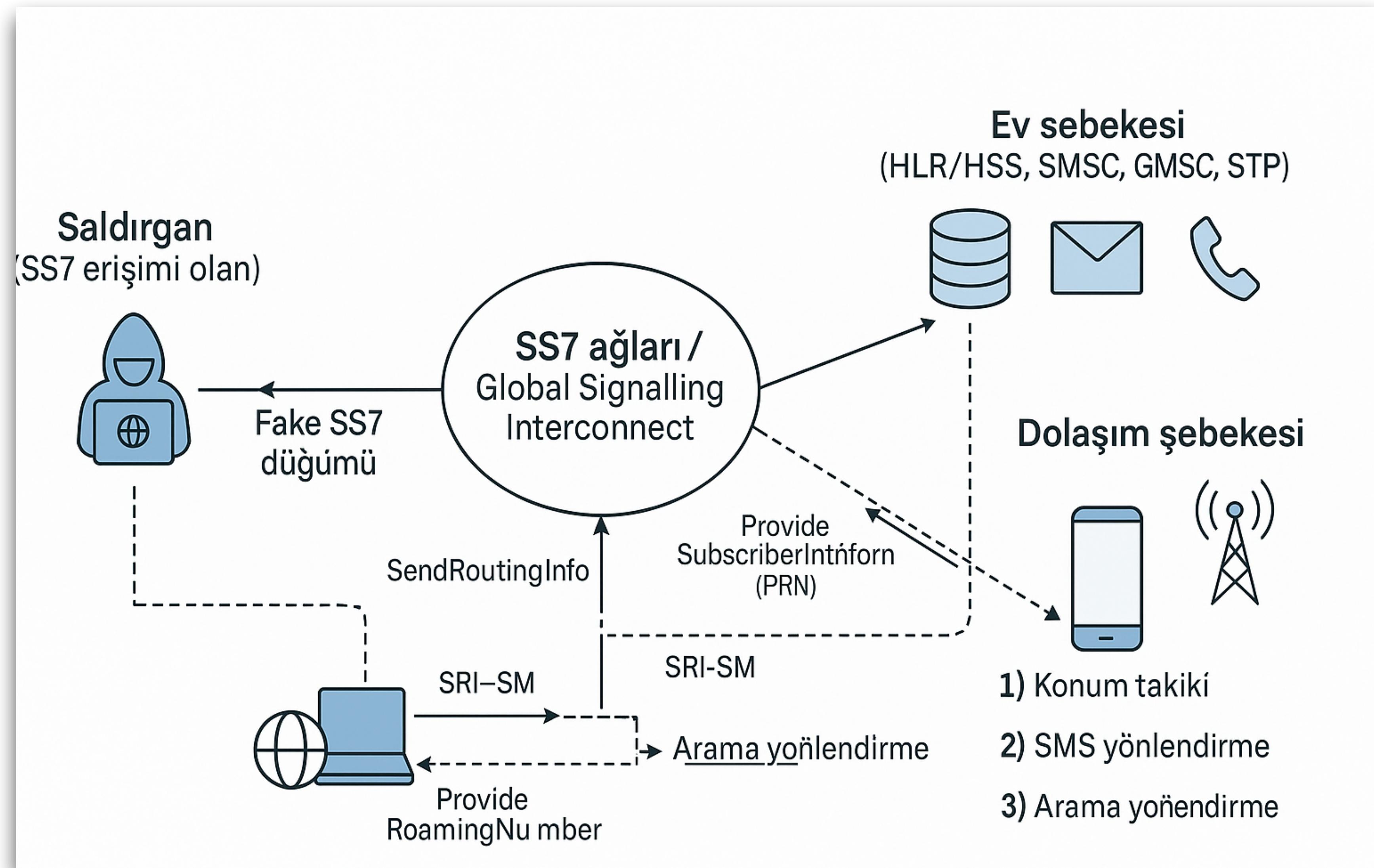


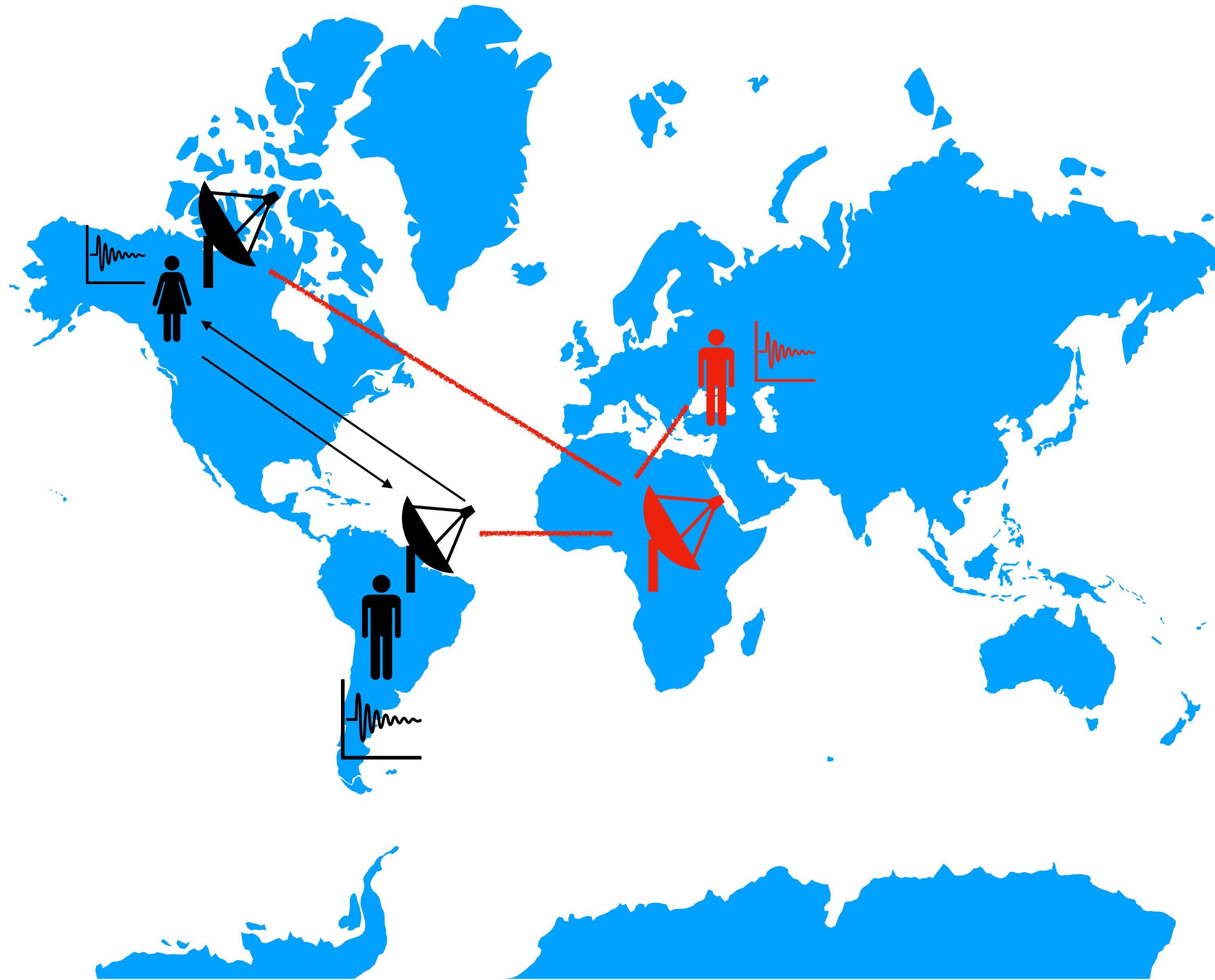
Gembos Teknik Sunu

**Berker Vergi
Giray Aksakal**

16.09.2025



Saldırı Senaryosu



CNN TÜRK

Son Dakika | Türkiye | Video | Finans | Dünya | Ekonomi | Spor | Magazin | Yaşam | Resmi İlanlar

Anasayfa > Türkiye Haberleri

Çin casusluk dosyası CNN TÜRK'te: Tüm bilgiler Çin'deki "Patron"a gitmiş!

20.05.2025 - 11:07 | Güncellenme Tarihi 20.05.2025 - 13:18

[Facebook](#) [Twitter](#) [WhatsApp](#) [Düzenle](#)

İŞTE O HAYALET BAZ İSTASYONU

KAYNAK CNN TÜRK

MİT, sahte baz istasyonu kurarak kişisel bilgilerini ele geçirmeye çalışan 7 kişilik casus şebekesi çökertti. Şüpheliler suçüstü yakalandı, cihazlar Çin merkezli çıktı. CNN TÜRK İstanbul Haber Müdürü Nihat Uludağ, Çin casusları soruşturmasının tüm detaylarını canlı yayında anlattı.

FINTECH FUTURES

[SUBSCRIBE](#)

BANKINGTECH

UK's Metro Bank hit by SS7 attack

Known telecommunications vulnerability exploited to target bank accounts.

Antony Peyton | February 1, 2019 | 2 Min Read

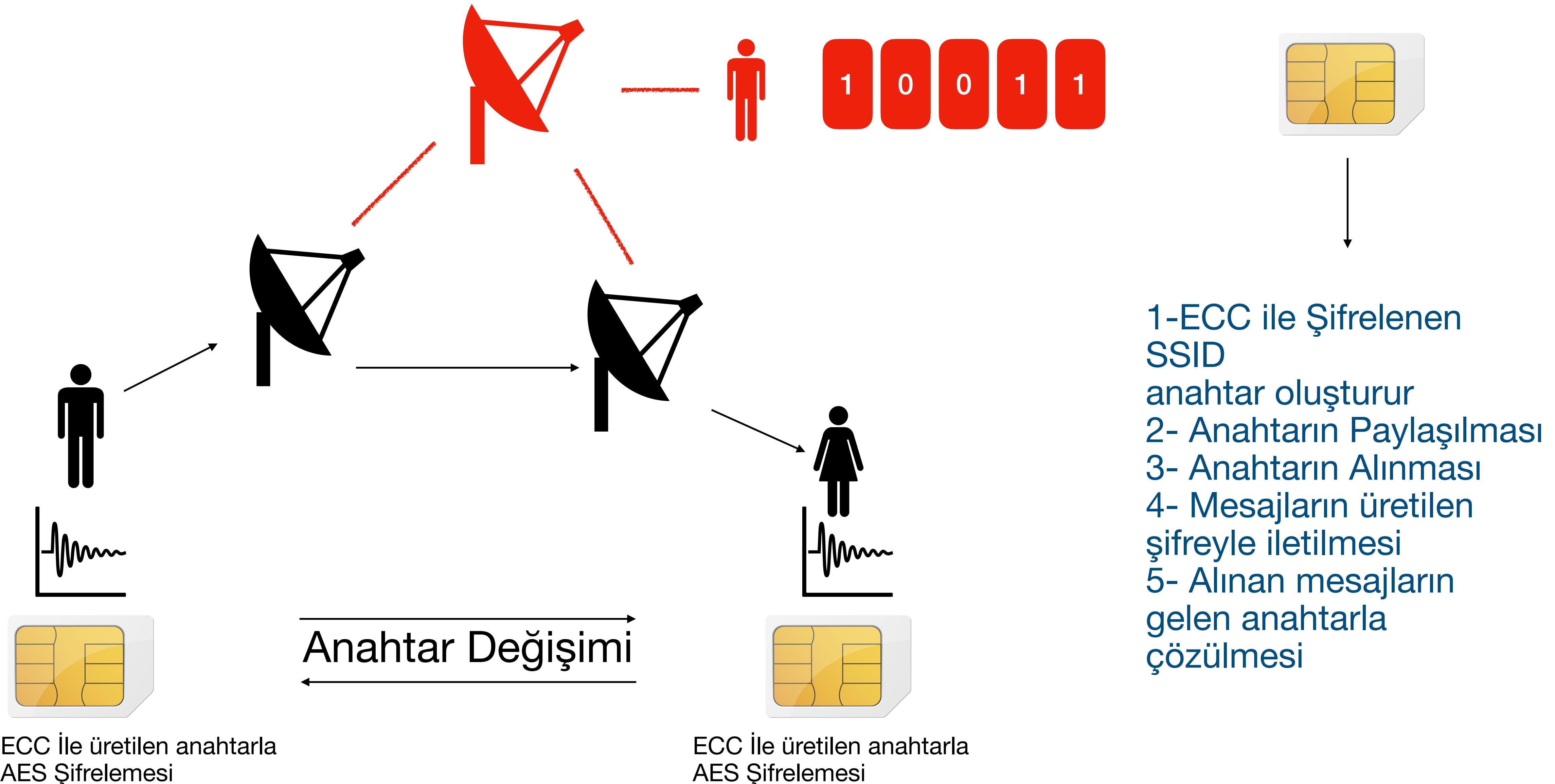
UK-based [Metro Bank](#) has suffered an SS7 attack as the financial world can't escape the attention of criminals.

According to [Motherboard](#), Metro Bank confirmed to the publication it had faced such an assault.

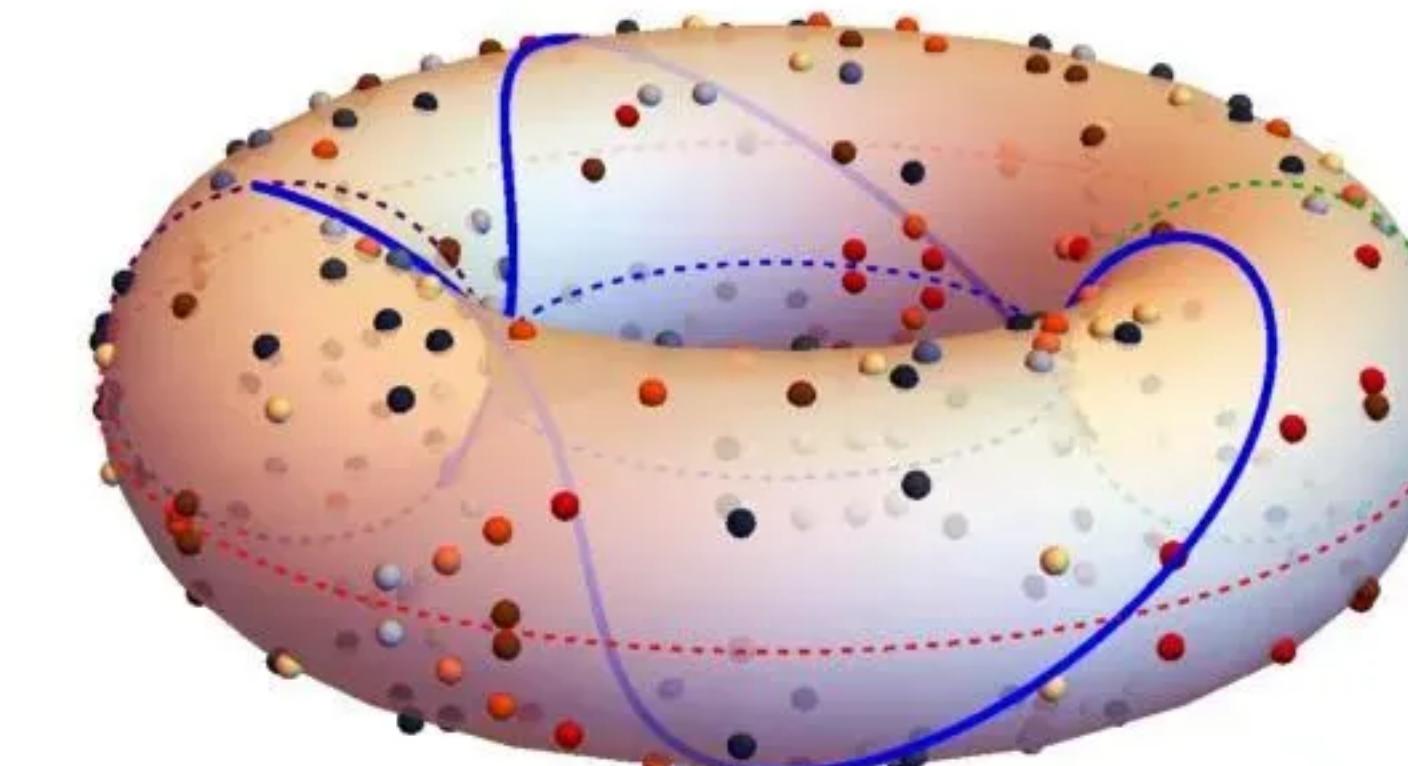
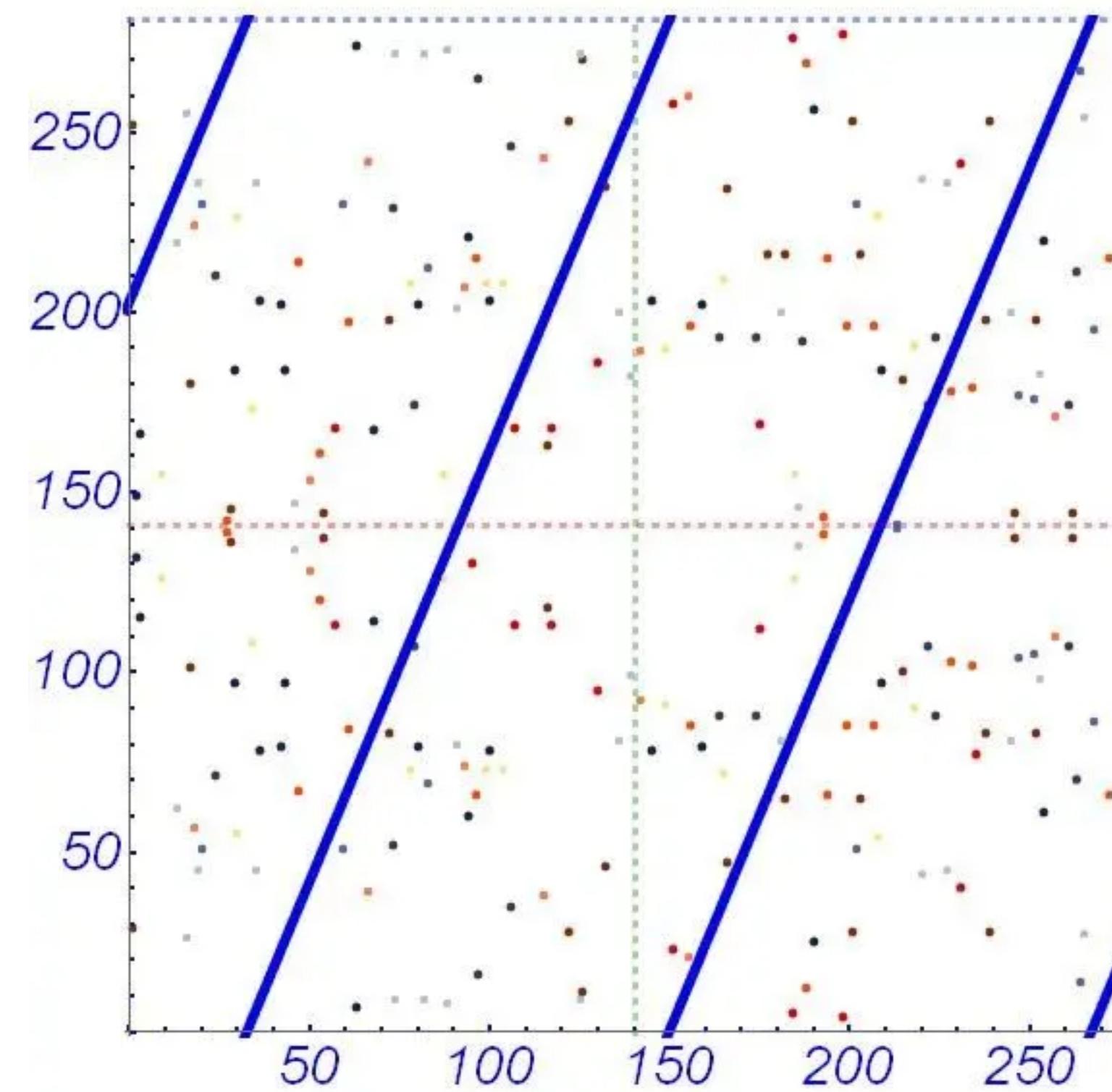
Hackers have long exploited flaws in SS7, a protocol used by telecom companies to coordinate how they route texts and calls around the world.

Those who exploit SS7 can potentially track phones across the other side of the planet, and intercept text messages and phone calls without hacking the phone itself.

Güvenli Senaryo

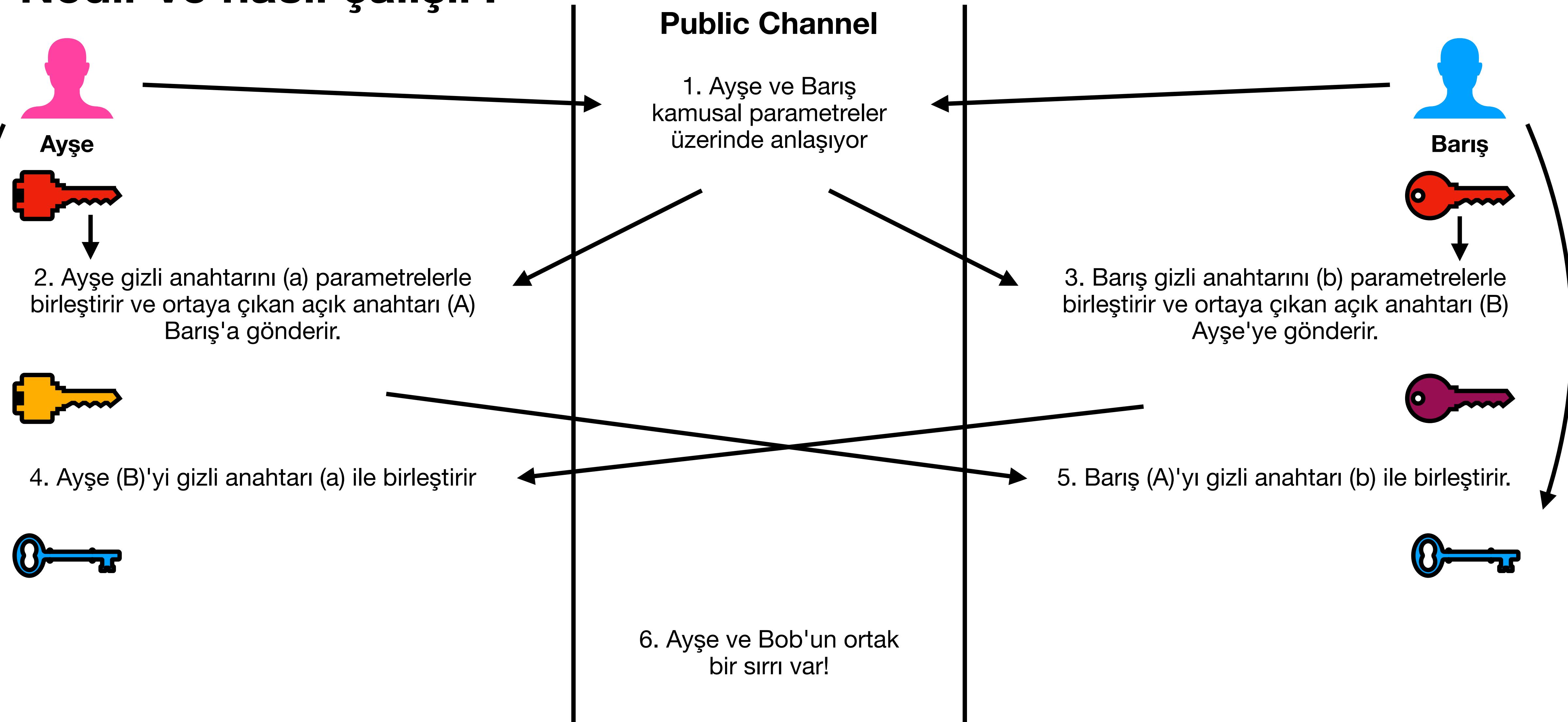


Elliptic Curve Algoritması



Diffie-Hellman Anahtar Değişim Algoritması

Nedir ve nasıl çalışır?



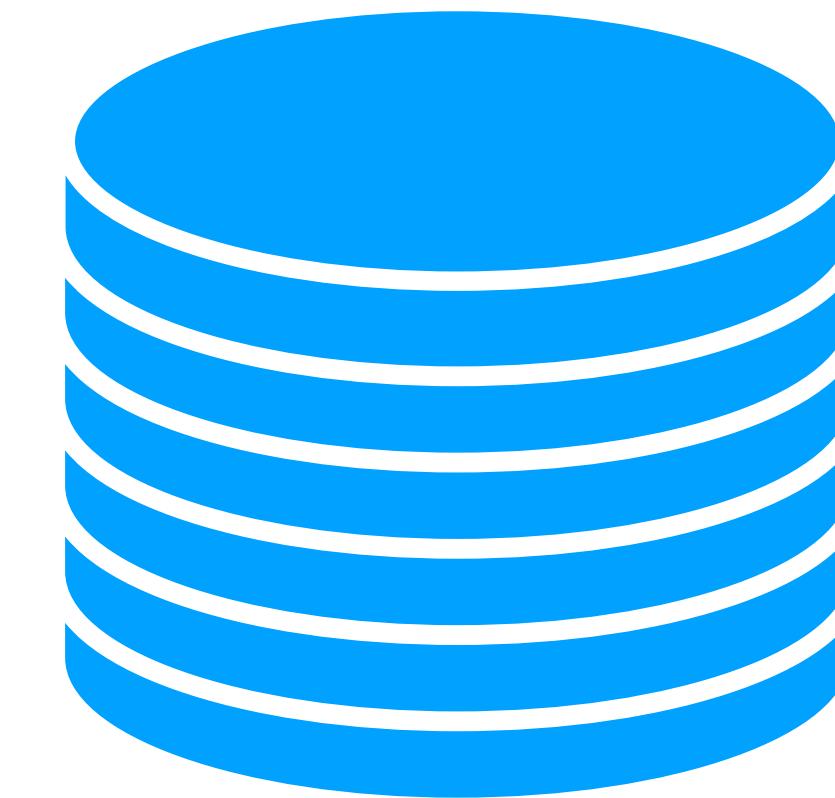
Yapılacak Sistem



SIM Applet



STK Uygulaması



Log Sistem Websitesi

İhtiyaçlar

SIM Kartı



İzinler



STK Uygulaması



Gönderen — UICC/SIM A

1) GEN_KEYPAIR (P-256)

SIM A içinde uzun süreli kimlik anahtarı oluşturur; sadece public key dışarı çıkar.

2) ECDH_Ephemeral

Her mesaj için geçici (ephemeral) ECDH anahtar çifti üretir (PFS sağlar).

3) Dizin/Key-Exchange

Karşı tarafın public key'ini dizinden BIP ile alır veya ilk kurulumda SMS ile değiş tokuş eder.

4) ECDH_DERIVE

Ortak sırrı $Z = \text{ECDH}(\text{ephemeral_A_priv}, \text{pub_B})$ olarak türetilir.

5) KDF_EXPORT (HKDF-SHA-256)

Salt + info ile SMS için şifreleme (K_{enc}) ve bütünlük (K_{mac}) anahtarları türetilir.

6) ENCRYPT_SMS (AES-GCM)

Mesaj: Header(counter, frag, senderKeyID) + plaintext → AES-GCM ile ciphertext + tag.

7) SEND SHORT MESSAGE (STK)

UDH + 23.048 secured packet + parçalama ile SMS gönderilir.

Alicı — UICC/SIM B

1) SMS-PP Data Download

SMS doğrudan SIM B'ye teslim edilir (ME üzerinden).

2) DECRYPT_SMS (AES-GCM)

Header'dan nonce ve counter okunur; AES-GCM ile doğrulama ve çözme yapılır.

3) ECDH_DERIVE

$Z = \text{ECDH}(\text{ephemeral_A_pub}, \text{priv_B})$ ile eş ortak sırrı türetilir.

4) KDF_EXPORT

HKDF ile aynı anahtar materyali çıkarılır; tag eşleşirse bütünlük doğrulanır.

5) STK DISPLAY TEXT / BIP

Mesaj kullanıcıya gösterilir veya BIP/Open Channel ile uygulamaya aktarılır.