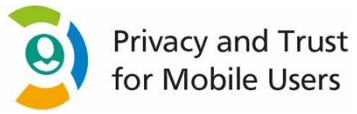
To Trust, or Not to Trust: Results from Analyzing and Refining Bluetooth Secure Connections

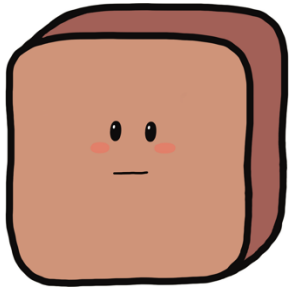
Olga Sanina

Cryptographic Applications Workshop

May the Force, 2025

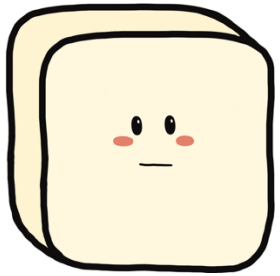


Disclaimer



Based on the joint work with Marc Fischlin.

Opinions are my own.



The presentation serves for educational purposes only.

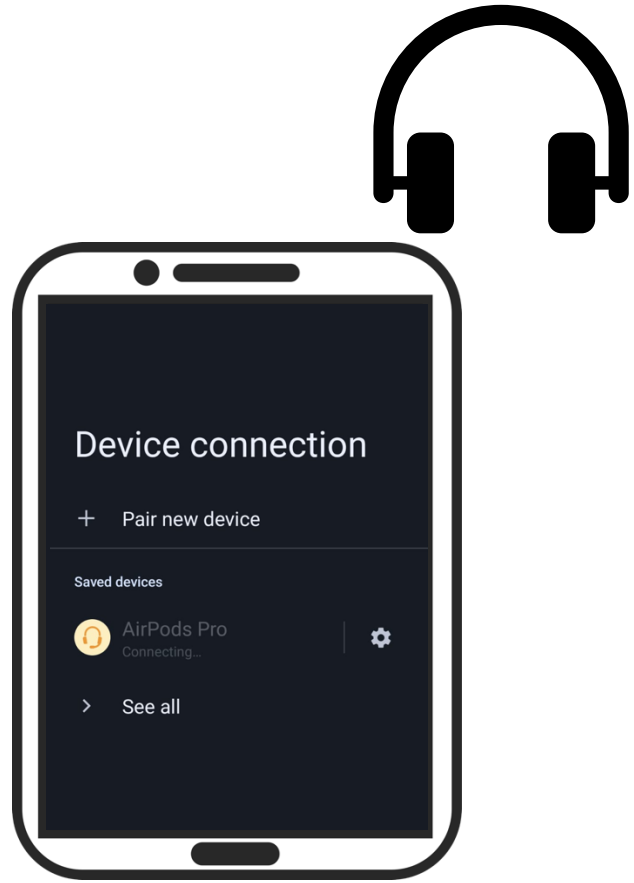
Why do you analyze a technology from the 1990s?!

Not TLS, eh? Are you sure? You could be great, you know, it's all here in your head,

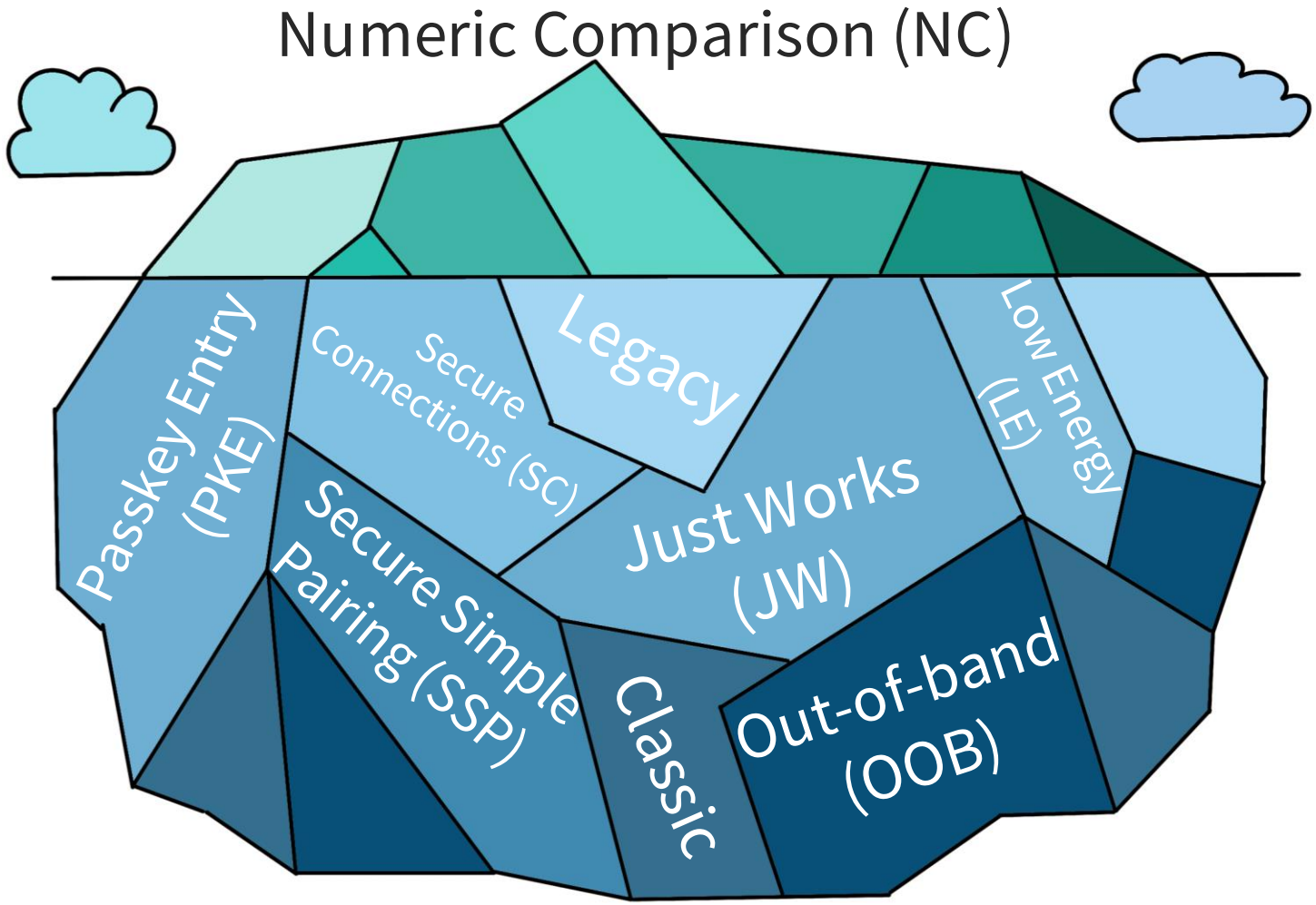
and TLS will help you on the way to greatness, no doubt about that—no?

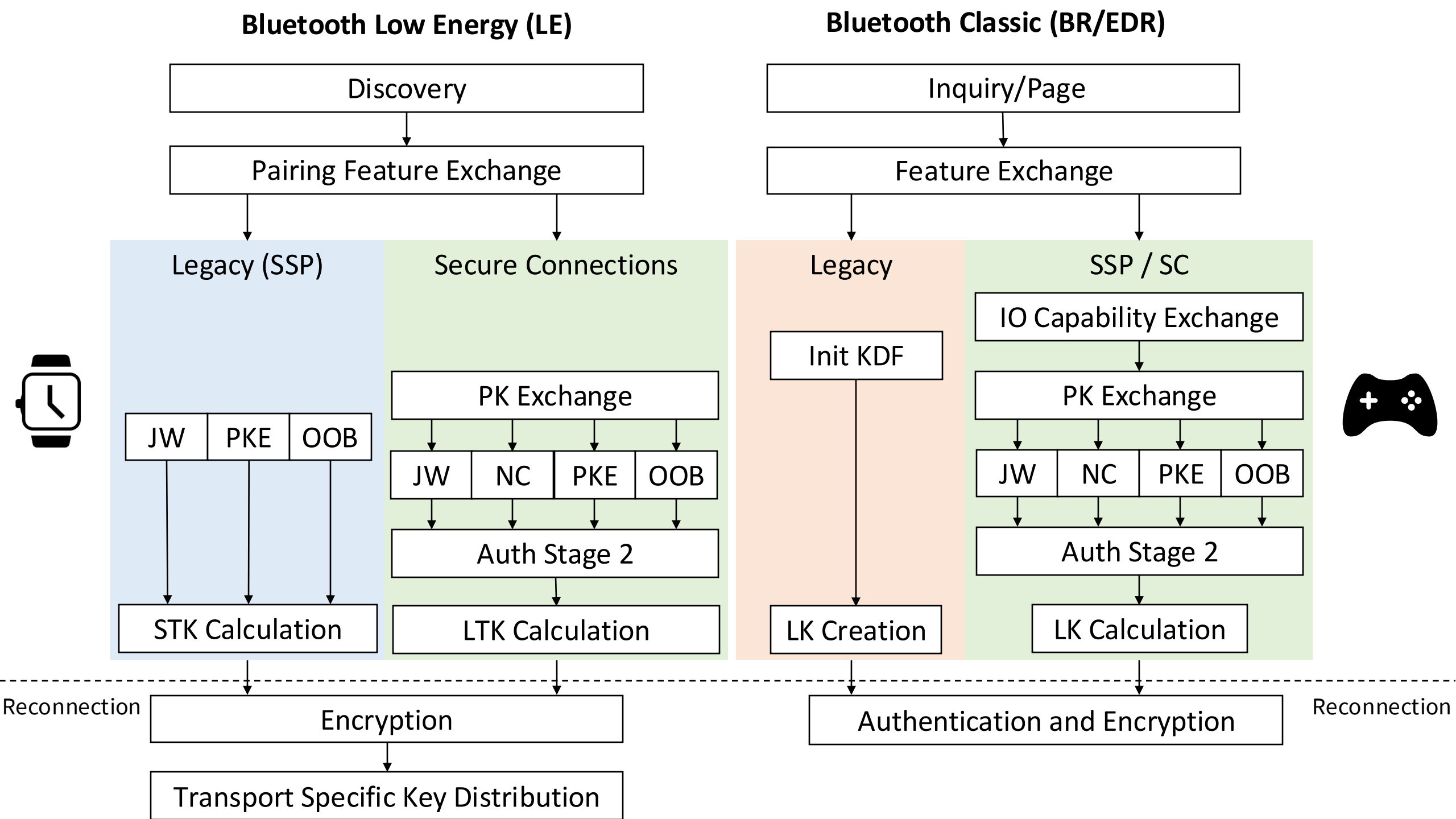

ROBOTICUS
Everything is better with Bluetooth.

Bluetooth Connection: User Experience

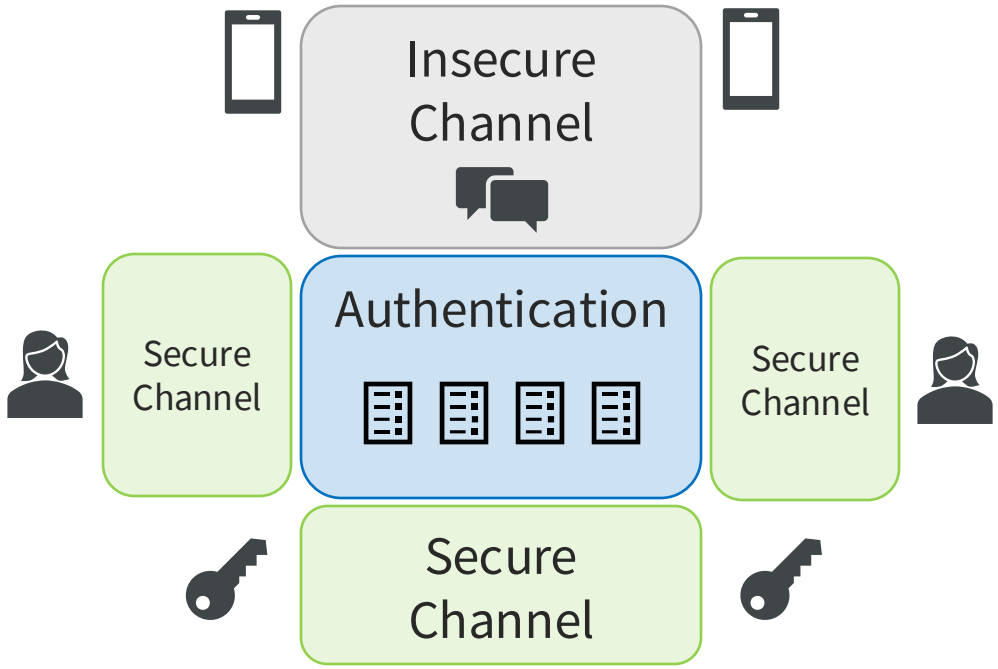


Bluetooth is a BIG protocol suite




Bluetooth Low Energy (LE)
Bluetooth Classic (BR/EDR)
Discovery
Pairing Feature Exchange
Inquiry/Page
Feature Exchange
Legacy (SSP)
Secure Connections
Legacy
SSP / SC
IO Capability Exchange
Init KDF
PK Exchange
PK Exchange
JW
PKE
OOB
JW
NC
PKE
OOB
JW
NC
PKE
OOB
Auth Stage 2
Auth Stage 2
STK Calculation
LTK Calculation
LK Creation
LK Calculation
Reconnection
Encryption
Authentication and Encryption
Reconnection
Transport Specific Key Distribution

Idea behind Bluetooth Key Exchange in SC



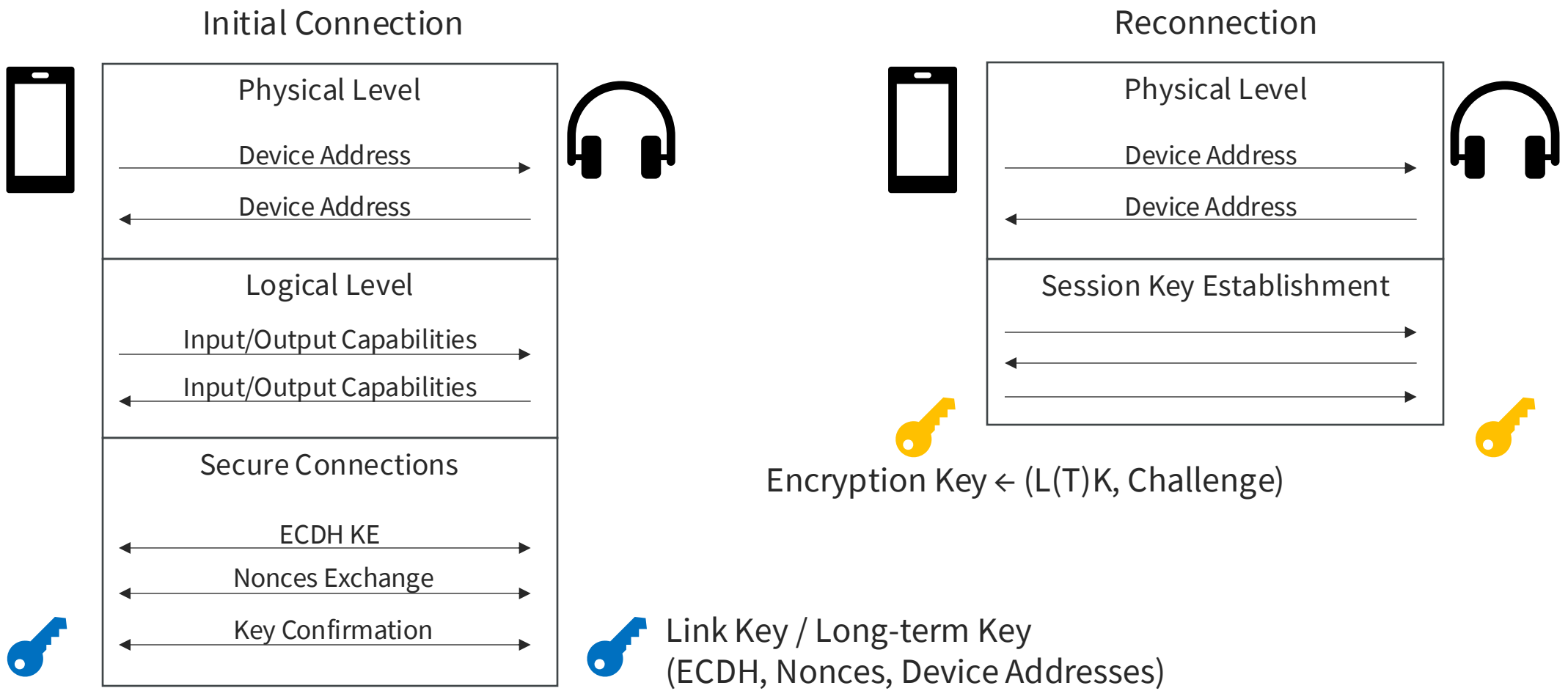
❌ **No** PKI

💡 Let's involve the user!

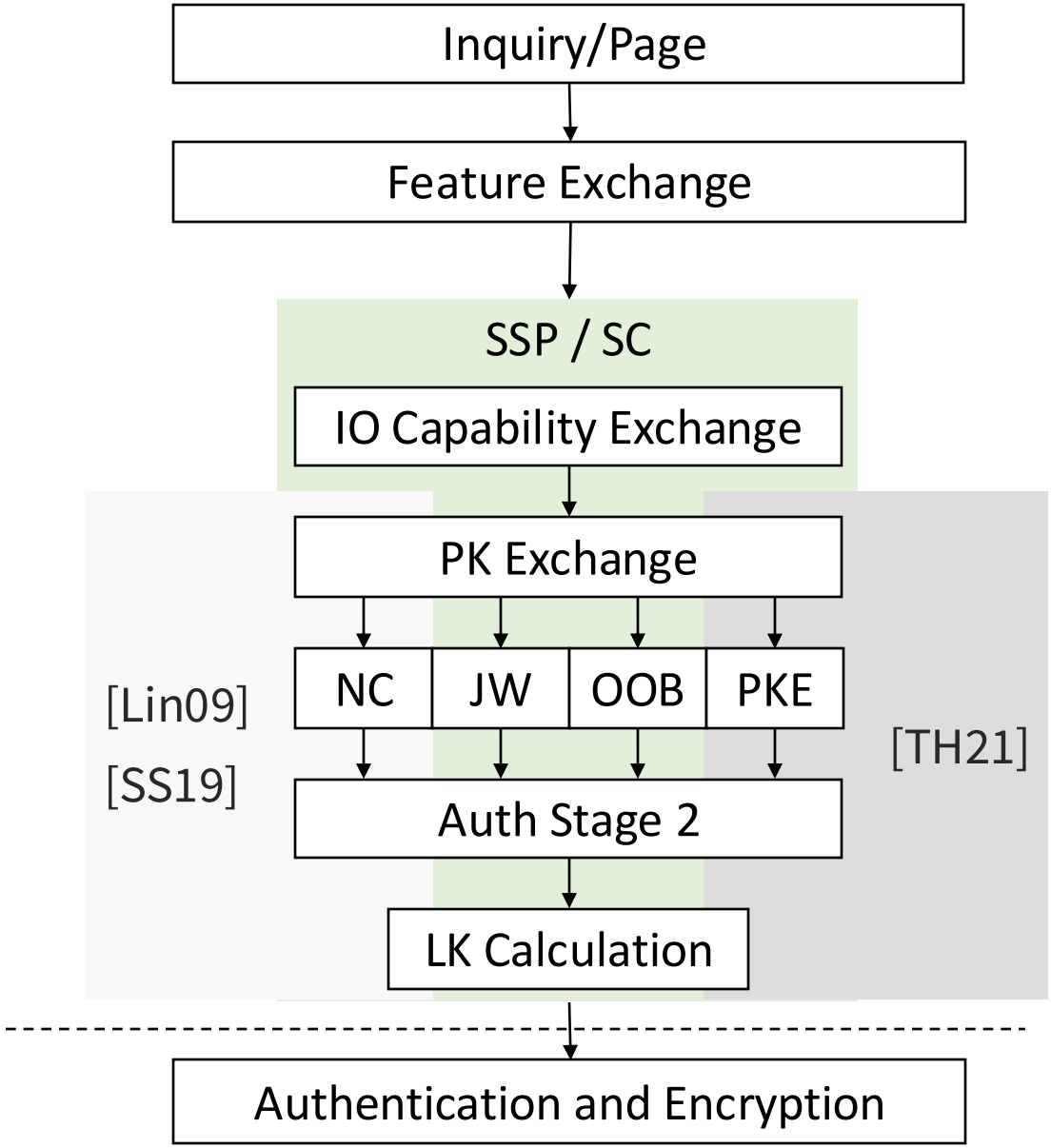
⚠️ Highly constrained devices

But the user doesn't understand…

High-Level SC Protocol Flow



Bluetooth Classic (BR/EDR)

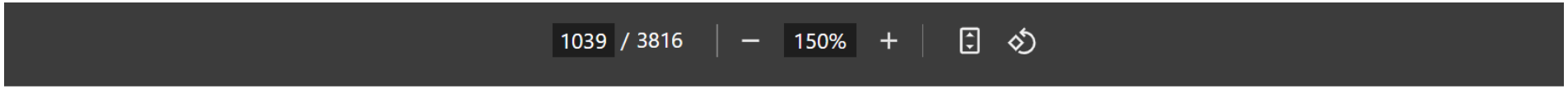


[Lin09] Lindell. Comparison-based key exchange and the security of the numeric comparison mode in Bluetooth v2.1, *CT-RSA 2009*

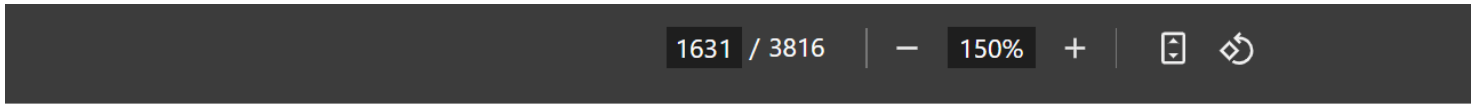
[SS19] Sun and Sun. On secure simple pairing in bluetooth standard v5.0-part i: Authenticated link key security and its home automation and entertainment applications, *Sensors 2019*

[TH21] Troncoso and Hale. The bluetooth cyborg: Analysis of the full human-machine passkey entry ake protocol, *NDSS 2021*

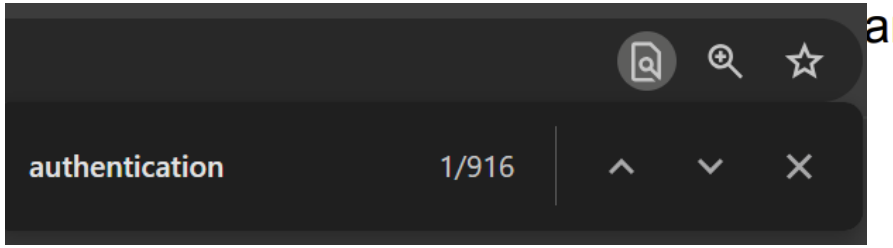
Why Analyzing Bluetooth is Difficult?



To protect a device's private key, a device should implement a method to prevent an attacker from retrieving useful information about the device's private key. For this purpose, a device should change its private key after every pairing (successful or failed). Otherwise, it should change its private key whenever S + 3F > 8, where S is the number of successful pairings and F the number of failed attempts since the key was last changed.



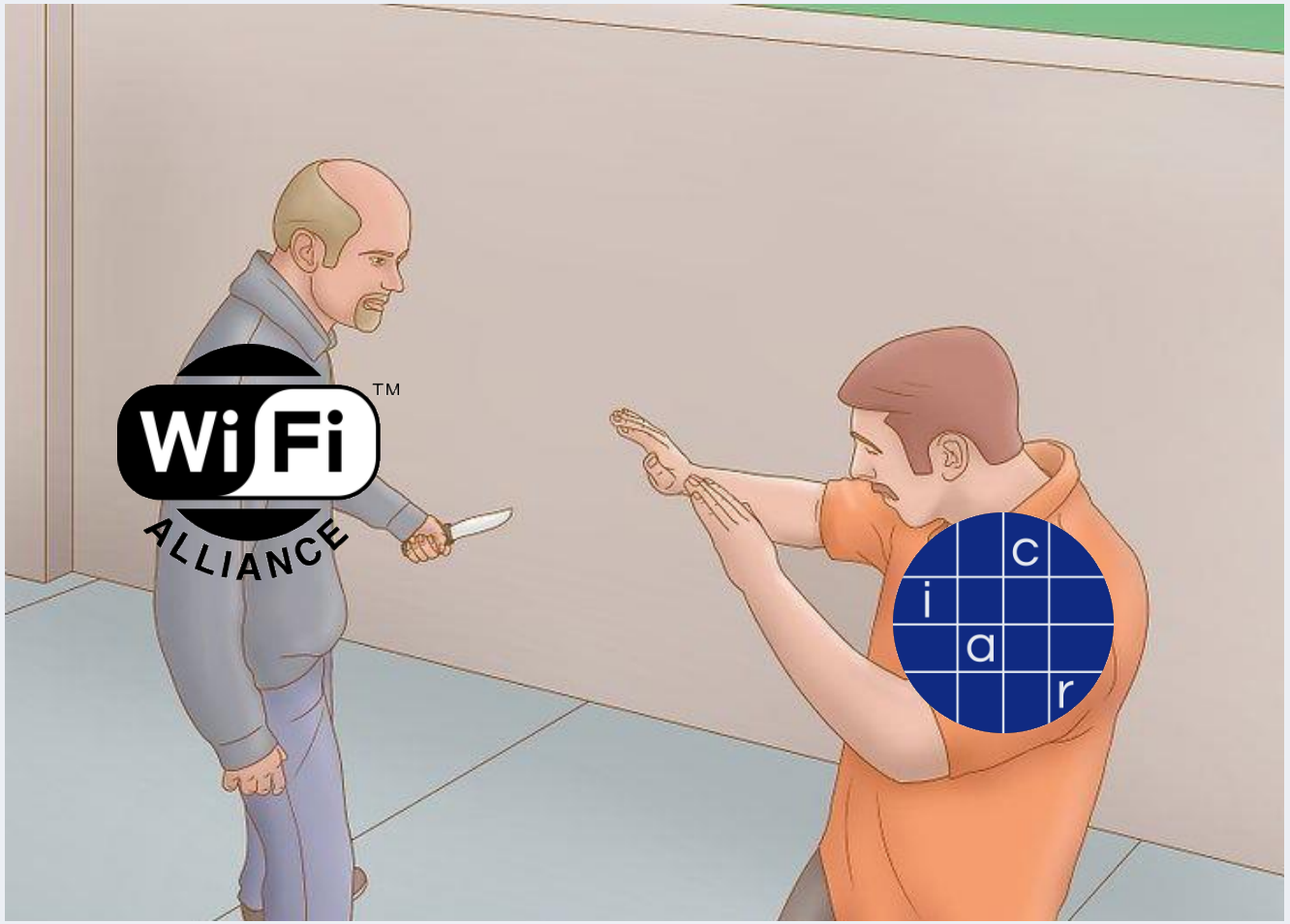
PKax denotes the x-coordinate of the public key PKa of A.



arly, PKbx denotes the x-coordinate of the public key PKb of B.

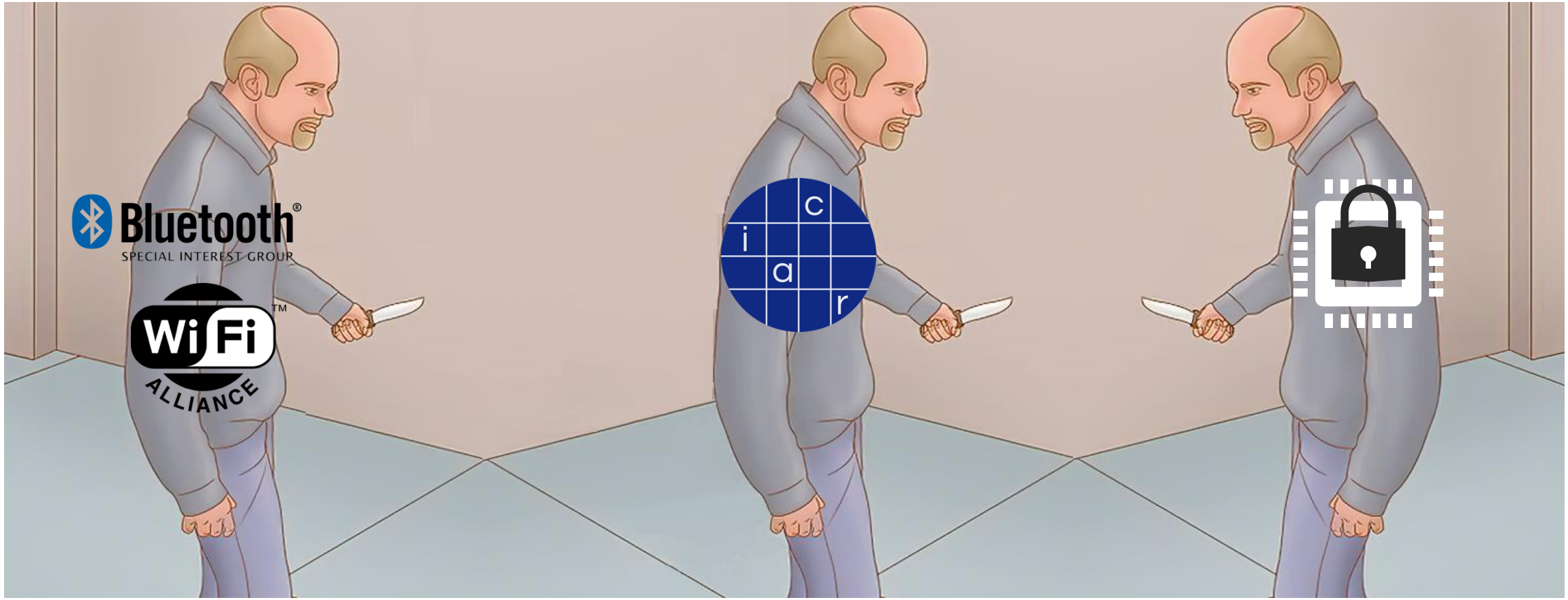
The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won’t save us.

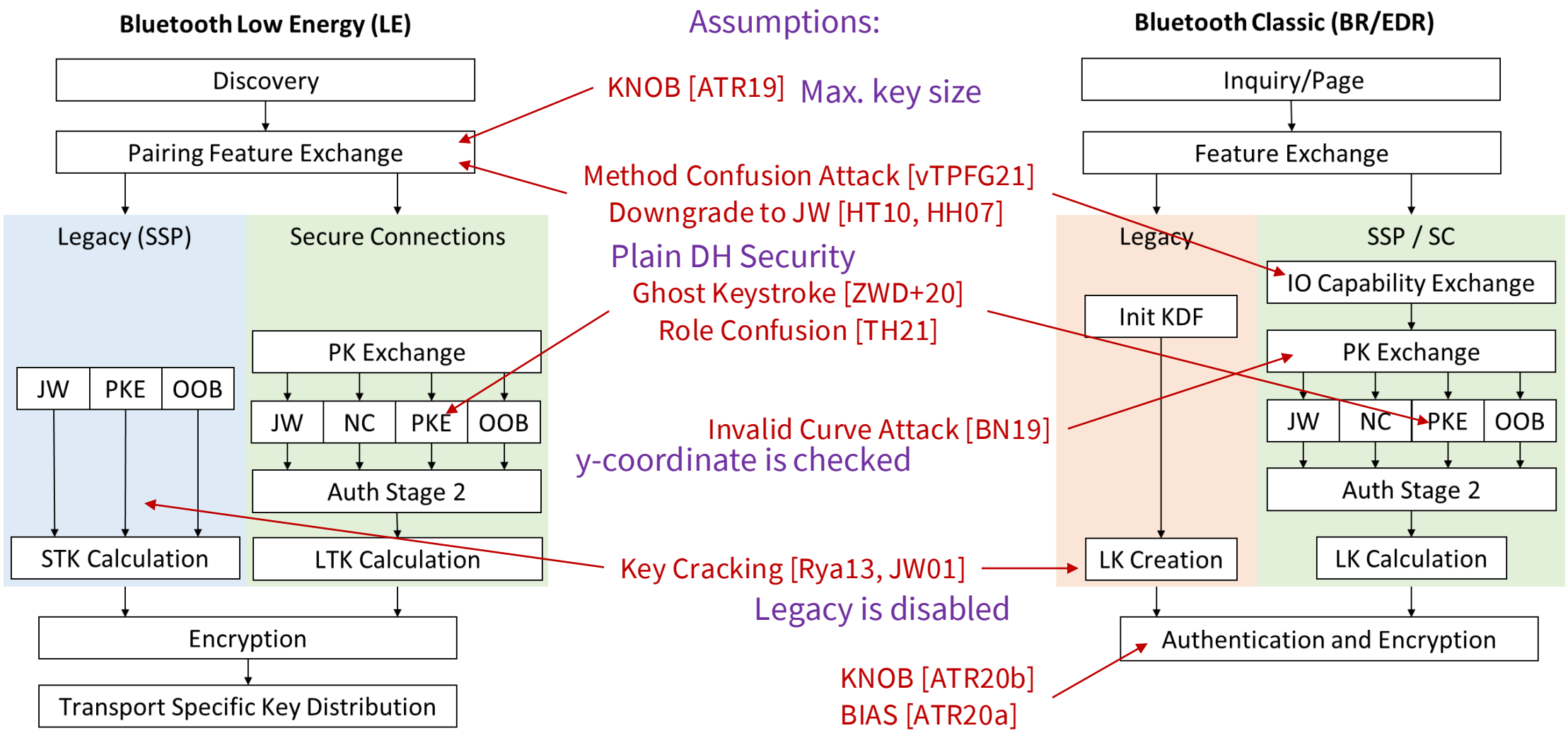


“Mesh Messaging for Large-Scale Protests: Cryptography Alone Won't Save Us”

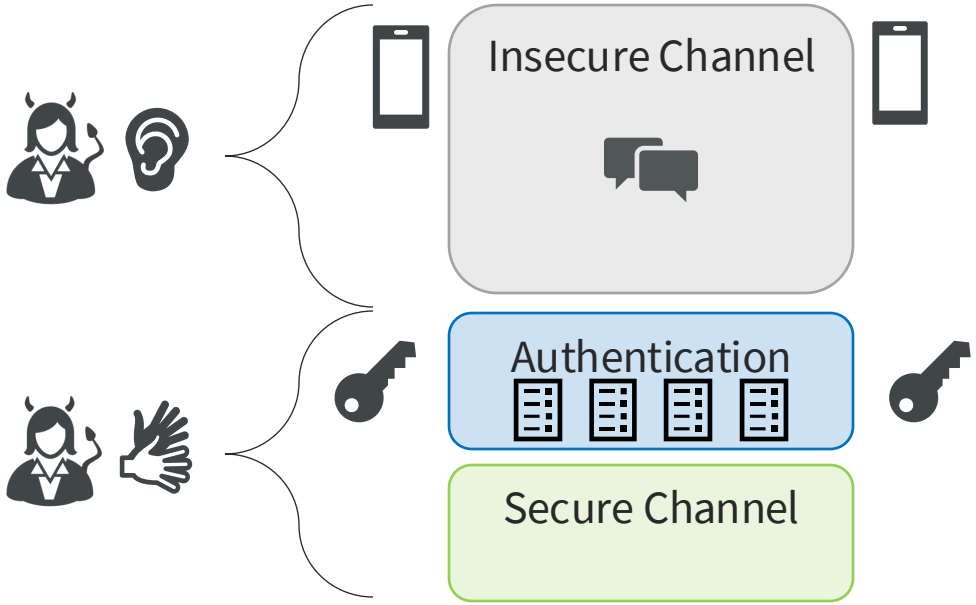
Wireless Standard Organizations vs Crypto Community vs Security Community



Distribution of the Attacks (2021)



Results [FS21]



Resulting analysis:

- Includes **full** SC protocol family
- Trust-On-First-Use (TOFU) model in [BR93]**-style**

Properties:

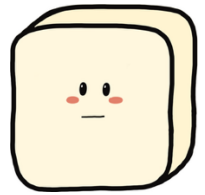
- Key Secrecy
- Match Security

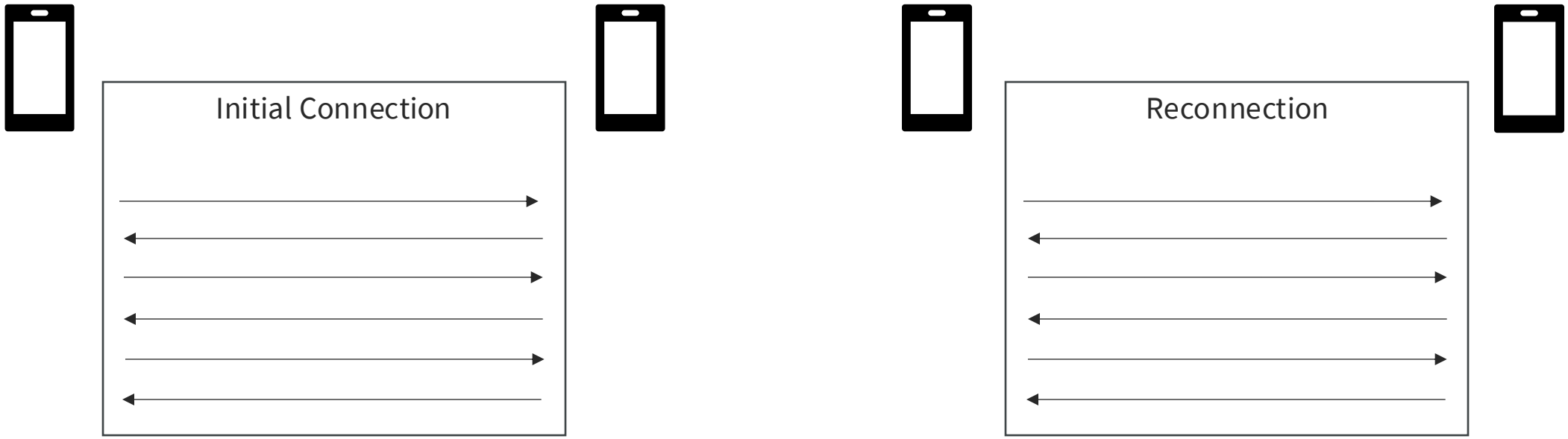
Adversarial oracles

- InitSession
- Reconnect
- NextPK
- No Corrupt

[FS21] Fischlin and Sanina. Cryptographic analysis of the bluetooth secure connection protocol suite, *Asiacrypt* 2021
[BR93] Bellare and Rogaway. Entity authentication and key distribution, *CRYPTO'93*

TOFU (**T**rust-**O**n-**F**irst-**U**se) Model [FS21]





Passive:
eavesdrop the communication

Active:
drop, modify messages, reveal the session key…

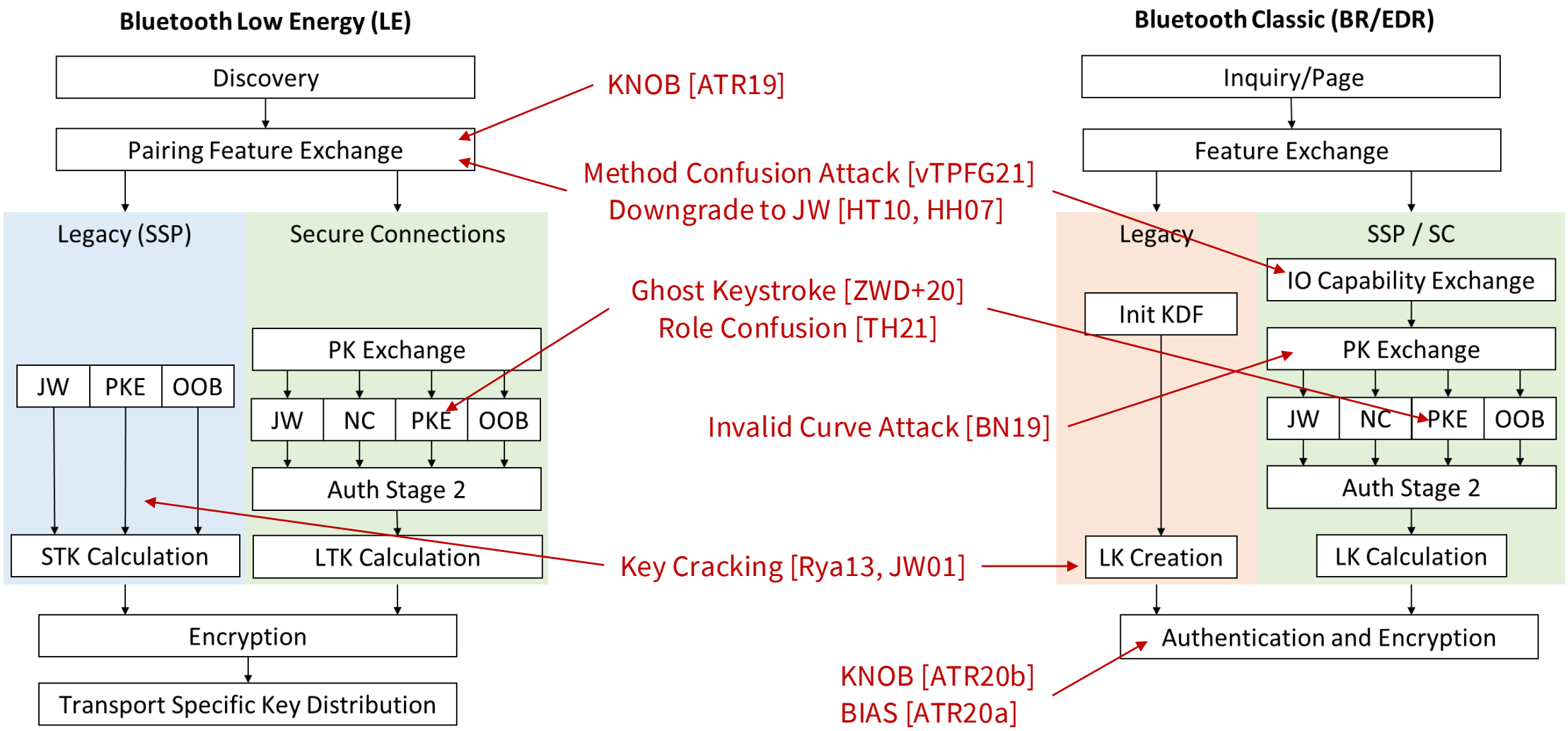
[FS21] Fischlin and Sanina. Cryptographic analysis of the bluetooth secure connection protocol suite, *Asiacrypt* 2021

Can we do better?

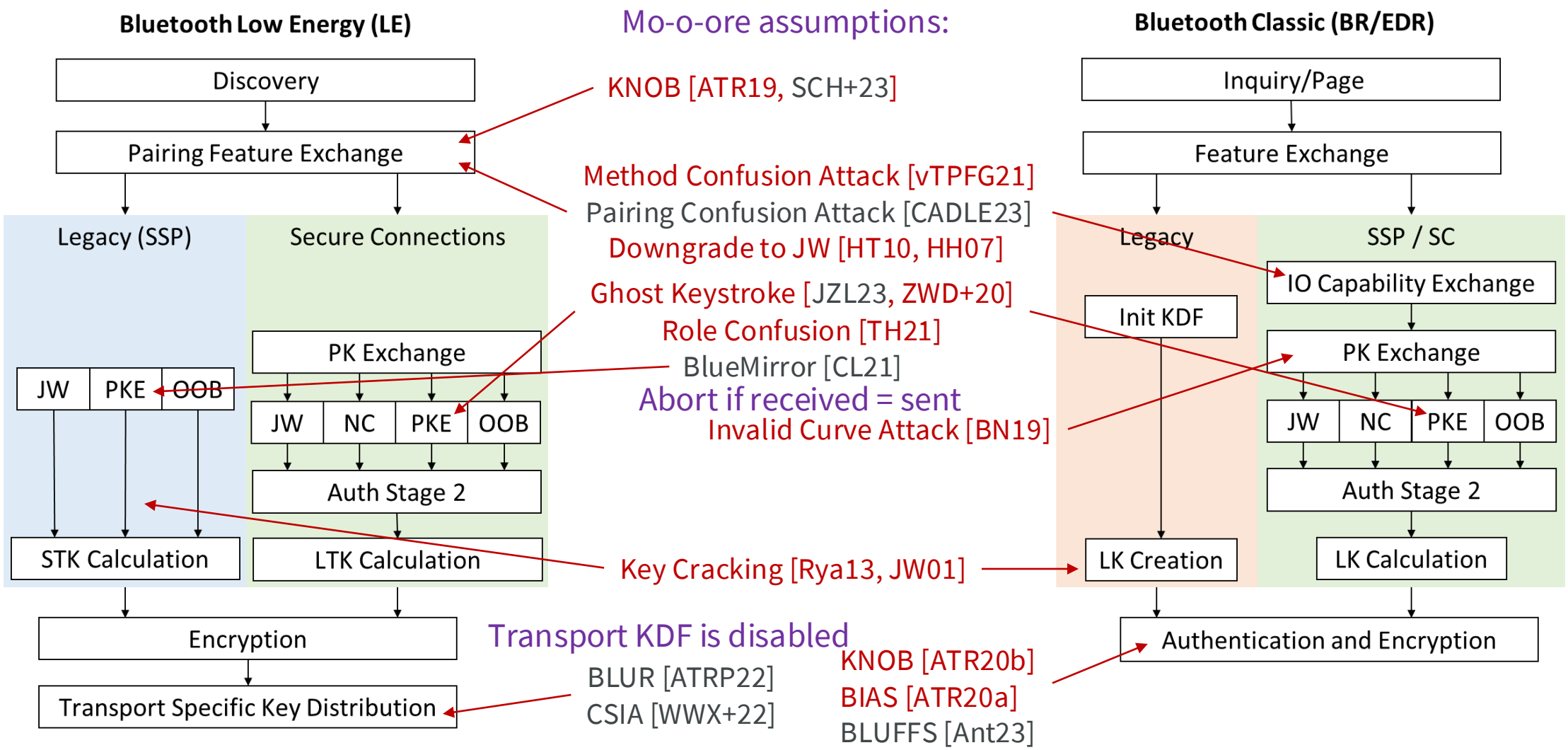
Bluetooth® security notices

Vulnerability	Publication Date	Details	Specifications Affected	CVE [NVD]
SUPPLEMENT: Impersonation in the Passkey Entry Protocol	19/09/2024	SIG Security Notice	Core Spec v2.1 to 5.4	CVE-2021-37577
BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses	27/11/2023	SIG Security Notice	Core Spec v4.2 to 5.2	CVE-2023-24023
Pairing Mode Confusion in Bluetooth LE Passkey Entry	09/12/2022	SIG Security Notice	Core Spec v4.0 to 5.3	CVE-2022-25836
Pairing Mode Confusion in BR/EDR	09/12/2022	SIG Security Notice	Core Spec v1.0B to 5.3	CVE-2022-25837
InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections	21/06/2021	SIG Security Notice	Core Spec, v4.0 to 5.2	CVE-2021-31615
Bluetooth Mesh Profile AuthValue leak	24/05/2021	SIG Security Notice	Mesh Profile Spec, v1.0 to v1.0.1	CVE-2020-26559
Malleable commitment in Bluetooth Mesh Profile provisioning	24/05/2021	SIG Security Notice	Mesh Profile Spec, v1.0 to v1.0.1	CVE-2020-26556
Predictable Authvalue in Bluetooth Mesh Profile provisioning leads to MITM	24/05/2021	SIG Security Notice	Mesh Profile Spec, v1.0 to v1.0.1	CVE-2020-2655[illegible]

Distribution of the Attacks (2021)



Distribution of the Attacks (2024)



Fix… is problematic

🦄 Universal fix for the whole stack against all attacks

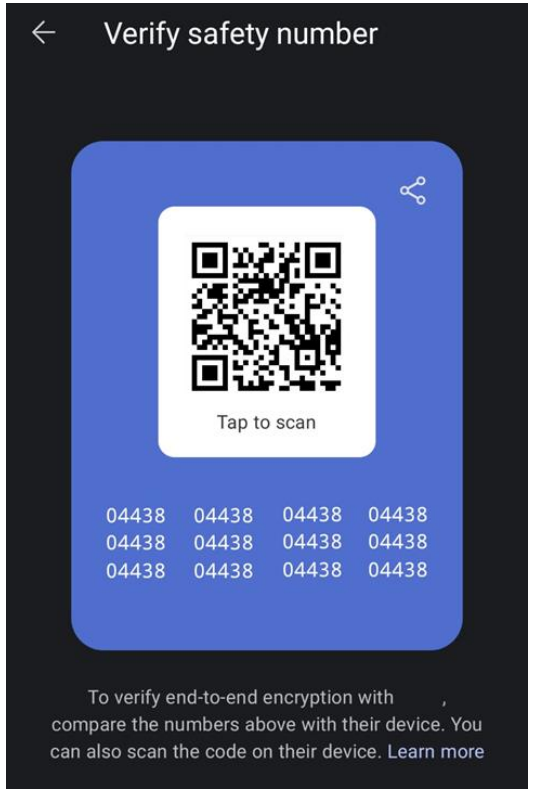
⏪ Backward compatibility:

- No changes in the protocol
- No storage of the transcript

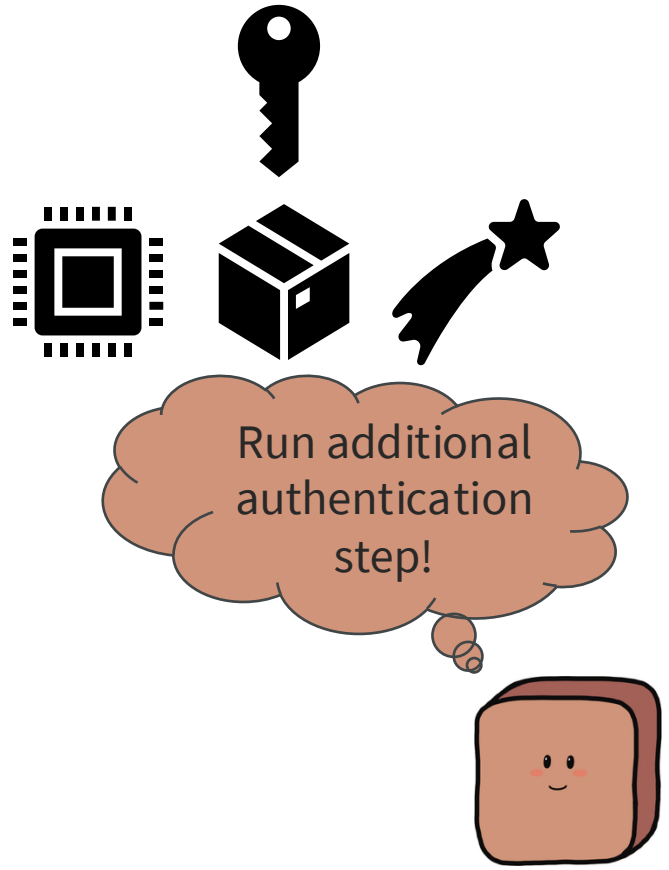
How to Do Better Than TOFU?

OOB: QR-codes / NFC

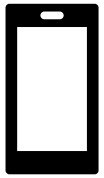
User Confirmation
(e.g., in Signal and WhatsApp)



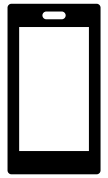
Pre-Shared Key (e.g., PSK in TLS)



Just Add Signatures!



LK



LK

SK_B
PK_B
$cert_B$

$challengeA \xleftarrow{\$} \{0,1\}^{128}$

$challengeB \xleftarrow{\$} \{0,1\}^{128}$

$challengeA$ →

$authData \leftarrow HMAC(LK, challengeA||challengeB)$

$\sigma_B \leftarrow Sig(SK_B, authData)$

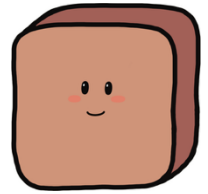
← $challengeB, \sigma_B, cert_B, PK_B$

$authData \leftarrow HMAC(LK, challengeA||challengeB)$

Verify $cert_B$ and σ_B

Mutual authentication: same protocol but with reversed roles

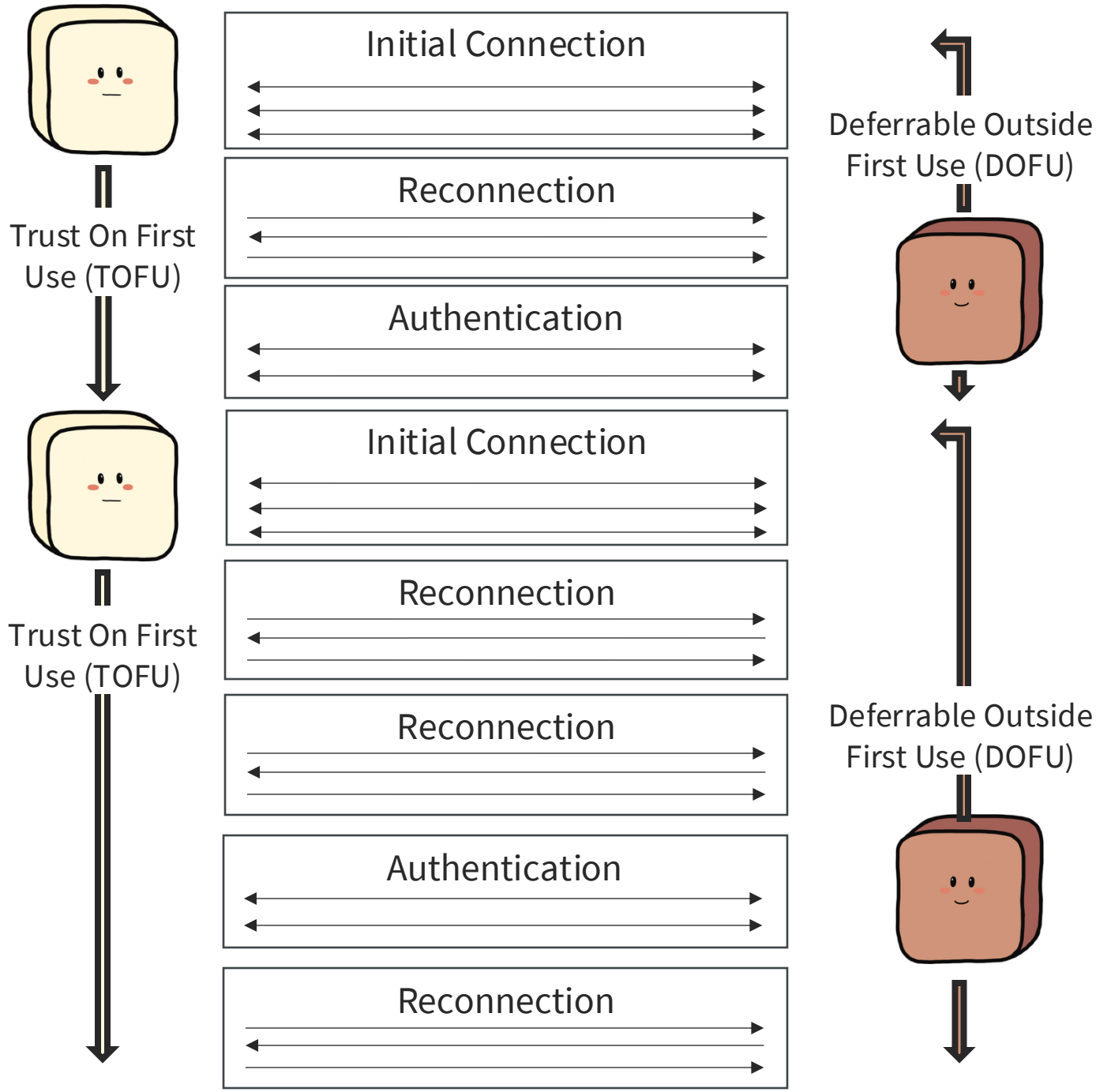
Our Solution



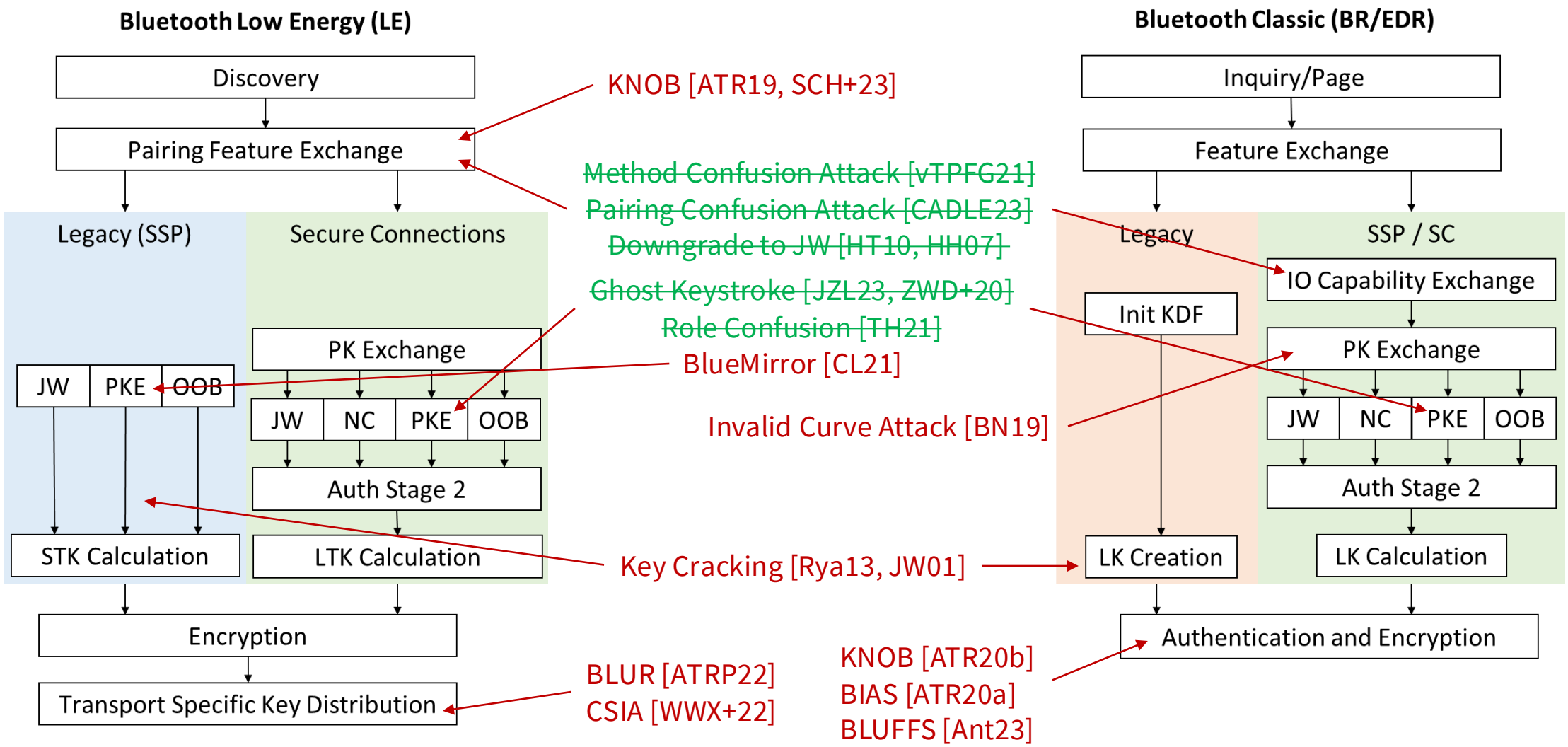
Run additional authentication step!

🔗 Links authentication to derived L(T)Ks
🛠️ Uses existing functions
⏳ Can run at any point of time

⚙️ Two types of the schemes: DH-based and signature-based → 4 in total


Initial Connection
Reconnection
Authentication
Trust On First Use (TOFU)
Deferrable Outside First Use (DOFU)
Initial Connection
Reconnection
Reconnection
Authentication
Reconnection
Trust On First Use (TOFU)
Deferrable Outside First Use (DOFU)

Distribution of the Attacks (2024)



Results [FS24]

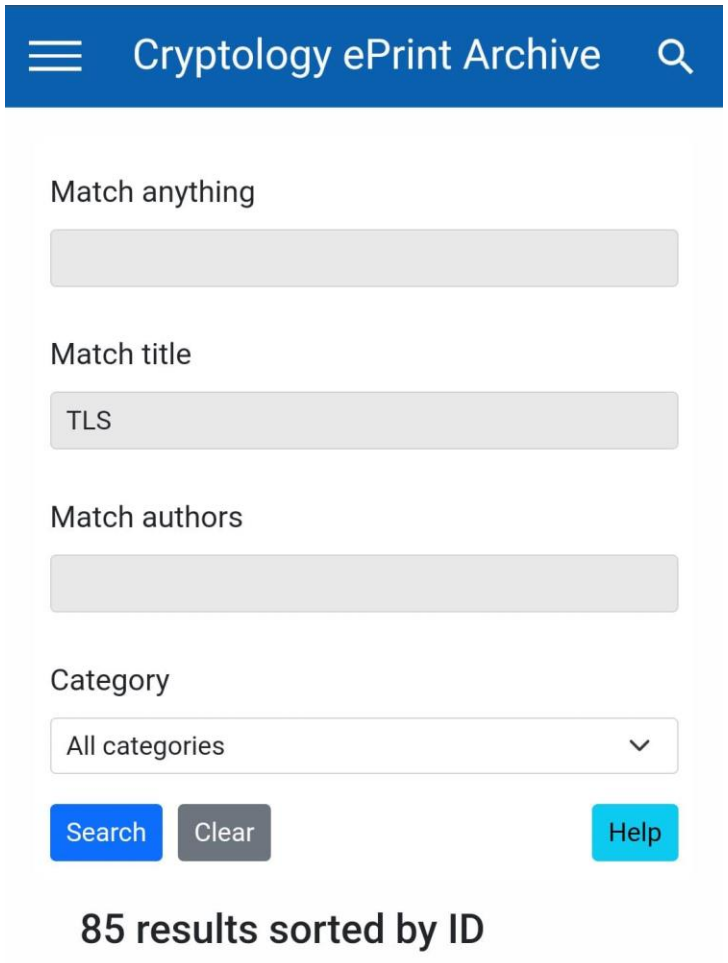
Extended the trust-on-first-use (TOFU) [FS21] security model…
to add deferrable-outside-first-use (DOFU) authentication

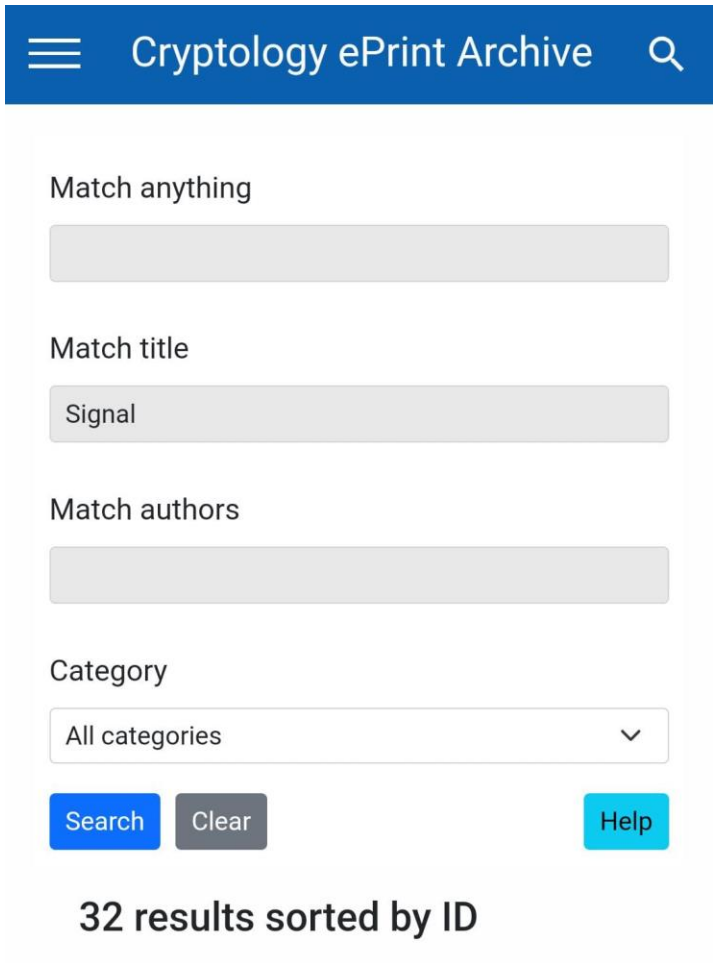
Proved BR/EDR to be secure in TOFU-or-DOFU model…
but failed with BLE ☹

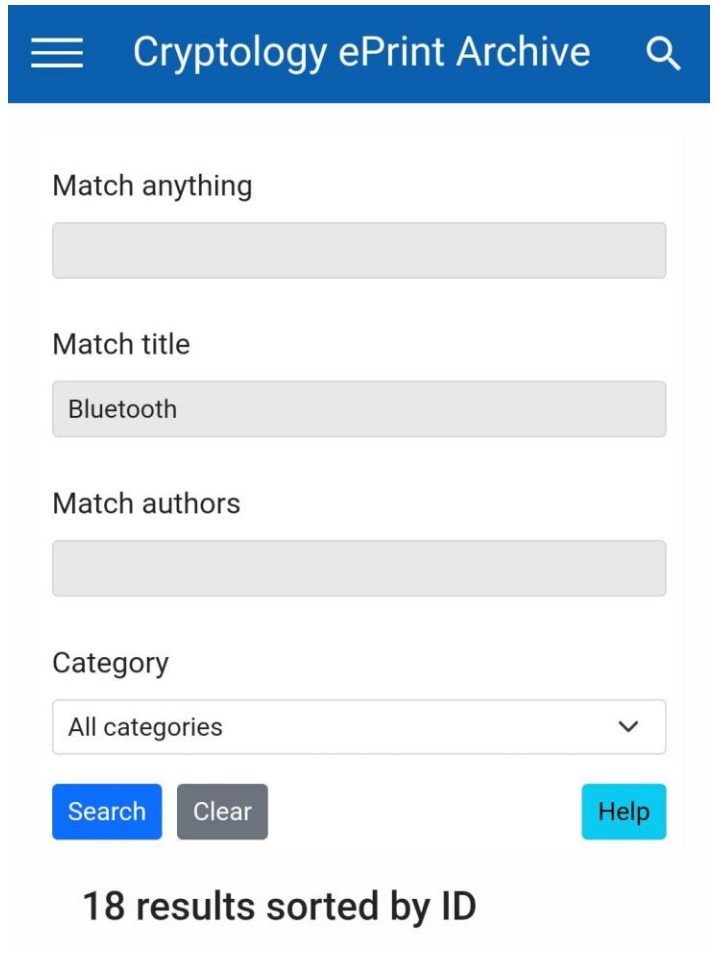
Security Notion	BR/EDR	BLE
Match Security	✓	✓
Authentication	✓	✓
Leakage Resistance	✓	✓
Key Secrecy	✓	✗

[FS24] Fischlin and Sanina. Fake It till You Make It: Enhancing Security of Bluetooth Secure Connections via Deferrable Authentication, *CCS* 2024
[FS21] Fischlin and Sanina. Cryptographic analysis of the bluetooth secure connection protocol suite, *Asiacrypt* 2021

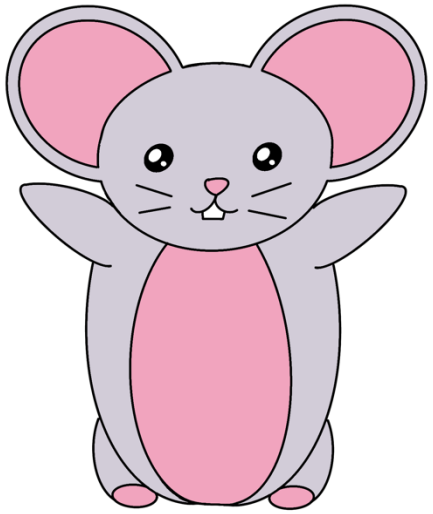
(Instead of) Conclusion

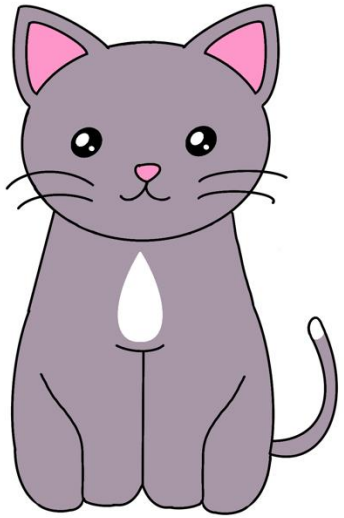


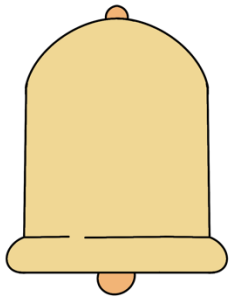




(Instead of) Conclusion







	TOFU-Security Analysis of Bluetooth	Bringing Authentication to Bluetooth
ePrint:	ia.cr/2021/1597	ia.cr/2024/874

Thank you!