



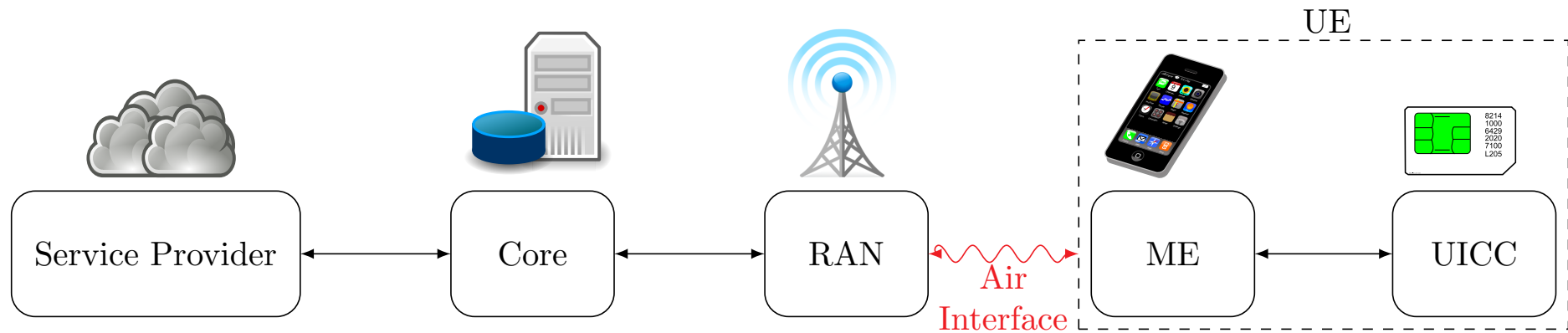
فصل ششم: امنیت در شبکه‌های مخابراتی


امنیت سیستم‌های کامپیوتری

ابوالفضل دیانت

آخرین ویرایش: ۱۹ اردیبهشت ۱۴۰۲ در ساعت ۱۳ و ۱ دقیقه - نسخه 1.0.0

امنیت در شبکه‌های تلفن همراه



معماری کلان شبکه‌های تلفن همراه از پنج گروه عملکردی (Functionality Group) تشکیل شده: 

● UICC (Universal Integrated Circuit Card)

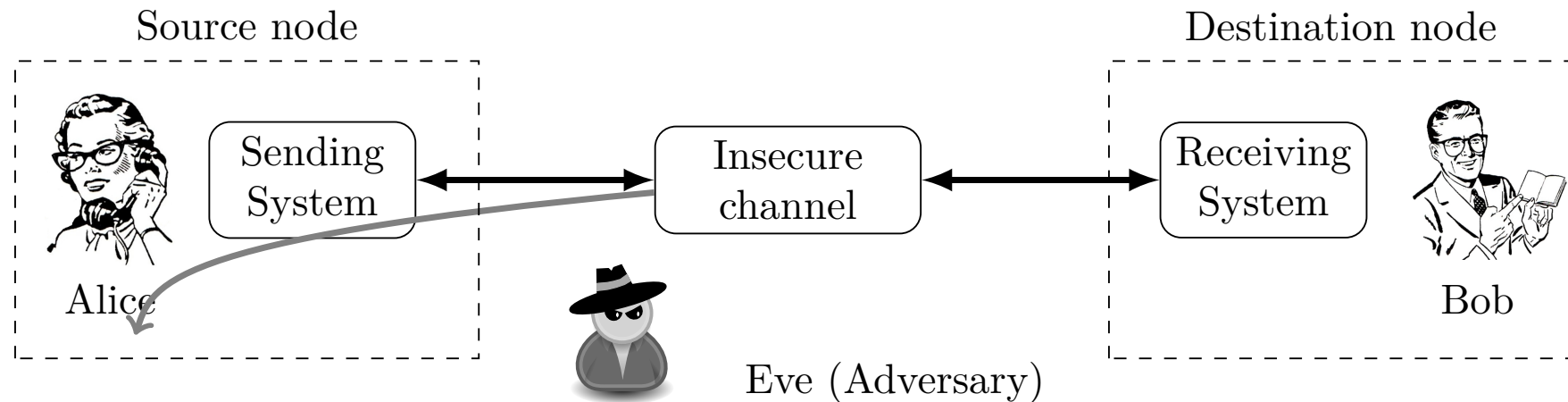
● ME (Mobile Equipment)

● شبکه دسترسی رادیویی (Radio Access Network)

● هسته شبکه (Core Network)

● ناحیه خدمات

چرا به احراز اصالت (Authentication) نیاز داریم؟

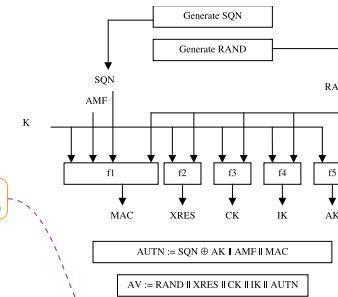
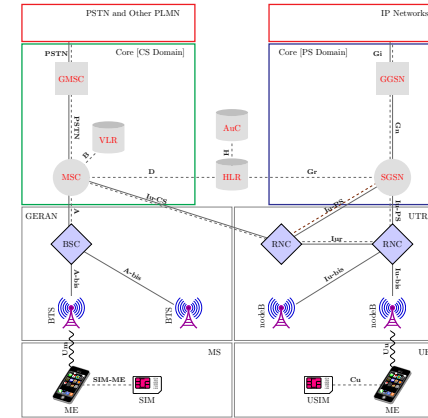
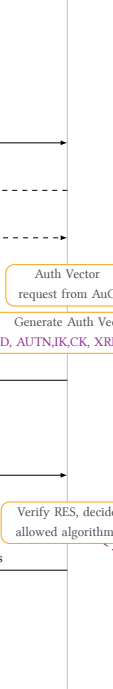
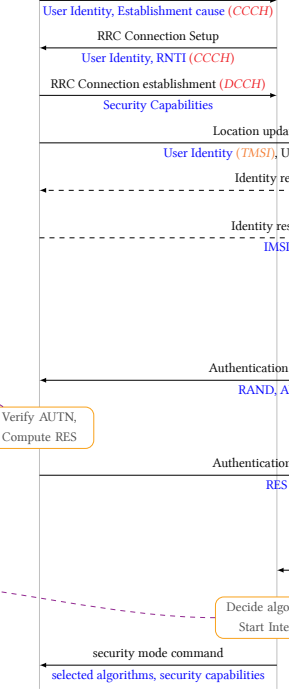
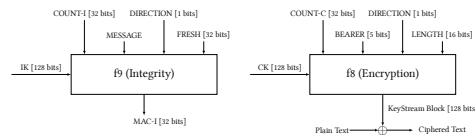
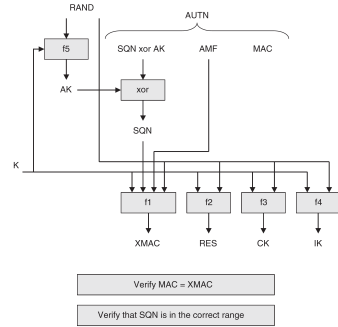
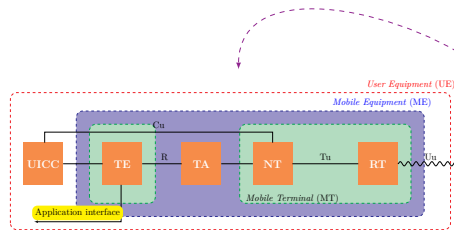


👉 برای محرمانه ماندن پیام می‌بایست از رمزگذاری (Encryption) استفاده کنیم، و برای آن نیاز به کلید داریم.

👉 استفاده از سازوکارهای برقراری کلید (Key Establishment) [۱، فصل ۱۲]:

- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

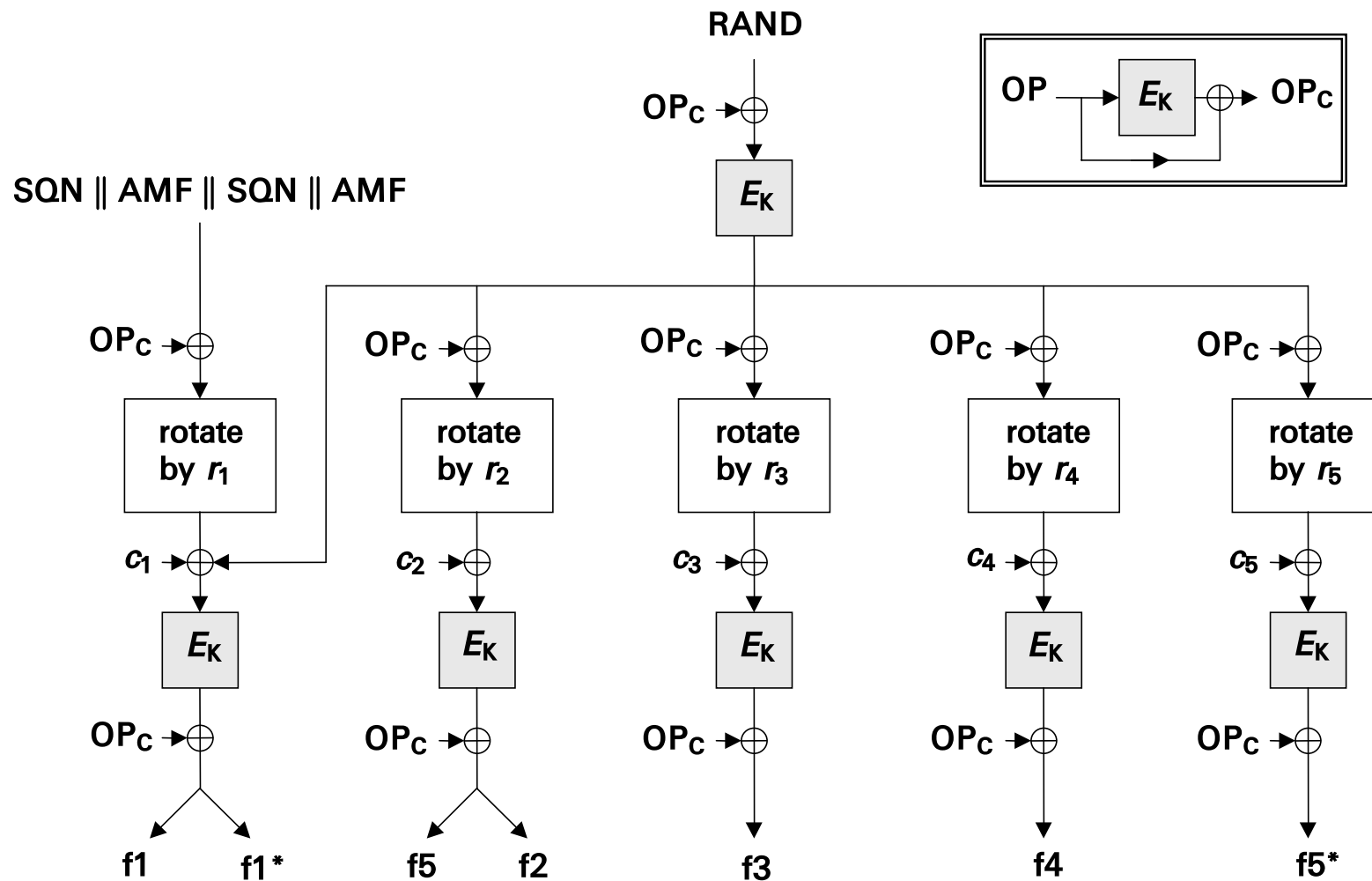
- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.



	RAND	IK	CK	MAC	AK	RES	SQN	AMF
	128	128	128	64	48	32-128	48	16

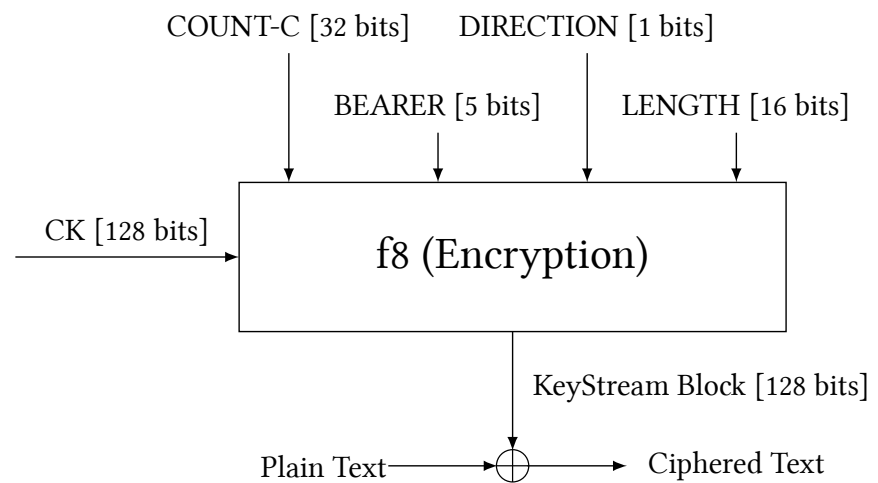
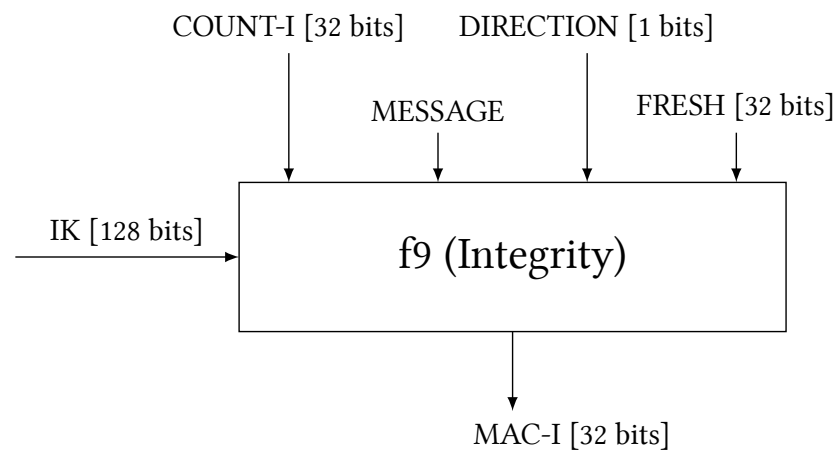
	Integrity	Encryption	Algorithm	UMTS	LTE	Year
UEA 0	Null	✓	✓	✓	✓	—
UEA 1	Kasumi	✓	✓	✓	✓	—
UEA 2	SNOW 3G	✓	✓	✓	✓	2004
UEA 3	AES	✓	✓	✓	✓	—

	Encryption	Integrity
User Plane	✓	✗
Control Plane	✓	✓



الگوریتم‌های تامین امنیت در UMTS (ادامه)

نمای کلی از ورودی‌های توابع f_8 و f_9



- [1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications, CRC Press, 1996.

فهرست اختصارات

واژه‌نامه انگلیسی به فارسی

واژه‌نامه فارسی به انگلیسی