Supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

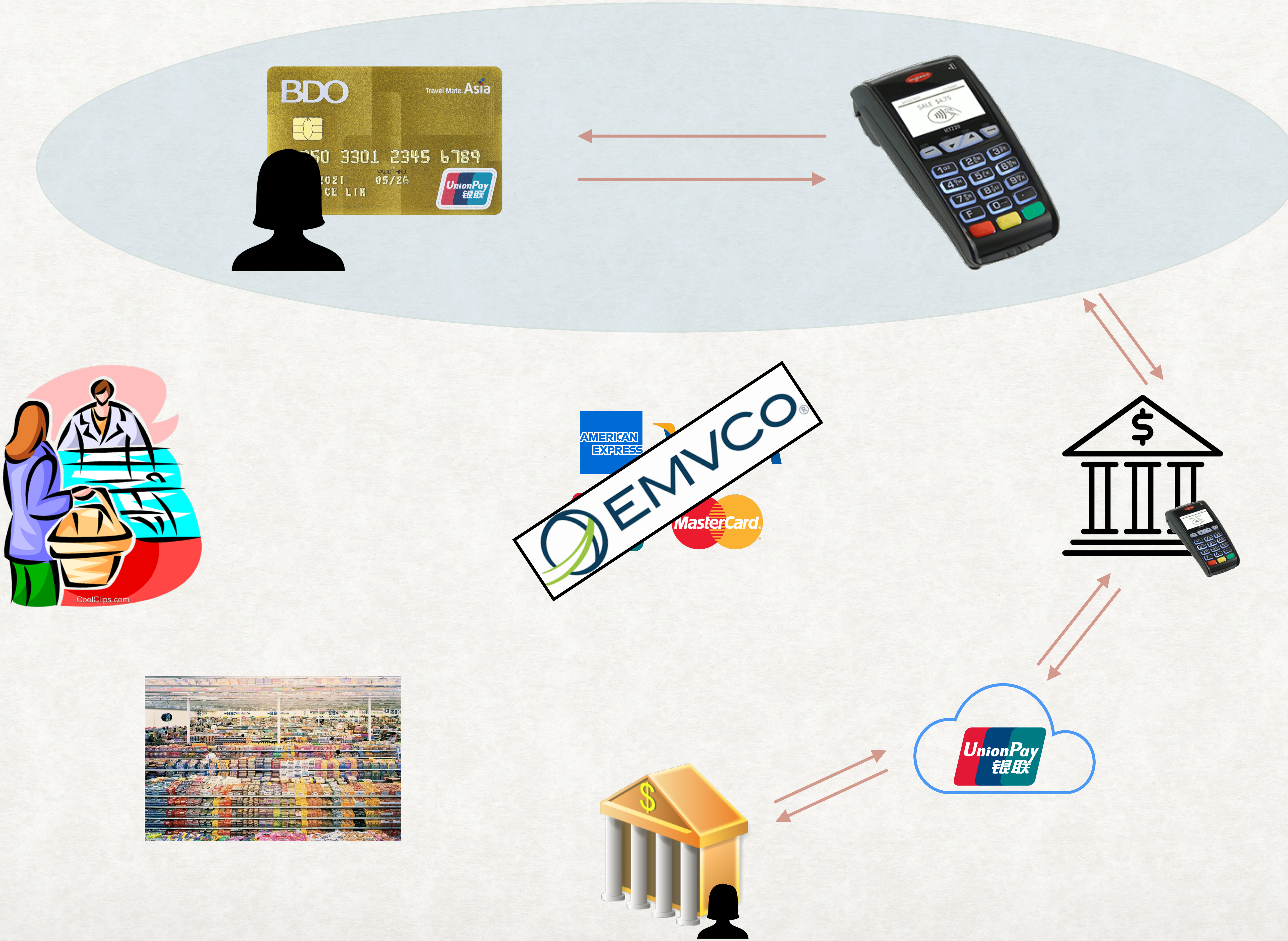
Unlinkability of an Improved Key Agreement protocol for EMV 2nd Gen Payments

Ross Horne Sjouke Mauw Semyon Yurkov

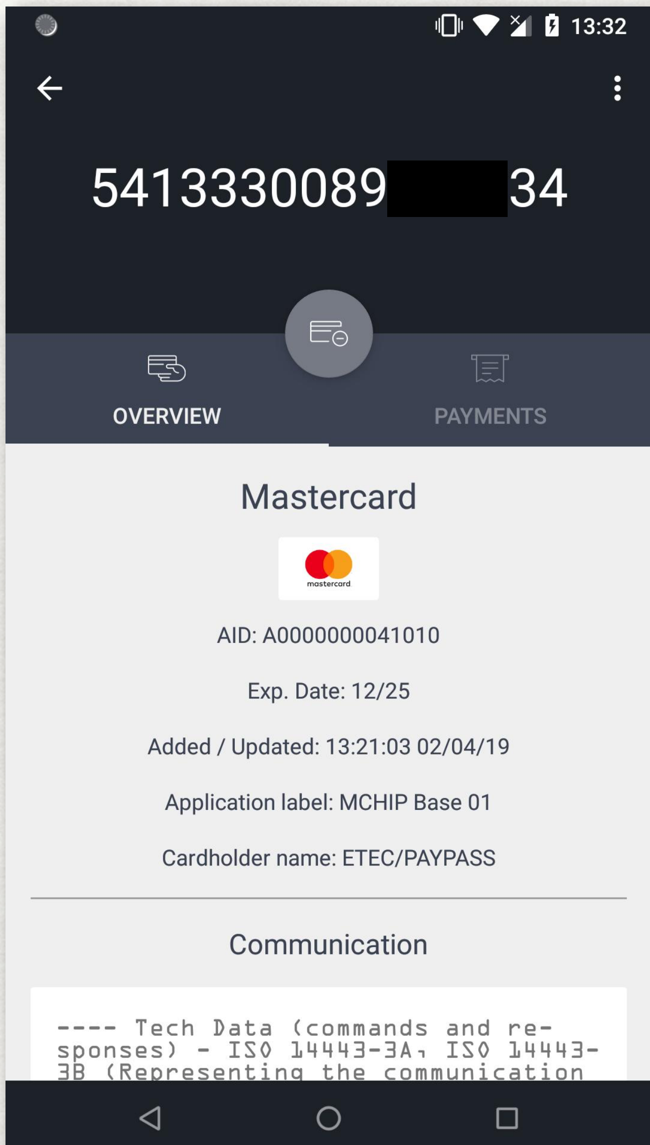
10.08.2022 Haifa, Israel

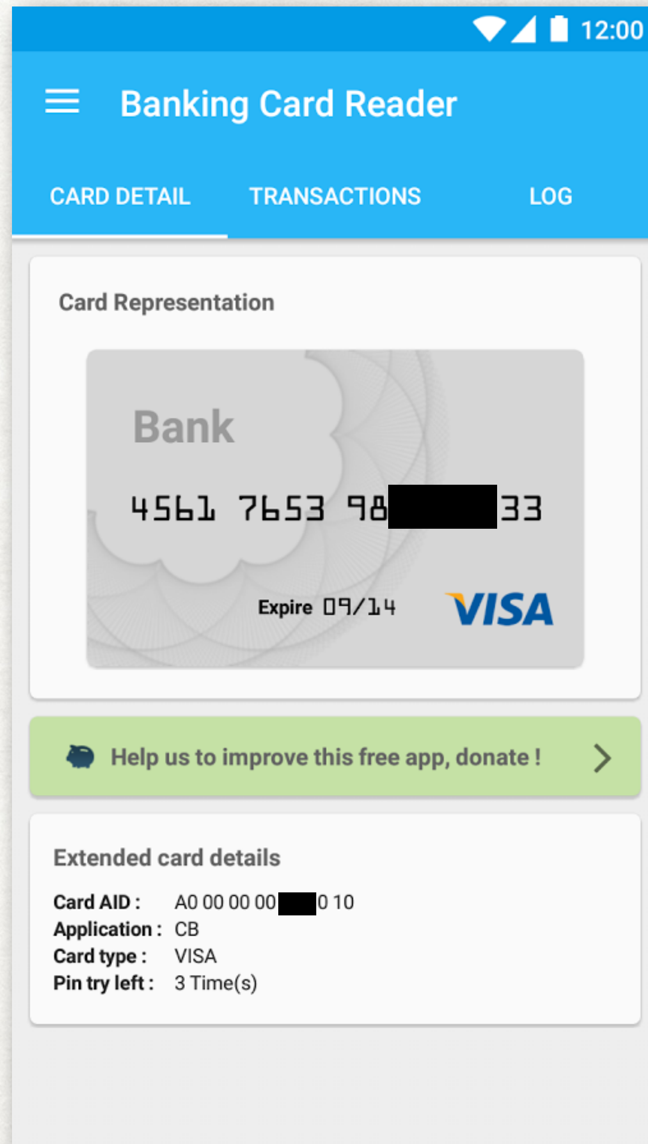
35th IEEE Computer Security Foundations Symposium (CSF)

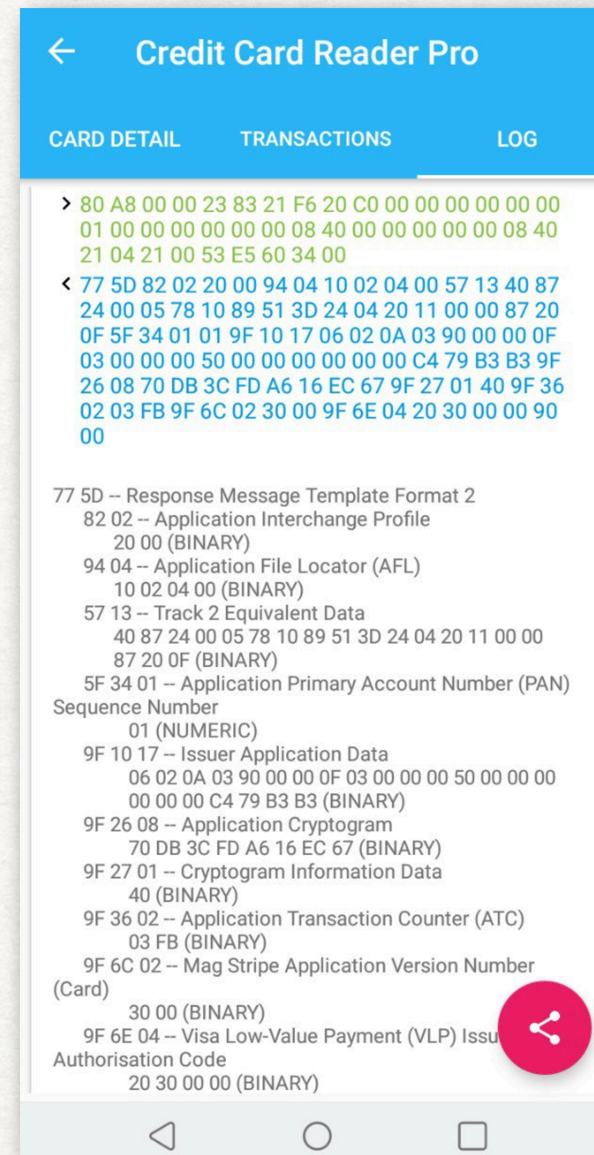
WHAT IS EMV?


BDO
Travel Mate. Asia
3301 2345 6789
05/26
UnionPay 银联
AMERICAN EXPRESS
EMVCO
MasterCard
CoolClips.com
UnionPay 银联

THERE IS NO PRIVACY IN EMV



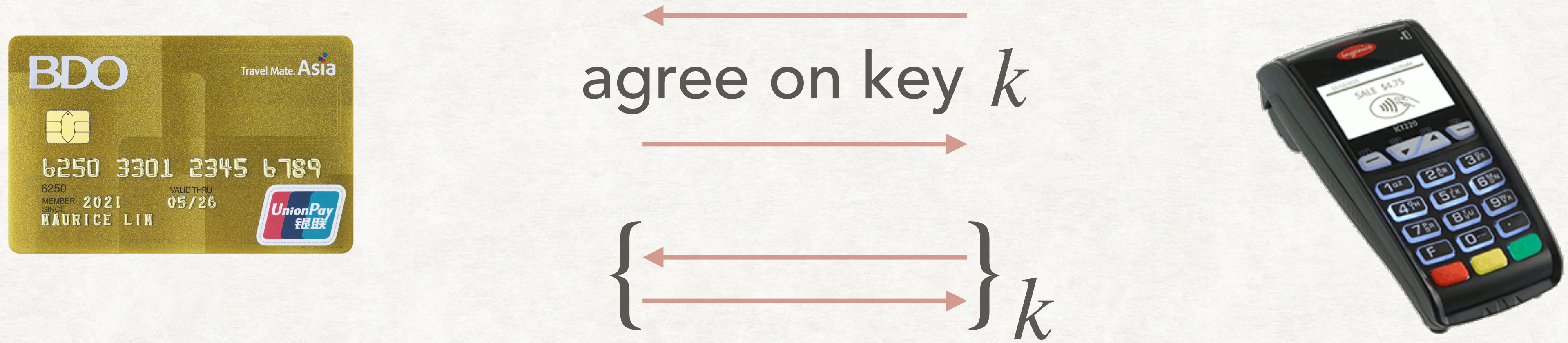




Unwanted data collection in contactless payments is straightforward.

10.08.2022

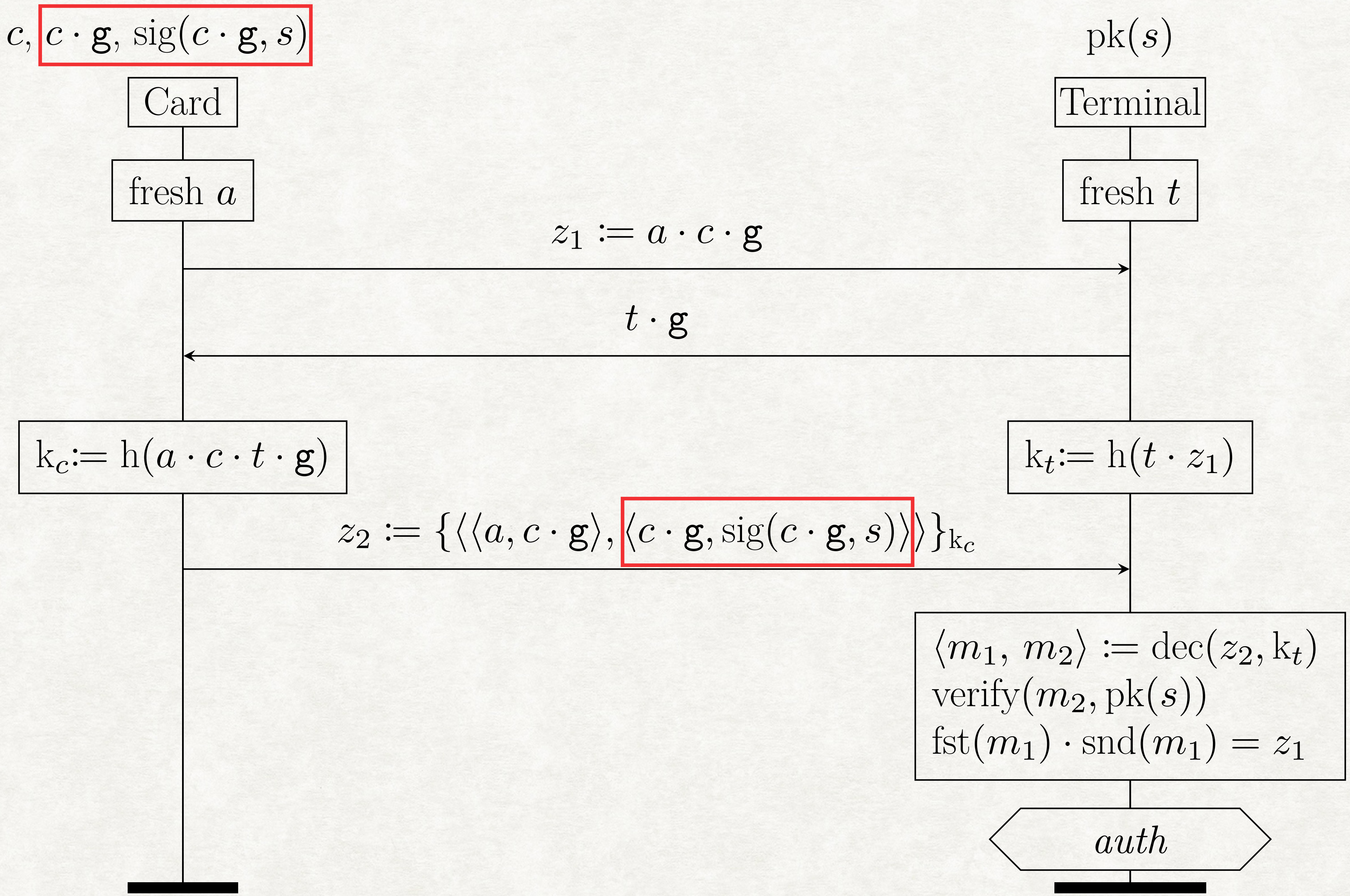
EMVCO PROPOSAL: KEY ESTABLISHMENT



2012: “Blinded Diffie-Hellman RFC”, EMVCo LLC

- provide authentication of the card by the terminal
- protect against eavesdropping and card tracking.

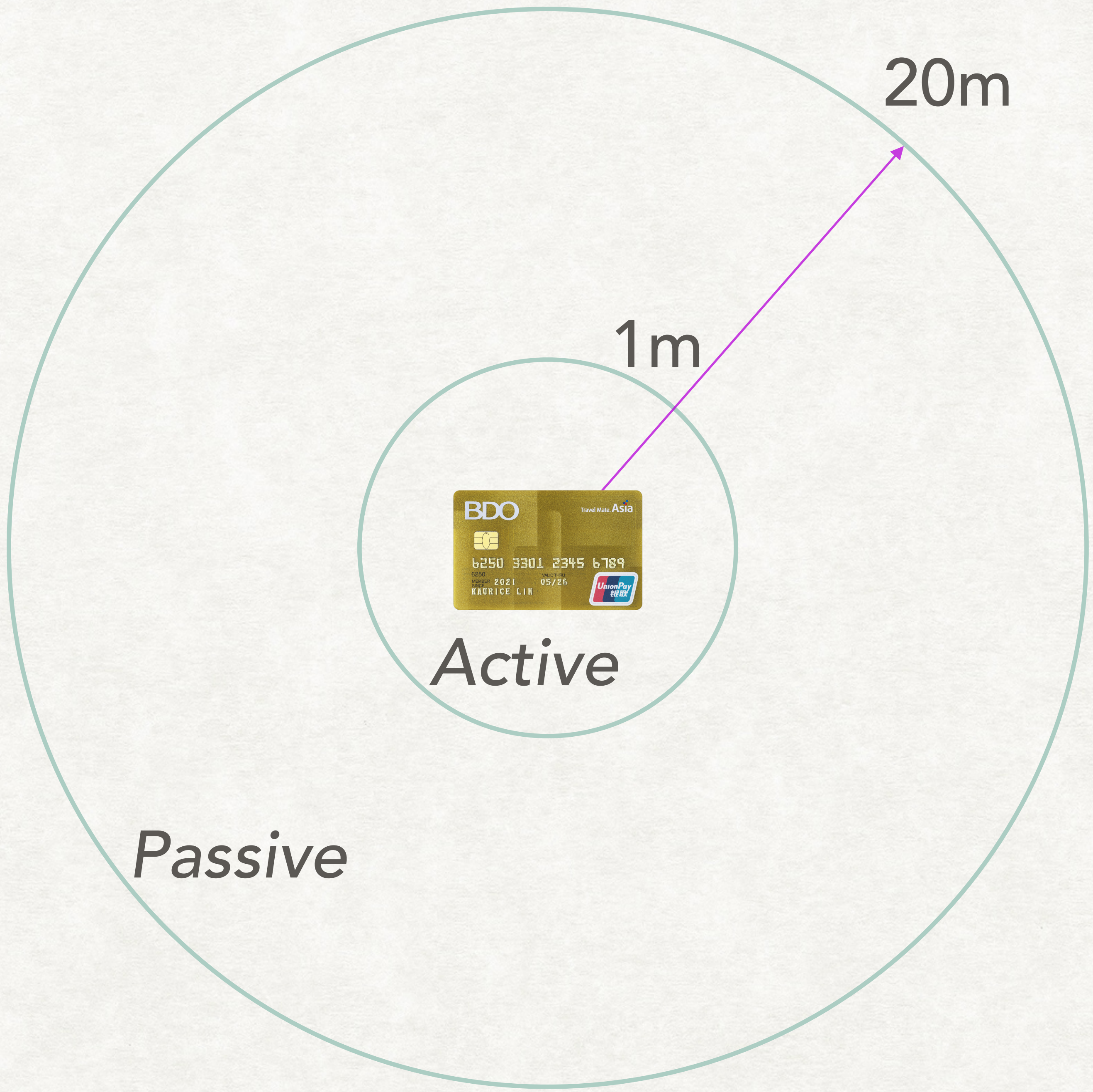
BLINDED DIFFIE-HELLMAN (BDH)



g the generator of the DH group, s PaySys signing key, $\mathrm{pk}(s)$ PaySys verification key

c card's secret key, $c \cdot \mathsf{g}$ card's public key, $\mathrm{sig}(c \cdot \mathsf{g}, s)$ signature on the card's public key

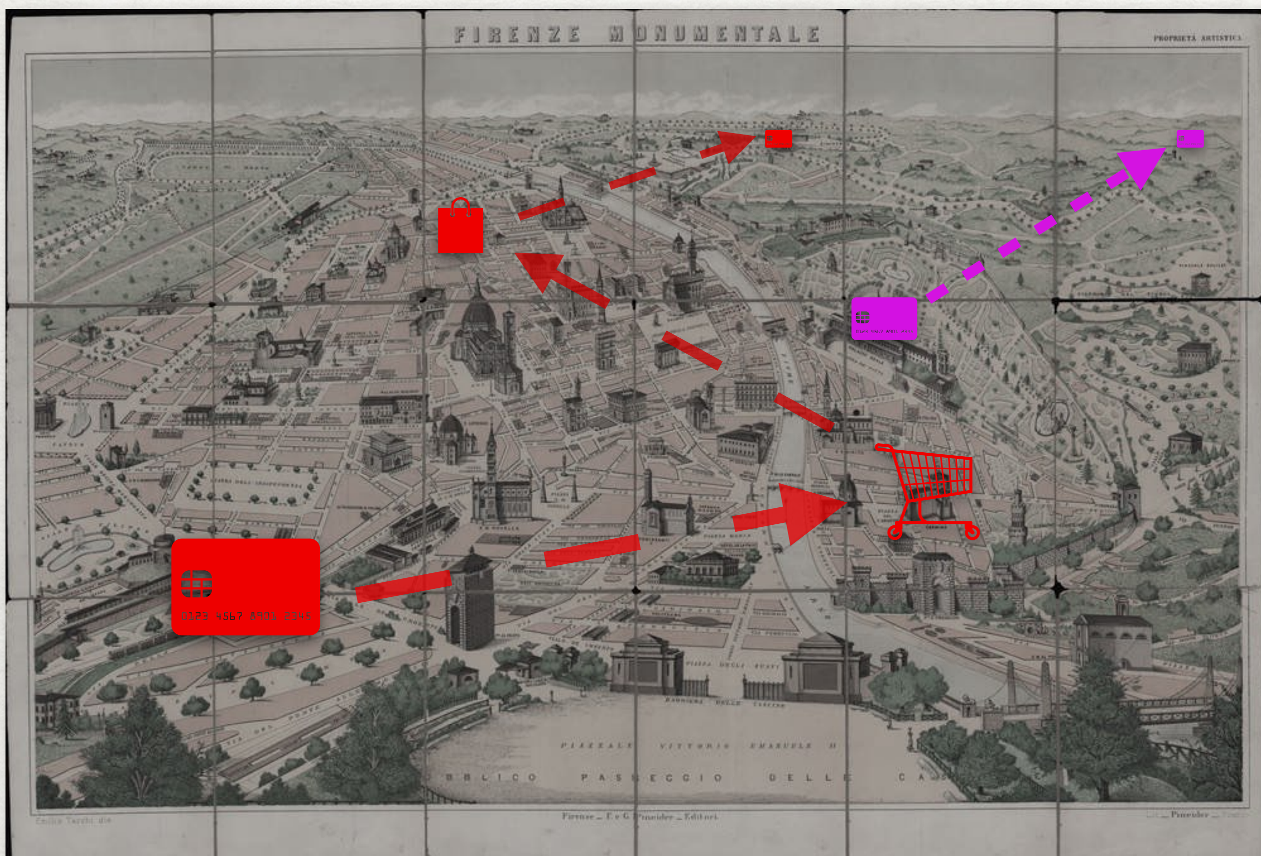
EAVESDROPPER → ACTIVE ATTACKER



1. An active attacker powers up the card
2. Establishes a symmetric key with the card
3. Obtains the long-term identities $\boxed{c \cdot \mathfrak{g},\ \mathsf{sig}(c \cdot \mathfrak{g}, s)}$

PASSIVE ATTACKER

Without BDH: no privacy



With BDH: privacy

(CLOSE) ACTIVE ATTACKER

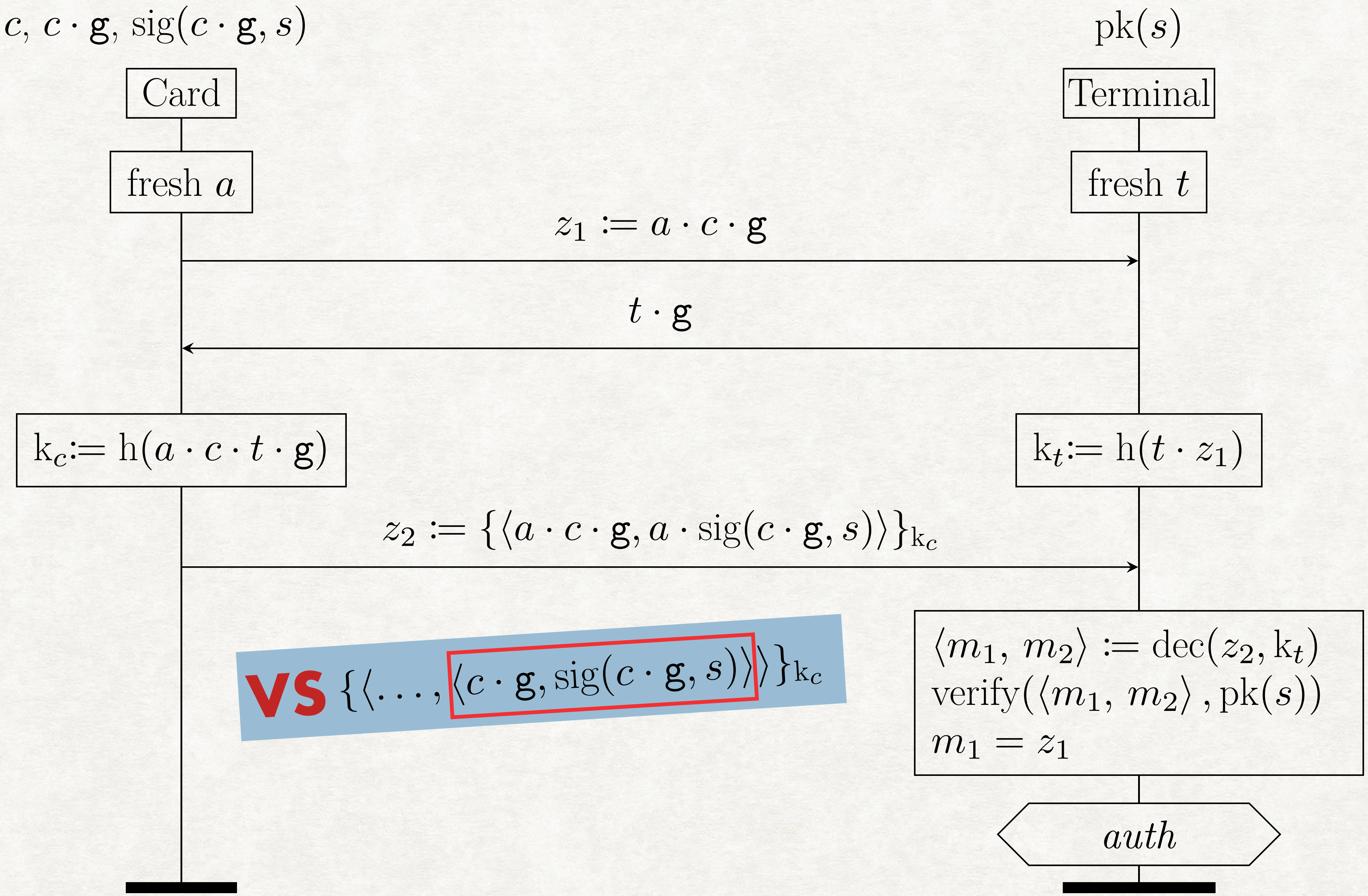
Without BDH: no privacy

With BDH: no privacy

NO DIFFERENCE!

UNLINKABLE BLINDED DIFFIE-HELLMAN (UBDH)

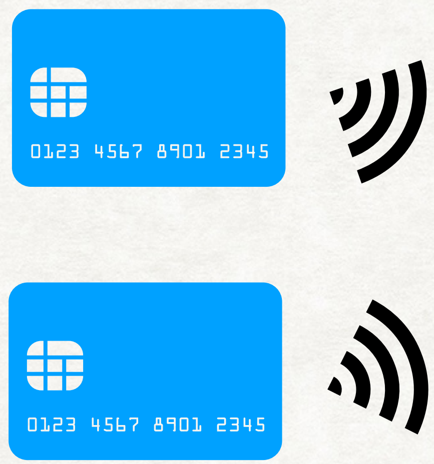
Verheul condition: $a \cdot \mathrm{sig}(M, s) =_E \mathrm{sig}(a \cdot M, s)$



g the generator of the DH group, s PaySys signing key, $\mathrm{pk}(s)$ PaySys verification key

c card's secret key, $c \cdot \mathrm{g}$ card's public key, $\mathrm{sig}(c \cdot \mathrm{g}, s)$ signature on the card's public key

UNLINKABILITY

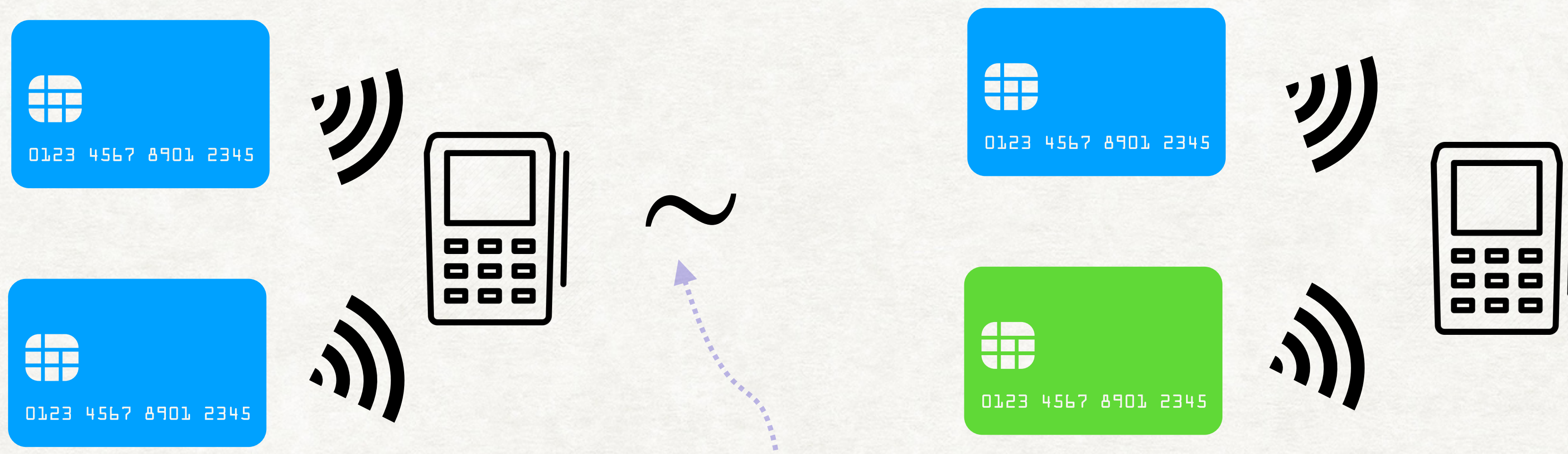


$\sim$

QUASI-OPEN BISIMILARITY

$$
\begin{aligned}
\mathit{Small\_Impl} \triangleq\ & \nu s. \\
& \overline{out}\langle \mathrm{pk}(s) \rangle. \\
& !\nu c. \\
& !\nu ch_c.\overline{card}\langle ch_c \rangle.C(s, ch_c, c)
\end{aligned}
\qquad \sim \qquad
\begin{aligned}
\mathit{Small\_Spec} \triangleq\ & \nu s. \\
& \overline{out}\langle \mathrm{pk}(s) \rangle. \\
& !\nu c. \\
& \nu ch_c.\overline{card}\langle ch_c \rangle.C(s, ch_c, c)
\end{aligned}
$$

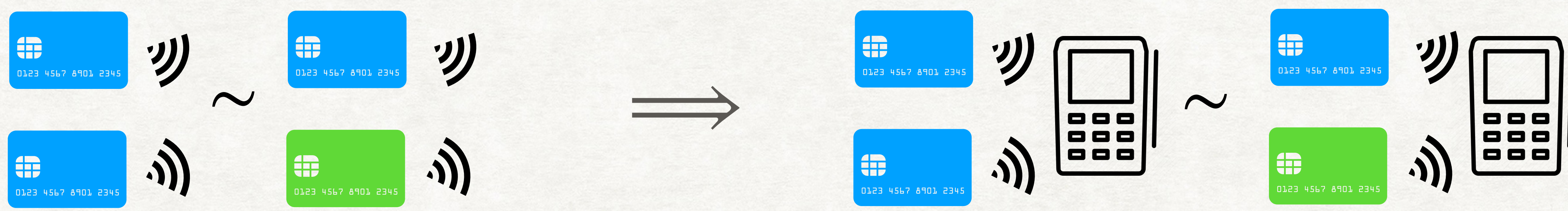
UNLINKABILITY



QUASI-OPEN BISIMILARITY

$$
\begin{aligned}
\mathit{Impl} \triangleq\ & \nu s. \\
& \big(!\nu c. \\
& !\nu ch_c.\overline{\mathit{card}}\langle ch_c\rangle.C(s, ch_c, c) \ \mid \\
& \overline{\mathit{out}}\langle \mathrm{pk}(s)\rangle. \\
& !\nu ch_t.\overline{\mathit{term}}\langle ch_t\rangle.T(s, ch_t) \ \big)
\end{aligned}
\quad \sim \quad
\begin{aligned}
\mathit{Spec} \triangleq\ & \nu s. \\
& \big(!\nu c. \\
& \nu ch_c.\overline{\mathit{card}}\langle ch_c\rangle.C(s, ch_c, c) \ \mid \\
& \overline{\mathit{out}}\langle \mathrm{pk}(s)\rangle. \\
& !\nu ch_t.\overline{\mathit{term}}\langle ch_t\rangle.T(s, ch_t) \ \big)
\end{aligned}
$$

RESULTS: CONGRUENCE ENABLES COMPOSITIONAL REASONING



Theorem 1: If *Small_Impl* ~ *Small_Spec*, then *Impl* ~ *Spec*.

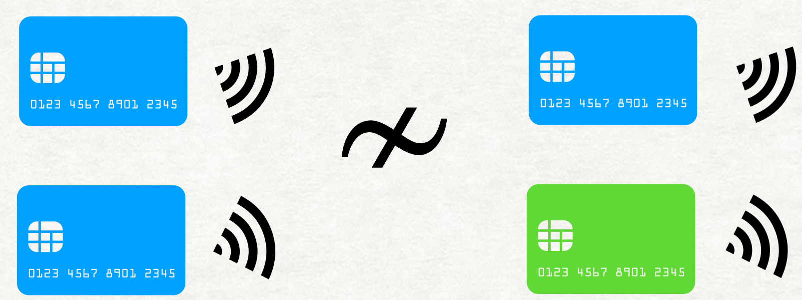
Proof.

- ~ is a congruence, hence is preserved by any context

- the context: $\nu out.\Big(\{\cdot\} \,|\, out(pk_s).\overline{out'}\langle pk_s\rangle ! \nu ch_t.\langle ch_t\rangle.T(pk_s, ch_t)\Big)$

■

RESULTS: BDH PROTOCOL IS NOT UNLINKABLE



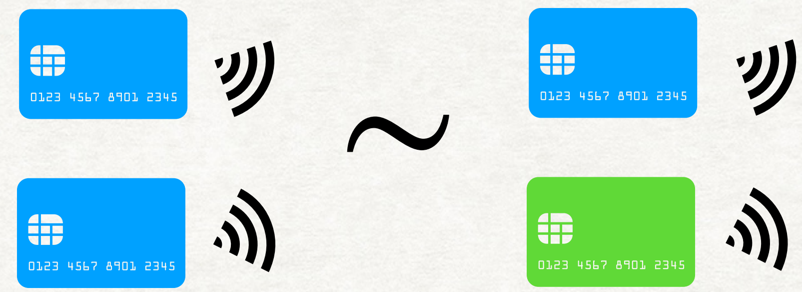
Theorem 2: *Small_Impl* $\not\sim$ *Small_Spec* for BDH.

Proof.

$$\textit{Small\_Impl} \models \begin{array}{l} \langle \overline{out}(pk_s) \rangle \\ \langle \overline{card}(u_1) \rangle \langle \overline{u_1}(v_1) \rangle \langle u_1\, y_1 \cdot \mathrm{g} \rangle \langle \overline{u_1}(w_1) \rangle \\ \langle \overline{card}(u_2) \rangle \langle \overline{u_2}(v_2) \rangle \langle u_2\, y_2 \cdot \mathrm{g} \rangle \langle \overline{u_2}(w_2) \rangle \\ \left(\mathrm{snd}(\mathrm{dec}(\mathrm{h}(y_1 \cdot v_1), w_1)) = \mathrm{snd}(\mathrm{dec}(\mathrm{h}(y_2 \cdot v_2), w_2)) \right) \end{array} \not\models \textit{Small\_Spec}$$

$\blacksquare$

RESULTS: UBDH PROTOCOL IS UNLINKABLE



Theorem 3: *Small_Impl* ~ *Small_Spec* for UBDH.

Proof.

- Define a relation (hard)
- Verify it is quasi-open bisimulation (not hard)

$$UPD_{\text{spec}} \ \mathfrak{R} \ UPD_{\text{impl}}$$

$$UPD^{\Psi}_{\text{spec}}(\vec{Y}) \triangleq \nu s, c_1, \cdots, c_L, ch_1, \cdots, ch_L, a_{l_1}, \cdots, a_{l_K}.(\sigma \mid C_1 \mid \cdots \mid C_L \mid !\nu c.\nu ch.\overline{card}\langle ch\rangle.C_{\text{upd}}(s, c, ch))$$

$$\mathfrak{R}$$

$$UPD^{\Psi,\Omega}_{\text{impl}}(\vec{Y}) \triangleq \nu s, c_1, \cdots, c_D, ch_1, \cdots, ch_L, a_{l_1}, \cdots, a_{l_K}.(\theta \mid \cdots \mid C^d_l \mid \cdots \mid !\nu ch.\overline{card}\langle ch\rangle.C_{\text{upd}}(s, c_d, ch) \mid !\nu c.!\nu ch.\overline{card}\langle ch\rangle.C_{\text{upd}}((s, ch, c)))$$

$$C_l = \begin{cases} \mathcal{E}^l(ch_l) & \text{if } l \in \alpha \\ \mathcal{F}^l(ch_l, a_l) & \text{if } l \in \beta \\ \mathcal{G}^l(ch_l, a_l, Y_l\sigma) & \text{if } l \in \gamma \\ \mathcal{H}^l & \text{if } l \in \delta \end{cases}$$

$$C^d_l = \begin{cases} \mathcal{E}^d(ch_l) & \text{if } l \in \zeta^d \cap \alpha \\ \mathcal{F}^d(ch_l, a_l) & \text{if } l \in \zeta^d \cap \beta \\ \mathcal{G}^d(ch_l, a_l, Y_l\theta) & \text{if } l \in \zeta^d \cap \gamma \\ \mathcal{H}^d & \text{if } l \in \zeta^d \cap \delta \end{cases}$$

$$\begin{array}{ll} pk_s\sigma = \mathtt{pk}(s) & \\ u_l\sigma = ch_l & \text{if } l \in \{1, \cdots, L\} \\ v_l\sigma = \phi(a_l, \phi(c_l, \mathrm{g})) & \text{if } l \in \beta \cup \gamma \cup \delta \\ w_l\sigma = m^l(a_l, Y_l\sigma) & \text{if } l \in \delta \end{array}$$

$$\begin{array}{ll} pk_s\theta = \mathtt{pk}(s) & \\ u_l\theta = ch_l & \text{if } l \in \{1, \cdots, L\} \\ v_l\theta = \phi(a_l, \phi(c_d, \mathrm{g})) & \text{if } l \in \zeta^d \cap (\beta \cup \gamma \cup \delta) \\ w_l\theta = m^d(a_l, Y_l\theta) & \text{if } l \in \zeta^d \cap \delta \end{array}$$

$$\Psi := \{\alpha, \beta, \gamma, \delta\}, \ \ \Omega := \{\zeta^1, \cdots, \zeta^D\} \text{ are partitions of } \{1, \cdots, L\}$$

$$K := |\beta \cup \gamma \cup \delta| \qquad l_1, \cdots, l_K \in \beta \cup \gamma \cup \delta$$

$$pk_s, u_l, v_l, w_l \ \# \ \{card, s\} \cup \{c_l, ch_l, a_l | l \in \{1, \cdots, L\}\}$$

$$Y_l \ \# \ \{s\} \cup \{c_l, ch_l, a_l | l \in \{1, \cdots, L\}\}$$

$$\mathrm{fv}(Y_l) \cap (\{v_i | i \in \alpha\} \cup \{w_i | i \in \alpha \cup \beta \cup \gamma \cup \{l\}\}) = \varnothing$$

$\blacksquare$

CONCLUSIONS

D. **Unlinkable** authenticated EMV **key establishment** in the presence of active attackers **is feasible**.

Quasi-open bisimilarity allows

A. To express **attacks** on privacy properties using **intuitionistic modal logic formulas**.

B. To prove that a privacy property holds by providing a **proof certificate** that is easy to check.

C. To reason about protocols **compositionally** by considering a **subsystem**, hence reducing the amount of work.

Thank you!

PICS SRC

https://d7hftxdivxxvm.cloudfront.net/?resize_to=fit&width=800&height=514&quality=80&src=https%3A%2F%2Fd32dm0rphc51dk.cloudfront.net%2FNoNyvpkQQ4Es0vm8qaBE7Q%2Fnormalized.jpg
https://www.list.lu/fileadmin/_processed_/a/b/csm_photos-MI-LIST-August2016-by-LugdivineUnfer_f735b483a2.jpg
https://www.bdo.com.ph/sites/default/files/images/BDO-Gold-UnionPay.png
https://icon2.cleanpng.com/20180423/jow/kisspng-emv-ingenico-pin-pad-contactless-payment-point-of-card-terminal-5ade27d8640d49.7372528315245086324098.jpg
https://upload.wikimedia.org/wikipedia/commons/thumb/1/1b/UnionPay_logo.svg/2560px-UnionPay_logo.svg.png
https://upload.wikimedia.org/wikipedia/commons/thumb/5/5e/Visa_Inc._logo.svg/1200px-Visa_Inc._logo.svg.png
https://upload.wikimedia.org/wikipedia/commons/thumb/b/b7/MasterCard_Logo.svg/2560px-MasterCard_Logo.svg.png
https://upload.wikimedia.org/wikipedia/commons/thumb/f/fa/American_Express_logo_%282018%29.svg/2052px-American_Express_logo_%282018%29.svg.png
https://www.emvco.com/wp-content/themes/emvco/images/EMVCo_logo.svg
https://cdn6.aptoide.com/imgs/6/8/d/68d45837115bf97a7be7868d3a734542_screen.png
https://pngimage.net/wp-content/uploads/2018/05/balconista-png-1.png
https://murdoch.is/papers/oakland10chipbroken-poster.pdf
https://static.thenounproject.com/png/2326744-200.png
https://www.geographicus.com/mm5/graphics/00000001/L/FirenzeMonumentale-tarchi-1900.jpg
https://poynting.tech/wp-content/uploads/product-images/lpda-92/A-LPDA-0092-4G-LTE-Back-View.png
http://vasya-lozhkin.ru/upload/iblock/111/1112d0899d362bce1c06652cdbdac690.jpg
https://img1.pnghut.com/10/19/6/4x9hbeRs2L/human-tooth-smile-free-content-lip.jpg
https://image.invaluable.com/housePhotos/tiroche/12/711412/H2594-L270162659_original.jpg