Implementation of Elliptic Curve Cryptography in Flood and Environmental Monitoring IoT Systems

Usman Adeel
School of Computing, Engineering and Digital Technologies, Teesside University, UK

Abstract

Introduction & Context: Traditional infrastructure is shifting globally toward decentralized Sustainable Drainage Systems (SuDS), as seen in the **Stanley SuDS Project**. These operations rely heavily on battery-powered edge sensor arrays (e.g., radar river-gauge elements, ultrasonic gully monitors) to measure critical environmental variables and prevent flash flood disasters.

This telemetry uses a split topology: short-range **Bluetooth** links handle manual configuration, while wide-area **5G cellular backhaul networks** route raw data directly to **AWS IoT Core** cloud instances for public emergency warning dashboards.

Problem Statement: Because these outdoor systems are deployed in remote, unmonitored geographic catchments, they face a severe cyber-physical attack surface. Malicious actors can capture field hardware to extract static memory signatures or execute **data injection spoofing**. For example, injecting a normal depth metric during an active storm can delay regional emergency evacuations.

Securing these channels using standard enterprise public-key ciphers like **RSA** is impossible due to hardware constraints. Heavy ciphers require massive computational overhead, which causes network latency and quickly drains the batteries of remote sensors.

Proposed Solution: Lightweight ECC: We evaluate **Elliptic Curve Cryptography (ECC)** as a lightweight public-key framework. Built on the algebraic structure of cubic curves over finite fields

$$y^2 = x^3 + ax + b$$

ECC derives its strength from the **Elliptic Curve Discrete Logarithm Problem (ECDLP)**. Because solving the scalar multiplication.

$$Q = k \cdot G$$

is computationally difficult for adversaries, ECC provides strong cryptographic security using exceptionally small keys.

End-to-End Handshake Pipeline:

1. **Agreement:** The field microcontrollers and AWS IoT Core select a standard curve (e.g., Secp256r1).
2. **Key Generation:** Nodes generate public/private key pairs (Q, k) directly on the edge chips.
3. **Secret Exchange:** Nodes establish a temporary session key across the 5G backhaul via an Elliptic Curve Diffie-Hellman (ECDH) handshake.
4. **Payload Encryption:** Telemetry readings are encrypted using a lightweight symmetric algorithm (AES-128) and uploaded.
5. **Cloud Processing:** The AWS IoT gateway decrypts and authenticates the packets using its cloud private key.

Quantitative Performance Comparison: ECC scales efficiently, providing strong security while keeping keys compact:

- **Key Length Correspondence:** A compact **256-bit ECC key** delivers the exact same security margin as a large **3072-bit RSA key**. This reduces payload size by **12x**.
- **Execution Latency Multipliers:** For standard 128-bit symmetric protection profiles, ECC operates approximately **10 to 100 times faster** than standard RSA alternatives during key generation.
- **Resource Optimization:** ECC uses significantly less static RAM and ROM. This preserves memory for data logging on small microcontrollers and reduces processing power to extend sensor battery lifespans.

Strategic Recommendations & Conclusion: To protect environmental telemetry networks, system architectures should incorporate the following security measures:

- **Physical Hardware Hardening:** Microcontrollers should use anti-tamper housings and cryptographic coprocessors to prevent physical extraction attacks.
- **Network-Side Intrusion Mitigation:** Field gateways must monitor network traffic to detect anomalies, such as repetitive authentication attempts or unusual data spikes, mitigating battery-exhaustion DoS exploits.
- **Quantum Proofing:** Future designs should incorporate post-quantum hybrid ciphers to protect long-term environmental datasets against emerging decryption risks.

Conclusion: Implementing Elliptic Curve Cryptography balances processing constraints with robust data security. It provides reliable end-to-end data integrity and origin authentication for critical flood safety workflows, without shortening the operational lifespan of remote field sensors.