Practical Invalid Curve Attacks on TLS-ECDH

Tibor Jager, Jörg Schwenk, Juraj Somorovsky
Horst Görtz Institute for IT Security
Ruhr University Bochum

@jurajsomorovsky

Recent years revealed many attacks on TLS…

- ESORICS 2004, Bard: The Insecurity of SSL to Chosen Plaintext Attacks

2011 BEAST

- Eurocrypt 2002, Vaudenay: Security Flaws Induced by CBC Padding—Applied to SSL, IPSEC, WTLS

2013/14 POODLE, Lucky13

- Crypto 1998, Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1

2014 at USENIX Sec

Another “forgotten” attack

- Invalid curve attack
- Crypto **2000**, Biehl et al.: Differential fault attacks on elliptic curve cryptosystems
- Targets elliptic curves
  - Allows one to extract private keys

- Are current libraries vulnerable?

Overview

1. Elliptic Curves
2. Invalid Curve Attacks
3. Application to TLS ECDH
4. Evaluation
5. Bonus Content

Elliptic Curve (EC) Crypto

- Key exchange, signatures, PRNGs
- Many sites switching to EC
- Fast, secure
  - openssl speed rsa2048 ecdhp256
  - ECDH about **10** times faster

Elliptic Curve

- Set of points over a finite field

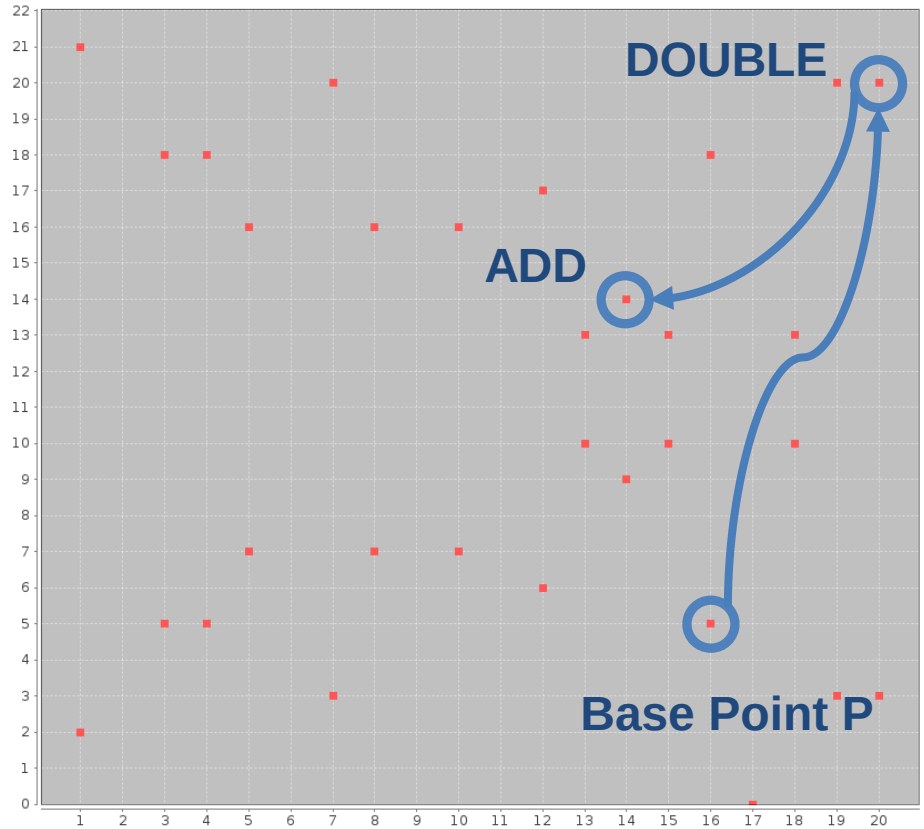
$$E:\ y^2 = x^3 + ax + b \bmod p$$

- Operations: ADD and DOUBLE
- Example:

$a = 9$

$b = 17$

$p = 23$



Elliptic Curve Diffie Hellman (ECDH)

Client

Secret q

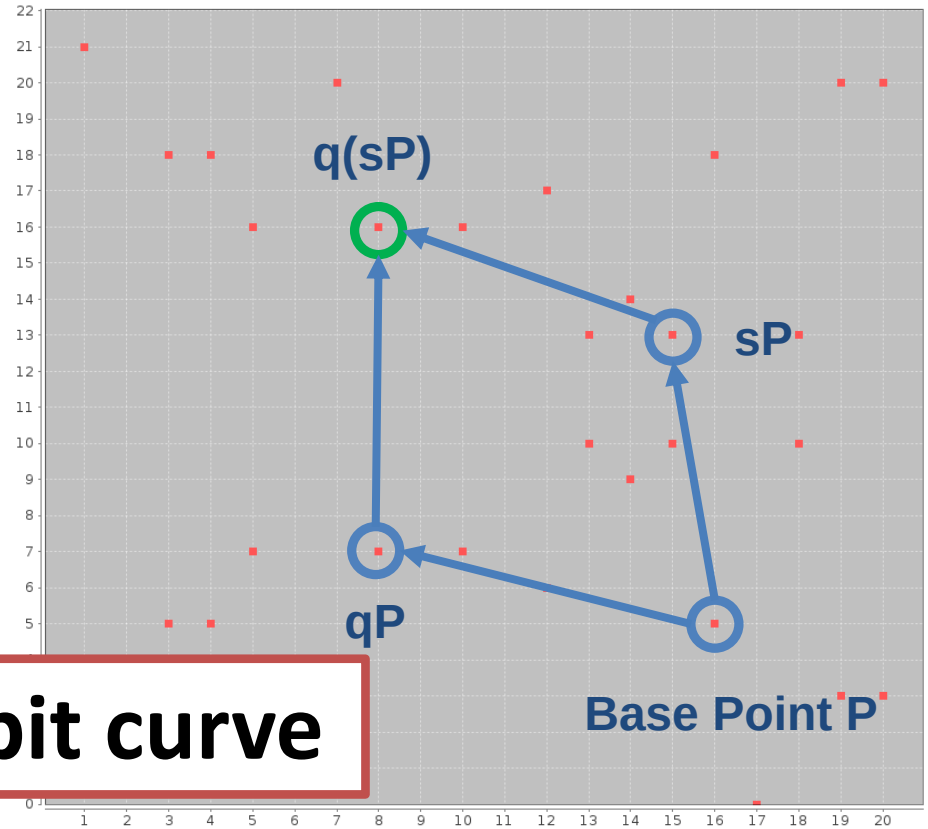
Server

Secret s

$\xrightarrow{\quad qP \quad}$

$\xleftarrow{\quad sP \quad}$

Shared secret: s(qP) = q(sP)



Small 5 bit curve

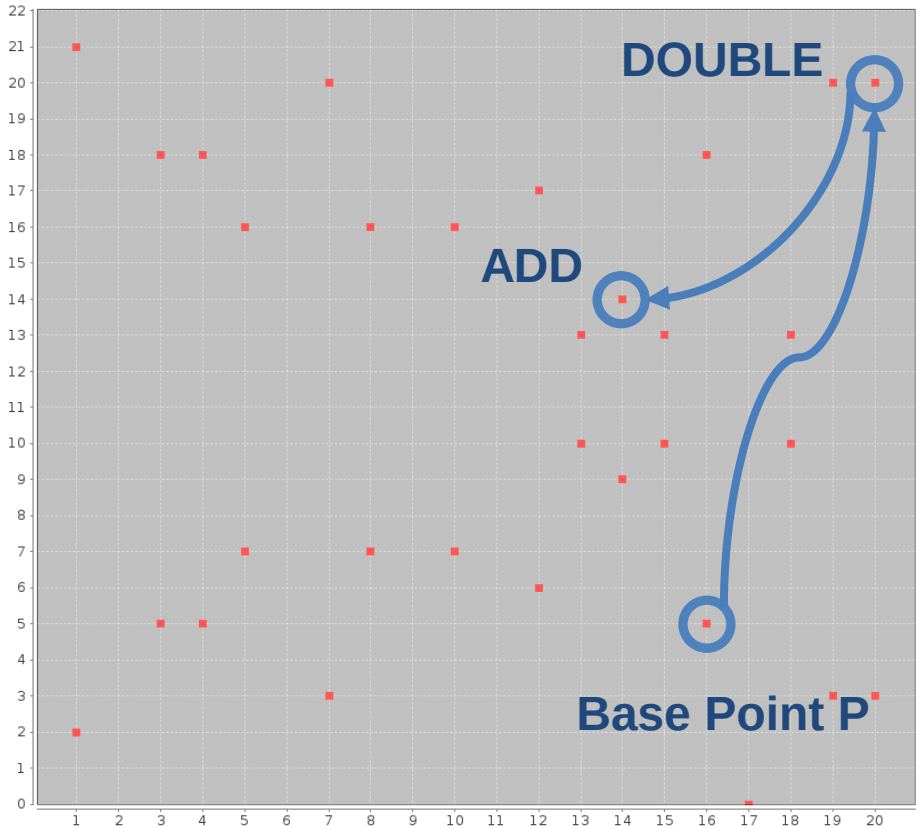
Elliptic Curves in Crypto

- Have to be chosen very carefully: **high** order
  - $\underbrace{\text{P -> ADD -> ADD -> … -> ADD -> P}}_{\textbf{order}}$

- Predefined curves

  > 256 bits

  NIST, brainpool, …



Overview

1. Elliptic Curves
2. Invalid Curve Attacks
3. Application to TLS ECDH
4. Evaluation
5. Bonus Content

Invalid Curve Attack

- What if we compute with a point P’ outside of curve E?
- P’ can have a small order

- Example:
  - E’ with 256 bits
  - P’ generates 5 points

Invalid Curve Attack

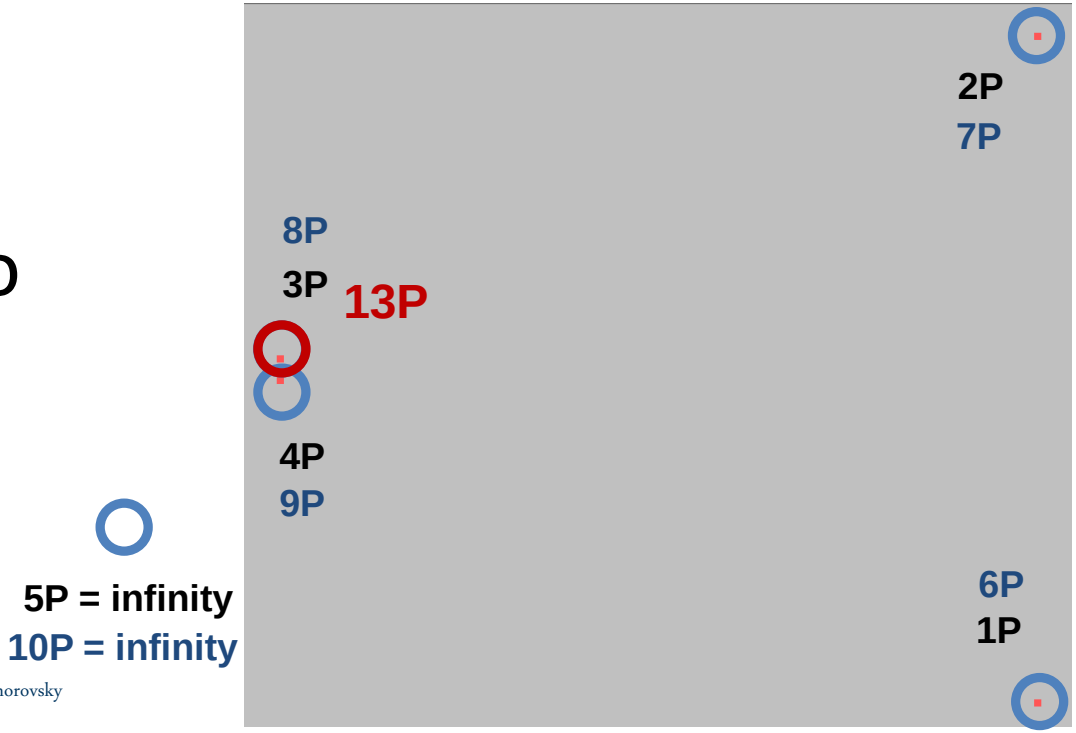
- What is the problem?
- Shared secret has only **5** possible values!

- Example

Server Secret s = 13

- Server attempts to multiply sP

$$3 = s \bmod 5$$



Invalid Curve Attack

- What is the problem?
- Shared secret has only **5** possible values!
- We can compute:

$$s_1 = s \; mod \; 5$$

$$s_2 = s \; mod \; 7$$
$$s_3 = s \; mod \; 11$$
$$s_4 = s \; mod \; 13$$

- Compute ***s*** with CRT

Overview

1. Elliptic Curves
2. Invalid Curve Attacks
3. Application to TLS ECDH
4. Evaluation
5. Bonus Content

Transport Layer Security (TLS)

- EC since 2006
- **Static** and ephemeral
- TLS server initialized with an EC certificate
  - Server has EC key

TLS ECDH

TLS Server

ClientHello →

ServerHello

Certificate: sP

← **ServerHelloDone**

ClientKeyExchange: qP →

Premaster secret
Used to compute keys

$$pms = s(qP) = q(sP)$$

ChangeCipherSpec

(Client-) Finished: →

ChangeCipherSpec

← **(Server-) Finished**

Invalid Curve Attack on TLS

1. Generate invalid points with order $p_i = 5, 7, 11, 13 \ldots$
2. Use TLS server to get equations $s = s_i \; mod \; p_i$
3. Compute CRT to get secret key ***s***

Overview

1. Elliptic Curves
2. Invalid Curve Attacks
3. Application to TLS ECDH
4. Evaluation
5. Bonus Content

Evaluation

- 8 libraries
  - **Bouncy Castle v1.50**, Bouncy Castle v1.52, MatrixSSL, mbedTLS, OpenSSL, Java NSS Provider, **Oracle JSSE**, WolfSSL
- 2 vulnerable
- Practical test with NIST secp256r1
  - Most commonly used [Bos et al., 2013]

Evaluation: Bouncy Castle v1.50

- Vulnerable
  - 74 equations
  - 3300 real server queries

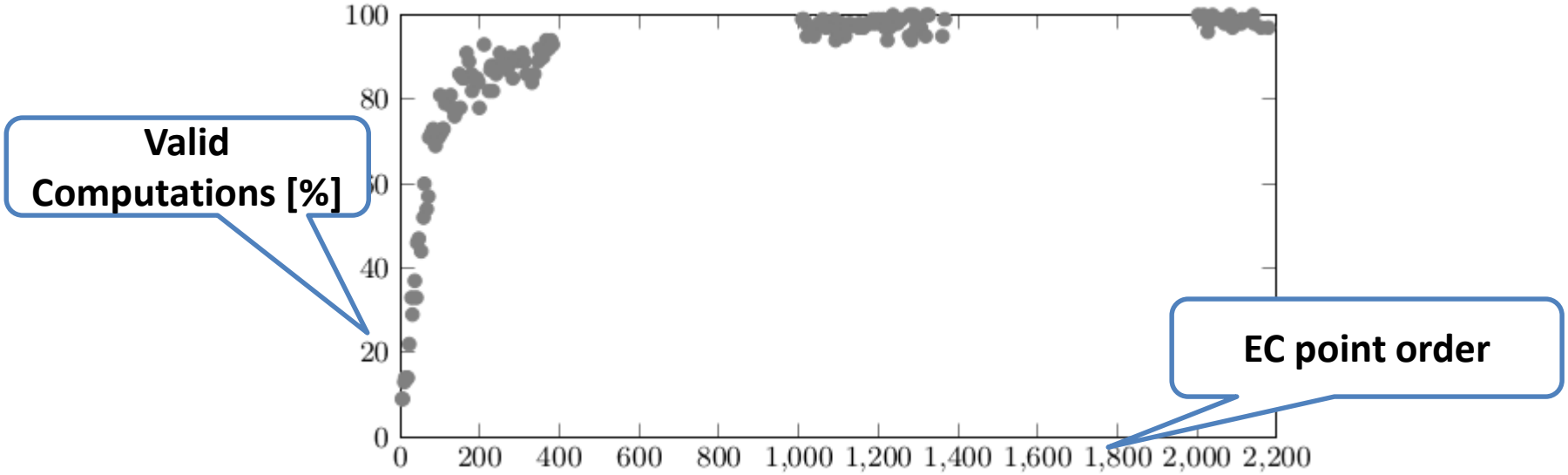
Evaluation: JSSE

- Java Secure Socket Extension (JSSE) server accepted invalid points

- However, the direct attack failed

Evaluation: JSSE

- Problem: invalid computation with some EC points



- Attack possible:
  - 52 equations, 17000 server requests

Impact

- Attacks extract server private keys
- Huge problem for Java servers using EC certificates
  - For example Apache Tomcat
  - Static ECDH enabled per default
- Key revocation

- Not only applicable to TLS
  - Also to other Java applications using EC

Overview

1. Elliptic Curves
2. Invalid Curve Attacks
3. Application to TLS ECDH
4. Evaluation
5. Bonus Content

What's next?

- Hardware Security Modules
- Devices for storage of crypto material

Attacker Model in HSM Scenarios

- Key never leaves HSMs

dec (C)

m

Attacker Model in HSM Scenarios

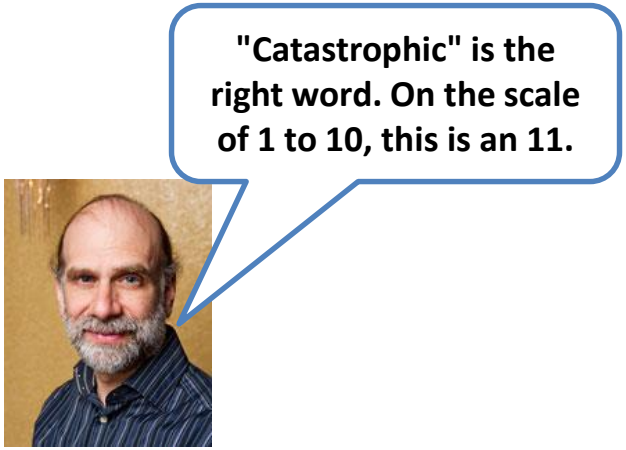
- Key never leaves HSMs

How about Invalid Curve Attacks?

- CVE-2015-6924 (with Dennis Felsch)
- Utimaco HSMs vulnerable
- < 100 queries to extract a key

- Only possible thanks to our cooperation
  - Provided sample code, fast fix
- Utimaco HSM is FIPS certified

- Other devices?



Conclusion

- Old attacks still applicable, we can learn a lot from them
- Bouncy Castle, JSSE and Utimaco broken
- More tools / analyses of crypto applications needed

- https://github.com/RUB-NDS/EccPlayground
- http://web-in-security.blogspot.de/
- http://safecurves.cr.yp.to/