SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

Pairing Based Cryptography の Invalid Point 攻撃に関して
On the Invalid Point Attack of Pairing Based Cryptography

星野 文学* 高橋 元 * 小林 鉄太郎 *
Fumitaka Hoshino Gen Takahashi Tetsutaro Kobayashi

あらまし 暗号系に不正な入力が行われた時に, 暗号系がどのような挙動を示すかは実装に強く依存する. そのため実装の詳細を抽象した暗号プロトコルに於いては, 入力は何らかの集合に収まっていると仮定し, 入力が集合に含まれなかった場合の系の挙動は捨象しがちである. Lim らは不正な入力を用いて離散対数に基づく暗号系攻撃する Small Subgroup 攻撃を提案した [LL97]. また Antipa らは不正な楕円曲線上の点を用いて楕円曲線暗号系を攻撃する Invalid Curve 攻撃を提案した [ABMSV03]. 本論文では Antipa らの Invalid Curve 攻撃を pairing に基づく暗号系 (PBC) へ拡張した Invalid Point 攻撃を考察し, pairing の型による, 対策コストの軽減を検討する.

Keywords: Weil Pairing, Invalid Point Attack, Pairing Based Cryptography

1 はじめに

不正な入力が行われた時に系がどのような挙動を示すかは実装に強く依存する問題である. その為, 現実の系を抽象した暗号プロトコルに於いては, 入力は何らかの集合に収まっていると仮定し, 入力が集合に含まれなかった場合の系の挙動は捨象しがちである.

例えば DH 鍵交換のような離散対数問題に基づく暗号プロトコルは $\mathbb{Z}/p\mathbb{Z}^*$ の真部分群である素数位数巡回群 $\langle g\rangle$ を使って設計される. 演算コストやデータ長を抑える為に, g の位数は $\mathbb{Z}/p\mathbb{Z}^*$ の位数より幾分小さく設計される事が多い. このような場合, もし 系が入力 $\bar{h} \in \mathbb{Z}/p\mathbb{Z}^*$ に対して, $\bar{h} \in \langle g\rangle$ であるか否かに頓着せず暗号プロトコルを実行すると秘密を漏らしてしまう事がある. 特に $\mathbb{Z}/p\mathbb{Z}^*$ が位数の小さい部分群を多く含めば, 攻撃者は多くの秘密を得ることが出来る. Lim らは この事実を利用した Small Subgroup 攻撃を提案した [LL97]. また Antipa らは, 楕円曲線暗号対する攻撃として, 意図している楕円曲線とは異なる楕円曲線上の点を入力し系から秘密を取り出す Invalid Curve 攻撃 [ABMSV03] を提案した. こうした 不正な値に対する脆弱性は Fault 攻撃が許される環境ではより深刻な問題となり得る.

もし暗号プロトコルが入力 h に対し $h \in G$ を仮定するるなら, 現実の系に於いては $\bar{h} \notin G$ なる入力 $\bar{h} \in \{0,1\}^*$ に対して, 攻撃されないような系の挙動を定義しておかなくてはならない. また暗号プロトコルが出力 h に対し $h \in G$ を仮定するるなら, Fault 攻撃を考慮した現実の系に於いては, 系の内部状態の情報を含むような $\bar{h} \notin G$ なる $\bar{h} \in \{0,1\}^*$ を出力すべきではない. 従って注意深く設計された暗号系 G に於いては, $h \in \{0,1\}^*$ に対して $h \in G$ か否かを効率的に判定するアルゴリズムが必ず用意される. さらに $h \in G$ 判定アルゴリズムがどのくらい効率的かは, 暗号プロトコルの設計に大きな影響を与える.

ところで 近年 Pairing Based Cryptography (PBC) が注目されている [SOK00, Jou00, BF01, BLS02, MSK02, BB04a, BB04b]. 本稿では PBC の設定に於いて不正な値が系にどのような影響を与えるかを考察し pairing の型に従い対策コストの軽減を検討する.

2 準備

最も単純な攻撃のモデルとして, 次のものを考える.

* NTT 情報流通プラットフォーム研究所, 〒 239-0847 神奈川県横須賀市光の丘 1-1, NTT Information Sharing Platform Laboratories, 1-1 Hikarinooka Yokosuka-Shi Kanagawa 239-0847 Japan

– $\langle g \rangle$ を十分大きな素数位数巡回群とし, その位数を ℓ とし, g をその生成元とする.
– $\alpha \in \mathbb{Z}/\ell\mathbb{Z}$ は攻撃者に対して (計算量的に) 秘匿されているとする.
– $h \in \langle g \rangle$ を入力すると h^α を出力するオラクルが攻撃者に与えられているとする.
– 攻撃者は $\log \ell$ の多項式回だけオラクルにクエリを発行できる.

離散対数や pairing に基づく鍵交換や署名を実現する暗号プロトコルの安全性を解析する際, あるいは耐タンパとされる装置への ある種の Fault 解析を行う際には, このような攻撃モデルは自然に与えられる事が多い. 現実に どのようにして不正な値を入力するか, あるいは不正な値を入力した場合にオラクルがどのように挙動するかといった問題は, 実装に強く依存する. ここでは $\langle g \rangle$ を含み $\langle g \rangle$ 上の群演算に相当する演算が定義された集合 G に於いて, α の加算連鎖により冪乗が実行されると仮定する.

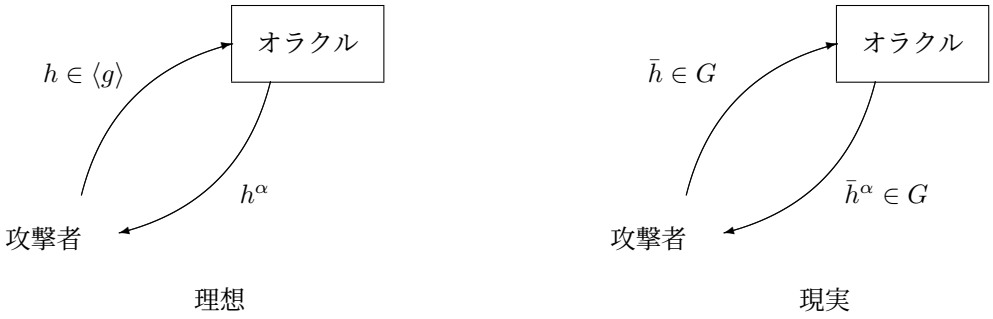

図 1: 理想と現実

現実の系を理想に近づける為には, 入力 $\bar{h} \notin \langle g \rangle$ に対して, 攻撃者に有利とならない系の挙動を定義しておかなくてはならない. 多くの場合不正な入力に対して系を停止する事によって攻撃を防ぐ事が出来る. しかし, より一般の暗号プロトコルに於いては, 系の停止が攻撃に直結する場合がある. 複雑な暗号プロトコルでは詳細な解析を必要とする. ここでは簡単の為, 不正な入力への対策として主に系が停止する事を考える.

3 Small Subgroup 攻撃

Small Subgroup 攻撃 [LL97] とは離散対数に基づく暗号への攻撃法の一つで, 暗号設計者が意図した巡回群上にない群要素を系に入力し, 通常取り出せない情報を引き出す攻撃の総称である. 離散対数問題に基づく暗号プロトコルは p を十分大きな素数として $\mathbb{Z}/p\mathbb{Z}^*$ の真部分群である素数位数巡回群 $\langle g \rangle$ を使って設計される. 演算コストやデータ長を抑える為, g の位数は $\mathbb{Z}/p\mathbb{Z}^*$ の位数より幾分小さく設計される事が多い. この時, $\mathbb{Z}/p\mathbb{Z}^*$ が小さい位数の巡回群を多く含んでいるとする.

攻撃者に上記のオラクルが与えられたとすると, 攻撃者はオラクルの出力を小さい位数 ℓ_i の巡回群上に潰してその離散対数 $\alpha \bmod \ell_i$ を求める事が出来る. 十分な数の互いに素な ℓ_i に対して $\alpha \bmod \ell_i$ が得られるなら, 中国人の剰余定理を用いて α を求める事が出来る.

$\mathbb{Z}/p\mathbb{Z}^*$ 位数 L が $\langle g \rangle$ の位数 ℓ に対して $\ell^2 \not| L$ として, 与えられた入力 $h \in \{0,1\}^*$ に対して, $h \in \langle g \rangle$ か否か判定を行う最も単純な方法は, 次の通り.

Step.1: $h \in G$ が成立するか.
Step.2: $h^\ell = 1$ が成立するか.

特殊な p に関しては, Step.2 をより高速な演算に置き換えることが出来る [HAK01]. また, 別の対策として出力を $\langle g \rangle$ に潰す方法もある. 但し, 良く用いられる設定の下では前者の方が高速である.

4 Invalid Curve 攻撃

Invalid Curve 攻撃 [ABMSV03] とは楕円曲線暗号系への攻撃法の一つで, 意図した楕円上にない点を系に入力し, 通常取り出せない情報を引き出す攻撃の総称である.

楕円曲線 E を

$$E/\mathbb{F}_q : y^2 =_2 x^3 + ax + b$$

とし, $\#g = \ell$ なる $g \in E(\mathbb{F}_q)$ に対して系が意図している巡回群を $\langle g \rangle$ とする.

ここでは オラクルは $\mathbb{F}_q \times \mathbb{F}_q$ を入力として受理し, Affine 座標あるいは Jacobian 座標の元での加算連鎖を用いた楕円スカラー倍を実行すると仮定する.

この時, 攻撃者がオラクルに対して楕円上にない点 $\bar{P} = (\bar{x}, \bar{y}) \in \mathbb{F}_q \times \mathbb{F}_q$ を入力すると, オラクルは

$$\bar{y}^2 = \bar{x}^3 + a\bar{x} + b'$$

なる b' を係数にもつ

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

なる楕円曲線の上での加算連鎖を実行してしまい, この楕円曲線上でのスカラー倍 $\alpha\bar{P}$ を出力する. 攻撃者は $\bar{P}$ を位数が小さい素数の積に分解出来るよう選ぶ. 攻撃者はオラクルの出力 $\alpha\bar{P}$ から Small Subgroup 攻撃と同様にして中国人剰余定理を用い α の値を導出する.

$\ell^2 \not| \#E(\mathbb{F}_q)$ なる場合に不正な点の判定を行う最も単純な方法は, 以下の通り.

Step.0: $x \in \mathbb{F}_q$ かつ $y \in \mathbb{F}_q$ が成立するか.
Step.1: $y^2 = x^3 + ax + b$ が成立するか.
Step.2: $\ell P = \mathcal{O}$ が成立するか.

$\ell = \#E(\mathbb{F}_q)$ なる場合は Step.2 は不要である. 幾つかの妥当な楕円曲線パラメタの設定では Step.2 をより高速な演算に置き換えることが出来る [HAK01].

5 pairing に基づく暗号系

pairing に基づく暗号系 (PBC) は一般の楕円曲線暗号より考慮すべき構造が幾分複雑である為より注意深い設計が必要である.

pairing e を使った暗号 (プロトコル) は, 通常

$$e : G_1 \times G_2 \to G_3$$

なる, 同型の巡回群 G_1, G_2, G_3 を仮定する. 一般に G_1, G_2 は楕円曲線上の同じ位数を持つ異なる巡回群であるが, 異なる巡回群の間に効率的に計算可能な双方向の同型写像が存在する場合には $G_1 = G_2$ とする事が出来る.

G_1, G_2 間の同型写像の計算可能性に関する事実 (または仮定) により pairing には 3 つの型がある [GPS06]. 即ち

Type 1: G_1, G_2 間に効率的に計算可能な同型写像が双方向に存在する.
Type 2: G_1, G_2 間に効率的に計算可能な一方向同型写像が存在する.
Type 3: G_1, G_2 間に効率的に計算可能な同型写像が存在しない.

一般に PBC を用いて上記のようなオラクルを構成する場合, 入力と出力が必ずしも同じ巡回群であるとは限らない. 例えば G_1 の元を入力し G_3 の元を得るようなオラクルを構成することが出来る. しかし, ここでは簡単の為入力と出力は同じ群であるとする.

効率的な実装を想定すると G_1 または G_2 のどちらか一方を $E(\mathbb{F}_q)$ またはその部分群に取る事が多い. ここでは G_1 を $E(\mathbb{F}_q)$ またはその部分群とする. そのような設定では G_1 への不正な入力または出力に関しては Invalid Curve 攻撃を想定すれば良い. 従って Type 1 の設定では楕円曲線上の点の入力を全て $E(\mathbb{F}_q)$ 上に取れば, 不正な点への対策はそれほど困難ではない.

G_3 は $\mathbb{F}_q$ の拡大体 $\mathbb{F}_{q^k}$ の乗法群の部分群である. 通常 $\#\mathbb{F}_{q^k}/\ell$ と ℓ は互いに素として良い. そのような設定では G_3 への不正な入力または出力に関しては Small Subgroup 攻撃を想定すれば良い.

6 Invalid Point 攻撃

一方 G_1 または G_2 の少なくとも一方は $E(\mathbb{F}_{q^k})$ の部分群でかつ $E(\mathbb{F}_q)$ に含まれない群に取らなくてはならない. 仮に G_2 が $E(\mathbb{F}_{q^k})$ の部分群でかつ $E(\mathbb{F}_q)$ に含まれない群であるとし g_2 を G_2 の生成元とする.

この時 入力 $P \in G_2$ に対して αP を返すオラクルが攻撃者に与えられているとする. 攻撃者はこのオラクルに対して $\bar{P} \notin G_2$ なる不正な点を入力して情報を得ようとする.

与えられた入力 $P = (x, y) \in \{0,1\}^*$ が G_2 の元であるか否かを判定するには, 一般には e_ℓ を Weil pairing として

Step.0: $x \in \mathbb{F}_{q^k}$ かつ $y \in \mathbb{F}_{q^k}$ が成立するか.
Step.1: $y^2 = x^3 + ax + b$ が成立するか.
Step.2: $\ell P = \mathcal{O}$ が成立するか.
Step.3: $e_\ell(P, g_2) = 1$ が成立するか.

を判定する必要がある.

ところで 上記 Step.3 は他の Step に比べ幾分重いので, なるべく実行したくない. 上記 Step.3 を省略した場合 $P \in E[\ell]$ である事しか確認できないが, Step.0 〜 Step.2 までを行えば, 少なくとも Small Subgroup 攻撃や Invalid Curve 攻撃のように, 異なる位数の元から情報が漏れるという事は無い. 従って, 上記 Step.3 を省略できないだろうかと考える事は妥当である. しかし, このような考えは必ずしも正しくない.

攻撃者は任意の $P_1 \in G_1$ 及び $P_2 \in G_2$ に対し $\bar{P} = P_1 + P_2$ とし Step.3 なしのオラクルに $\bar{P}$ および P_2 を入力する. このとき $\bar{P} \in E[\ell]$ であるから攻撃者は $\alpha\bar{P}$ および αP_2 を得ることが出来る. 従って

$$\alpha P_1 = \alpha\bar{P} - \alpha P_2$$

によって, αP_1 を得ることが出来る.

この事は Type 2 および Type 3 の場合に Step.3 を欠いたオラクルを持つ攻撃者は α に関する DH 問題を G_1 上で解決できる能力を持つ事を示しており, Step.3 付のオラクルを持つ攻撃者より多くの知識を得ている事を示している.

7 より軽い対策

ϕ をフロベニウス写像とし $\tau_\ell : E[\ell] \times E[\ell] \longrightarrow \mu_\ell$ を Tate pairing とする.

Step.0 〜 Step.2 までを実行していると仮定して Type 2 の場合に Step.3 の代わりに

$$\tau_\ell\left(\sum_{i=0}^{k-1}\phi^i P, (\phi - 1)g_2\right) = \tau_\ell\left(\sum_{i=0}^{k-1}\phi^i g_2, (\phi - 1)P\right)$$

を用いる事が出来る. $\sum_{i=0}^{k-1}\phi^i P$ や $\sum_{i=0}^{k-1}\phi^i g_2$ は $E(\mathbb{F}_q)$ 上の点であるので, Weil pairing のように full Miller アルゴリズムを必要とせず, Miller lite アルゴリズムを用いる事が出来る [KM05].

Type 3 の場合は同様に Step.0 〜 Step.2 までを実行していると仮定して Step.3 の代わりに

$$\sum_{i=0}^{k-1}\phi^i P = \mathcal{O}$$

を用いる事が出来る. k が合成数の場合には $\sum_{i=0}^{k-1}\phi^i$ を因数分解してより軽い検査式を作る事が出来る. また, k が 2 の倍数であるなら, P を圧縮表現により, 一般の $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ の半分のサイズで表現する事が可能で [KM05], 圧縮表現を用いる事で Step.3 そのものを省略可能である. 圧縮表現による Step.3 の省略は Type 2 へも応用できる.

8 まとめと課題

本論文では PBC における Invalid Point Attack を考察し, pairing の型が Type 2 の場合および Type 3 の場合に Weil pairing によるチェックを欠いたオラクルが攻撃者へ知識を漏らしている事を示した. 従って, Type 2 の場合および Type 3 の場合には, 与えられた $E(\mathbb{F}_{q^k})$ 上の点が例え $E[\ell]$ 上にあったとしても, 本当に目的の巡回群に入っているか否かをチェックする必要がある.

また, Type 2 及び Type 3 で幾つかの Weil pairing のコストを軽減する代替案を示した. これらの軽減策は $E(\mathbb{F}_{q^k})$ における楕円スカラー倍 (Step.2) を必要とする. このコストを軽減する事が今後の課題である.

参考文献

[ABMSV03] Adrian Antipa, Daniel Brown, Alfred Menezes, Rene Struik, and Scott Vanstone, "Validation of Elliptic Curve Public Keys," Proc. PKC 2003, LNCS 2567, pp. 211-223, 2003, Springer-Verlag Berlin Heidelberg 2003

[BaLS02] P.S.L.M.Barreto, B.Lynn, M.Scott, "Constructing elliptic curves with prescribed embedding degrees," Proc. SCN'2002, LNCS 2576, pp.257-267, Springer-Verlag, 2003

[BB04a] D. Boneh and X. Boyen, "Short signatures without random oracles," Proc. Advances in Cryptology — Eurocrypt 2004, LNCS 3027, pp.56-73, Springer-Verlag, 2004.

[BB04b] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," Proc. Advances in Cryptology — Crypto 2004, LNCS 3152 , pp. 443-459. Springer-Verlag, 2004.

[BF01] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," Proc. CRYPTO' 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001

[BLS02] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," Proc. ASIACRYPT'2001, LNCS 2248, pp.514-532, Springer-Verlag 2002,

[DEM02] R.Dupont, A.Enge, F.Morain, "Building curves with arbitrary small MOV degree over finite prime fields," http://eprint.iacr.org/2002/094/

[GPS06] S.D. Galbraith, K.G. Paterson, N.P. Smart, "Pairings for Cryptographers," http://eprint.iacr.org/2006/165.pdf

[HAK01] F. Hoshino, M. Abe, T. Kobayashi, "Lenient/Strict Batch Verification in Several Groups," Proc. the 4th International Conference on Information Security — ISC 2001, LNCS 2200, pp.81-94, Springer-Verlag, 2001.

[HSV06] F. Hess, N. Smart, F. Vercauteren, "The Eta Pairing Revisited," IEEE Transactions on Information Theory, volume 52, number 10, pp.4595-4602, 2006.

[JN01] A.Joux and K.Nguyen ,"Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups," http://eprint.iacr.org/2001/003/

[Jou00] A.Joux, "A one round protocol for tripartite Diffie-Hellman," Proc. ANTS IV, LNCS 1838, pp.385-394, Springer-Verlag, 2000

[KM05] N. Koblitz, A. Menezes, "Pairing-Based Cryptography at High Security Levels," http://eprint.iacr.org/2005/076.pdf

[LL97] C. Lim and P. Lee, "A key recovery attack on discrete log-based schemes using a prime order subgroup," Proc. Advances in Cryptology — CRYPTO'97, LNCS 1294, pp. 249-263, 1997, Springer-Verlag Berlin Heidelberg 1997

[Mil04] V.S. Miller, "The Weil Pairing, and Its Efficient Calculation," Journal of Cryptology, volume 17, number 4, pp235-261, 2004, Springer-Verlag New York, 2004.

[MNT01] A.Miyaji, M.Nakabayashi, S.Takano, "New explicit conditions of elliptic curve traces for FR-Reduction," IEICE Trans. Fundamentals, vol.E84-A, no.5, pp.1234-1243, May 2001

[MOV93] A.J.Menezes, T.Okamoto, S.A.Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Trans. IT,39, pp.1639-1646, 1993

[MSK02] S. Mitsunari, R. Sakai, M. Kasahara, "A New Traitor Tracing," Traitor Tracing, IEICE Trans. Fundamentals, vol. E85-A, No. 2, pp.481-484, 2002

[SB04] M.Scott, P.S.L.M.Barreto, "Generating more MNT elliptic curves," http://eprint.iacr.org/2004/058/

[Sch87] R.Schoof, "Nonsingular plane cubic curves over finite fields," J.Comb. Theory A, vol.46, pp.183-211, 1987

[SHUK03] T.Saito, F.Hoshino, S.Uchiyama, T. Kobayashi, "Candidate One-Way Functions on Non-Supersingular Elliptic Curves," Technical Report of IEICE. ISEC 2003-65 (2003-09)

[SHUK04] T.Saito, F.Hoshino, S.Uchiyama, T. Kobayashi, "Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems," IEICE Trans. Fundamentals, VOL.E87-A, NO.5, pp.1203-1205, May 2004

[SOK00] R. Sakai, K. Ohgishi, M. Kasahara, "Cryptosystems based on pairing," Proc. SCIS 2000

[Ver01] E.R.Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," Proc. Eurocrypt 2001, LNCS 2045, pp.195-210, Springer-Verlag 2001

[Wat69] W.C.Waterhouse, "Abelian varieties over finite fields," Ann. Sci. Ecole Norm. Sup., Ser.2, no.4, pp.521-560, 1969