 44 06 4A 00 04 00	4A 08 10 00 4E 08 20 00	♫ D♯ J N
0000003220: 5E 08 10 00 9E 08 10 00	AE 08 04 00 BE 08 10 00	^ ▢ ▢ ▢ ▢ ▢
0000003230: C2 08 20 00 D2 08 10 00	12 09 10 00 22 09 00 00	> ▢ ▢ ▢ ▢ ▢ ▢
0000003240: 00 00 00 00 00 00 00 00	00 00 42 4B 4D 4B 00 00	▢ ▢ ▢ ▢ ▢ ▢ ▢ ▢
0000003250: 00 00 B8 03 39 3D 8E 40	9B 4B 58 74 86 E2 70 9E	ВКМК
0000003260: 84 BD E4 9F 7A F0 58 41	DD 13 CF ED 65 AA B1 77	♥9=KXtP
0000003270: 14 94 47 EF C8 90 B0 19	C8 E3 11 4A 3A 92 D9 B2	>>>> zXA!!eW
0000003280: DB 80 CE 12 21 F3 2F 76	C0 D9 2C B9 91 FD B4 F3	GGR>↓-J: >
0000003290: 4A EC E0 11 7E 66 96 EE	2B EC 91 CE 5F 64 CB 73	>▢! ▢/v▢, ▢▢▢▢
00000032A0: 8E 4E B2 93 B3 CD 06 E8	7E 35 7E 14 57 2B 6B 56	J▢~f▢+▢▢_d▢s
00000032B0: D6 D7 FE A3 8E A6 96 AA	88 DC 43 5C 13 83 50 F1	>N▢▢▢▢~5~JW+kV
00000032C0: 54 9A E7 4C 68 22 44 86	26 04 D1 0E A1 22 97 D7	>>>>>>>>>C\!!P▢
00000032D0: 2A C2 D3 AD FA EC 22 A9	52 04 FC E2 35 3F 44 F0	T▢Lh"D▢&▢▢"▢▢
00000032E0: DA D4 8B B6 2A 98 D3 E8	2B 14 72 18 F2 B7 B5 06	*▢▢>▢▢"▢R▢▢5?D▢
00000032F0: 88 3D 6D E9 D1 49 2E 82	B1 EB 6D A6 37 8F D2 A0	>▢>▢*▢▢+▢r↑▢▢▢▢
0000003300: FE 19 C4 88 26 89 9D 84	ED A6 33 D7 93 58 DD 93	>=m▢▢I . ▢▢m▢7▢K>
0000003310: 0A 29 F0 0E BA 0A 64 3E	2D F4 7A 10 F7 AA 47 74	>↓Ĉ>&▢▢▢▢3▢>X▢>
0000003320: 77 A6 EE B7 3D 52 81 31	9D F2 82 F9 9F E3 FF 84	▢)▢▢▢▢ed>-▢z▢-▢▢Gt
0000003330: E0 9C 6D CD 55 5E DC C2	00 00 00 00 00 00 00 00	w▢▢▢=R▢1▢▢▢▢▢▢▢▢
0000003340: EC 69 D6 51 AF A1 99 0B	00 00 00 00 00 00 00 00	>>m▢U^▢▢>+'Z▢>>A
0000003350: A5 0D 00 00 00 00 00 00	00 00 00 00 00 00 00 00	>i▢Q▢▢▢▢▢B\k▢g▢>
0000003360: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	>▢
0000003370: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003380: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003390: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000033A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000033B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000033C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000033D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000033E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000033F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003400: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003410: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003420: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003430: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003440: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003450: 00 00 00 01 00 00 00 00	00 00 00 01 00 01 00 00	© © ©
0000003460: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000003470: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

зашифрованный RSA-ключ

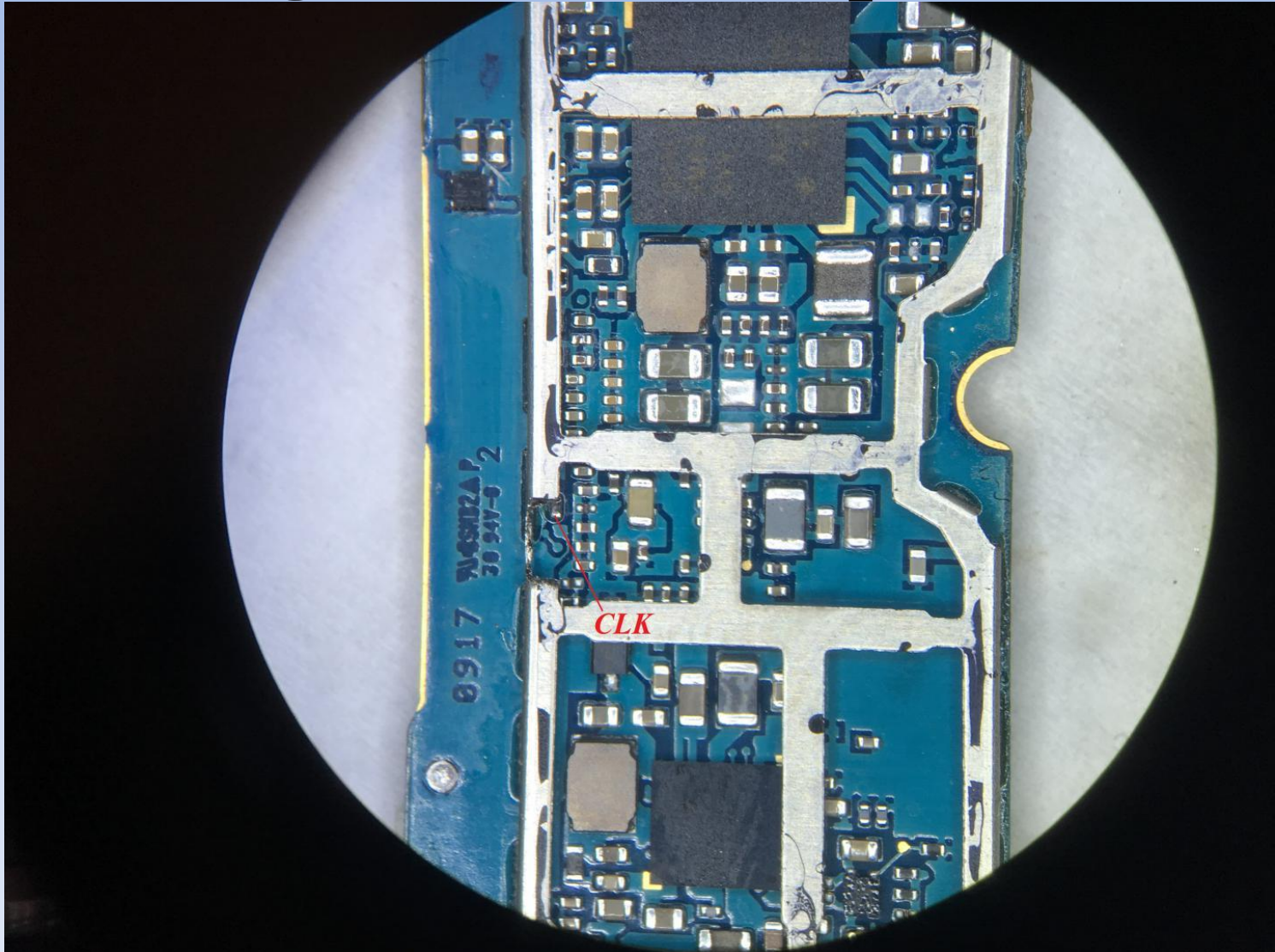
Samsung J5 (2016): подходы

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

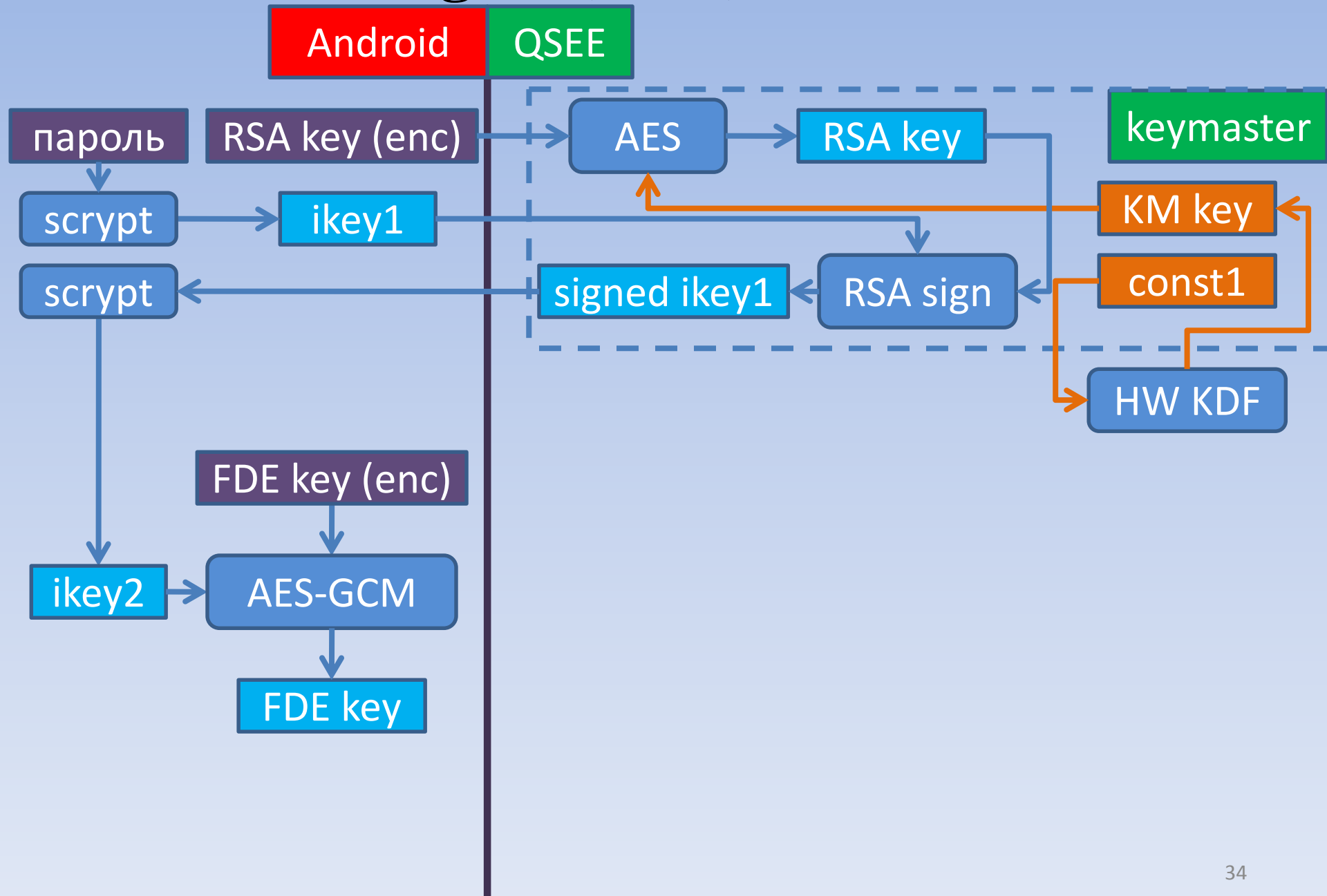
Samsung J5 (2016): подходы

- ~~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 (QPSIR-909) – нет прог-файла~~
5. Уязвимость в PBL MSM8916

Samsung J5 (2016): перевод в EDL



Samsung J5 (2016): cxema FDE



Samsung J510F: итоги

1. Возможна компрометация **Secure Boot** через уязвимость в **PBL (MSM8952)**
2. Перебор **offline** возможен путём извлечения ключа **КМ 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!