GSMA 5GSTF#51 presentation, for information to 3GPP SA3

Nori

Concealing the Concealed Identifier in 5G

https://www.precisionnutrition.com/encyclopedia/food/nori

John Preuß Mattsson

Prajwol Kumar Nakarmi

Ericsson

2021-04-26

Analysis of the SUCI protection mechanism in 5G

- SUCI is an essential mechanism for 5G privacy. Will hopefully be deployed everywhere.
- SUCI provide excellent properties as long as:
  - Null-scheme is not used
  - **Identifiers have fixed length**
  - All users belong to the same MNC / realm
  - Public key of HN is refreshed frequently
  - No large quantum computers.
- SUCI will be easy to extend to Post-Quantum Cryptography, also for NB-IoT.
- **When used with variable length identifiers, e.g., SUPI of type NSI (NAI), SUCI provide very poor anonymity.**
- **SUCI should be augmented with mechanisms and recommendation for padding.**

SUPI (Subscription Permanent Identifier)

— A globally unique 5G Subscription Permanent Identifier allocated to each subscriber in the 5G System.

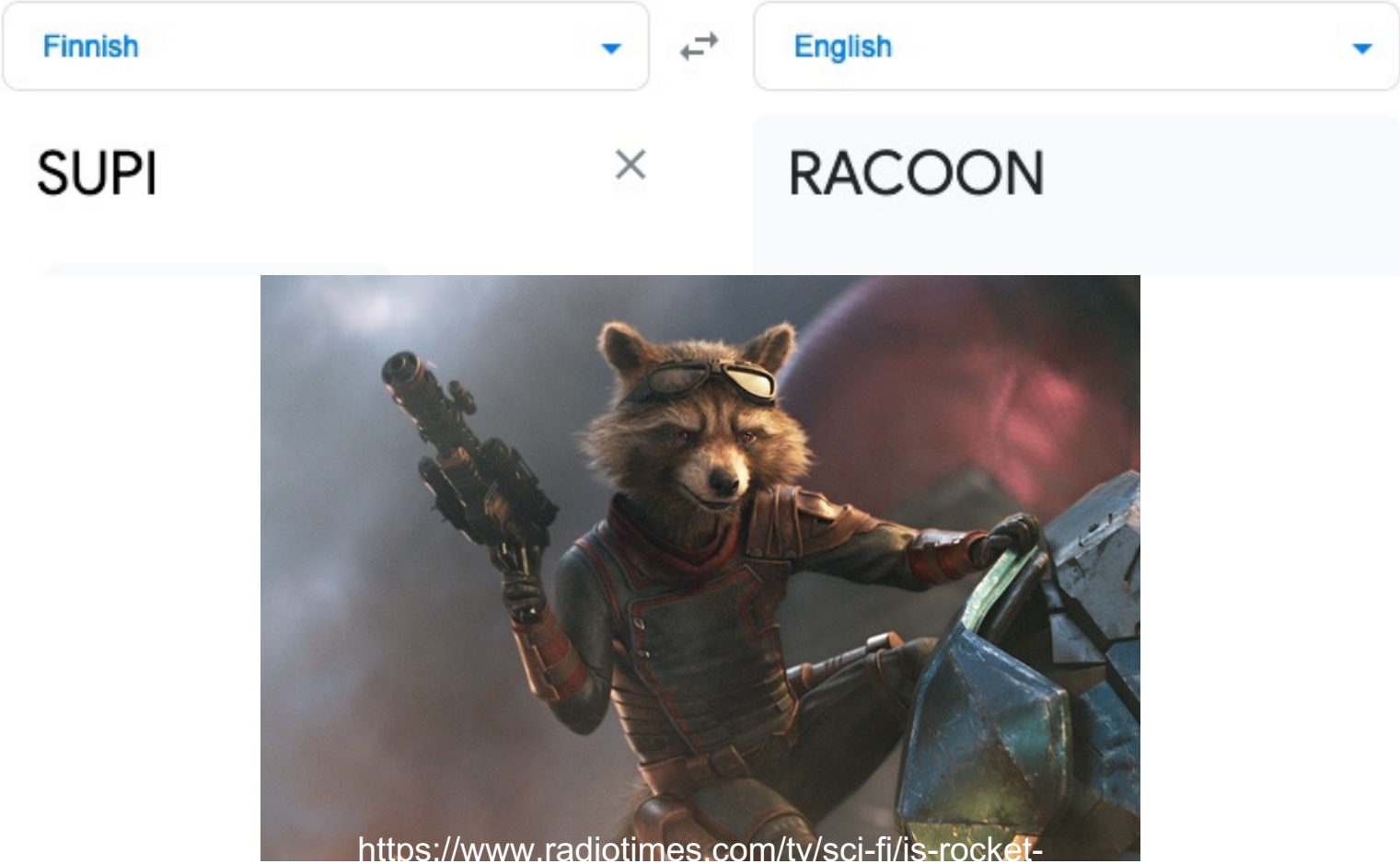
```
SUPI =     SUPI type,
           SUPI value
```

— There are currently four types of SUPI:

Type		Value
International Mobile Subscription Identity	IMSI	MCC || MNC || MSIN
Network Specific Identifier	NSI	username@realm Network Access Identifier (NAI) format
Global Line Identifier	GLI	
Global Cable Identifier	GCI	

— MSIN has fixed length for a given MNC. **NAI username has variable length.**

SUPI (Subscription Permanent Identifier)

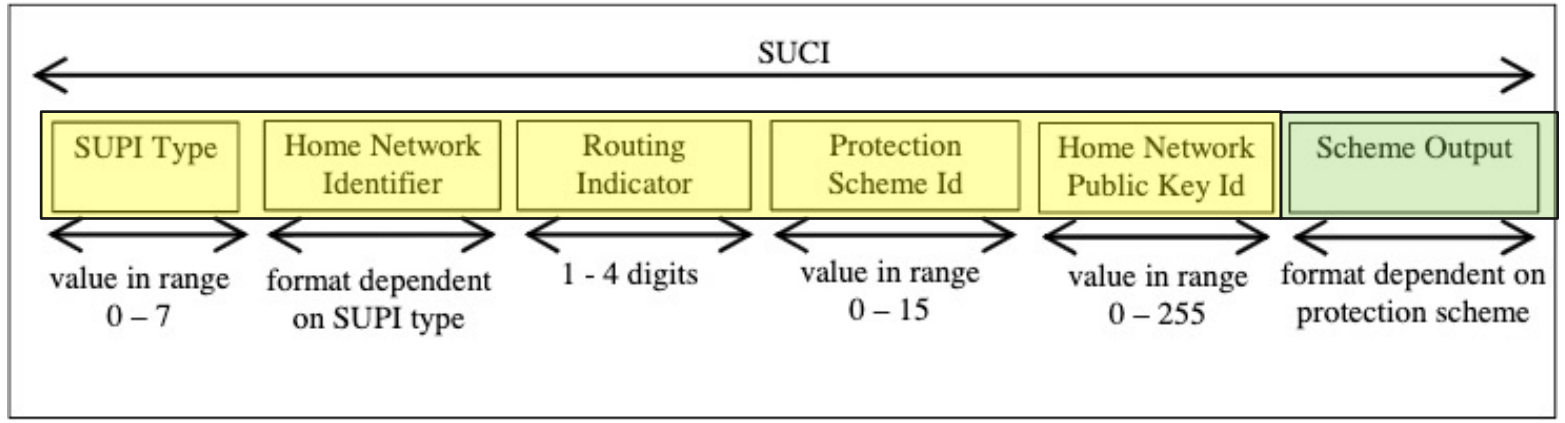


SUCI (Subscription Concealed Identifier)

- A privacy preserving identifier containing the concealed SUPI
  - Only encrypts subscription identifier (MSIN or username)

```
SUCI =   SUPI type,
         Home Network Identifier,
         Other parameters,
         Concealed subscription identifier
```

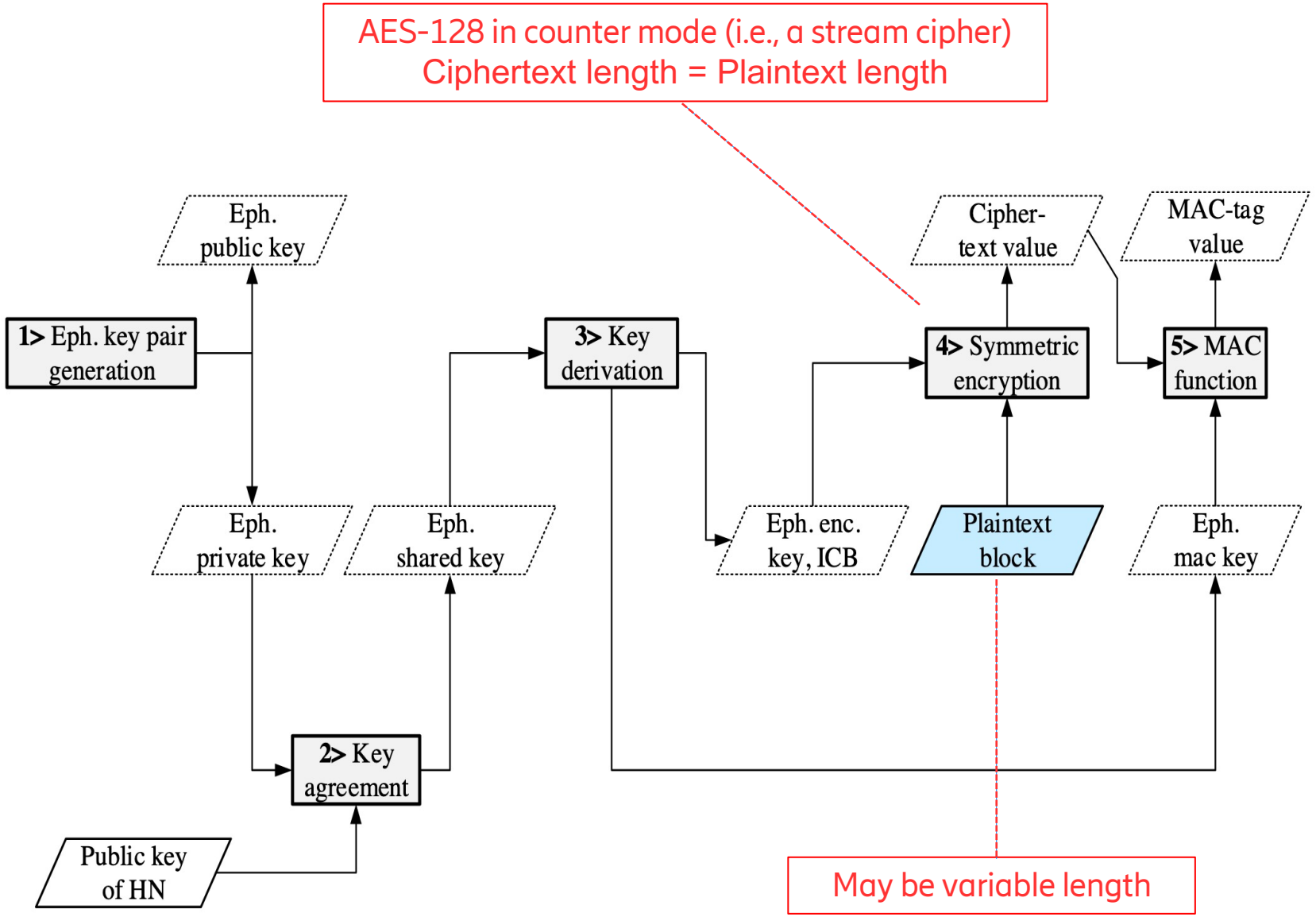
Encrypted



https://rasamalaysia.com/california-roll-recipe/

SUPI Protection Schemes

- Null-scheme
- Profile A
  - ECIES
  - Curve25519
  - HMAC-SHA-256
  - AES-128-CTR
- Profile B
  - ECIES
  - secp256r1
  - HMAC-SHA-256
  - AES-128-CTR



SUPI Protection Schemes - Analysis

- When used with NSI with variable length usernames, SUCI reveals the length of the username. This may enable an attacker to distinguish individual users.
- If large quantum computers are built, a quantum attacker can decrypt SUCI recorded in the past.
- MCC, MNC, and realm are not encrypted. In roaming scenarios an attacker might distinguish individual users.
- If public key of HN leaks (e.g., through side-channel attacks) and attacker can decrypt all SUCI protected with that key.
- Null-scheme provides no privacy whatsoever

- When used with IMSI with fixed length MSIN, SUCI reveals no information about MSIN.
- Easy to augment SUCI with Post-Quantum Key-Encapsulation Mechanisms.
- Well-known hard problem: Other technologies have the same vulnerability; routing information is not encrypted.
- Networks might limit impact by changing public key with regular intervals.
- Might deprecate null-scheme in the future.

SUCI and Post-Quantum Cryptography (PQC)

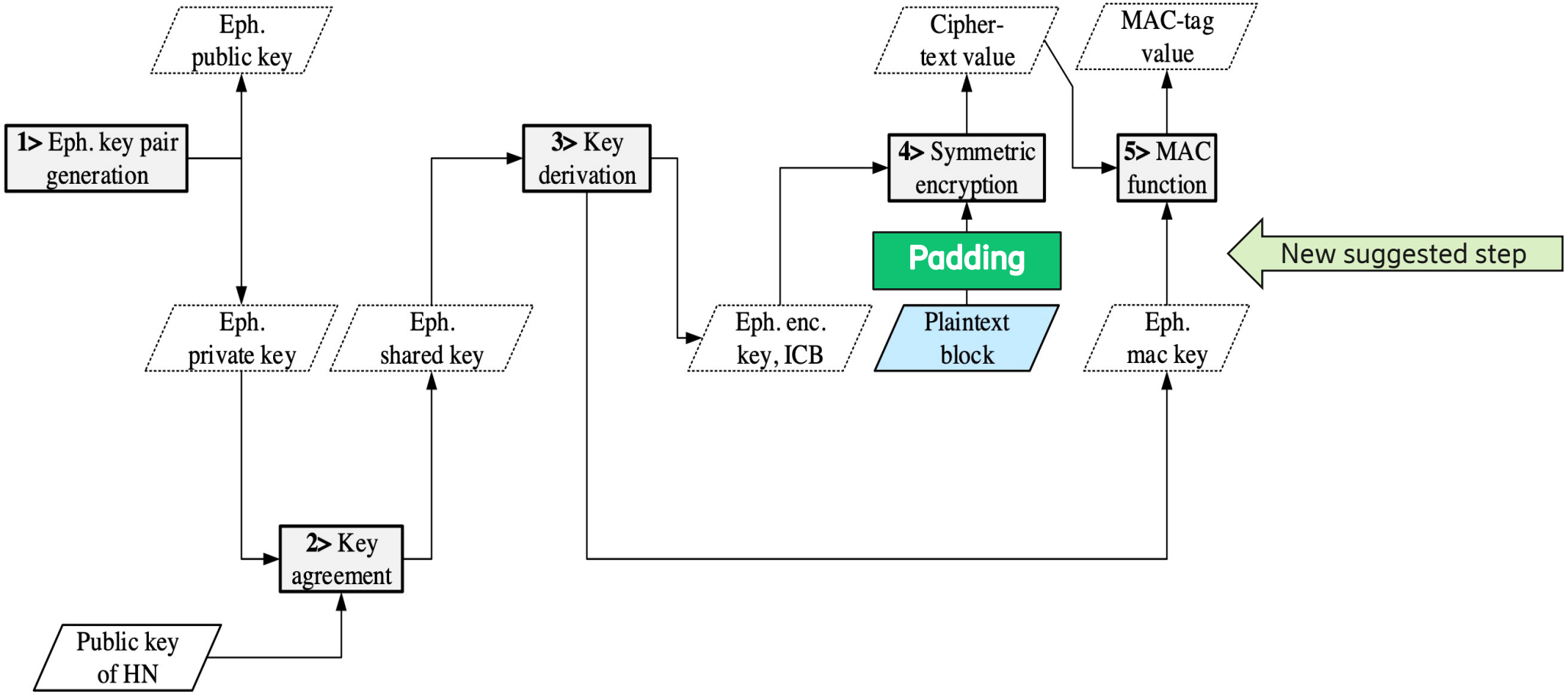
- AES-128 achieves NIST's preliminary post-quantum security level 1 and SHA-256 achieves NIST's post-quantum security level 2.
- Curve25519 and P-256 will be broken if a very large quantum computer (approximately a million **physical** qubits) is ever built.
  - Possible to replace Curve25519 and P-256 with PQC algorithms when NIST finalizes PQC standardization in 2024.
  - The allocated size (1600 - 3000 bytes) will be more than enough for NIST post-quantum security level 1.
  - Lattice- and code-based crypto is faster than ECC but have larger public keys and ciphertexts.

Algorithm	Generate key pair	Sign	Verify	Encapsulate	Decapsulate	Public key size	Signature/ciphertext size
LMS/XMSS/HSS/MXSS^MT (hash-based PQC)	43 - 165000 ms	0.51 - 6.0 ms	0.096 - 5.3 ms			50 - 100 B	700 - 8000 B
Picnic picnic3-L1 (symmetric primitives)	0.001 ms	7.272 ms	5.508 ms			35 B	12492 B
Rainbow 1a (multivariate PQC)	401.505 ms	0.020 ms	0.014 ms			152097 B	64 B
Dilithium-1024x768-AES (lattice-based PQC)	0.018 ms	0.098 ms	0.025 ms			1184 B	2044 B
EdDSA Ed25519	0.018 ms	0.019 ms	0.066 ms			64 B	64 B
ECDSA P-256	0.041 ms	0.053 ms	0.113 ms			64 B	64 B
RSA-3072	232.704 ms	3.542 ms	0.033 ms	0.038 ms	3.530 ms	384 B	384 B
NIST P-256	0.094 ms			0.231 ms	0.231 ms	32 B	32 B
Curve25519	0.050 ms			0.054 ms	0.054 ms	32 B	32 B
Kyber-512-90s (lattice-based PQC)	0.006 ms			0.010 ms	0.008 ms	800 B	736 B
Classic McEliece 348864 (code-based PQC)	18.494 ms			0.015 ms	0.048 ms	261120 B	128 B
SIKE p503 (isogeny-based PQC)	4.292 ms			7.041 ms	7.511 ms	378 B	402 B

Single-core performance on Skylake 2.5 GHz https://bench.cr.yp.to/ebats.html (lower is better)

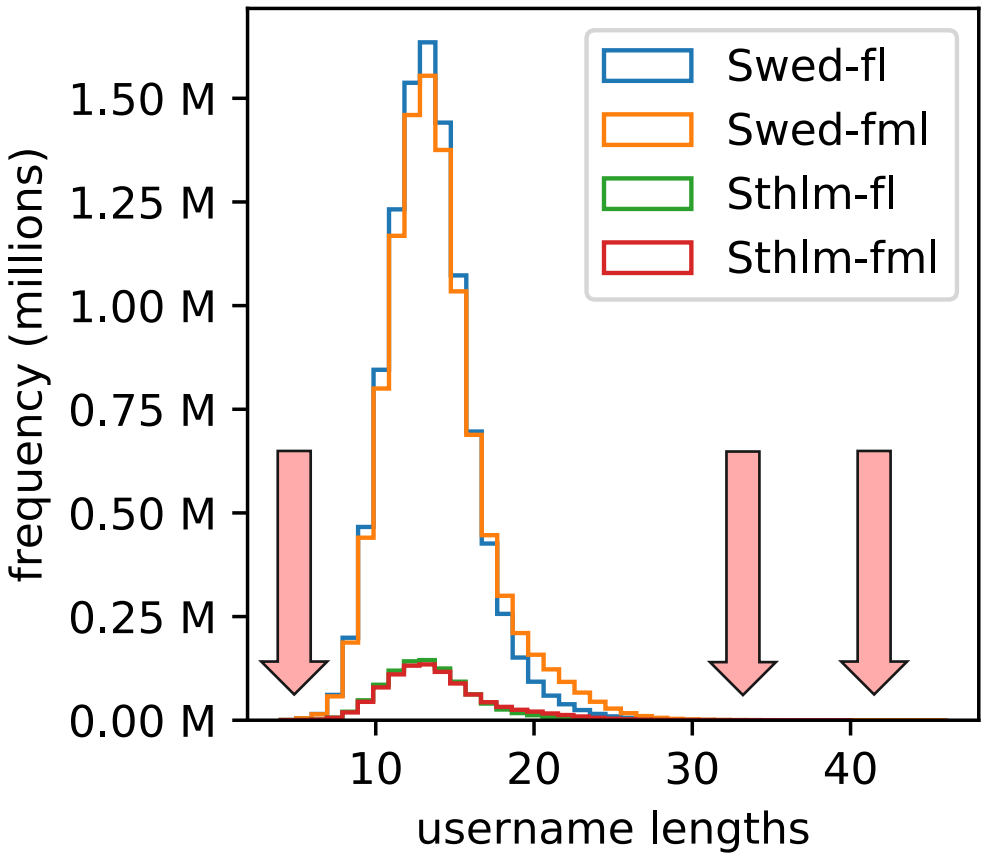
SUCI – Padding before Encryption

— To provide acceptable anonymity for usernames with variable lengths we suggested to introduce a padding step before encryption (and after decryption).



Name data – Sweden

- Assumption: NSI usernames will be based on real-world names.
- We obtained the name distribution for Sweden and Stockholm from Swedish government. USA, India, and China seems to have similar distributions.
- Current SUCI protection schemes only provide 3-anonymity or worse (likely 1-anonymity).
- Individual users with very short or very long names can be distinguished.
- Can be assumed that attacker can use additional information like location and time.



SUCI – Padding before Encryption

Based on real-world name distributions, we have evaluated a large number of different padding method. Padding methods have been evaluated by assigning an attacker cost and a defender cost to each instance.

Attacker cost 1

- Conditional entropy
- Uncertainty about the original unpadded distribution when the padded distribution is known
- Expected number of bits needed to describe the original unpadded distribution given that the padded distribution is known

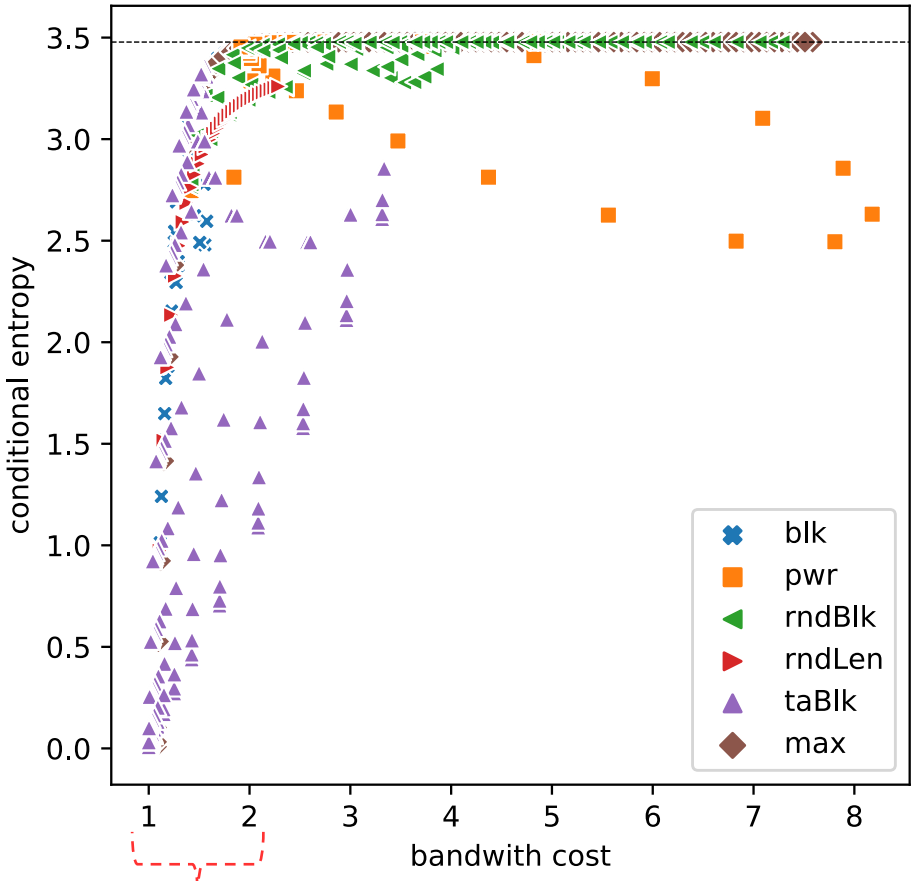
Attacker cost 2

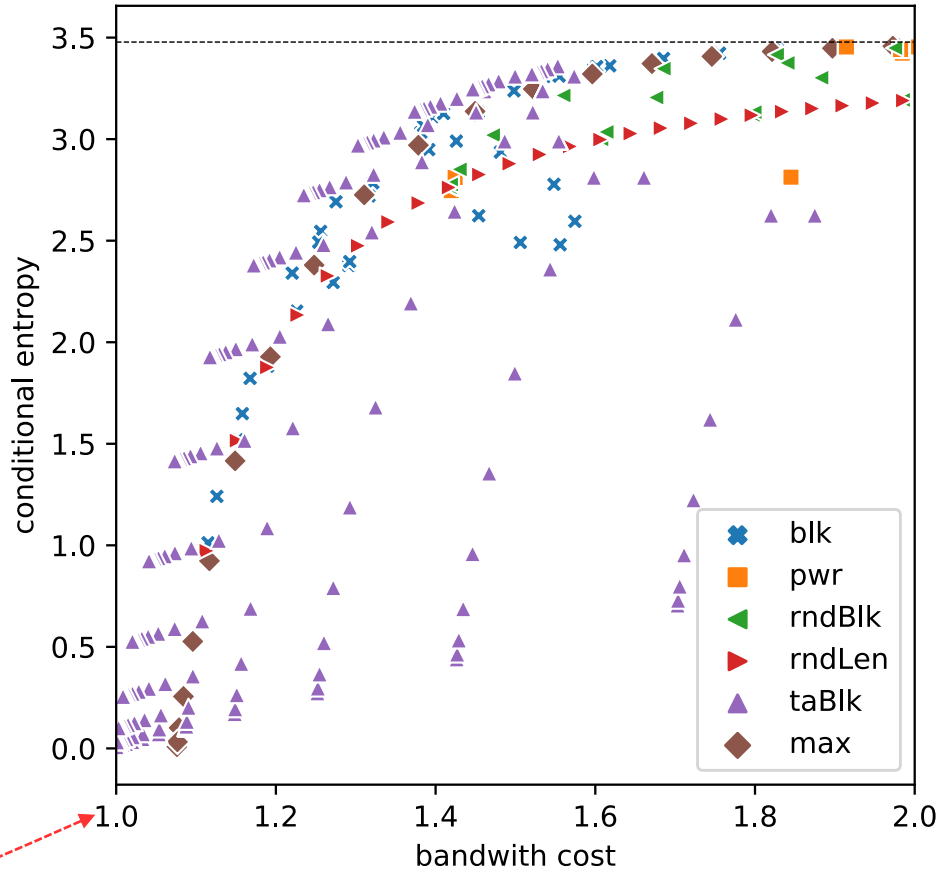
- k-anonymity
- Each person cannot be distinguished from at least k-1 individuals
- Hiding in the crowd

Defender cost

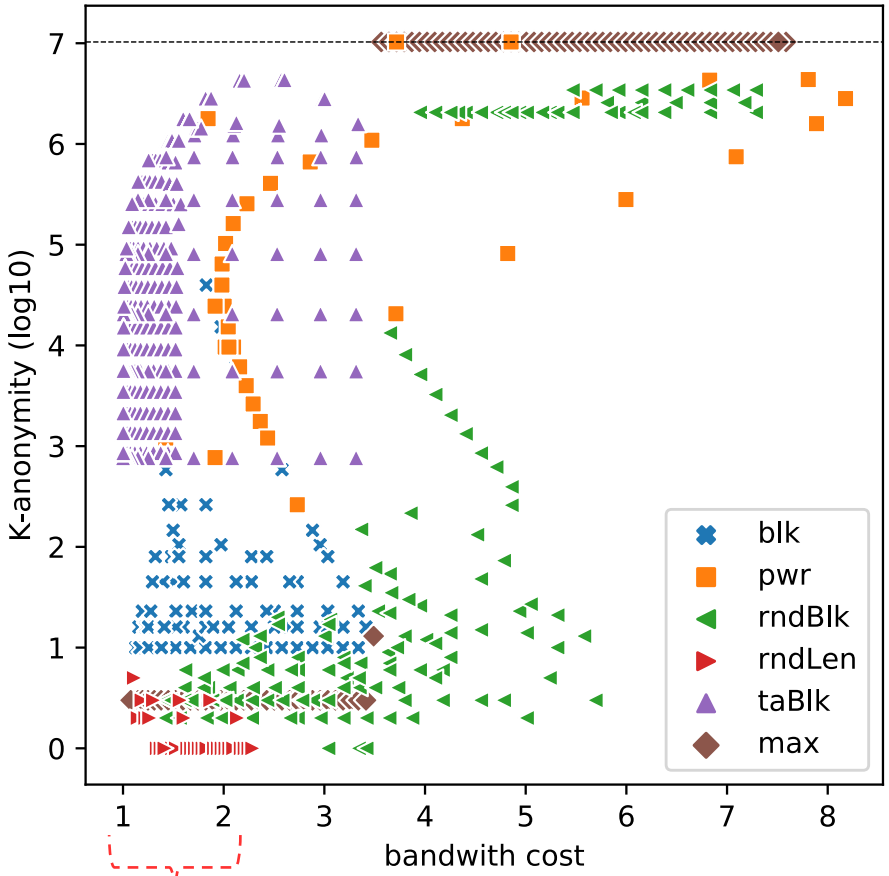
- Bandwidth
- Average increase in message size

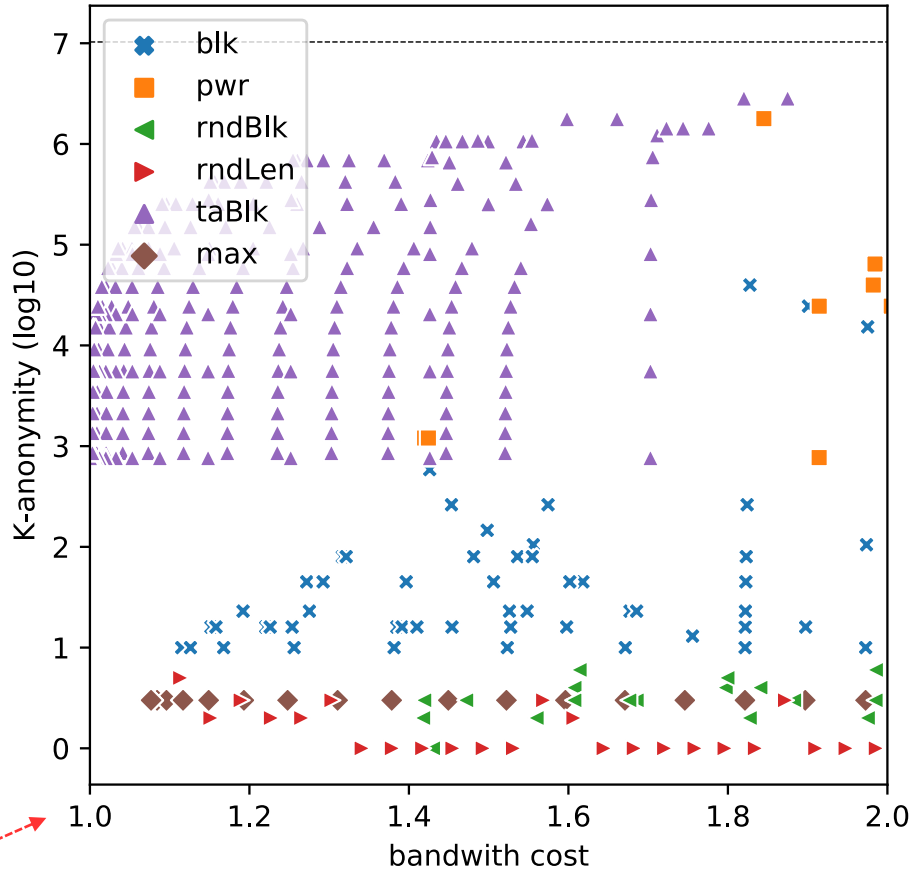
Defender vs attacker cost 1 – Conditional entropy





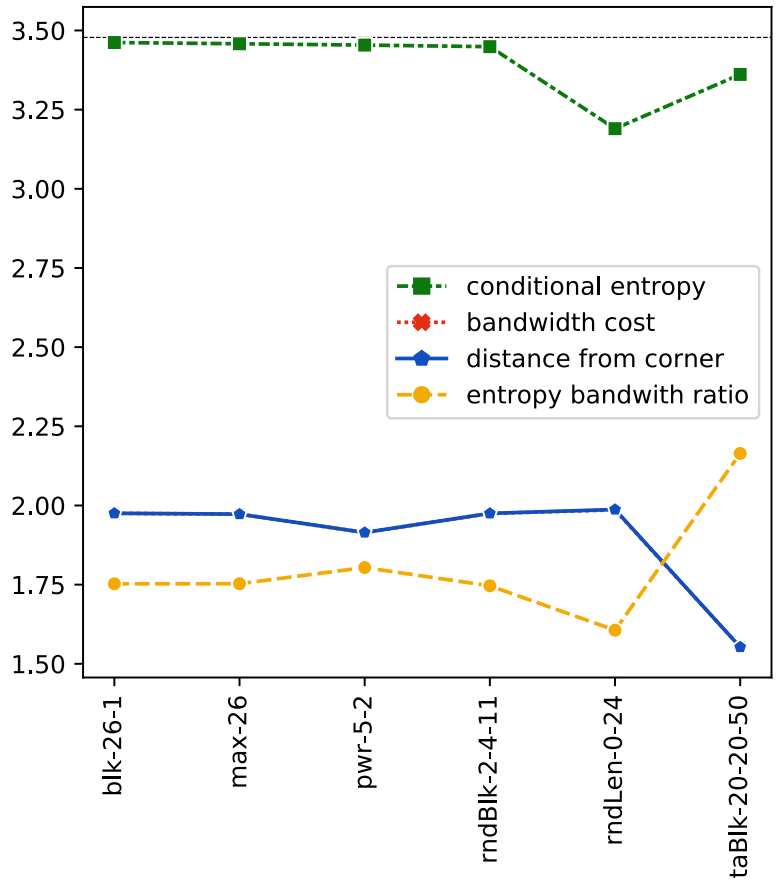
Defender vs attacker cost 2 – k-anonymity



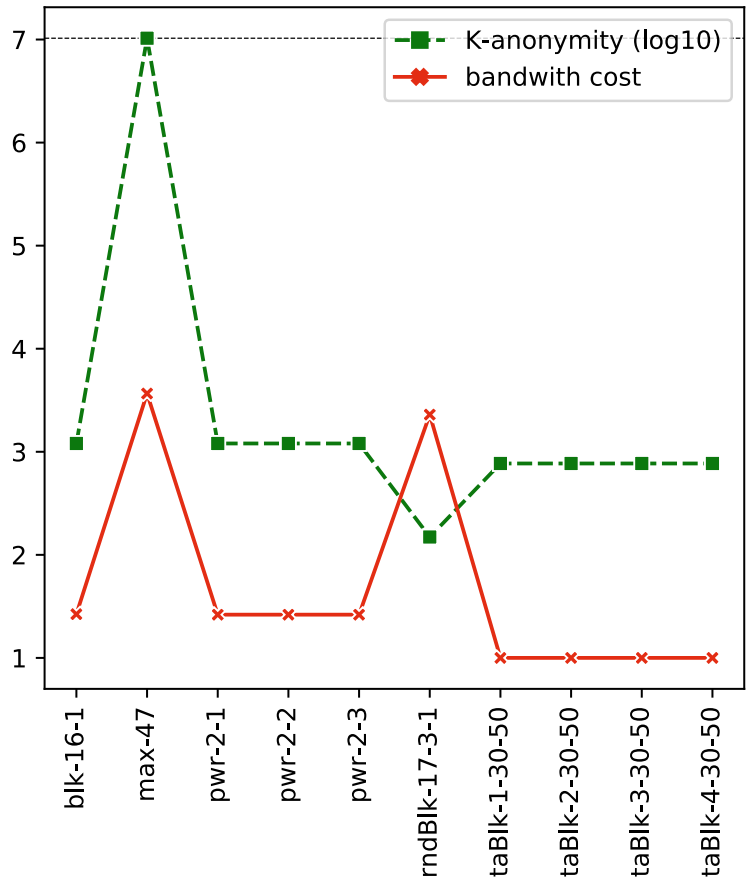


Other observations

For bandwidth-cost <= 2



For k-anonymity >= 100



Standardization suggestions for 3GPP SA3

A focused Work Item (WID) for Rel-18 (or later)

- Introduce a new profile(s) with padding in the current release
- For earlier releases (i.e., 15, 16, 17, ...) add a note, e.g., Profile A and B used with NSI reveal length of username to an attacker. Future profiles introduced must enable use of padding before encryption.

After NIST have standardized PQC algorithms (expected in 2024)

- Introduce a new quantum-safe algorithm.

ericsson.com